Systemverwaltungshandbuch: Sicherheitsservices

Teilenr.: E23287
August 2011

Copyright © 2002, 2011, Oracle und/oder verbundene Unternehmen. Alle Rechte vorbehalten.

Diese Software und zugehörige Dokumentation werden im Rahmen eines Lizenzvertrages zur Verfügung gestellt, der Einschränkungen hinsichtlich Nutzung und Offenlegung enthält und durch Gesetze zum Schutz geistigen Eigentums geschützt ist. Sofern nicht ausdrücklich in Ihrem Lizenzvertrag vereinbart oder gesetzlich geregelt, darf diese Software weder ganz noch teilweise in irgendeiner Form oder durch irgendein Mittel zu irgendeinem Zweck kopiert, reproduziert, übersetzt, gesendet, verändert, lizenziert, übertragen, verteilt, ausgestellt, ausgeführt, veröffentlicht oder angezeigt werden. Reverse Engineering, Disassemblierung oder Dekompilierung der Software ist verboten, es sei denn, dies ist erforderlich, um die gesetzlich vorgesehene Interoperabilität mit anderer Software zu ermöglichen.

Die hier angegebenen Informationen können jederzeit und ohne vorherige Ankündigung geändert werden. Wir übernehmen keine Gewähr für deren Richtigkeit. Sollten Sie Fehler oder Unstimmigkeiten finden, bitten wir Sie, uns diese schriftlich mitzuteilen.

Wird diese Software oder zugehörige Dokumentation an die Regierung der Vereinigten Staaten von Amerika bzw. einen Lizenznehmer im Auftrag der Regierung der Vereinigten Staaten von Amerika geliefert, gilt Folgendes:

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065, USA.

Diese Software oder Hardware ist für die allgemeine Anwendung in verschiedenen Informationsmanagementanwendungen konzipiert. Sie ist nicht für den Einsatz in potenziell gefährlichen Anwendungen bzw. Anwendungen mit einem potenziellen Risiko von Personenschäden geeignet. Falls die Software oder Hardware für solche Zwecke verwendet wird, verpflichtet sich der Lizenznehmer, sämtliche erforderlichen Maßnahmen wie Fail Safe, Backups und Redundancy zu ergreifen, um den sicheren Einsatz dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihren verbundenen Unternehmen. Andere Namen und Bezeichnungen können Marken ihrer jeweiligen Inhaber sein.

Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Alle SPARC-Marken werden in Lizenz verwendet und sind Marken oder eingetragene Marken der SPARC International, Inc. AMD, Opteron, das AMD-Logo und das AMD Opteron-Logo sind Marken oder eingetragene Marken der Advanced Micro Devices. UNIX ist eine eingetragene Marke der The Open Group.

Diese Software oder Hardware und die zugehörige Dokumentation können Zugriffsmöglichkeiten auf Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Verluste, Kosten oder Schäden, die aufgrund des Zugriffs oder der Verwendung von Inhalten, Produkten und Serviceleistungen von Dritten entstehen.

111013@25097

Inhalt

Vorwort 25

Teil I Übersicht über die Sicherheit 29

1 Sicherheitsservices (Überblick) 31
Systemsicherheit 32
Kryptografische Services 33
Authentifizierungsservices 34
Authentifizierung mit Verschlüsselung 35
Prüfung 35
Sicherheitsrichtlinie 35

Teil II System-, Datei- und Gerätesicherheit 37

2 Verwalten von Rechnersicherheit (Übersicht) 39
Verbesserungen der Rechnersicherheit in der Solaris 10-Version 39
Steuern des Zugriffs auf ein Computersystem 40
Gewährleisten physischer Sicherheit 40
Steuern von Anmeldungen 41
Steuern des Zugriffs auf Dateien 47
Geräterichtlinie (Übersicht) 48
Gerätezuordnung (Übersicht) 49
Steuern des Zugriffs auf Rechnerressourcen 50
Beschränken und Überwachen von Superuser-Zugriffen 50
Konfigurieren von rollenbasierter Zugriffssteuerung zum Ersetzen des Superusers 50
Verhindern von unbeabsichtigten Verwendungsfehlern bei Rechnerressourcen 51
Beschränken von ausführbaren `setuid`-Dateien 52

Verwenden des Automated Security Enhancement Tool 53
Verwenden des Oracle Solaris Security Toolkit 53
Verwenden der Konfiguration "Secure by Default" 53
Verwenden von Ressourcenverwaltungsfunktionen 54
Verwenden von Oracle Solaris-Zonen 54
Überwachen der Verwendung von Rechnerressourcen 54
Überwachen von Dateiintegrität 55
Steuern von Zugriff auf Dateien 55
Schützen von Dateien durch Verschlüsselung 55
Verwenden von Zugriffssteuerungslisten 55
Gemeinsames Nutzen von Dateien auf Rechnern 56
Beschränken des `root`-Zugriffs auf gemeinsam genutzte Dateien 56
Steuern von Netzwerkzugriff 57
Netzwerksicherheitsmechanismen 57
Authentifizierung und Autorisierung für Remote-Zugriff 58
Firewall-Systeme 60
Verschlüsselung und Firewall-Systeme 61
Melden von Sicherheitsproblemen 62

3 Steuern des Zugriffs auf Systeme (Aufgaben) 63
Steuern von Systemzugriff (Übersicht der Schritte) 63
Schützen von Anmeldungen und Passwörtern (Übersicht der Schritte) 64
Schützen von Anmeldungen und Passwörtern 65
▼ So zeigen Sie den Anmeldestatus eines Benutzers an 65
▼ So zeigen Sie Benutzer ohne Passwort an 66
▼ So deaktivieren Sie Benutzeranmeldungen vorübergehend 67
▼ So überwachen Sie fehlgeschlagene Anmeldeversuche 67
▼ So überwachen Sie alle fehlgeschlagenen Anmeldeversuche 68
▼ So erstellen Sie ein Einwahl-Passwort 70
▼ So deaktivieren Sie Einwahl-Anmeldungen vorübergehend 72
Ändern des Passwortalgorithmus (Übersicht der Schritte) 72
Ändern des Standardalgorithmus zur Passwortverschlüsselung 73
▼ So geben Sie einen Algorithmus zur Passwortverschlüsselung an 73
▼ So geben Sie einen neuen Passwortalgorithmus für eine NIS-Domain an 74
▼ So geben Sie einen neuen Passwortalgorithmus für eine NIS+-Domain an 75

▼ So geben Sie einen neuen Passwortalgorithmus für eine LDAP-Domain an 75
▼ So installieren Sie ein Passwortverschlüsselungsmodul eines anderen Anbieters 76
Überwachen und Beschränken des Superusers (Übersicht der Schritte) 77
Überwachen und Beschränken des Superusers 77
▼ So überwachen Sie, wer den Befehl su ausführt 78
▼ So beschränken und überwachen Sie Superuser-Anmeldungen 78
SPARC: Steuern von Zugriff auf Systemhardware (Übersicht der Schritte) 80
Steuern des Zugriffs auf Systemhardware 80
▼ So legen Sie fest, dass ein Passwort für Hardwarezugriff erforderlich ist 80
▼ So deaktivieren Sie die Abbruch-Sequenz eines Systems 81

4 Steuern des Zugriffs auf Geräte (Aufgaben) 83
Konfigurieren von Geräten (Übersicht der Schritte) 83
Konfigurieren der Geräterichtlinie (Übersicht der Schritte) 84
Konfigurieren der Geräterichtlinie 84
▼ So zeigen Sie die Geräterichtlinie an 84
▼ So ändern Sie die Geräterichtlinie auf einem vorhandenen Gerät 85
▼ So prüfen Sie Änderungen der Geräterichtlinie 86
▼ So rufen Sie IP MIB-II-Informationen von einem /dev/*-Gerät ab 86
Verwalten der Gerätezuordnung (Übersicht der Schritte) 87
Verwalten der Gerätezuordnung 88
▼ So aktivieren Sie die Zuordnung eines Geräts 88
▼ So autorisieren Sie Benutzer für die Zuordnung eines Geräts 89
▼ So zeigen Sie Zuordnungsinformationen zu einem Gerät an 90
▼ Erzwingen der Gerätezuordnung 90
▼ Erzwingen der Aufhebung der Gerätezuordnung 91
▼ So ändern Sie die Zuordenbarkeit von Geräten 91
▼ So prüfen Sie die Gerätezuordnung 92
Zuordnen von Geräten (Übersicht der Schritte) 93
Zuordnen von Geräten 93
▼ So ordnen Sie ein Gerät zu 93
▼ So hängen Sie ein zugeordnetes Gerät ein 94
▼ So heben Sie die Zuordnung eines Geräts auf 97
Geräteschutz (Referenz) 98
Befehle der Geräterichtlinie 98

Gerätezuordnung 99

5 Verwenden von Basic Audit Reporting Tool (Aufgaben) 107
Basic Audit Reporting Tool (Übersicht) 107
Funktionen von BART 108
Komponenten von BART 108
Verwenden von BART (Übersicht der Schritte) 111
Verwenden von BART (Aufgaben) 111
Sicherheitsüberlegungen zu BART 112
▼ So erstellen Sie ein Manifest 112
▼ So passen Sie ein Manifest an 114
▼ So vergleichen Sie Manifeste für das gleiche System über einen längeren Zeitraum 118
▼ So vergleichen Sie Manifeste von verschiedenen Systemen 120
▼ So passen Sie einen BART-Bericht durch Angeben von Dateiattributen an 123
▼ So passen Sie einen BART-Bericht durch eine Regeldatei an 124
Manifeste, Regeldateien und Berichte von BART (Referenz) 125
Format der BART-Manifest-Datei 125
Format der BART-Regeldatei 126
Berichterstellung bei BART 128

6 Steuern des Zugriffs auf Dateien (Aufgaben) 131
Schützen von Dateien mithilfe von UNIX-Berechtigungen 131
Befehle zum Anzeigen und Schützen von Dateien 131
Datei- und Verzeichniseigentümerschaft 132
UNIX-Dateiberechtigungen 133
Besondere Dateiberechtigungen (`setuid`, `setgid` und Sticky Bit) 134
`umask`-Standardwert 135
Dateiberechtigungsmodi 136
Schützen von UFS-Dateien mithilfe von Zugriffssteuerungslisten 138
ACL-Einträge für UFS-Dateien 140
ACL-Einträge für UFS-Verzeichnisse 140
Befehle zum Verwalten von UFS-ACLs 141
Vermeiden von Sicherheitsrisiken in Verbindung mit ausführbaren Dateien 141
Schützen von Dateien (Übersicht der Schritte) 142
Schützen von Dateien mithilfe von UNIX-Berechtigungen (Übersicht der Schritte) 143

▼ So zeigen Sie Dateiinformationen an ... 143
▼ So ändern Sie den Eigentümer einer lokalen Datei ... 144
▼ So ändern Sie die Gruppeneigentümerschaft einer Datei ... 145
▼ So ändern Sie die Dateiberechtigungen im symbolischen Modus ... 146
▼ So ändern Sie Dateiberechtigungen im absoluten Modus ... 147
▼ So ändern Sie besondere Dateiberechtigungen im absoluten Modus ... 148
Schützen von UFS-Dateien mit ACLs (Übersicht der Schritte) ... 149
▼ So stellen Sie fest, ob eine Datei über eine ACL verfügt ... 149
▼ So fügen Sie einer Datei ACL-Einträge hinzu ... 150
▼ So kopieren Sie eine ACL ... 152
▼ So ändern Sie die ACL-Einträge für eine Datei ... 152
▼ So löschen Sie ACL-Einträge aus einer Datei ... 153
▼ So zeigen Sie ACL-Einträge für eine Datei an ... 153
Schützen vor Programmen mit Sicherheitsrisiko (Übersicht der Schritte) ... 155
▼ So suchen Sie Dateien mit besonderen Dateiberechtigungen ... 155
▼ So hindern Sie Programme an der Verwendung ausführbarer Stacks ... 156

7 Verwenden von Automated Security Enhancement Tool (Aufgaben) ... 159
Automated Security Enhancement Tool (ASET) ... 159
ASET-Sicherheitsebenen ... 160
ASET-Aufgabenliste ... 161
ASET-Ausführungsprotokoll ... 164
ASET-Berichte ... 165
ASET-Master-Dateien ... 167
ASET-Umgebungsdatei (`asetenv`) ... 168
Konfigurieren von ASET ... 168
Wiederherstellen der von ASET geänderten Systemdateien ... 171
Netzwerkbetrieb mit dem NFS-System ... 172
ASET-Umgebungsvariablen ... 173
Beispiele für ASET-Dateien ... 176
Ausführen von ASET (Übersicht der Schritte) ... 178
▼ So führen Sie ASET interaktiv aus ... 178
▼ So führen Sie ASET in regelmäßigen Abständen aus ... 180
▼ So halten Sie die regelmäßige Ausführung von ASET an ... 180
▼ So erfassen Sie ASET-Berichte auf einem Server ... 181

Fehlerbehebung bei ASET-Problemen 182
ASET-Fehlermeldungen 182

Teil III Rollen, Berechtigungsprofile und Berechtigungen 187

8 Verwenden von Rollen und Berechtigungen (Übersicht) 189
Neuerungen bei RBAC 189
Rollenbasierte Zugriffssteuerung (Übersicht) 190
RBAC: eine Alternative zum Superuser-Modell 190
Oracle Solaris RBAC-Elemente und Basiskonzepte 193
Berechtigungseskalation 196
RBAC-Autorisierungen 196
Autorisierungen und Berechtigungen 197
Privilegierte Anwendungen und RBAC 197
RBAC-Berechtigungsprofile 198
RBAC-Rollen 199
Profil-Shells und RBAC 200
Name Service-Bereich und RBAC 200
Sicherheitsüberlegungen bei direkter Zuweisung von Sicherheitsattributen 201
Berechtigungen (Übersicht) 201
Berechtigungen zum Schutz von Kernel-Prozessen 202
Berechtigungsbeschreibungen 203
Administrative Unterschiede auf einem System mit Berechtigungen 204
Berechtigungen und Systemressourcen 205
Implementieren von Berechtigungen 206
Zuweisen von Berechtigungen zu Prozessen 207
Zuweisen von Berechtigungen 208
Berechtigungen und Geräte 210
Berechtigungen und Fehlersuche 211

9 Rollenbasierte Zugriffssteuerung (Aufgaben) 213
Verwenden von RBAC (Übersicht der Schritte) 213
Konfigurieren von RBAC (Übersicht der Schritte) 214
Konfigurieren von RBAC 215

▼ So planen Sie die RBAC-Implementierung 215
▼ So können Sie eine Rolle mit der GUI erstellen und zuweisen 218
▼ So erstellen Sie eine Rolle über die Befehlszeile 221
▼ So weisen Sie eine Rolle einem lokalen Benutzer zu 224
▼ So prüfen Sie Rollen 225
▼ So wandeln Sie den `root`-Benutzer in eine Rolle um 226
Verwenden von Rollen (Übersicht der Schritte) 229
Verwenden von Rollen 230
▼ So nehmen Sie eine Rolle in einem Terminalfenster an 230
▼ So nehmen Sie eine Rolle in der Solaris Management Console an 232
Verwalten von RBAC (Übersicht der Schritte) 233
Verwalten von RBAC 234
▼ So ändern Sie das Passwort einer Rolle 234
▼ So ändern Sie die Eigenschaften einer Rolle 236
▼ So erstellen oder ändern Sie ein Berechtigungsprofil 238
▼ So ändern Sie die RBAC-Eigenschaften eines Benutzers 241
▼ So fügen Sie RBAC-Eigenschaften zu Legacy-Anwendungen hinzu 243

10 Rollenbasierte Zugriffssteuerung (Übersicht) 247
Inhalt der Berechtigungsprofile 247
Berechtigungsprofil "Primary Administrator" 248
Berechtigungsprofil "System Administrator" 249
Berechtigungsprofil "Operator" 249
Berechtigungsprofil "Printer Management" 250
Berechtigungsprofil "Basic Solaris User" 250
Berechtigungsprofil "All" 251
Reihenfolge der Berechtigungsprofile 251
Anzeigen des Inhalts von Berechtigungsprofilen 252
Autorisierungsbenennung und -delegation 252
Autorisierungs-Namenskonventionen 252
Beispiel für Autorisierungsgranularität 253
Delegationsautorität in Autorisierungen 253
Datenbanken, die RBAC unterstützen 253
RBAC-Datenbankbeziehungen 254
RBAC-Datenbanken und die Naming Services 255

Datenbank `user_attr` 255
Datenbank `auth_attr` 256
Datenbank `prof_attr` 258
Datenbank `exec_attr` 259
Datei `policy.conf` 260
RBAC-Befehle 261
Befehle zum Verwalten von RBAC 261
Befehle, die Autorisierungen erfordern 262

11 Berechtigungen (Aufgaben) 265
Verwalten und Verwenden von Berechtigungen (Übersicht der Schritte) 265
Verwalten von Berechtigungen (Übersicht der Schritte) 266
Verwalten von Berechtigungen 266
▼ So legen Sie die Berechtigungen auf einem Prozess fest 267
▼ So legen Sie die für ein Programm erforderlichen Berechtigungen fest 268
▼ So fügen Sie Berechtigungen zu einem Befehl hinzu 270
▼ So weisen Sie Berechtigungen einem Benutzer oder einer Rolle zu 271
▼ So begrenzen Sie die Berechtigungen eines Benutzers oder einer Rolle 272
▼ So führen Sie ein Shell-Skript mit privilegierten Befehlen aus 274
Festlegen Ihrer Berechtigungen (Übersicht der Schritte) 275
Festlegen Ihrer zugewiesenen Berechtigungen 275
▼ So legen Sie die Ihnen direkt zugewiesenen Berechtigungen fest 275
▼ So legen Sie die ausführbaren privilegierten Befehle fest 277
▼ So legen Sie die von einer Rolle ausführbaren privilegierten Befehle fest 278

12 Berechtigungen (Referenz) 281
Administrative Befehle zum Verarbeiten von Berechtigungen 281
Dateien mit Berechtigungsinformationen 282
Berechtigungen und Prüfung 283
Verhindern von Berechtigungseskalation 284
Legacy-Anwendungen und das Berechtigungsmodell 285

Teil IV Kryptografische Services 287

13 Oracle Solaris Cryptographic Framework (Übersicht) 289
Neuerungen bei Oracle Solaris Cryptographic Framework 289
Oracle Solaris Cryptographic Framework 290
Terminologie in Oracle Solaris Cryptographic Framework 291
Geltungsbereich von Oracle Solaris Cryptographic Framework 292
Administrative Befehle in Oracle Solaris Cryptographic Framework 293
Befehle auf Benutzerebene in Oracle Solaris Cryptographic Framework 293
Binäre Signaturen für Drittanbietersoftware 294
Plugins von Oracle Solaris Cryptographic Framework 294
Kryptografische Services und Zonen 295

14 Oracle Solaris Cryptographic Framework (Aufgaben) 297
Verwenden von Cryptographic Framework (Übersicht der Schritte) 297
Schützen von Dateien mit Oracle Solaris Cryptographic Framework (Übersicht der Schritte) 298
Schützen von Dateien mit Cryptographic Framework (Aufgaben) 298
▼ So generieren Sie einen symmetrischen Schlüssel mit dem Befehl `dd` 298
▼ So generieren Sie einen symmetrischen Schlüssel mit dem Befehl `pktool` 301
▼ So berechnen Sie den Digest einer Datei 304
▼ So berechnen Sie den MAC einer Datei 305
▼ So entschlüsseln und verschlüsseln Sie eine Datei 307
Verwalten von Cryptographic Framework (Übersicht der Schritte) 309
Verwalten von Cryptographic Framework (Aufgaben) 310
▼ So listen Sie verfügbare Provider auf 310
▼ So fügen Sie einen Softwareprovider hinzu 313
▼ So verhindern Sie die Verwendung eines Mechanismus auf Benutzerebene 314
▼ So verhindern Sie die Verwendung eines Kernel-Modul-Softwareproviders 316
▼ So listen Sie Hardwareprovider auf 318
▼ So deaktivieren Sie Mechanismen und Funktionen eines Hardwareproviders 319
▼ So führen Sie eine Aktualisierung oder einen Neustart aller kryptografischen Services durch 321

15 Oracle Solaris Key Management Framework 323
Verwalten von Public-Key-Technologien 323
Dienstprogramme von Key Management Framework 324
KMF-Richtlinienverwaltung 325
KMF-Schlüsselspeicherverwaltung 325
Verwenden von Key Management Framework (Übersicht der Schritte) 325
Verwenden von Key Management Framework (Aufgaben) 326
▼ So erstellen Sie ein Zertifikat mit dem Befehl `pktool gencert` 326
▼ So importieren Sie ein Zertifikat in den Schlüsselspeicher 327
▼ So exportieren Sie ein Zertifikat und einen privaten Schlüssel im PKCS #12-Format 329
▼ So generieren Sie einen Passwortsatz mit dem Befehl `pktool setpin` 330

Teil V Authentifizierungsservices und sichere Kommunikation 333

16 Verwenden von Authentifizierungsservices (Aufgaben) 335
Übersicht zu Secure RPC 335
NFS-Services und Secure RPC 335
DES-Verschlüsselung mit Secure NFS 336
Kerberos-Authentifizierung 336
Diffie-Hellman-Authentifizierung und Secure RPC 336
Verwalten von Secure RPC (Übersicht der Schritte) 340
Verwalten von Authentifizierung mit Secure RPC (Aufgaben) 341
▼ So starten Sie den Schlüsselserver mit Secure RPC neu 341
▼ So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS+-Host ein 342
▼ So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS+-Benutzer ein 343
▼ So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS-Host ein 344
▼ So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS-Benutzer ein 344
▼ So können Sie NFS-Dateien mit Diffie-Hellman-Authentifizierung gemeinsam nutzen . 346

17 Verwenden von PAM 347
PAM (Übersicht) 347
Vorteile der Verwendung von PAM 347
Einführung zum PAM-Framework 348
Änderungen am PAM in der Version Solaris 10 349

PAM (Aufgaben) 350
PAM (Übersicht der Schritte) 350
Planen Ihrer PAM-Implementierung 351
▼ So fügen Sie ein PAM-Modul hinzu 352
▼ So verhindern Sie mit PAM den Zugriff von Remote-Systemen im Rhost-Stil 353
▼ So protokollieren Sie PAM-Fehlerberichte 353
PAM-Konfiguration (Referenz) 353
PAM-Konfigurationsdateisyntax 354
Funktionsweise von PAM-Stacking 354
Beispiel für PAM-Stacking 358

18 Verwenden von SASL 361
SASL (Übersicht) 361
SASL (Referenz) 362
SASL-Plugins 362
SASL-Umgebungsvariable 362
SASL-Optionen 363

19 Verwenden von Oracle Solaris Secure Shell (Aufgaben) 365
Oracle Solaris Secure Shell (Übersicht) 365
Oracle Solaris Secure Shell-Authentifizierung 366
Secure Shell in the Enterprise 368
Oracle Solaris Secure Shell und das OpenSSH-Projekt 368
Oracle Solaris Secure Shell (Übersicht der Schritte) 370
Konfigurieren von Oracle Solaris Secure Shell (Übersicht der Schritte) 370
Konfigurieren von Oracle Solaris Secure Shell (Aufgaben) 370
▼ So richten Sie eine hostbasierte Authentifizierung für Secure Shell ein 371
▼ So aktivieren Sie Secure Shell v1 373
▼ So konfigurieren Sie die Port-Weiterleitung in Secure Shell 374
Verwenden von Oracle Solaris Secure Shell (Übersicht der Schritte) 375
Verwenden von Oracle Solaris Secure Shell (Aufgaben) 376
▼ So generieren Sie ein Paar aus öffentlichem und privatem Schlüssel für Secure Shell 376
▼ So ändern Sie den Passwortsatz für einen privaten Secure Shell-Schlüssel 378
▼ So melden Sie sich bei einem Remote-Host mithilfe von Secure Shell an 379
▼ So reduzieren Sie die Aufforderungen zur Passworteingabe in Secure Shell 380

▼ So richten Sie den Befehl `ssh-agent` zur automatischen Ausführung in CDE ein 381
▼ So verwenden Sie die Port-Weiterleitung in Secure Shell 382
▼ So kopieren Sie Dateien mit Secure Shell 384
▼ So richten Sie Standardverbindungen mit Hosts außerhalb einer Firewall ein 385

20 Oracle Solaris Secure Shell (Referenz) 389
Eine typische Secure Shell-Sitzung 389
Sitzungsmerkmale in Secure Shell 390
Authentifizierung und Schlüsselaustausch in Secure Shell 390
Befehlsausführung und Datenweiterleitung in Secure Shell 391
Client- und Serverkonfiguration in Secure Shell 392
Clientkonfiguration in Secure Shell 392
Serverkonfiguration in Secure Shell 392
Schlüsselwörter in Secure Shell 393
Hostspezifische Parameter in Secure Shell 396
Secure Shell und Variablen für die Anmeldeumgebung 397
Verwalten bekannter Hosts in Secure Shell 398
Secure Shell-Pakete und Initialisierung 398
Secure Shell-Dateien 399
Secure Shell-Befehle 401

Teil VI Kerberos-Service 405

21 Einführung zum Kerberos-Service 407
Allgemeine Informationen zum Kerberos-Service 407
Funktionsweise des Kerberos-Service 408
Erstauthentifizierung: das Ticket-gewährende Ticket 409
Nachfolgende Kerberos-Authentifizierungen 411
Die Kerberos-Remote-Anwendungen 412
Kerberos-Hauptelemente 413
Kerberos-Bereiche 413
Kerberos-Server 414
Kerberos-Sicherheitsservices 415
Die Komponenten verschiedener Kerberos-Versionen 416

Kerberos-Komponenten 416
Kerberos-Ergänzungen für die Version Solaris 10 5/08 418
Kerberos-Ergänzungen für die Version Solaris 10 8/07 418
Kerberos-Ergänzungen für die Version Solaris 10 6/06 418
Kerberos-Erweiterungen in der Version Solaris 10 3/05 418
Kerberos-Komponenten in der Version Solaris 9 421
SEAM 1.0.2-Komponenten 421
Kerberos-Komponenten in der Version Solaris 8 422
SEAM 1.0.1-Komponenten 422
SEAM 1.0-Komponenten 423

22 Planen des Kerberos-Service 425
Notwendigkeit des Planens von Kerberos-Bereitstellungen 425
Planen von Kerberos-Bereichen 426
Bereichsnamen 426
Anzahl der Bereiche 426
Bereichshierarchie 427
Zuordnen von Hostnamen zu Bereichen 427
Client- und Service-Hauptelementnamen 428
Ports für die KDC- und Admin-Services 429
Die Anzahl der Slave-KDCs 429
Zuordnen von GGS-Berechtigungsnachweisen zu UNIX-Berechtigungsnachweisen 430
Automatische Benutzermigration in einen Kerberos-Bereich 430
Entscheidung über das zu verwendende System für die Datenbankweitergabe 431
Synchronisierung von Uhren innerhalb eines Bereichs 431
Optionen zur Clientkonfiguration 431
Verbessern der Sicherheit bei der Clientanmeldung 432
Optionen zur KDC-Konfiguration 433
Kerberos-Verschlüsselungstypen 433
Onlinehilfe-URL im Graphical Kerberos Administration Tool 434

23 Konfigurieren des Kerberos-Service (Aufgaben) 435
Konfigurieren des Kerberos-Service (Übersicht der Schritte) 435
Konfigurieren zusätzlicher Kerberos-Services (Übersicht der Schritte) 436
Konfigurieren von KDC-Servern 437

▼ So konfigurieren Sie ein Master-KDC manuell ... 438
▼ So konfigurieren Sie ein KDC zur Verwendung eines LDAP-Datenservers ... 443
▼ So konfigurieren Sie ein Slave-KDC manuell ... 451
▼ So aktualisieren Sie die Ticket Granting Service-Schlüssel auf einem Master-Server ... 455
Konfigurieren von bereichsübergreifender Authentifizierung ... 456
▼ So richten Sie eine hierarchische bereichsübergreifende Authentifizierung ein ... 456
▼ So richten Sie eine direkte bereichsübergreifende Authentifizierung ein ... 457
Konfigurieren von Kerberos-Netzwerkanwendungsservern ... 458
▼ So konfigurieren Sie einen Kerberos-Netzwerkanwendungsserver ... 459
Konfigurieren von Kerberos-NFS-Servern ... 461
▼ So konfigurieren Sie Kerberos-NFS-Server ... 462
▼ So erstellen Sie eine Berechtigungsnachweistabelle ... 463
▼ So fügen Sie der Berechtigungstabelle einen einzelnen Eintrag hinzu ... 464
▼ So ordnen Sie Berechtigungsnachweise zwischen Bereichen zu ... 465
▼ So richten Sie eine sichere NFS-Umgebung mit mehreren Kerberos-Sicherheitsmodi ein ... 466
Konfigurieren von Kerberos-Clients ... 468
Konfigurieren von Kerberos-Clients (Übersicht der Schritte) ... 468
▼ So erstellen Sie ein Kerberos-Clientinstallationsprofil ... 469
▼ So konfigurieren Sie einen Kerberos-Client automatisch ... 469
▼ So konfigurieren Sie einen Kerberos-Client interaktiv ... 471
▼ So konfigurieren Sie einen Kerberos-Client manuell ... 472
▼ So deaktivieren Sie die Überprüfung des TGT (Ticket Granting Ticket) ... 478
▼ So greifen Sie auf ein durch Kerberos geschütztes NFS-Dateisystem als `root`-Benutzer zu ... 478
▼ So konfigurieren Sie eine automatische Migration von Benutzern in einem Kerberos-Bereich ... 480
Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients ... 482
Austauschen von Master-KDC und Slave-KDC ... 484
▼ So konfigurieren Sie ein austauschbares Slave-KDC ... 484
▼ So tauschen Sie ein Master-KDC gegen ein Slave-KDC aus ... 484
Verwalten der Kerberos-Datenbank ... 489
Backup und Weitergabe der Kerberos-Datenbank ... 489
▼ So erstellen Sie ein Backup der Kerberos-Datenbank ... 491
▼ So stellen Sie die Kerberos-Datenbank wieder her ... 492
▼ So konvertieren Sie eine Kerberos-Datenbank nach einem Server-Upgrade ... 492

▼ So konfigurieren Sie ein Master-KDC zur Verwendung der inkrementellen Weitergabe 493
▼ So konfigurieren Sie ein Slave-KDC zur Verwendung der inkrementellen Weitergabe ... 495
▼ So konfigurieren Sie ein Slave-KDC zur Verwendung der vollständigen Weitergabe 496
▼ So überprüfen Sie die Synchronisierung der KDC-Server 500
▼ So führen Sie eine manuelle Weitergabe der Kerberos-Datenbank an Slave-KDCs durch 501
Einrichten von paralleler Weitergabe 502
Konfigurationsschritte zum Einrichten einer parallelen Weitergabe 502
Verwalten der Stash-Datei 503
▼ So entfernen Sie eine Stash-Datei 504
Verwalten eines KDC auf einem LDAP-Verzeichnisserver 504
▼ So kombinieren Sie Kerberos-Hauptelementattribute mit einem nicht zu Kerberos gehörenden Objektklassentyp 504
▼ So löschen Sie einen Bereich auf einem LDAP-Verzeichnisserver 505
Erhöhen der Sicherheit auf Kerberos-Servern 506
▼ So aktivieren Sie nur kerberisierte Anwendungen 506
▼ So beschränken Sie den Zugriff auf KDC-Server 506
▼ So verwenden Sie eine Wörterbuchdatei zur Erhöhung der Passwortsicherheit 507

24 Kerberos-Fehlermeldungen und -Fehlerbehebung 509
Kerberos-Fehlermeldungen 509
Fehlermeldungen des SEAM-Tools 509
Häufige Kerberos-Fehlermeldungen (A – M) 510
Häufige Kerberos-Fehlermeldungen (N – Z) 519
Kerberos-Fehlerbehebung 523
Probleme mit dem Format der Datei `krb5.conf` 523
Probleme bei der Weitergabe der Kerberos-Datenbank 523
Probleme beim Einhängen eines kerberisierten NFS-Dateisystems 523
Probleme beim Authentifizieren als `root` 524
Überwachen der Zuordnungen von GSS-Berechtigungsnachweisen zu UNIX-Berechtigungsnachweisen 525

25 Verwalten von Kerberos-Hauptelementen und Richtlinien (Aufgaben) 527
Möglichkeiten zur Verwaltung von Kerberos-Hauptelementen und -Richtlinien 527
SEAM-Tool 528

Befehlszeilenäquivalente des SEAM-Tools 529
Die einzige vom SEAM-Tool geänderte Datei 530
Druck- und Onlinehilfefunktionen des SEAM-Tools 530
Arbeiten mit großen Listen im SEAM-Tool 530
▼ So starten Sie das SEAM-Tool 531
Verwalten von Kerberos-Hauptelementen 532
Verwalten von Kerberos-Hauptelementen (Übersicht der Schritte) 532
Automatisieren der Erstellung neuer Kerberos-Hauptelemente 533
▼ So zeigen Sie die Liste der Kerberos-Hauptelemente an 534
▼ So zeigen Sie die Attribute eines Kerberos-Hauptelements an 536
▼ So erstellen Sie ein neues Kerberos-Hauptelement 538
▼ So duplizieren Sie ein Kerberos-Hauptelement 541
▼ So ändern Sie ein Kerberos-Hauptelement 542
▼ So löschen Sie ein Kerberos-Hauptelement 543
▼ So richten Sie Standardwerte zur Erstellung neuer Kerberos-Hauptelemente ein 543
▼ So ändern Sie die Kerberos-Administratorberechtigungen 544
Verwalten von Kerberos-Richtlinien 546
Verwalten von Kerberos-Richtlinien (Übersicht der Schritte) 546
▼ So zeigen Sie die Liste der Kerberos-Richtlinien an 547
▼ So zeigen Sie die Attribute einer Kerberos-Richtlinie an 549
▼ So erstellen Sie eine neue Kerberos-Richtlinie 551
▼ So duplizieren Sie eine Kerberos-Richtlinie 553
▼ So ändern Sie eine Kerberos-Richtlinie 553
▼ So löschen Sie eine Kerberos-Richtlinie 554
SEAM-Tool-Referenz 555
Beschreibungen der SEAM-Tool-Fensterbereiche 555
Verwenden des SEAM-Tools mit eingeschränkten Kerberos-Administratorberechtigungen 558
Verwalten von Schlüsseltabellendateien 560
Verwalten von Schlüsseltabellendateien (Übersicht der Schritte) 561
▼ So fügen Sie ein Service-Hauptelement von Kerberos zu einer Schlüsseltabellendatei hinzu 562
▼ So entfernen Sie ein Service-Hauptelement aus einer Schlüsseltabellendatei 564
▼ So zeigen Sie die Schlüsselliste (Hauptelemente) in einer Schlüsseltabellendatei an 565
▼ So deaktivieren Sie vorübergehend die Authentifizierung für einen Service auf einem Host 565

26 Verwenden von Kerberos-Anwendungen (Aufgaben) 569
Kerberos-Ticketverwaltung 569
Automatisches Abrufen von Tickets 569
Erstellen eines Kerberos-Tickets 570
Anzeigen von Kerberos-Tickets 571
Löschen von Kerberos-Tickets 572
Kerberos-Passwortverwaltung 573
Hinweis zum Auswählen eines Passworts 573
Ändern Ihres Passworts 574
Gewähren von Zugriff auf Ihr Konto 576
Kerberos-Benutzerbefehle 578
Übersicht über kerberisierte Befehle 579
Weiterleiten von Kerberos-Tickets 581
Verwenden kerberisierter Befehle (Beispiele) 583

27 Der Kerberos-Service (Referenz) 587
Kerberos-Dateien 587
Kerberos-Befehle 589
Kerberos-Dämonen 590
Kerberos-Terminologie 591
Kerberos-spezifische Terminologie 591
Authentifizierungsspezifische Terminologie 591
Typen von Tickets 593
Funktionsweise des Kerberos-Authentifizierungssystems 598
Interaktion des Kerberos-Service mit DNS und der Datei `nsswitch.conf` 598
Erhalten von Zugriff auf einen Service mit Kerberos 598
Abrufen eines Berechtigungsnachweises für den Ticket-gewährenden Service 599
Abrufen eines Berechtigungsnachweises für einen Server 600
Abrufen von Zugriff auf einen bestimmten Service 601
Verwenden von Kerberos-Verschlüsselungstypen 602
Verwenden der Tabelle `gsscred` 604
Wesentliche Unterschiede zwischen Oracle Solaris Kerberos und MIT Kerberos 605

Teil VII Prüfung bei Oracle Solaris 607

28 Prüfung bei Oracle Solaris (Übersicht) 609
Was ist eine Prüfung? 609
Wie funktioniert eine Prüfung? 611
Welcher Zusammenhang besteht zwischen Prüfung und Sicherheit? 612
Terminologie und Konzepte der Prüfung 613
Prüfereignisse 614
Prüfklassen und Vorauswahl 615
Prüfdatensätze und Prüf-Token 616
Prüf-Plugin-Module 617
Prüfprotokolle 617
Speichern des Prüfpfads 619
Untersuchen des Prüfpfads 620
Prüfung auf Systemen mit Oracle Solaris-Zonen 620
Erweiterungen der Prüffunktionen in der Solaris 10-Version 621

29 Planen der Oracle Solaris-Prüfung 623
Planen der Oracle Solaris-Prüfung (Übersicht der Schritte) 623
Planen der Oracle Solaris-Prüfung (Aufgaben) 624
▼ So planen Sie die Prüfung der Zonen 624
▼ So planen Sie Speicherplatz für Prüfdatensätze 626
▼ So planen Sie die zu prüfenden Personen und Objekte 627
Festlegen der Prüfrichtlinien 629
Prüfrichtlinien für asynchrone und synchrone Ereignisse 632
Steuerung des Prüfungsaufwands 633
Höhere Verarbeitungszeit der Prüfungsdaten 633
Aufwand für Analyse der Prüfungsdaten 634
Aufwand für Speicherung der Prüfungsdaten 634
Effiziente Prüfung 635

30 Verwalten der Oracle Solaris-Prüfung (Aufgaben) 637
Prüfung bei Oracle Solaris (Übersicht der Schritte) 637
Konfigurieren der Prüfdateien (Übersicht der Schritte) 638

Konfigurieren von Prüfdateien (Aufgaben) 639
▼ So ändern Sie die Datei `audit_control` 639
▼ So konfigurieren Sie `syslog`-Prüfprotokolle 641
▼ So ändern Sie die Prüfmerkmale eines Benutzers 644
▼ So fügen Sie eine Prüfklasse hinzu 646
▼ So ändern Sie die Klassenmitgliedschaft eines Prüfereignisses 647
Konfigurieren und Aktivieren des Prüfservice (Übersicht der Schritte) 648
Konfigurieren und Aktivieren des Prüfservice (Aufgaben) 649
▼ So erstellen Sie Partitionen für Prüfdateien 649
▼ So konfigurieren Sie den E-Mail-Alias `audit_warn` 653
▼ So konfigurieren Sie die Prüfrichtlinie 653
▼ So aktivieren Sie den Prüfservice 656
▼ So deaktivieren Sie den Prüfservice 658
▼ So aktualisieren Sie den Prüfservice 659
Konfigurieren des Prüfservice in Zonen (Aufgaben) 660
▼ So können Sie alle Zonen für die Prüfung identisch konfigurieren 661
▼ So konfigurieren Sie eine zonenweise Prüfung 663
Verwalten der Prüfdatensätze (Übersicht der Schritte) 665
Verwalten der Prüfdatensätze 665
▼ So zeigen Sie Prüfdatensatzformate an 665
▼ So führen Sie Prüfdateien aus dem Prüfpfad zusammen 667
▼ So wählen Sie Prüfereignisse aus dem Prüfpfad aus 669
▼ So zeigen Sie den Inhalt der binären Prüfdateien an 671
▼ So bereinigen Sie eine Prüfdatei des Typs `not_terminated` 673
▼ So verhindern Sie eine Prüfpfadüberlauf 674
Fehlerbehebung bei der Oracle Solaris-Prüfung (Aufgaben) 675
Fehlerbehebung bei der Oracle Solaris-Prüfung (Übersicht der Schritte) 675
▼ So können Sie die Ausführung der Oracle Solaris-Prüfung feststellen 676
▼ So verringern Sie den Umfang der erstellten Prüfdatensätze 679
▼ So prüfen Sie alle Befehle der Benutzer 680
▼ So suchen Sie nach Prüfdatensätzen der Änderungen an bestimmten Dateien 683
▼ So ändern Sie die Vorauswahlmaske eines Benutzers 683
▼ So verhindern Sie die Prüfung bestimmter Ereignisse 685
▼ So beschränken Sie die Größe binärer Prüfdateien 686
▼ So prüfen Sie Anmeldungen von anderen Betriebssystemen 686
▼ So prüfen Sie FTP- und SFTP-Dateiübertragungen 687

31 Prüfung bei Oracle Solaris (Referenz) 689
Befehle zur Prüfung 689
Dämon `auditd` 690
Befehl `audit` 691
Befehl `bsmrecord` 691
Befehl `auditreduce` 691
Befehl `praudit` 693
Befehl `auditconfig` 695
Im Prüfservice verwendete Dateien 695
Datei `system` 696
Datei `syslog.conf` 696
Datei `audit_class` 696
Datei `audit_control` 697
Datei `audit_event` 698
Skript `audit_startup` 699
Datenbank `audit_user` 699
Skript `audit_warn` 700
Skript `bsmconv` 701
Berechtigungsprofile für Verwalten der Prüfung 702
Prüfung und Oracle Solaris-Zonen 702
Prüfklassen 703
Definitionen der Prüfklassen 703
Syntax der Prüfklassen 704
Prüf-Plugins 706
Prüfrichtlinie 706
Verarbeiten der Prüfungsmerkmale 707
Prüfpfad 707
Namenskonventionen für binäre Prüfdateien 708
Namen von binären Prüfdateien 708
Zeitstempel für binäre Prüfdateien 709
Struktur von Prüfdatensätzen 709
Analyse von Prüfdatensätzen 710
Formate der Prüf-Token 711
Token `acl` 712
Token `arbitrary` (veraltet) 713
Token `arg` 714

Token attribute 714
Token cmd 715
Token exec_args 715
Token exec_env 716
Token exit (veraltet) 716
Token file 716
Token group (veraltet) 717
Token groups 717
Token header 717
Token ip_addr 718
Token ip (veraltet) 719
Token ipc 719
Token ipc_perm 720
Token iport 720
Token opaque (veraltet) 721
Token path 721
Token path_attr 722
Token privilege 722
Token process 722
Token return 724
Token sequence 725
Token socket 725
Token subject 726
Token text 728
Token trailer 728
Token uauth 729
Token upriv 729
Token zonename 729

Glossar 731

Index 745

Vorwort

System Administration Guide: Security Services ist Teil eines mehrbändigen Dokumentationssatzes, der zahlreiche wichtige Informationen zur Verwaltung des Betriebssystems Oracle Solaris-Betriebssystem (Oracle Solaris) enthält. In diesem Buch wird davon ausgegangen, dass die aktuelle Version bereits installiert und eventuell erforderliche Netzwerksoftware eingerichtet ist. Oracle Solaris-Betriebssystem ist Teil der Oracle Solaris-Produktfamilie, die eine Vielzahl von Funktionen wie Oracle Solaris Secure Shell enthält.

Hinweis – Diese Oracle Solaris-Version unterstützt Systeme auf der Basis der Prozessorarchitekturen SPARC und x86. Die unterstützten Systeme sind unter *Oracle Solaris OS: Hardware Compatibility Lists* aufgeführt. Eventuelle Implementierungsunterschiede zwischen den Plattformtypen sind in diesem Dokument angegeben.

In diesem Dokument bedeuten x86-bezogene Begriffe Folgendes:

- "x86" bezieht sich auf die große Familie der 64-Bit- und 32-Bit-kompatiblen x86-Produkte.
- "x64" bezieht sich insbesondere auf mit 64-Bit-x86-Architekturen kompatible CPUs.
- `32-Bit x86` weist auf bestimmte 32-Bit-Informationen zu x86-basierten Systemen hin.

Die unterstützten Systeme können Sie den *Oracle Solaris OS: Hardware Compatibility Lists* entnehmen.

Zielgruppe dieses Handbuchs

Dieses Buch richtet sich an alle Benutzer, die für die Verwaltung von Systemen verantwortlich sind, auf denen Oracle Solaris ausgeführt wird. Um die Informationen in diesem Buch richtig umsetzen zu können, sollten Sie über mindestens zwei Jahre Erfahrung in der Verwaltung von UNIX-Systemen verfügen. Die Teilnahme an Schulungen zur Verwaltung von UNIX-Systemen wird empfohlen.

Organisation der Systemverwaltungshandbücher

Hier finden Sie eine Liste der Themen, die in den Systemverwaltungshandbüchern behandelt werden.

Buchtitel	Themen
System Administration Guide: Basic Administration	Benutzerkonten und Gruppen, Server- und Clientunterstützung, Herunterfahren und Booten eines Systems, Verwalten der Services
System Administration Guide: Advanced Administration	Terminale und Modems, Systemressourcen (Datenträgerkontingente, Accounting und Crontabs), Systemprozesse und Beheben von Problemen mit der Oracle Solaris-Software
System Administration Guide: Devices and File Systems	Wechselmedien, Festplatten und Geräte, Dateisysteme und Backup und Wiederherstellen von Daten
Systemverwaltungshandbuch: IP Services	TCP/IP-Netzwerkverwaltung, Verwaltung von IPv4- und IPv6-Adressen, DHCP, IPsec, IKE, IP Filter, Mobile IP, IP-Netzwerk-Multipathing (IPMP) und IPQoS
Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)	DNS-, NIS- und LDAP-Naming Services und -Directory Services, einschließlich Übergang von NIS zu LDAP und Übergang von NIS+ zu LDAP
System Administration Guide: Naming and Directory Services (NIS+)	NIS+-Naming Services und Directory Services
Systemverwaltungshandbuch: Netzwerkdienste	Webcache-Server, zeitorientierte Services, Netzwerk-Dateisysteme (NFS und Autofs), Mail, SLP und PPP
System Administration Guide: Printing	Druckthemen und -aufgaben, wie Sie mithilfe von Services, Tools, Protokollen und Technologien Druckdienste und Drucker einrichten und verwalten
Systemverwaltungshandbuch: Sicherheitsservices	Auditing, Geräteverwaltung, Dateisicherheit, BART, Kerberos-Services, PAM, Oracle Solaris Cryptographic Framework, Berechtigungen, RBAC, SASL und Oracle Solaris Secure Shell
Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones	Projekte und Aufgaben im Rahmen der Ressourcenverwaltung, Extended Accounting, Resource Controls, Fair Share Scheduler (FSS), Steuerung des physischen Arbeitsspeichers mithilfe des Resource Capping Daemon (rcapd) und Resource Pools; Virtualisierung mithilfe der Softwarepartitionierungstechnologie Solaris Zones und `lx`-Branded Zones

Buchtitel	Themen
Oracle Solaris ZFS-Administrationshandbuch	ZFS-Speicherpool und Dateisystemerstellung und -verwaltung, Momentaufnahmen, Klone, Backups, verwenden von Zugriffssteuerlisten (Access Control Lists/ACLs) zum Schutz von ZFS-Dateien, verwenden von ZFS auf einem Oracle Solaris-System mit installierten Zonen, emulierte Datenträger und Problembehandlung und Datenwiederherstellung
Oracle Solaris Trusted Extensions Administrator's Procedures	Systemadministration, die nur für die Trusted Extensions-Funktion von Oracle Solaris gilt
Oracle Solaris Trusted Extensions Configuration Guide	Ab Version Solaris 10 5/08: Hier wird beschrieben, wie Sie die Trusted Extensions-Funktion von Oracle Solaris planen, aktivieren und die Erstkonfiguration durchführen.

Themenverwandte Websites von Fremdanbietern

In dieser Dokumentation wird auf URLs von Fremdanbietern verwiesen, auf denen zusätzliche relevante Informationen zur Verfügung gestellt werden.

Oracle ist nicht für die Verfügbarkeit von den in diesem Dokument genannten Fremd-Websites verantwortlich. Oracle ist in keinerlei Weise verantwortlich oder haftbar für Inhalte, Werbung, Produkte oder Materialien, die mittels solcher Websites oder Ressourcen bereitgestellt werden. Oracle übernimmt keine Verantwortung oder Haftung für tatsächliche oder angebliche Schäden oder Verluste, die im Zusammenhang mit den auf diesen Websites angebotenen Informationen, Waren oder Dienstleistungen entstanden sind.

Kontakt zum Support von Oracle

Oracle-Kunden können über My Oracle Support den Online-Support nutzen. Informationen dazu erhalten Sie unter `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` bzw. `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` (für Hörgeschädigte).

Typografische Konventionen

In der folgenden Tabelle sind die in diesem Handbuch verwendeten typografischen Konventionen aufgeführt.

TABELLE P–1 Typografische Konventionen

Schriftart	Bedeutung	Beispiel
`AaBbCc123`	Die Namen von Befehlen, Dateien, Verzeichnissen sowie Bildschirmausgabe.	Bearbeiten Sie Ihre `.login`-Datei. Verwenden Sie `ls -a`, um eine Liste aller Dateien zu erhalten. `system% Sie haben eine neue Nachricht.`
`AaBbCc123`	Von Ihnen eingegebene Zeichen (im Gegensatz zu auf dem Bildschirm angezeigten Zeichen)	`Computername%` **`su`** `Passwort:`
aabbcc123	Platzhalter: durch einen tatsächlichen Namen oder Wert zu ersetzen	Der Befehl zum Entfernen einer Datei lautet `rm` *Dateiname* .
AaBbCc123	Buchtitel, neue Ausdrücke; hervorgehobene Begriffe	Lesen Sie hierzu Kapitel 6 im *Benutzerhandbuch*. Ein *Cache* ist eine lokal gespeicherte Kopie. Diese Datei *nicht* speichern. **Hinweis:** Einige hervorgehobene Begriffe werden online fett dargestellt.

Shell-Eingabeaufforderungen in Befehlsbeispielen

Die folgende Tabelle zeigt die UNIX-Standardeingabeaufforderung und die Superuser-Eingabeaufforderung für Shells, die zum Betriebssystem Oracle Solaris gehören. Die in den Befehlsbeispielen angezeigte Standard-Systemeingabeaufforderung variiert, abhängig von der Oracle Solaris-Version.

TABELLE P–2 Shell-Eingabeaufforderungen

Shell	Eingabeaufforderung
Bash-Shell, Korn-Shell und Bourne-Shell	`$`
Bash-Shell, Korn-Shell und Bourne-Shell für Superuser	`#`
C-Shell	`system%`
C-Shell für Superuser	`system#`

TEIL I

Übersicht über die Sicherheit

In diesem Dokument stehen die Funktionen zur Erhöhung der Sicherheit im Oracle Solaris-Betriebssystem im Vordergrund. Dieses Dokument richtet sich an Systemadministratoren und Benutzer der Sicherheitsfunktionen. In Kapitel 1, „Sicherheitsservices (Überblick)“ werden die Themen in diesem Dokument vorgestellt.

◆ ◆ ◆ KAPITEL 1

1 Sicherheitsservices (Überblick)

Um die Sicherheit des Oracle Solaris-Betriebssystem (Oracle Solaris-Betriebssystem) zu gewährleisten, bietet die Software folgende Funktionen:

- „Systemsicherheit“ auf Seite 32: Verhindert unbefugte Zugriffe und schützt Rechnerressourcen und Geräte vor dem unsachgemäßen Gebrauch und Dateien vor böswilligen oder unbeabsichtigten Änderungen durch Benutzer oder Eindringlinge.

  Eine Diskussion zur lokalen Systemsicherheit finden Sie unter Kapitel 2, „Verwalten von Rechnersicherheit (Übersicht)“.
- „Kryptografische Services“ auf Seite 33: Verschlüsselt Daten so, dass nur der Absender und der angegebene Empfänger den Inhalt lesen können, und verwaltet kryptografische Provider sowie Public-Key-Objekte.
- „Authentifizierungsservices“ auf Seite 34: Identifiziert Benutzer auf sichere Weise. Hierfür sind ein Benutzername und eine Form des Nachweises (üblicherweise ein Passwort) erforderlich.
- „Authentifizierung mit Verschlüsselung“ auf Seite 35: Stellt sicher, dass authentifizierte Teilnehmer ohne Abhörversuche, Änderungen oder Spoofing miteinander kommunizieren können.
- „Prüfung“ auf Seite 35: Identifiziert die Quelle der Sicherheitsänderungen gegenüber dem System, einschließlich Dateizugriff, sicherheitsbezogener Systemaufrufe und Authentifizierungsfehlern.
- „Sicherheitsrichtlinie“ auf Seite 35: Entwurf und Implementierung von Sicherheitsrichtlinien für ein System oder ein Netzwerk von Systemen

Systemsicherheit

Die Systemsicherheit gewährleistet, dass die Ressourcen des Systems ordnungsgemäß verwendet werden. Durch die Zugriffssteuerung kann die Anzahl der Personen, die zum Zugriff auf Ressourcen im System berechtigt sind, eingeschränkt werden. Zu den Funktionen des Oracle Solaris-Betriebssystem für die Systemsicherheit und Zugriffssteuerung gehören die folgenden:

- **Tools für die Anmeldeverwaltung**: Befehle zum Überwachen und Steuern der Fähigkeit eines Benutzers, sich anzumelden. Weitere Informationen finden Sie unter „Schützen von Anmeldungen und Passwörtern (Übersicht der Schritte)“ auf Seite 64.
- **Hardwarezugriff**: Befehle zum Einschränken des Zugriffs auf den PROM und zum Begrenzen der Anzahl der Personen, die das System booten können. Weitere Informationen finden Sie unter „SPARC: Steuern von Zugriff auf Systemhardware (Übersicht der Schritte)“ auf Seite 80.
- **Ressourcenzugriff**: Tools und Strategien zur bestmöglichen Nutzung der Rechnerressourcen bei gleichzeitiger Vermeidung von unsachgemäßer Verwendung. Weitere Informationen finden Sie unter „Steuern des Zugriffs auf Rechnerressourcen“ auf Seite 50.
- **RBAC (Role-based access control, rollenbasierte Zugriffssteuerung)**: Eine Architektur für die Erstellung spezieller eingeschränkter Konten von Benutzern, die zur Ausführung bestimmter administrativer Aufgaben berechtigt sind. Weitere Informationen finden Sie unter „Rollenbasierte Zugriffssteuerung (Übersicht)“ auf Seite 190.
- **Berechtigungen**: Einzelne Berechtigungen für Prozesse hinsichtlich der Ausführung von Vorgängen. Diese Prozessberechtigungen werden im Kernel durchgesetzt. Weitere Informationen finden Sie unter „Berechtigungen (Übersicht)“ auf Seite 201.
- **Geräteverwaltung**: Die *Geräterichtlinie* bietet einen zusätzlichen Schutz für Geräte, die bereits durch UNIX-Berechtigungen geschützt werden. Die *Gerätezuordnung* steuert den Zugriff auf Peripheriegeräte wie z. B. ein Mikrofon oder ein CD-ROM-Laufwerk. Wenn die Zuordnung aufgehoben wird, können Bereinigungsskripten alle Daten vom Gerät löschen. Weitere Informationen finden Sie unter „Steuern des Zugriffs auf Dateien“ auf Seite 47.
- **BART (Basic Audit Reporting Tool)**: Ein Schnappschuss der Dateiattribute von Dateien auf einem System, der als *Manifest* bezeichnet wird. Durch Vergleichen der Manifeste auf einem oder mehreren Systemen über einen längeren Zeitraum können an Dateien vorgenommene Änderungen überwacht werden, um Sicherheitsrisiken zu verringern. Weitere Informationen finden Sie in Kapitel 5, „Verwenden von Basic Audit Reporting Tool (Aufgaben)“.
- **Dateiberechtigungen**: Attribute einer Datei oder eines Verzeichnisses. Die Berechtigungen beschränken die Anzahl der Benutzer und Gruppen, die zum Lesen, Schreiben oder Ausführen einer Datei oder zum Suchen eines Verzeichnisses berechtigt sind. Weitere Informationen finden Sie in Kapitel 6, „Steuern des Zugriffs auf Dateien (Aufgaben)“.

- **Skripten für die Verbesserung der Sicherheit**: Durch die Verwendung von Skripten können viele Dateisysteme und Parameter angepasst werden, um Sicherheitsrisiken zu verringern. Weitere Informationen finden Sie unter Kapitel 7, „Verwenden von Automated Security Enhancement Tool (Aufgaben)“.

Kryptografische Services

Kryptografie ist die Wissenschaft vom Verschlüsseln und Entschlüsseln von Daten. Mithilfe von Kryptografie werden Integrität, Vertraulichkeit und Authentizität sichergestellt. Integrität bedeutet, dass die Daten nicht geändert wurden. Vertraulichkeit heißt, dass die Daten nicht von anderen gelesen werden können. Authentizität für Daten besagt, dass die Daten, die weitergeleitet wurden, exakt den gesendeten Daten entsprechen. Benutzerauthentifizierung bedeutet, dass der Benutzer mindestens einen Identitätsnachweis erbracht hat. Authentifizierungsmechanismen überprüfen mathematisch die Datenquelle oder den Identitätsnachweis. Verschlüsselungsmechanismen verschlüsseln Daten so, dass diese nicht von zufälligen Beobachtern gelesen werden können. Kryptografische Services bieten Authentifizierungs- und Verschlüsselungsmechanismen für Anwendungen und Benutzer.

Kryptografische Algorithmen verwenden Hashing, Verkettung und weitere mathematische Techniken zum Erstellen von Code, der schwierig zu entschlüsseln ist. Authentifizierungsmechanismen erfordern, dass der Absender und der Empfänger eine identische Zahl aus den Daten berechnen. Verschlüsselungsmechanismen verwenden die von Sender und Empfänger gemeinsam genutzten Informationen über die Verschlüsselungsmethode. Diese Informationen ermöglichen nur dem Empfänger und dem Sender, die Meldung zu entschlüsseln. Oracle Solaris stellt ein zentralisiertes kryptografisches Framework sowie Verschlüsselungsmechanismen bereit, die an bestimmte Anwendungen gebunden sind.

- **Oracle Solaris Cryptographic Framework**: Ein zentrales Framework von kryptografischen Services für Verbraucher auf Kernel- und auf Benutzerebene, das auf folgendem Standard basiert: RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki). Dieses Framework umfasst Passwörter, IPsec und Drittanbieteranwendungen. Es zentralisiert Hardware- und Softwarequellen für die Verschlüsselung. Die PKCS #11-Bibliothek stellt eine API für Drittentwickler bereit, um die kryptografischen Anforderungen für ihre Anwendungen zu erfüllen. Weitere Informationen finden Sie in Kapitel 13, „Oracle Solaris Cryptographic Framework (Übersicht)“.
- **Verschlüsselungsmechanismen pro Anwendung**:
  - Informationen zur Verwendung von DES in sicherem RPC finden Sie unter „Übersicht zu Secure RPC“ auf Seite 335.
  - Informationen zur Verwendung von DES, 3DES, AES und ARCFOUR im Kerberos-Service finden Sie in Kapitel 21, „Einführung zum Kerberos-Service“.
  - Informationen zur Verwendung von RSA, DSA und Codes wie Blowfish in Secure Shell, finden Sie in Kapitel 19, „Verwenden von Oracle Solaris Secure Shell (Aufgaben)“.

- Informationen zur Verwendung kryptografischer Algorithmen zur Passwortverschlüsselung finden Sie in „Ändern des Passwortalgorithmus (Übersicht der Schritte)“ auf Seite 72.

Ab Version &S10Update4 bietet KMF (Key Management Framework) ein zentrales Dienstprogramm für die Verwaltung von Public-Key-Objekten, einschließlich Richtlinie, Schlüsseln und Zertifikaten. KMF verwaltet diese Objekte für die Public-Key-Technologien OpenSSL, NSS und PKCS #11. Weitere Informationen finden Sie in Kapitel 15, „Oracle Solaris Key Management Framework“.

Authentifizierungsservices

Bei der Authentifizierung handelt es sich um einen Mechanismus zur Identifizierung eines Benutzers oder Service auf der Grundlage vordefinierter Kriterien. Die Authentifizierungsservices reichen von einfachen Paaren aus Name und Passwort bis hin zu komplexeren Challenge-Response-Systemen, wie z. B. Token-Karten und Biometrie. Strenge Authentifizierungsmechanismen verwenden die von einem Benutzer angegebenen Informationen, die nur jenem bekannt sind, und ein persönliches Element, das überprüft werden kann. Ein Benutzername ist ein Beispiel für Informationen, die nur der Benutzer kennt. Eine Smartcard oder ein Fingerabdruck beispielsweise können überprüft werden. Zu den Funktionen von Oracle Solaris für die Authentifizierung gehören die folgenden:

- **Sicheres RPC**: Ein Authentifizierungsmechanismus, der das Diffie-Hellman-Protokoll zum Schutz von NFS-Einhängevorgängen und einen Naming Service wie z. B. NIS oder NIS+ verwendet. Weitere Informationen finden Sie unter „Übersicht zu Secure RPC“ auf Seite 335.
- **PAM (Pluggable Authentication Module)**: Ein Framework, das die Integration verschiedener Authentifizierungstechnologien in einen Systemeintragsservice ermöglicht, ohne dass der Service neu kompiliert werden muss. Einige der Systemeintragsservices umfassen `login` und `ftp`. Weitere Informationen finden Sie in Kapitel 17, „Verwenden von PAM“.
- **SASL (Simple Authentication and Security Layer)**: Ein Framework, das Authentifizierungs- und Sicherheitsservices an Netzwerkprotokolle bereitstellt. Weitere Informationen finden Sie in Kapitel 18, „Verwenden von SASL“.
- **Secure Shell**: Ein sicheres Protokoll für Remote-Anmeldungen und Übertragungen, das die Kommunikation in einem unsicheren Netzwerk verschlüsselt. Weitere Informationen finden Sie in Kapitel 19, „Verwenden von Oracle Solaris Secure Shell (Aufgaben)“.
- **Kerberos-Service**: Eine Client-Server-Architektur, die Verschlüsselung in Verbindung mit Authentifizierung bietet. Weitere Informationen finden Sie in Kapitel 21, „Einführung zum Kerberos-Service“.
- **Solaris-Smartcard**: Eine Plastikkarte mit einem Mikroprozessor und einem Speicher, die mit einem Kartenlesegerät für den Zugriff auf Systeme verwendet werden kann. Weitere Informationen finden Sie unter *Solaris Smartcard Administration Guide* .

Authentifizierung mit Verschlüsselung

Die Authentifizierung mit Verschlüsselung ist die Grundlage für sichere Kommunikation. Mithilfe von Authentifizierung kann besser gewährleistet werden, dass es sich bei Quelle und Ziel tatsächlich um die vorgesehenen Teilnehmer handelt. Bei der Verschlüsselung wird die Kommunikation an der Quelle verschlüsselt und am Ziel entschlüsselt. Die Verschlüsselung hindert Eindringlinge daran, abgefangene Übertragungsdaten zu lesen. Zu den Funktionen von Oracle Solaris für die sichere Kommunikation gehören die folgenden:

- **Secure Shell**: Ein Protokoll für den Schutz von Datenübertragungen und Netzwerksitzungen mit interaktiven Benutzern vor dem Abhören, dem "Entführen" von Sitzungen und vor Man-in-the-middle-Angriffen. Die strenge Authentifizierung wird durch Public-Key-Kryptografie sichergestellt. X Window-Services und andere Netzwerkdienste können sicher über Secure Shell-Verbindungen getunnelt werden, was einen zusätzlichen Schutz bedeutet. Weitere Informationen finden Sie in Kapitel 19, „Verwenden von Oracle Solaris Secure Shell (Aufgaben)“.
- **Kerberos-Service**: Eine Client-Server-Architektur, die Authentifizierung in Verbindung mit Verschlüsselung bietet. Weitere Informationen finden Sie in Kapitel 21, „Einführung zum Kerberos-Service“.
- **IPsec (Internet Protocol Security Architecture)**: Eine Architektur, die einen Schutz des IP-Datagramms bietet. Die Schutzmaßnahmen umfassen Vertraulichkeit, starke Integrität der Daten, Datenauthentifizierung und partielle Sequenzintegrität. Weitere Informationen finden Sie in Kapitel 19, „IP Security Architecture (Übersicht)“ in *Systemverwaltungshandbuch: IP Services*.

Prüfung

Die Prüfung ist ein grundlegendes Konzept zur Sicherheit und Verwaltbarkeit von Systemen. Dabei wird der Verlauf von Aktionen und Ereignissen auf einem System untersucht, um festzustellen, was sich ereignet hat. Der Verlauf wird in einem Protokoll gespeichert, in dem festgehalten wird, welche Aktion ausgeführt wurde, zu welchem Zeitpunkt sie sich ereignet hat, von wem sie durchgeführt wurde und worauf sie sich ausgewirkt hat. Weitere Informationen finden Sie in Kapitel 28, „Prüfung bei Oracle Solaris (Übersicht)“.

Sicherheitsrichtlinie

Der Begriff Sicherheitsrichtlinie (oder auch nur Richtlinie) bezieht sich im vorliegenden Buch durchweg auf die Sicherheitsrichtlinien einer Organisation. Die für Ihren Standort geltende Sicherheitsrichtlinie stellt eine Reihe von Regeln dar, die die Sensitivität der verarbeiteten Informationen sowie die zum Schutz der Informationen vor unberechtigtem Zugriff angewendeten Maßnamen bestimmen. Sicherheitstechnologien wie Secure Shell, Authentifizierung, RBAC, Autorisierung, Berechtigungen und Ressourcensteuerung bieten Maßnahmen zum Schutz von Informationen.

Einige Sicherheitstechnologien verwenden das Wort "Richtlinie" zur Beschreibung bestimmter Aspekte der Implementierung. Zum Beispiel verwendet Oracle Solaris Prüfrichtlinienoptionen zum Konfigurieren bestimmter Aspekte der Prüfrichtlinie. Die folgende Tabelle verweist auf Glossar, Manpage sowie auf Informationen zu Funktionen, die mit dem Wort "Richtlinie" bestimmte Aspekte ihrer Implementierung beschreiben.

TABELLE 1–1 Verwendung der Richtlinie im Oracle Solaris-Betriebssystem

Definition im Glossar	Ausgewählte Manpages	Weitere Informationen
Prüfrichtlinie	`audit_control`(4), `audit_user`(4), `auditconfig`(1M)	Kapitel 28, „Prüfung bei Oracle Solaris (Übersicht)“
Richtlinie im kryptografischen Framework	`cryptoadm`(1M)	Kapitel 13, „Oracle Solaris Cryptographic Framework (Übersicht)“
Geräterichtlinie	`getdevpolicy`(1M)	„Steuern des Zugriffs auf Dateien“ auf Seite 47
Kerberos-Richtlinie	`krb5.conf`(4)	Kapitel 25, „Verwalten von Kerberos-Hauptelementen und Richtlinien (Aufgaben)“
Netzwerkrichtlinien	`ipfilter`(5), `ifconfig`(1M), `ike.config`(4), `ipsecconf`(1M), `routeadm`(1M)	Teil IV, „IP-Sicherheit“ in *Systemverwaltungshandbuch: IP Services*
Passwortrichtlinie	`passwd`(1), `nsswitch.conf`(4), `crypt.conf`(4), `policy.conf`(4)	„Steuern von Anmeldungen“ auf Seite 41
Richtlinie für öffentliche Schlüsseltechnologien	`kmfcfg`(1)	Kapitel 15, „Oracle Solaris Key Management Framework“
RBAC-Richtlinie	`rbac`(5). `policy.conf`(4)	„Datei `policy.conf`“ auf Seite 260

TEIL II

System-, Datei- und Gerätesicherheit

In diesem Abschnitt werden Sicherheitsmaßnahmen behandelt, die auf einem nicht vernetzten System konfiguriert werden können. In den entsprechenden Kapiteln wird die Planung, Überwachung und Steuerung des Zugriffs auf die Festplatte, auf Dateien und auf Peripheriegeräte erläutert.

- Kapitel 2, „Verwalten von Rechnersicherheit (Übersicht)“
- Kapitel 3, „Steuern des Zugriffs auf Systeme (Aufgaben)“
- Kapitel 4, „Steuern des Zugriffs auf Geräte (Aufgaben)“
- Kapitel 5, „Verwenden von Basic Audit Reporting Tool (Aufgaben)“
- Kapitel 6, „Steuern des Zugriffs auf Dateien (Aufgaben)“
- Kapitel 7, „Verwenden von Automated Security Enhancement Tool (Aufgaben)“

◆ ◆ ◆ KAPITEL 2

Verwalten von Rechnersicherheit (Übersicht)

Die Gewährleistung der Sicherheit von Informationen auf Rechnern ist eine wichtige Aufgabe für Systemadministratoren. Dieses Kapitel bietet allgemeine Informationen zur Verwaltung der Rechnersicherheit.

Im Folgenden ist eine Übersicht der Informationen in diesem Kapitel aufgeführt.

- „Verbesserungen der Rechnersicherheit in der Solaris 10-Version“ auf Seite 39
- „Steuern des Zugriffs auf ein Computersystem“ auf Seite 40
- „Steuern des Zugriffs auf Dateien“ auf Seite 47
- „Steuern des Zugriffs auf Rechnerressourcen“ auf Seite 50
- „Steuern von Zugriff auf Dateien“ auf Seite 55
- „Steuern von Netzwerkzugriff“ auf Seite 57
- „Melden von Sicherheitsproblemen“ auf Seite 62

Verbesserungen der Rechnersicherheit in der Solaris 10-Version

Ab der Version Solaris 9 sind folgende Funktionen zur Verbesserung der Systemsicherheit verfügbar:

- Starke Passwortverschlüsselung ist verfügbar und kann konfiguriert werden. Weitere Informationen finden Sie unter „Passwortverschlüsselung“ auf Seite 43.
- Geräterichtlinien werden mithilfe von Berechtigungen durchgesetzt. Weitere Informationen finden Sie unter „Geräterichtlinie (Übersicht)“ auf Seite 48.

  Für die Gerätezuordnung wird das Verzeichnis `/etc/security/dev` in zukünftigen Versionen von Oracle Solaris möglicherweise nicht mehr unterstützt.
- Das Programm BART (Basic Audit Reporting Tool) kann die Authentizität der Dateien auf Ihrem System überwachen. Weitere Informationen finden Sie in Kapitel 5, „Verwenden von Basic Audit Reporting Tool (Aufgaben)“.

- Dateien können mit starker Verschlüsselung geschützt werden. Weitere Informationen finden Sie unter „Schützen von Dateien durch Verschlüsselung“ auf Seite 55.
- Berechtigungen setzen Prozessrechte auf Kernel-Ebene durch. Weitere Informationen finden Sie unter „Berechtigungen (Übersicht)“ auf Seite 201.
- Cryptographic Framework zentralisiert Verschlüsselungsservices für Anbieter und Verbraucher. Weitere Informationen finden Sie in Kapitel 13, „Oracle Solaris Cryptographic Framework (Übersicht)“.
- Das PAM-Framework bietet Funktionen für viele Programme, wie Secure Shell. Weitere Informationen finden Sie unter „Änderungen am PAM in der Version Solaris 10“ auf Seite 349.
- Die Zonen und Ressourcenverwaltung von Oracle Solaris steuern den Zugriff auf Rechnerressourcen. Weitere Informationen finden Sie im *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.

Steuern des Zugriffs auf ein Computersystem

Alle an einem Arbeitsplatz mit einem Server verbundenen Computer können als ein großes, vielseitiges System betrachtet werden. Sie sind für die Sicherheit dieses größeren Systems verantwortlich. Sie müssen das Netzwerk vor Zugriffsversuchen Außenstehender schützen. Sie müssen auch die Integrität der Daten auf den Computern im Netzwerk sicherstellen.

Auf Dateiebene bietet Oracle Solaris Standardsicherheitsfunktionen, die Sie zum Schutz von Dateien, Verzeichnissen und Geräten verwenden können. Auf System- und Netzwerkebene liegen meistens die gleichen Probleme vor. Der erste Ansatz zur Gewährleistung der Sicherheit besteht darin, den Zugriff auf das System zu steuern.

Sie können den Zugriff auf das System folgendermaßen steuern und überwachen:

- „Gewährleisten physischer Sicherheit“ auf Seite 40
- „Steuern von Anmeldungen“ auf Seite 41
- „Steuern des Zugriffs auf Dateien“ auf Seite 47
- „Steuern des Zugriffs auf Rechnerressourcen“ auf Seite 50
- „Steuern von Zugriff auf Dateien“ auf Seite 55
- „Steuern von Netzwerkzugriff“ auf Seite 57
- „Melden von Sicherheitsproblemen“ auf Seite 62

Gewährleisten physischer Sicherheit

Um den Zugriff auf das System zu steuern, müssen Sie die physische Sicherheit Ihrer Computerumgebung gewährleisten. Beispielsweise stellen Systeme, die nach der Anmeldung unbeaufsichtigt gelassen werden, Sicherheitsrisiken dar. Sie bieten Eindringlingen die

Möglichkeit, sich Zugriff auf das Betriebssystem und das Netzwerk zu verschaffen. Die Umgebung und die Hardware des Computers muss physisch vor unberechtigtem Zugriff geschützt werden.

Sie können ein SPARC-System vor unberechtigtem Zugriff auf die Hardwareeinstellungen schützen. Verwenden Sie den Befehl `eeprom`, damit ein Passwort für den Zugriff auf den PROM erforderlich ist. Weitere Informationen finden Sie unter „So legen Sie fest, dass ein Passwort für Hardwarezugriff erforderlich ist“ auf Seite 80.

Steuern von Anmeldungen

Sie müssen außerdem unberechtigte Anmeldungen bei einem System oder Netzwerk verhindern, und zwar durch Zuweisen von Passwörtern und Steuern von Anmeldungen. Alle Konten auf einem System müssen über ein Passwort verfügen. Ein Passwort ist ein einfacher Authentifizierungsmechanismus. Mit einem Konto ohne Passwort kann sich jeder Zugriff auf das Netzwerk verschaffen, der einen Benutzernamen erraten kann. Ein starker Passwortalgorithmus schützt vor Brute-Force-Angriffen.

Wenn sich ein Benutzer beim System anmeldet, überprüft der Befehl `login` die Naming Service- oder Directory Service-Datenbank entsprechend den Informationen in der Datei `/etc/nsswitch.conf`. Diese Datei kann folgende Einträge enthalten:

- `files`: `/etc`-Dateien auf dem lokalen System
- `ldap`: LDAP-Verzeichnisservice auf dem LDAP-Server
- `nis`: NIS-Datenbank auf dem NIS-Master-Server
- `nisplus`: NIS+-Datenbank auf dem NIS+-Root-Server

Eine Beschreibung der Datei `nsswitch.conf` finden Sie auf der Manpage `nsswitch.conf(4)`. Informationen zu Naming Services und Directory Services finden Sie in *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)* oder in *System Administration Guide: Naming and Directory Services (NIS+)*.

Der Befehl `login` überprüft den vom Benutzer eingegebenen Benutzernamen und das Passwort. Wenn der Benutzername in der Passwortdatei nicht vorhanden ist, verweigert der Befehl `login` den Zugriff auf das System. Wenn nicht das richtige Passwort für den angegebenen Benutzernamen eingegeben wird, verweigert der Befehl `login` den Zugriff auf das System. Wenn der Benutzer einen gültigen Benutzernamen und das entsprechende Passwort angibt, gewährt das System dem Benutzer Zugriff.

PAM-Module können die Anmeldung bei Anwendungen nach einer erfolgreichen Anmeldung beim System optimieren. Weitere Informationen finden Sie in Kapitel 17, „Verwenden von PAM“.

Auf Oracle Solaris-Systemen stehen anspruchsvolle Authentifizierungs- und Autorisierungsmechanismen zur Verfügung. Authentifizierungs- und Autorisierungsmechanismen auf Netzwerkebene werden unter „Authentifizierung und Autorisierung für Remote-Zugriff“ auf Seite 58 beschrieben.

Verwalten von Passwortinformationen

Wenn sich Benutzer bei einem System anmelden, müssen sie einen Benutzernamen und ein Passwort angeben. Anmeldenamen können bekannt sein, Passwörter müssen jedoch geheim gehalten werden. Passwörter sollten nur den einzelnen Benutzern bekannt sein. Bitten Sie Benutzer, ihre Passwörter mit Bedacht zu wählen. Benutzer sollten ihre Passwörter oft ändern.

Passwörter werden anfänglich bei der Einrichtung eines Benutzerkontos erstellt. Um die Sicherheit der Benutzerkonten zu gewährleisten, können Sie Benutzer mithilfe der Passwortdatierung zur regelmäßigen Änderung ihrer Passwörter zwingen. Sie können ein Benutzerkonto auch deaktivieren, indem Sie das Passwort sperren. Detaillierte Informationen zur Verwaltung von Passwörtern finden Sie in Kapitel 4, „Managing User Accounts and Groups (Overview)“ in *System Administration Guide: Basic Administration* und auf der Manpage `passwd(1)`.

Lokale Passwörter

Wenn in Ihrem Netzwerk lokale Dateien zur Authentifizierung von Benutzern verwendet werden, sind die Passwortinformationen in den Dateien `/etc/passwd` und `/etc/shadow` des Systems enthalten. Der Benutzername und andere Informationen befinden sich in der Datei `/etc/passwd`. Das verschlüsselte Passwort befindet sich in einer separaten *shadow*-Datei, `/etc/shadow`. Dank dieser Sicherheitsmaßnahme haben Benutzer keinen Zugriff auf die verschlüsselten Passwörter. Während die Datei `/etc/passwd` für jeden verfügbar ist, der sich bei einem System anmelden kann, kann nur der Superuser oder eine entsprechende Rolle die Datei `/etc/shadow` lesen. Mit dem Befehl `passwd` können Sie das Passwort eines Benutzers auf einem lokalen System ändern.

NIS- und NIS+-Passwörter

Wenn in Ihrem Netzwerk NIS zur Authentifizierung von Benutzern verwendet wird, befinden sich die Passwortinformationen in der NIS-Passwort-Map. NIS unterstützt keine Passwortdatierung. Mit dem Befehl `passwd -r nis` ändern Sie ein in einer NIS-Passwort-Map gespeichertes Benutzerpasswort.

Wenn in Ihrem Netzwerk NIS+ zur Authentifizierung von Benutzern verwendet wird, werden Passwortinformationen in der NIS+-Datenbank gespeichert. Informationen in der NIS+-Datenbank können geschützt werden, indem der Zugriff auf autorisierte Benutzer beschränkt wird. Mit dem Befehl `passwd -r nisplus` können Sie das in einer NIS+-Datenbank gespeicherte Passwort eines Benutzers ändern.

LDAP-Passwörter

Der Oracle Solaris LDAP-Naming Service speichert Passwort- und Shadow-Informationen im Container `ou=people` des LDAP-Verzeichnisbaums. Auf dem Oracle Solaris LDAP-Naming Service-Client können Sie das Passwort eines Benutzers mit dem Befehl `passwd -r ldap` ändern. Der LDAP-Naming Service speichert das Passwort im LDAP-Repository.

Die Passwortrichtlinie wird auf dem Sun Java System Directory Server durchgesetzt. Insbesondere das Modul `pam_ldap` des Clients wird von den Passwortrichtlinien gesteuert, die auf dem Sun Java System Directory Server durchgesetzt werden. Weitere Informationen finden Sie unter „LDAP-Naming Services-Sicherheitsmodell“ in *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)*.

Passwortverschlüsselung

Starke Passwortverschlüsselung bietet einen vorzeitigen Schutz gegen Angriffe. Oracle Solaris-Software bietet sechs Passwortverschlüsselungsalgorithmen. Die Algorithmen Blowfish, MD5 und SHA bieten eine robustere Passwortverschlüsselung als der UNIX-Algorithmus.

Passwort-Algorithmuskennungen

Die Algorithmuskonfiguration für einen Standort wird in der Datei `/etc/security/policy.conf` angegeben. In der Datei `policy.conf` werden die in der folgenden Tabelle genannten Kennungen für Algorithmen verwendet. Eine Zuordnung zwischen Kennung und Algorithmus finden Sie in der Datei `/etc/security/crypt.conf`.

TABELLE 2–1 Passwortverschlüsselungsalgorithmen

Kennung	Beschreibung	Algorithmus-Manpage
`1`	Der MD5-Algorithmus ist mit den MD5-Algorithmen auf BSD- und Linux-Systemen kompatibel.	`crypt_bsdmd5(5)`
`2a`	Der Blowfish-Algorithmus ist mit dem Blowfish-Algorithmus auf BSD-Systemen kompatibel.	`crypt_bsdbf(5)`
`md5`	Im Vergleich zur BSD- und Linux-Version von MD5 gilt der Sun MD5-Algorithmus als stärker.	`crypt_sunmd5(5)`
`5`	Der SHA256-Algorithmus. SHA steht für Secure Hash Algorithm. Dieser Algorithmus gehört zur SHA-2-Familie. SHA256 unterstützt Passwörter mit 255 Zeichen.	`crypt_sha256(5)`
`6`	Der SHA512-Algorithmus	`crypt_sha512(5)`
`__unix__`	Der traditionelle UNIX-Verschlüsselungsalgorithmus. Dieser Algorithmus ist das Standardmodul in der Datei `policy.conf`.	`crypt_unix(5)`

Algorithmuskonfiguration in der Datei policy.conf

Der folgende Abschnitt zeigt die Standard-Algorithmuskonfiguration in der Datei `policy.conf`:

```
#
...
# crypt(3c) Algorithms Configuration
```

```
#
# CRYPT_ALGORITHMS_ALLOW specifies the algorithms that are allowed to
# be used for new passwords.  This is enforced only in crypt_gensalt(3c).
#
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6

# To deprecate use of the traditional unix algorithm, uncomment below
# and change CRYPT_DEFAULT= to another algorithm.  For example,
# CRYPT_DEFAULT=1 for BSD/Linux MD5.
#
#CRYPT_ALGORITHMS_DEPRECATE=__unix__

# The Solaris default is the traditional UNIX algorithm.  This is not
# listed in crypt.conf(4) since it is internal to libc.  The reserved
# name __unix__ is used to refer to it.
#
CRYPT_DEFAULT=__unix__
...
```

Wenn Sie den Wert für `CRYPT_DEFAULT` ändern, werden die Passwörter neuer Benutzer mit dem Algorithmus verschlüsselt, der durch den neuen Wert angegeben wird.

Wenn vorhandene Benutzer ihre Passwörter ändern, wirkt sich die Verschlüsselung des alten Passworts auf diejenige des neuen Passwort aus. Nehmen Sie beispielsweise Folgendes an: `CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6` und `CRYPT_DEFAULT=1` . Die nachstehende Tabelle zeigt, welche Algorithmen verwendet werden, um das verschlüsselte Passwort zu generieren.

Kennung = Passwortalgorithmus		
Anfängliches Passwort	**Geändertes Passwort**	**Erläuterung**
`1` = `crypt_bsdmd5`	Verwendet den gleichen Algorithmus	Die Kennung `1` ist auch der Wert von `CRYPT_DEFAULT`. Das Passwort des Benutzers wird weiterhin mit dem Algorithmus `crypt_bsdmd5` verschlüsselt.
`2a` = `crypt_bsdbf`	Verwendet den gleichen Algorithmus	Die Kennung `2a` befindet sich in der Liste `CRYPT_ALGORITHMS_ALLOW`. Daher wird das neue Passwort mit dem Algorithmus `crypt_bsbdf` verschlüsselt.
`md5` = `crypt_md5`	Verwendet den gleichen Algorithmus	Die Kennung `md5` befindet sich in der Liste `CRYPT_ALGORITHMS_ALLOW`. Daher wird das neue Passwort mit dem Algorithmus `crypt_md5` verschlüsselt.
`5` = `crypt_sha256`	Verwendet den gleichen Algorithmus	Die Kennung `5` befindet sich in der Liste `CRYPT_ALGORITHMS_ALLOW`. Daher wird das neue Passwort mit dem Algorithmus `crypt_sha256` verschlüsselt.
`6` = `crypt_sha512`	Verwendet den gleichen Algorithmus	Die Kennung `6` befindet sich in der Liste `CRYPT_ALGORITHMS_ALLOW`. Daher wird das neue Passwort mit dem Algorithmus `crypt_sha512` verschlüsselt.

Kennung = Passwortalgorithmus		
Anfängliches Passwort	**Geändertes Passwort**	**Erläuterung**
`__unix__` = `crypt_unix`	Verwendet den Algorithmus `crypt_bsdmd5`	Die Kennung `__unix__` befindet sich in der Liste `CRYPT_ALGORITHMS_ALLOW`. Daher kann der Algorithmus `crypt_unix` nicht verwendet werden. Das neue Passwort wird mit dem Algorithmus `CRYPT_DEFAULT` verschlüsselt.

Weitere Informationen zur Konfiguration von Algorithmusoptionen finden Sie auf der Manpage `policy.conf(4)`. Informationen zur Angabe der Passwortverschlüsselungsalgorithmen finden Sie unter „Ändern des Passwortalgorithmus (Übersicht der Schritte)“ auf Seite 72.

Spezielle Systemkonten

Das `root`-Konto ist eines von mehreren speziellen *Systemkonten*. Von diesen Konten verfügt nur das `root`-Konto über ein Passwort und kann zur Anmeldung verwendet werden. Das `nuucp`-Konto kann zur Anmeldung bei Dateiübertragungen verwendet werden. Die anderen Systemkonten schützen entweder Dateien oder führen administrative Vorgänge aus, ohne vollständige `root`-Berechtigung.

Achtung – Ändern Sie nie die Passworteinstellung eines Systemkontos. Ein Konto mit `NP` oder `*LK*sys` im zweiten Feld der `shadow`-Datei ist ein Systemkonto.

In der folgenden Tabelle werden einige Systemkonten und ihre Verwendung aufgeführt. Die Systemkonten haben spezielle Funktionen. Jedes Konto hat eine UID unter 100.

TABELLE 2–2 Systemkonten und ihre Verwendung

Systemkonto	GID	Verwendung
`root`	`0`	Hat fast keine Beschränkungen. Kann andere Schutzmaßnahmen und Berechtigungen überschreiben. Das `root`-Konto hat Zugriff auf das gesamte System. Das Passwort für die `root`-Anmeldung muss sorgfältig geschützt werden. Das `root`-Konto (Superuser) verfügt über Zugriff auf die meisten Oracle Solaris-Befehle.
`daemon`	`1`	Steuert die Hintergrundverarbeitung
`bin`	`2`	Verfügt über Zugriff auf einige Oracle Solaris-Befehle
`sys`	`3`	Verfügt über Zugriff auf zahlreiche Systemdateien
`adm`	`4`	Verfügt über Zugriff auf einige administrative Dateien
`lp`	`71`	Verfügt über Zugriff auf die Objektdatendateien und gespoolten Datendateien für den Drucker

TABELLE 2–2 Systemkonten und ihre Verwendung *(Fortsetzung)*

Systemkonto	GID	Verwendung
uucp	5	Verfügt über Zugriff auf die Objektdatendateien und gespoolten Datendateien für UUCP, das Programm zum Kopieren von UNIX zu UNIX
nuucp	9	Wird von Remote-Systemen zur Anmeldung bei Systemen und zum Starten der Dateiübertragung verwendet

Remote-Anmeldungen

Remote-Anmeldungen stellen eine Versuchung für Eindringlinge dar. Oracle Solaris bietet mehrer Befehle zum Überwachen, Beschränken und Deaktivieren von Remote-Anmeldungen. Die Vorgänge werden unter „Schützen von Anmeldungen und Passwörtern (Übersicht der Schritte)“ auf Seite 64 beschrieben.

Standardmäßig können Systemgeräte, wie beispielsweise die Maus, die Tastatur, der Bildspeicher oder ein Audiogerät, mit bestimmten Anmeldungen nicht gesteuert oder gelesen werden. Weitere Informationen finden Sie auf der Manpage `logindevperm(4)`.

Einwahlanmeldungen

Wenn über ein Modem oder einen Einwahlport auf einen Computer zugegriffen wird, können Sie weitere Sicherheitsmaßnahmen ergreifen. Sie können ein *Einwahl-Passwort* für Benutzer festlegen, die über ein Modem oder einen Einwahlport auf ein System zugreifen. Ein Benutzer muss dieses zusätzliche Passwort eingeben, bevor er Zugriff auf das System erhält.

Nur ein Superuser kann ein Einwahl-Passwort erstellen oder ändern. Ändern Sie das Passwort ungefähr einmal im Monat, um die Integrität des Systems zu gewährleisten. Diese Funktion wird am effizientesten verwendet, um ein Einwahl-Passwort für den Zugriff auf ein Gateway-System anzufordern. Informationen zur Einrichtung von Einwahl-Passwörtern finden Sie unter „So erstellen Sie ein Einwahl-Passwort“ auf Seite 70.

Zwei Dateien sind an der Erstellung eines Einwahl-Passworts beteiligt: `/etc/dialups` und `/etc/d_passwd`. Die Datei `dialups` enthält eine Liste von Ports, für die ein Einwahl-Passwort eingegeben werden muss. Die Datei `d_passwd` enthält eine Liste von Shell-Programmen, für die ein verschlüsseltes Passwort als zusätzliches Einwahl-Passwort eingegeben werden muss. Die Informationen in diesen beiden Dateien werden wie folgt verarbeitet:

- Wenn die Anmelde-Shell des Benutzers in `/etc/passwd` einem Eintrag in `/etc/d_passwd` entspricht, muss der Benutzer ein Einwahl-Passwort angeben.
- Wenn die Anmelde-Shell des Benutzers in `/etc/passwd` nicht in `/etc/d_passwd` gefunden wird, muss der Benutzer das Standardpasswort eingeben. Das Standardpasswort entspricht dem Eintrag für `/usr/bin/sh`.
- Wenn das Feld für die Anmelde-Shell in `/etc/passwd` leer ist, muss der Benutzer das Standardpasswort eingeben. Das Standardpasswort entspricht dem Eintrag für `/usr/bin/sh`.

- Wenn `/etc/d_passwd` keinen Eintrag für `/usr/bin/sh` enthält, werden die Benutzer, deren Feld für die Anmelde-Shell in `/etc/passwd` leer ist oder die mit keinem Eintrag in `/etc/d_passwd` übereinstimmen, nicht zur Eingabe eines Einwahl-Passworts aufgefordert.
- Einwahl-Anmeldungen sind deaktiviert, wenn `/etc/d_passwd` nur den Eintrag `/usr/bin/sh:*:` enthält.

Steuern des Zugriffs auf Dateien

Mit einem Computersystem verbundene Peripheriegeräte stellen ein Sicherheitsrisiko dar. Mikrofone können Unterhaltungen empfangen und an Remote-Systeme übertragen. CD-ROMs können Informationen hinterlassen, die vom nächsten Benutzer des CD-ROM-Geräts gelesen werden können. Remote-Systeme können auf Drucker zugreifen. Auch integrierte Geräte können Sicherheitsrisiken für das System bedeuten. Beispielweise gelten Netzwerkschnittstellen wie `hme0` als integrierte Geräte.

Oracle Solaris-Software bietet zwei Methoden für die Steuerung des Zugriffs auf Geräte. Die *Geräterichtlinie* beschränkt oder verhindert den Zugriff auf integrierte Geräte des Systems. Die Geräterichtlinie wird im Kernel durchgesetzt. Die *Gerätezuordnung* beschränkt oder verhindert den Zugriff auf Peripheriegeräte. Die Gerätezuordnung wird bei der Benutzerzuordnung durchgesetzt.

Die Geräterichtlinie verwendet Berechtigungen zum Schutz ausgewählter Geräte im Kernel. Beispielsweise legt die Geräterichtlinie fest, dass für Netzwerkschnittstellen wie `hme` alle Berechtigungen zum Lesen oder Schreiben erforderlich sind.

Die Gerätezuordnung schützt Peripheriegeräte wie Drucker oder Mikrofone durch Autorisierungen. Standardmäßig ist die Gerätezuordnung nicht aktiviert. Sobald sie aktiviert ist, kann die Gerätezuordnung konfiguriert werden, um die Verwendung eines Geräts zu verhindern oder von einer Autorisierung abhängig zu machen. Wenn ein Gerät zur Verwendung zugeordnet ist, kann kein anderer Benutzer auf das Gerät zugreifen, bis der aktuelle Benutzer die Zuordnung aufhebt.

Ein Oracle Solaris-System kann in verschiedenen Bereichen konfiguriert werden, um den Zugriff auf Geräte zu steuern:

- **Einstellen der Geräterichtlinie**: In Oracle Solaris können Sie festlegen, dass der Prozess, der auf ein bestimmtes Gerät zugreift, mit einem Satz von Berechtigungen ausgeführt werden muss. Prozesse ohne diese Berechtigungen können das Gerät nicht verwenden. Beim Systemstart wird die Geräterichtlinie von der Oracle Solaris-Software konfiguriert. Treiber von Drittanbietern können bei der Installation mit der Geräterichtlinie konfiguriert werden. Nach der Installation können Sie als Administrator einem Gerät eine Geräterichtlinie hinzufügen.
- **Aktivieren der Gerätezuordnung**: Wenn Sie die Gerätezuordnung aktivieren, können Sie die Verwendung des Geräts auf jeweils einen Benutzer beschränken. Sie können festlegen, dass der Benutzer einige Sicherheitsanforderungen erfüllen muss. Beispielsweise können Sie bestimmen, dass der Benutzer zur Verwendung des Geräts autorisiert sein muss.
- **Verhindern der Verwendung von Geräten**: Sie können verhindern, dass ein Gerät, wie beispielsweise ein Mikrofon, von einem beliebigen Benutzer oder Computersystem verwendet wird. Beispielsweise kann bei einem Computer-Kiosk die Verwendung bestimmter Geräte verhindert werden.
- **Beschränken eines Geräts auf eine bestimmte Zone**: Sie können die Verwendung eines Geräts auf eine nicht globale Zone beschränken. Weitere Informationen finden Sie unter „Gerätenutzung in nicht-globalen Zonen“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*. Allgemeinere Informationen zu Geräten und Zonen finden Sie unter „Konfigurierte Geräte in Zonen“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.

Geräterichtlinie (Übersicht)

Mithilfe der Geräterichtlinie können Sie festlegen, dass Prozesse, die auf ein Gerät zugreifen, bestimmte Berechtigungen benötigen. Nur die Prozesse, die mit den in der Geräterichtlinie angegebenen Berechtigungen ausgeführt werden, können auf Geräte zugreifen, die durch diese Geräterichtlinie geschützt werden. Oracle Solaris bietet eine Standardgeräterichtlinie. Beispielsweise müssen Prozesse, die auf Netzwerkschnittstellen wie `hme0` zugreifen, mit der Berechtigung `net_rawaccess` ausgeführt werden. Die Anforderung wird im Kernel durchgesetzt. Weitere Informationen zu Berechtigungen finden Sie unter „Berechtigungen (Übersicht)“ auf Seite 201.

In früheren Versionen wurden Geräteknoten nur durch Dateiberechtigungen geschützt. Geräte, die der Gruppe `sys` angehörten, konnten z. B. nur von Mitgliedern der Gruppe `sys` geöffnet werden. Dateiberechtigungen sehen nicht voraus, wer ein Gerät öffnen kann. Stattdessen werden Geräte durch Dateiberechtigungen *und* eine Geräterichtlinie geschützt. Beispielsweise verfügt die Datei `/dev/ip` über die Berechtigungen `666`. Das Gerät kann jedoch nur von einem Prozess mit den geeigneten Berechtigungen geöffnet werden.

Die Konfiguration einer Geräterichtlinie kann geprüft werden. Das Prüfereignis `AUE_MODDEVPLCY` zeichnet Änderungen der Geräterichtlinie auf.

Weitere Informationen zu Geräterichtlinien finden Sie unter:

- „Konfigurieren der Geräterichtlinie (Übersicht der Schritte)“ auf Seite 84
- „Befehle der Geräterichtlinie“ auf Seite 98
- „Berechtigungen und Geräte“ auf Seite 210

Gerätezuordnung (Übersicht)

Mithilfe des Gerätezuordnungsmechanismus können Sie den Zugriff auf ein Peripheriegerät, wie beispielsweise eine CD-ROM, beschränken. Der Mechanismus kann lokal verwaltet werden. Wenn Gerätezuordnungen nicht aktiviert sind, werden Peripheriegeräte nur durch Dateiberechtigungen geschützt. Beispielsweise sind Peripheriegeräte für folgende Zwecke standardmäßig verfügbar:

- Jeder Benutzer kann eine Diskette oder CD-ROM lesen oder darauf schreiben.
- Jeder Benutzer kann ein Mikrofon anschließen.
- Jeder Benutzer kann auf einen angeschlossenen Drucker zugreifen.

Die Gerätezuordnung kann die Verwendung eines Geräts auf autorisierte Benutzer beschränken. Die Gerätezuordnung kann auch ganz verhindern, dass auf ein Gerät zugegriffen wird. Ein Benutzer, der ein Gerät zuordnet, hat ausschließlichen Zugriff auf das Gerät, bis er die Zuordnung aufhebt. Wenn die Zuordnung eines Geräts aufgehoben wird, löschen Bereinigungsskripten alle verbliebenen Daten. Sie können ein Bereinigungsskript schreiben, um Informationen von Geräten zu löschen, die über kein solches Skript verfügen. Ein Beispiel finden Sie unter „Erstellen neuer Bereinigungsskripten“ auf Seite 105.

Versuche, ein Gerät zuzuordnen, die Zuordnung eines Geräts aufzuheben und zuordenbare Geräte aufzulisten, können geprüft werden. Die Prüfereignisse sind Teil der Prüfklasse `other`.

Weitere Informationen zur Gerätezuordnung finden Sie unter:

- „Verwalten der Gerätezuordnung (Übersicht der Schritte)“ auf Seite 87
- „Gerätezuordnung“ auf Seite 99
- „Befehle der Gerätezuordnung“ auf Seite 99

Steuern des Zugriffs auf Rechnerressourcen

Als Systemadministrator können Sie die Systemaktivität steuern und überwachen. Sie können beschränken, wer welche Ressourcen verwenden kann. Sie können die Ressourcenverwendung protokollieren und überwachen, wer die Ressourcen verwendet. Sie können Ihre Systeme auch einrichten, um die unsachgemäße Verwendung von Ressourcen zu minimieren.

Beschränken und Überwachen von Superuser-Zugriffen

Für Superuser-Zugriff auf Ihrem System müssen Sie ein `root`-Passwort eingeben. In der Standardkonfiguration kann kein Benutzer über eine Remote-Anmeldung als `root` auf das System zugreifen. Bei einer Remote-Anmeldung muss sich ein Benutzer mit seinem Benutzernamen anmelden und dann den Befehl `su` eingeben, um `root`-Berechtigungen zu erhalten. Sie können die Verwendung des Befehls `su` überwachen, insbesondere die Benutzer, die versucht haben, Superuser-Zugriff zu erhalten. Verfahren zum Überwachen des Superusers und zur Beschränkung des Superuser-Zugriffs finden Sie unter „Überwachen und Beschränken des Superusers (Übersicht der Schritte)“ auf Seite 77.

Konfigurieren von rollenbasierter Zugriffssteuerung zum Ersetzen des Superusers

Die rollenbasierte Zugriffssteuerung (Role-based Access Control, RBAC) dient zur Beschränkung der Superuser-Fähigkeiten. Der Superuser, der `root`-Benutzer, hat Zugriff auf alle Ressourcen im System. Mit RBAC können Sie `root` durch einen Satz von Rollen mit unterschiedlichen Berechtigungen ersetzen. Beispielsweise können Sie eine Rolle zur Erstellung der Benutzerkonten einrichten und eine andere für Systemdateiänderungen. Wenn Sie eine Rolle für eine Funktion oder einen Satz von Funktionen eingerichtet haben, können Sie diese Funktionen aus den Fähigkeiten des `root`-Benutzers entfernen.

Für jede Rolle muss sich ein Benutzer mit seinem Namen und Passwort anmelden. Nach der Anmeldung übernimmt der Benutzer die Rolle mithilfe eines bestimmten Rollenpassworts. Eine Person, die das `root`-Passwort herausfindet, kann in diesem Fall nur beschränkten Schaden im System verursachen. Weitere Informationen zu RBAC finden Sie unter „Rollenbasierte Zugriffssteuerung (Übersicht)“ auf Seite 190.

Verhindern von unbeabsichtigten Verwendungsfehlern bei Rechnerressourcen

Sie können unbeabsichtigte Verwendungsfehler wie folgt verhindern:

- Sie können die Ausführung eines Trojaners verhindern, indem Sie die Variable PATH richtig einstellen.
- Sie können Benutzern eine eingeschränkte Shell zuweisen. Eine eingeschränkte Shell verhindert Benutzerfehler, indem sie Benutzer zu den Teilen des Systems führt, die sie zur Ausführung ihrer Aufgaben benötigen. Durch eine sorgfältige Einrichtung können Sie sicherstellen, dass Benutzer nur auf die Teile des Systems zugreifen können, die sie für eine effiziente Arbeit benötigen.
- Sie können Beschränkungen für Dateien definieren, auf die Benutzer nicht zugreifen müssen.

Einstellen der Variable PATH

Sie sollten darauf achten, dass die Variable PATH richtig eingestellt ist. Andernfalls können Sie unbeabsichtigt ein Programm ausführen, das von einer anderen Person eingeschleust wurde. Ein schädliches Programm kann die Daten oder das System beschädigen. Diese Art von Programmen, die ein Sicherheitsrisiko darstellen, wird als *Trojaner* bezeichnet. Beispielsweise kann in einem öffentlichen Verzeichnis das Programm `su` durch ein Skript ersetzt werden, das Sie als Systemadministrator ausführen. Ein solches Skript sieht wie ein normaler `su`-Befehl aus. Da das Skript nach der Ausführung automatisch entfernt wird, können Sie nicht mehr nachweisen, dass Sie einen Trojaner ausgeführt haben.

Die Umgebungsvariable PATH wird automatisch bei der Anmeldung eingestellt. Der Pfad wird mithilfe der Startdateien `.login`, `.profile` und `.cshrc` eingestellt. Wenn Sie den Benutzersuchpfad so einrichten, dass das aktuelle Verzeichnis (`.`) an letzter Stelle steht, verhindern Sie die Ausführung dieser Art von Trojanern. Die Variable PATH für Superuser sollte das aktuelle Verzeichnis überhaupt nicht enthalten.

Das Programm ASET (Automated Security Enhancement Tool) überprüft die Startdateien, um sicherzustellen, dass die Variable PATH richtig eingestellt ist. ASET stellt außerdem sicher, dass die Variable PATH keinen Punkt (`.`) als Eintrag enthält.

Zuweisen einer eingeschränkten Shell zu Benutzern

Die Standard-Shell ermöglicht einem Benutzer das Öffnen von Dateien, Ausführen von Befehlen usw. Die eingeschränkte Shell beschränkt die Fähigkeit eines Benutzers, Verzeichnisse zu ändern und Befehle auszuführen. Die eingeschränkte Shell wird mit dem Befehl `/usr/lib/rsh` aufgerufen. Beachten Sie, dass die eingeschränkte Shell keine Remote-Shell ist. Dies ist `/usr/sbin/rsh`.

Die eingeschränkte Shell unterscheidet sich von der Standard-Shell wie folgt:

- Die Verwendung durch den Benutzer ist auf dessen Home-Verzeichnis beschränkt, sodass der Benutzer nicht mit dem Befehl `cd` in ein anderes Verzeichnis wechseln kann. Daher hat er keinen Zugriff auf Systemdateien.
- Der Benutzer kann die Variable `PATH` nicht ändern, sodass er nur Befehle in dem vom Systemadministrator eingestellten Pfad verwenden kann. Der Benutzer kann keine Befehle oder Skripten ausführen, indem er den vollständigen Pfadnamen verwendet.
- Der Benutzer kann die Ausgabe nicht mit > oder >> umleiten.

Mit der eingeschränkten Shell können Sie verhindern, dass Benutzer irrtümlich auf Systemdateien zugreifen. Die Shell erstellt eine beschränkte Umgebung für Benutzer, die bestimmte Aufgaben ausführen müssen. Die eingeschränkte Shell bietet jedoch keine vollständige Sicherheit, sie soll lediglich verhindern, dass unerfahrene Benutzer Schäden verursachen.

Um weitere Informationen zur eingeschränkten Shell zu erhalten, geben Sie den Befehl `man -s1m rsh` ein, um die Manpage `rsh(1M)` anzuzeigen.

Beschränken des Zugriffs auf Daten in Dateien

Da Oracle Solaris eine Mehrbenutzerumgebung ist, ist die Sicherheit des Dateisystems grundlegend für die Sicherheit des gesamten Systems. Sie können den herkömmlichen UNIX-Dateischutz verwenden, um die Dateien zu schützen. Sie können auch Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, die mehr Sicherheit bieten.

Beispielsweise können Sie einigen Benutzern das Lesen bestimmter Dateien gestatten, während andere Benutzer zum Ändern oder Löschen von Dateien befugt sein sollen. Oder Sie verfügen über Daten, in die keine andere Person Einblick haben soll. In Kapitel 6, „Steuern des Zugriffs auf Dateien (Aufgaben)“ wird die Einrichtung von Dateiberechtigungen beschrieben.

Beschränken von ausführbaren `setuid`-Dateien

Ausführbare Dateien können Sicherheitsrisiken darstellen. Viele ausführbare Programme müssen als `root` bzw. Superuser ausgeführt werden, um ordnungsgemäß zu funktionieren. Diese `setuid`-Programme werden mit der Benutzer-ID `0` ausgeführt. Jeder, der dieses Programme ausführt, erhält eine `root`-ID. Ein Programm, das mit der `root`-ID ausgeführt wird, stellt ein potenzielles Sicherheitsrisiko dar, wenn bei der Entwicklung des Programms die Sicherheit nicht angemessen berücksichtigt wurde.

Abgesehen von den ausführbaren Dateien von Oracle, in denen das `setuid`-Bit auf `root` eingestellt ist, sollten Sie die Verwendung von `setuid`-Programmen unterbinden. Wenn Sie auch `setuid`-Programme nicht vollständig verbieten können, sollten Sie dennoch ihre Verwendung wenigstens beschränken. Die Voraussetzung für eine sichere Verwaltung sind möglichst wenige `setuid`-Programme.

Weitere Informationen finden Sie unter „Vermeiden von Sicherheitsrisiken in Verbindung mit ausführbaren Dateien“ auf Seite 141. Informationen zu Verfahren finden Sie unter „Schützen vor Programmen mit Sicherheitsrisiko (Übersicht der Schritte)“ auf Seite 155.

Verwenden des Automated Security Enhancement Tool

Das ASET-Sicherheitspaket bietet automatische Verwaltungswerkzeuge, mit denen Sie die Sicherheit des Systems steuern und überwachen können. ASET bietet drei Sicherheitsebenen: niedrig, mittel und hoch. Geben Sie eine ASET-Sicherheitsebene an. Bei steigender Sicherheitsebene bietet ASET weitere Dateisteuerungsfunktionen, um den Dateizugriff einzuschränken und die Systemsicherheit zu erhöhen. Weitere Informationen finden Sie in Kapitel 7, „Verwenden von Automated Security Enhancement Tool (Aufgaben)“.

Verwenden des Oracle Solaris Security Toolkit

Während mit ASET eine geringe Anzahl von Sicherheitsänderungen an einem System vorgenommen werden kann, bietet das Oracle Solaris Security Toolkit einen flexiblen und erweiterbaren Mechanismus, um die Sicherheitsrisiken auf einem Oracle Solaris-System zu minimieren und das System zu verstärken und abzusichern. Mit dem Oracle Solaris Security Toolkit, inoffiziell auch als JASS-Toolkit bekannt, kann der Benutzer Sicherheitsänderungen am System vornehmen. Das Tool ermöglicht die Ausgabe eines Berichts zum Sicherheitsstatus eines Oracle Solaris-Systems. Vorherige Durchläufe mit dem Tool können rückgängig gemacht werden. Das JASS-Toolkit kann von der Website Oracle and Sun (`http://www.oracle.com/us/sun/index.htm`) heruntergeladen werden. Klicken Sie auf "Sun Downloads: A-Z", und suchen Sie in der alphabetisch geordneten Downloads-Liste nach der Zeichenfolge `Solaris Security Toolkit`.

Das Toolkit wird ausführlich beschrieben unter *Securing Systems with the Solaris Security Toolkit* von Alex Noordergraaf und Glenn Brunette, ISBN 0-13-141071-7, Juni 2003. Dieses Buch ist Teil der Sun BluePrints Series, die von Sun Microsystems Press veröffentlicht wird.

Verwenden der Konfiguration "Secure by Default"

Standardmäßig sind bei Installation der Version Solaris 10 zahlreiche Netzwerkdienste aktiviert. Um die Netzwerkkonnektivität eines Systems zu beschränken, führen Sie den Befehl `netservices limited` aus. Dieser Befehl aktiviert die Konfiguration "Secure by Default" (SBD). Mit SBD ist der einzige Netzwerkdienst, der Netzwerkanforderungen annimmt, der `sshd`-Dämon. Alle anderen Netzwerkdienste sind deaktiviert oder verarbeiten nur lokale Anforderungen. Um einzelne Netzwerkdienste wie `ftp` zu aktivieren, verwenden Sie die Service Management Facility (SMF). Weitere Informationen finden Sie auf den Manpages `netservices(1M)` und `smf(5)`.

Verwenden von Ressourcenverwaltungsfunktionen

Die Oracle Solaris-Software bietet hoch entwickelte Ressourcenverwaltungsfunktionen. Mit diesen Funktionen können Sie die Ressourcenverwendung von Anwendungen in einer Serverkonsolidierungsumgebung zuweisen, planen, überwachen und beschränken. Das Ressourcensteuerungs-Framework ermöglicht Ihnen, die von Prozessen beanspruchten Systemressourcen zu beschränken. Diese Beschränkungen helfen, Denial-of-Service-Angriffe zu vermeiden, bei denen ein Skript versucht, die Ressourcen eines Systems zu überlasten.

Mit den Oracle Solaris-Ressourcenverwaltungsfunktionen können Sie Ressourcen bestimmten Projekten zuweisen. Sie können die verfügbaren Ressourcen auch dynamisch anpassen. Weitere Informationen finden Sie unter Teil I, „Ressourcenverwaltung“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.

Verwenden von Oracle Solaris-Zonen

Oracle Solaris-Zonen bieten eine Ausführungsumgebung für Anwendungen, in der Prozesse vom Rest des Systems isoliert innerhalb einer einzigen Instanz des Oracle Solaris-Betriebssystem ausgeführt werden. Diese Isolation verhindert, dass Prozesse in einer Zone Prozesse in anderen Zonen überwachen oder beeinflussen. Selbst ein Prozess, der mit Berechtigungen eines Superuser ausgeführt wird, kann Aktivitäten in anderen Zonen weder anzeigen noch beeinflussen.

Oracle Solaris-Zonen sind ideal für Umgebungen mit zahlreichen Anwendungen auf einem einzigen Server geeignet. Weitere Informationen finden Sie unter Teil II, „Zonen“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.

Überwachen der Verwendung von Rechnerressourcen

Als Systemadministrator müssen Sie die Aktivität des Systems überwachen. Sie müssen über alle Aspekte Ihrer Rechner informiert sein, beispielsweise:

- Wie hoch ist die normale Systemauslastung?
- Wer hat Zugriff auf das System?
- Wann greifen Benutzer auf das System zu?
- Welche Programme werden normalerweise auf dem System ausgeführt?

Mit diesen Informationen können Sie die verfügbaren Tools zur Prüfung der Systemverwendung und Überwachung von Aktivitäten einzelner Benutzer verwenden. Überwachung ist eine sehr nützliche Maßnahme, wenn eine Sicherheitsverletzung für möglich gehalten wird. Weitere Informationen zum Prüfservice finden Sie in Kapitel 28, „Prüfung bei Oracle Solaris (Übersicht)“.

Überwachen von Dateiintegrität

Als Systemadministrator müssen Sie sicherstellen, dass die Dateien auf den Systemen, für die Sie zuständig sind, nicht auf unerwartete Art geändert wurden. Bei großen Installationen können Sie ein Vergleichs- und Berichtstool für den Software-Stack auf jedem der Systeme verwenden. BART (Basic Audit Reporting Tool) ermöglicht eine umfassende Validierung von Systemen, indem auf einem oder mehreren Systemen über einen längeren Zeitraum hinweg Überprüfungen auf Dateiebene durchgeführt werden. Durch Änderungen in einem BART-*Manifest* in einem oder mehreren Systemen kann die Integrität der Systeme validiert werden. BART ermöglicht das Erstellen und Vergleichen von Manifesten und bietet Regeln für Berichterstellung. Weitere Informationen finden Sie in Kapitel 5, „Verwenden von Basic Audit Reporting Tool (Aufgaben)“.

Steuern von Zugriff auf Dateien

Oracle Solaris ist eine Mehrbenutzerumgebung. In einer Mehrbenutzerumgebung können alle beim System angemeldeten Benutzer die Dateien von anderen Benutzern lesen. Mit den entsprechenden Dateiberechtigungen können Benutzer auch die Dateien anderer Benutzer verwenden. Weitere Informationen finden Sie in Kapitel 6, „Steuern des Zugriffs auf Dateien (Aufgaben)“. Eine schrittweise Anleitung zum Einstellen geeigneter Dateiberechtigungen finden Sie unter „Schützen von Dateien (Übersicht der Schritte)“ auf Seite 142.

Schützen von Dateien durch Verschlüsselung

Sie können eine Datei schützen, indem Sie festlegen, dass sie für andere Benutzer nicht verfügbar ist. Eine Datei mit der Berechtigung `600` kann nur von dem Eigentümer und dem Superuser gelesen werden. Ein Verzeichnis mit der Berechtigung `700` ist auf ähnliche Art nicht verfügbar. Personen, die Ihr Passwort oder das `root`-Passwort herausfinden, können auf diese Datei zugreifen. Bei jedem Backup der Systemdateien auf einem Offline-Datenträger wird die ansonsten unzugängliche Datei auf einem Sicherungsband gespeichert.

Das kryptografische Framework bietet die Befehle `digest`, `mac` und `encrypt` zum Schützen von Dateien. Weitere Informationen finden Sie in Kapitel 13, „Oracle Solaris Cryptographic Framework (Übersicht)“.

Verwenden von Zugriffssteuerungslisten

ACLs (Access Control Lists, Zugriffssteuerungslisten) bieten größere Kontrolle über Dateiberechtigungen. Sie fügen ACLs hinzu, wenn der traditionelle UNIX-Dateischutz nicht ausreicht. Traditioneller UNIX-Dateischutz bietet Lese-, Schreib- und Ausführungsberechtigungen für drei Benutzerklassen: Dateieigentümer, Dateigruppe und andere Benutzer. Mit ACLs kann die Dateisicherheit genauer bestimmt werden.

ACLs ermöglichen die Definition der folgenden Dateiberechtigungen:

- Dateiberechtigungen für den Eigentümer
- Dateiberechtigungen für die Gruppe des Eigentümers
- Dateiberechtigungen für andere Benutzer, die sich nicht in der Gruppe des Eigentümers befinden
- Dateiberechtigungen für bestimmte Benutzer
- Dateiberechtigungen für bestimmte Gruppen
- Standardberechtigungen für jede der oben stehenden Kategorien

Weitere Informationen zur Verwendung von ACLs finden Sie unter „Schützen von UFS-Dateien mithilfe von Zugriffssteuerungslisten“ auf Seite 138.

Gemeinsames Nutzen von Dateien auf Rechnern

Ein Netzwerkdateiserver kann steuern, welche Dateien gemeinsam genutzt werden können. Außerdem kann er steuern, welche Clients Zugriff auf die Dateien haben und welche Art von Zugriff diesen Clients gewährt wird. Im Allgemeinen kann der Dateiserver Lese- und Schreibzugriff oder nur Lesezugriff auf einen oder alle Clients oder bestimmte Clients gewähren. Die Zugriffssteuerung wird angegeben, wenn Ressourcen mit dem Befehl `share` zur Verfügung gestellt werden.

In der Datei `/etc/dfs/dfstab` auf dem Dateiserver werden die Dateisysteme aufgelistet, die der Server Clients auf dem Netzwerk zur Verfügung stellt. Weitere Informationen zur gemeinsamen Nutzung von Dateisystemen finden Sie unter „Automatische Freigabe von Dateisystemen“ in *Systemverwaltungshandbuch: Netzwerkdienste*.

Wenn Sie eine NFS-Freigabe auf einem ZFS-Dateisystem erstellen, wird das Dateisystem dauerhaft zur gemeinsamen Nutzung freigegeben, bis Sie dies aufheben. SMF implementiert die gemeinsame Nutzung automatisch, wenn das System neu gestartet wird. Weitere Informationen finden Sie in Kapitel 3, „Unterschiede zwischen Oracle Solaris ZFS und herkömmlichen Dateisystemen“ in *Oracle Solaris ZFS-Administrationshandbuch*.

Beschränken des `root`-Zugriffs auf gemeinsam genutzte Dateien

Im Allgemeinen hat ein Superuser keinen `root`-Zugriff auf gemeinsam genutzte Dateisysteme in einem Netzwerk. Das NFS-System verhindert `root`-Zugriff auf eingehängte Dateisysteme, indem der Anforderer in den Benutzer `nobody` mit der Benutzer-ID `60001` umgewandelt wird. Der Benutzer `nobody` hat die gleichen Zugriffsrechte wie die Öffentlichkeit. Der Benutzer `nobody` hat die Zugriffsrechte eines Benutzers ohne Berechtigungsnachweise. Wenn die

Öffentlichkeit beispielsweise nur über eine Ausführungsberechtigung für eine Datei verfügt, kann der Benutzer `nobody` diese Datei nur ausführen.

Ein NFS-Server kann Superuser-Fähigkeiten für ein gemeinsam genutztes Dateisystem pro Host ermöglichen. Um diese Berechtigungen zu gewähren, verwenden Sie `root=`*hostname* als Option des Befehls `share`. Verwenden Sie diese Option nur nach sorgfältigen Überlegungen. Eine Beschreibung der Sicherheitsoptionen für NFS finden Sie in Kapitel 6, „Zugreifen auf Netzwerkdateisysteme (Referenz) “ in *Systemverwaltungshandbuch: Netzwerkdienste*.

Steuern von Netzwerkzugriff

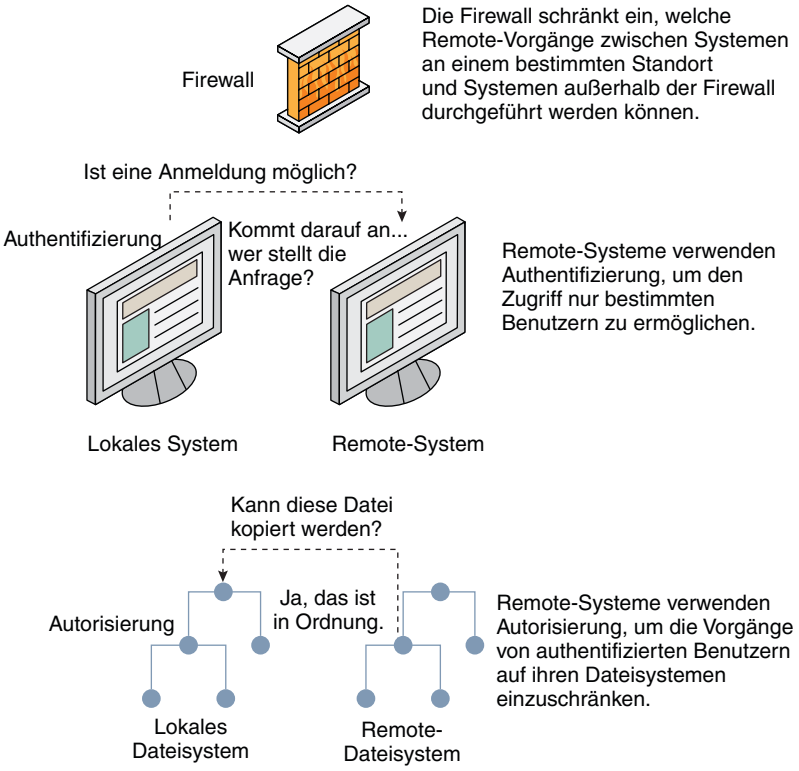
Computer gehören oft zu einem *Netzwerk* von Computern. Ein Netzwerk ermöglicht den Austausch von Informationen zwischen Computern. Vernetzte Computer können auf die Daten und anderen Ressourcen von anderen Computern im Netzwerk zugreifen. Computernetzwerke stellen leistungsfähige und fortschrittliche Computerumgebungen dar. Durch Netzwerke wird aber auch die Sicherheit von Computern zu einem komplexen Thema.

Innerhalb eines Computernetzwerks können die einzelnen Systeme Informationen gemeinsam nutzen. Unberechtigter Zugriff stellt ein Sicherheitsrisiko dar. Da viele Benutzer Zugriff auf ein Netzwerk haben, treten unberechtigte Zugriffe häufiger auf, besonders durch Benutzerfehler. Darüber hinaus kann eine ineffiziente Verwendung von Passwörtern unberechtigte Zugriffe ermöglichen.

Netzwerksicherheitsmechanismen

Die Netzwerksicherheit basiert normalerweise auf der Einschränkung oder Verhinderung von Vorgängen über Remote-Systeme. Die folgende Abbildung veranschaulicht die Sicherheitsbeschränkungen, die für Remote-Vorgänge möglich sind.

ABBILDUNG 2–1 Sicherheitsbeschränkungen für Remote-Vorgänge



Authentifizierung und Autorisierung für Remote-Zugriff

Authentifizierung ist eine Möglichkeit, den Zugriff auf bestimmte Benutzer zu beschränken, wenn sich diese bei einem Remote-System anmelden. Authentifizierung kann auf Systemebene und Netzwerkebene eingerichtet werden. Nachdem ein Benutzer Zugriff auf ein Remote-System erhalten hat, können die Vorgänge, die er ausführen darf, durch *Autorisierung* beschränkt werden. In der folgenden Tabelle werden die Services aufgeführt, die Authentifizierung und Autorisierung ermöglichen.

TABELLE 2–3 Authentifizierungs- und Autorisierungsservices für Remote-Zugriff

Service	Beschreibung	Weitere Informationen
IPsec	IPsec bietet eine host- und zertifikatbasierte Authentifizierung und Netzwerkverkehr-Verschlüsselung.	Kapitel 19, „IP Security Architecture (Übersicht)“ in *Systemverwaltungshandbuch: IP Services*

TABELLE 2–3 Authentifizierungs- und Autorisierungsservices für Remote-Zugriff *(Fortsetzung)*

Service	Beschreibung	Weitere Informationen
Kerberos	Kerberos verwendet Verschlüsselung zur Authentifizierung und Autorisierung eines Benutzers, der sich beim System anmeldet.	Ein Beispiel finden Sie unter „Funktionsweise des Kerberos-Service“ auf Seite 408.
LDAP und NIS+	Der LDAP-Directory Service und der NIS+-Naming Service können Authentifizierung und Autorisierung auf Netzwerkebene bereitstellen.	*Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)* und *System Administration Guide: Naming and Directory Services (NIS+)*
Remote-Anmeldungsbefehle	Remote-Anmeldungsbefehle ermöglichen Benutzern die Anmeldung bei einem Remote-System über das Netzwerk und die Verwendung seiner Ressourcen. Zu den Remote-Anmeldungsbefehlen gehören `rlogin`, `rcp` und `ftp`. Wenn Sie als "vertrauenswürdiger Host" eingestuft sind, erfolgt die Authentifizierung automatisch. Andernfalls müssen Sie sich authentifizieren.	Kapitel 29, „Zugriff auf Remote-Systeme (Aufgaben)“ in *Systemverwaltungshandbuch: Netzwerkdienste*
SASL	Simple Authentication and Security Layer (SASL) ist ein Framework, das von Netzwerkprotokollen zur Authentifizierung verwendet wird und optionale Sicherheitsservices bietet. Plugins ermöglichen die Auswahl eines geeigneten Authentifizierungsprotokolls.	„SASL (Übersicht)“ auf Seite 361
Secure RPC	Secure RPC verbessert die Sicherheit von Netzwerkumgebungen durch Authentifizierung der Benutzer, die Anforderungen auf Remote-Rechnern stellen. Sie können ein UNIX-, DES- oder Kerberos-Authentifizierungssystem für Secure RPC verwenden.	„Übersicht zu Secure RPC“ auf Seite 335
	Secure RPC kann außerdem verwendet werden, um die Sicherheit in einer NFS-Umgebung zu erhöhen. Eine NFS-Umgebung mit Secure RPC wird als Secure NFS bezeichnet. In einer Secure NFS-Umgebung wird die Diffie-Hellman-Authentifizierung für öffentliche Schlüssel verwendet.	„NFS-Services und Secure RPC“ auf Seite 335
Secure Shell	Secure Shell verschlüsselt den Netzwerkverkehr über ein ungesichertes Netzwerk. Secure Shell bietet eine Authentifizierung mithilfe von Passwörtern, öffentlichen Schlüsseln oder beidem. Secure Shell verwendet RSA- und DSA-Authentifizierung für öffentliche Schlüssel.	„Oracle Solaris Secure Shell (Übersicht)“ auf Seite 365

Eine mögliche Alternative zu Secure RPC ist der Oracle Solaris-Mechanismus für *privilegierte Ports*. Einem privilegiertem Port wird eine Portnummer unter `1024` zugewiesen. Nachdem ein Clientsystem den Berechtigungsnachweis eines Clients authentifiziert hat, erstellt der Client eine Verbindung zum Server unter Verwendung des privilegiertem Ports. Dieser Server überprüft den Berechtigungsnachweis des Clients anhand der Portnummer der Verbindung.

Clients, auf denen die Oracle Solaris-Software nicht ausgeführt wird, können möglicherweise nicht über den privilegierten Port kommunizieren. Wenn die Clients nicht über den Port kommunizieren können, wird eine Fehlermeldung ähnlich der folgenden angezeigt:

```
“Weak Authentication
NFS request from unprivileged port”
```

Firewall-Systeme

Sie können ein Firewall-System einrichten, um die Ressourcen in Ihrem Netzwerk vor Zugriff von Außen zu schützen. Ein *Firewall-System* ist ein sicherer Host, der das interne gegenüber dem externen Netzwerk abgrenzt. Das interne Netzwerk behandelt alle anderen Netzwerke als nicht vertrauenswürdig. Betrachten Sie dies als obligatorische Einrichtung für Ihr internes Netzwerk und alle externen Netzwerke, wie dem Internet, mit denen Sie kommunizieren.

Eine Firewall hat die Funktion eines Gateways und einer Barriere. Eine Firewall fungiert als Gateway, das Daten zwischen Netzwerken überträgt. Eine Firewall fungiert als Barriere, die die Übertragung von Daten in und aus dem Netzwerk blockiert. Benutzer im internen Netzwerk müssen sich beim Firewall-System anmelden, um auf Hosts in Remote-Netzwerken zuzugreifen. Ähnlich muss ein Benutzer in einem externen Netzwerk sich zunächst bei einem Firewall-System anmelden, bevor er Zugriff auf einen Host im internen Netzwerk erhält.

In manchen Fällen kann auch eine Firewall zwischen internen Netzwerken nützlich sein. Beispielsweise können Sie eine Firewall oder einen sicheren Gateway-Computer einrichten, um die Übertragung von Paketen zu beschränken. Das Gateway kann den Austausch von Paketen zwischen zwei Netzwerken unterbinden, es sei denn der Gateway-Computer ist die Ausgangs- oder Zieladresse des Pakets. Eine Firewall sollte außerdem so eingerichtet sein, dass nur Pakete für bestimmte Protokolle weitergeleitet werden. Beispielsweise können Sie Pakete zur Übertragung von Mail zulassen, Pakete für die Befehle `telnet` oder `rlogin` jedoch nicht. Wird ASET mit einer hohen Sicherheitsstufe ausgeführt, wird die Weiterleitung von Internet Protocol-Paketen (IP) deaktiviert.

Darüber hinaus werden alle E-Mails aus dem internen Netzwerk zuerst an das Firewall-System gesendet. Die Firewall überträgt dann die Mail an einen Host in einem externen Netzwerk. Das Firewall-System empfängt außerdem alle eingehenden Mails und verteilt sie an die Hosts im internen Netzwerk.

Achtung – Eine Firewall verhindert, dass unberechtigte Benutzer auf die Hosts in Ihrem Netzwerk zugreifen. Sie sollten strenge und konsequent durchgesetzte Sicherheitsmaßnahmen für Ihre Firewall einsetzen, die Sicherheitsmaßnahmen auf anderen Hosts im Netzwerk können dagegen lockerer sein. Ein Eindringling, der Ihre Firewall durchbricht, hat dann allerdings Zugriff auf alle anderen Hosts im internen Netzwerk.

Ein Firewall-System sollte keine vertrauenswürdigen Hosts haben. Ein *vertrauenswürdiger Host* ist ein Host, auf dem sich ein Benutzer ohne Passwort anmelden kann. Ein Firewall-System sollte keine eigenen Dateisysteme zur gemeinsamen Nutzung freigeben oder Dateisysteme von anderen Hosts einhängen.

Mit den folgenden Technologien kann ein System zu einer Firewall verstärkt werden:

- ASET setzt hohe Sicherheit auf einem Firewall-System durch, wie in Kapitel 7, „Verwenden von Automated Security Enhancement Tool (Aufgaben)“ beschrieben.
- Das Oracle Solaris Security Toolkit, inoffiziell auch als JASS-Toolkit bezeichnet, kann ein Oracle Solaris-System zu einer Firewall verstärken. Das Toolkit kann von der Sun Downloads-Website Oracle Sun (`http://www.oracle.com/us/sun/index.htm`) heruntergeladen werden.
- IPsec und Oracle Solaris-IP-Filter können für Firewall-Schutz sorgen. Weitere Informationen zum Schutz von Netzwerkverkehr finden Sie unter Teil IV, „IP-Sicherheit“ in *Systemverwaltungshandbuch: IP Services*.

Verschlüsselung und Firewall-Systeme

In den meisten lokalen Netzwerken werden Daten zwischen Computern in Blöcken übertragen, die auch als *Pakete* bezeichnet werden. Durch *Paketzerstörung* können unberechtigte Benutzer von außerhalb des Netzwerks Daten beschädigen oder zerstören.

Dabei werden Pakete abgefangen, bevor sie ihr Ziel erreichen. Sie werden mit willkürlichen Daten gefüllt und wieder auf den ursprünglichen Weg geschickt. In einem lokalen Netzwerk können keine Pakete auf diese Art zerstört werden, da sie alle Systeme, einschließlich des Servers, gleichzeitig erreichen. Auf einem Gateway können jedoch Pakete zerstört werden. Stellen Sie also sicher, dass alle Gateways im Netzwerk geschützt sind.

Am gefährlichsten sind die Angriffe auf die Integrität der Daten. Dabei wird der Inhalt der Pakete geändert oder ein Angreifer gibt sich als Benutzer aus. Abhörangriffe gefährden die Datenintegrität nicht. Stattdessen wird der Verkehr zur späteren Wiedergabe aufgezeichnet. Die abhörende Person gibt sich nicht als Benutzer aus. Abhörangriffe beeinträchtigen zwar nicht die Datenintegrität, stellen jedoch eine Verletzung des Datenschutzes dar. Sie können vertrauliche Informationen schützen, indem Sie die über das Netzwerk versendeten Daten verschlüsseln.

- Informationen zur Verschlüsselung von Remote-Vorgängen in einem unsicheren Netzwerk finden Sie in Kapitel 19, „Verwenden von Oracle Solaris Secure Shell (Aufgaben)“.
- Informationen zur Verschlüsselung und Authentifizierung von Daten in einem Netzwerk finden Sie in Kapitel 21, „Einführung zum Kerberos-Service“.
- Informationen zur Verschlüsselung von IP-Datagrammen finden Sie in Kapitel 19, „IP Security Architecture (Übersicht)“ in *Systemverwaltungshandbuch: IP Services*.

Melden von Sicherheitsproblemen

Bei Verdacht auf eine Sicherheitsverletzung können Sie sich an das Computer Emergency Response Team/Coordination Center (CERT/CC) wenden. CERT/CC ist ein von der Defense Advanced Research Projects Agency (DARPA) gefördertes Projekt, das am Software Engineering Institute der Carnegie Mellon University durchgeführt wird. Diese Organisation unterstützt Sie bei Sicherheitsproblemen. Sie kann Sie an andere Computer Emergency Response Teams weiterleiten, die für Ihre Anforderungen geeigneter sind. Aktuelle Kontaktinformationen finden Sie auf der Website CERT/CC (`http://www.cert.org/contact_cert/`).

◆ ◆ ◆ KAPITEL 3

Steuern des Zugriffs auf Systeme (Aufgaben)

In diesem Kapitel werden die Verfahren beschrieben, mit denen gesteuert werden kann, wer auf Oracle Solaris-Systeme Zugriff hat. Im Folgenden ist eine Liste der Informationen in diesem Kapitel aufgeführt.

- „Steuern von Systemzugriff (Übersicht der Schritte)“ auf Seite 63
- „Schützen von Anmeldungen und Passwörtern (Übersicht der Schritte)“ auf Seite 64
- „Ändern des Passwortalgorithmus (Übersicht der Schritte)“ auf Seite 72
- „Überwachen und Beschränken des Superusers (Übersicht der Schritte)“ auf Seite 77
- „SPARC: Steuern von Zugriff auf Systemhardware (Übersicht der Schritte)“ auf Seite 80

Eine Übersicht über Systemsicherheit finden Sie in Kapitel 2, „Verwalten von Rechnersicherheit (Übersicht)“.

Steuern von Systemzugriff (Übersicht der Schritte)

Ein System ist so sicher wie sein schwächster Eintrittspunkt. In der folgenden Übersicht der Schritte werden die Bereiche aufgeführt, die Sie überwachen und schützen müssen.

Aufgabe	Description (Beschreibung)	Anweisungen
Überwachen, Erlauben und Verweigern von Benutzeranmeldungen	Dient zum Überwachen ungewöhnlicher Anmeldeaktivität. Verhindert Anmeldungen vorübergehend. Verwaltet Einwahlanmeldungen	„Schützen von Anmeldungen und Passwörtern (Übersicht der Schritte)“ auf Seite 64
Bereitstellen von starker Passwortverschlüsselung	Gibt Algorithmen zur Verschlüsselung von Benutzerpasswörtern an. Installiert zusätzliche Algorithmen	„Ändern des Passwortalgorithmus (Übersicht der Schritte)“ auf Seite 72
Überwachen und Einschränken von Superuser-Aktivitäten	Überwacht regelmäßig die Superuser-Aktivität. Verhindert Remote-Anmeldung eines `root`-Benutzers	„Überwachen und Beschränken des Superusers (Übersicht der Schritte)“ auf Seite 77

Aufgabe	Description (Beschreibung)	Anweisungen
Verhindern von Zugriff auf Hardware-Einstellungen	Verhindert, dass normale Benutzer auf den PROM zugreifen können	„SPARC: Steuern von Zugriff auf Systemhardware (Übersicht der Schritte)“ auf Seite 80

Schützen von Anmeldungen und Passwörtern (Übersicht der Schritte)

In der folgenden Übersicht werden Verfahren zum Überwachen und Deaktivieren von Benutzeranmeldungen genannt.

Aufgabe	Description (Beschreibung)	Anweisungen
Anzeigen des Anmeldestatus eines Benutzers	Bietet ausführliche Informationen zum Anmeldekonto eines Benutzers, beispielsweise vollständiger Name und Passwort-Datierungsinformationen	„So zeigen Sie den Anmeldestatus eines Benutzers an“ auf Seite 65
Anzeigen von Benutzern ohne Passwort	Zeigt nur die Benutzer an, für deren Konten kein Passwort erforderlich ist	„So zeigen Sie Benutzer ohne Passwort an“ auf Seite 66
Vorübergehendes Deaktivieren von Anmeldungen	Verhindert während einer Systemabschaltung oder Routinewartung vorübergehend, dass sich ein Benutzer auf einem Rechner anmelden kann	„So deaktivieren Sie Benutzeranmeldungen vorübergehend“ auf Seite 67
Aufzeichnen von fehlgeschlagenen Anmeldeversuchen	Erstellt eine Protokolldatei der Benutzer, die nach fünf Versuchen immer noch nicht das richtige Passwort eingegeben haben	„So überwachen Sie fehlgeschlagene Anmeldeversuche“ auf Seite 67
Aufzeichnen aller fehlgeschlagenen Anmeldeversuche	Zeichnet fehlgeschlagene Anmeldeversuche in einer Protokolldatei auf	„So überwachen Sie alle fehlgeschlagenen Anmeldeversuche“ auf Seite 68
Erstellen eines Einwahl-Passworts	Fordert Remote-Benutzer, die sich über ein Modem oder einen Einwahlport anmelden, zur Eingabe eines zusätzlichen Passworts auf	„So erstellen Sie ein Einwahl-Passwort“ auf Seite 70
Vorübergehendes Deaktivieren von Einwahlanmeldungen	Hindert Remote-Benutzer an der Einwahl über ein Modem oder einen Port	„So deaktivieren Sie Einwahl-Anmeldungen vorübergehend“ auf Seite 72

Schützen von Anmeldungen und Passwörtern

Sie können Remote-Anmeldungen einschränken und festlegen, dass Benutzer Passwörter benötigen. Sie können außerdem fehlgeschlagene Zugriffsversuche überwachen und Anmeldungen vorübergehend deaktivieren.

▼ So zeigen Sie den Anmeldestatus eines Benutzers an

1 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Zeigen Sie mit dem Befehl `logins` den Anmeldestatus eines Benutzers an.**

`# logins -x -l` *username*

`-x`	Zeigt einen erweiterten Satz von Anmeldestatusinformationen an
`-l` *username*	Zeigt den Anmeldestatus des angegebenen Benutzers an. Die Variable *username* entspricht dem Anmeldenamen eines Benutzers. Mehrere Anmeldedaten müssen in einer durch Komma getrennten Liste angegeben werden.

Der Befehl `logins` ruft den Anmeldestatus des Benutzers aus der entsprechenden Passwortdatenbank ab. Bei der Datenbank kann es sich um die lokale Datei `/etc/passwd` oder eine Passwortdatenbank des Naming Service handeln. Weitere Informationen finden Sie auf der Manpage `logins(1M)`.

Beispiel 3–1 Anzeigen des Anmeldestatus eines Benutzers

In dem folgenden Beispiel wird der Anmeldestatus des Benutzers `rimmer` angezeigt.

```
# logins -x -l rimmer
rimmer       500     staff           10   Annalee J. Rimmer
                     /export/home/rimmer
                     /bin/sh
                     PS 010103 10 7 -1
```

`rimmer`	Entspricht dem Anmeldenamen des Benutzers
`500`	Entspricht der Benutzer-ID (UID, User ID)
`staff`	Entspricht der primären Gruppe des Benutzers
`10`	Entspricht der Gruppen-ID (GID)

`Annalee J. Rimmer`	Entspricht dem Kommentar
`/export/home/rimmer`	Entspricht dem Home-Verzeichnis des Benutzers
`/bin/sh`	Entspricht der Anmelde-Shell
`PS 010170 10 7 -1`	Gibt die Passwort-Datierungsinformationen an: ■ Datum der letzten Passwortänderung ■ Anzahl der Tage, die zwischen Änderungen erforderlich sind ■ Anzahl der Tage, bevor eine Änderung erforderlich ist ■ Warnungszeitraum

▼ So zeigen Sie Benutzer ohne Passwort an

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Zeigen Sie mit dem Befehl `logins` alle Benutzer ohne Passwort an.

```
# logins -p
```

Mit der Option `-p` zeigen Sie eine Liste von Benutzern ohne Passwort an. Der Befehl `logins` greift auf die Passwortdatenbank des lokalen Systems zu, wenn kein Naming Service aktiviert ist.

Beispiel 3–2 Anzeigen von Benutzern ohne Passwort

In dem folgenden Beispiel verfügt der Benutzer `pmorph` über kein Passwort.

```
# logins -p
pmorph          501     other           1       Polly Morph
#
```

▼ So deaktivieren Sie Benutzeranmeldungen vorübergehend

Deaktivieren Sie Benutzeranmeldungen vorübergehend während einer Systemabschaltung oder Routinewartung. Superuser-Anmeldungen sind nicht betroffen. Weitere Informationen finden Sie auf der Manpage `nologin(4)`.

1. **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

   Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Erstellen Sie die Datei `/etc/nologin` in einem Texteditor.**

   ```
   # vi /etc/nologin
   ```

3. **Geben Sie eine Nachricht zur Systemverfügbarkeit ein.**

4. **Schließen und speichern Sie die Datei.**

Beispiel 3–3 Deaktivieren von Benutzeranmeldungen

In diesem Beispiel werden Benutzer darüber informiert, dass das System nicht verfügbar ist.

```
# vi /etc/nologin
(Add system message here)

# cat /etc/nologin
***No logins permitted.***

***The system will be unavailable until 12 noon.***
```

Sie können das System auch auf Runlevel 0, Einzelbenutzermodus, herunterschalten, um Anmeldungen zu deaktivieren. Weitere Informationen zum Herunterschalten des Systems in den Einzelbenutzermodus finden Sie in Kapitel 10, „Shutting Down a System (Tasks)“ in *System Administration Guide: Basic Administration*.

▼ So überwachen Sie fehlgeschlagene Anmeldeversuche

Mit diesem Verfahren können Sie fehlgeschlagene Anmeldeversuche von Terminalfenstern überwachen. Anmeldeversuche oder fehlgeschlagene Anmeldeversuche von einer CDE können nicht verfolgt werden.

1. **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

   Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Erstellen Sie die Datei `loginlog` im Verzeichnis `/var/adm`.**

   ```
   # touch /var/adm/loginlog
   ```

3. **Legen Sie fest, dass der `root`-Benutzer über Lese- und Schreibzugriff auf die Datei `loginlog` verfügt.**

   ```
   # chmod 600 /var/adm/loginlog
   ```

4. **Ändern Sie die Gruppenmitgliedschaft der Datei `loginlog` in `sys`.**

   ```
   # chgrp sys /var/adm/loginlog
   ```

5. **Vergewissern Sie sich, dass Anmeldeversuche im Protokoll gespeichert werden.**

   Melden Sie sich beispielsweise fünfmal mit dem falschen Passwort an. Zeigen Sie dann die Datei `/var/adm/loginlog` an.

   ```
   # more /var/adm/loginlog
   jdoe:/dev/pts/2:Tue Nov  4 10:21:10 2010
   jdoe:/dev/pts/2:Tue Nov  4 10:21:21 2010
   jdoe:/dev/pts/2:Tue Nov  4 10:21:30 2010
   jdoe:/dev/pts/2:Tue Nov  4 10:21:40 2010
   jdoe:/dev/pts/2:Tue Nov  4 10:21:49 2010
   #
   ```

   Die Datei `loginlog` enthält für jeden fehlgeschlagenen Versuch einen Eintrag. Jeder Eintrag enthält den Anmeldenamen des Benutzers, TTY-Gerät und die Uhrzeit des fehlgeschlagenen Versuchs. Bei weniger als fünf fehlgeschlagenen Versuchen werden keine Einträge in das Protokoll aufgenommen.

   Wenn sich die Datei `loginlog` vergrößert, kann dies auf einen Einbruchsversuch in das Computersystem deuten. Überprüfen und löschen Sie deshalb regelmäßig den Inhalt der Datei. Weitere Informationen finden Sie auf der Manpage `loginlog(4)`.

▼ So überwachen Sie alle fehlgeschlagenen Anmeldeversuche

Mit diesem Verfahren werden alle fehlgeschlagenen Anmeldeversuche im `syslog` aufgezeichnet.

1. **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

   Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Richten Sie die Datei `/etc/default/login` mit den gewünschten Werten für `SYSLOG` und `SYSLOG_FAILED_LOGINS` ein.**

   Bearbeiten Sie die Datei `/etc/default/login`, um den Eintrag zu ändern. Stellen Sie sicher, dass **`SYSLOG=YES`** nicht auskommentiert ist.

   ```
   # grep SYSLOG /etc/default/login
   # SYSLOG determines whether the syslog(3) LOG_AUTH facility
   # should be used
   SYSLOG=YES
   ...
   SYSLOG_FAILED_LOGINS=0
   #
   ```

3. **Erstellen Sie eine Datei mit den richtigen Berechtigungen, um die Protokollinformationen aufzunehmen.**

   a. **Erstellen Sie die Datei `authlog` im Verzeichnis `/var/adm`.**

      ```
      # touch /var/adm/authlog
      ```

   b. **Legen Sie fest, dass der `root`-Benutzer über Lese- und Schreibzugriff auf die Datei `authlog` verfügt.**

      ```
      # chmod 600 /var/adm/authlog
      ```

   c. **Ändern Sie die Gruppenmitgliedschaft der Datei `authlog` in `sys`.**

      ```
      # chgrp sys /var/adm/authlog
      ```

4. **Bearbeiten Sie die Datei `syslog.conf`, um fehlgeschlagene Anmeldeversuche aufzuzeichnen.**

   Die Fehlschläge sollten in die Datei `authlog` geschrieben werden.

   a. **Geben Sie den folgenden Eintrag in die Datei `syslog.conf` ein.**

      Felder in derselben Zeile müssen in `syslog.conf` durch Tabulatorzeichen getrennt werden.

      ```
      auth.notice     <Press Tab>  /var/adm/authlog
      ```

   b. **Aktualisieren Sie die Konfigurationsinformationen für den Dämon `syslog`.**

      ```
      # svcadm refresh system/system-log
      ```

5 **Vergewissern Sie sich, dass Anmeldeversuche im Protokoll gespeichert werden.**

Melden Sie sich beispielsweise als normaler Benutzer mit einem falschen Passwort beim System an. Zeigen Sie dann mit der Rolle "Primary Administrator" oder als Superuser die Datei `/var/adm/authlog` an.

```
# more /var/adm/authlog
Nov  4 14:46:11 example1 login: [ID 143248 auth.notice]
 Login failure on /dev/pts/8 from example2, stacey
#
```

6 **Überwachen Sie regelmäßig die Datei `/var/adm/authlog`.**

Beispiel 3–4 Protokollieren von Anmeldeversuchen nach drei fehlgeschlagenen Anmeldungen

Führen Sie das oben stehende Verfahren aus mit dem Unterschied, dass Sie `SYSLOG_FAILED_LOGINS` in der Datei `/etc/default/login` auf `3` einstellen.

Beispiel 3–5 Trennen der Verbindung nach drei fehlgeschlagenen Anmeldungen

Entfernen Sie die Auskommentierung von `RETRIES` in der Datei `/etc/default/login` und stellen Sie den Wert von `RETRIES` auf `3` ein. Ihre Änderungen sind sofort wirksam. Nach drei Anmeldeversuchen in einer Sitzung wird die Verbindung des Systems getrennt.

▼ So erstellen Sie ein Einwahl-Passwort

Achtung – Achten Sie bei der ersten Einrichtung eines Einwahl-Passworts darauf, bei mindestens einem Port angemeldet zu bleiben. Testen Sie das Passwort auf einem anderen Port. Wenn Sie sich abmelden, um das neue Passwort zu testen, können Sie sich möglicherweise nicht mehr anmelden. Wenn Sie weiterhin bei einem anderen Port angemeldet sind, können Sie zurückkehren und den Fehler korrigieren.

1 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Erstellen Sie eine Datei `/etc/dialups`, die eine Liste von seriellen Geräten enthält.

Schließen Sie alle Ports ein, die durch Einwahl-Passwörter geschützt werden. Die Datei `/etc/dialups` sollte etwa folgendermaßen aussehen:

```
/dev/term/a
/dev/term/b
/dev/term/c
```

3 Erstellen Sie eine Datei `/etc/d_passwd` mit den Anmeldeprogrammen, für die ein Einwahl-Passwort erforderlich sein soll.

Schließen Sie die Shell-Programme ein, die ein Benutzer bei der Anmeldung ausführen kann, beispielsweise `uucico`, `sh`, `ksh` und `csh`. Die Datei `/etc/d_passwd` sollte etwa folgendermaßen aussehen:

```
/usr/lib/uucp/uucico:encrypted-password:
/usr/bin/csh:encrypted-password:
/usr/bin/ksh:encrypted-password:
/usr/bin/sh:encrypted-password:
/usr/bin/bash:encrypted-password:
```

Zu einem späteren Zeitpunkt fügen Sie in diesem Verfahren das verschlüsselte Passwort für die einzelnen Anmeldeprogramme hinzu.

4 Legen Sie fest, dass `root` der Eigentümer der beiden Dateien ist.

```
# chown root /etc/dialups /etc/d_passwd
```

5 Legen Sie `root` als Gruppeneigentümerschaft für die beiden Dateien fest.

```
# chgrp root /etc/dialups /etc/d_passwd
```

6 Legen Sie fest, dass der `root`-Benutzer über Lese- und Schreibzugriff auf die beiden Dateien verfügt.

```
# chmod 600 /etc/dialups /etc/d_passwd
```

7 Erstellen Sie die verschlüsselten Passwörter.

a. Erstellen Sie einen vorübergehenden Benutzer.

```
# useradd username
```

b. Erstellen Sie ein Passwort für den vorübergehenden Benutzer.

```
# passwd username
New Password:       <Type password>
Re-enter new Password:        <Retype password>
passwd: password successfully changed for username
```

c. Erfassen Sie das verschlüsselte Passwort.

```
# grep username /etc/shadow > username.temp
```

d. Bearbeiten Sie die Datei *username*.temp.

Löschen Sie alle Felder außer dem verschlüsselten Passwort. Das zweite Feld enthält das verschlüsselte Passwort.

Beispielsweise enthält die folgende Zeile das verschlüsselte Passwort `U9gp9SyA/JlSk`.

```
temp:U9gp9SyA/JlSk:7967:::::7988:
```

e. Löschen Sie den vorübergehenden Benutzer.

```
# userdel username
```

8 Kopieren Sie das verschlüsselte Passwort aus der Datei *username*`.temp` in die Datei `/etc/d_passwd`.

Sie können ein anderes Passwort für jede Anmelde-Shell erstellen. Sie können auch für jede Anmelde-Shell das gleiche Passwort verwenden.

9 Teilen Sie Ihren Einwahl-Benutzern das Passwort mit.

Achten Sie darauf, dass dies auf sicherem Wege geschieht.

▼ So deaktivieren Sie Einwahl-Anmeldungen vorübergehend

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Fügen Sie folgenden einzeiligen Eintrag in die Datei `/etc/d_passwd` ein:

```
/usr/bin/sh:*:
```

Ändern des Passwortalgorithmus (Übersicht der Schritte)

Die folgende Übersicht der Schritte enthält Verfahren zur Verwaltung von Passwortalgorithmen.

Aufgabe	Anweisungen
Bereitstellen von starker Passwortverschlüsselung	„So geben Sie einen Algorithmus zur Passwortverschlüsselung an“ auf Seite 73

Aufgabe	Anweisungen
Bereitstellen starker Passwortverschlüsselung mit einem Naming Service	„So geben Sie einen neuen Passwortalgorithmus für eine NIS-Domain an“ auf Seite 74
	„So geben Sie einen neuen Passwortalgorithmus für eine NIS+-Domain an“ auf Seite 75
	„So geben Sie einen neuen Passwortalgorithmus für eine LDAP-Domain an“ auf Seite 75
Hinzufügen neuer Module zur Passwortverschlüsselung	„So installieren Sie ein Passwortverschlüsselungsmodul eines anderen Anbieters“ auf Seite 76

Ändern des Standardalgorithmus zur Passwortverschlüsselung

Standardmäßig werden Benutzerpasswörter mit `crypt_unix`-Algorithmen verschlüsselt. Sie können statt des Standard-Verschlüsselungsalgorithmus auch einen stärkeren Algorithmus wie MD5 oder Blowfish verwenden.

▼ So geben Sie einen Algorithmus zur Passwortverschlüsselung an

In diesem Verfahren ist die BSD-Linux-Version des MD5-Algorithmus der Standard-Verschlüsselungsalgorithmus, der verwendet wird, wenn Benutzer ihr Passwort ändern. Dieser Algorithmus ist für ein Netzwerk mit Rechnern geeignet, auf denen die Oracle Solaris-, BSD- und Linux-Versionen von UNIX ausgeführt werden. Eine Liste von Passwortverschlüsselungsalgorithmen und Algorithmuskennungen finden Sie in Tabelle 2–1.

1 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Geben Sie die Kennung für den gewünschten Verschlüsselungsalgorithmus an.**

Geben Sie die Kennung als Wert der Variablen `CRYPT_DEFAULT` in der Datei `/etc/security/policy.conf` ein.

Sie sollten einen Kommentar in die Datei einfügen, um Ihre Wahl zu erläutern.

```
# cat  /etc/security/policy.conf
...
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6
```

```
#
# Use the version of MD5 that works with Linux and BSD systems.
# Passwords previously encrypted with __unix__ will be encrypted with MD5
# when users change their passwords.
#
#
CRYPT_DEFAULT=__unix__
CRYPT_DEFAULT=1
```

In diesem Beispiel stellt die Algorithmuskonfiguration sicher, dass der schwächste Algorithmus, `crypt_unix`, nicht zum Verschlüsseln von Passwörtern verwendet wird. Benutzer, deren Passwörter mit dem Modul `crypt_unix` verschlüsselt wurden, erhalten ein mit `crypt_bsdmd5` verschlüsseltes Passwort, wenn sie ihr Passwort ändern.

Weitere Informationen zur Konfiguration von Algorithmusoptionen finden Sie auf der Manpage `policy.conf(4)`.

Beispiel 3–6 Verwenden des Blowfish-Algorithmus zur Passwortverschlüsselung

In diesem Beispiel ist die Kennung für den Blowfish-Algorithmus, `2a`, als Wert der Variablen `CRYPT_DEFAULT` in der Datei `policy.conf` angegeben:

```
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6
#CRYPT_ALGORITHMS_DEPRECATE=__unix__
CRYPT_DEFAULT=2a
```

Diese Konfiguration ist mit BSD-Systemen kompatibel, die den Blowfish-Algorithmus verwenden.

▼ So geben Sie einen neuen Passwortalgorithmus für eine NIS-Domain an

Wenn ein Benutzer in einer NIS-Domain sein Passwort ändert, ruft der NIS-Client die lokale Algorithmuskonfiguration in der Datei `/etc/security/policy.conf` ab. Der NIS-Clientrechner verschlüsselt das Passwort.

1. **Geben Sie den Passwortverschlüsselungsalgorithmus in die Datei `/etc/security/policy.conf` auf dem NIS-Client ein.**
2. **Kopieren Sie die Datei `/etc/security/policy.conf` auf alle Clientrechner in der NIS-Domain.**
3. **Um Verwechslungen zu vermeiden, kopieren Sie die geänderte Datei `/etc/security/policy.conf` auf den NIS-Root-Server und die Slave-Server.**

▼ So geben Sie einen neuen Passwortalgorithmus für eine NIS+-Domain an

Wenn ein Benutzer in einer NIS+-Domain sein Passwort ändert, ruft der NIS+ Naming Service die Algorithmuskonfiguration in der Datei `/etc/security/policy.conf` auf dem NIS+-Master ab. Der NIS+-Master, der den Dämon `rpc.nispasswd` ausführt, erstellt das verschlüsselte Passwort.

1. **Geben Sie den Passwortverschlüsselungsalgorithmus in die Datei `/etc/security/policy.conf` auf dem NIS+-Master ein.**

2. **Um Verwechslungen zu vermeiden, kopieren Sie die Datei `/etc/security/policy.conf` des NIS+-Masters auf jeden Host in der NIS+Domain.**

▼ So geben Sie einen neuen Passwortalgorithmus für eine LDAP-Domain an

Wenn der LDAP-Client richtig konfiguriert ist, kann er die neuen Passwortalgorithmen verwenden. Der LDAP-Client verhält sich wie ein NIS-Client.

1. **Geben Sie einen Passwortverschlüsselungsalgorithmus in der Datei `/etc/security/policy.conf` auf dem LADP-Client an.**

2. **Kopieren Sie die Datei `policy.conf` auf alle Clientrechner in der LDAP-Domain.**

3. **Stellen Sie sicher, dass die Datei `/etc/pam.conf` des Clients nicht das Modul `pam_ldap` verwendet.**

   Stellen Sie sicher, dass ein Kommentarzeichen (#) allen Einträgen vorangestellt ist, die `pam_ldap.so.1` enthalten. Verwenden Sie die neue Option `server_policy` nicht in Verbindung mit dem Modul `pam_authtok_store.so.1`.

   Die PAM-Einträge in der Datei `pam.conf` des Clients ermöglichen, dass das Passwort entsprechend der lokalen Algorithmuskonfiguration verschlüsselt wird. Die PAM-Einträge ermöglichen außerdem die Authentifizierung des Passworts.

   Wenn ein Benutzer in einer LDAP-Domain sein Passwort ändert, ruft der LDAP-Client die lokale Algorithmuskonfiguration in der Datei `/etc/security/policy.conf` ab. Der LDAP-Clientrechner verschlüsselt das Passwort. Dann sendet der Client das verschlüsselte Passwort mit einem `{crypt}`-Tag an den Server. Durch das Tag wird dem Server mitgeteilt, dass das Passwort bereits verschlüsselt ist. Das Passwort wird dann ohne nochmalige Verschlüsselung auf dem Server gespeichert. Zur Authentifizierung ruft der Client das

gespeicherte Passwort auf dem Server ab. Der Client vergleicht dann das gespeicherte Passwort mit der verschlüsselten Version, die der Client zuvor aus dem vom Benutzer eingegebenen Passwort generiert hat.

Hinweis – Um die Passwort-Richtliniensteuerung auf dem LDAP-Server zu nutzen, verwenden Sie die Option `server_policy` in Verbindung mit den `pam_authtok_store`-Einträgen in der Datei `pam.conf`. Die Passwörter werden auf dem Server mithilfe des kryptografischen Mechanismus von Sun Java System Directory Server verschlüsselt. Das Verfahren wird in Kapitel 11, „Einrichten von Sun Java System Directory Server mit LDAP-Clients (Aufgaben)“ in *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)* beschrieben.

▼ So installieren Sie ein Passwortverschlüsselungsmodul eines anderen Anbieters

Ein Passwortverschlüsselungsalgorithmus eines anderen Anbieters wird typischerweise als Modul in einem Softwarepaket bereitgestellt. Wenn Sie den Befehl `pkgadd` ausführen, wird die Datei `/etc/security/crypt.conf` von Skripten des Anbieters geändert. Fügen Sie anschließend der Datei `/etc/security/policy.conf` das neue Modul und dessen Kennung hinzu.

1 Fügen Sie die Software mit dem Befehl `pkgadd` hinzu.

Ausführliche Anweisungen zum Hinzufügen von Software finden Sie unter „Adding or Removing a Software Package (pkgadd)“ in *System Administration Guide: Basic Administration*.

2 Vergewissern Sie sich, dass das neue Modul und die Modulkennung hinzugefügt wurden.

Lesen Sie die Liste der Verschlüsselungsalgorithmen in der Datei `/etc/security/crypt.conf`.

Die folgenden Zeilen zeigen beispielsweise, dass ein Modul zur Implementierung des Algorithmus `crypt_rot13` installiert wurde.

```
# crypt.conf
#
md5 /usr/lib/security/$ISA/crypt_md5.so
rot13 /usr/lib/security/$ISA/crypt_rot13.so

# For *BSD - Linux compatibility
# 1 is MD5,  2a is Blowfish
1 /usr/lib/security/$ISA/crypt_bsdmd5.so
2a /usr/lib/security/$ISA/crypt_bsdbf.so
```

3. **Fügen Sie die Kennung des neu installierten Algorithmus der Datei `/etc/security/policy.conf` hinzu.**

   Die folgenden Zeilen zeigen Auszüge der Datei `policy.conf`, die geändert werden müssen, um die Kennung `rot13` hinzuzufügen.

```
# Copyright 1999-2002 Sun Microsystems, Inc.  All rights reserved.
# ...
#ident  "@(#)policy.conf        1.12     08/05/14 SMI"
# ...
# crypt(3c) Algorithms Configuration
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6,,rot13
#CRYPT_ALGORITHMS_DEPRECATE=__unix__
CRYPT_DEFAULT=md5
```

   In diesem Beispiel wird der Algorithmus `rot13` verwendet, wenn das aktuelle Passwort mit dem Algorithmus `crypt_rot13` verschlüsselt wurde. Die Passwörter neuer Benutzer werden mit dem Algorithmus `crypt_sunmd5` verschlüsselt. Diese Algorithmuskonfiguration funktioniert bei reinen Solaris-Netzwerken.

Überwachen und Beschränken des Superusers (Übersicht der Schritte)

In der Übersicht der Schritte wird beschrieben, wie die `root`-Benutzeranmeldung überwacht und beschränkt wird.

Aufgabe	Description (Beschreibung)	Anweisungen
Überwachen, wer den Befehl `su` ausführt	Durchsucht regelmäßig die Datei `sulog`.	„So überwachen Sie, wer den Befehl `su` ausführt“ auf Seite 78
Anzeigen von Superuser-Aktivität auf der Konsole	Überwacht die laufenden Superuser-Zugriffsversuche	„So beschränken und überwachen Sie Superuser-Anmeldungen“ auf Seite 78

Überwachen und Beschränken des Superusers

Eine Alternative zur Verwendung des Superuser-Kontos ist die Einrichtung einer rollenbasierten Zugriffssteuerung. Die rollenbasierte Zugriffssteuerung wird auch als RBAC (Role Based Access Control) bezeichnet. Eine Übersicht über RBAC finden Sie unter „Rollenbasierte Zugriffssteuerung (Übersicht)“ auf Seite 190. Informationen zur Einrichtung von RBAC finden Sie unter Kapitel 9, „Rollenbasierte Zugriffssteuerung (Aufgaben)“.

▼ So überwachen Sie, wer den Befehl `su` ausführt

In der Datei `sulog` wird jede Verwendung des Befehls `su` aufgezeichnet, nicht nur die Versuche, um mit dem Befehl `su` vom normalen zum Superuser zu wechseln.

- **Überwachen Sie regelmäßig den Inhalt der Datei `/var/adm/sulog`.**

```
# more /var/adm/sulog
SU 12/20 16:26 + pts/0 stacey-root
SU 12/21 10:59 + pts/0 stacey-root
SU 01/12 11:11 + pts/0 root-rimmer
SU 01/12 14:56 + pts/0 pmorph-root
SU 01/12 14:57 + pts/0 pmorph-root
```

Die Einträge enthalten folgende Informationen:

- Datum und Uhrzeit der Befehlseingabe
- Erfolg des Versuchs. Ein Pluszeichen (+) gibt an, dass der Versuch erfolgreich war. Ein Minuszeichen (-) kennzeichnet einen fehlgeschlagenen Versuch.
- Der Port, über den der Befehl eingegeben wurde
- Der Name des Benutzers und der Name der gewechselten Identität

Die `su`-Protokollierung in dieser Datei wird standardmäßig durch folgenden Eintrag in der Datei `/etc/default/su` aktiviert:

```
SULOG=/var/adm/sulog
```

Allgemeine Fehler

Wenn die Einträge `???` enthalten, weist das darauf hin, dass das Steuerungsterminal für den Befehl `su` nicht identifiziert werden kann. Üblicherweise enthalten Systemaufrufe des Befehls `su` vor der Desktopanzeige die Zeichen `???`, beispielsweise `SU 10/10 08:08 + ??? root-root`. Nachdem der Benutzer eine Desktopsitzung gestartet hat, gibt der Befehl `ttynam` den Wert des Steuerungsterminals an die Datei `sulog` zurück: `SU 10/10 10:10 + pts/3 jdoe-root`.

Einträge ähnlich dem folgenden können darauf hinweisen, dass der Befehl `su` nicht über die Befehlszeile aufgerufen wurde: `SU 10/10 10:20 + ??? root-oracle`. Der Benutzer kann mithilfe einer GUI zu einer `oracle`-Rolle gewechselt sein.

▼ So beschränken und überwachen Sie Superuser-Anmeldungen

Diese Methode erkennt automatisch alle Superuser-Zugriffsversuche auf das lokale System.

1. **Zeigen Sie den Eintrag `CONSOLE` in der Datei `/etc/default/login` an.**

```
CONSOLE=/dev/console
```

Standardmäßig ist für das Konsolengerät `/dev/console` eingestellt. Mit dieser Einstellung kann sich der `root`-Benutzer bei der Konsole anmelden. Der `root`-Benutzer kann keine Remote-Anmeldung durchführen.

2 Vergewissern Sie sich, dass der `root`-Benutzer keine Remote-Anmeldung durchführen kann.

Versuchen Sie, sich über ein Remote-System als Superuser anzumelden.

```
mach2 % rlogin -l root mach1
Password:      <Type root password of mach1>
Not on system console
Connection closed.
```

3 Überwachen Sie die Superuser-Anmeldungsversuche.

Standardmäßig werden Anmeldeversuche eines Superusers auf der Konsole vom Dienstprogramm `SYSLOG` ausgegeben.

a. Öffnen Sie eine Terminalkonsole auf Ihrem Desktop.

b. Geben Sie in einem anderen Fenster den Befehl `su` ein, um sich als Superuser anzumelden.

```
% su -
Password:      <Type root password>
#
```

Auf der Terminalkonsole wird eine Meldung ausgegeben.

```
Sep 7 13:22:57 mach1 su: 'su root' succeeded for jdoe on /dev/pts/6
```

Beispiel 3–7 Aufzeichnen von Superuser-Zugriffsversuchen

In diesem Beispiel werden Superuser-Anmeldeversuche nicht von `SYSLOG` aufgezeichnet. Daher sorgt der Administrator für die Aufzeichnung dieser Versuche, indem er das Kommentarzeichen vor dem Eintrag `#CONSOLE=/dev/console` in der Datei `/etc/default/su` entfernt.

```
# CONSOLE determines whether attempts to su to root should be logged
# to the named device
#
CONSOLE=/dev/console
```

Wenn ein Benutzer versucht, sich als Superuser anzumelden, wird der Versuch auf der Terminalkonsole ausgegeben.

```
SU 09/07 16:38 + pts/8 jdoe-root
```

Allgemeine Fehler Um von einem Remote-System aus Superuser-Rechte zu erhalten, wenn die Datei `/etc/default/login` den standardmäßigen `CONSOLE`-Eintrag enthält, müssen sich Benutzer zuerst mit ihrem Namen anmelden. Danach können sie mit dem Befehl `su` zum Superuser wechseln.

Wenn die Konsole `Mar 16 16:20:36 mach1 login: ROOT LOGIN /dev/pts/14 FROM mach2.Example.COM` oder einen ähnlichen Eintrag anzeigt, lässt das System `root`-Anmeldungen über ein Remote-System zu. Um Superuser-Zugriff über ein Remote-System zu verhindern, ändern Sie in der Datei `/etc/default/login` den Eintrag `#CONSOLE=/dev/console` in `CONSOLE=/dev/console`.

SPARC: Steuern von Zugriff auf Systemhardware (Übersicht der Schritte)

In der folgende Übersicht der Schritte wird beschrieben, wie der PROM vor unerwünschten Zugriffen geschützt wird.

Aufgabe	Description (Beschreibung)	Anweisungen
Verhindern, dass Benutzer die Einstellungen für Systemhardware ändern	Legt fest, dass ein Passwort zum Ändern der PROM-Einstellungen erforderlich ist	„So legen Sie fest, dass ein Passwort für Hardwarezugriff erforderlich ist“ auf Seite 80
Deaktivieren der Abbruch-Sequenz	Verhindert, dass Benutzer auf den PROM zugreifen	„So deaktivieren Sie die Abbruch-Sequenz eines Systems“ auf Seite 81

Steuern des Zugriffs auf Systemhardware

Sie können den physischen Rechner schützen, indem Sie festlegen, dass für den Zugriff auf die Hardware-Einstellungen ein Passwort erforderlich ist. Sie können den Rechner auch schützen, indem Sie verhindern, dass Benutzer die Abbruch-Sequenz verwenden, um das Fenstersystem zu verlassen.

▼ So legen Sie fest, dass ein Passwort für Hardwarezugriff erforderlich ist

Auf einem x86-System muss statt dem PROM das BIOS geschützt werden. Informationen zum Schutz des BIOS finden Sie im Handbuch zu Ihrem Rechner.

1 **Melden Sie sich als Superuser oder mit einer Rolle an, die das Profil "Device Security", "Maintenance and Repair" oder "System Administrator" beinhaltet.**

Das Profil "System Administrator" beinhaltet das Profil "Maintenance and Repair". Informationen zum Erstellen einer Rolle, die das Profil "Network Security" beinhaltet und zum Zuweisen dieser Rolle zu einem Benutzer finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2 **Geben Sie in einem Terminalfenster den PROM-Sicherheitsmodus ein.**

```
# eeprom security-mode=command

Changing PROM password:
New password:      <Type password>
Retype new password:      <Retype password>
```

Wählen Sie den Wert `command` oder `full`. Weitere Details finden Sie auf der Manpage `eeprom(1M)`.

Wenn Sie beim vorhergehenden Befehl nicht aufgefordert wurden, ein PROM-Passwort einzugeben, verfügt das System bereits über eines.

3 **(Optional) Um das PROM-Passwort zu ändern, geben Sie folgenden Befehl ein:**

```
# eeprom security-password=      Press Return
Changing PROM password:
New password:      <Type password>
Retype new password:      <Retype password>
```

Der neue PROM-Sicherheitsmodus und das Passwort sind unmittelbar gültig. Sie werden jedoch wahrscheinlich erst beim nächsten Booten erkannt.

Achtung – Vergessen Sie das PROM-Passwort auf keinen Fall. Ohne dieses Passwort kann die Hardware nicht verwendet werden.

▼ So deaktivieren Sie die Abbruch-Sequenz eines Systems

Einige Serversysteme verfügen über einen Schlüsselschalter. Wenn der Schlüsselschalter sich in der gesicherten Stellung befindet, überschreibt er die Softwareeinstellungen für den Abbruch über die Tastatur. Alle Änderungen, die Sie mit dem folgenden Verfahren vornehmen, werden also möglicherweise nicht implementiert.

1 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Ändern Sie den Wert von `KEYBOARD_ABORT` in `disable`.**

Kennzeichnen Sie die `enable`-Zeile in der Datei `/etc/default/kbd` als Kommentar. Fügen Sie dann eine `disable`-Zeile hinzu:

```
# cat /etc/default/kbd
...
```

```
# KEYBOARD_ABORT affects the default behavior of the keyboard abort
# sequence, see kbd(1) for details.  The default value is "enable".
# The optional value is "disable".  Any other value is ignored.
...
#KEYBOARD_ABORT=enable
KEYBOARD_ABORT=disable
```

3 Aktualisieren Sie die Standardeinstellungen für die Tastatur.

```
# kbd -i
```

◆ ◆ ◆ KAPITEL 4

Steuern des Zugriffs auf Geräte (Aufgaben)

Dieses Kapitel enthält schrittweise Anweisungen zum Schützen von Geräten sowie einen Referenzabschnitt. Im Folgenden ist eine Liste der Informationen in diesem Kapitel aufgeführt.

- „Konfigurieren von Geräten (Übersicht der Schritte)“ auf Seite 83
- „Konfigurieren der Geräterichtlinie (Übersicht der Schritte)“ auf Seite 84
- „Verwalten der Gerätezuordnung (Übersicht der Schritte)“ auf Seite 87
- „Zuordnen von Geräten (Übersicht der Schritte)“ auf Seite 93
- „Geräteschutz (Referenz)“ auf Seite 98

Eine Übersicht der Informationen zum Geräteschutz erhalten Sie unter „Steuern des Zugriffs auf Dateien“ auf Seite 47.

Konfigurieren von Geräten (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf Aufgaben zum Verwalten des Zugriffs auf Geräte.

Aufgabe	Anweisungen
Verwalten der Geräterichtlinie	„Konfigurieren der Geräterichtlinie (Übersicht der Schritte)“ auf Seite 84
Verwalten der Gerätezuordnung	„Verwalten der Gerätezuordnung (Übersicht der Schritte)“ auf Seite 87
Verwenden der Gerätezuordnung	„Zuordnen von Geräten (Übersicht der Schritte)“ auf Seite 93

Konfigurieren der Geräterichtlinie (Übersicht der Schritte)

In der folgenden Übersicht der Schritte wird auf Verfahren zur Gerätekonfiguration im Bezug auf die Geräterichtlinie verwiesen.

Aufgabe	Beschreibung	Anweisungen
Anzeigen der Geräterichtlinie für die Geräte im System	Führt die Geräte und die zugehörige Geräterichtlinie auf	„So zeigen Sie die Geräterichtlinie an“ auf Seite 84
Anfordern von Berechtigung für Geräteverwendung	Verwendet Berechtigungen zum Schützen eines Geräts	„So ändern Sie die Geräterichtlinie auf einem vorhandenen Gerät“ auf Seite 85
Entfernen von Berechtigungsanforderungen von einem Gerät	Entfernt die für einen Gerätezugriff benötigten Berechtigungen oder setzt sie herab	Beispiel 4–3
Prüfen von Änderungen der Geräterichtlinie	Zeichnet Änderungen der Geräterichtlinie im Prüfpfad auf	„So prüfen Sie Änderungen der Geräterichtlinie“ auf Seite 86
Zugriff auf `/dev/arp`	Ruft die Oracle Solaris IP MIB-II-Informationen ab	„So rufen Sie IP MIB-II-Informationen von einem `/dev/*`-Gerät ab“ auf Seite 86

Konfigurieren der Geräterichtlinie

Die Geräterichtlinie beschränkt oder verhindert den Zugriff auf integrierte Geräte des Systems. Die Richtlinie wird im Kernel durchgesetzt.

▼ So zeigen Sie die Geräterichtlinie an

- **Zeigen Sie die Geräterichtlinie für alle Geräte im System an.**

```
% getdevpolicy | more
DEFAULT
        read_priv_set=none
        write_priv_set=none
ip:*
        read_priv_set=net_rawaccess
        write_priv_set=net_rawaccess
...
```

Beispiel 4–1 Anzeigen der Geräterichtlinie eines bestimmten Geräts

Im folgenden Beispiel wird die Geräterichtlinie für drei Geräte angezeigt.

```
% getdevpolicy /dev/allkmem /dev/ipsecesp /dev/hme
/dev/allkmem
        read_priv_set=all
```

```
        write_priv_set=all
/dev/ipsecesp
        read_priv_set=sys_net_config
        write_priv_set=sys_net_config
/dev/hme
        read_priv_set=net_rawaccess
        write_priv_set=net_rawaccess
```

▼ So ändern Sie die Geräterichtlinie auf einem vorhandenen Gerät

1 **Nehmen Sie eine Rolle an, die das Berechtigungsprofil "Device Security" beinhaltet, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das Berechtigungsprofil "Device Security". Außerdem können Sie das Berechtigungsprofil "Device Security" einer von Ihnen erstellten Rolle zuweisen. Weitere Informationen zum Erstellen einer Rolle und Zuweisen der Rolle zu einem Benutzer finden Sie unter Beispiel 9–3.

2 **Fügen Sie dem Gerät eine Richtlinie hinzu.**

`# update_drv -a -p` *policy device-driver*

`-a`	Gibt *policy* für *device-driver* an.
`-p` *policy*	Entspricht der Geräterichtlinie für *device-driver*. Die Geräterichtlinie gibt zwei Berechtigungssätze an. Ein Satz ist für den Lesezugriff auf das Gerät erforderlich. Der andere Satz wird für den Schreibzugriff auf das Gerät benötigt.
device-driver	Entspricht dem Gerätetreiber

Weitere Informationen erhalten Sie auf der Manpage `update_drv(1M)`.

Beispiel 4–2 Hinzufügen einer Richtlinie zu einem vorhandenen Gerät

Im folgenden Beispiel wird die Geräterichtlinie zum Gerät `ipnat` hinzugefügt.

```
# getdevpolicy /dev/ipnat
/dev/ipnat
        read_priv_set=none
        write_priv_set=none
# update_drv -a \
-p 'read_priv_set=net_rawaccess write_priv_set=net_rawaccess' ipnat
# getdevpolicy /dev/ipnat
/dev/ipnat
        read_priv_set=net_rawaccess
        write_priv_set=net_rawaccess
```

Beispiel 4–3 Entfernen einer Richtlinie von einem Gerät

Im folgenden Beispiel wird der für den Lesezugriff benötigte Satz von Berechtigungen von der Geräterichtlinie für das Gerät `ipnat` entfernt.

```
# getdevpolicy /dev/ipnat
/dev/ipnat
        read_priv_set=net_rawaccess
        write_priv_set=net_rawaccess
# update_drv -a -p write_priv_set=net_rawaccess ipnat
# getdevpolicy /dev/ipnat
/dev/ipnat
        read_priv_set=none
        write_priv_set=net_rawaccess
```

▼ So prüfen Sie Änderungen der Geräterichtlinie

Die Prüfklasse `as` enthält standardmäßig das Prüfereignis `AUE_MODDEVPLCY`.

1. **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

   Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Führen Sie eine Vorauswahl der Prüfklasse durch, die das Prüfereignis `AUE_MODDEVPLCY` enthält.**

   Fügen Sie die Klasse `as` zur Zeile `flags` der Datei `audit_control` hinzu. Die Ausgabe der Datei sieht ähnlich wie im Folgenden aus:

   ```
   # audit_control file
   dir:/var/audit
   flags:lo,as
   minfree:20
   naflags:lo
   ```

   Ausführliche Anweisungen erhalten Sie unter „So ändern Sie die Datei `audit_control`“ auf Seite 639.

▼ So rufen Sie IP MIB-II-Informationen von einem `/dev/*`-Gerät ab

Von Anwendungen, die Oracle Solaris IP MIB-II-Information abrufen, sollte `/dev/arp` und nicht `/dev/ip` geöffnet werden.

1 **Legen Sie die Geräterichtlinie auf `/dev/ip` und `/dev/arp` fest.**

```
% getdevpolicy /dev/ip /dev/arp
/dev/ip
        read_priv_set=net_rawaccess
        write_priv_set=net_rawaccess
/dev/arp
        read_priv_set=none
        write_priv_set=none
```

Beachten Sie, dass die Berechtigung `net_rawaccess` für den Lese- und Schreibzugriff auf `/dev/ip` erforderlich ist. Es werden keine Berechtigungen für `/dev/arp` benötigt.

2 **Öffnen Sie `/dev/arp` und stellen Sie die Module `tcp` und `udp` bereit.**

Hierfür werden keine Berechtigungen benötigt. Diese Methode entspricht dem Öffnen von `/dev/ip` und Bereitstellen der Module `arp`, `tcp` und `udp`. Da zum Öffnen von `/dev/ip` nun eine Berechtigung benötigt wird, ist die Methode über `/dev/arp` vorzuziehen.

Verwalten der Gerätezuordnung (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf Verfahren zum Aktivieren und Konfigurieren der Gerätezuordnung. Die Gerätezuordnung ist nicht standardmäßig aktiviert. Weitere Informationen zu den Schritten nach dem Aktivieren der Gerätezuordnung erhalten Sie unter „Zuordnen von Geräten (Übersicht der Schritte)“ auf Seite 93.

Aufgabe	Beschreibung	Anweisungen
Aktivieren der Gerätezuordnung	Ermöglicht das Zuordnen eines Geräts zu jeweils einem Benutzer	„So aktivieren Sie die Zuordnung eines Geräts“ auf Seite 88
Autorisieren von Benutzern für die Zuordnung eines Geräts	Weist Berechtigungen für die Gerätezuordnung den Benutzern zu	„So autorisieren Sie Benutzer für die Zuordnung eines Geräts“ auf Seite 89
Anzeigen der zuordenbaren Geräte im System	Führt die zuordenbaren Geräte und den zugehörigen Status auf	„So zeigen Sie Zuordnungsinformationen zu einem Gerät an“ auf Seite 90
Erzwingen einer Gerätezuordnung	Weist ein Gerät einem Benutzer zu, der es dringend benötigt	„Erzwingen der Gerätezuordnung“ auf Seite 90
Erzwingen der Aufhebung der Gerätezuordnung	Hebt die Zuordnung eines Geräts auf, das derzeit einem Benutzer zugeordnet ist	„Erzwingen der Aufhebung der Gerätezuordnung“ auf Seite 91
Ändern der Zuordnungseigenschaften eines Geräts	Ändert die Anforderungen für das Zuordnen eines Geräts	„So ändern Sie die Zuordenbarkeit von Geräten“ auf Seite 91
Erstellen eines Bereinigungsskripts	Bereinigt Daten von einem physischen Gerät	„Erstellen neuer Bereinigungsskripten“ auf Seite 105

Aufgabe	Beschreibung	Anweisungen
Deaktivieren der Gerätezuordnung	Entfernt Zuordnungsbeschränkungen von allen Geräten	„So deaktivieren Sie den Prüfservice“ auf Seite 658
Prüfen der Gerätezuordnung	Zeichnet die Gerätezuordnung im Prüfpfad auf	„So prüfen Sie die Gerätezuordnung“ auf Seite 92

Verwalten der Gerätezuordnung

Die Gerätezuordnung beschränkt oder verhindert den Zugriff auf Peripheriegeräte. Die Beschränkungen werden während der Benutzerzuordnung durchgesetzt. Standardmäßig müssen die Benutzer über eine Autorisierung für den Zugriff auf zuordenbare Geräte verfügen.

▼ So aktivieren Sie die Zuordnung eines Geräts

Wenn Sie den Befehl `bsmconv` für das Aktivieren der Prüfung ausgeführt haben, ist die Gerätezuordnung bereits auf dem System aktiviert. Weitere Informationen finden Sie auf der Manpage `bsmconv(1M)`.

1 **Nehmen Sie eine Rolle an, die das Berechtigungsprofil "Audit Control" beinhaltet, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das Berechtigungsprofil "Audit Control". Außerdem können Sie das Berechtigungsprofil "Audit Control" einer von Ihnen erstellten Rolle zuweisen. Weitere Informationen zum Erstellen einer Rolle und Zuweisen der Rolle zu einem Benutzer finden Sie unter Beispiel 9–3.

2 **Aktivieren Sie die Gerätezuordnung.**

```
# bsmconv
This script is used to enable the Basic Security Module (BSM).
Shall we continue with the conversion now? [y/n] y
bsmconv: INFO: checking startup file.
bsmconv: INFO: move aside /etc/rc3.d/S81volmgt.
bsmconv: INFO: turning on audit module.
bsmconv: INFO: initializing device allocation files.

The Basic Security Module is ready.
If there were any errors, please fix them now.
Configure BSM by editing files located in /etc/security.
Reboot this system now to come up with BSM enabled.
```

Hinweis – Der Dämon für Volume-Management (`/etc/rc3.d/S81volmgt`) wird durch diesen Befehl deaktiviert.

▼ So autorisieren Sie Benutzer für die Zuordnung eines Geräts

1 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Erstellen Sie ein Berechtigungsprofil, das die entsprechende Autorisierung und Befehle enthält.**

Normalerweise erstellen Sie ein Berechtigungsprofil, das die Autorisierung `solaris.device.allocate` enthält. Befolgen Sie die Anweisungen unter „So erstellen oder ändern Sie ein Berechtigungsprofil“ auf Seite 238. Weisen Sie dem Berechtigungsprofil beispielsweise folgende Eigenschaften zu:

- Berechtigungsprofilname: `Device Allocation`
- Gewährte Autorisierungen: `solaris.device.allocate`
- Befehle mit Sicherheitsattributen: `mount` mit der Berechtigung `sys_mount` und `umount` mit der Berechtigung `sys_mount`

3 **Erstellen Sie eine Rolle für das Berechtigungsprofil.**

Befolgen Sie die Anweisungen unter „So können Sie eine Rolle mit der GUI erstellen und zuweisen“ auf Seite 218. Die folgenden Rolleneigenschaften dienen zur Orientierung:

- Rollename: `devicealloc`
- Vollständiger Rollenname: `Device Allocator`
- Rollenbeschreibung: `Allocates and mounts allocated devices`
- Berechtigungsprofil: `Device Allocation`

  Dieses Berechtigungsprofil muss sich an oberster Stelle in der Liste der Profile befinden, die in der Rolle enthalten sind.

4 **Weisen Sie die Rolle allen Benutzern zu, die über eine Berechtigung zum Zuordnen eines Geräts verfügen.**

5 **Erklären Sie den Benutzern die Verwendung der Gerätezuordnung.**

Beispiele für das Zuordnen von Wechseldatenträgern erhalten Sie unter „So ordnen Sie ein Gerät zu“ auf Seite 93.

Da der Dämon für Volume-Management (`vold`) nicht ausgeführt wird, werden Wechseldatenträger nicht automatisch eingehängt. Beispiele zum Einhängen eines zugeordneten Geräts finden Sie unter „So hängen Sie ein zugeordnetes Gerät ein“ auf Seite 94.

▼ So zeigen Sie Zuordnungsinformationen zu einem Gerät an

Bevor Sie beginnen Die Gerätezuordnung muss aktiviert sein, damit dieses Verfahren erfolgreich durchgeführt wird. Weitere Informationen zum Aktivieren der Gerätezuordnung finden Sie unter „So aktivieren Sie die Zuordnung eines Geräts“ auf Seite 88.

1 Nehmen Sie eine Rolle an, die das Berechtigungsprofil "Device Security" beinhaltet, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das Berechtigungsprofil "Device Security". Außerdem können Sie das Berechtigungsprofil "Device Security" einer von Ihnen erstellten Rolle zuweisen. Weitere Informationen zum Erstellen einer Rolle und Zuweisen der Rolle zu einem Benutzer finden Sie unter Beispiel 9–3.

2 Zeigen Sie die Informationen zu den zuordenbaren Geräten im System an.

```
# list_devices device-name
```

device-name kann einen der folgenden Werte annehmen:

- `audio`[*n*]: Entspricht einem Mikrofon und Lautsprecher
- `fd`[*n*]: Entspricht einem Diskettenlaufwerk
- `sr`[*n*]: Entspricht einem CD-ROM-Laufwerk
- `st`[*n*]: Entspricht einem Bandlaufwerk

Allgemeine Fehler Wenn der Befehl `list_devices` eine Fehlermeldung ähnlich der folgenden zurückgibt, ist entweder die Gerätezuordnung nicht aktiviert oder Sie verfügen nicht über ausreichende Berechtigungen zum Abrufen der Informationen.

```
list_devices: No device maps file entry for specified device.
```

Damit der Befehl erfolgreich ausgeführt wird, aktivieren Sie die Gerätezuordnung und nehmen Sie eine Rolle mit der Autorisierung `solaris.device.revoke` an.

▼ Erzwingen der Gerätezuordnung

Die erzwungene Zuordnung wird verwendet, wenn das Aufheben einer Gerätezuordnung versehentlich nicht durchgeführt wurde. Außerdem kann diese Art der Zuordnung durchgeführt werden, wenn ein Benutzer ein Gerät dringend benötigt.

Bevor Sie beginnen Der Benutzer oder die Rolle muss über die Autorisierung `solaris.device.revoke` verfügen.

1 Bestimmen Sie, ob Ihre Rolle die entsprechenden Autorisierungen enthält.

```
$ auths
solaris.device.allocate solaris.device.revoke
```

2. **Erzwingen Sie die Zuordnung des Geräts zu einem Benutzer, der das Gerät benötigt.**

   Im folgenden Beispiel wird die Zuordnung des Bandlaufwerks für den Benutzer `jdoe` erzwungen.

   ```
   $ allocate -U jdoe
   ```

▼ Erzwingen der Aufhebung der Gerätezuordnung

Die Zuordnung von Geräten durch einen Benutzer wird nicht automatisch aufgehoben, wenn der Prozess beendet wird oder der Benutzer sich abmeldet. Die erzwungene Aufhebung der Zuordnung wird verwendet, wenn das Aufheben einer Gerätezuordnung versehentlich nicht durchgeführt wurde.

Bevor Sie beginnen Der Benutzer oder die Rolle muss über die Autorisierung `solaris.device.revoke` verfügen.

1. **Bestimmen Sie, ob Ihre Rolle die entsprechenden Autorisierungen enthält.**

   ```
   $ auths
   solaris.device.allocate solaris.device.revoke
   ```

2. **Erzwingen Sie die Aufhebung der Gerätezuordnung.**

   In diesem Beispiel wird die Aufhebung der Druckerzuordnung erzwungen. Der Drucker kann jetzt einem anderen Benutzer zugeordnet werden.

   ```
   $ deallocate -f /dev/lp/printer-1
   ```

▼ So ändern Sie die Zuordenbarkeit von Geräten

1. **Nehmen Sie eine Rolle an, die das Berechtigungsprofil "Device Security" beinhaltet, oder melden Sie sich als Superuser an.**

   Die Rolle "Primary Administrator" enthält das Berechtigungsprofil "Device Security". Außerdem können Sie das Berechtigungsprofil "Device Security" einer von Ihnen erstellten Rolle zuweisen. Weitere Informationen zum Erstellen einer Rolle und Zuweisen der Rolle zu einem Benutzer finden Sie unter Beispiel 9–3.

2. **Geben Sie an, ob eine Autorisierung erforderlich ist, oder geben Sie die Autorisierung `solaris.device.allocate` an.**

   Ändern Sie das fünfte Feld im Geräteeintrag der Datei `device_allocate`.

   ```
   audio;audio;reserved;reserved;solaris.device.allocate;/etc/security/lib/audio_clean
   fd0;fd;reserved;reserved;solaris.device.allocate;/etc/security/lib/fd_clean
   sr0;sr;reserved;reserved;solaris.device.allocate;/etc/security/lib/sr_clean
   ```

   Ersetzen Sie `solaris.device.allocate` durch einen Benutzer, der über die Autorisierung `solaris.device.allocate` für die Verwendung des Geräts verfügt.

Beispiel 4–4 Zulassen der Gerätezuordnung für alle Benutzer

Im folgenden Beispiel kann die Zuordnung aller Geräte von allen Benutzern im System durchgeführt werden. Das fünfte Feld im Geräteeintrag der Datei `device_allocate` wurde in ein At-Zeichen (@) geändert.

```
$ whoami
devicesec
$ vi /etc/security/device_allocate
audio;audio;reserved;reserved;@;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;@;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;@;/etc/security/lib/sr_clean
...
```

Beispiel 4–5 Verhindern der Verwendung einiger Peripheriegeräte

Im folgenden Beispiel kann das Audiogerät nicht verwendet werden. Das fünfte Feld im Audiogeräteintrag der Datei `device_allocate` wurde in ein Sternchen (*) geändert.

```
$ whoami
devicesec
$ vi /etc/security/device_allocate
audio;audio;reserved;reserved;*;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;solaris device.allocate;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;solaris device.allocate;/etc/security/lib/sr_clean
...
```

Beispiel 4–6 Verhindern der Verwendung aller Peripheriegeräte

Im folgenden Beispiel kann kein Peripheriegerät verwendet werden. Das fünfte Feld in allen Geräteeinträgen der Datei `device_allocate` wurde in ein Sternchen (*) geändert.

```
$ whoami
devicesec
$ vi /etc/security/device_allocate
audio;audio;reserved;reserved;*;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;*;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;*;/etc/security/lib/sr_clean
...
```

▼ So prüfen Sie die Gerätezuordnung

Die Befehle für die Gerätezuordnung sind standardmäßig in der Prüfklasse `other` enthalten.

1 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Führen Sie eine Vorauswahl der Klasse `ot` für die Prüfung durch.**

Fügen Sie die Klasse `ot` zur Zeile `flags` der Datei `audit_control` hinzu. Die Ausgabe der Datei sieht ähnlich wie im Folgenden aus:

```
# audit_control file
dir:/var/audit
flags:lo,ot
minfree:20
naflags:lo
```

Ausführliche Anweisungen erhalten Sie unter „So ändern Sie die Datei `audit_control`“ auf Seite 639.

Zuordnen von Geräten (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf Verfahren, in denen die Gerätezuordnung durch Benutzer beschrieben wird.

Aufgabe	Beschreibung	Anweisungen
Zuordnen eines Geräts	Ermöglicht die Verwendung eines Geräts durch einen Benutzer und verhindert die Verwendung des Geräts durch andere Benutzer	„So ordnen Sie ein Gerät zu“ auf Seite 93
Einhängen eines zugeordneten Geräts	Ermöglicht dem Benutzer das Anzeigen eines einzuhängenden Geräts (z. B. CD-ROM- oder Diskettenlaufwerk)	„So hängen Sie ein zugeordnetes Gerät ein“ auf Seite 94
Aufheben der Zuordnung eines Geräts	Ermöglicht die Verwendung eines zuordenbaren Geräts durch einen anderen Benutzer	„So heben Sie die Zuordnung eines Geräts auf“ auf Seite 97

Zuordnen von Geräten

Durch die Gerätezuordnung kann nur ein Benutzer gleichzeitig ein Gerät verwenden. Geräte, die einen Einhängepunkt erfordern, müssen eingehängt werden.

▼ So ordnen Sie ein Gerät zu

Bevor Sie beginnen Die Gerätezuordnung muss aktiviert sein (siehe Beschreibung unter „So aktivieren Sie die Zuordnung eines Geräts“ auf Seite 88). Wenn eine Autorisierung erforderlich ist, muss der Benutzer über die Autorisierung verfügen.

1 **Ordnen Sie das Gerät zu.**

Geben Sie das Gerät durch den Gerätenamen an.

```
% allocate device-name
```

2 Vergewissern Sie sich, dass das Gerät zugeordnet ist.

Führen Sie den identischen Befehl aus.

```
% allocate device-name
allocate. Device already allocated.
```

Beispiel 4–7 Zuordnen eines Mikrofons

Im folgenden Beispiel ordnet der Benutzer `jdoe` ein Mikrofon (`audio`) zu.

```
% whoami
jdoe
% allocate audio
```

Beispiel 4–8 Zuordnen eines Druckers

Im folgenden Beispiel ordnet der Benutzer einen Drucker zu. Druckvorgänge an `printer-1` sind erst möglich, nachdem der Benutzer die Zuordnung aufgehoben hat oder die Zuordnung des Druckers an einen anderen Benutzer erzwungen wurde.

```
% allocate /dev/lp/printer-1
```

Ein Beispiel zu einer erzwungenen Aufhebung der Zuordnung finden Sie unter „Erzwingen der Aufhebung der Gerätezuordnung“ auf Seite 91.

Beispiel 4–9 Zuordnen eines Bandlaufwerks

Im folgenden Beispiel ordnet der Benutzer `jdoe` ein Bandlaufwerk (`st0`) zu.

```
% whoami
jdoe
% allocate st0
```

Allgemeine Fehler Wenn durch den Befehl `allocate` das Gerät nicht zugeordnet werden kann, wird eine Fehlermeldung im Konsolenfenster angezeigt. Eine Liste der Fehlermeldungen zu Zuordnungen finden Sie auf der Manpage `allocate(1)`.

▼ So hängen Sie ein zugeordnetes Gerät ein

Bevor Sie beginnen Der Benutzer oder die Rolle hat das Gerät zugeordnet. Um ein Gerät einzuhängen, muss der Benutzer oder die Rolle über Berechtigungen zum Einhängen des Geräts verfügen. Weitere Informationen zum Gewähren der erforderlichen Berechtigungen erhalten Sie unter „So autorisieren Sie Benutzer für die Zuordnung eines Geräts“ auf Seite 89.

1. **Nehmen Sie eine Rolle an, mit der Sie ein Gerät zuordnen und einhängen können.**

   ```
   % su - role-name
   Password:       <Type role-name password>
   $
   ```

2. **Erstellen und schützen Sie einen Einhängepunkt im Home-Verzeichnis der Rolle.**

   Diesen Schritt müssen Sie nur bei der erstmaligen Verwendung eines Einhängepunkts durchführen.

   ```
   $ mkdir mount-point ; chmod 700 mount-point
   ```

3. **Führen Sie die zuordenbaren Geräte auf.**

   ```
   $ list_devices -l
   List of allocatable devices
   ```

4. **Ordnen Sie das Gerät zu.**

   Geben Sie das Gerät durch den Gerätenamen an.

   ```
   $ allocate device-name
   ```

5. **Hängen Sie das Gerät ein.**

   ```
   $ mount -o ro -F filesystem-type device-path mount-point
   ```

   Hierbei gilt:

`-o ro`	Gibt an, dass das Gerät nur für den Lesezugriff eingehängt werden soll. Mit `-o rw` geben Sie an, dass ein Schreibzugriff auf das Gerät möglich sein soll.
`-F` *filesystem-type*	Gibt das Dateisystemformat des Geräts an. Normalerweise werden CD-ROM-Laufwerke mit einem HSFS-Dateisystem formatiert, während Diskettenlaufwerke üblicherweise mit einem PCFS-Dateisystem formatiert werden.
device-path	Gibt den Pfad zum Gerät an. Die Ausgabe des Befehls `list_devices -l` enthält *device-path*.
mount-point	Gibt den in Schritt 2 erstellten Einhängepunkt an

Beispiel 4–10 Zuordnen eines Diskettenlaufwerks

In diesem Beispiel nimmt der Benutzer eine Rolle an, durch die ein Diskettenlaufwerk (`fd0`) zugeordnet und eingehängt werden kann. Diskettenlaufwerke werden mit einem PCFS-Dateisystem formatiert.

```
% roles
devicealloc
% su - devicealloc
Password:       <Type devicealloc password>
```

```
$ mkdir /home/devicealloc/mymnt
$ chmod 700 /home/devicealloc/mymnt
$ list_devices -l
...
device: fd0 type: fd files: /dev/diskette /dev/rdiskette /dev/fd0a
...
$ allocate fd0
$ mount -o ro -F pcfs /dev/diskette /home/devicealloc/mymnt
$ ls /home/devicealloc/mymnt
```

List of the contents of diskette

Beispiel 4–11 Zuordnen eines CD-ROM-Laufwerks

In diesem Beispiel nimmt der Benutzer eine Rolle an, durch die ein CD-ROM-Laufwerk (`sr0`) zugeordnet und eingehängt werden kann. Das Laufwerk wird als ein HSFS-Dateisystem formatiert.

```
% roles
devicealloc
% su - devicealloc
Password:      <Type devicealloc password>
$ mkdir /home/devicealloc/mymnt
$ chmod 700 /home/devicealloc/mymnt
$ list_devices -l
...
device: sr0 type: sr files: /dev/sr0 /dev/rsr0 /dev/dsk/c0t2d0s0 ...
...
$ allocate sr0
$ mount -o ro -F hsfs /dev/sr0 /home/devicealloc/mymnt
$ cd /home/devicealloc/mymnt ; ls
```

List of the contents of CD-ROM

Allgemeine Fehler

Wenn durch den Befehl `mount` das Gerät nicht eingehängt werden kann, wird eine Fehlermeldung angezeigt: `mount: insufficient privileges`. Überprüfen Sie Folgendes:

- Vergewissern Sie sich, dass der Befehl `mount` in einer Profil-Shell ausgeführt wird. Wenn Sie eine Rolle angenommen haben, weist die Rolle eine Profil-Shell auf. Wenn Ihnen als Benutzer ein Profil mit dem Befehl `mount` zugewiesen wurde, müssen Sie eine Profil-Shell erstellen. Durch die Befehle `pfsh`, `pfksh` und `pfcsh` wird eine Profil-Shell erstellt.
- Vergewissern Sie sich, dass Sie der Eigentümer des angegebenen Einhängepunkts sind. Sie sollten über Lese-, Schreib- und Ausführungszugriff für den Einhängepunkt verfügen.

Wenden Sie sich an den Administrator, wenn das zugeordnete Gerät weiterhin nicht eingehängt werden kann.

▼ So heben Sie die Zuordnung eines Geräts auf

Durch das Aufheben der Zuordnung können andere Benutzer das Gerät zuordnen und verwenden, wenn Sie die Verwendung abgeschlossen haben.

Bevor Sie beginnen Das Gerät muss zugeordnet sein.

1 Wenn das Gerät eingehängt ist, hängen Sie das Gerät aus.

```
$ cd $HOME
$ umount mount-point
```

2 Heben Sie die Zuordnung des Geräts auf.

```
$ deallocate device-name
```

Beispiel 4–12 Aufheben der Zuordnung eines Mikrofons

Im folgenden Beispiel hebt der Benutzer `jdoe` die Zuordnung für das Mikrofon (`audio`) auf.

```
% whoami
jdoe
% deallocate audio
```

Beispiel 4–13 Aufheben der Zuordnung eines CD-ROM-Laufwerks

Im folgenden Beispiel wird durch die Rolle "Device Allocator" die Zuordnung eines CD-ROM-Laufwerks aufgehoben. Nach der Meldungsausgabe wird die CD-ROM ausgeworfen.

```
$ whoami
devicealloc
$ cd /home/devicealloc
$ umount /home/devicealloc/mymnt
$ ls /home/devicealloc/mymnt
$
$ deallocate sr0
/dev/sr0:      326o
/dev/rsr0:     326o
...
sr_clean: Media in sr0 is ready.  Please, label and store safely.
```

Geräteschutz (Referenz)

Die Geräte in Oracle Solaris werden durch die Geräterichtlinie geschützt. Die Peripheriegeräte werden durch die Gerätezuordnung geschützt. Die Geräterichtlinie wird durch den Kernel durchgesetzt. Die Gerätezuordnung ist optional aktiviert und wird auf Benutzerebene durchgesetzt.

Befehle der Geräterichtlinie

Mit den Befehlen zur Geräteverwaltung kann die Geräterichtlinie auf lokalen Dateien verwaltet werden. Die Geräterichtlinie kann Berechtigungsanforderungen enthalten. Geräte können nur vom Superuser oder einer Rolle mit ähnlichen Funktionen verwaltet werden.

In der folgenden Tabelle sind die Befehle zur Geräteverwaltung aufgeführt.

TABELLE 4–1 Befehle zur Geräteverwaltung

Befehl	Zweck	Manpage
`devfsadm`	Verwaltet Geräte und Gerätetreiber auf einem ausgeführten System. Die Geräterichtlinie wird ebenfalls geladen. Mit dem Befehl `devfsadm` können Sie nicht verwendete `/dev`-Links auf Festplatten-, Band-, Port-, Audio- und Pseudogeräten bereinigen. Die Geräte für einen benannten Treiber können ebenfalls neu konfiguriert werden.	`devfsadm`(1M)
`getdevpolicy`	Zeigt die Richtlinie an, die mindestens einem Gerät zugewiesen ist. Dieser Befehl kann von allen Benutzern ausgeführt werden.	`getdevpolicy`(1M)
`add_drv`	Fügt einen neuen Gerätetreiber zu einem ausgeführten System hinzu. Enthält Optionen zum Hinzufügen der Geräterichtlinie zum neuen Gerät. Dieser Befehl wird normalerweise in einem Skript aufgerufen, wenn ein Gerätetreiber installiert wurde.	`add_drv`(1M)
`update_drv`	Aktualisiert die Attribute eines vorhandenen Gerätetreibers. Enthält Optionen zum Aktualisieren der Geräterichtlinie für das Gerät. Dieser Befehl wird normalerweise in einem Skript aufgerufen, wenn ein Gerätetreiber installiert wurde.	`update_drv`(1M)
`rem_drv`	Entfernt ein Gerät oder einen Gerätetreiber.	`rem_drv`(1M)

Gerätezuordnung

Durch die Gerätezuordnung kann Ihr Standort vor Datenverlust, Computerviren und anderen Sicherheitsverletzungen geschützt werden. Im Gegensatz zur Geräterichtlinie ist die Gerätezuordnung optional. Geräte können erst zugeordnet werden, nachdem das Skript `bsmconv` ausgeführt wurde. Die Gerätezuordnung verwendet Autorisierungen, um den Zugriff auf zuordenbare Geräte einzuschränken.

Komponenten der Gerätezuordnung

Der Gerätezuordnungsmechanismus verwendet folgende Komponenten:

- Die Befehle `allocate`, `deallocate`, `dminfo` und `list_devices`. Weitere Informationen erhalten Sie unter „Befehle der Gerätezuordnung“ auf Seite 99.
- Bereinigungsskripten für die jeweiligen zuordenbaren Geräte

Diese Befehle und Skripten verwenden folgende lokale Dateien für die Implementierung der Gerätezuordnung:

- Die Datei `/etc/security/device_allocate`. Weitere Informationen erhalten Sie auf der Manpage `device_allocate(4)`.
- Die Datei `/etc/security/device_maps`. Weitere Informationen erhalten Sie auf der Manpage `device_maps(4)`.
- Eine Sperrdatei im Verzeichnis `/etc/security/dev` für die jeweiligen zuordenbaren Geräte
- Die geänderten Attribute der Sperrdateien, die den jeweiligen zuordenbaren Geräten zugewiesen sind

---

Hinweis – Das Verzeichnis `/etc/security/dev` wird in zukünftigen Versionen von Oracle Solaris möglicherweise nicht mehr unterstützt.

Befehle der Gerätezuordnung

Bei den Optionen in Großbuchstaben sind `allocate`, `deallocate` und `list_devices` administrative Befehle. Andernfalls sind es Benutzerbefehle. In der folgenden Tabelle sind die Befehle der Gerätezuordnung aufgeführt.

TABELLE 4–2 Befehle der Gerätezuordnung

Befehl	Zweck	Manpage
`bsmconv`	Erstellt Datenbanken für die Verarbeitung der Gerätezuordnung. Aktiviert ebenfalls den Prüfservice. Sie müssen als Superuser oder mit der Rolle "Primary Administrator" angemeldet sein. `devalloc_adm`: Aktivieren der Zuordenbarkeit von Geräten, sodass einzelne Benutzer ein Gerät für eine private Verwendung zuordnen können. Verhindert die Gerätezuordnung, wodurch die Verwendung von Peripheriegeräten in einem System verhindert wird. Entfernt Geräte aus der Liste der zuordenbaren Geräte Wenn Sie eine Prüfung verwenden möchten, können Sie mit dem Befehl `devalloc_adm` die Gerätezuordnung aktivieren.	`bsmconv(1M)`
`dminfo`	Sucht nach einem zuordenbaren Gerät nach Gerätetyp, Gerätename und vollständigem Pfadnamen	`dminfo(1M)`
`list_devices`	Führt den Status der zuordenbaren Geräte auf Führt alle gerätespezifischen Dateien auf, die einem in der Datei `device_maps` enthaltenen Gerät zugewiesen sind	`list_devices(1)`
`list_devices -U`	Führt die Geräte auf, die einer bestimmten Benutzer-ID zuordenbar oder zugeordnet sind. Mit dieser Option können Sie überprüfen, welche Geräte einem anderen Benutzer zuordenbar oder zugeordnet sind. Sie müssen über die Autorisierung `solaris.device.revoke` verfügen.	
`allocate`	Reserviert ein zuordenbares Gerät für die Verwendung durch einen Benutzer Ein Benutzer muss standardmäßig über die Autorisierung `solaris.device.allocate` zum Zuordnen eines Geräts verfügen. Sie können die Datei `device_allocate` so ändern, dass keine Benutzerautorisierung erforderlich ist. Dadurch können alle Benutzer im System die Zuordnung des Geräts für eine Verwendung anfordern.	`allocate(1)`
`deallocate`	Entfernt die Zuordnungsreservierung von einem Gerät	`deallocate(1)`

Autorisierungen für Zuordnungsbefehle

Die Benutzer müssen standardmäßig über die Autorisierung `solaris.device.allocate` verfügen, um ein zuordenbares Gerät zu reservieren. Weitere Informationen zum Erstellen eines Berechtigungsprofils, das die Autorisierung `solaris.device.allocate` enthält, finden Sie unter „So autorisieren Sie Benutzer für die Zuordnung eines Geräts“ auf Seite 89.

Administratoren müssen über die Autorisierung `solaris.device.revoke` verfügen, um den Zuordnungsstatus von Geräten zu ändern. Beispielsweise ist für die Option `-U` der Befehle `allocate` und `list_devices` und für die Option `-F` des Befehls `deallocate` die Autorisierung `solaris.device.revoke` erforderlich.

Weitere Informationen erhalten Sie unter „Befehle, die Autorisierungen erfordern“ auf Seite 262.

Zuweisungsfehlerstatus

Ein Gerät wird in einen *Zuweisungsfehlerstatus* versetzt, wenn durch den Befehl `deallocate` die Zuordnung nicht aufgehoben oder durch den Befehl `allocate` die Zuordnung nicht durchgeführt werden kann. Wenn ein zuordenbares Gerät in den Zuweisungsfehlerstatus versetzt wird, muss die Aufhebung der Gerätezuordnung erzwungen werden. Nur der Superuser oder eine Rolle mit dem Berechtigungsprofil "Device Management" bzw. "Device Security" kann einen Zuweisungsfehlerstatus verarbeiten.

Durch den Befehl `deallocate` mit der Option `-F` wird das Aufheben der Zuordnung erzwungen. Stattdessen können Sie auch durch `allocate -U` das Gerät einem Benutzer zuweisen. Nach dem Zuordnen des Geräts können Sie die gegebenenfalls auftretenden Fehlermeldungen untersuchen. Wenn Sie die gegebenenfalls aufgetretenen Fehler bei dem Gerät behoben haben, können Sie das Aufheben der Gerätezuordnung erzwingen.

Datei `device_maps`

Geräte-Maps werden erstellt, wenn Sie die Gerätezuordnung einrichten. Eine standardmäßige Datei `/etc/security/device_maps` wird durch den Befehl `bsmconv` erstellt, wenn der Prüfservice aktiviert ist. Diese anfängliche Datei `device_maps` kann für Ihren Standort angepasst werden. Die Datei `device_maps` enthält Gerätenamen, Gerätetypen und gerätespezifische Dateien, die den jeweiligen zuordenbaren Geräten zugewiesen sind.

Die Datei `device_maps` definiert die gerätespezifischen Dateizuordnungen für die jeweiligen Geräte, die in den meisten Fällen nicht intuitiv ist. Durch diese Datei können Programme feststellen, welche gerätespezifischen Dateien welchen Geräten zugewiesen sind. Sie können mit dem Befehl `dminfo` beispielsweise den Gerätenamen, Gerätetyp und die gerätespezifischen Dateien abrufen, um sie beim Einrichten eines zuordenbaren Geräts zu verwenden. Der Befehl `dminfo` verwendet die Datei `device_maps`, um diese Informationen zu melden.

Jedes Gerät wird durch einen einzeiligen Eintrag im folgenden Format dargestellt:

device-name:*device-type*:*device-list*

BEISPIEL 4–14 Beispiel des Eintrags `device_maps`

Das folgende Beispiel zeigt einen Eintrag in der Datei `device_maps` eines Diskettenlaufwerks (`fd0`):

BEISPIEL 4–14 Beispiel des Eintrags `device_maps` *(Fortsetzung)*

```
fd0:\
        fd:\
        /dev/diskette /dev/rdiskette /dev/fd0a /dev/rfd0a \
/dev/fd0b /dev/rfd0b /dev/fd0c /dev/fd0 /dev/rfd0c /dev/rfd0:\
```

Zeilen in der Datei `device_maps` können auf einen umgekehrten Schrägstrich (\) enden, um den Eintrag auf der nächsten Zeile fortzusetzen. Kommentare können ebenfalls enthalten sein. Ein Rautezeichen (#) definiert den gesamten nachfolgenden Text bis zum nächsten Zeilenendezeichen als Kommentar, sofern kein umgekehrter Schrägstrich unmittelbar vor dem Zeilenendezeichen angegeben ist. Vorangestellte und nachgestellte Leerstellen sind in allen Feldern zulässig. Die Felder sind wie folgt definiert:

device-name Gibt den Namen des Geräts an. Eine Liste der aktuellen Gerätenamen finden Sie unter „So zeigen Sie Zuordnungsinformationen zu einem Gerät an“ auf Seite 90.

device-type Gibt den generischen Gerätetyp an. Der generische Name entspricht dem Namen der Geräteklasse wie `st`, `fd` oder `audio`. Im Feld *device-type* werden verwandte Geräte logisch gruppiert.

device-list Führt die gerätespezifischen Dateien auf, die dem physischen Gerät zugewiesen sind. Unter *device-list* müssen alle spezifischen Dateien aufgeführt sein, die den Zugriff auf ein bestimmtes Gerät ermöglichen. Wenn die Liste unvollständig ist, kann ein böswilliger Benutzer weiterhin private Informationen erhalten oder ändern. Gültige Einträge für das Feld *device-list* stellen die Gerätedateien dar, die im Verzeichnis `/dev` enthalten sind.

Datei `device_allocate`

Eine anfängliche Datei `/etc/security/device_allocate` wird durch den Befehl `bsmconv` erstellt, wenn der Prüfservice aktiviert wurde. Diese anfängliche Datei `device_allocate` kann als Ausgangspunkt verwendet werden. Sie können die Datei `/etc/security/device_allocate` ändern, um die Geräte von zuordenbar in nicht zuordenbar zu ändern oder neue Geräte hinzuzufügen. Im Folgenden sehen Sie eine Beispieldatei `device_allocate`.

```
st0;st;;;;/etc/security/lib/st_clean
fd0;fd;;;;/etc/security/lib/fd_clean
sr0;sr;;;;/etc/security/lib/sr_clean
audio;audio;;;*;/etc/security/lib/audio_clean
```

Ein Eintrag in der Datei `device_allocate` bedeutet nicht, dass das Gerät zugeordnet werden kann. Dies ist nur der Fall, wenn in dem Eintrag ausdrücklich angegeben ist, dass das Gerät zugeordnet werden kann. Beachten Sie in der Beispieldatei `device_allocate` das Sternchen (*) im fünften Feld des Audiogeräteintrags. Ein Sternchen im fünften Feld weist das System darauf

hin, dass das Gerät nicht zuordenbar ist. Daher kann das Gerät nicht verwendet werden. Andere Werte oder kein Wert in diesem Feld bedeuten, dass das Gerät verwendet werden kann.

In der Datei `device_allocate` wird jedes Gerät durch einen einzeiligen Eintrag im folgenden Format dargestellt:

device-name;*device-type*;`reserved`;`reserved`;*auths*;*device-exec*

Zeilen in der Datei `device_allocate` können auf einen umgekehrten Schrägstrich (`\`) enden, um den Eintrag auf der nächsten Zeile fortzusetzen. Kommentare können ebenfalls enthalten sein. Ein Rautezeichen (`#`) definiert den gesamten nachfolgenden Text bis zum nächsten Zeilenendezeichen als Kommentar, sofern kein umgekehrter Schrägstrich unmittelbar vor dem Zeilenendezeichen angegeben ist. Vorangestellte und nachgestellte Leerstellen sind in allen Feldern zulässig. Die Felder sind wie folgt definiert:

device-name — Gibt den Namen des Geräts an. Eine Liste der aktuellen Gerätenamen finden Sie unter „So zeigen Sie Zuordnungsinformationen zu einem Gerät an“ auf Seite 90.

device-type — Gibt den generischen Gerätetyp an. Der generische Name entspricht dem Namen der Geräteklasse wie `st`, `fd` und `sr`. Im Feld *device-type* werden verwandte Geräte logisch gruppiert. Wenn Sie die Zuordnung für ein Gerät aktivieren, rufen Sie den Gerätenamen aus dem Feld *device-type* in der Datei `device_maps` ab.

`reserved` — Die mit `reserved` gekennzeichneten Felder werden für eine spätere Verwendung von Oracle reserviert.

auths — Gibt an, ob das Gerät zugeordnet werden kann. Ein Sternchen (`*`) in diesem Feld bedeutet, dass das Gerät nicht zugeordnet werden kann. Eine Autorisierungszeichenfolge oder ein leeres Feld bedeutet, dass das Gerät zugeordnet werden kann. Beispielsweise bedeutet die Zeichenfolge `solaris.device.allocate` im Feld *auths*, dass die Autorisierung `solaris.device.allocate` für die Gerätezuordnung erforderlich ist. Ein At-Zeichen (`@`) in dieser Datei weist darauf hin, dass das Gerät von allen Benutzern zugeordnet werden kann.

device-exec — Gibt den Pfadnamen eines Skripts an, das für eine spezielle Verarbeitung aufgerufen werden soll, beispielsweise Bereinigung und Objektwiederverwendungsschutz während der Zuordnung. Das Skript *device-exec* wird ausgeführt, wenn das Gerät durch den Befehl `deallocate` verwendet wird.

Beispielsweise gibt der folgende Eintrag für das Gerät `sr0` an, dass das CD-ROM-Laufwerk durch einen Benutzer mit der Autorisierung `solaris.device.allocate` zugeordnet werden kann:

```
sr0;sr;reserved;reserved;solaris.device.allocate;/etc/security/lib/sr_clean
```

Sie können die Standardgeräte und die zugehörigen definierten Merkmale übernehmen. Nach dem Installieren neuer Geräte können Sie die Einträge ändern. Alle Geräte, die vor einer Verwendung zugeordnet werden müssen, müssen in den Dateien `device_allocate` und `device_maps` für das System dieses Geräts definiert sein. Derzeit können Magnetbandkassetten-, Disketten-, CD-ROM-Laufwerke und Audiochips zugeordnet werden. Diese Gerätetypen verfügen über Bereinigungsskripten.

Hinweis – Xylogics-Bandlaufwerke oder Archivierungsbandlaufwerke verwenden ebenfalls das Skript `st_clean`, das für SCSI-Geräte verfügbar ist. Sie müssen eigene Bereinigungsskripten für andere Geräte wie Modems, Terminals, Grafiktablette und andere zuordenbare Geräte erstellen. Das Skript muss die Anforderungen für die Objektwiederverwendung für diesen Gerätetyp erfüllen.

Bereinigungsskripten

Die Gerätezuordnung erfüllt einen Teil der Anforderung für die Objektwiederverwendung. Die *Bereinigungsskripten* entsprechen der Sicherheitsanforderung, dass vor der Wiederverwendung alle verwendbaren Daten von einem physischen Laufwerk gelöscht werden müssen. Die Daten werden gelöscht, bevor das Gerät einem anderen Benutzer zugeordnet werden kann. Für Magnetbandkassetten-, Disketten-, CD-ROM-Laufwerke und Audiogeräte sind standardmäßig Bereinigungsskripten erforderlich. Oracle Solaris stellt diese Skripten zur Verfügung. In diesem Abschnitt wird der Verwendungszweck von Bereinigungsskripten beschrieben.

Bereinigungsskript für Bandlaufwerke

Das Bereinigungsskript `st_clean` unterstützt drei Bandgeräte:

- ¼-Zoll-SCSI-Band
- ¼-Zoll-Archivierungsband
- ½-Zoll-Tonband

Das Skript `st_clean` verwendet die Option `rewoffl` für den Befehl `mt`, um das Gerät zu bereinigen. Weitere Informationen erhalten Sie auf der Manpage `mt(1)`. Wenn das Skript beim Booten des Systems ausgeführt wird, stellt es fest, ob das Gerät online ist. Wenn das Gerät online ist, stellt das Skript fest, ob Datenträger im Gerät enthalten sind. Die ¼-Zoll-Bandgeräte, in denen Datenträger enthalten sind, werden in den Zuweisungsfehlerstatus versetzt. Durch den Zuweisungsfehlerstatus muss der Administrator das Gerät manuell bereinigen.

Wenn während des normalen Systembetriebs der Befehl `deallocate` im interaktiven Modus ausgeführt wird, wird der Benutzer aufgefordert, den Datenträger zu entfernen. Das Aufheben der Zuordnung wird verzögert, bis der Datenträger aus dem Gerät entfernt wurde.

Bereinigungsskripten für Disketten- und CD-ROM-Laufwerke

Die folgenden Bereinigungsskripten werden für Disketten- und CD-ROM-Laufwerke zur Verfügung gestellt:

- **`fd_clean` (Skript)**: Ist ein Bereinigungsskript für Diskettenlaufwerke
- **`sr_clean` (Skript)**: Ist ein Bereinigungsskript für CD-ROM-Laufwerke

Die Skripten verwenden den Befehl `eject`, um den Datenträger aus dem Laufwerk zu entfernen. Wenn der Befehl `eject` fehlschlägt, wird das Gerät in den Zuweisungsfehlerstatus versetzt. Weitere Informationen finden Sie auf der Manpage `eject(1)`.

Bereinigungsskript für Audio

Audiogeräte werden mit einem `audio_clean`-Skript bereinigt. Das Skript führt einen `AUDIO_GETINFO`-ioctl-Systemaufruf durch, um das Gerät zu lesen. Anschließend führt das Skript einen `AUDIO_SETINFO`-ioctl-Systemaufruf durch, um die Gerätekonfiguration auf die Standardeinstellung zurückzusetzen.

Erstellen neuer Bereinigungsskripten

Wenn Sie weitere zuordenbare Geräte zum System hinzufügen, müssen Sie möglicherweise eigene Bereinigungsskripten erstellen. Der Befehl `deallocate` leitet einen Parameter an die Bereinigungsskripten weiter. Der im Folgenden gezeigte Parameter besteht aus einer Zeichenfolge, die den Gerätenamen enthält. Weitere Informationen erhalten Sie auf der Manpage `device_allocate(4)`.

clean-script `-[I|i|f|S]` *device-name*

Bereinigungsskripten müssen `0` für eine erfolgreiche Durchführung und einen Wert höher als `0` für eine fehlerhafte Durchführung zurückgeben. Die Optionen `-I`, `-f` und `-S` bestimmen den Ausführungsmodus des Skripts:

`-I` Wird nur während beim Booten des Systems benötigt. Die gesamte Ausgabe muss an die Systemkonsole erfolgen. Wenn ein Fehler auftritt oder das Auswerfen des Datenträgers nicht erzwungen werden kann, muss das Gerät in den Zuweisungsfehlerstatus versetzt werden.

`-i` Ähnlich wie die Option `-I`, mit der Ausnahme, dass die Ausgabe unterdrückt wird

`-f` Entspricht einer erzwungenen Bereinigung. Die Option ist interaktiv und geht davon aus, dass der Benutzer auf Eingabeaufforderungen reagieren kann. Durch ein Skript mit dieser Option muss die Bereinigung abgeschlossen werden, wenn ein Teil der Bereinigung fehlschlägt.

`-S` Entspricht einer standardmäßigen Bereinigung. Die Option ist interaktiv und geht davon aus, dass der Benutzer auf Eingabeaufforderungen reagieren kann.

◆ ◆ ◆ KAPITEL 5

Verwenden von Basic Audit Reporting Tool (Aufgaben)

In diesem Kapitel wird beschrieben, wie Sie ein Manifest der Dateien auf einem System erstellen und mit diesem Manifest die Systemintegrität überprüfen. BART (Basic Audit Reporting Tool) ermöglicht eine umfassende Validierung von Systemen, indem über einen längeren Zeitraum hinweg Überprüfungen auf Dateiebene in einem System durchgeführt werden.

Im Folgenden ist eine Liste der Informationen in diesem Kapitel aufgeführt:

- „Basic Audit Reporting Tool (Übersicht)“ auf Seite 107
- „Verwenden von BART (Aufgaben)“ auf Seite 111
- „Manifeste, Regeldateien und Berichte von BART (Referenz)“ auf Seite 125

Basic Audit Reporting Tool (Übersicht)

BART ist ein Tool für die Überwachung von Dateien, das vollständig auf Dateisystemebene verwendet wird. Mit BART können Sie schnell, einfach und zuverlässig Informationen zu den Komponenten in dem auf den bereitgestellten Systemen installierten Software-Stack erfassen. Durch BART kann der Verwaltungsaufwand eines Netzwerks von Systemen erheblich verringert werden, indem zeitaufwendige administrative Aufgaben vereinfacht werden.

Mit BART können Sie die Änderungen feststellen, die im Vergleich zu festgelegten Basiswerten auf Dateiebene eines Systems durchgeführt wurden. Durch BART können Sie ein Basiswerte- oder *Steuerungs*-Manifest von einem vollständig installierten und konfigurierten System erstellen. Anschließend können Sie diese Basiswerte mit einem Schnappschuss des Systems zu einem späteren Zeitpunkt vergleichen und einen Bericht generieren, in dem Änderungen auf Dateiebene, die seit Installation des Systems durchgeführt wurden, aufgezeichnet werden.

Der Befehl `bart` ist ein standardmäßiger UNIX-Befehl. Sie können die Ausgabe des Befehls `bart` an eine Datei umleiten und zu einem späteren Zeitpunkt verarbeiten.

Funktionen von BART

Eine einfache Syntax, die sowohl leistungsstark als auch flexibel ist, war der Schwerpunkt der Entwicklung von BART. Mit dem Tool können Sie Manifeste eines bestimmten Systems über einen längeren Zeitraum generieren. Bei der Validierung der Dateien des Systems können Sie einen Bericht generieren und das alte und neue Manifest miteinander vergleichen. Außerdem können Sie BART verwenden, um Manifeste ähnlicher Systeme zu generieren und Vergleiche zwischen Systemen durchzuführen. Der Hauptunterschied zwischen BART und anderen Prüfungs-Tools ist die Flexibilität von BART, sowohl was die überwachten als auch im Bericht enthaltenen Informationen angeht.

Zu den zusätzlichen Vorteilen und Verwendungen von BART zählen:

- Effiziente und einfache Methode zum Katalogisieren eines Systems, auf dem die Oracle Solaris-Software auf Dateiebene ausgeführt wird
- Definieren der zu überwachenden Dateien und gegebenenfalls Ändern von Profilen. Durch diese Flexibilität können Sie lokale Anpassungen überwachen und die Software einfach und effizient neu konfigurieren.
- Sicherstellen der Ausführung zuverlässiger Software auf den Systemen
- Überwachen von Änderungen auf Dateiebene eines Systems über einen längeren Zeitraum, wodurch beschädigte oder ungewöhnliche Dateien festgestellt werden können
- Beheben von Problemen bei der Systemleistung

Komponenten von BART

BART enthält zwei Hauptkomponenten und eine optionale Komponente:

- BART-Manifest
- BART-Bericht
- BART-Regeldatei

BART-Manifest

Mit dem Befehl `bart create` können Sie einen Schnappschuss eines Systems auf Dateiebene zu einem bestimmten Zeitpunkt erstellen. Als Ausgabe werden ein Katalog von Dateien und Dateiattribute erstellt, die als *Manifest* bezeichnet werden. In einem Manifest sind Informationen zu allen Dateien oder bestimmten Dateien auf einem System aufgeführt. Es bietet Informationen zu Attributen von Dateien, die einige eindeutig identifizierbare Informationen wie eine MD5-Prüfsumme enthalten. Weitere Informationen zur MD5-Prüfsumme erhalten Sie auf der Manpage `md5(3EXT)`. Ein Manifest kann gespeichert und zwischen Client- und Serversystemen übertragen werden.

Hinweis – BART wird *nicht* über Dateisystemgrenzen hinweg verwendet (mit Ausnahme von Dateisystemen des gleichen Typs). Durch diese Beschränkung ist die Ausgabe des Befehls `bart create` besser vorhersehbar. Wenn keine Argumente vorhanden sind, werden beispielsweise durch den Befehl `bart create` alle Dateisysteme unter dem Stammverzeichnis (`/`) katalogisiert. Jedoch werden keine NFS- oder TMPFS-Dateisysteme oder eingehängte CD-ROMs katalogisiert. Prüfen Sie während der Erstellung eines Manifests keine Dateisysteme in einem Netzwerk. Beachten Sie, dass bei der Verwendung von BART für die Überwachung von vernetzten Dateisystemen umfangreiche Ressourcen zur Generierung von wenig nützlichen Manifesten benötigt werden.

Weitere Informationen zu BART-Manifesten erhalten Sie unter „Format der BART-Manifest-Datei“ auf Seite 125.

BART-Bericht

Das Berichterstellungs-Tool weist drei Arten von Eingaben auf: zwei zu vergleichende Manifeste und eine vom Benutzer zur Verfügung gestellte Regeldatei, in der die zu kennzeichnenden Abweichungen angegeben sind.

Mit dem `bart compare`-Befehl können Sie zwei Manifeste vergleichen, ein *Steuerungs-Manifest* und ein *Test-Manifest*. Diese Manifeste müssen mit den gleichen Dateisystemen, Optionen und der gleichen Regeldatei, die Sie mit dem Befehl `bart create` verwenden, vorbereitet worden sein.

Die Ausgabe des Befehls `bart compare` ist ein Bericht, in dem Abweichungen auf Dateibasis zwischen den zwei Manifesten aufgeführt sind. Eine *Abweichung* ist eine Änderung an einem Attribut einer bestimmten Datei, die für beide Manifeste katalogisiert ist. Hinzufügungen oder Löschungen von Dateieinträgen zwischen den zwei Manifesten werden ebenfalls als Abweichungen bezeichnet.

Bei der Berichterstellung zu Abweichungen bestehen zwei Steuerungsebenen:

- Beim Generieren eines Manifests
- Beim Erstellen von Berichten

Diese Steuerungsebenen sind beabsichtigt, da das Generieren eines Manifests aufwendiger ist als die Berichterstellung von Abweichungen zwischen zwei Manifesten. Nach dem Erstellen von Manifesten können Sie Manifeste aus unterschiedlichen Perspektiven vergleichen, indem Sie den Befehl `bart compare` mit verschiedenen Regeldateien ausführen.

Weitere Informationen zu BART-Berichten erhalten Sie unter „Berichterstellung bei BART“ auf Seite 128.

BART-Regeldatei

Die *Regeldatei* ist eine Textdatei, die Sie optional als Eingabe für den Befehl `bart` verwenden können. Diese Datei verwendet Einschließungs- und Ausschließungsregeln. Eine Regeldatei wird zum Erstellen von benutzerdefinierten Manifesten und Berichten verwendet. In einer Regeldatei können Sie durch eine kurze und präzise Syntax ausdrücken, welche Sätze von Dateien katalogisiert sowie welche Attribute für einen bestimmten Satz von Dateien überwacht werden sollen. Beim Vergleichen von Manifesten dient die Regeldatei zum Kennzeichnen von Abweichungen zwischen den Manifesten. Durch eine Regeldatei können Sie bestimmte Informationen zu den Dateien in einem System effizient erfassen.

Eine Regeldatei kann in einem Texteditor erstellt werden. Mit einer Regeldatei können Sie folgende Aufgaben durchführen:

- Erstellen Sie mit dem Befehl `bart create` ein Manifest, in dem Informationen zu allen oder bestimmten Dateien in einem System aufgeführt sind.
- Generieren Sie mit dem Befehl `bart compare` einen Bericht, durch den bestimmte Attribute eines Dateisystems überwacht werden.

Hinweis – Sie können verschiedene Regeldateien für unterschiedliche Zwecke erstellen. Wenn Sie jedoch ein Manifest mithilfe einer Regeldatei erstellen, müssen Sie die gleiche Regeldatei verwenden, um die Manifeste miteinander zu vergleichen. Andernfalls werden bei der Ausgabe des Befehls `bart compare` verschiedene ungültige Abweichungen aufgeführt.

Eine Regeldatei kann ebenfalls Syntaxfehler und andere mehrdeutige Informationen als Ergebnis eines Benutzerfehlers enthalten. Wenn eine Regeldatei falsche Informationen enthält, werden diese Benutzerfehler ebenfalls gemeldet.

Die Überwachung bestimmter Dateien und Dateiattribute in einem System mithilfe einer Regeldatei muss geplant werden. Legen Sie vor dem Erstellen einer Regeldatei fest, welche Dateien und Dateiattribute im System überwacht werden sollen. Je nach gewünschtem Ergebnis können Sie mit einer Regeldatei beispielsweise Manifeste erstellen, Manifeste vergleichen usw.

Weitere Informationen zur BART-Regeldatei finden Sie unter „Format der BART-Regeldatei“ auf Seite 126 und auf der Manpage `bart_rules(4)`.

Verwenden von BART (Übersicht der Schritte)

Aufgabe	Beschreibung	Anweisungen
Erstellen eines BART-Manifests	Generiert eine Liste von Informationen zu allen in einem System installierten Dateien.	„So erstellen Sie ein Manifest“ auf Seite 112
Erstellen eines benutzerdefinierten BART-Manifests	Generiert auf eine der folgenden Arten eine Liste von Informationen zu bestimmten in einem System installierten Dateien: ■ Durch Angeben eines Teilbaums ■ Durch Angeben eines Dateinamens ■ Durch Verwenden einer Regeldatei	„So passen Sie ein Manifest an“ auf Seite 114 Beispiel 5–2 Beispiel 5–3 Beispiel 5–4
Vergleichen von BART-Manifesten	Generiert einen Bericht, in dem die über einen längeren Zeitraum durchgeführten Änderungen an einem System verglichen werden. Oder es wird ein Bericht generiert, in dem ein oder mehrere Systeme mit dem Steuerungssystem verglichen werden.	„So vergleichen Sie Manifeste für das gleiche System über einen längeren Zeitraum“ auf Seite 118 „So vergleichen Sie Manifeste von verschiedenen Systemen“ auf Seite 120
(Optional) Anpassen eines BART-Berichts	Generiert auf eine der folgenden Arten einen benutzerdefinierten BART-Bericht: ■ Durch Angeben von Attributen ■ Durch Verwenden einer Regeldatei	„So passen Sie einen BART-Bericht durch Angeben von Dateiattributen an“ auf Seite 123 „So passen Sie einen BART-Bericht durch eine Regeldatei an“ auf Seite 124

Verwenden von BART (Aufgaben)

Sie können den Befehl `bart` als gewöhnlicher Benutzer, Superuser oder Benutzer mit der Rolle "Primary Administrator" ausführen. Wenn Sie den Befehl `bart` als gewöhnlicher Benutzer ausführen, können Sie nur Dateien katalogisieren und überwachen, für die Sie über Zugriffsberechtigung verfügen, wie Dateien in Ihrem Home-Verzeichnis. Das Ausführen des Befehls `bart` als Superuser bietet den Vorteil, dass die erstellten Manifeste Informationen zu verborgenen und privaten Dateien, die Sie überwachen können, enthalten. Wenn Sie Informationen zu Dateien mit eingeschränkten Berechtigungen (beispielsweise Datei `/etc/passwd` oder `/etc/shadow`) katalogisieren und überwachen möchten, führen Sie den Befehl `bart` als Superuser aus. Weitere Informationen zu rollenbasierter Zugriffssteuerung finden Sie unter „Rollenbasierte Zugriffssteuerung (Übersicht)“ auf Seite 190.

Sicherheitsüberlegungen zu BART

Wenn Sie den Befehl `bart` als Superuser ausführen, ist die Ausgabe für alle Benutzer lesbar. Diese Ausgabe enthält Dateinamen, die als privat betrachtet werden. Wenn Sie den Befehl `bart` als Superuser ausführen, führen Sie entsprechende Maßnahmen zum Schützen der Ausgabe durch. Verwenden Sie beispielsweise Optionen, durch die Ausgabedateien mit einschränkenden Berechtigungen generiert werden.

Hinweis – Die Verfahren und Beispiele in diesem Kapitel zeigen, wie der Befehl `bart` von einem Superuser ausgeführt wird. Sofern nicht anders angegeben, ist das Ausführen des Befehls `bart` als Superuser optional.

▼ So erstellen Sie ein Manifest

Das Manifest eines Systems wird unmittelbar nach einer Erstinstallation der Oracle Solaris-Software erstellt. Durch diese Art von Manifest erhalten Sie Basiswerte, um die über einen längeren Zeitraum hinweg an einem System durchgeführten Änderungen zu vergleichen. Außerdem können Sie mit diesem Manifest die Manifeste verschiedener Systeme vergleichen. Wenn Sie beispielsweise einen Schnappschuss der Systeme im Netzwerk erstellen und anschließend die Test-Manifeste mit dem Steuerungs-Manifest vergleichen, können Sie schnell die erforderlichen Maßnahmen feststellen, um das Testsystem mit der Basiswertekonfiguration zu synchronisieren.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Erstellen Sie nach der Installation der Oracle Solaris-Software ein Steuerungs-Manifest und leiten Sie die Ausgabe an eine Datei weiter.

```
# bart create options > control-manifest
```

`-R` Gibt das Stammverzeichnis für das Manifest an. Alle von den Regeln angegebenen Pfade werden relativ zu diesem Verzeichnis interpretiert. Alle im Manifest gemeldeten Pfade sind relativ zu diesem Verzeichnis.

`-I` Akzeptiert eine Liste einzelner zu katalogisierender Dateien, entweder über die Befehlszeile oder von der Standardeingabe.

`-r` Entspricht dem Namen der Regeldatei für dieses Manifest. Wenn – zusammen mit der Option `-r` verwendet wird, wird die Regeldatei von der Standardeingabe gelesen.

`-n` Deaktiviert die Inhaltssignatur für alle regulären Dateien in der Dateiliste. Durch diese Option kann die Leistung verbessert werden. Außerdem können Sie diese Option verwenden, wenn der Inhalt der Dateiliste geändert werden sollte, wie im Falle von Systemprotokolldateien.

3 Untersuchen Sie den Inhalt des Manifests.

4 Speichern Sie das Manifest für eine spätere Verwendung.

Wählen Sie einen aussagekräftigen Namen für das Manifest. Verwenden Sie beispielsweise den Systemnamen und das Datum der Manifest-Erstellung.

Beispiel 5–1 Erstellen eines Manifests mit Informationen zu Dateien in einem System

Wenn Sie den Befehl `bart create` ohne Optionen ausführen, werden die Informationen zu den im System installierten Dateien katalogisiert. Verwenden Sie diese Art von Manifest als Basiswerte, wenn Sie mehrere Systeme von einem zentralen Image installieren. Außerdem können Sie diese Art von Manifest verwenden, um durch Vergleiche sicherzustellen, dass die Installationen identisch sind.

Beispiel:

```
# bart create
! Version 1.0
! Thursday, December 04, 2003 (16:17:39)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 1024 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9ea47 0 0
/.java D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f8dc04d 0 10
/.java/.userPrefs D 512 40700 user::rwx,group::---,mask:---
other:--- 3f8dc06b 010
/.java/.userPrefs/.user.lock.root F 0 100600 user::rw-
group::---,mask:---,other:--- 3f8dc06b 0 10 -
/.java/.userPrefs/.userRootModFile.root F 0 100600 user::rw-,
group::---,mask:---,other:--- 3f8dc0a1 0 10 -
.
.
.
/var/sadm/pkg/SUNWdtmad/install/depend F 932 100644 user::rw-,
group::r--,mask:r--,other:r-- 3c23a19e 0 0 -
/var/sadm/pkg/SUNWdtmad/pkginfo F 594 100644 user::rw-
group::r--,mask:r--,other:r-- 3f81e416 0 0 -
/var/sadm/pkg/SUNWdtmad/save D 512 40755 user::rwx,group::r-x
mask:r-x,other:r-x 3f81e416 0 0
/var/sadm/pkg/SUNWdtmaz D 512 40755 user::rwx,group::r-x
mask:r-x,other:r-x 3f81e41b 0 0
```

```
/var/sadm/pkg/TSIpgxw/save D 512 40755 user::rwx
group::r-x,mask:r-x,other:r-x 3f81e892 0 0
.
.
.
```

Die Manifeste bestehen aus einem Header und Einträgen. Je nach Dateityp besteht jeder Manifest-Dateieintrag aus einer Zeile. Beispielsweise entspricht bei den Manifest-Einträgen in der vorhergehenden Ausgabe der Typ `F` einer Datei und der Typ `D` einem Verzeichnis. Außerdem sind Informationen zu Größe, Inhalt, Benutzer-ID, Gruppen-ID und Berechtigungen aufgeführt. Dateieinträge in der Ausgabe werden durch die codierten Versionen der Dateinamen sortiert, um Sonderzeichen ordnungsgemäß zu verarbeiten. Alle Einträge werden in aufsteigender Reihenfolge nach Dateiname sortiert. Bei allen nicht standardmäßigen Dateinamen, beispielsweise mit eingebetteten Zeilenende- oder Tabulatorzeichen, werden die nicht standardmäßigen Zeichen in Anführungszeichen gesetzt, bevor die Sortierung durchgeführt wird.

Zeilen, die mit `!` beginnen, stellen Metadaten zum Manifest zur Verfügung. Die Zeile mit der Manifestversion gibt die Version der Manifestspezifikation an. Die Datumszeile gibt das Datum der Manifest-Erstellung im Datumsformat an. Weitere Informationen erhalten Sie auf der Manpage `date(1)`. Einige Zeilen werden vom Vergleichs-Tool des Manifests ignoriert. Zu den ignorierten Zeilen zählen leere Zeilen, Zeilen aus Leerstellen und mit `#` beginnende Kommentare.

▼ So passen Sie ein Manifest an

Sie können ein Manifest auf eine der folgenden Arten anpassen:

- Durch Angeben eines Teilbaums

  Indem Sie ein Manifest für einen einzelnen Teilbaum auf einem System erstellen, können Sie die Überwachung der Änderungen an bestimmten Dateien effizient durchführen, anstatt am gesamten Inhalt eines umfangreichen Verzeichnisses. Sie können ein Basiswerte-Manifest für einen bestimmten Teilbaum auf Ihrem System erstellen und anschließend in regelmäßigen Abständen Test-Manifeste für den gleichen Teilbaum erstellen. Verwenden Sie den Befehl `bart compare`, um das Steuerungs-Manifest mit dem Test-Manifest zu vergleichen. Durch diese Option können Sie wichtige Dateisysteme effizient überwachen und feststellen, ob die Sicherheit von Dateien durch einen Eindringling gefährdet wurde.
- Durch Angeben eines Dateinamens

  Da das Erstellen eines Manifests für die Katalogisierung des gesamten Systems zeit- und arbeitsaufwendiger ist sowie mehr Speicherplatz erfordert, können Sie diese Option des Befehls `bart` verwenden, wenn Sie nur Informationen zu einer oder mehreren bestimmten Dateien im System aufführen möchten.

- Durch Verwenden einer Regeldatei

  Mit der Regeldatei erstellen Sie angepasste Manifeste, in denen Informationen zu bestimmten Dateien und Teilbäumen in einem System aufgeführt werden. Außerdem verwenden Sie eine Regeldatei zum Überwachen bestimmter Dateiattribute. Indem Sie eine Regeldatei zum Erstellen und Vergleichen von Manifesten verwenden, können Sie mehrere Attribute für verschiedene Dateien oder Teilbäume angeben. Über die Befehlszeile können Sie stattdessen nur eine globale Attributdefinition angeben, die für alle Dateien in den erstellten Manifesten oder generierten Berichten gilt.

1. **Legen Sie die zu katalogisierenden und zu überwachenden Dateien fest.**

2. **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

   Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

3. **Erstellen Sie nach dem Installieren der Oracle Solaris-Software ein benutzerdefiniertes Manifest, indem Sie eine der folgenden Optionen verwenden:**

   - Durch Angeben eines Teilbaums:

     ```
     # bart create -R root-directory
     ```

   - Durch Angeben eines oder mehrerer Dateinamen:

     ```
     # bart create -I filename...
     ```

     Beispiel:

     ```
     # bart create -I /etc/system /etc/passwd /etc/shadow
     ```

   - Durch Verwenden einer Regeldatei:

     ```
     # bart create -r rules-file
     ```

4. **Untersuchen Sie den Inhalt des Manifests.**

5. **Speichern Sie das Manifest für eine spätere Verwendung.**

Beispiel 5–2 Erstellen eines Manifests durch Angeben eines Teilbaums

In diesem Beispiel wird beschrieben, wie Sie ein Manifest erstellen, das nur Informationen zu den Dateien im Teilbaum `/etc/ssh` enthält.

```
# bart create -R /etc/ssh
! Version 1.0
! Saturday, November 29, 2003 (14:05:36)
# Format:
```

```
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f81eab9 0 3
/ssh_config F 861 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81e504 0 3 422453ca0e2348cd9981820935600395
/ssh_host_dsa_key F 668 100600 user::rw-,group::---,mask:---,
other:--- 3f81eab9 0 0 5cc28cdc97e833069fd41ef89e4d9834
/ssh_host_dsa_key.pub F 602 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81eab9 0 0 16118c736995a4e4754f5ab4f28cf917
/ssh_host_rsa_key F 883 100600 user::rw-,group::---,mask:---,
other:--- 3f81eaa2 0 0 6ff17aa968ecb20321c448c89a8840a9
/ssh_host_rsa_key.pub F 222 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81eaa2 0 0 9ea27617efc76058cb97aa2caa6dd65a
.
.
.
```

Beispiel 5–3 Anpassen eines Manifests durch Angeben eines Dateinamens

In diesem Beispiel wird beschrieben, wie Sie ein Manifest erstellen, das nur Informationen zu den Dateien `/etc/passwd` und `/etc/shadow` eines Systems enthält.

```
# bart create -I /etc/passwd /etc/shadow
! Version 1.0
! Monday, December 15, 2003 (16:28:55)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/etc/passwd F 542 100444 user::r--,group::r--,mask:r--,
other:r-- 3fcfd45b 0 3 d6
84554f85d1de06219d80543174ad1a
/etc/shadow F 294 100400 user::r--,group::---,mask:---,
other:--- 3f8dc5a0 0 3 fd
c3931c1ae5ee40341f3567b7cf15e2
```

Im Folgenden finden Sie einen Vergleich zwischen der Standardausgabe des Befehls `ls -al` für die Datei `/etc/passwd` und `/etc/shadow` auf dem gleichen System.

```
# ls -al /etc/passwd
-r--r--r--   1 root     sys          542 Dec  4 17:42 /etc/passwd

# ls -al /etc/shadow
-r--------   1 root     sys          294 Oct 15 16:09 /etc/shadow
```

Beispiel 5–4 Anpassen eines Manifests durch Verwenden einer Regeldatei

In diesem Beispiel wird beschrieben, wie Sie ein Manifest erstellen, indem Sie mit einer Regeldatei nur die Dateien im Verzeichnis `/etc` katalogisieren. Die gleiche Regeldatei enthält Direktiven, die vom Befehl `bart compare` zur die Überwachung der Änderungen am Attribut `acl` der Datei `/etc/system` verwendet werden.

- Erstellen Sie mit einem Texteditor eine Regeldatei, durch die nur diese Dateien im Verzeichnis `/etc` katalogisiert werden.

```
# List information about all the files in the /etc directory.

CHECK all
/etc

# Check only acl changes in the /etc/system file

IGNORE all
CHECK acl
/etc/system
```

  Weitere Informationen zum Erstellen von Regeldateien finden Sie unter „BART-Regeldatei“ auf Seite 110.

- Erstellen Sie ein Steuerungs-Manifest anhand der zuvor erstellten Regeldatei.

```
# bart create -r etc.rules-file > etc.system.control-manifest
! Version 1.0
! Thursday, December 11, 2003 (21:51:32)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/etc/system F 1883 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81db61 0 3
```

- Erstellen Sie ein Test-Manifest, um Änderungen am System zu überwachen. Bereiten Sie das Test-Manifest genauso wie das Steuerungs-Manifest vor, indem Sie die gleichen `bart`-Optionen und die gleiche Regeldatei verwenden.
- Vergleichen Sie die Manifeste, indem Sie die gleiche Regeldatei verwenden.

▼ So vergleichen Sie Manifeste für das gleiche System über einen längeren Zeitraum

Verwenden Sie dieses Verfahren, wenn Sie Änderungen auf Dateiebene für das gleiche System über einen längeren Zeitraum vergleichen möchten. Mit dieser Art von Manifest können Sie beschädigte oder ungewöhnliche Dateien erkennen, Sicherheitsverletzungen feststellen oder Probleme bei der Systemleistung beheben.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Erstellen Sie nach der Installation der Oracle Solaris-Software ein Steuerungs-Manifest der zu überwachenden Dateien im System.

```
# bart create -R /etc > control-manifest
```

3 Erstellen Sie ein Test-Manifest, das genau wie das Steuerungs-Manifest vorbereitet ist, wenn Sie Änderungen am System überwachen möchten.

```
# bart create -R /etc > test-manifest
```

4 Vergleichen Sie das Steuerungs-Manifest mit dem Test-Manifest.

```
# bart compare options control-manifest test-manifest > bart-report
```

`-r`	Entspricht dem Namen der Regeldatei für diesen Vergleich. Wenn Sie die Option `-r` zusammen mit – verwenden, werden die Direktiven aus der Standardausgabe gelesen.
`-i`	Ermöglicht dem Benutzer, globale `IGNORE`-Direktiven über die Befehlszeile festzulegen.
`-p`	Entspricht dem programmatischen Modus, der eine standardmäßige nicht lokalisierte Ausgabe für programmatisches Parsing generiert.
control-manifest	Entspricht der Ausgabe des Befehls `bart create` für das Steuerungssystem.
test-manifest	Entspricht der Ausgabe des Befehls `bart create` für das Testsystem.

5 Untersuchen Sie den BART-Bericht auf ungewöhnliche Vorfälle.

Beispiel 5–5 Vergleichen von Manifesten für das gleiche System über einen längeren Zeitraum

In diesem Beispiel wird beschrieben, wie Sie Änderungen überwachen, die im Verzeichnis `/etc` zwischen zwei angegebenen Zeitpunkten durchgeführt wurden. Durch diesen Vergleich können Sie schnell feststellen, ob die Sicherheit wichtiger Dateien im System gefährdet wurde.

- Erstellen Sie ein Steuerungs-Manifest.

```
# bart create -R /etc > system1.control.121203
! Version 1.0
! Friday, December 12, 2003 (08:34:51)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 4096 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9dfb4 0 3
/.cpr_config F 2236 100644 user::rw-,group::r--,mask:r--,other:r--
3fd9991f 0 0
67cfa2c830b4ce3e112f38c5e33c56a2
/.group.lock F 0 100600 user::rw-,group::---,mask:---,other:--- 3f81f14d
0 1 d41
d8cd98f00b204e9800998ecf8427e
/.java D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f81dcb5 0 2
/.java/.systemPrefs D 512 40755 user::rwx,group::r-x,mask:r-x,
other:r-x 3f81dcb7
.
.
.
```

- Erstellen Sie ein Test-Manifest, wenn Sie Änderungen am Verzeichnis `/etc` überwachen möchten.

```
# bart create -R /etc > system1.test.121503
Version 1.0
! Monday, December 15, 2003 (08:35:28)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 4096 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9dfb4 0 3
/.cpr_config F 2236 100644 user::rw-,group::r--,mask:r--,other:r--
3fd9991f 0 0
67cfa2c830b4ce3e112f38c5e33c56a2
/.group.lock F 0 100600 user::rw-,group::---,mask:---,other:---
3f81f14d 0 1 d41d8cd98f00b204e9800998ecf8427e
/.java D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f81dcb5 0 2
/.java/.systemPrefs D 512 40755 user::rwx,group::r-x,mask:r-x,
other:r-x 3f81dcb70 2
/.java/.systemPrefs/.system.lock F 0 100644 user::rw-,group::r--
```

```
,mask:r--,other:
r-- 3f81dcb5 0 2 d41d8cd98f00b204e9800998ecf8427e
/.java/.systemPrefs/.systemRootModFile F 0 100644 user::rw-,
group::r--,mask:r--,
other:r-- 3f81dd0b 0 2 d41d8cd98f00b204e9800998ecf8427e
.
.
.
```

- Vergleichen Sie das Steuerungs-Manifest mit dem Test-Manifest.

```
# bart compare system1.control.121203 system1.test.121503
/vfstab:
  mode  control:100644  test:100777
  acl  control:user::rw-,group::r--,mask:r--,other:r--  test:user::rwx,
group::rwx,mask:rwx,other:rwx
```

Die vorhergehende Ausgabe bedeutet, dass Berechtigungen der Datei `vfstab` seit der Erstellung des Steuerungs-Manifests geändert wurden. Mit diesem Bericht können Sie untersuchen, ob Eigentümer, Datum, Inhalt oder andere Dateiattribute geändert wurden. Durch diese Art von Informationen können Sie nachverfolgen, wer die Datei manipuliert hat und wann die Änderung durchgeführt wurde.

▼ So vergleichen Sie Manifeste von verschiedenen Systemen

Indem Sie Vergleiche zwischen Systemen durchführen, können Sie schnell feststellen, ob Unterschiede auf Dateiebene zwischen einem Basiswertesystem und anderen Systemen bestehen. Wenn Sie beispielsweise eine bestimmte Version der Oracle Solaris-Software auf einem Basiswertesystem installiert haben und feststellen möchten, ob auf anderen Systemen die gleichen Pakete installiert sind, können Sie Manifeste für diese Systeme erstellen und anschließend die Test-Manifeste mit dem Steuerungs-Manifest vergleichen. Bei diesem Vergleich werden Abweichungen im Dateiinhalt zwischen den Testsystemen und dem Steuerungssystem aufgeführt.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Erstellen Sie nach dem Installieren der Oracle Solaris-Software ein Steuerungs-Manifest.

```
# bart create options > control-manifest
```

3 Speichern Sie das Steuerungs-Manifest.

4. **Erstellen Sie auf dem Testsystem mit den gleichen `bart`-Optionen ein Manifest und leiten Sie die Ausgabe an eine Datei weiter.**

   `# bart create` *options* `>` *test1-manifest*

   Wählen Sie einen eindeutigen und aussagekräftigen Namen für das Testmanifest.

5. **Speichern Sie das Testmanifest an einem zentralen Speicherort im System, bis Sie die Manifeste vergleichen können.**

6. **Wenn Sie die Manifeste vergleichen möchten, kopieren Sie das Steuerungs-Manifest in den Speicherort des Test-Manifests. Stattdessen können Sie auch das Test-Manifest in das Steuerungssystem kopieren.**

   Beispiel:

   # **`cp`** *control-manifest /net/test-server/bart/manifests*

   Wenn das Testsystem kein über NFS eingehängtes System ist, verwenden Sie beispielsweise FTP, um das Steuerungs-Manifest auf das Testsystem zu kopieren.

7. **Vergleichen Sie das Steuerungs-Manifest mit dem Test-Manifest und leiten Sie die Ausgabe an eine Datei weiter.**

   `# bart compare` *control-manifest test1-manifest > test1.report*

8. **Untersuchen Sie den BART-Bericht auf ungewöhnliche Vorfälle.**

9. **Wiederholen Sie die Schritte 4 bis 9 für jedes Test-Manifest, das Sie mit dem Steuerungs-Manifest vergleichen möchten.**

   Verwenden Sie die gleichen `bart`-Optionen für jedes Testsystem.

Beispiel 5–6 Vergleichen von Manifesten verschiedener Systeme mit dem Manifest eines Steuerungssystems

In diesem Beispiel wird beschrieben, wie Sie Änderungen am Inhalt des Verzeichnisses `/usr/bin` überwachen, indem Sie ein Steuerungs-Manifest mit einem Test-Manifest eines anderen Systems vergleichen.

- Erstellen Sie ein Steuerungs-Manifest.

```
# bart create -R /usr/bin > control-manifest.121203
!Version 1.0
! Friday, December 12, 2003 (09:19:00)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
```

```
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 13312 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9e925 0 2
/.s F 14200 104711 user::rwx,group::--x,mask:--x,other:--x
3f8dbfd6 0 1 8ec7e52d8a35ba3b054a6394cbf71cf6
/ControlPanel L 28 120777 - 3f81dc71 0 1 jre/bin/ControlPanel
/HtmlConverter L 25 120777 - 3f81dcdc 0 1 bin/HtmlConverter
/acctcom F 28300 100555 user::r-x,group::r-x,mask:r-x,other:r-x
3f6b5750 0 2 d6e99b19c847ab4ec084d9088c7c7608
/activation-client F 9172 100755 user::rwx,group::r-x,mask:r-x,
other:r-x 3f5cb907 0 1 b3836ad1a656324a6e1bd01edcba28f0
/adb F 9712 100555 user::r-x,group::r-x,mask:r-x,other:r-x
3f6b5736 0 2 5e026413175f65fb239ee628a8870eda
/addbib F 11080 100555 user::r-x,group::r-x,mask:r-x,other:r-x
3f6b5803 0 2 a350836c36049febf185f78350f27510
.
.
.
```

- Erstellen Sie ein Test-Manifest für jedes System, das Sie mit dem Steuerungssystem vergleichen möchten.

```
# bart create -R /usr/bin > system2-manifest.121503
! Version 1.0
! Friday, December 15, 2003 (13:30:58)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 13312 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9ea9c 0 2
/.s F 14200 104711 user::rwx,group::--x,mask:--x,other:--x
3f8dbfd6 0 1 8ec7e52d8a35ba3b054a6394cbf71cf6
/ControlPanel L 28 120777 - 3f81dc71 0 1 jre/bin/ControlPanel
/HtmlConverter L 25 120777 - 3f81dcdc 0 1 bin/HtmlConverter
/acctcom F 28300 100555 user::r-x,group::r-x,mask:r-x,other:
r-x 3f6b5750 0 2 d6e99b19c847ab4ec084d9088c7c7608
.
.
.
```

- Wenn Sie die Manifeste miteinander vergleichen möchten, kopieren Sie die Manifeste an den gleichen Speicherort.

```
# cp control-manifest /net/system2.central/bart/manifests
```

- Vergleichen Sie das Steuerungs-Manifest mit dem Test-Manifest.

```
# bart compare control-manifest  system2.test > system2.report
/su:
  gid  control:3  test:1
/ypcat:
  mtime  control:3fd72511  test:3fd9eb23
```

Die vorhergehende Ausgabe gibt an, dass die Gruppen-ID der Datei `su` im Verzeichnis `/usr/bin` nicht identisch mit der des Steuerungssystems ist. Anhand dieser Angabe können Sie feststellen, ob eine andere Version der Software auf dem Testsystem installiert wurde oder ob jemand die Datei manipuliert hat.

▼ So passen Sie einen BART-Bericht durch Angeben von Dateiattributen an

In diesem optionalen Verfahren wird beschrieben, wie Sie einen BART-Bericht anpassen, indem Sie Dateiattribute über die Befehlszeile angeben. Wenn Sie ein Basiswerte-Manifest erstellen, in dem Informationen zu allen oder bestimmten Dateien im System enthalten sind, können Sie bei der Ausführung des Befehls `bart compare` je nach Bedarf andere Attribute angeben, um Änderungen an einem bestimmten Verzeichnis, Unterverzeichnis, einer Datei oder Dateien zu überwachen. Sie können verschiedene Arten von Vergleichen für die gleichen Manifeste ausführen, indem Sie unterschiedliche Dateiattribute über die Befehlszeile angeben.

1. **Legen Sie fest, welche Dateiattribute Sie überwachen möchten.**

2. **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

   Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

3. **Erstellen Sie nach dem Installieren der Oracle Solaris-Software ein Steuerungs-Manifest.**

4. **Erstellen Sie ein Test-Manifest, um die Änderungen zu überwachen.**

   Bereiten Sie das Test-Manifest genauso vor wie das Steuerungs-Manifest.

5. **Vergleichen Sie die Manifeste.**

   Beispiel:

   ```
   # bart compare -i dirmtime,lnmtime,mtime control-manifest.121503 \
   test-manifest.010504 > bart.report.010504
   ```

   Beachten Sie, dass die Attribute durch ein Komma in der Befehlszeilensyntax getrennt werden.

6. **Untersuchen Sie den BART-Bericht auf ungewöhnliche Vorfälle.**

▼ So passen Sie einen BART-Bericht durch eine Regeldatei an

In diesem optionalen Verfahren wird beschrieben, wie Sie einen BART-Bericht anpassen, indem Sie eine Regeldatei als Eingabe für den Befehl `bart compare` verwenden. Das Anpassen eines BART-Berichts durch eine Regeldatei bietet Ihnen Flexibilität, um verschiedene Attribute für mehrere Dateien oder Teilbäume anzugeben. Sie können verschiedene Vergleiche für die gleichen Manifeste ausführen, indem Sie unterschiedliche Regeldateien verwenden.

1. **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

   Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Legen Sie fest, welche Dateien und Dateiattribute Sie überwachen möchten.**

3. **Erstellen Sie mit einem Texteditor eine Regeldatei mit den entsprechenden Direktiven.**

4. **Erstellen Sie nach dem Installieren der Oracle Solaris-Software ein Steuerungs-Manifest, indem Sie die zuvor erstellte Regeldatei verwenden.**

   ```
   # bart create -r rules-file > control-manifest
   ```

5. **Erstellen Sie ein Test-Manifest, das identisch wie das Steuerungs-Manifest vorbereitet ist.**

   ```
   # bart create -r rules-file > test-manifest
   ```

6. **Vergleichen Sie das Steuerungs-Manifest mit dem Test-Manifest, indem Sie die gleiche Regeldatei verwenden.**

   ```
   # bart compare -r rules-file control-manifest test-manifest > bart.report
   ```

7. **Untersuchen Sie den BART-Bericht auf ungewöhnliche Vorfälle.**

Beispiel 5–7 Anpassen eines BART-Berichts durch Verwenden einer Regeldatei

Die folgende Regeldatei enthält Direktiven für die Befehle `bart create` und `bart compare`. Die Regeldatei weist den Befehl `bart create` an, Informationen zum Inhalt des Verzeichnisses `/usr/bin` aufzuführen. Außerdem weist die Regeldatei den Befehl `bart compare` an, nur Änderungen an Größe und Inhalt im gleichen Verzeichnis zu überwachen.

```
# Check size and content changes in the /usr/bin directory.
# This rules file only checks size and content changes.
# See rules file example.
```

```
IGNORE all
CHECK size contents
/usr/bin
```

- Erstellen Sie ein Steuerungs-Manifest anhand der zuvor erstellten Regeldatei.

  ```
  # bart create -r bartrules.txt > usr_bin.control-manifest.121003
  ```

- Erstellen Sie ein Test-Manifest, wenn Sie Änderungen am Verzeichnis `/usr/bin` überwachen möchten.

  ```
  # bart create -r bartrules.txt > usr_bin.test-manifest.121103
  ```

- Vergleichen Sie die Manifeste, indem Sie die gleiche Regeldatei verwenden.

  ```
  # bart compare -r bartrules.txt usr_bin.control-manifest \
  usr_bin.test-manifest
  ```

- Untersuchen Sie die Ausgabe des Befehls `bart compare`.

  ```
   /usr/bin/gunzip:  add
  /usr/bin/ypcat:
    delete
  ```

In der vorhergehenden Ausgabe wurde durch den Befehl `bart compare` eine Abweichung im Verzeichnis `/usr/bin` gemeldet. Diese Ausgabe weist darauf hin, dass die Datei `/usr/bin/ypcat` gelöscht und die Datei `/usr/bin/gunzip` hinzugefügt wurde.

Manifeste, Regeldateien und Berichte von BART (Referenz)

Dieser Abschnitt enthält die folgenden Referenzinformationen:

- „Format der BART-Manifest-Datei“ auf Seite 125
- „Format der BART-Regeldatei“ auf Seite 126
- „Berichterstellung bei BART“ auf Seite 128

In diesem Abschnitt wird das Format der von BART erstellten und verwendeten Dateien beschrieben.

Format der BART-Manifest-Datei

Je nach Dateityp besteht jeder Manifest-Dateieintrag aus einer Zeile. Jeder Eintrag beginnt mit *fname*, was dem Namen der Datei entspricht. Um Parsing-Fehler durch in Dateinamen eingebettete Sonderzeichen zu vermeiden, sind die Dateinamen codiert. Weitere Informationen erhalten Sie unter „Format der BART-Regeldatei“ auf Seite 126.

Die nachfolgenden Felder stellen die folgenden Dateiattribute dar:

type Dateityp mit den folgenden möglichen Werten:

- B für einen Blockgeräteknoten
- C für einen Zeichengeräteknoten
- D für ein Verzeichnis
- F für eine Datei
- L für einen symbolischen Link
- P für eine Pipe-Verkettung
- S für ein Socket

size Dateigröße in Byte

mode Oktalzahl, die die Berechtigungen der Datei darstellt

acl ACL-Attribute für die Datei. Enthält bei einer Datei mit ACL-Attributen die Ausgabe von `acltotext()`

uid Numerische Benutzer-ID des Eigentümers dieses Eintrags

gid Numerische Gruppen-ID des Eigentümers dieses Eintrags

dirmtime Zeit der letzten Änderung (in Sekunden) seit 00:00:00 (UTC), 1. Januar 1970, für Verzeichnisse

lnmtime Zeit der letzten Änderung (in Sekunden) seit 00:00:00 (UTC), 1. Januar 1970, für Links

mtime Zeit der letzten Änderung (in Sekunden) seit 00:00:00 (UTC), 1. Januar 1970, für Dateien

contents Prüfsummenwert der Datei. Dieses Attribut wird nur für reguläre Dateien angegeben. Wenn Sie die Kontextprüfung deaktivieren oder wenn Prüfsummen nicht berechnet werden können, weist dieses Feld den Wert – auf.

dest Ziel eines symbolischen Links

devnode Wert eines Geräteknotens. Dieses Attribut gilt nur für Zeichengerätdateien und Blockgerätdateien.

Weitere Informationen zu BART-Manifesten erhalten Sie auf der Manpage `bart_manifest(4)`.

Format der BART-Regeldatei

Die Eingabedateien für den Befehl `bart` sind Textdateien. Diese Dateien bestehen aus Zeilen, die angeben, welche Dateien im Manifest und welche Dateiattribute im Bericht enthalten sein sollen. Die gleiche Eingabedatei kann für beide BART-Funktionen verwendet werden. Mit # beginnende Zeilen, leere Zeilen und Zeilen mit Leerstellen werden vom Tool ignoriert.

Die Eingabedateien weisen drei Arten von Direktiven auf:

- Teilbaumdirektive mit optionalen Mustervergleichsmodifikatoren
- Direktive `CHECK`
- Direktive `IGNORE`

BEISPIEL 5–8 Regeldateiformat

```
<Global CHECK/IGNORE Directives>
<subtree1> [pattern1..]
<IGNORE/CHECK Directives for subtree1>

<subtree2> [pattern2..]
<subtree3> [pattern3..]
<subtree4> [pattern4..]
<IGNORE/CHECK Directives for subtree2, subtree3, subtree4>
```

Hinweis – Alle Direktiven werden der Reihe nach gelesen, wobei die früheren durch spätere Direktiven überschrieben werden können.

Es gibt eine Teilbaumdirektive pro Zeile. Die Direktive *muss* mit einem absoluten Pfadnamen beginnen, der von keiner oder mehreren Mustervergleichsanweisungen gefolgt wird.

Regeldateiattribute

Der Befehl `bart` verwendet die Anweisungen `CHECK` und `IGNORE`, um zu definieren, welche Attribute nachverfolgt oder ignoriert werden sollen. Jedem Attribut ist ein Schlüsselwort zugewiesen.

Das Attribut *Schlüsselwörter* kann aus Folgendem bestehen:

- `acl`
- `all`
- `contents`
- `dest`
- `devnode`
- `dirmtime`
- `gid`
- `lnmtime`
- `mode`
- `mtime`
- `size`
- `type`
- `uid`

Das Schlüsselwort `all` bezieht sich auf alle Dateiattribute.

Zitatzeichensyntax

Die von BART verwendete Regeldatei-Spezifikationssprache entspricht der standardmäßigen UNIX-Zitatzeichensyntax für die Darstellung von nicht standardmäßigen Dateinamen. Eingebettete Tabulator-, Leer-, Zeilenende- oder Sonderzeichen sind im entsprechenden oktalen Format codiert, damit das Tool die Dateinamen lesen kann. Diese nicht einheitliche Zitatzeichensyntax verhindert, dass bestimmte Dateinamen (beispielsweise mit einem eingebetteten Wagenrücklaufzeichen) in einer Befehls-Pipeline ordnungsgemäß verarbeitet werden. Die Regelspezifikationssprache ermöglicht die Angabe komplexer Dateinamen-Filterkriterien, die bei Verwendung einer Shell-Syntax nur schwierig und ineffizient zu beschreiben wären.

Weitere Informationen zur BART-Regeldatei oder der von BART verwendeten Zitatzeichensyntax finden Sie auf der Manpage `bart_rules(4)`.

Berichterstellung bei BART

Im Standardmodus werden durch den Befehl `bart compare` (siehe folgendes Beispiel) alle Dateien im System überprüft, mit Ausnahme der geänderten Verzeichniszeitstempel (`dirmtime`):

```
CHECK all
IGNORE    dirmtime
```

Wenn Sie eine Regeldatei angeben, werden die globalen Direktiven von `CHECK all` und `IGNORE dirmtime` (in dieser Reihenfolge) automatisch an die Regeldatei vorangestellt.

Ausgabe bei BART

Die folgenden Endewerte werden zurückgegeben:

0 Erfolgreich

1 Nicht schwerwiegender Fehler beim Verarbeiten der Dateien, wie Berechtigungsfehler

>1 Schwerwiegender Fehler, wie ungültige Befehlszeilenoption

Der Berichterstellungsmechanismus bietet zwei Arten von Ausgaben: ausführlich und programmatisch:

- Standardmäßig wird die ausführliche Ausgabe verwendet, die lokalisiert und auf mehreren Zeilen dargestellt wird. Die ausführliche Ausgabe ist internationalisiert und wird in Klartext angezeigt. Wenn durch den Befehl `bart compare` zwei System-Manifeste verglichen werden, wird eine Liste von Dateiunterschieden generiert.

  Beispiel:

  filename attribute control:xxxx test:yyyy

  filename — Name der Datei, die sich zwischen dem Steuerungs-Manifest und dem Test-Manifest unterscheidet

  attribute — Name des Dateiattributs, das sich zwischen den verglichenen Manifesten unterscheidet. *xxxx* entspricht dem Attributwert des Steuerungs-Manifests und *yyyy* dem Attributwert des Test-Manifests. Wenn Abweichungen zwischen mehreren Attributen in der gleichen Datei auftreten, wird jede Abweichung auf einer separaten Zeile dargestellt.

  Im Folgenden sehen Sie ein Beispiel der Standardausgabe für den Befehl `bart compare`. Die Attributunterschiede gelten für die Datei `/etc/passwd`. Die Ausgabe gibt an, dass die Attribute `size`, `mtime` und `contents` geändert wurden.

```
/etc/passwd:
size    control:74    test:81
mtime control:3c165879    test:3c165979
contents    control:daca28ae0de97afd7a6b91fde8d57afa
test:84b2b32c4165887355317207b48a6ec7
```

- Programmatische Ausgabe wird generiert, wenn Sie die Option `-p` für den Befehl `bart compare` verwenden. Diese Ausgabe wird in einer für die programmatische Bearbeitung geeigneten Form generiert. Bei der programmatischen Ausgabe kann einfach ein Parsing von anderen Programmen durchgeführt werden. Diese Ausgabe dient als Eingabe für andere Tools.

  Beispiel:

  filename attribute control-val test-val [*attribute control-val test-val*]*

  filename — Identisch mit dem Attribut *filename* im Standardformat

  Attribut control-val test-val — Eine Beschreibung der Dateiattribute, die sich zwischen den Steuerungs- und Test-Manifesten der einzelnen Dateien unterscheiden

Eine Liste der Attribute, die vom Befehl `bart` unterstützt werden, erhalten Sie unter „Regeldateiattribute“ auf Seite 127.

Weitere Informationen zu BART erhalten Sie auf der Manpage `bart(1M)`.

◆ ◆ ◆ KAPITEL 6

Steuern des Zugriffs auf Dateien (Aufgaben)

In diesem Kapitel wird beschrieben, wie Sie Dateien in Oracle Solaris schützen können. Sie erfahren außerdem, wie Sie das System vor Dateien schützen, deren Berechtigungen ein Sicherheitsrisiko darstellen.

Hinweis – Weitere Informationen zum Schützen von ZFS-Dateien mit Zugriffssteuerungslisten (Access Control Lists, ACLs) finden Sie unter Kapitel 8, „Schützen von Oracle Solaris ZFS-Dateien mit Zugriffssteuerungslisten und Attributen“ in *Oracle Solaris ZFS-Administrationshandbuch*.

Im Folgenden ist eine Liste der Informationen in diesem Kapitel aufgeführt.

- „Schützen von Dateien mithilfe von UNIX-Berechtigungen“ auf Seite 131
- „Schützen von UFS-Dateien mithilfe von Zugriffssteuerungslisten“ auf Seite 138
- „Vermeiden von Sicherheitsrisiken in Verbindung mit ausführbaren Dateien“ auf Seite 141
- „Schützen von Dateien (Übersicht der Schritte)“ auf Seite 142
- „Schützen von Dateien mithilfe von UNIX-Berechtigungen (Übersicht der Schritte)“ auf Seite 143
- „Schützen von UFS-Dateien mit ACLs (Übersicht der Schritte)“ auf Seite 149
- „Schützen vor Programmen mit Sicherheitsrisiko (Übersicht der Schritte)“ auf Seite 155

Schützen von Dateien mithilfe von UNIX-Berechtigungen

Dateien können mithilfe von UNIX-Dateiberechtigungen und ACLs gesichert werden. Dateien mit Sticky Bits und ausführbare Dateien erfordern spezielle Sicherheitsmaßnahmen.

Befehle zum Anzeigen und Schützen von Dateien

In dieser Tabelle werden die Befehle zum Überwachen und Schützen von Dateien und Verzeichnissen aufgeführt.

TABELLE 6–1 Befehle zum Schützen von Dateien und Verzeichnissen

Befehl	Description (Beschreibung)	Manpage
`ls`	Zeigt die Dateien in einem Verzeichnis und Informationen zu den Dateien an	`ls(1)`
`chown`	Ändert die Eigentümerschaft einer Datei	`chown(1)`
`chgrp`	Ändert die Gruppeneigentümerschaft einer Datei	`chgrp(1)`
`chmod`	Ändert die Berechtigungen für eine Datei. Sie können die Berechtigungen für eine Datei entweder im symbolischen Modus (mit Buchstaben und Symbolen) oder im absoluten Modus (mit Oktalzahlen) ändern.	`chmod(1)`

Datei- und Verzeichniseigentümerschaft

Herkömmliche UNIX-Dateiberechtigungen können drei Klassen von Benutzern Eigentümerschaft zuweisen:

- **User**: Der Datei- oder Verzeichniseigentümer, der normalerweise dem Benutzer entspricht, der die Datei erstellt hat. Der Benutzer einer Datei kann entscheiden, wer in der Datei lesen, schreiben (Änderungen vornehmen) oder (bei ausführbaren Dateien) wer sie ausführen kann.
- **Group**: Mitglieder einer Gruppe von Benutzern
- **Other**: Alle anderen Benutzer, die weder Eigentümer der Datei noch Mitglieder der Gruppe sind.

Der Eigentümer der Datei kann normalerweise Dateiberechtigungen zuweisen oder ändern. Darüber hinaus können Benutzer oder Rollen mit administrativen Fähigkeiten, wie der Superuser oder die Rolle "Primary Administrator", die Eigentümerschaft für eine Datei ändern. Informationen zum Überschreiben der Systemrichtlinie finden Sie unter Beispiel 6–2.

Es gibt sieben Dateitypen. Jeder Typ wird durch ein Symbol dargestellt:

- (Minussymbol)	Text oder Programm
b	Spezielle Blockdatei
c	Spezielle Zeichendatei
d	Verzeichnis
l	Symbolischer Link
s	Socket
D	Door (Verweis)
P	Benannte Pipe (FIFO)

UNIX-Dateiberechtigungen

In der folgenden Tabelle werden die Berechtigungen aufgeführt und beschrieben, die Sie den einzelnen Benutzerklassen für eine Datei oder ein Verzeichnis gewähren können.

TABELLE 6–2 Datei- und Verzeichnisberechtigungen

Symbol	Berechtigung	Objekt	Description (Beschreibung)
`r`	Lesen	Datei	Die angegebenen Benutzer können eine Datei öffnen und ihren Inhalt lesen.
		Verzeichnis	Die angegebenen Benutzer können die Dateien im Verzeichnis anzeigen.
`w`	Schreiben	Datei	Die angegebenen Benutzer können den Inhalt der Datei ändern oder die Datei löschen.
		Verzeichnis	Die angegebenen Benutzer können Dateien hinzufügen oder dem Verzeichnis Links hinzufügen. Sie können außerdem Dateien oder Links aus dem Verzeichnis entfernen.
`x`	Ausführen	Datei	Die angegebenen Benutzer können die Datei ausführen, wenn sie ein Programm oder Shell-Skript ist. Sie können das Programm auch mit einem der `exec(2)`-Systemaufrufe ausführen.
		Verzeichnis	Die angegebenen Benutzer können Dateien im Verzeichnis öffnen oder ausführen. Sie können das Verzeichnis und dessen Unterverzeichnisse als das aktuelle Verzeichnis festlegen.
-	Verweigert	Datei und Verzeichnis	Die angegebenen Benutzer können die Datei nicht lesen, nicht darin schreiben und sie auch nicht ausführen.

Die Dateiberechtigungen gelten für normale und besondere Dateien wie Geräte, Sockets oder benannte Pipes (FIFOs).

Für einen symbolischen Link gelten die gleichen Berechtigungen wie für die Datei, auf die der Link verweist.

Sie können die Dateien in einem Verzeichnis und dessen Unterverzeichnissen schützen, indem Sie die Berechtigungen für dieses Verzeichnis einschränken. Beachten Sie jedoch, dass der Superuser auf alle Dateien und Verzeichnisse im System Zugriff hat.

Besondere Dateiberechtigungen (`setuid`, `setgid` und Sticky Bit)

Drei besondere Berechtigungstypen sind für ausführbare Dateien und öffentliche Verzeichnisse verfügbar: `setuid`, `setgid` und Sticky Bit. Wenn diese Berechtigungen eingestellt sind, übernimmt jeder Benutzer, der die ausführbare Datei ausführt, die ID des Eigentümers (oder der Gruppe) der ausführbaren Datei.

Sie müssen bei der Gewährung besonderer Berechtigungen überlegt vorgehen, da diese Berechtigungen ein Sicherheitsrisiko darstellen können. Ein Benutzer kann beispielsweise Superuser-Rechte erhalten, indem er ein Programm ausführt, dass die Benutzer-ID (UID) auf `0` einstellt. Dies entspricht der UID des `root`-Benutzers. Außerdem können alle Benutzer besondere Berechtigungen für ihre eigenen Dateien einstellen, was ein weiteres Sicherheitsrisiko bedeutet.

Überwachen Sie Ihr System auf nicht autorisierte Verwendung der `setuid`- und `setgid`-Berechtigung zum Erhalt von Superuser-Rechten. Eine verdächtige Berechtigung weist einem Benutzer statt `root` oder `bin` die Eigentümerschaft für ein administratives Programm zu. Informationen zum Suchen und Anzeigen aller Dateien, die diese besondere Berechtigung verwenden, finden Sie unter „So suchen Sie Dateien mit besonderen Dateiberechtigungen“ auf Seite 155.

`setuid`-Berechtigung

Wenn eine `setuid`-Berechtigung für eine ausführbare Datei eingestellt wird, erhält der ausführende Prozess Zugriff auf der Basis des Dateieigentümers. Der Zugriff entspricht *nicht* dem Benutzer, der die Datei ausführt. Diese besondere Berechtigung ermöglicht einem Benutzer, auf die Datei und die Verzeichnisse zuzugreifen, die normalerweise nur für den Eigentümer verfügbar sind.

Die `setuid`-Berechtigung im `passwd`-Befehl ermöglicht Benutzern beispielsweise, Passwörter zu ändern. Ein `passwd`-Befehl mit einer `setuid`-Berechtigung kann wie folgt aussehen:

```
-r-sr-sr-x   3 root     sys       28144 Jun 17 12:02 /usr/bin/passwd
```

Diese besondere Berechtigung stellt ein Sicherheitsrisiko dar. Entschlossene Benutzer finden sicher eine Möglichkeit, die vom `setuid`-Prozess gewährten Berechtigungen nach der Beendigung des Prozesses weiterhin zu behalten.

Hinweis – Bei Verwendung der `setuid`-Berechtigungen mit den reservierten UIDs (0 – 100) von einem Programm wird die effektive UID möglicherweise nicht richtig eingestellt. Verwenden Sie ein Shell-Skript oder vermeiden Sie die Verwendung der reservierten UIDs mit `setuid`-Berechtigungen.

`setgid`-Berechtigung

Die `setgid`-Berechtigung ist der `setuid`-Berechtigung ähnlich. Die effektive Gruppen-ID (GID) des Prozesses wird in die Gruppe geändert, die über die Datei verfügt, und ein Benutzer erhält basierend auf den der Gruppe gewährten Berechtigungen Zugriff. Der Befehl `/usr/bin/mail` verfügt über `setgid`-Berechtigungen:

```
-r-x--s--x   1 root   mail     67504 Jun 17 12:01 /usr/bin/mail
```

Wenn die `setgid`-Berechtigung auf ein Verzeichnis angewendet wird, gehören die in diesem Verzeichnis erstellten Dateien zu der gleichen Gruppe wie das Verzeichnis. Die Dateien gehören nicht der Gruppe, zu der der erstellende Prozess gehört. Jeder Benutzer, der über Schreib- und Ausführungsberechtigungen in dem Verzeichnis verfügt, kann eine Datei dort erstellen. Die Datei gehört jedoch zu der Gruppe, zu der das Verzeichnis gehört, und nicht zu der Gruppe, zu der der Benutzer gehört.

Überwachen Sie Ihr System auf nicht autorisierte Verwendung der `setgid`-Berechtigung zum Erhalt von Superuser-Rechten. Eine verdächtige Berechtigung gewährt einer ungewöhnlichen Gruppe Gruppenzugriff auf ein solches Programm anstatt auf `root` oder `bin`. Informationen zum Suchen und Anzeigen aller Dateien, die diese Berechtigung verwenden, finden Sie unter „So suchen Sie Dateien mit besonderen Dateiberechtigungen“ auf Seite 155.

Sticky Bit

Die *Sticky Bit*-Berechtigung schützt die Dateien in einem Verzeichnis. Wenn für das Verzeichnis das Sticky Bit eingestellt ist, kann eine Datei nur von dem Dateieigentümer, dem Verzeichniseigentümer oder einem privilegierten Benutzer gelöscht werden. Der `root`-Benutzer und die Rolle "Primary Administrator" sind Beispiele für privilegierte Benutzer. Das Sticky Bit verhindert, dass ein Benutzer Dateien anderer Benutzer in öffentlichen Verzeichnissen wie `/tmp` löscht:

```
drwxrwxrwt 7  root  sys   400 Sep  3 13:37 tmp
```

Stellen Sie das Sticky Bit unbedingt manuell ein, wenn Sie ein öffentliches Verzeichnis oder ein TMPFS-Dateisystem einrichten. Anweisungen finden Sie unter Beispiel 6–5.

`umask`-Standardwert

Dateien oder Verzeichnisse werden mit Standardberechtigungen erstellt. Die Standardwerte des Systems sind offen. Eine Textdatei verfügt über die Berechtigungen `666`, die allen Benutzern Lese- und Schreibzugriff auf die Datei gewährt. Ein Verzeichnis und eine ausführbare Datei verfügen über die Berechtigungen `777`, die alle Benutzer zum Lesen, Schreiben und Ausführen berechtigen. Üblicherweise überschreiben Benutzer die Standardwerte des Systems in den Dateien `/etc/profile`, `.cshrc` oder `.login`.

Der durch den Befehl `umask` zugewiesene Wert wird vom Standardwert subtrahiert. Mit diesem Prozess werden Berechtigungen verweigert und zwar auf ähnliche Art, wie sie vom Befehl `chmod` gewährt werden. Mit dem Befehl `chmod 022` gewähren Sie der Gruppe und anderen Benutzern eine Schreibberechtigung. Mit dem Befehl `umask 022` entziehen Sie der Gruppe und anderen Benutzern die Schreibberechtigung.

Die folgende Tabelle zeigt einige typische `umask`-Einstellungen und wie sie sich auf eine ausführbare Datei auswirken.

TABELLE 6–3 `umask`-Einstellungen für unterschiedliche Sicherheitsebenen

Sicherheitsebene	`umask`-Einstellung	Verweigerte Berechtigungen
Niedrig (`744`)	`022`	`w` für Gruppe und andere Benutzer
Mittel (`740`)	`027`	`w` für Gruppe, `rwx` für andere Benutzer
Mittel (`741`)	`026`	`w` für Gruppe, `rw` für andere Benutzer
Hoch (`700`)	`077`	`rwx` für Gruppe und andere Benutzer

Weitere Informationen zum Einstellen des `umask`-Werts finden Sie auf der Manpage `umask(1)`.

Dateiberechtigungsmodi

Mit dem Befehl `chmod` können Sie die Berechtigungen für eine Datei ändern. Sie müssen Superuser oder Eigentümer einer Datei oder eines Verzeichnisses sein, um dessen Berechtigungen zu ändern.

Mit dem Befehl `chmod` können Sie die Berechtigungen in einem der beiden Modi einstellen:

- **Absoluter Modus**: Dateiberechtigungen werden als Zahlen dargestellt. Wenn Sie Berechtigungen im absoluten Modus ändern, stellen Sie die Berechtigungen für jede Dreiergruppe als Oktalmoduszahl dar. Der absolute Modus wird zum Einstellen der Berechtigungen am häufigsten verwendet.
- **Symbolischer Modus**: Um Berechtigungen hinzuzufügen oder zu ändern, werden Kombinationen aus Buchstaben und Symbolen verwendet.

In der folgenden Tabelle werden die Oktalwerte zur Einstellung der Dateiberechtigungen im absoluten Modus aufgeführt. Die Zahlen werden in Dreiergruppen verwendet, um die Berechtigungen für Eigentümer, Gruppe und andere Benutzer (in dieser Reihenfolge) einzustellen. Mit dem Wert `644` werden beispielsweise Lese- und Schreibberechtigungen für den Eigentümer sowie Leseberechtigungen für die Gruppe und andere Benutzer eingestellt.

TABELLE 6–4 Einstellen der Dateiberechtigungen im absoluten Modus

Oktalwert	Eingestellte Dateiberechtigungen	Beschreibung der Berechtigungen
`0`	`---`	Keine Berechtigungen
`1`	`--x`	Nur Ausführungsberechtigung
`2`	`-w-`	Nur Schreibberechtigung
`3`	`-wx`	Schreib- und Ausführungsberechtigung
`4`	`r--`	Nur Leseberechtigung
`5`	`r-x`	Lese- und Ausführungsberechtigung
`6`	`rw-`	Lese- und Schreibberechtigung
`7`	`rwx`	Lese-, Schreib- und Ausführungsberechtigung

In der folgenden Tabelle werden die Symbole zum Festlegen von Dateiberechtigungen im symbolischen Modus aufgeführt. Symbole können angeben, wessen Berechtigungen eingestellt oder geändert werden, welcher Vorgang ausgeführt wird und welche Berechtigungen zugewiesen oder geändert werden.

TABELLE 6–5 Einstellen der Dateiberechtigungen im symbolischen Modus

Symbol	Funktion	Description (Beschreibung)
`u`	*wer*	Benutzer (Eigentümer)
`g`	*wer*	Gruppe
`o`	*wer*	Andere
`a`	*wer*	Alle
`=`	*Operator*	Zuweisen
`+`	*Operator*	Hinzufügen
`-`	*Operator*	Entfernen
`r`	*Berechtigungen*	Lesen
`w`	*Berechtigungen*	Schreiben
`x`	*Berechtigungen*	Ausführen
`l`	*Berechtigungen*	Obligatorische Sperrung, `setgid`-Bit ist aktiviert, Gruppenausführungs-Bit ist deaktiviert
`s`	*Berechtigungen*	`setuid`- oder `setgid`-Bit ist aktiviert

TABELLE 6–5 Einstellen der Dateiberechtigungen im symbolischen Modus *(Fortsetzung)*

Symbol	Funktion	Description (Beschreibung)
`t`	*Berechtigungen*	Sticky Bit ist aktiviert, Ausführungs-Bit für andere Benutzer ist aktiviert

Die Bezeichnungen *wer, Operator, Berechtigungen* in der Spalte "Funktion" dienen zur näheren Beschreibung der Symbole zum Ändern der Berechtigungen für die Datei oder das Verzeichnis.

wer Gibt an, wessen Berechtigungen geändert werden

Operator Gibt an, welcher Vorgang ausgeführt wird

Berechtigungen Gibt an, welche Berechtigungen geändert werden sollen

Sie können besondere Berechtigungen für eine Datei im absoluten oder symbolischen Modus einstellen. Um `setuid`-Berechtigungen für ein Verzeichnis einzustellen oder zu entfernen, müssen Sie jedoch den symbolischen Modus verwenden. Im absoluten Modus stellen Sie besondere Berechtigungen ein, indem Sie links neben der Berechtigungsdreiergruppe einen neuen Oktalwert hinzufügen. In der folgenden Tabelle werden die Oktalwerte zum Einstellen besonderer Berechtigungen für eine Datei aufgeführt.

TABELLE 6–6 Einstellen der Dateiberechtigungen im absoluten Modus

Oktalwert	Besondere Dateiberechtigungen
`1`	Sticky Bit
`2`	`setgid`
`4`	`setuid`

Schützen von UFS-Dateien mithilfe von Zugriffssteuerungslisten

Traditioneller UNIX-Dateischutz bietet Lese-, Schreib- und Ausführungsberechtigungen für drei Benutzerklassen: Dateieigentümer, Dateigruppe und andere Benutzer. In einem UFS-Dateisystem erhöht eine Zugriffssteuerungsliste (Access Control List, ACL) die Dateisicherheit, da sie Folgendes ermöglicht:

- Definieren von Dateiberechtigungen für den Dateieigentümer, die Gruppe oder andere Benutzer, bestimmte Benutzer oder Gruppen
- Definieren von Standardberechtigungen für jede der oben stehenden Kategorien

Hinweis – Informationen zu ACLs im ZFS-Dateisystem und ACLs für NFSv4-Dateien finden Sie in Kapitel 8, „Schützen von Oracle Solaris ZFS-Dateien mit Zugriffssteuerungslisten und Attributen“ in *Oracle Solaris ZFS-Administrationshandbuch*.

Damit beispielsweise alle Mitglieder einer Gruppe eine Datei lesen können, erteilen Sie einfach der gesamten Gruppe die Leseberechtigung für diese Datei. Nehmen Sie an, dass nur eine Person in der Gruppe über eine Schreibberechtigung für die Datei verfügen soll. Bei standardmäßigem UNIX ist diese Ebene der Dateisicherheit nicht möglich, bei einer ACL dagegen schon.

In einem UFS-Dateisystem werden ACL-Einträge für eine Datei mit dem Befehl `setfacl` eingestellt. UFS-ACL-Einträge bestehen aus den folgenden Feldern, die durch Doppelpunkte getrennt sind:

entry-type:[*uid*|*gid*]:*perms*

entry-type Entspricht dem Typ des ACL-Eintrags für den Dateiberechtigungen eingestellt werden sollen. Beispielsweise kann *entry-type* ein `user` (der Eigentümer einer Datei) oder `mask` (die ACL-Maske) sein. Eine Liste der ACL-Einträge finden Sie in Tabelle 6–7 und Tabelle 6–8.

uid Entspricht dem Benutzernamen oder der Benutzer-ID (UID)

gid Entspricht dem Gruppennamen oder der Gruppen-ID (GID)

perms Entspricht den für *entry-type* eingestellten Berechtigungen Im Feld *perms* können die symbolischen Zeichen `rwx` oder eine Oktalzahl angegeben werden. Dies sind die gleichen Zahlen, die für den Befehl `chmod` verwendet werden.

In dem folgenden Beispiel gewährt ein ACL-Eintrag dem Benutzer `stacey` Lese- und Schreibberechtigungen.

```
user:stacey:rw-
```

Achtung – UFS-Dateisystemattribute wie ACLs werden nur in UFS-Dateisystemen unterstützt. Wenn Sie daher das Verzeichnis `/tmp`, das normalerweise als TMPFS-Dateisystem eingehängt ist, als Zielverzeichnis bei einer Wiederherstellung oder einem Kopiervorgang verwenden, gehen die ACL-Einträge verloren. Verwenden Sie das Verzeichnis `/var/tmp`, um UFS-Dateien vorübergehend zu speichern.

ACL-Einträge für UFS-Dateien

In der folgenden Tabelle werden die gültigen ACL-Einträge aufgeführt, die Sie beim Einstellen von ACLs für Dateien verwenden können. Die drei ersten ACL-Einträge bieten den grundlegenden UNIX-Dateischutz.

TABELLE 6–7 ACL-Einträge für UFS-Dateien

ACL-Eintrag	Description (Beschreibung)
`u[ser]::`*perms*	Dateieigentümer-Berechtigungen
`g[roup]::`*perms*	Dateigruppen-Berechtigungen
`o[ther]:`*perms*	Berechtigungen für andere Benutzer als den Dateieigentümer oder die Mitglieder der Dateigruppe
`m[ask]:`*perms*	ACL-Maske. Der Maskeneintrag gibt die maximalen Berechtigungen an, die für Benutzer (andere als der Eigentümer) und für Gruppen gewährt werden können. Die Maske ist eine Möglichkeit zum schnellen Ändern von Berechtigungen für alle Benutzer und Gruppen. Der Eintrag `mask:r--` gibt beispielsweise an, dass Benutzer und Gruppen nur über Leseberechtigungen verfügen dürfen, auch wenn in ihren Konten Schreib- und Ausführungsberechtigungen angegeben sind.
`u[ser]:`*uid:perms*	Berechtigungen für einen bestimmten Benutzer. Für *uid* können Sie entweder einen Benutzernamen oder eine numerische UID angeben.
`g[roup]:`*gid:perms*	Berechtigungen für eine bestimmte Gruppe. Für *gid* können Sie entweder einen Gruppennamen oder eine numerische GID angeben.

ACL-Einträge für UFS-Verzeichnisse

Zusätzlich zu den in Tabelle 6–7 beschriebenen ACL-Einträgen können Sie Standard-ACL-Einträge für ein Verzeichnis einstellen. Dateien oder Verzeichnisse, die in einem Verzeichnis mit Standard-ACL-Einträgen erstellt werden, weisen die gleichen ACL-Einträge wie die Standard-ACL-Einträge auf. In Tabelle 6–8 werden die Standard-ACL-Einträge für Verzeichnisse aufgeführt.

Wenn Sie die Standard-ACL-Einträge für bestimmte Benutzer und Gruppen in einem Verzeichnis zum ersten Mal einstellen, müssen Sie auch die Standard-ACL-Einträge für den Dateieigentümer, die Dateigruppen, andere Benutzer und die ACL-Maske angeben. Diese Einträge sind obligatorisch. Es handelt sich um die ersten vier Standard-ACL-Einträge in der folgenden Tabelle.

TABELLE 6–8 Standard-ACL-Einträge für UFS-Verzeichnisse

Standard-ACL-Eintrag	Description (Beschreibung)
`d[efault]:u[ser]::`*perms*	Standardmäßige Dateieigentümer-Berechtigungen
`d[efault]:g[roup]::`*perms*	Standardmäßige Dateigruppen-Berechtigungen
`d[efault]:o[ther]:`*perms*	Standardberechtigungen für andere Benutzer als den Dateieigentümer oder die Mitglieder der Dateigruppe
`d[efault]:m[ask]:`*perms*	Standard-ACL-Maske
`d[efault]:u[ser]:`*uid:perms*	Standardberechtigungen für einen bestimmten Benutzer. Für *uid* können Sie entweder einen Benutzernamen oder eine numerische UID angeben.
`d[efault]:g[roup]:`*gid:perms*	Standardberechtigungen für eine bestimmte Gruppe. Für *gid* können Sie entweder einen Gruppennamen oder eine numerische GID angeben.

Befehle zum Verwalten von UFS-ACLs

Mit den folgenden Befehlen können ACLs für UFS-Dateien oder -Verzeichnisse verwaltet werden.

Befehl `setfacl` — Dient zum Festlegen, Hinzufügen und Löschen von ACL-Einträgen. Weitere Informationen finden Sie auf der Manpage `setfacl(1)`.

Befehl `getfacl` — Dient zum Anzeigen von ACL-Einträgen. Weitere Informationen finden Sie auf der Manpage `getfacl(1)`.

Vermeiden von Sicherheitsrisiken in Verbindung mit ausführbaren Dateien

Eine Reihe von Sicherheitslücken sind mit standardmäßigen ausführbaren Stacks verbunden, wenn diese über Lese-, Schreib- und Ausführungsberechtigungen verfügen. Stacks mit Ausführungsberechtigungen sind zwar zulässig, jedoch funktionieren die meisten Programme auch ohne ausführbare Stacks.

Die Variable `noexec_user_stack` ermöglicht Ihnen anzugeben, ob Stack-Zuordnungen ausführbar sind. Die Variable ist ab der Version Solaris 2.6 verfügbar. Standardmäßig ist diese Variable auf null eingestellt, ausgenommen in 64-Bit-Anwendungen, wodurch ABI-konformes Verhalten sichergestellt wird. Wenn die Variable auf einen anderen Wert als null eingestellt wird, markiert das System den Stack jedes Prozesses im System als lesbar und beschreibbar, jedoch nicht als ausführbar.

Sobald diese Variable eingestellt ist, wird Programmen, die versuchen Code in ihrem Stack auszuführen, ein `SIGSEGV`-Signal gesendet. Dadurch wird das Programm normalerweise mit einem Speicherabzug beendet. Solche Programme generieren auch eine Warnung, die den Namen des Programms, die Prozess-ID und die tatsächliche UID des Benutzers, der das Programm ausgeführt hat, enthalten. Beispiel:

```
a.out[347] attempt to execute code on stack by uid 555
```

Die Meldung wird vom Dämon `syslog` ausgegeben, wenn die `syslog` `kern`-Funktion auf die Ebene `notice` eingestellt ist. Diese Ausgabe wird standardmäßig in der Datei `syslog.conf` eingestellt, d. h. die Meldung wird sowohl auf der Konsole als auch in die Datei `/var/adm/messages` ausgegeben. Weitere Informationen finden Sie auf den Manpages `syslogd(1M)` und `syslog.conf(4)`.

Anhand der `syslog`-Meldung lassen sich mögliche Sicherheitsprobleme feststellen. Die Meldung gibt auch gültige Programme an, die von ausführbaren Stacks abhängen, deren ordnungsgemäße Funktion durch die Einstellung dieser Variablen verhindert wurde. Wenn keine Meldungen ausgegeben werden sollen, stellen Sie für die Variable `noexec_user_stack_log` in der Datei `/etc/system` einen Wert von null ein. Auch wenn keine Meldungen ausgegeben werden, kann das SIGSEGV-Signal das ausführende Programm weiterhin mit einem Speicherabzug beenden.

Mit der Funktion `mprotect()` können Sie erreichen, dass Programme ihren Stack explizit als ausführbar markieren. Weitere Informationen finden Sie auf der Manpage `mprotect(2)`.

Aufgrund von Hardwarebeschränkungen können auf den meisten x86-basierten Systemen keine Probleme mit ausführbaren Stacks erkannt und gemeldet werden. Bei Systemen der ADM64-Produktfamilie werden jedoch Probleme mit ausführbaren Stacks erkannt und gemeldet.

Schützen von Dateien (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf Verfahren zum Schützen von Dateien.

Aufgabe	Description (Beschreibung)	Anweisungen
Schützen von Dateien mithilfe von UNIX-Berechtigungen	Zeigt UNIX-Berechtigungen für Dateien an. Schützt Dateien mit UNIX-Berechtigungen.	„Schützen von Dateien mithilfe von UNIX-Berechtigungen (Übersicht der Schritte)“ auf Seite 143
Schützen von Dateien mithilfe von ACLs	Fügt ACLs hinzu, um Dateien auf einer feiner abgestimmten Ebene zu schützen, als mit UNIX-Berechtigungen möglich ist	„Schützen von UFS-Dateien mit ACLs (Übersicht der Schritte)“ auf Seite 149

Aufgabe	Description (Beschreibung)	Anweisungen
Schützen des Systems vor Dateien, die ein Sicherheitsrisiko darstellen	Sucht ausführbare Dateien mit einer verdächtigen Eigentümerschaft. Deaktiviert Dateien, die das System beschädigen können.	„Schützen vor Programmen mit Sicherheitsrisiko (Übersicht der Schritte)“ auf Seite 155

Schützen von Dateien mithilfe von UNIX-Berechtigungen (Übersicht der Schritte)

In der folgenden Übersicht der Schritte wird auf Verfahren verwiesen, die Dateiberechtigungen auflisten und ändern, sowie Dateien mit besonderen Dateiberechtigungen schützen.

Aufgabe	Anweisungen
Anzeigen von Dateiinformationen	„So zeigen Sie Dateiinformationen an“ auf Seite 143
Ändern von Dateieigentümerschaft	„So ändern Sie den Eigentümer einer lokalen Datei“ auf Seite 144 „So ändern Sie die Gruppeneigentümerschaft einer Datei“ auf Seite 145
Ändern von Dateiberechtigungen	„So ändern Sie die Dateiberechtigungen im symbolischen Modus“ auf Seite 146 „So ändern Sie Dateiberechtigungen im absoluten Modus“ auf Seite 147 „So ändern Sie besondere Dateiberechtigungen im absoluten Modus“ auf Seite 148

▼ So zeigen Sie Dateiinformationen an

Mit dem Befehl `ls` zeigen Sie Informationen zu allen Dateien in einem Verzeichnis an.

- **Geben Sie den folgenden Befehl ein, um eine lange Liste aller Dateien im aktuellen Verzeichnis anzuzeigen.**

```
% ls -la
```

`-l` Zeigt das lange Format an, das Benutzereigentümerschaft, Gruppeneigentümerschaft und Dateiberechtigungen enthält

`-a` Zeigt alle Dateien an, einschließlich verborgener Dateien, die mit einem Punkt (`.`) beginnen

Beispiel 6–1 Anzeigen von Dateiinformationen

In dem folgenden Beispiel wird eine partielle Liste von Dateien im Verzeichnis `/sbin` angezeigt.

```
% cd /sbin
% ls -la
```

```
total 13456
drwxr-xr-x   2 root     sys          512 Sep  1 14:11 .
drwxr-xr-x  29 root     root        1024 Sep  1 15:40 ..
-r-xr-xr-x   1 root     bin       218188 Aug 18 15:17 autopush
lrwxrwxrwx   1 root     root          21 Sep  1 14:11 bpgetfile -> ...
-r-xr-xr-x   1 root     bin       505556 Aug 20 13:24 dhcpagent
-r-xr-xr-x   1 root     bin       456064 Aug 20 13:25 dhcpinfo
-r-xr-xr-x   1 root     bin       272360 Aug 18 15:19 fdisk
-r-xr-xr-x   1 root     bin       824728 Aug 20 13:29 hostconfig
-r-xr-xr-x   1 root     bin       603528 Aug 20 13:21 ifconfig
-r-xr-xr-x   1 root     sys       556008 Aug 20 13:21 init
-r-xr-xr-x   2 root     root      274020 Aug 18 15:28 jsh
-r-xr-xr-x   1 root     bin       238736 Aug 21 19:46 mount
-r-xr-xr-x   1 root     sys         7696 Aug 18 15:20 mountall
   .
   .
   .
```

Jede Zeile enthält Informationen zu einer Datei in der folgenden Reihenfolge:

- Dateityp – Beispiel: `d`. Eine Liste von Dateitypen finden Sie unter „Datei- und Verzeichniseigentümerschaft“ auf Seite 132.
- Berechtigungen – Beispiel: `r-xr-xr-x`. Eine Beschreibung finden Sie unter „Datei- und Verzeichniseigentümerschaft“ auf Seite 132.
- Anzahl der Hard Links – Beispiel: `2`
- Eigentümer der Datei – Beispiel `root`
- Gruppe der Datei – Beispiel: `bin`
- Dateigröße in Byte – Beispiel: `7696`
- Erstellungsdatum oder letztes Änderungsdatum der Datei – Beispiel: `Aug 18 15:20`
- Name der Datei – Beispiel `mountall`

▼ So ändern Sie den Eigentümer einer lokalen Datei

Der Dateieigentümer, die Rolle "Primary Administrator" oder der Superuser können die Eigentümerschaft einer beliebigen Datei ändern.

1 Zeigen Sie die Berechtigungen für eine Datei an.

```
% ls -l example-file
-rw-r--r--   1 janedoe   staff   112640 May 24 10:49 example-file
```

2 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

3 **Ändern Sie den Eigentümer der Datei.**

```
# chown stacey example-file
```

4 **Überprüfen Sie, ob der Eigentümer der Datei geändert wurde.**

```
# ls -l example-file
-rw-r--r--   1 stacey   staff   112640 May 26 08:50 example-file
```

Beispiel 6–2 Benutzern erlauben, die Eigentümerschaft für ihre eigenen Dateien zu ändern

Sicherheitshinweis: Ändern Sie die Einstellung der Variablen `rstchown` nicht ohne guten Grund in null. Diese Einstellung ermöglicht einem Benutzer, für die eigenen Dateien einen anderen Eigentümer zu definieren.

In diesem Beispiel ist die Variable `rstchown` in der Datei `/etc/system` auf null eingestellt. Diese Einstellung ermöglicht dem Eigentümer einer Datei, mit dem Befehl `chown` einen anderen Benutzer als Eigentümer der Datei zu definieren. Diese Einstellung ermöglicht dem Eigentümer, mit dem Befehl `chgrp` eine Gruppe, zu der er selbst nicht gehört, als Eigentümer der Datei zu definieren. Die Änderung wird erst nach einem Neustart des Systems wirksam.

```
set rstchown = 0
```

Weitere Informationen finden Sie auf den Manpages `chown(1)` und `chgrp(1)`.

Beachten Sie, dass das Ändern von Eigentümerschaft und Gruppen bei über NFS eingehängten Dateisystemen noch weiter eingeschränkt ist. Weitere Informationen zum Einschränken des Zugriffs auf über NFS eingehängten Systemen finden Sie in Kapitel 6, „Zugreifen auf Netzwerkdateisysteme (Referenz) “ in *Systemverwaltungshandbuch: Netzwerkdienste*.

▼ So ändern Sie die Gruppeneigentümerschaft einer Datei

1 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Ändern Sie die Gruppeneigentümerschaft für eine Datei.**

```
$ chgrp scifi example-file
```

Informationen zum Einrichten von Gruppen finden Sie in Kapitel 4, „Managing User Accounts and Groups (Overview)“ in *System Administration Guide: Basic Administration*.

3 Überprüfen Sie, ob sich die Gruppeneigentümerschaft der Datei geändert hat.

```
$ ls -l example-file
 -rw-r--r--   1 stacey   scifi   112640 June 20 08:55  example-file
```

Weitere Informationen finden Sie unter Beispiel 6–2.

▼ So ändern Sie die Dateiberechtigungen im symbolischen Modus

1 Wenn Sie nicht der Eigentümer der Datei oder des Verzeichnisses sind, melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Nur der aktuelle Eigentümer oder der Superuser kann die Berechtigungen für eine Datei oder ein Verzeichnis mit dem Befehl `chmod` ändern.

2 Ändern Sie die Berechtigungen in symbolischen Modus.

`% chmod` *who operator permissions filename*

wer	Gibt an, wessen Berechtigungen geändert werden
Operator	Gibt an, welcher Vorgang ausgeführt wird
Berechtigungen	Gibt an, welche Berechtigungen geändert werden sollen Eine Liste gültiger Symbole finden Sie in Tabelle 6–5.
filename	Gibt die Datei oder das Verzeichnis an.

3 Überprüfen Sie, ob die Berechtigungen für die Datei geändert wurden.

`% ls -l` *filename*

Beispiel 6–3 Ändern der Berechtigungen im symbolischen Modus

In dem folgenden Beispiel wird anderen Benutzern die Leseberechtigung entzogen.

```
% chmod o-r example-file1
```

In dem folgenden Beispiel werden dem Benutzer, der Gruppe und anderen Benutzern Lese- und Ausführungsberechtigungen gewährt.

```
$ chmod a+rx example-file2
```

In dem folgenden Beispiel werden der Gruppe Lese-, Schreib- und Ausführungsberechtigungen zugewiesen.

```
$ chmod g=rwx example-file3
```

▼ So ändern Sie Dateiberechtigungen im absoluten Modus

1 **Wenn Sie nicht der Eigentümer der Datei oder des Verzeichnisses sind, melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Nur der aktuelle Eigentümer oder der Superuser kann die Berechtigungen für eine Datei oder ein Verzeichnis mit dem Befehl `chmod` ändern.

2 **Ändern Sie die Berechtigungen im absoluten Modus.**

`% chmod` *nnn filename*

nnn Gibt die Oktalwerte an, die den Berechtigungen des Dateieigentümers, der Dateigruppe und der anderen Benutzer (in dieser Reihenfolge) entspricht. Eine Liste der gültigen Oktalwerte finden Sie in Tabelle 6–4.

filename Gibt die Datei oder das Verzeichnis an.

Hinweis – Wenn Sie mit dem Befehl `chmod` die Dateigruppenberechtigungen für eine Datei mit ACL-Einträgen ändern, werden sowohl die Dateigruppenberechtigungen als auch die ACL-Maske an die neuen Dateigruppenberechtigungen angepasst. Beachten Sie, dass die neuen ACL-Maskenberechtigungen die Berechtigungen für andere Benutzer und Gruppen ändern können, die über ACL-Einträge für die Datei verfügen. Stellen Sie mit dem Befehl `getfacl` sicher, dass geeignete Berechtigungen für alle ACL-Einträge eingestellt sind. Weitere Informationen finden Sie auf der Manpage `getfacl(1)`.

---

3 **Überprüfen Sie, ob die Berechtigungen für die Datei geändert wurden.**

`% ls -l` *filename*

Beispiel 6–4 Ändern der Berechtigungen im absoluten Modus

In dem folgenden Beispiel werden die Berechtigungen für ein öffentliches Verzeichnis von 744 (Lesen, Schreiben, Ausführen; nur Lesen; und nur Lesen) in 755 (Lesen, Schreiben, Ausführen; Lesen und Ausführen; und Lesen und Ausführen) geändert.

```
# ls -ld public_dir
drwxr--r--  1 jdoe   staff    6023 Aug  5 12:06 public_dir
# chmod 755 public_dir
# ls -ld public_dir
drwxr-xr-x  1 jdoe   staff    6023 Aug  5 12:06 public_dir
```

In dem folgenden Beispiel werden die Berechtigungen für ein ausführbares Shell-Skript von Lesen und Schreiben in Lesen, Schreiben und Ausführen geändert.

```
% ls -l my_script
-rw------- 1 jdoe   staff    6023 Aug  5 12:06 my_script
% chmod 700 my_script
% ls -l my_script
-rwx------ 1 jdoe   staff    6023 Aug  5 12:06 my_script
```

▼ So ändern Sie besondere Dateiberechtigungen im absoluten Modus

1 Wenn Sie nicht der Eigentümer der Datei oder des Verzeichnisses sind, melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Nur der aktuelle Eigentümer oder ein Benutzer mit Superuser-Rechten kann die besonderen Berechtigungen für eine Datei oder ein Verzeichnis mit dem Befehl `chmod` ändern.

2 Ändern Sie besondere Berechtigungen im absoluten Modus.

`% chmod` *nnnn filename*

nnnn Gibt die Oktalwerte an, mit denen die Berechtigungen für die Datei oder das Verzeichnis geändert werden. Der am weitesten links befindliche Oktalwert stellt die besonderen Berechtigungen für die Datei ein. Eine Liste der gültigen Oktalwerte für besondere Berechtigungen finden Sie in Tabelle 6–6.

filename Gibt die Datei oder das Verzeichnis an.

Hinweis – Wenn Sie mit dem Befehl `chmod` die Dateigruppenberechtigungen für eine Datei mit ACL-Einträgen ändern, werden sowohl die Dateigruppenberechtigungen als auch die ACL-Maske an die neuen Dateigruppenberechtigungen angepasst. Beachten Sie, dass die neuen ACL-Maskenberechtigungen die Berechtigungen für weitere Benutzer und Gruppen ändern können, die über ACL-Einträge für die Datei verfügen. Stellen Sie mit dem Befehl `getfacl` sicher, dass geeignete Berechtigungen für alle ACL-Einträge eingestellt sind. Weitere Informationen finden Sie auf der Manpage `getfacl(1)`.

---

3 Überprüfen Sie, ob die Berechtigungen für die Datei geändert wurden.

`% ls -l` *filename*

Beispiel 6–5 Einstellen der Dateiberechtigungen im absoluten Modus

In dem folgenden Beispiel ist die `setuid`-Berechtigung für die Datei `dbprog` eingestellt.

```
# chmod 4555 dbprog
# ls -l dbprog
-r-sr-xr-x   1 db     staff        12095 May  6 09:29 dbprog
```

In dem folgenden Beispiel ist die `setgid`-Berechtigung für die Datei `dbprog2` eingestellt.

```
# chmod 2551 dbprog2
# ls -l dbprog2
-r-xr-s--x   1 db     staff       24576 May  6 09:30 dbprog2
```

In dem folgenden Beispiel wird die Sticky Bit-Berechtigung für das Verzeichnis `public_dir` eingestellt.

```
# chmod 1777 public_dir
# ls -ld public_dir
drwxrwxrwt   2 jdoe   staff          512 May 15 15:27 public_dir
```

Schützen von UFS-Dateien mit ACLs (Übersicht der Schritte)

In der folgenden Übersicht der Schritte wird auf Verfahren verwiesen, mit denen die ACLs für eine UFS-Datei aufgelistet, geändert und in eine andere Datei kopiert werden können.

Aufgabe	Anweisungen
Feststellen, ob eine Datei über eine ACL verfügt	„So stellen Sie fest, ob eine Datei über eine ACL verfügt“ auf Seite 149
Hinzufügen einer ACL zu einer Datei	„So fügen Sie einer Datei ACL-Einträge hinzu“ auf Seite 150
Kopieren einer ACL	„So kopieren Sie eine ACL“ auf Seite 152
Ändern einer ACL	„So ändern Sie die ACL-Einträge für eine Datei“ auf Seite 152
Entfernen von ACLs aus einer Datei	„So löschen Sie ACL-Einträge aus einer Datei“ auf Seite 153
Anzeigen der ACLs für eine Datei	„So zeigen Sie ACL-Einträge für eine Datei an“ auf Seite 153

▼ So stellen Sie fest, ob eine Datei über eine ACL verfügt

- **Prüfen Sie, ob eine Datei über eine ACL verfügt.**

  `% ls -l` *filename*

  Ersetzen Sie *filename* durch die Datei oder das Verzeichnis.

  In der Ausgabe gibt ein Pluszeichen (+) rechts neben dem Modusfeld an, dass die Datei über eine ACL verfügt.

Hinweis – Wenn Sie keine ACL-Einträge zur Erweiterung der UNIX-Dateiberechtigungen hinzugefügt haben, wird angenommen, dass eine Datei über eine einfache ACL verfügt und das Pluszeichen (+) wird nicht angezeigt.

Beispiel 6–6 Prüfen, ob eine Datei über eine ACL verfügt

In dem folgenden Beispiel verfügt die Datei `ch1.sgm` über eine ACL. Die ACL wird durch das Pluszeichen (+) rechts neben dem Modusfeld gekennzeichnet.

```
% ls -l ch1.sgm
-rwxr-----+  1 stacey   techpubs      167 Nov 11 11:13 ch1.sgm
```

▼ So fügen Sie einer Datei ACL-Einträge hinzu

1 Stellen Sie mit dem Befehl `setfacl` eine ACL für eine Datei ein.

`% setfacl -s user::`*perms*`,group::`*perms*`,other:`*perms*`,mask:`*perms*`,`*acl-entry-list* *filename ...*

`-s`	Stellt eine ACL für eine Datei ein. Wenn bereits eine ACL vorhanden ist, wird sie ersetzt. Diese Option erfordert mindestens die Einträge `user::`, `group::` und `other::`.
`user::`*perms*	Gibt die Dateieigentümer-Berechtigungen an
`group::`*perms*	Gibt die Gruppeneigentümer-Berechtigungen an
`other:`*perms*	Gibt die Berechtigungen für andere Benutzer als den Dateieigentümer oder die Mitglieder der Dateigruppe an
`mask:`*perms*	Gibt die Berechtigungen für die ACL-Maske an Die Maske gibt die maximalen Berechtigungen an, die für Benutzer (andere als der Eigentümer) und für Gruppen gewährt werden können.
acl-entry-list	Gibt eine Liste von ACL-Einträgen an, die für bestimmte Benutzer oder Gruppen für die Datei oder das Verzeichnis eingestellt werden sollen. Sie können auch die Standard-ACL-Einträge für ein Verzeichnis einstellen: Tabelle 6–7 und Tabelle 6–8 enthalten gültige ACL-Einträge.
filename ...	Gibt eine oder mehrere Dateien oder Verzeichnisse an, für die die ACL eingestellt wird. Mehrere Dateinamen werden durch Leerzeichen getrennt.

Achtung – Wenn in der Datei bereits eine ACL vorhanden ist, ersetzt die Option `-s` die gesamte ACL durch die neue ACL.

Weitere Informationen finden Sie auf der Manpage `setfacl(1)`.

2. **Überprüfen Sie, ob die ACL-Einträge für die Datei eingestellt wurden.**

   ```
   % getfacl filename
   ```

   Informationen finden Sie unter „So stellen Sie fest, ob eine Datei über eine ACL verfügt“ auf Seite 149.

Beispiel 6–7 Einstellen einer ACL für eine Datei

In dem nachstehenden Beispiel werden folgende Berechtigungen für die Datei `ch1.sgm` eingestellt: Der Eigentümer der Datei ist zum Lesen und Schreiben und die Gruppe zum Lesen berechtigt, während andere Benutzer über keine Berechtigungen verfügen. Außerdem erhält der Benutzer `anusha` Lese- und Schreibberechtigungen für die Datei. Die Ach-Maskenberechtigungen werden auf Lesen und Schreiben eingestellt, d. h. dass kein Benutzer und keine Gruppe über Ausführungsberechtigungen verfügt.

```
% setfacl -s user::rw-,group::r--,other:---,mask:rw-,user:anusha:rw- ch1.sgm
% ls -l
total 124
-rw-r-----+  1 stacey  techpubs   34816 Nov 11 14:16 ch1.sgm
-rw-r--r--   1 stacey  techpubs   20167 Nov 11 14:16 ch2.sgm
-rw-r--r--   1 stacey  techpubs    8192 Nov 11 14:16 notes
% getfacl ch1.sgm
# file: ch1.sgm
# owner: stacey
# group: techpubs
user::rw-
user:anusha:rw-    #effective:rw-
group::r--         #effective:r--
mask:rw-
other:---
```

In dem nachstehenden Beispiel werden folgende Berechtigungen eingestellt: Der Eigentümer der Datei ist zum Lesen, Schreiben und Ausführen und die Gruppe zum Lesen berechtigt, während andere Benutzer über keine Berechtigungen verfügen. Außerdem werden die ACL-Maskenberechtigungen für die Datei `ch2.sgm` auf Lesen eingestellt. Zuletzt erhält noch der Benutzer `anusha` Lese- und Schreibberechtigungen. Aufgrund der ACL-Maske hat `anusha` jedoch nur eine Leseberechtigung.

```
% setfacl -s u::7,g::4,o:0,m:4,u:anusha:7 ch2.sgm
% getfacl ch2.sgm
# file: ch2.sgm
# owner: stacey
# group: techpubs
user::rwx
user:anusha:rwx         #effective:r--
group::r--              #effective:r--
mask:r--
other:---
```

▼ So kopieren Sie eine ACL

- **Kopieren Sie die ACL einer Datei in eine andere Datei durch Umleiten der `getfacl`-Ausgabe.**

  ```
  % getfacl filename1 | setfacl -f - filename2
  ```

  filename1 Gibt die Datei an, von der die ACL kopiert werden soll

  filename2 Gibt die Datei an, für die die kopierte ACL eingestellt werden soll

Beispiel 6–8 Kopieren einer ACL

In dem folgenden Beispiel wird eine ACL von `ch2.sgm` in `ch3.sgm` kopiert.

```
% getfacl ch2.sgm | setfacl -f - ch3.sgm
```

▼ So ändern Sie die ACL-Einträge für eine Datei

1. **Ändern Sie die ACL-Einträge für eine Datei mit dem Befehl `setfacl`.**

   ```
   % setfacl -m acl-entry-list filename ...
   ```

   `-m` Ändert den vorhandenen ACL-Eintrag

   acl-entry-list Gibt eine Liste mit mindestens einem ACL-Eintrag an, um die Datei oder das Verzeichnis zu ändern. Sie können auch die Standard-ACL-Einträge für ein Verzeichnis ändern. Tabelle 6–7 und Tabelle 6–8 enthalten die gültigen ACL-Einträge.

   filename ... Gibt eine oder mehrere Dateien oder Verzeichnisse an, die durch Leerzeichen getrennt werden.

2. **Überprüfen Sie, ob die ACL-Einträge für die Datei geändert wurden.**

   ```
   % getfacl filename
   ```

Beispiel 6–9 Ändern von ACL-Einträgen für eine Datei

In dem folgenden Beispiel werden die Berechtigungen für den Benutzer `anusha` in Lese- und Schreibberechtigungen geändert.

```
% setfacl -m user:anusha:6 ch3.sgm
% getfacl ch3.sgm
# file: ch3.sgm
# owner: stacey
# group: techpubs
user::rw-
user::anusha:rw-        #effective:r--
group::r-               #effective:r--
```

```
mask:r--
other:r-
```

In dem folgenden Beispiel werden die Standardberechtigungen für die Gruppe `staff` im Verzeichnis `book` in Leseberechtigungen geändert. Außerdem werden die Standard-ACL-Maskenberechtigungen in Lese- und Schreibberechtigungen geändert.

```
% setfacl -m default:group:staff:4,default:mask:6 book
```

▼ So löschen Sie ACL-Einträge aus einer Datei

1 Löschen Sie ACL-Einträge aus einer Datei.

`% setfacl -d` *acl-entry-list filename ...*

`-d`	Löscht die angegebenen ACL-Einträge
acl-entry-list	Gibt eine Liste von ACL-Einträgen an (ohne die Berechtigungen festzulegen), die aus der Datei oder dem Verzeichnis gelöscht werden sollen. Sie können nur ACL-Einträge und Standard-ACL-Einträge für bestimmte Benutzer und Gruppen löschen. Tabelle 6–7 und Tabelle 6–8 enthalten die gültigen ACL-Einträge.
filename ...	Gibt eine oder mehrere Dateien oder Verzeichnisse an, die durch Leerzeichen getrennt werden.

Alternativ können Sie mit dem Befehl `setfacl -s` alle ACL-Einträge für eine Datei löschen und durch die neuen ACL-Einträge ersetzen.

2 Überprüfen Sie, ob die ACL-Einträge aus der Datei gelöscht wurden.

`% getfacl` *filename*

Beispiel 6–10 Löschen von ACL-Einträgen aus einer Datei

In dem folgenden Beispiel wird der Benutzer `anusha` aus der Datei `ch4.sgm` gelöscht.

```
% setfacl -d user:anusha ch4.sgm
```

▼ So zeigen Sie ACL-Einträge für eine Datei an

- **Zeigen Sie ACL-Einträge für eine Datei mit dem Befehl `getfacl` an.**

`% getfacl [-a | -d]` *filename ...*

`-a`	Zeigt den Dateinamen, den Dateieigentümer, die Dateigruppe und die ACL-Einträge für die angegebene Datei oder das Verzeichnis an.

`-d` Zeigt den Dateinamen, den Dateieigentümer und die Standard-ACL-Einträge, falls vorhanden, für das angegebene Verzeichnis an.

filename ... Gibt eine oder mehrere Dateien oder Verzeichnisse an, die durch Leerzeichen getrennt werden.

Wenn Sie mehrere Dateinamen auf der Befehlszeile angeben, werden die einzelnen ACL-Einträge durch jeweils eine Leerzeile getrennt.

Beispiel 6–11 Anzeigen von ACL-Einträgen für eine Datei

In dem folgenden Beispiel werden alle ACL-Einträge für die Datei `ch1.sgm` angezeigt. Der Hinweis `#effective:` neben Benutzer- und Gruppeneinträgen gibt die Berechtigungen nach der Änderung durch die ACL-Maske an.

```
% getfacl ch1.sgm

# file: ch1.sgm
# owner: stacey
# group: techpubs
user::rw-
user:anusha:r-        #effective:r--
group::rw-            #effective:rw-
mask:rw-
other:---
```

In dem folgenden Beispiel werden die Standard-ACL-Einträge für das Verzeichnis `book` angezeigt.

```
% getfacl -d book

# file: book
# owner: stacey
# group: techpubs
user::rwx
user:anusha:r-x       #effective:r-x
group::rwx            #effective:rwx
mask:rwx
other:---
default:user::rw-
default:user:anusha:r--
default:group::rw-
default:mask:rw-
default:other:---
```

Schützen vor Programmen mit Sicherheitsrisiko (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf Verfahren, mit denen gefährliche ausführbare Dateien im System gesucht werden können und die Programme daran hindern, einen ausführbaren Stack zu nutzen.

Aufgabe	Description (Beschreibung)	Anweisungen
Suchen von Dateien mit besonderen Berechtigungen	Sucht Dateien, für die das `setuid`-Bit eingestellt ist, die jedoch nicht dem `root`-Benutzer gehören	„So suchen Sie Dateien mit besonderen Dateiberechtigungen“ auf Seite 155
Verhindern eines Überlaufs des ausführbaren Stack	Hindert Programme an der Nutzung eines ausführbaren Stack	„So hindern Sie Programme an der Verwendung ausführbarer Stacks“ auf Seite 156
Verhindern der Protokollierung ausführbarer Stack-Meldungen	Deaktiviert die Protokollierung ausführbarer Stack-Meldungen	Beispiel 6–13

▼ So suchen Sie Dateien mit besonderen Dateiberechtigungen

Überwachen Sie Ihr System auf nicht autorisierte Verwendung von `setuid`- und `setgid`-Berechtigungen für Programme. Mit `setuid`- und `setgid`-Berechtigungen können normale Benutzer Superuser-Rechte erhalten. Eine verdächtige ausführbare Datei weist einem Benutzer statt `root` oder `bin` die Eigentümerschaft zu.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Suchen Sie Dateien mit `setuid`-Berechtigungen, indem Sie den Befehl `find` verwenden.

```
# find directory -user root -perm -4000 -exec ls -ldb {} \; >/tmp/filename
```

`find` *directory*	Überprüft alle eingehängten Pfade, beginnend mit dem für *directory* angegebenen Verzeichnis; diese Pfade können root (`/`), `sys`, `bin` oder `mail` entsprechen
`-user root`	Zeigt nur die Dateien an, die Eigentum von `root` sind
`-perm -4000`	Zeigt nur Dateien an, deren Berechtigungen auf `4000` eingestellt sind
`-exec ls -ldb`	Zeigt die Ausgabe des Befehls `find` im Format `ls -ldb` an

`/tmp/`*filename* Datei, die das Ergebnis des Befehls `find` enthält

3 Zeigen Sie die Ergebnisse in `/tmp/`*filename* an.

```
# more /tmp/filename
```

Hintergrundinformationen zu `setuid`-Berechtigungen finden Sie unter „`setuid`-Berechtigung“ auf Seite 134.

Beispiel 6–12 Suchen von Dateien mit `setuid`-Berechtigungen

Die Ausgabe des folgenden Beispiels zeigt, dass ein Benutzer der Gruppe `rar` eine persönliche Kopie von `/usr/bin/sh` erstellt und die Berechtigungen für `setuid` auf `root` eingestellt hat. Daher wird das Programm `/usr/rar/bin/sh` mit `root`-Berechtigungen ausgeführt.

Diese Ausgabe wurde für eine zukünftige Referenz gespeichert, indem das Verzeichnis `/var/tmp/chkprm` in das Verzeichnis `/export/sysreports/ckprm` verschoben wurde.

```
# find / -user root -perm -4000 -exec ls -ldb {} \; > /var/tmp/ckprm
# cat /var/tmp/ckprm
-r-sr-xr-x 1 root bin 38836 Aug 10 16:16 /usr/bin/at
-r-sr-xr-x 1 root bin 19812 Aug 10 16:16 /usr/bin/crontab
---s--x--x 1 root sys 46040 Aug 10 15:18 /usr/bin/ct
-r-sr-xr-x 1 root sys 12092 Aug 11 01:29 /usr/lib/mv_dir
-r-sr-sr-x 1 root bin 33208 Aug 10 15:55 /usr/lib/lpadmin
-r-sr-sr-x 1 root bin 38696 Aug 10 15:55 /usr/lib/lpsched
---s--x--- 1 root rar 45376 Aug 18 15:11 /usr/rar/bin/sh
-r-sr-xr-x 1 root bin 12524 Aug 11 01:27 /usr/bin/df
-rwsr-xr-x 1 root sys 21780 Aug 11 01:27 /usr/bin/newgrp
-r-sr-sr-x 1 root sys 23000 Aug 11 01:27 /usr/bin/passwd
-r-sr-xr-x 1 root sys 23824 Aug 11 01:27 /usr/bin/su
# mv /var/tmp/ckprm /export/sysreports/ckprm
```

▼ So hindern Sie Programme an der Verwendung ausführbarer Stacks

Eine Beschreibung der Sicherheitsrisiken ausführbarer Stacks finden Sie unter „Vermeiden von Sicherheitsrisiken in Verbindung mit ausführbaren Dateien“ auf Seite 141.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Fügen Sie der Datei `/etc/system` folgende Zeile hinzu:**

   ```
   set noexec_user_stack=1
   ```

3. **Starten Sie das System neu.**

   ```
   # init 6
   ```

Beispiel 6–13 Deaktivieren der Protokollierung ausführbarer Stack-Meldungen

In diesem Beispiel wird die Protokollierung ausführbarer Stack-Meldungen deaktiviert und das System neu gestartet.

```
# cat /etc/system
set noexec_user_stack=1
set noexec_user_stack_log=0
# init 6
```

◆ ◆ ◆ KAPITEL 7

Verwenden von Automated Security Enhancement Tool (Aufgaben)

In diesem Kapitel wird beschrieben, wie Sie mit ASET (Automated Security Enhancement Tool) den Zugriff auf Systemdateien und -verzeichnisse überwachen oder beschränken können.

Im Folgenden sind die schrittweisen Anleitungen in diesem Kapitel aufgeführt.

- „Automated Security Enhancement Tool (ASET)“ auf Seite 159
- „Ausführen von ASET (Übersicht der Schritte)“ auf Seite 178
- „Fehlerbehebung bei ASET-Problemen“ auf Seite 182

Wenn Sie ein umfangreicheres Tool als ASET benötigen, verwenden Sie das Oracle Solaris Security Toolkit. Das Oracle Solaris Security Toolkit bietet eine Grundstruktur zur Absicherung und Minimierung eines Oracle Solaris-Systems. Das Toolkit enthält ein Profilierungs-Tool, ein Berichterstellungs-Tool und eine Funktion zum Rückgängigmachen. Weitere Informationen finden Sie unter „Verwenden des Oracle Solaris Security Toolkit“ auf Seite 53.

Automated Security Enhancement Tool (ASET)

Im Lieferumfang von Oracle Solaris-Betriebssystem ist das Automated Security Enhancement Tool (ASET) enthalten. Mithilfe von ASET kann die Systemsicherheit überwacht und gesteuert werden, indem normalerweise manuell durchgeführte Aufgaben automatisiert werden.

Das ASET-Sicherheitspaket bietet automatische Verwaltungswerkzeuge, mit denen Sie die Sicherheit des Systems steuern und überwachen können. Sie geben eine Sicherheitsebene an, bei der ASET ausgeführt wird. Verfügbar sind die Sicherheitsebenen niedrig, mittel und hoch. Bei steigender Sicherheitsebene bietet ASET weitere Dateisteuerungsfunktionen, um den Dateizugriff einzuschränken und die Systemsicherheit zu erhöhen.

ASET führt sieben Aufgaben aus. Bei jeder Aufgabe werden bestimmte Prüfungen und Anpassungen an den Systemdateien durchgeführt. Durch die ASET-Aufgaben werden die Dateizugriffsrechte eingeschränkt, der Inhalt kritischer Systemdateien auf

Sicherheitsschwächen überprüft und wichtige Bereiche überwacht. Mit ASET können Sie außerdem ein Netzwerk schützen, indem Sie allgemeine Anforderungen eines Firewallsystems auf ein als Gatewaysystem dienendes System anwenden. Weitere Informationen erhalten Sie unter „Firewallkonfiguration“ auf Seite 163.

ASET verwendet Master-Dateien für die Konfiguration. Master-Dateien, Berichte und andere ASET-Dateien sind im Verzeichnis `/usr/aset` gespeichert. Diese Dateien können an die Anforderungen Ihres Standorts angepasst werden.

Durch jede Aufgabe wird ein Bericht generiert. Im Bericht sind die festgestellten Sicherheitsschwächen und alle durch die Aufgabe durchgeführten Änderungen an den Systemdateien aufgelistet. Beim Ausführen der höchsten Sicherheitsebene versucht ASET alle Systemsicherheitsschwächen zu lösen. Wenn ASET ein potenzielles Sicherheitsproblem nicht beheben kann, generiert ASET einen Bericht zum Fehler.

Sie können eine ASET-Sitzung durch den Befehl `/usr/aset/aset` interaktiv starten. Stattdessen können Sie angeben, dass ASET in regelmäßigen Abständen ausgeführt wird, indem Sie einen Eintrag in der Datei `crontab` hinzufügen.

Für ASET-Aufgaben wird viel Festplattenspeicher benötigt. Die Aufgaben können mit den normalerweise stattfindenden Aktivitäten in Konflikt treten. Um die Auswirkungen auf die Systemleistung so gering wie möglich zu halten, planen Sie die Ausführung von ASET bei niedriger Systemaktivität. Beispielsweise können Sie ASET alle 24 oder 48 Stunden um Mitternacht ausführen.

ASET-Sicherheitsebenen

Für die Ausführung von ASET können drei Sicherheitsebenen festgelegt werden: niedrig, mittel oder hoch. Bei steigender Sicherheitsebene bietet ASET weitere Dateisteuerungsfunktionen, um den Dateizugriff einzuschränken und die Systemsicherheit zu erhöhen. Diese Funktionen reichen von Überwachen der Systemsicherheit ohne Einschränkung des Dateizugriffs der Benutzer bis zu zunehmender Einschränkung der Zugriffsrechte, bis das System vollständig gesichert ist.

In der folgenden Tabelle werden diese drei Sicherheitsebenen aufgeführt.

Sicherheitsebene	Beschreibung
Niedrig	Stellt sicher, dass die Attribute der Systemdateien auf Standardversionswerte festgelegt sind. ASET führt verschiedene Prüfungen durch und generiert anschließend Berichte zu den potenziellen Sicherheitsschwächen. Auf dieser Ebene führt ASET keine Aktion durch, dadurch wirkt sich ASET nicht auf die Systemservices aus.

Sicherheitsebene	Beschreibung
Mittel	Bietet geeignete Sicherheitssteuerung für die meisten Umgebungen. Von ASET werden einige Einstellungen der Systemdateien und -parameter geändert. ASET beschränkt den Systemzugriff, um das Risiko von Sicherheitsangriffen zu verringern. ASET generiert Berichte zu Sicherheitsschwächen und die von ASET zur Zugriffsbeschränkung durchgeführten Änderungen. Auf dieser Ebene wirkt sich ASET nicht auf die Systemservices aus.
Hoch	Stellt ein im höchsten Maße sicheres System bereit. Von ASET werden viele Einstellungen der Systemdateien und -parameter auf minimale Zugriffsrechte gesetzt. Die meisten Systemanwendungen und -befehle können weiterhin normal verwendet werden. Auf dieser Ebene haben jedoch Sicherheitsbedenken Vorrang vor anderem Systemverhalten.

Hinweis – ASET ändert nicht die Berechtigungen einer Datei, um die Sicherheit der Datei herabzusetzen, es sei denn, Sie setzen die Sicherheitsebene herunter. Außerdem können Sie das System auf die Einstellungen zurücksetzen, die vor dem Ausführen von ASET vorhanden waren.

ASET-Aufgabenliste

In diesem Abschnitt wird beschrieben, welche Aufgaben von ASET durchgeführt werden. Sie sollten die Funktionsweise der einzelnen ASET-Aufgaben kennen. Indem Sie die Ziele von ASET, die von ASET durchgeführten Vorgänge und die von ASET betroffenen Systemkomponenten kennen, können Sie die Berichte effizient interpretieren und verwenden.

Die ASET-Berichtdateien enthalten Meldungen, in denen so genau wie möglich die während der einzelnen ASET-Aufgaben festgestellten Probleme beschrieben werden. Anhand dieser Meldungen können Sie diese Probleme diagnostizieren und beheben. Die Voraussetzung für eine erfolgreiche Verwendung von ASET ist, dass Sie über allgemeine Kenntnisse der Systemverwaltung und der Systemkomponenten verfügen. Wenn Sie noch über geringe Kenntnisse der Systemadministration verfügen, erhalten Sie weitere Informationen in der Dokumentation zur Systemadministration von Oracle Solaris. Lesen Sie beispielsweise die entsprechenden Handbuchseiten, um sich auf die ASET-Administration vorzubereiten.

Durch das Dienstprogramm `taskstat` werden die abgeschlossenen Aufgaben festgestellt. Außerdem erkennt das Dienstprogramm die noch ausgeführten Aufgaben. Durch eine abgeschlossene Aufgabe wird eine Berichtdatei generiert. Eine ausführliche Beschreibung des Dienstprogramms `taskstat` erhalten Sie unter `taskstat(1M)`.

Optimierung der Systemdateienberechtigungen

Durch diese Aufgabe werden die Berechtigungen der Systemdateien auf die von Ihnen angegebene Sicherheitsebene festgelegt. Diese Aufgabe wird bei der Installation des Systems ausgeführt. Wenn Sie zu einem späteren Zeitpunkt die festgelegten Ebenen ändern möchten,

führen Sie diese Aufgabe erneut aus. Bei niedriger Sicherheitsebene werden die Berechtigungen auf Werte gesetzt, die für eine Umgebung mit offenem Informationsaustausch geeignet sind. Bei mittlerer Sicherheitsebene werden die Berechtigungen eingeschränkt, um eine für die meisten Umgebungen geeignete Sicherheit zu bieten. Bei hoher Sicherheitsebene werden die Berechtigungen eingeschränkt, um den Zugriff erheblich einzuschränken.

Alle durch diese Aufgabe durchgeführten Änderungen an Systemdateienberechtigungen oder Parametereinstellungen werden in der Datei `tune.rpt` protokolliert. Ein Beispiel der Dateien, die ASET beim Festlegen der Berechtigungen abfragt, finden Sie unter „Beispiele für tune-Dateien“ auf Seite 176.

Prüfungen der Systemdateien

Durch diese Aufgabe werden Systemdateien untersucht und jede Datei mit einer Beschreibung dieser Datei in einer Master-Datei verglichen. Die Master-Datei wird erstellt, wenn ASET diese Aufgabe erstmalig ausführt. Die Master-Datei enthält die Systemdateieinstellungen, die von `checklist` für die angegebene Sicherheitsebene durchgesetzt werden.

Eine Liste der Verzeichnisse, dessen Dateien überprüft werden sollen, wird für jede Sicherheitsebene definiert. Sie können die Standardliste verwenden oder die Liste durch die Angabe unterschiedlicher Verzeichnisse für jede Ebene ändern.

Für jede Datei werden die folgenden Kriterien überprüft:

- Eigentümer oder Gruppe
- Berechtigungsbits
- Größe und Prüfsumme
- Anzahl der Verknüpfungen
- Zeit der letzten Änderung

Alle von ASET festgestellten Unstimmigkeiten werden in der Datei `cklist.rpt` protokolliert. Diese Datei enthält die Ergebnisse des Vergleichs der Systemdateigröße, Berechtigung und Prüfsummenwerte mit der Master-Datei.

Prüfungen der Benutzer und Gruppen

Diese Aufgabe prüft Benutzerkonten und Gruppen auf Einheitlichkeit und Integrität. Die Aufgabe verwendet die Definitionen in den Dateien `passwd` und `group`. Diese Aufgabe prüft die lokalen und NIS- bzw. NIS+-Passwortdateien. Die Probleme bei Passwortdateien für NIS+ werden gemeldet, aber nicht behoben.

Diese Aufgabe führt eine Prüfung auf die folgenden Verletzungen durch:

- Doppelte Namen oder IDs
- Einträge im falschen Format
- Konten ohne Passwort
- Ungültige Anmeldeverzeichnisse

- Konto `nobody`
- Leeres Gruppenpasswort
- Pluszeichen (+) in der Datei `/etc/passwd` auf einem NIS- bzw. NIS+-Server

Unstimmigkeiten werden in der Datei `usrgrp.rpt` protokolliert.

Prüfung der Systemkonfigurationsdateien

Während dieser Aufgabe prüft ASET verschiedene Systemtabellen, die sich hauptsächlich im Verzeichnis `/etc` befinden.

Dabei handelt es sich um folgende Dateien:

- `/etc/default/login`
- `/etc/hosts.equiv`
- `/etc/inetd.conf`
- `/etc/aliases`
- `/var/adm/utmpx`
- `/.rhosts`
- `/etc/vfstab`
- `/etc/dfs/dfstab`
- `/etc/ftpd/ftpusers`

ASET führt verschiedene Prüfungen und Änderungen an diesen Dateien durch. Von ASET werden Probleme in der Datei `sysconf.rpt` protokolliert.

Prüfung der Umgebungsvariablen

In dieser Aufgabe wird überprüft, wie die Umgebungsvariablen `PATH` und `UMASK` für Root- und andere Benutzer festgelegt werden. Die Aufgabe prüft die Dateien `/.profile`, `/.login` und `/.cshrc`.

Die Ergebnisse der Sicherheitsprüfung der Umgebung werden in der Datei `env.rpt` protokolliert.

`eeprom`-Prüfung

Diese Aufgabe prüft den Wert des Sicherheitsparameters `eeprom`, um sicherzustellen, dass für den Parameter die geeignete Sicherheitsebene festgelegt ist. Sie können den Sicherheitsparameter `eeprom` auf `none`, `command` oder `full` festlegen.

ASET ändert diese Einstellung nicht, die empfohlenen Änderungen werden jedoch in der Datei `eeprom.rpt` gespeichert.

Firewallkonfiguration

Durch diese Aufgabe wird sichergestellt, dass das System als ein Netzwerk-Relay sicher verwendet werden kann. Durch diese Aufgabe wird ein internes Netzwerk vor externen öffentlichen Netzwerken geschützt, indem ein dediziertes System als eine Firewall eingerichtet

wird (siehe Beschreibung unter „Firewall-Systeme“ auf Seite 60). Das Firewallsystem erstellt zwei getrennte Netzwerke. In diesem Fall erfolgt der Zugriff zwischen den Netzwerken über eine nicht vertrauenswürdige Verbindung. Die Aufgabe der Firewallkonfiguration deaktiviert die Weiterleitung von IP-Paketen (Internet Protocol). Außerdem blendet die Firewall Routing-Informationen vom externen Netzwerk aus.

Die Firewallaufgabe wird auf allen Sicherheitsebenen ausgeführt, jedoch werden Aktionen nur auf der höchsten Ebene durchgeführt. Wenn Sie ASET mit der höchsten Sicherheitsebene ausführen möchten, jedoch keinen Firewallschutz für das System benötigen, können Sie die Firewallaufgabe entfernen. Die Aufgabe können Sie durch Bearbeiten der Datei `asetenv` entfernen.

Alle durchgeführten Änderungen werden in der Datei `firewall.rpt` protokolliert.

ASET-Ausführungsprotokoll

ASET generiert ein Ausführungsprotokoll, unabhängig davon, ob ASET interaktiv oder im Hintergrund ausgeführt wird. Standardmäßig generiert ASET die Protokolldatei bei der Standardausgabe. Im Ausführungsprotokoll wird bestätigt, dass ASET zu der festgelegten Zeit ausgeführt wurde. Es enthält ebenfalls Fehlermeldungen zur Ausführung. Durch den Befehl `aset -n` wird das Protokoll per E-Mail an den angegebenen Benutzer weitergeleitet. Eine vollständige Liste der ASET-Optionen erhalten Sie auf der Manpage `aset(1M)`.

Beispiel einer ASET-Ausführungsprotokolldatei

```
ASET running at security level low

Machine=example; Current time = 0325_08:00


aset: Using /usr/aset as working directory

Executing task list...
        firewall
        env
        sysconfig
        usrgrp
        tune
        cklist
        eeprom
All tasks executed. Some background tasks may still be running.

Run /usr/aset/util/taskstat to check their status:
     $/usr/aset/util/taskstat     aset_dir
Where aset_dir is ASET's operating directory, currently=/usr/aset

When the tasks complete, the reports can be found in:
     /usr/aset/reports/latest/*.rpt
You can view them by:
more /usr/aset/reports/latest/*.rpt
```

Im Ausführungsprotokoll werden zunächst das System und die Zeit der ASET-Ausführung angezeigt. Anschließend werden die einzelnen Aufgaben nach Startzeitpunkt aufgeführt.

ASET ruft einen im Hintergrund ausgeführten Prozess für diese Aufgaben auf, die unter „ASET-Aufgabenliste“ auf Seite 161 beschrieben sind. Die Aufgabe wird im Ausführungsprotokoll aufgeführt, wenn sie gestartet wird. Dabei wird nicht angegeben, ob die Aufgabe abgeschlossen wurde. Den Status der im Hintergrund ausgeführten Aufgaben können Sie prüfen, indem Sie den Befehl `taskstat` verwenden.

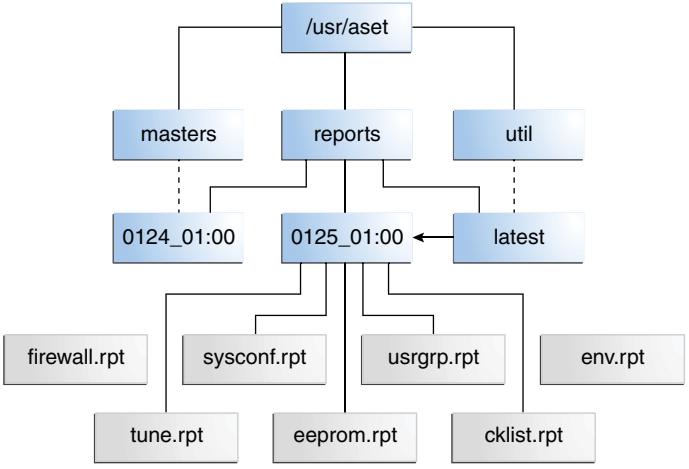
ASET-Berichte

Alle aus ASET-Aufgaben generierten Berichtdateien werden in Unterverzeichnissen des Verzeichnisses `/usr/aset/reports` gespeichert. Dieser Abschnitt enthält eine Beschreibung der Struktur des Verzeichnisses `/usr/aset/reports` und Richtlinien zur Verwaltung der Berichtdateien.

ASET speichert die Berichtdateien in Unterverzeichnissen, die mit der Uhrzeit und dem Datum der Berichtgenerierung benannt werden. Durch diese Konvention können Sie die den Systemstatus dokumentierenden Datensätze sortieren, da der Status je nach ASET-Ausführung unterschiedlich sein kann. Sie können diese Berichte überwachen und vergleichen, um den Sicherheitszustand des Systems festzustellen.

Die folgende Abbildung zeigt ein Beispiel der Struktur des Verzeichnisses `reports`.

ABBILDUNG 7–1 Struktur des ASET-Verzeichnisses `reports`



Dieses Beispiel zeigt zwei Unterverzeichnisse von Berichten.

- `0124_01:00`

- `0125_01:00`

Die Namen der Unterverzeichnisse geben das Datum und die Uhrzeit der Berichtgenerierung an. Die Namen der Berichtunterverzeichnisse weisen folgendes Format auf:

monthdate_hour:minute

month, *date*, *hour* und *minute* sind zweistellige Zahlen. Beispiel: `0125_01:00` steht für 25. Januar um 1 Uhr nachts.

Diese zwei Berichtunterverzeichnisse enthalten verschiedene Berichte, die aus einer Ausführung von ASET generiert wurden.

Das Verzeichnis `latest` ist eine symbolische Verknüpfung, die auf das Unterverzeichnis verweist, das die aktuellen Berichte enthält. Die aktuellen von ASET generierten Berichte finden Sie im Verzeichnis `/usr/aset/reports/latest`. Dieses Verzeichnis enthält eine Berichtdatei für jede Aufgabe, die ASET während der letzten Ausführung durchgeführt hat.

Format der ASET-Berichtdateien

Die Berichtdateien werden nach den Aufgaben benannt, die den Bericht generieren. In der folgenden Tabelle sind die Aufgaben und die zugehörigen Berichte aufgeführt.

TABELLE 7–1 ASET-Aufgaben und zugehörige Berichte

Aufgaben	Bericht
Optimierung der Systemdateienberechtigungen (`tune`)	`tune.rpt`
Prüfungen der Systemdateien (`cklist`)	`cklist.rpt`
Prüfungen der Benutzer und Gruppen (`usrgrp`)	`usrgrp.rpt`
Prüfung der Systemkonfigurationsdateien (`sysconf`)	`sysconf.rpt`
Prüfung der Umgebungsvariablen (`env`)	`env.rpt`
`eeprom`-Prüfung (`eeprom`)	`eeprom.rpt`
Firewallkonfiguration (`firewall`)	`firewall.rpt`

In den Berichtdateien sind die Meldungen am Anfang und Ende durch eine Banner-Zeile eingeschlossen. In einigen Fällen kann eine Aufgabe vorzeitig abgebrochen werden. Dies ist beispielsweise der Fall, wenn eine ASET-Komponente versehentlich entfernt oder beschädigt wurde. In diesen Fällen ist am Ende der Berichtdatei normalerweise eine Meldung enthalten, die den Grund für die vorzeitige Beendigung angibt.

Im Folgenden sehen Sie als Beispiel die Berichtdatei `usrgrp.rpt`.

```
*** Begin User and Group Checking ***

Checking /etc/passwd ...
Warning! Password file, line 10, no passwd
:sync::1:1::/:/bin/sync
..end user check; starting group check ...
Checking /etc/group...
*** End User And group Checking ***
```

Untersuchen von ASET-Berichtdateien

Wenn Sie ASET erstmalig ausführen oder erneut konfigurieren, untersuchen Sie sorgfältig die Berichtdateien. Bei einer Neukonfiguration werden die Datei `asetenv` oder die Master-Dateien im Unterverzeichnis `masters` oder die Sicherheitsebene für die ASET-Ausführung geändert.

Die Berichte enthalten alle Fehler, die bei der Neukonfiguration von ASET versehentlich eingegeben wurden. Indem Sie die Berichte sorgfältig untersuchen, können Sie beim Auftreten von Problemen auf diese reagieren oder sie lösen.

Vergleichen von ASET-Berichtdateien

Wenn Sie die Berichtdateien während eines Zeitraums überwachen, in dem keine Konfigurationsänderungen oder Systemaktualisierungen durchgeführt wurden, haben Sie möglicherweise den Eindruck, dass der Inhalt der Berichte gleich ist. Wenn die Berichte nur geringfügige Änderungen enthalten, können Sie mithilfe des Dienstprogramms `diff` die Berichte vergleichen.

ASET-Master-Dateien

Die ASET-Master-Dateien `tune.high`, `tune.low` , `tune.med` und `uid_aliases` sind im Verzeichnis `/usr/aset/masters` gespeichert. ASET definiert mithilfe der Master-Dateien die Sicherheitsebenen. Weitere Informationen erhalten Sie auf der Manpage `asetmasters(4)`.

tune-Dateien

Durch die Master-Dateien `tune.low`, `tune.med` und `tune.high` werden die verfügbaren ASET-Sicherheitsebenen definiert. Die Dateien geben die Attribute der Systemdateien auf jeder Ebene an und werden zu Vergleichs- und Referenzzwecken verwendet.

Datei `uid_aliases`

Die Datei `uid_aliases` enthält eine Liste mehrerer Benutzerkonten, die die gleiche Benutzer-ID (UID) aufweisen. Normalerweise gibt ASET eine Warnung zu mehreren Benutzerkonten aus, da dadurch die Verantwortlichkeit schwieriger festgestellt werden kann. Sie können Ausnahmen zu dieser Regel zulassen, indem Sie die Ausnahmen in der Datei `uid_aliases` angeben. ASET protokolliert keine Einträge in der Datei `passwd` mit doppelten UIDs, wenn diese Einträge in der Datei `uid_aliases` angegeben sind.

Versuchen Sie zu vermeiden, dass mehrere Benutzerkonten die gleiche UID verwenden. Verwenden Sie andere Methoden, um das gewünschte Ziel zu erreichen. Wenn beispielsweise verschiedene Benutzer einen Satz von Berechtigungen gemeinsam verwenden sollen, können Sie ein Gruppenkonto erstellen. Außerdem können Sie eine Rolle erstellen. Das gemeinsame Verwenden von UIDs sollte ausschließlich nur dann verwendet werden, wenn Sie mit den anderen Methoden das gewünschte Ziel nicht erreichen.

Mit der Umgebungsvariable `UID_ALIASES` können Sie eine alternative Aliase-Datei angeben. Die Standarddatei lautet `/usr/aset/masters/uid_aliases`.

Checklisten-Dateien

Die Master-Dateien, die von den Prüfungen der Systemdateien verwendet werden, werden beim erstmaligen Ausführen von ASET generiert. Die Master-Dateien werden ebenfalls generiert, wenn Sie ASET nach dem Ändern der Sicherheitsebene ausführen.

Die folgenden Umgebungsvariablen definieren die Dateien, die von dieser Aufgabe geprüft werden:

- `CKLISTPATH_LOW`
- `CKLISTPATH_MED`
- `CKLISTPATH_HIGH`

ASET-Umgebungsdatei (`asetenv`)

Die Umgebungsdatei `asetenv` enthält eine Liste der Umgebungsvariablen, die sich auf ASET-Aufgaben auswirken. Einige dieser Variablen können geändert werden, um die ASET-Ausführung anzupassen. Weitere Informationen zur Datei `asetenv` erhalten Sie unter `asetenv(4)`.

Konfigurieren von ASET

In diesem Abschnitt wird die Konfiguration von ASET beschrieben. Außerdem wird die Umgebung für die Ausführung von ASET beschrieben.

ASET erfordert nur eine geringfügige Verwaltung und Konfiguration. In den meisten Fällen können Sie ASET mit den Standardwerten ausführen. Jedoch können Sie einige der Parameter, die sich auf die Ausführung und das Verhalten von ASET auswirken, einstellen, um die Leistung zu optimieren. Vor dem Ändern der Standardwerte sollten Sie verstehen, wie ASET funktioniert und sich auf die Systemkomponenten auswirkt.

ASET verwendet vier Konfigurationsdateien, um das Verhalten der Aufgaben zu steuern:

- `/usr/aset/asetenv`
- `/usr/aset/masters/tune.low`
- `/usr/aset/masters/tune.med`
- `/usr/aset/masters/tune.high`

Ändern der Umgebungsdatei (`asetenv`)

Die Datei `/usr/aset/asetenv` ist in zwei Abschnitte unterteilt:

- Einen Abschnitt mit benutzerkonfigurierbaren Umgebungsvariablen
- Einen Abschnitt mit internen Umgebungsvariablen

Den Abschnitt mit benutzerkonfigurierbaren Parametern können Sie bearbeiten. Die Einstellungen im Abschnitt mit internen Umgebungsvariablen sind jedoch nur für die interne Verwendung. Ändern Sie diese Einstellungen nicht.

Gehen Sie wie folgt vor, um die Einträge im Abschnitt mit benutzerkonfigurierbaren Variablen zu bearbeiten:

- Wählen Sie die auszuführenden Aufgaben.
- Geben Sie die Verzeichnisse für die Aufgabe der Prüfung der Systemdateien an.
- Planen Sie die ASET-Ausführung.
- Geben Sie eine UID-Aliase-Datei an.
- Erweitern Sie die Prüfungen auf die NIS+-Tabellen.

Auswählen der auszuführenden Aufgaben: `TASKS`

Jede von ASET ausgeführte Aufgaben überwacht einen bestimmten Bereich der Systemsicherheit. In den meisten Systemumgebungen sind alle Aufgaben erforderlich, um die Sicherheit entsprechend zu gewährleisten. Sie können jedoch eine oder mehrere Aufgaben entfernen.

Beispielsweise wird die Firewallaufgabe auf allen Sicherheitsebenen ausgeführt, jedoch werden Aktionen nur auf der hohen Sicherheitsebene durchgeführt. Möglicherweise möchten Sie ASET auf der hohen Sicherheitsebene ausführen, benötigen jedoch keinen Firewallschutz.

Sie können ASET so einrichten, dass das Programm auf der hohen Sicherheitsebene ohne die Firewallfunktion ausgeführt wird. Bearbeiten Sie dazu die `TASKS`-Liste der Umgebungsvariablen in der Datei `asetenv`. Die `TASKS`-Liste enthält standardmäßig alle ASET-Aufgaben. Sie können eine Aufgabe entfernen, indem Sie die aufgabenbezogene Umgebungsvariable aus der Datei löschen. Löschen Sie in diesem Fall die Umgebungsvariable `firewall` aus der Liste. Bei der nächsten Ausführung von ASET wird die entfernte Aufgabe nicht durchgeführt.

Im folgenden Beispiel wird die `TASKS`-Liste mit allen ASET-Aufgaben angezeigt.

```
TASKS=”env sysconfig usrgrp tune cklist eeprom firewall”
```

Angeben von Verzeichnissen für die Aufgabe der Prüfungen der Systemdateien: CKLISTPATH

Bei der Prüfung der Systemdateien werden die Attribute der Dateien in den ausgewählten Systemverzeichnissen überprüft. Sie können die zu überprüfenden Verzeichnisse angeben, indem Sie die folgenden Umgebungsvariablen verwenden.

Die Variable `CKLISTPATH_LOW` definiert die Verzeichnisse, die auf der niedrigen Sicherheitsebene überprüft werden. Die Umgebungsvariablen `CKLISTPATH_MED` und `CKLISTPATH_HIGH` werden auf ähnliche Weise für die mittlere und hohe Sicherheitsebene verwendet.

Die Verzeichnisliste, die von einer Umgebungsvariable auf der niedrigen Sicherheitsebene definiert wird, sollte ein untergeordneter Satz der Verzeichnisliste sein, die auf der nächsthöheren Ebene definiert wird. Beispielsweise müssen alle Verzeichnisse, die für `CKLISTPATH_LOW` angegeben werden, in `CKLISTPATH_MED` enthalten sein. Ebenso müssen alle Verzeichnisse, die für `CKLISTPATH_MED` angegeben werden, in `CKLISTPATH_HIGH` enthalten sein.

Die für diese Verzeichnisse durchgeführten Prüfungen sind nicht rekursiv. ASET prüft nur die Verzeichnisse, die explizit in der Umgebungsvariable aufgeführt sind. Es werden keine Unterverzeichnisse überprüft.

Sie können diese Umgebungsvariablendefinitionen bearbeiten, um Verzeichnisse hinzuzufügen oder zu entfernen, die von ASET überprüft werden sollen. Beachten Sie, dass diese Checklisten nur für Systemdateien geeignet sind, die nicht täglich geändert werden. Das Home-Verzeichnis eines Benutzers ist normalerweise zu dynamisch, um als Checkliste zu dienen.

Planen der ASET-Ausführung: PERIODIC_SCHEDULE

Sie können ASET interaktiv starten oder mit der Option `-p` die ASET-Aufgaben zu einer geplanten Zeit ausführen. Sie können ASET in regelmäßigen Abständen während einer geringen Systemauslastung ausführen. Beispielsweise wird `PERIODIC_SCHEDULE` von ASET abgefragt, um die Häufigkeit und den Zeitpunkt für die Ausführung von ASET-Aufgaben festzulegen. Ausführliche Anweisungen zum Einrichten der regelmäßigen Ausführung von ASET finden Sie unter „So führen Sie ASET in regelmäßigen Abständen aus“ auf Seite 180.

Das Format von `PERIODIC_SCHEDULE` entspricht dem Format der Einträge von `crontab`. Ausführliche Informationen erhalten Sie unter `crontab(1)`.

Angeben einer Aliase-Datei: UID_ALIASES

Die Variable `UID_ALIASES` gibt eine Aliase-Datei an, die gemeinsam genutzte UIDs enthält. Die Standarddatei lautet `/usr/aset/masters/uid_aliases`.

Erweitern der Prüfungen auf NIS+-Tabellen: YPCHECK

Die Umgebungsvariable YPCHECK gibt an, ob ASET auch Tabellen der Systemkonfigurationsdatei prüfen soll. YPCHECK ist eine boolesche Variable. Sie können für YPCHECK nur "true" oder "false" angeben. Der Standardwert ist "false", wodurch die Prüfung der NIS+-Tabelle deaktiviert wird.

Die Funktionsweise dieser Umgebungsvariable können Sie anhand der Datei passwd sehen. Bei der Einstellung "false" prüft ASET die lokale passwd-Datei. Bei der Einstellung "true" prüft die Aufgabe ebenfalls die passwd-Tabelle von NIS+ für die Domain des Systems.

Hinweis – Obwohl ASET die lokalen Dateien automatisch repariert, werden nur potenzielle Probleme in den NIS+-Tabellen protokolliert. Die Tabellen werden von ASET nicht geändert.

Ändern der tune-Dateien

ASET verwendet drei tune-Master-Dateien (tune.low, tune.med und tune.high), um den Zugriff auf kritische Systemdateien zuzulassen oder einzuschränken. Diese Master-Dateien sind im Verzeichnis /usr/aset/masters gespeichert. Sie können die Dateien an Ihre Umgebung anpassen. Beispiele dazu finden Sie unter „Beispiele für tune-Dateien“ auf Seite 176.

Durch die Datei tune.low werden Berechtigungen auf Werte gesetzt, die sich für die standardmäßigen Systemeinstellungen eignen. Durch die Datei tune.med werden diese Berechtigungen weiter eingeschränkt. Die Datei tune.med enthält ebenfalls Einträge, die nicht in der Datei tune.low enthalten sind. Die Datei tune.high schränkt die Berechtigungen weiter ein.

Hinweis – Ändern Sie die Einstellungen in den tune-Dateien, indem Sie Einträge hinzufügen oder entfernen. Für eine Berechtigung können nicht geringere Einschränkungen als die aktuelle Einstellung festgelegt werden. Durch die ASET-Aufgaben werden die Einschränkungen der Berechtigungen nur dann aufgehoben, wenn Sie für die Systemsicherheit eine niedrigere Ebene festlegen.

Wiederherstellen der von ASET geänderten Systemdateien

Wenn Sie ASET erstmalig ausführen, speichert und archiviert ASET die ursprünglichen Systemdateien. Durch das Dienstprogramm aset.restore werden diese Dateien wiederhergestellt. Außerdem hebt dieses Dienstprogramm die Ausführung von ASET auf, wenn die regelmäßige Ausführung von ASET derzeit geplant ist. Der Befehl aset.restore ist im ASET-Betriebsverzeichnis unter /usr/aset gespeichert.

Die an Systemdateien durchgeführten Änderungen gehen verloren, wenn Sie den Befehl aset.restore ausführen.

Verwenden Sie den Befehl `aset.restore` in den folgenden Fällen:

- Wenn Sie ASET-Änderungen entfernen und das ursprüngliche System wiederherstellen möchten

  Um ASET dauerhaft zu deaktivieren, können Sie ASET von der `cron`-Planung entfernen, wenn der Befehl `aset` zu `crontab` des Roots hinzugefügt wurde. Anweisungen dazu, wie Sie mit `cron` die automatische Ausführung beenden können, finden Sie unter „So halten Sie die regelmäßige Ausführung von ASET an“ auf Seite 180.
- Wenn Sie nach einer kurzzeitigen Verwendung von ASET den ursprünglichen Systemstatus wiederherstellen möchten
- Wenn eine wichtige Systemfunktion nicht ordnungsgemäß funktioniert und Sie vermuten, dass das Problem von ASET verursacht wird

Netzwerkbetrieb mit dem NFS-System

Normalerweise wird ASET im Standalone-Modus verwendet, auch wenn das System in einem Netzwerk vorhanden ist. Als Systemadministrator für das Standalone-System sind Sie für die Sicherheit des Systems zuständig. Daher sind Sie für die Ausführung und Verwaltung von ASET verantwortlich, um das System zu schützen.

Außerdem können Sie ASET in der verteilten NFS-Umgebung verwenden. Als Netzwerkadministrator sind Sie für die Installation, Ausführung und Verwaltung verschiedener administrativer Aufgaben für alle Clients verantwortlich. Um die ASET-Verwaltung auf mehreren Clientsystemen zu erleichtern, können Sie Konfigurationsänderungen durchführen, die auf alle Clients angewendet werden. Durch das globale Anwenden der Änderungen brauchen Sie sich nicht an jedem System anzumelden und die Konfigurationsänderungen erneut durchzuführen.

Beim Planen der Einrichtung von ASET auf Netzwerksystemen sollten Sie überlegen, von welchen Personen die Sicherheit kontrolliert werden soll. Beispielsweise können Sie festlegen, dass die Benutzer einige Sicherheitsfunktionen auf ihren Systemen kontrollieren. Oder Sie können eine zentrale Verantwortung für die Kontrolle der Sicherheit festlegen.

Globale Konfiguration für jede Sicherheitsebene

In einigen Fällen möchten Sie möglicherweise mehrere Netzwerkkonfigurationen einrichten. Beispielsweise möchten Sie eine Konfiguration für Clients einrichten, denen eine niedrige Sicherheitsebene zugewiesen ist. Oder Sie möchten eine andere Konfiguration für Clients mit mittlerer Sicherheitsebene und eine weitere Konfiguration für Clients mit einer hohen Sicherheitsebene einrichten.

Um eine separate ASET-Netzwerkkonfiguration für jede Sicherheitsebene zu erstellen, können Sie drei ASET-Konfigurationen auf dem Server erstellen. Sie erstellen eine Konfiguration für jede Ebene. Die einzelnen Konfigurationen können mit der entsprechenden Sicherheitsebene

auf die Clients exportiert werden. Einige ASET-Komponenten, die bei allen drei Konfigurationen verwendet werden, können durch Verknüpfungen gemeinsam verwendet werden.

Erfassen von ASET-Berichten

Sie können nicht nur die ASET-Komponenten auf einem Server zentral verwalten, sondern auch ein zentrales Verzeichnis auf einem Server einrichten, um alle ASET-Berichte zu erfassen. Der Zugriff auf den Server durch Clients erfolgt mit oder ohne Superuser-Berechtigungen. Anweisungen zum Einrichten einer Methode zur Erfassung finden Sie unter „So erfassen Sie ASET-Berichte auf einem Server“ auf Seite 181.

Durch Einrichten der Erfassung von Berichten auf einem Server können Sie die Berichte für alle Clients von einem Speicherort aufrufen. Diese Methode können Sie unabhängig davon verwenden, ob der Client über Superuser-Berechtigungen verfügt. Stattdessen können Sie auch das Verzeichnis "reports" im lokalen System verwenden, wenn die Benutzer ihre eigenen ASET-Berichte überprüfen sollen.

ASET-Umgebungsvariablen

Im Folgenden ist eine Liste der ASET-Umgebungsvariablen und der von den Variablen definierten Werte aufgeführt.

`ASETDIR`	Gibt das ASET-Arbeitsverzeichnis an
`ASETSECLEVEL`	Gibt die Sicherheitsebene an
`PERIODIC_SCHEDULE`	Gibt die Planung der regelmäßigen Ausführung an
`TASKS`	Gibt die auszuführenden ASET-Aufgaben an
`UID_ALIASES`	Gibt eine Aliase-Datei an
`YPCHECK`	Gibt an, ob Prüfungen auf NIS-Maps und NIS+-Tabellen erweitert werden sollen
`CKLISTPATH_LOW`	Ist die Verzeichnisliste für die niedrige Sicherheitsebene
`CKLISTPATH_MED`	Ist die Verzeichnisliste für die mittlere Sicherheitsebene
`CKLISTPATH_HIGH`	Ist die Verzeichnisliste für die hohe Sicherheitsebene

Die in den folgenden Abschnitten aufgeführten Umgebungsvariablen sind in der Datei `/usr/aset/asetenv` gespeichert. Die Variablen `ASETDIR` und `ASETSECLEVEL` sind optional. Die Variablen können nur über die Shell durch den Befehl `/usr/aset/aset` festgelegt werden. Die anderen Umgebungsvariablen können durch Bearbeiten der Datei angegeben werden.

Umgebungsvariable ASETDIR

ASETDIR gibt ein ASET-Arbeitsverzeichnis an.

Geben Sie über die C-Shell Folgendes ein:

```
% setenv ASETDIR pathname
```

Geben Sie über die Bourne-Shell oder Korn-Shell Folgendes ein:

```
$ ASETDIR=pathname
$ export ASETDIR
```

Geben Sie für *pathname* den vollständigen Pfadnamen des ASET-Arbeitsverzeichnisses an.

Umgebungsvariable ASETSECLEVEL

Die Variable ASETSECLEVEL gibt eine Sicherheitsebene an, bei der ASET-Aufgaben ausgeführt werden.

Geben Sie über die C-Shell Folgendes ein:

```
% setenv ASETSECLEVEL level
```

Geben Sie über die Bourne-Shell oder Korn-Shell Folgendes ein:

```
$ ASETSECLEVEL=level
$ export ASETSECLEVEL
```

In diesen Befehlen können Sie für *level* einen der folgenden Werte festlegen:

`low` Niedrige Sicherheitsebene

`med` Mittlere Sicherheitsebene

`high` Hohe Sicherheitsebene

Umgebungsvariable PERIODIC_SCHEDULE

Der Wert von PERIODIC_SCHEDULE entspricht dem gleichen Format wie in der Datei `crontab`. Geben Sie für den Variablenwert eine Zeichenfolge aus fünf Feldern an, die in doppelten Anführungszeichen eingeschlossen ist, wobei jedes Feld durch ein Leerzeichen getrennt wird:

"*minutes hours day-of-month month day-of-week*"

minutes hours Gibt die Startzeit in Anzahl von Minuten (0-59) nach der Stunde und die Stunde (0-23) an

day-of-month Gibt den Tag des Monats für die ASET-Ausführung an; die Werte reichen von 1 bis 31

month Gibt den Monat des Jahres für die ASET-Ausführung an; die Werte reichen von 1 bis 12

day-of-week Gibt den Tag der Woche für die ASET-Ausführung an; die Werte reichen von 0 bis 6. Sonntag entspricht dem Wert 0.

Die folgenden Regeln gelten für die Erstellung der Planung einer regelmäßigen ASET-Ausführung:

- Sie können eine Liste der Werte, die durch ein Komma getrennt sind, für ein beliebiges Feld angeben.
- Sie können den Wert als eine Zahl oder einen Bereich angeben. Ein Bereich ist ein Zahlenpaar, das durch einen Bindestrich verbunden ist. Durch einen Bereich wird angegeben, dass die ASET-Aufgaben zu jedem im Bereich enthaltenen Zeitpunkt ausgeführt werden.
- Sie können ein Sternchen (*) als Wert für ein Feld angeben. Ein Sternchen kann alle möglichen Werte des Felds annehmen.

Durch den Standardeintrag für die Variable `PERIODIC_SCHEDULE` wird ASET täglich um 00:00 Mitternacht ausgeführt:

```
PERIODIC_SCHEDULE=”0 0 * * *”
```

Umgebungsvariable `TASKS`

Durch die Variable `TASKS` werden die von ASET durchgeführten Aufgaben aufgelistet. Standardmäßig werden alle sieben Aufgaben aufgeführt:

```
TASKS=”env sysconfig usrgrp tune cklist eeprom firewall”
```

Umgebungsvariable `UID_ALIASES`

Die Variable `UID_ALIASES` gibt eine Aliase-Datei an. Wenn diese Datei vorhanden ist, fragt ASET diese Datei nach einer Liste der zugelassenen mehrfachen Aliase ab. Das Format ist `UID_ALIASES=`*pathname*, wobei *pathname* für den vollständigen Pfadnamen der Aliase-Datei steht.

Der Standardwert lautet wie folgt:

```
UID_ALIASES=${ASETDIR}/masters/uid_aliases
```

Umgebungsvariable `YPCHECK`

Die Variable `YPCHECK` erweitert die Aufgabe der Prüfung von Systemtabellen auf die NIS- bzw. NIS+-Tabellen. Die Variable `YPCHECK` ist boolesch und kann entweder den Wert "true" oder "false" annehmen.

Der Standardwert lautet "false", wodurch nur lokale Systemtabellen überprüft werden:

```
YPCHECK=false
```

Umgebungsvariablen `CKLISTPATH_`*level*

Durch die drei Checklisten-Pfad-Variablen werden die Verzeichnisse aufgeführt, die von der Aufgabe der Prüfungen der Systemdateien überprüft werden. Die folgenden Definitionen der Variablen werden standardmäßig eingestellt. Die Definitionen zeigen die Beziehung zwischen den Variablen auf unterschiedlichen Ebenen:

```
CKLISTPATH_LOW=${ASETDIR}/tasks:${ASETDIR}/util:${ASETDIR}/masters:/etc
CKLISTPATH_MED=${CKLISTPATH_LOW}:/usr/bin:/usr/ucb
CKLISTPATH_HIGH=${CKLISTPATH_MED}:/usr/lib:/sbin:/usr/sbin:/usr/ucblib
```

Die Werte der Checklisten-Pfad-Umgebungsvariablen sind ähnlich wie die Werte der Shell-Pfad-Variablen. Ebenso wie die Shell-Pfad-Variablen sind die Checklisten-Pfad-Umgebungsvariablen Listen von Verzeichnisnamen. Die Verzeichnisnamen werden durch Doppelpunkte getrennt. Durch ein Gleichheitszeichen (=) können Sie den Variablennamen mit dem zugehörigen Wert verbinden.

Beispiele für ASET-Dateien

Dieser Abschnitt enthält Beispiele einiger ASET-Dateien, einschließlich tune-Dateien und der Aliase-Datei.

Beispiele für tune-Dateien

ASET verwaltet drei tune-Dateien. Jeder Eintrag in einer tune-Datei steht in einer Zeile. Die Felder in einem Eintrag sind in der folgenden Reihenfolge vorhanden:

pathname mode owner group type

pathname	Vollständiger Pfadname der Datei
mode	Fünfstellige Zahl für die Berechtigungseinstellung
owner	Eigentümer der Datei
group	Gruppeneigentümer der Datei
type	Typ der Datei

Beim Bearbeiten der tune-Dateien gelten folgende Regeln:

- Sie können die üblichen Platzhalterzeichen einer Shell, beispielsweise Sternchen (`*`) und Fragezeichen (`?`), für verschiedene Referenzzwecke im Pfadnamen verwenden. Weitere Informationen erhalten Sie unter `sh(1)`.
- *mode* steht für den Wert mit den wenigsten Einschränkungen. Wenn die aktuelle Einstellung mehr Einschränkungen aufweist als der angegebene Wert, werden die Berechtigungseinstellungen durch ASET nicht herabgesetzt. Wenn der angegebene Wert beispielsweise `00777` lautet, wird die Berechtigung nicht geändert, da `00777` immer weniger Einschränkungen aufweist als die aktuelle Einstellung.

  Dieser Vorgang legt fest, wie von ASET die Einstellung "mode" behandelt wird. Der Vorgang ändert sich, wenn die Sicherheitsebene herabgesetzt oder ASET entfernt wird. Wenn Sie eine geringere Sicherheitsebene als bei der letzten Ausführung verwenden oder die Systemdateien auf einen Status vor der ersten Ausführung von ASET zurücksetzen möchten, werden die von Ihnen durchgeführten Vorgänge von ASET erkannt und die Sicherheitsebene herabgesetzt.
- Verwenden Sie für *owner* und *group* Namen und nicht numerische IDs.
- Sie können ein Fragezeichen (`?`) anstatt *owner*, *group* und *type* verwenden, damit die vorhandenen Werte dieser Parameter von ASET nicht geändert werden.
- *type* kann entweder ein `symlink`, ein Verzeichnis oder eine Datei darstellen. Ein `symlink` ist ein symbolischer Link.
- Durch tune-Dateien mit höheren Sicherheitsebenen werden die Dateiberechtigungen auf mindestens die gleichen Einschränkungen wie die Dateiberechtigungen auf niedrigen Sicherheitsebenen zurückgesetzt. Bei höheren Sicherheitsebenen werden ebenfalls weitere Dateien zur Liste hinzugefügt.
- Eine Datei kann mehreren tune-Dateieinträgen entsprechen. Beispielsweise entspricht `etc/passwd` den Einträgen `etc/pass*` und `/etc/*`.
- Wenn zwei Einträge mit unterschiedlichen Berechtigungen vorhanden sind, wird die Dateiberechtigung auf den Wert mit der höchsten Einschränkung gesetzt. Im folgenden Beispiel wird die Berechtigung der Datei `/etc/passwd` auf den Wert `00755` gesetzt, der `00755` und `00770` weiter einschränkt.

  ```
  /etc/pass* 00755 ? ? file
  /etc/* 00770 ? ? file
  ```
- Wenn zwei Einträge unterschiedliche *owner*- oder *group*-Bezeichnungen aufweisen, hat der letzte Eintrag Vorrang. Im folgenden Beispiel wird der Eigentümer ("owner") von `/usr/sbin/chroot` auf `root` gesetzt.

  ```
  /usr/sbin/chroot 00555 bin bin file
  /usr/sbin/chroot 00555 root bin file
  ```

Beispiele für Aliase-Dateien

Die Aliase-Datei enthält eine Liste der Aliase, die die gleiche Benutzer-ID verwenden.

Die Einträge liegen im folgenden Format vor:

uid=alias1 =alias2=alias3 =. . .

uid Gemeinsam genutzte UID

aliasn Benutzerkonten, die die gleiche UID verwenden

Im folgenden Eintrag ist beispielsweise die UID `0` aufgeführt. Die UID wird von den Konten `sysadm` und `root` gemeinsam verwendet:

```
0=root=sysadm
```

Ausführen von ASET (Übersicht der Schritte)

Aufgabe	Beschreibung	Anweisungen
Ausführen von ASET über die Befehlszeile	Schützt das System auf der angegebenen ASET-Ebene. Zeigt das Ausführungsprotokoll an, um die Änderungen anzugeben	„So führen Sie ASET interaktiv aus“ auf Seite 178
Ausführen von ASET im Batch-Modus in regelmäßigen Abständen	Richtet einen cron-Job ein, um sicherzustellen, dass das System von ASET geschützt wird	„So führen Sie ASET in regelmäßigen Abständen aus“ auf Seite 180
Anhalten der Ausführung von ASET im Batch-Modus	Entfernt den cron-Job von ASET	„So halten Sie die regelmäßige Ausführung von ASET an“ auf Seite 180
Speichern von ASET-Berichten auf einem Server	Erfasst zu überwachende ASET-Berichte von Clients an einem zentralen Speicherort	„So erfassen Sie ASET-Berichte auf einem Server“ auf Seite 181

Weitere Informationen zum Festlegen von Variablen in ASET finden Sie unter „ASET-Umgebungsvariablen“ auf Seite 173. Weitere Informationen zu ASET erhalten Sie unter „Konfigurieren von ASET“ auf Seite 168.

▼ So führen Sie ASET interaktiv aus

1 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2 Führen Sie ASET interaktiv aus, indem Sie den Befehl `aset` verwenden.

```
# /usr/aset/aset -l level -d pathname
```

level Gibt die Sicherheitsebene an. Gültige Werte sind `low`, `medium` oder `high`. Der Standardwert ist `low`. Ausführliche Informationen zu Sicherheitsebenen finden Sie unter „ASET-Sicherheitsebenen“ auf Seite 160.

pathname Gibt das Arbeitsverzeichnis für ASET an. Der Standardwert ist `/usr/aset`.

3 Vergewissern Sie sich, dass ASET ausgeführt wird, indem Sie das auf dem Bildschirm angezeigte ASET-Ausführungsprotokoll aufrufen.

Die Meldung im Ausführungsprotokoll gibt an, welche Aufgaben ausgeführt werden.

Beispiel 7–1 Interaktives Ausführen von ASET

Im folgenden Beispiel wird ASET auf niedriger Sicherheitsebene im standardmäßigen Arbeitsverzeichnis ausgeführt.

```
# /usr/aset/aset -l low
======= ASET Execution Log =======

ASET running at security level low

Machine = jupiter; Current time = 0111_09:26

aset: Using /usr/aset as working directory

Executing task list ...
    firewall
    env
    sysconf
    usrgrp
    tune
    cklist
    eeprom

All tasks executed. Some background tasks may still be running.

Run /usr/aset/util/taskstat to check their status:
 /usr/aset/util/taskstat [aset_dir]

where aset_dir is ASET's operating
directory,currently=/usr/aset.

When the tasks complete, the reports can be found in:
 /usr/aset/reports/latest/*.rpt

You can view them by:
 more /usr/aset/reports/latest/*.rpt
```

▼ So führen Sie ASET in regelmäßigen Abständen aus

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2 **Geben Sie gegebenenfalls den Zeitpunkt für die regelmäßige Ausführung von ASET an.**

Führen Sie ASET aus, wenn die Systemauslastung gering ist. Mit der Umgebungsvariablen `PERIODIC_SCHEDULE` in der Datei `/usr/aset/asetenv` können Sie den Zeitpunkt für die regelmäßige Ausführung von ASET festlegen. Standardmäßig ist eine tägliche Ausführung um Mitternacht angegeben.

Wenn Sie einen anderen Zeitpunkt angeben möchten, bearbeiten Sie die Variable `PERIODIC_SCHEDULE` in der Datei `/usr/aset/asetenv`. Ausführliche Informationen zum Festlegen der Variable `PERIODIC_SCHEDULE` finden Sie unter „Umgebungsvariable `PERIODIC_SCHEDULE`“ auf Seite 174.

3 **Fügen Sie einen Eintrag zur Datei `crontab` hinzu, indem Sie den Befehl `aset` verwenden.**

```
# /usr/aset/aset -p
```

Durch die Option `-p` wird eine Zeile in die Datei `crontab` eingefügt, durch die ASET zu dem durch die Umgebungsvariable `PERIODIC_SCHEDULE` in der Datei `/usr/aset/asetenv` festgelegten Zeitpunkt ausgeführt wird.

4 **Überprüfen Sie durch den Eintrag `crontab` die geplante Ausführungszeit von ASET.**

```
# crontab -l root
```

▼ So halten Sie die regelmäßige Ausführung von ASET an

1 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Bearbeiten Sie die Datei `crontab`.**

```
# crontab -e root
```

3 **Entfernen Sie den ASET-Eintrag.**

4. **Speichern Sie die Änderungen und schließen Sie die Datei.**

5. **Überprüfen Sie durch den Eintrag `crontab`, dass der ASET-Eintrag entfernt ist.**

   ```
   # crontab -l root
   ```

▼ So erfassen Sie ASET-Berichte auf einem Server

1. **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

   Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Richten Sie ein Verzeichnis auf dem Server ein:**

   a. **Wechseln Sie in das Verzeichnis `/usr/aset`.**

      ```
      mars# cd /usr/aset
      ```

   b. **Erstellen Sie ein Verzeichnis *rptdir*.**

      ```
      mars# mkdir rptdir
      ```

   c. **Wechseln Sie in das Verzeichnis *rptdir* und erstellen Sie ein Verzeichnis *client_rpt*.**

      In diesem Schritt wird ein Unterverzeichnis *client_rpt* für einen Client erstellt. Wiederholen Sie diesen Schritt für die Clients, dessen Berichte Sie erfassen möchten.

      ```
      mars# cd rptdir
      mars# mkdir client_rpt
      ```

      Im folgenden Verzeichnis werden das Verzeichnis `all_reports` und die Unterverzeichnisse `pluto_rpt` und `neptune_rpt` erstellt.

      ```
      mars# cd /usr/aset
      mars# mkdir all_reports
      mars# cd all_reports
      mars# mkdir pluto_rpt
      mars# mkdir neptune_rpt
      ```

3. **Fügen Sie die Verzeichnisse *client_rpt* zur Datei `/etc/dfs/dfstab` hinzu.**

   Die Verzeichnisse sollten über Lese- und Schreibzugriff verfügen.

   Beispielsweise werden die folgenden Einträge in der Datei `dfstab` mit Lese- und Schreibberechtigung gemeinsam verwendet.

   ```
   share -F nfs -o rw=pluto /usr/aset/all_reports/pluto_rpt
   share -F nfs -o rw=neptune /usr/aset/all_reports/neptune_rpt
   ```

4. **Stellen Sie die Ressourcen in der Datei `dfstab` den Clients zur Verfügung.**

   ```
   # shareall
   ```

5. **Hängen Sie auf den einzelnen Clients das Clientunterverzeichnis vom Server am Einhängepunkt `/usr/aset/masters/reports` ein.**

   ```
   # mount server:/usr/aset/client_rpt /usr/aset/masters/reports
   ```

6. **Bearbeiten Sie die Datei `/etc/vfstab`, um das Verzeichnis beim Booten automatisch einzuhängen.**

   Im folgenden Beispieleintrag in `/etc/vfstab` auf `neptune` ist das von `mars` einzuhängende Verzeichnis (`/usr/aset/all_reports/neptune_rpt`) und der Einhängepunkt auf `neptune` (`/usr/aset/reports`) angegeben. Beim Booten werden die in `vfstab` aufgeführten Verzeichnisse automatisch eingehängt.

   ```
   mars:/usr/aset/all_reports/neptune.rpt /usr/aset/reports nfs - yes hard
   ```

Fehlerbehebung bei ASET-Problemen

In diesem Abschnitt werden die von ASET generierten Fehlermeldungen beschrieben.

ASET-Fehlermeldungen

`ASET failed: no mail program found.`

Grund: ASET wird angewiesen, das Ausführungsprotokoll an einen Benutzer zu senden, es wurde jedoch kein Mailprogramm gefunden.

Lösung: Installieren Sie ein Mailprogramm.

`Usage: aset [-n user[@host]] in /bin/mail or /usr/ucb/mail.`

`Cannot decide current and previous security levels.`

Grund: ASET kann die Sicherheitsebenen für den aktuellen und vorherigen Aufruf nicht feststellen.

Lösung: Vergewissern Sie sich, dass die aktuelle Sicherheitsebene entweder über die Umgebungsvariable `ASETSECLEVEL` oder die Befehlszeilenoption definiert wird. Stellen Sie außerdem sicher, dass in der letzten Zeile von `ASETDIR/archives/asetseclevel.arch` die vorherige Sicherheitsebene ordnungsgemäß angegeben ist. Wenn diese Werte nicht oder nicht ordnungsgemäß definiert sind, geben Sie die entsprechenden Werte ein.

`ASET working directory undefined.`

`Um die Einstellung anzugeben, definieren Sie die Umgebungsvariable ASETDIR oder verwenden Sie die Befehlszeilenoption -d.`

`ASET startup unsuccessful.`

Grund: Das ASET-Arbeitsverzeichnis wurde nicht oder nicht ordnungsgemäß definiert. Bei dem Arbeitsverzeichnis handelt es sich um das Betriebsverzeichnis.

Lösung: Verwenden Sie die Umgebungsvariable `ASETDIR` oder die Befehlszeilenoption `-d`, um den Fehler zu beheben, und starten Sie ASET erneut.

`ASET working directory $ASETDIR missing.`

`ASET startup unsuccessful.`

Grund: Das ASET-Arbeitsverzeichnis wurde nicht oder nicht ordnungsgemäß definiert. Bei dem Arbeitsverzeichnis handelt es sich um das Betriebsverzeichnis. Dieses Problem kann auftreten, wenn die Variable `ASETDIR` oder die Befehlszeilenoption `-d` auf ein nicht vorhandenes Verzeichnis verweisen.

Lösung: Vergewissern Sie sich, dass auf das richtige Verzeichnis, d. h. das Verzeichnis mit der ASET-Verzeichnishierarchie, verwiesen wird.

`Cannot expand $ASETDIR to full pathname.`

Grund: ASET kann den Verzeichnisnamen, der durch die Variable `ASETDIR` oder die Befehlszeilenoption `-d` angegeben ist, nicht auf einen vollständigen Pfadnamen erweitern.

Lösung: Stellen Sie sicher, dass der Verzeichnisname ordnungsgemäß angegeben ist. Vergewissern Sie sich, dass auf ein vorhandenes Verzeichnis verwiesen wird, auf das der Benutzer zugreifen kann.

`aset: invalid/undefined security level.`

`Um die Einstellung anzugeben, definieren Sie die Umgebungsvariable ASETSECLEVEL oder verwenden Sie die Befehlszeilenoption -l, wobei argument= low/med/high entspricht.`

Grund: Die Sicherheitsebene wurde nicht oder nicht ordnungsgemäß definiert. Nur die Werte `low`, `med` oder `high` sind zulässig.

Lösung: Verwenden Sie die Variable `ASETSECLEVEL` oder die Befehlszeilenoption `-l`, um einen der drei Werte anzugeben.

`ASET environment file asetenv not found in $ASETDIR.`

`ASET startup unsuccessful.`

Grund: ASET kann die Datei `asetenv` im Arbeitsverzeichnis nicht finden.

Lösung: Vergewissern Sie sich, dass die Datei `asetenv` im Arbeitsverzeichnis von ASET vorhanden ist. Ausführliche Informationen zu dieser Datei erhalten Sie auf der Manpage `asetenv(4)`.

`filename doesn't exist or is not readable.`
Grund: Die Datei, auf die durch *filename* verwiesen wird, ist entweder nicht vorhanden oder kann nicht gelesen werden. Dieses Problem kann auftreten, wenn Sie die Option `-u` verwenden. Durch die Option können Sie eine Datei angeben, die eine Liste der zu überprüfenden Benutzer enthält.

Lösung: Vergewissern Sie sich, dass das Argument der Option `-u` vorhanden und lesbar ist.

`ASET task list TASKLIST undefined.`
Grund: Die ASET-Aufgabenliste, die normalerweise in der Datei `asetenv` definiert wird, wurde nicht angegeben. Diese Meldung kann bedeuten, dass die Datei `asetenv` beschädigt ist.

Lösung: Untersuchen Sie die Datei `asetenv`. Vergewissern Sie sich, dass die Aufgabenliste im Abschnitt `User Configurable` definiert wurde. Überprüfen Sie ebenfalls andere Dateiabschnitte, um sicherzustellen, dass die Datei keine Fehler aufweist. Weitere Informationen zum Inhalt einer gültigen `asetenv`-Datei finden Sie auf der Manpage `asetenv(4)`.

`ASET task list $TASKLIST missing.`

`ASET startup unsuccessful.`
Grund: Die ASET-Aufgabenliste, die normalerweise in der Datei `asetenv` definiert wird, wurde nicht angegeben. Diese Meldung kann bedeuten, dass die Datei `asetenv` beschädigt ist.

Lösung: Untersuchen Sie die Datei `asetenv`. Vergewissern Sie sich, dass die Aufgabenliste im Abschnitt `User Configurable` definiert wurde. Überprüfen Sie ebenfalls andere Dateiabschnitte, um sicherzustellen, dass die Datei keine Fehler aufweist. Weitere Informationen zum Inhalt einer gültigen `asetenv`-Datei finden Sie auf der Manpage `asetenv(4)`.

`Schedule undefined for periodic invocation.`

`No tasks executed or scheduled. Check asetenv file.`
Grund: Die ASET-Planung wird durch die Option `-p` angefordert, jedoch ist die Umgebungsvariable `PERIODIC_SCHEDULE` in der Datei `asetenv` nicht definiert.

Lösung: Überprüfen Sie den Abschnitt `User Configurable` der Datei `asetenv`, um sicherzustellen, dass die Variable definiert ist. Vergewissern Sie sich, dass die Variable im richtigen Format vorliegt.

`Warning! Duplicate ASET execution scheduled.`

`Check crontab file.`

Grund: Es wurde eine mehrfache Ausführung von ASET geplant. Das heißt, eine ASET-Planung wurde angefordert, obwohl ein Plan bereits vorhanden ist. Diese Meldung weist nicht unbedingt auf einen Fehler hin, wenn mehrere Pläne benötigt werden. In diesem Fall stellen die Meldungen nur eine Warnung dar. Wenn mehrere Pläne erforderlich sind, verwenden Sie das entsprechende Planungsformat mit dem Befehl `crontab`. Weitere Informationen finden Sie auf der Manpage `crontab(1)`.

Lösung: Überprüfen Sie mithilfe des Befehls `crontab`, ob der richtige Plan verwendet wird. Vergewissern Sie sich, dass keine nicht erforderlichen `crontab`-Einträge für ASET vorhanden sind.

TEIL III

Rollen, Berechtigungsprofile und Berechtigungen

In diesem Abschnitt werden rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) und Prozessberechtigungsverwaltung behandelt. Zu den RBAC-Komponenten gehören Rollen, Berechtigungsprofile und Autorisierungen. Prozessberechtigungsverwaltung wird durch Berechtigungen implementiert. Berechtigungen arbeiten mit RBAC zusammen, um eine sicherere Verwaltungsalternative zur Systemverwaltung durch einen Superuser zur Verfügung zu stellen.

- Kapitel 8, „Verwenden von Rollen und Berechtigungen (Übersicht)“
- Kapitel 9, „Rollenbasierte Zugriffssteuerung (Aufgaben)“
- Kapitel 10, „Rollenbasierte Zugriffssteuerung (Übersicht)“
- Kapitel 11, „Berechtigungen (Aufgaben)“
- Kapitel 12, „Berechtigungen (Referenz)“

◆ ◆ ◆ KAPITEL 8

Verwenden von Rollen und Berechtigungen (Übersicht)

Oracle Solaris rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) und Berechtigungen bieten eine sicherere Alternative zum Superuser. In diesem Kapitel erhalten Sie eine Übersicht über RBAC und Berechtigungen.

Im Folgenden ist eine Übersicht der Informationen in diesem Kapitel aufgeführt.

- „Rollenbasierte Zugriffssteuerung (Übersicht)“ auf Seite 190
- „Berechtigungen (Übersicht)“ auf Seite 201

Neuerungen bei RBAC

Solaris 10 8/07: Mit dieser Version werden die Ressourcensteuerungen `project.max-locked-memory` und `zone.max-locked-memory` eingeführt. Wenn die Berechtigung `PRIV_PROC_LOCK_MEMORY` einem Benutzer oder einer nicht globalen Zone zugeordnet wird, können diese Ressourcensteuerungen so eingestellt werden, dass sie das Sperren des gesamten Speichers durch den Benutzer oder die Zone verhindern. Weitere Informationen finden Sie unter „Berechtigungen und Systemressourcen“ auf Seite 205.

Solaris 10 10/08: In dieser Version wurden die `solaris.admin.usermgr`-Autorisierungen neu organisiert, um die *Aufteilung der Pflichten*, eine Sicherheitsanforderung bei Hochsicherheitsinstallationen, zu unterstützen. Um der Aufteilung der Pflichten gerecht zu werden, sind zwei Konten zum Erstellen eines Benutzerkontos erforderlich. Informationen zum Konfigurieren der Software für diese Anforderung finden Sie unter „Create Rights Profiles That Enforce Separation of Duty“ in *Oracle Solaris Trusted Extensions Configuration Guide* . Bei dieser Version wird zudem im Handbuch unter „So ändern Sie das Passwort einer Rolle“ auf Seite 234 beschrieben, wie Sie das Passwort einer Rolle ändern können.

Solaris 10 9/10: In dieser Version wird die Berechtigung `net_access` zum Basisberechtigungssatz hinzugefügt. Eine Beschreibung der Berechtigung finden Sie auf der Manpage `privileges(5)`.

Rollenbasierte Zugriffssteuerung (Übersicht)

Rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) ist eine Sicherheitsfunktion zur Steuerung des Zugriffs von Benutzern auf Aufgaben, die normalerweise auf Superuser beschränkt wären. Durch das Anwenden von Sicherheitsattributen auf Prozesse und Benutzer kann RBAC Superuser-Berechtigungen auf mehrere verschiedene Administratoren aufteilen. Prozessberechtigungsverwaltung wird durch *Berechtigungen* implementiert. Benutzerberechtigungsverwaltung wird durch RBAC implementiert.

- Informationen zur Prozessberechtigungsverwaltung finden Sie unter „Berechtigungen (Übersicht)“ auf Seite 201.
- Informationen zu RBAC-Aufgaben finden Sie unter Kapitel 9, „Rollenbasierte Zugriffssteuerung (Aufgaben)“.
- Referenzinformationen finden Sie in Kapitel 10, „Rollenbasierte Zugriffssteuerung (Übersicht)“.

RBAC: eine Alternative zum Superuser-Modell

In konventionellen UNIX-Systemen ist der `root`-Benutzer, auch als Superuser bezeichnet, allmächtig. Programme, die als `root` ausgeführt werden, oder `setuid`-Programme sind allmächtig. Der `root`-Benutzer hat Lese- und Schreibzugriff auf alle Dateien, kann alle Programme ausführen und die Beendigung beliebiger Prozesse erzwingen. Effektiv kann jeder, der Superuser werden kann, die Firewall eines Standorts oder den Prüfpfad ändern, vertrauliche Datensätze lesen und das gesamte Netzwerk herunterfahren. Wenn ein `setuid`-Programm "entführt" wird, kann es jede beliebige Aktion auf dem System ausführen.

Rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) bietet eine sicherere Alternative zum allumfassenden Superuser-Modell. Mit RBAC können Sie die Sicherheitsrichtlinien auf exaktere Weise durchsetzen. RBAC verwendet das Sicherheitsprinzip der *niedrigsten Berechtigung*. Niedrigste Berechtigung bedeutet, dass einem Benutzer nur genau die Berechtigungen zur Verfügung stehen, die für die Ausführung eines Jobs erforderlich sind. Gewöhnliche Benutzer verfügen über ausreichend Berechtigungen, um ihre Anwendungen zu verwenden, den Status ihrer Jobs zu überprüfen, Dateien zu drucken, neue Dateien zu erstellen usw. Berechtigungen, die über normale Benutzerberechtigungen hinausgehen, werden in Berechtigungsprofilen gruppiert. Benutzer, von denen die Ausführung von Jobs erwartet wird, die Superuser-Berechtigungen erfordern, nehmen eine Rolle an, die das entsprechende Berechtigungsprofil umfasst.

RBAC fasst Superuser-Berechtigungen in *Berechtigungsprofilen* zusammen. Diese Berechtigungsprofile werden speziellen Benutzerkonten zugewiesen, den so genannten *Rollen*. Ein Benutzer kann dann eine Rolle übernehmen, um einen Job auszuführen, der einige Superuser-Berechtigungen erfordert. Vordefinierte Berechtigungsprofile werden mit Oracle Solaris-Software unterstützt. Sie können die Rollen selbst erstellen und die Profile zuweisen.

Berechtigungsprofile können umfassende Berechtigungen zur Verfügung stellen. Das Berechtigungsprofil "Primary Administrator" stellt z. B. ein Äquivalent zum Superuser dar. Berechtigungsprofile können auch stark eingeschränkt definiert werden. Das Berechtigungsprofil "Cron Management" verwaltet beispielsweise nur `at`- und `cron`-Jobs. Wenn Sie Rollen erstellen, können Sie sich für das Erstellen von Rollen mit umfassenden Berechtigungen, Rollen mit eingeschränkten Berechtigungen oder beides entscheiden.

Im RBAC-Modell erstellt der Superuser eine oder mehrere Rollen. Die Rollen basieren auf Berechtigungsprofilen. Der Superuser weist die Rollen dann vertrauenswürdigen Benutzern zur Ausführung zu. Benutzer melden sich mit ihrem Benutzernamen an. Nach der Anmeldung nehmen die Benutzer Rollen an, die eingeschränkte Administrationsbefehle und Tools mit grafischen Benutzeroberflächen (Graphical User Interface, GUI) ausführen.

Die Flexibilität beim Einrichten von Rollen ermöglicht eine Vielzahl von Sicherheitsrichtlinien. Es werden nur wenige Rollen mit Oracle Solaris geliefert; drei empfohlene Rollen können jedoch leicht konfiguriert werden. Diese Rollen basieren auf den Berechtigungsprofilen des gleichen Namens:

- **Primary Administrator**: Eine leistungsstarke Rolle, die ein Äquivalent zum `root`-Benutzer oder Superuser darstellt.
- **Root**: Eine leistungsstarke Rolle, die ein Äquivalent zum `root`-Benutzer darstellt. Dieser `root` kann sich jedoch nicht anmelden. Ein gewöhnlicher Benutzer muss sich anmelden und dann die ihm zugewiesene `root`-Rolle annehmen.
- **System Administrator**: Eine weniger leistungsstarke Rolle für die Verwaltung, die nicht mit der Sicherheit in Zusammenhang steht. Diese Rolle kann Dateisysteme, Mail und Softwareinstallationen verwalten. Diese Rolle kann jedoch keine Passwörter festlegen.
- **Operator**: Eine Juniorverwaltungsrolle für Vorgänge wie Backups und Druckerverwaltung.

Hinweis – Das Berechtigungsprofil "Media Backup" bietet Zugriff auf das gesamte Root-Dateisystem. Daher müssen Sie sicherstellen, dass der Benutzer tatsächlich vertrauenswürdig ist, während die Berechtigungsprofile "Media Backup" und "Operator" für einen Junioradministrator entwickelt werden.

Diese drei Rollen müssen nicht implementiert werden. Rollen stellen eine Funktion der Sicherheitsansprüche eines Unternehmens dar. Rollen können für Administratoren mit besonderen Funktionen in Bereichen wie Sicherheit, Vernetzung oder Firewall-Verwaltung eingerichtet werden. Eine andere Strategie besteht darin, eine einzelne, leistungsstarke Administratorrolle und eine Rolle für fortgeschrittene Benutzer zu erstellen. Die Rolle für fortgeschrittene Benutzer ist für Benutzer gedacht, die dazu berechtigt sind, Teile ihres eigenen Systems selbst zu reparieren.

Das Superuser-Modell und das RBAC-Modell können nebeneinander existieren. In der folgenden Tabelle werden die verschiedenen Abstufungen von Superuser bis zum

gewöhnlichen Benutzer aufgelistet, die im RBAC-Modell möglich sind. Die Tabelle umfasst auch die administrativen Aktionen, die in beiden Modellen verfolgt werden können. Eine Zusammenfassung der Auswirkungen von Berechtigungen allein auf einem System finden Sie in Tabelle 8–2.

TABELLE 8–1 Superuser-Modell im Gegensatz zu RBAC-Modell mit Berechtigungen

Benutzerberechtigungen auf einem System	Superuser-Modell	RBAC-Modell
Kann Superuser mit vollständigen Superuser-Berechtigungen werden	Ja	Ja
Kann sich als Benutzer mit vollständigen Benutzerberechtigungen anmelden	Ja	Ja
Kann Superuser mit eingeschränkten Berechtigungen werden	Nein	Ja
Kann sich als Benutzer anmelden und sporadisch Superuser-Berechtigungen verwenden	Ja, nur mit `setuid`-Programmen	Ja, mit `setuid`-Programmen und RBAC
Kann sich als Benutzer mit administrativen Berechtigungen, aber ohne vollständige Superuser-Berechtigungen anmelden	Nein	Ja, mit RBAC und direkt zugewiesenen Berechtigungen und Autorisierungen
Kann sich als Benutzer mit weniger Berechtigungen als ein gewöhnlicher Benutzer anmelden	Nein	Ja, mit RBAC und entfernten Berechtigungen
Kann Aktionen von Superusern verfolgen	Ja, durch Prüfen des Befehls `su`	Ja, durch Prüfen von Profil-Shell-Befehlen Wenn der `root`-Benutzer deaktiviert ist, befindet sich der Name des Benutzers, der die `root`-Rolle angenommen hat, zudem im Prüfpfad

Oracle Solaris RBAC-Elemente und Basiskonzepte

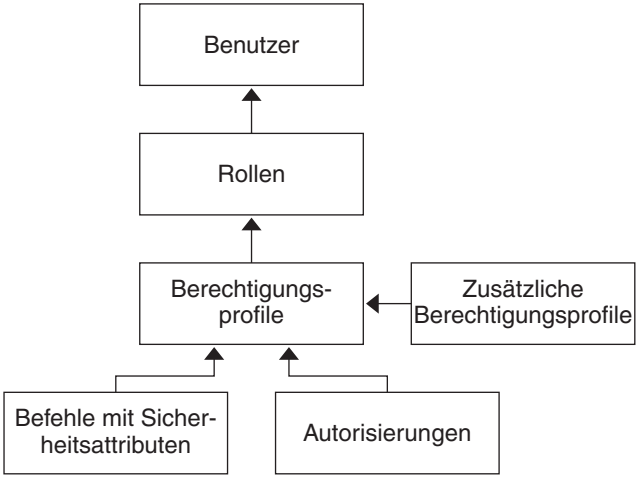
Das RBAC-Modell in Oracle Solaris führt folgende Elemente ein:

- **Autorisierung**: Eine Erlaubnis, die einem Benutzer oder einer Rolle das Ausführen von Aktionen ermöglicht, die zusätzliche Berechtigungen erfordern. Durch die Sicherheitsrichtlinien bei der Installation erhalten gewöhnliche Benutzer beispielsweise die Autorisierung `solaris.device.cdrw`. Diese Autorisierung ermöglicht Benutzern Lese- und Schreibvorgänge auf einem CD-ROM-Gerät. Eine Liste der Autorisierungen finden Sie in der Datei `/etc/security/auth_attr`.
- **Berechtigung**: Ein einzelnes Recht, das einem Befehl, einem Benutzer, einer Rolle oder einem System gewährt werden kann. Berechtigungen ermöglichen einem Prozess erfolgreiches Arbeiten. Durch die Berechtigung `proc_exec` kann ein Prozess beispielsweise `execve()` aufrufen. Gewöhnliche Benutzer verfügen über Basisberechtigungen. Um Ihre Basisberechtigungen einzusehen, führen Sie den Befehl `ppriv -vl basic` aus.
- **Sicherheitsattribute**: Ein Attribut, das einem Prozess das Ausführen eines Vorgangs ermöglicht. In einer typischen UNIX-Umgebung ermöglicht ein Sicherheitsattribut einem Prozess das Ausführen eines Vorgangs, der gewöhnlichen Benutzern andernfalls verboten ist. `setuid`- und `setgid`-Programme verfügen z. B. über Sicherheitsattribute. Im RBAC-Modell erfordern Vorgänge, die gewöhnliche Benutzer ausführen, möglicherweise Sicherheitsattribute. Zusätzlich zu den `setuid`- und `setgid`-Programmen stellen Autorisierungen und Berechtigungen auch Sicherheitsattribute im RBAC-Modell dar. Ein Benutzer mit der Autorisierung `solaris.device.allocate` kann beispielsweise ein Gerät für die exklusive Verwendung zuordnen. Ein Prozess mit der Berechtigung `sys_time` kann Systemzeit bearbeiten.
- **Privilegierte Anwendung**: Eine Anwendung oder ein Befehl, der/die Systemsteuerungen durch Überprüfen auf *Sicherheitsattribute* überschreiben kann. In einer typischen UNIX-Umgebung und im RBAC-Modell sind Programme, die `setuid` und `setgid` verwenden, privilegierte Anwendungen. Im RBAC-Modell sind Programme, die zur erfolgreichen Ausführung Berechtigungen oder Autorisierungen benötigen, ebenfalls privilegierte Anwendungen. Weitere Informationen finden Sie unter „Privilegierte Anwendungen und RBAC“ auf Seite 197.
- **Berechtigungsprofil**: Eine Sammlung administrativer Berechtigungen, die einer Rolle oder einem Benutzer zugewiesen werden können. Ein Berechtigungsprofil kann aus Autorisierungen, Befehlen mit Sicherheitsattributen und anderen Berechtigungsprofilen bestehen. Berechtigungsprofile bieten eine einfache Weise, Sicherheitsattribute zu gruppieren.
- **Rolle**: Eine spezielle Identität zum Ausführen privilegierter Anwendungen. Diese spezielle Identität kann nur von zugewiesenen Benutzern angenommen werden. In einem System, das mit Rollen ausgeführt wird, sind keine Superuser erforderlich. Superuser-Berechtigungen werden auf verschiedene Rollen verteilt. In einem System mit zwei Rollen werden z. B. Sicherheitsaufgaben von einer Sicherheitsrolle erfüllt. Die zweite Rolle bearbeitet nicht sicherheitsbezogene Systemverwaltungsaufgaben. Rollen können

genauer abgegrenzt sein. Ein System kann beispielsweise separate administrative Rollen zur Verwaltung des kryptografischen Frameworks, der Drucker, der Systemzeit, der Dateisysteme und der Prüfungen umfassen.

Die folgende Abbildung zeigt, wie die RBAC-Elemente zusammenarbeiten.

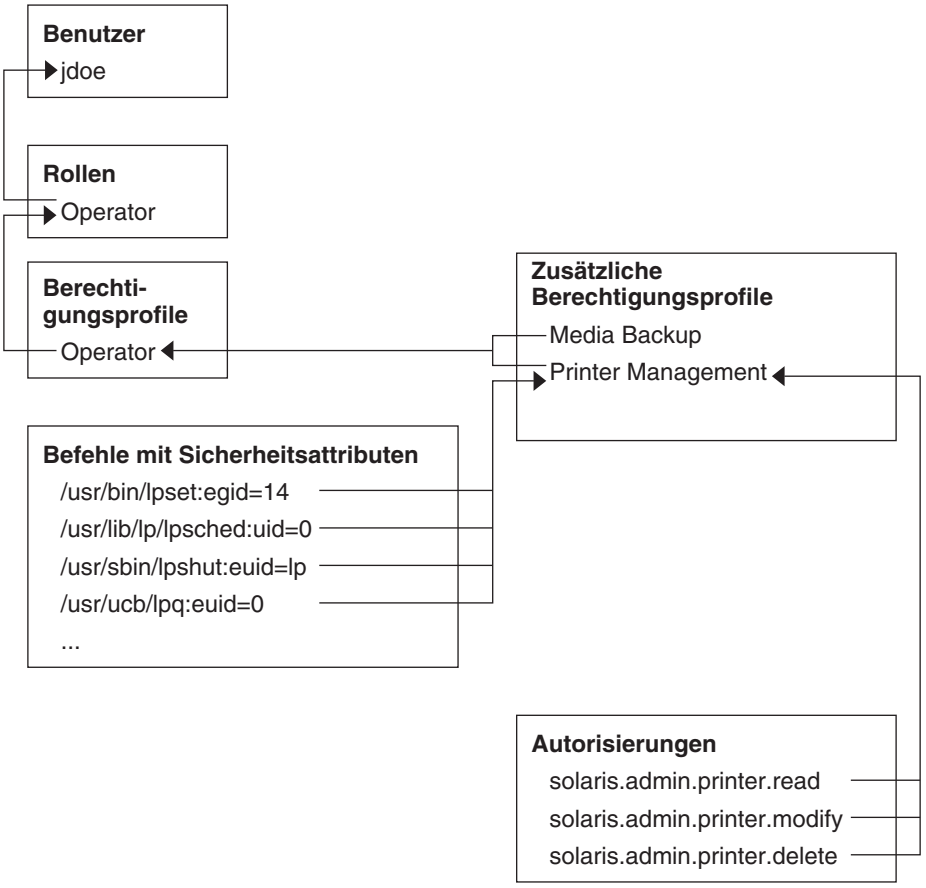
ABBILDUNG 8–1 Oracle Solaris RBAC-Elementbeziehungen



In RBAC werden Benutzern Rollen zugewiesen. Wenn ein Benutzer eine Rolle annimmt, stehen ihm die Berechtigungen der Rolle zur Verfügung. Rollen erhalten ihre Berechtigungen aus Berechtigungsprofilen. Berechtigungsprofile können Autorisierungen, direkt zugewiesene Berechtigungen, privilegierte Befehle und andere, zusätzliche Berechtigungsprofile enthalten. Privilegierte Befehle sind Befehle, die mit Sicherheitsattributen ausgeführt werden.

In der folgenden Abbildung werden RBAC-Beziehungen anhand der Rolle "Network Security" und des Berechtigungsprofils "Network Security" gezeigt.

ABBILDUNG 8–2 Beispiel für Oracle Solaris RBAC-Elementbeziehungen



Die Rolle "Network Security" wird zum Verwalten von IPsec, Wifi und Netzwerklinks verwendet. Die Rolle ist dem Benutzer `jdoe` zugewiesen. `jdoe` kann die Rolle durch Wechseln zur Rolle und anschließende Eingabe des Rollenpassworts annehmen.

Das Berechtigungsprofil "Network Security" wurde der Rolle "Network Security" zugewiesen. Das Berechtigungsprofil "Network Security" enthält zusätzliche, der Reihe nach bewertete Profile: Network Wifi Security, Network Link Security und Network IPsec Management. Diese zusätzlichen Profile erfüllen die Primäraufgaben der Rolle.

Das Berechtigungsprofil "Network Security" verfügt über drei direkt zugewiesene Autorisierungen, keine direkt zugewiesenen Berechtigungen und zwei Befehle mit Sicherheitsattributen. Die zusätzlichen Berechtigungsprofile verfügen über direkt zugewiesene Autorisierungen, und zwei von ihnen verfügen über Befehle mit Sicherheitsattributen. In der

Rolle "Network Security" hat `jdoe` alle zugewiesenen Autorisierungen in diesen Profilen und kann alle Befehle mit Sicherheitsattributen in diesen Profilen ausführen. `jdoe` kann die Netzwerksicherheit verwalten

Berechtigungseskalation

Oracle Solaris bietet Administratoren hohe Flexibilität bei Sicherheitskonfigurationen. Nach der Installation der Software ist zunächst keine Berechtigungseskalation möglich. Berechtigungseskalation tritt auf, wenn ein Benutzer oder ein Prozess mehr administrative Berechtigungen erhält, als er eigentlich bekommen sollte. In diesem Zusammenhang mit Berechtigung ein beliebiges Sicherheitsattribut gemeint, nicht nur eine Berechtigung.

Oracle Solaris-Software enthält Sicherheitsattribute, die nur dem `root`-Benutzer zugewiesen sind. Wenn noch andere Sicherheitsschutzmechanismen vorhanden sind, weist ein Administrator möglicherweise Attribute, die für den `root`-Benutzer ausgelegt sind, anderen Konten zu. Solche Zuweisungen müssen jedoch vorsichtig vorgenommen werden.

Das Berechtigungsprofil "Media Restore" ist beispielsweise zwar vorhanden, stellt jedoch keinen Teil eines anderen Berechtigungsprofils dar. Da `Media Restore` Zugriff auf das gesamte Root-Dateisystem bietet, stellt seine Verwendung eine mögliche Berechtigungseskalation dar. Absichtlich geänderte Dateien oder Ersatzmedien könnten wiederhergestellt werden. Standardmäßig verfügt nur der `root`-Benutzer über dieses Berechtigungsprofil.

Informationen zu Eskalationen, die das Berechtigungssicherheitsattribut beeinflussen, finden Sie unter „Verhindern von Berechtigungseskalation“ auf Seite 284.

RBAC-Autorisierungen

Eine *Autorisierung* ist eine einzelne Berechtigung, die einer Rolle oder einem Benutzer gewährt werden kann. Autorisierungen setzen Richtlinien auf der Benutzeranwendungsstufe durch.

Obwohl Autorisierungen einer Rolle oder einem Benutzer direkt zugewiesen werden können, empfiehlt es sich, Autorisierungen in einem Berechtigungsprofil festzuhalten. Das Berechtigungsprofil wird dann einer Rolle hinzugefügt und die Rolle einem Benutzer zugewiesen. Ein Beispiel finden Sie unter Abbildung 8–2.

RBAC-konforme Anwendungen können die Autorisierungen eines Benutzers überprüfen, bevor sie Zugriff auf die Anwendung oder spezifische Vorgänge innerhalb der Anwendung gewähren. Diese Überprüfung ersetzt die Überprüfung in konventionellen UNIX-Anwendungen für `UID=0`. Weitere Informationen zu Autorisierungen finden Sie in den folgenden Abschnitten:

- „Autorisierungsbenennung und -delegation“ auf Seite 252
- „Datenbank `auth_attr`“ auf Seite 256

- „Befehle, die Autorisierungen erfordern“ auf Seite 262

Autorisierungen und Berechtigungen

Berechtigungen setzen die Sicherheitsrichtlinie im Kernel durch. Der Unterschied zwischen Autorisierungen und Berechtigungen betrifft die Ebene, auf der die Sicherheitsrichtlinie durchgesetzt wird. Ohne die entsprechende Berechtigung kann ein Prozess durch den Kernel von der Ausführung privilegierter Vorgänge abgehalten werden. Ohne die entsprechende Autorisierung kann ein Benutzer von der Verwendung einer privilegierten Anwendung oder dem Ausführen sicherheitsempfindlicher Vorgänge innerhalb einer privilegierten Anwendung abgehalten werden. Weitere Informationen zu Berechtigungen finden Sie unter „Berechtigungen (Übersicht)“ auf Seite 201.

Privilegierte Anwendungen und RBAC

Anwendungen und Befehle, die Systemsteuerungen überschreiben können, werden als privilegierte Anwendungen bezeichnet. Durch Sicherheitsattribute wie `UID=0`, Berechtigungen und Autorisierungen wird eine Anwendung als privilegierte Anwendung definiert.

Anwendungen, die UIDs und GIDs prüfen

Privilegierte Anwendungen, die auf `root` (`UID=0`) oder andere spezielle UIDs oder GIDs hin überprüfen, gibt es bereits seit langer Zeit in der UNIX-Umgebung. Der Berechtigungsprofilmechanismus ermöglicht Ihnen das Isolieren von Befehlen, die eine spezifische ID erfordern. Anstatt die ID in einem Befehl zu ändern, auf den jeder zugreifen kann, können Sie den Befehl mit Ausführungssicherheitsattributen in einem Berechtigungsprofil platzieren. Ein Benutzer oder eine Rolle mit diesem Berechtigungsprofil kann das Programm anschließend ausführen, ohne dafür Superuser werden zu müssen.

IDs können als real oder effektiv eingestuft werden. Das Zuweisen von effektiven IDs wird dem Zuweisen realer IDs vorgezogen. Effektive IDs stellen ein Äquivalent zur Funktion `setuid` in den Dateiberechtigungsbits dar. Effektive IDs identifizieren zudem die UID für die Prüfung. Da jedoch einige Shell-Skripten und Programme eine reale UID von `root` benötigen, können auch reale UIDs eingestellt werden. Der Befehl `pkgadd` beispielsweise erfordert eine reale statt einer effektiven UID. Wenn eine effektive ID nicht ausreicht, um einen Befehl auszuführen, müssen Sie die ID in eine reale ID ändern. Informationen zu diesem Vorgang finden Sie unter „So erstellen oder ändern Sie ein Berechtigungsprofil“ auf Seite 238.

Anwendungen, die auf Berechtigungen prüfen

Privilegierte Anwendungen können die Verwendung von Berechtigungen überprüfen. Der RBAC-Berechtigungsprofilmechanismus ermöglicht das Festlegen von Berechtigungen für spezifische Befehle. Sie können den Befehl mit Ausführungssicherheitsattributen in einem

Berechtigungsprofil isolieren, damit keine Superuser-Berechtigungen zur Verwendung einer Anwendung oder eines Befehls erforderlich sind. Eine Benutzerrolle mit diesem Berechtigungsprofil kann den Befehl anschließend allein mit den Berechtigungen ausführen, die der Befehl für die erfolgreiche Ausführung benötigt.

Zu den Befehlen, die auf Berechtigungen prüfen, gehören die folgenden:

- Kerberos-Befehle wie `kadmin`, `kprop` und `kdb5_util`
- Netzwerkbefehle wie `ifconfig`, `routeadm` und `snoop`
- Datei- und Dateisystembefehle wie `chmod`, `chgrp` und `mount`
- Befehle, die Prozesse steuern, wie `kill`, `pcred` und `rcapadm`

Informationen zum Hinzufügen von Befehlen mit Berechtigungen zu einem Berechtigungsprofil finden Sie unter „So erstellen oder ändern Sie ein Berechtigungsprofil“ auf Seite 238. Informationen zum Festlegen, welche Befehle ein bestimmtes Profil auf Berechtigungen prüfen, finden Sie unter „Festlegen Ihrer zugewiesenen Berechtigungen“ auf Seite 275.

Anwendungen, die Autorisierungen prüfen

Oracle Solaris bietet zusätzlich Befehle, die Autorisierungen prüfen. Definitionsgemäß verfügt der `root`-Benutzer über alle Autorisierungen. Daher kann der `root`-Benutzer jede beliebige Anwendung ausführen. Zu den Anwendungen, die auf Autorisierungen prüfen, gehören die folgenden:

- Die gesamte Solaris Management Console-Toolsuite
- Prüfverwaltungsbefehle wie `auditconfig` und `auditreduce`
- Druckerverwaltungsbefehle wie `lpadmin` und `lpfilter`
- Die Batch-Job-bezogenen Befehle wie `at`, `atq`, `batch` und `crontab`
- Geräteorientierte Befehle wie `allocate`, `deallocate`, `list_devices` und `cdrw`.

Informationen zum Prüfen eines Skripts oder Programms auf Autorisierungen finden Sie in Beispiel 9–24. Informationen zum Schreiben eines Programms, das Autorisierungen erfordert, finden Sie unter „About Authorizations“ in *Developer's Guide to Oracle Solaris Security*.

RBAC-Berechtigungsprofile

Ein *Berechtigungsprofil* ist eine Sammlung von Systemüberschreibungen, die einer Rolle oder einem Benutzer zugewiesen werden können. Ein Berechtigungsprofil kann Autorisierungen, Befehle mit zugewiesenen Sicherheitsattributen und andere Berechtigungsprofile enthalten. Berechtigungsprofilinformationen werden zwischen den Datenbanken `prof_attr` und `exec_attr` aufgeteilt. Berechtigungsprofilnamen und -autorisierungen befinden sich in der Datenbank `prof_attr`. Der Berechtigungsprofilname und die Befehle mit zugewiesenen Sicherheitsattributen befinden sich in der Datenbank `exec_attr`.

Weitere Informationen zu Berechtigungsprofilen finden Sie in den folgenden Abschnitten:

- „Inhalt der Berechtigungsprofile“ auf Seite 247
- „Datenbank `prof_attr`“ auf Seite 258
- „Datenbank `exec_attr`“ auf Seite 259

RBAC-Rollen

Eine *Rolle* ist ein bestimmter Benutzerkontotyp, von dem aus Sie privilegierte Anwendungen ausführen können. Rollen werden auf die gleiche allgemeine Weise wie Benutzerkonten erstellt. Rollen haben ein Home-Verzeichnis, eine Gruppenzuweisung, ein Passwort usw. Berechtigungsprofile und Autorisierungen verleihen der Rolle administrative Fähigkeiten. Rollen können keine Berechtigungen von anderen Rollen oder Benutzern übernehmen. Superuser-Berechtigungen werden auf einzelne Rollen aufgeteilt und ermöglichen so sicherere administrative Praktiken.

Wenn ein Benutzer eine Rolle annimmt, ersetzen die Attribute der Rolle alle Benutzerattribute. Die Rolleninformationen werden in den Datenbanken `passwd`, `shadow` und `user_attr` gespeichert. Es können Rolleninformationen zur Datenbank `audit_user` hinzugefügt werden. Ausführliche Informationen zum Einrichten von Rollen finden Sie in den folgenden Abschnitten:

- „So planen Sie die RBAC-Implementierung“ auf Seite 215
- „So erstellen Sie eine Rolle über die Befehlszeile“ auf Seite 221
- „So ändern Sie die Eigenschaften einer Rolle“ auf Seite 236

Eine Rolle kann mehr als einem Benutzer zugewiesen werden. Alle Benutzer, die dieselbe Rolle annehmen können, haben das gleiche Rollen-Home-Verzeichnis, arbeiten in der gleichen Umgebung und haben Zugriff auf die gleichen Dateien. Benutzer können Rollen aus der Befehlszeile annehmen, indem sie den Befehl `su` ausführen und den Rollennamen und das Passwort eingeben. Benutzer können eine Rolle zudem im Solaris Management Console-Tool annehmen.

Eine Rolle kann sich nicht direkt anmelden. Ein Benutzer meldet sich an und nimmt anschließend eine Rolle an. Sobald ein Benutzer eine Rolle angenommen hat, kann er keine andere Rolle mehr annehmen, solange er seine derzeitige Rolle nicht verlässt. Nach Verlassen der Rolle kann der Benutzer eine andere Rolle annehmen.

Sie können anonyme `root`-Anmeldungen verhindern, indem Sie den `root`-Benutzer, wie in „So wandeln Sie den `root`-Benutzer in eine Rolle um“ auf Seite 226 beschrieben, als Rolle konfigurieren. Wenn der Profil-Shell-Befehl `pfexec` geprüft wird, enthält der Prüfpfad die reale UID des Anmeldebenutzers, die Rollen, die der Benutzer angenommen hat, sowie die Aktionen, die die Rolle ausgeführt hat. Informationen zum Prüfen des Systems oder eines bestimmten Benutzers für Rollenvorgänge finden Sie unter „So prüfen Sie Rollen“ auf Seite 225.

Mit Oracle Solaris-Software werden keine vordefinierten Rollen geliefert. Die Berechtigungsprofile, die mit der Software geliefert werden, wurden jedoch für die Zuordnung zu Rollen entwickelt. Das Berechtigungsprofil "Primary Administrator" kann beispielsweise zum Erstellen der Rolle "Primary Administrator" verwendet werden.

- Informationen zum Konfigurieren der Rolle "Primary Administrator" finden Sie unter „Using the Solaris Management Tools With RBAC (Task Map)“ in *System Administration Guide: Basic Administration* .
- Informationen zum Konfigurieren weiterer Rollen finden Sie unter „So können Sie eine Rolle mit der GUI erstellen und zuweisen“ auf Seite 218.
- Informationen zum Erstellen von Rollen in der Befehlszeile finden Sie unter „Verwalten von RBAC (Übersicht der Schritte)“ auf Seite 233.

Profil-Shells und RBAC

Rollen können privilegierte Anwendungen vom Solaris Management Console Launcher oder von einer Profil-Shell aus starten. Eine *Profil-Shell* ist eine besondere Shell, die die in einem Berechtigungsprofil eingeschlossenen Sicherheitsattribute erkennt. Profil-Shells werden gestartet, wenn der Benutzer den Befehl `su` ausführt, um eine Rolle anzunehmen. Die Profil-Shells sind `pfsh`, `pfcsh` und `pfksh`. Die Shells entsprechen Bourne-Shell (`sh`), C-Shell (`csh`) und Korn-Shell (`ksh`).

Benutzer, denen direkt ein Berechtigungsprofil zugewiesen wurde, müssen eine Profil-Shell aufrufen, um die Befehle mit Sicherheitsattributen auszuführen. Informationen zu Benutzungs- und Sicherheitsfragen finden Sie unter „Sicherheitsüberlegungen bei direkter Zuweisung von Sicherheitsattributen“ auf Seite 201.

Alle Befehle, die in einer Profil-Shell ausgeführt werden, können geprüft werden. Weitere Informationen finden Sie unter „So prüfen Sie Rollen“ auf Seite 225.

Name Service-Bereich und RBAC

Der Name Service-Bereich ist ein für das Verständnis von RBAC wichtiges Konzept. Der Bereich einer Rolle kann auf einen einzelnen Host beschränkt sein. Alternativ kann der Bereich alle Hosts umfassen, die einen Naming Service wie NIS, NIS+ oder LDAP verwenden. Der Name Service-Bereich für ein System wird in der Datei `/etc/nsswitch.conf` angegeben. Eine Suche hält bei der ersten Übereinstimmung an. Wenn ein Berechtigungsprofil z. B. in zwei Name Service-Bereichen vorhanden ist, werden nur die Einträge im ersten Name Service-Bereich verwendet. Wenn die erste Übereinstimmung `files` ist, ist der Bereich der Rolle auf den lokalen Host beschränkt.

Sicherheitsüberlegungen bei direkter Zuweisung von Sicherheitsattributen

Normalerweise erhält ein Benutzer administrative Berechtigungen durch eine Rolle. Autorisierungen und privilegierte Befehle werden in ein Berechtigungsprofil gruppiert. Das Berechtigungsprofil wird in eine Rolle eingeschlossen und diese einem Benutzer zugewiesen.

Direkte Zuweisungen von Berechtigungsprofilen und Sicherheitsattributen sind ebenfalls möglich:

- Berechtigungsprofile, Berechtigungen und Autorisierungen können Benutzern direkt zugewiesen werden.
- Berechtigungen und Autorisierungen können Benutzern und Rollen direkt zugewiesen werden.

Die direkte Zuweisung von Berechtigungen ist jedoch keine sichere Vorgehensweise. Benutzer und Rollen mit einer direkt zugewiesenen Berechtigung könnten die Sicherheitsrichtlinie überschreiben, falls diese Berechtigung vom Kernel benötigt wird. Eine sicherere Vorgehensweise ist das Zuweisen der Berechtigung als Sicherheitsattribut eines Befehls in einem Berechtigungsprofil. Diese Berechtigung ist dann für diesen Befehl nur für Personen mit diesem Berechtigungsprofil verfügbar.

Da Autorisierungen auf Benutzerebene arbeiten, ist die direkte Zuweisung von Autorisierungen möglicherweise weniger gefährlich als die direkte Zuweisung von Berechtigungen. Autorisierungen können einem Benutzer jedoch das Ausführen äußerst sicherer Aufgaben wie das Zuweisen von Prüf-Flags ermöglichen.

Ein Berechtigungsprofil, das einem Benutzer direkt zugewiesen wird, verursacht eher Verwendungs- als Sicherheitsprobleme. Die Befehle mit Sicherheitsattributen im Berechtigungsprofil können nur in einer Profil-Shell erfolgreich ausgeführt werden. Der Benutzer muss eine Profil-Shell öffnen und dann die Befehle in diese Shell eingeben. Eine Rolle, der ein Berechtigungsprofil zugewiesen ist, erhält automatisch eine Profil-Shell. Daher werden die Befehle erfolgreich in der Shell der Rolle ausgeführt.

Berechtigungen (Übersicht)

Bei der Prozessberechtigungsverwaltung können Prozesse auf Befehls-, Benutzer-, Rollen- oder Systemebene beschränkt werden. Oracle Solaris implementiert Prozessberechtigungsverwaltung über *Berechtigungen*. Berechtigungen reduzieren das Sicherheitsrisiko, das entsteht, wenn ein Benutzer oder ein Prozess auf einem System vollständige Superuser-Berechtigungen hat. Berechtigungen und RBAC stellen ein leistungsstarkes Alternativmodell zum traditionellen Superuser-Modell dar.

- Informationen zu RBAC finden Sie unter „Rollenbasierte Zugriffssteuerung (Übersicht)“ auf Seite 190.

- Informationen zum Verwalten von Berechtigungen finden Sie in Kapitel 11, „Berechtigungen (Aufgaben)“.
- Referenzinformationen zu Berechtigungen finden Sie in Kapitel 12, „Berechtigungen (Referenz)“.

Berechtigungen zum Schutz von Kernel-Prozessen

Eine Berechtigung ist ein einzelnes Recht, das ein Prozess zum Durchführen eines Vorgangs benötigt. Die Berechtigung wird im Kernel durchgesetzt. Ein Programm, das innerhalb der Grenzen des Oracle Solaris-Berechtigungs-*Basissatzes* arbeitet, arbeitet innerhalb der Grenzen der Systemsicherheitsrichtlinie. `setuid`-Programme sind Beispiele für Programme, die außerhalb der Grenzen der Systemsicherheitsrichtlinie arbeiten. Durch die Verwendung von Berechtigungen müssen Programme `setuid` nicht mehr aufrufen.

Berechtigungen führen die Arten der auf einem System ausführbaren Vorgänge einzeln auf. Programme können mit genau den Berechtigungen ausgeführt werden, die die erfolgreiche Ausführung des Programms ermöglichen. Ein Programm, das das Datum festlegt und es in eine administrative Datei schreibt, erfordert z. B. möglicherweise die Berechtigungen `file_dac_write` und `sys_time`. Durch diese Berechtigungen entfällt die Notwendigkeit, ein anderes Programm als `root` auszuführen.

Historisch gesehen folgen Systeme nicht dem Berechtigungsmodell. Sie verwendeten eher das Superuser-Modell. Im Superuser-Modell werden Prozesse als `root` oder als Benutzer ausgeführt. Benutzerprozesse wurden auf die Ausführung im Verzeichnis und den Dateien des Benutzers beschränkt. `root`-Prozesse konnten Verzeichnisse und Dateien an einem beliebigen Ort im System erstellen. Ein Prozess, der die Erstellung eines Verzeichnisses außerhalb des Benutzerverzeichnisses erforderte, wurde mit einer `UID=0` ausgeführt, d. h. als `root`. Die Sicherheitsrichtlinie stützte sich auf wahlfreie Zugangskontrollen (Discretionary Access Controls, DAC), um Systemdateien zu schützen. Geräteknoten wurden von DAC geschützt. Geräte, die der Gruppe `sys` angehörten, konnten z. B. nur von Mitgliedern der Gruppe `sys` geöffnet werden.

`setuid`-Programme, Dateiberechtigungen und administrative Konten sind jedoch anfällig für Missbrauch. Die Anzahl der Aktionen, die ein `setuid`-Prozess ausführen darf, ist höher als zur Ausführung des Vorgangs durch den Prozess erforderlich. Ein `setuid`-Programm kann von einem Eindringling ausgeführt werden, der dann als allmächtiger `root`-Benutzer arbeitet. Auf ähnliche Weise kann ein Benutzer mit Zugriff auf das `root`-Passwort das gesamte System beeinträchtigen.

Im Gegensatz dazu ermöglicht ein System, das Richtlinien mit Berechtigungen durchsetzt, eine Abstufung zwischen Benutzer- und `root`-Berechtigungen. Ein Benutzer kann Berechtigungen zum Ausführen von Vorgängen erhalten, die über die Berechtigungen gewöhnlicher Benutzer hinausgehen, und `root` kann auf weniger Berechtigungen beschränkt werden, als `root` derzeit besitzt. Mithilfe von RBAC kann ein Befehl, der mit Berechtigungen ausgeführt wird, in einem

Berechtigungsprofil isoliert und einem Benutzer oder einer Rolle zugewiesen werden. In Tabelle 8–1 wird die Abstufung zwischen Benutzer- und Root-Berechtigungen zusammengefasst, die das Modell aus RBAC und dem Berechtigungsmodell bietet.

Das Berechtigungsmodell bietet höhere Sicherheit als das Superuser-Modell. Berechtigungen, die aus einem Prozess entfernt wurden, können nicht genutzt werden. Prozessberechtigungen verhindern, dass ein Programm oder Verwaltungskonto Zugriff auf alle Berechtigungen erhält. Prozessberechtigungen können eine zusätzliche Schutzmaßnahme für vertrauliche Dateien zur Verfügung stellen, wobei DAC-Schutz genutzt werden kann, um Zugriff zu erhalten.

Berechtigungen können Programme und Prozesse auf die Berechtigungen beschränken, die das Programm zur Ausführung benötigt. Dies wird als *Prinzip der geringsten Berechtigung* bezeichnet. Auf einem System, das die geringste Berechtigung implementiert, hat ein Eindringling bei Übernahme eines Prozesses nur Zugriff auf die Berechtigungen dieses Prozesses. Das restliche System wird nicht beeinträchtigt.

Berechtigungsbeschreibungen

Berechtigungen werden logisch auf der Basis des Bereichs der Berechtigung gruppiert.

- `FILE` **Berechtigungen**: Berechtigungen, die mit der Zeichenfolge `file` beginnen, werden auf Dateisystemobjekte angewendet. Die Berechtigung `file_dac_write` überschreibt beispielsweise beim Schreiben in Dateien wahlfreie Zugangskontrollen.
- `IPC` **Berechtigungen**: Berechtigungen, die mit der Zeichenfolge `ipc` beginnen, überschreiben die IPC-Objektzugriffssteuerung. Die Berechtigung `ipc_dac_read` ermöglicht einem Prozess beispielsweise, gemeinsam genutzten Remote-Speicher, der durch DAC geschützt wird, zu lesen.
- `NET` **Berechtigungen**: Berechtigungen, die mit der Zeichenfolge `net` beginnen, gewähren Zugriff auf spezifische Netzwerkfunktionen. Die Berechtigung `net_rawaccess` ermöglicht Geräten beispielsweise, eine Verbindung zum Netzwerk herzustellen.
- `PROC` **Berechtigungen**: Berechtigungen, die mit der Zeichenfolge `proc` beginnen, ermöglichen Prozessen das Ändern beschränkter Eigenschaften des Prozesses selbst. `PROC`-Berechtigungen umfassen auch Berechtigungen mit sehr eingeschränkten Auswirkungen. Die Berechtigung `proc_clock_highres` ermöglicht einem Prozess die Verwendung hochauflösender Timer.
- `SYS` **Berechtigungen**: Berechtigungen, die mit der Zeichenfolge `sys` beginnen, gewähren Prozessen unbeschränkten Zugriff auf verschiedene Systemeigenschaften. Die Berechtigung `sys_linkdir` ermöglicht einem Prozess beispielsweise, Hard Links zu Verzeichnissen herzustellen und zu entfernen.

Einige Berechtigungen haben beschränkte, andere umfassende Auswirkungen auf das System. Die Definition der Berechtigung `proc_taskid` weist auf ihre beschränkten Auswirkungen hin:

```
proc_taskid
        Allows a process to assign a new task ID to the calling process.
```

Die Definition der Berechtigung `file_setid` weist auf ihre umfassenden Auswirkungen hin:

```
net_rawaccess
        Allow a process to have direct access to the network layer.
```

Auf der Manpage `privileges(5)` finden Sie Beschreibungen zu allen Berechtigungen. Der Befehl `ppriv -lv` druckt eine standardmäßige Beschreibung jeder Berechtigung.

Administrative Unterschiede auf einem System mit Berechtigungen

Ein System mit Berechtigungen weist mehrere sichtbare Unterschiede zu einem System ohne Berechtigungen auf. In der folgenden Tabelle werden einige dieser Unterschiede aufgeführt.

TABELLE 8–2 Sichtbare Unterschiede zwischen einem System mit Berechtigungen und einem System ohne Berechtigungen

Funktion	Keine Berechtigungen	Berechtigungen
Dämonen	Dämonen werden als `root` ausgeführt.	Dämonen werden als Benutzer `daemon` ausgeführt. Die folgenden Dämonen haben beispielsweise geeignete Berechtigungen erhalten und werden als `daemon` ausgeführt: `lockd`, `nfsd` und `rpcbind`.
Eigentümerschaft der Protokolldatei	Protokolldateien gehören `root`.	Protokolldateien gehören nicht `daemon`, der die Protokolldatei erstellt hat. Die Datei gehört nicht dem `root`-Benutzer.
Fehlermeldungen	Fehlermeldungen beziehen sich auf den Superuser. Beispiel: `chroot: not superuser`	Fehlermeldungen geben die Verwendung von Berechtigungen wieder. Die äquivalente Fehlermeldung bei Fehlschlagen von `chroot` ist z. B. `chroot: exec failed`.
`setuid`-Programme	Programme verwenden `setuid` zum Erfüllen von Aufgaben, zu deren Ausführung gewöhnliche Benutzer nicht berechtigt sind.	Viele `setuid`-Programme wurden für die Ausführung mit Berechtigungen geändert. Die folgenden Dienstprogramme verwenden beispielsweise Berechtigungen: `ufsdump`, `ufsrestore`, `rsh`, `rlogin`, `rcp` , `rdist`, `ping`, `traceroute` und `newtask`.

TABELLE 8–2 Sichtbare Unterschiede zwischen einem System mit Berechtigungen und einem System ohne Berechtigungen *(Fortsetzung)*

Funktion	Keine Berechtigungen	Berechtigungen
Dateiberechtigungen	Geräteberechtigungen werden von DAC kontrolliert. Mitglieder der Gruppe `sys` können beispielsweise `/dev/ip` öffnen.	Dateiberechtigungen (DAC) sehen nicht voraus, wer ein Gerät öffnen kann. Geräte werden von DAC *und* Geräterichtlinien geschützt. Die Datei `/dev/ip` hat beispielsweise die `666` Berechtigungen, aber das Gerät kann nur von einem Prozess mit den geeigneten Berechtigungen geöffnet werden. Raw-Sockets werden noch immer durch DAC geschützt.
Prüfereignisse	Die Prüfung der Verwendung des Befehls `su` deckt viele administrative Funktionen ab.	Die Prüfung der Verwendung von Berechtigungen deckt die meisten administrativen Funktionen ab. Die Prüfklassen `pm` und `as` enthalten Prüfereignisse, die Geräterichtlinien konfigurieren und Prüfereignisse, die Berechtigungen festlegen.
Prozesse	Prozesse werden vom Eigentümer des Prozesses geschützt.	Prozesse werden von Berechtigungen geschützt. Prozessberechtigungen und Prozess-Flags sind als neuer Eintrag `priv` im Verzeichnis `/proc/<pid>` sichtbar.
Fehlersuche	Keine Referenz zu Berechtigungen in Speicherabzügen	Der Hinweisabschnitt ELF von Speicherabzügen enthält Informationen zu Prozessberechtigungen und Flags in den Hinweisen `NT_PRPRIV` und `NT_PRPRIVINFO`. Das Dienstprogramm `ppriv` und andere Dienstprogramme zeigen die korrekte Anzahl von Sätzen der richtigen Größe. Die Dienstprogramme ordnen die Bits in den Bit-Sätzen den korrekten Berechtigungsnamen zu.

Berechtigungen und Systemressourcen

Ab der Version Solaris 10 8/07 können die Ressourcensteuerungen `project.max-locked-memory` und `zone.max-locked-memory` verwendet werden, um den Speicherplatzverbrauch von Prozessen zu begrenzen, denen die Berechtigung `PRIV_PROC_LOCK_MEMORY` zugewiesen ist. Diese Berechtigung ermöglicht einem Prozess das Sperren von Seiten im physischen Speicher.

Wenn Sie die Berechtigung `PRIV_PROC_LOCK_MEMORY` einem Berechtigungsprofil zuweisen, können Sie den Prozessen mit dieser Berechtigung die Möglichkeit zum Sperren des gesamten Speichers geben. Richten Sie als Schutzmaßnahme eine Ressourcensteuerung ein, um zu verhindern, dass der Benutzer der Berechtigung den gesamten Speicher sperrt. Stellen Sie für privilegierte Prozesse, die in einer nicht globalen Zone ausgeführt werden, die Ressourcensteuerung `zone.max-locked-memory` ein. Erstellen Sie ein Projekt für privilegierte Prozesse, die auf einem System ausgeführt werden, und richten Sie die Ressourcensteuerung `project.max-locked-memory` ein. Informationen zu diesen Ressourcensteuerungen finden Sie in Kapitel 6, „Einführung in die Resource Controls“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones* und Kapitel 17, „Einführung in die

Konfiguration einer nicht-globalen Zone“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.

Implementieren von Berechtigungen

Jeder Prozess hat vier Berechtigungssätze, die festlegen, ob ein Prozess eine bestimmte Berechtigung verwenden kann. Der Kernel berechnet automatisch den *effektiven Berechtigungssatz*. Sie können den ursprünglichen *vererbbaren Berechtigungssatz* ändern. Ein Programm, das zur Verwendung von Berechtigungen verschlüsselt wurde, kann den *zugelassenen Berechtigungssatz* des Programms reduzieren. Sie können den *begrenzten Berechtigungssatz* verkleinern.

- **Effektiver Berechtigungssatz oder E**: Der derzeit ausgeführte Berechtigungssatz. Ein Prozess kann Berechtigungen hinzufügen, die sich im zugelassenen Satz oder dem effektiven Satz befinden. Ein Prozess kann zudem Berechtigungen aus E entfernen.
- **Zugelassener Berechtigungssatz oder P**: Der für die Verwendung verfügbare Berechtigungssatz. Berechtigungen können einem Programm durch Vererbung oder Zuweisung zur Verfügung stehen. Ein Ausführungsprofil stellt eine Methode dar, einem Programm Berechtigungen zuzuweisen. Der Befehl `setuid` weist alle Berechtigungen von `root` einem Programm zu. Berechtigungen können aus dem zugelassenen Satz entfernt, ihm jedoch nicht hinzugefügt werden. Berechtigungen, die aus P entfernt werden, werden automatisch auch aus E entfernt.

  Ein *Berechtigungen erkennendes* Programm entfernt die Berechtigungen, die ein Programm nie verwendet, aus dem zugelassenen Satz des Programms. Auf diese Weise können nicht erforderliche Berechtigungen nicht vom Programm oder einem böswilligen Prozess ausgenutzt werden. Weitere Informationen zu Berechtigungen erkennenden Programmen finden Sie in Kapitel 2, „Developing Privileged Applications“ in *Developer's Guide to Oracle Solaris Security*.
- **Vererbbarer Berechtigungssatz oder I**: Der Berechtigungssatz, den ein Prozess über einen Aufruf von `exec` erben kann. Nach dem Aufruf von `exec` sind die zugelassenen und effektiven Sätze gleich, außer im Sonderfall eines `setuid`-Programms.

  Für ein `setuid`-Programm wird der vererbbare Satz nach dem Aufruf von `exec` zunächst vom begrenzten Satz eingeschränkt. Anschließend wird der geerbte Berechtigungssatz (I), abzüglich aller Berechtigungen im begrenzten Satz (L), den Berechtigungssätzen P und E für diesen Prozess zugewiesen.
- **Begrenzter Berechtigungssatz oder L**: Die äußere Begrenzung dessen, welche Berechtigungen einem Prozess und seinen untergeordneten Prozessen zur Verfügung stehen. Standardmäßig umfasst der begrenzte Satz alle Berechtigungen. Prozesse können den begrenzten Satz einschränken, aber nicht erweitern. L wird verwendet, um I einzuschränken. Infolgedessen beschränkt L bei Aufruf von `exec` P und E.

Wenn einem Benutzer ein Profil zugewiesen wurde, das ein Programm umfasst, dem Berechtigungen zugewiesen wurden, kann der Benutzer dieses Programm normalerweise ausführen. Auf einem unveränderten System befinden sich die zugewiesenen Berechtigungen eines Programms innerhalb des begrenzten Satzes des Benutzers. Die Berechtigungen, die dem Programm zugewiesen wurden, werden Teil des zugelassenen Satzes des Benutzers. Um das Programm auszuführen, dem Berechtigungen zugewiesen wurden, muss der Benutzer das Programm von einer Profil-Shell ausführen.

Der Kernel erkennt einen *grundlegendes Berechtigungssatz*. Auf einem unveränderten System entspricht der ursprünglich vererbbare Satz jedes Benutzers dem grundlegenden Satz bei der Anmeldung. Sie können den ursprüngliche vererbbaren Satz des Benutzers ändern. Der grundlegende Satz kann nicht geändert werden.

Auf einem unveränderten System würde der Berechtigungssatz eines Benutzers bei der Anmeldung ähnlich dem folgenden aussehen:

```
E (Effective): basic
I (Inheritable): basic
P (Permitted): basic
L (Limit): all
```

Daher ist der grundlegende Satz aller Benutzer bei der Anmeldung in ihrem vererbbaren Satz, ihrem zugelassenen Satz und ihrem effektiven Satz enthalten. Der begrenzte Satz eines Benutzers enthält alle Berechtigungen. Um mehr Berechtigungen zum effektiven Satz des Benutzers hinzuzufügen, müssen Sie dem Benutzer ein Berechtigungsprofil zuweisen. Das Berechtigungsprofil schließt dann Befehle ein, denen Sie Berechtigungen hinzugefügt haben. Sie können zudem Berechtigungen direkt dem Benutzer oder der Rolle zuweisen, auch wenn solche Berechtigungszuweisungen riskant sein können. Informationen zu den Risiken finden Sie unter „Sicherheitsüberlegungen bei direkter Zuweisung von Sicherheitsattributen“ auf Seite 201.

Zuweisen von Berechtigungen zu Prozessen

Prozesse können Berechtigungen erben. Es können ihnen auch Berechtigungen zugewiesen werden. Ein Prozess erbt Berechtigungen von seinem übergeordneten Prozess. Bei der Anmeldung legt der ursprüngliche vererbbare Berechtigungssatz des Benutzers fest, welche Berechtigungen den Prozessen des Benutzers zur Verfügung stehen. Alle untergeordneten Prozesse der erstmaligen Anmeldung des Benutzers erben diesen Satz.

Sie können Programmen, Benutzern und Rollen auch direkt Berechtigungen zuweisen. Wenn ein Programm Berechtigungen erfordert, weisen Sie die Berechtigungen der ausführbaren Datei des Programms in einem Berechtigungsprofil zu. Benutzern oder Rollen, die zur Ausführung des Programms zugelassen sind, wird das Profil zugewiesen, das das Programm enthält. Bei der Anmeldung oder beim Zugriff auf eine Profil-Shell wird das Programm mit Berechtigung ausgeführt, wenn die ausführbare Datei des Programms in die Profil-Shell

eingegeben wird. Eine Rolle, die das Profil "Object Access Management" beinhaltet, kann den Befehl `chmod` mit der Berechtigung `file_chown` ausführen.

Wenn eine Rolle oder ein Benutzer ein Programm ausführt, dem direkt eine zusätzliche Berechtigung zugewiesen wurde, wird die zugewiesene Berechtigung dem vererbbaren Satz der Rolle oder des Benutzers hinzugefügt. Untergeordnete Prozesse des Programms, dem Berechtigungen zugewiesen wurden, erben die Berechtigungen des übergeordneten Prozesses. Wenn der untergeordnete Prozess mehr Berechtigungen erfordert als der übergeordnete Prozess, müssen dem untergeordneten Prozess diese Berechtigungen direkt zugewiesen werden.

Programme, die zur Verwendung von Berechtigungen entwickelt wurden, werden als Berechtigungen erkennende Programme bezeichnet. Ein *Berechtigungen erkennendes* Programm aktiviert und deaktiviert die Verwendung von Berechtigungen während der Programmausführung. Um in einer Produktionsumgebung erfolgreich ausgeführt zu werden, müssen dem Programm die Berechtigungen zugewiesen werden, die es aktiviert und deaktiviert.

Beispiele für Berechtigungen erkennenden Code finden Sie in Kapitel 2, „Developing Privileged Applications“ in *Developer's Guide to Oracle Solaris Security*. Informationen zum Zuweisen der erforderlichen Berechtigungen zu einem Programm finden Sie unter „So fügen Sie Berechtigungen zu einem Befehl hinzu“ auf Seite 270.

Zuweisen von Berechtigungen

Sie sind in Ihrer Funktion als Systemadministrator für das Zuweisen von Berechtigungen verantwortlich. Normalerweise weisen Sie die Berechtigung einem Befehl in einem Berechtigungsprofil zu. Das Berechtigungsprofil wird dann einer Rolle oder einem Benutzer zugewiesen. Die Solaris Management Console bietet eine grafische Benutzeroberfläche (Graphical User Interface, GUI) zum Zuweisen von Berechtigungen. Berechtigungen können auch durch Verwenden von Befehlen wie `smuser` und `smrole` zugewiesen werden. Weitere Informationen zur Verwendung der GUI zum Zuweisen von Berechtigungen finden Sie in Kapitel 9, „Rollenbasierte Zugriffssteuerung (Aufgaben)“.

Berechtigungen können einem Benutzer direkt zugewiesen werden. Wenn Sie einem Teil der Benutzer eine Berechtigung zur verantwortungsvollen Verwendung während ihrer Sitzungen gewähren möchten, können Sie diese Berechtigung direkt zuweisen. Besonders geeignet für direkte Zuweisung sind Berechtigungen mit beschränkten Auswirkungen, z. B. `proc_clock_highres`. Berechtigungen mit umfassenden Auswirkungen, z. B. `file_dac_write`, sind weniger für direkte Zuweisung geeignet.

Berechtigungen können einem Benutzer oder einem System auch verweigert werden. Beim Entfernen von Berechtigungen aus dem ursprünglichen vererbbaren Satz oder dem begrenzten Satz eines Benutzers oder Systems muss äußerst vorsichtig vorgegangen werden.

Erweitern der Berechtigungen eines Benutzers oder einer Rolle

Benutzer und Rollen verfügen über einen vererbbaren Berechtigungssatz und einen begrenzten Berechtigungssatz. Der begrenzte Satz kann nicht erweitert werden, da die ursprünglich festgelegte Begrenzung alle Berechtigungen umfasst. Der ursprüngliche vererbbare Satz kann für Benutzer, Rollen und Systeme erweitert werden. Eine Berechtigung, die nicht im vererbbaren Satz enthalten ist, kann auch einem Prozess zugewiesen werden.

Die Zuweisung von Berechtigungen pro Prozess ist die präziseste Art zum Hinzufügen von Berechtigungen. Sie können die Anzahl privilegierter Vorgänge, die ein Benutzer ausführen kann, erweitern, indem Sie dem Benutzer das Annehmen einer Rolle ermöglichen. Der Rolle würden Profile zugewiesen, die Befehle mit hinzugefügten Berechtigungen umfassen. Wenn der Benutzer die Rolle annimmt, erhält er die Profil-Shell der Rolle. Bei Eingabe in die Shell der Rolle werden die Befehle in den Profilen der Rolle mit den hinzugefügten Berechtigungen ausgeführt.

Sie können auch ein Profil dem Benutzer zuweisen statt einer Rolle, die der Benutzer annimmt. Das Profil würde Befehle mit hinzugefügten Berechtigungen einschließen. Wenn der Benutzer eine Profil-Shell öffnet, z. B. `pfksh`, kann er die Befehle im Profil des Benutzers mit Berechtigung ausführen. In einer normalen Shell werden die Befehle nicht mit Berechtigung ausgeführt. Der privilegierte Prozess kann nur in einer privilegierten Shell ausgeführt werden.

Das Erweitern der ursprünglich vererbbaren Berechtigungssätze für Benutzer, Rollen oder Systeme ist eine riskantere Methode zum Zuweisen von Berechtigungen. Alle Berechtigungen im vererbbaren Satz befinden sich in den zugelassenen und effektiven Sätzen. Alle Befehle, die der Benutzer oder die Rolle in eine Shell eingibt, können die direkt zugewiesenen Berechtigungen verwenden. Direkt zugewiesene Berechtigungen ermöglichen einem Benutzer oder einer Rolle die einfache Ausführung von Vorgängen, die außerhalb der Grenzen ihrer administrativen Verantwortlichkeiten liegen können.

Wenn Sie etwas zum ursprünglichen vererbbaren Berechtigungssatz auf einem System hinzufügen, steht allen Benutzern, die sich beim System anmelden, ein größerer Satz grundlegender Berechtigungen zur Verfügung. Eine solche direkte Zuweisung ermöglicht allen Benutzern des Systems die einfache Ausführung von Vorgängen, die wahrscheinlich außerhalb der Grenzen gewöhnlicher Benutzer liegen.

Hinweis – Der begrenzte Satz kann nicht erweitert werden, da die ursprünglich festgelegte Begrenzung alle Berechtigungen umfasst.

Beschränken der Berechtigungen eines Benutzers oder einer Rolle

Durch das Entfernen von Berechtigungen können Sie verhindern, dass Benutzer und Rollen bestimmte Aufgaben ausführen. Sie können Berechtigungen aus dem ursprünglichen vererbbaren Satz und dem begrenzten Satz entfernen. Sie sollten das Entfernen von Berechtigungen vorsichtig testen, bevor Sie einen ursprünglichen vererbbaren Satz oder einen

begrenzten Satz verteilen, der kleiner als der Standardsatz ist. Durch das Entfernen von Berechtigungen aus dem ursprünglichen vererbbaren Satz können Sie Benutzer an der Anmeldung hindern. Wenn Berechtigungen aus dem begrenzten Satz entfernt werden, schlägt ein `setuid`-Legacy-Programm möglicherweise fehl, da das Programm eine Berechtigung erfordert, die entfernt wurde.

Zuweisen von Berechtigungen zu einem Skript

Skripten sind ebenso wie Befehle ausführbare Dateien. Daher können Sie in einem Berechtigungsprofil ebenso Berechtigungen zu einem Skript hinzufügen wie zu einem Befehl. Das Skript wird mit den hinzugefügten Berechtigungen ausgeführt, wenn ein Benutzer oder eine Rolle, dem/der das Profil zugewiesen wurde, das Skript in einer Profil-Shell ausführt. Wenn das Skript Befehle enthält, die Berechtigungen erfordern, sollten sich die Befehle mit hinzugefügten Berechtigungen ebenfalls im Profil befinden.

Berechtigungen erkennende Programme können Berechtigungen pro Prozess beschränken. Ihre Aufgabe mit einem Berechtigungen erkennenden Programm besteht darin, der ausführbaren Datei nur die Berechtigungen zuzuweisen, die das Programm benötigt. Anschließend testen Sie das Programm, um sicherzustellen, dass es seine Aufgaben erfolgreich ausführt. Sie müssen auch prüfen, dass das Programm seine Berechtigungen nicht missbraucht.

Berechtigungen und Geräte

Das Berechtigungsmodell verwendet Berechtigungen zum Schutz von Systemschnittstellen, die allein durch Dateiberechtigungen im Superuser-Modell geschützt werden. In einem System mit Berechtigungen sind Dateiberechtigungen zu schwach, um die Schnittstellen zu schützen. Eine Berechtigung wie `proc_owner` könnte Dateiberechtigungen überschreiben und vollen Zugriff auf das gesamte System gewähren.

Daher reicht die Eigentümerschaft des Geräteverzeichnisses nicht zum Öffnen eines Geräts aus. So dürfen beispielsweise Elemente der Gruppe `sys` nicht mehr automatisch das Gerät `/dev/ip` öffnen. `/dev/ip` hat die Dateiberechtigungen `0666`, aber es wird die Berechtigung `net_rawaccess` wird benötigt, um das Gerät zu öffnen.

Die Geräterichtlinie wird von Berechtigungen gesteuert. Der Befehl `getdevpolicy` zeigt die Geräterichtlinie für jedes Gerät an. Der Gerätekonfigurationsbefehl `devfsadm` installiert die Geräterichtlinie. Der Befehl `devfsadm` verbindet Berechtigungssätze mit dem Befehl `open` zum Lesen und Schreiben auf bzw. von Geräten. Weitere Informationen finden Sie auf den Manpages `getdevpolicy(1M)` und `devfsadm(1M)`.

Die Geräterichtlinie ermöglicht höhere Flexibilität durch Gewähren von Berechtigungen zum Öffnen von Geräten. Sie können andere oder mehr Berechtigungen als von der Standardgeräterichtlinie vorgesehen anfordern. Die Berechtigungsanforderungen können für die Geräterichtlinie und den Treiber entsprechend geändert werden. Sie können die Berechtigungen beim Installieren, Hinzufügen oder Aktualisieren eines Gerätetreibers ändern.

Mit den Befehlen `add_drv` und `update_drv` können Geräterichtlinieneinträge und treiberspezifische Berechtigungen geändert werden. Sie müssen einen Prozess mit dem vollständigen Berechtigungssatz ausführen, um die Geräterichtlinie zu ändern. Weitere Informationen finden Sie auf den Manpages `add_drv(1M)` und `update_drv(1M)`.

Berechtigungen und Fehlersuche

Oracle Solaris bietet Tools zur Fehlersuche beim Fehlschlagen von Berechtigungen. Die Befehle `ppriv` und `truss` bieten eine Fehlersuchausgabe. Beispiele hierzu finden Sie auf der Manpage `ppriv(1)`. Ein Beispiel für ein Verfahren finden Sie unter „So legen Sie die für ein Programm erforderlichen Berechtigungen fest“ auf Seite 268.

◆ ◆ ◆ KAPITEL 9

Rollenbasierte Zugriffssteuerung (Aufgaben)

In diesem Kapitel werden die Aufgaben beschrieben, die zur Verteilung der Superuser-Funktionen auf unterschiedliche Rollen ausgeführt werden müssen. Zu den Mechanismen, die von Rollen verwendet werden können, gehören Berechtigungsprofile, Autorisierungen und Berechtigungen. Im Folgenden sind die Übersichten der Schritte in diesem Kapitel aufgeführt.

- „Verwenden von RBAC (Übersicht der Schritte)“ auf Seite 213
- „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214
- „Verwenden von Rollen (Übersicht der Schritte)“ auf Seite 229
- „Verwalten von RBAC (Übersicht der Schritte)“ auf Seite 233

Eine Übersicht zur rollenbasierten Zugriffssteuerung (Role-based Access Control, RBAC) finden Sie unter „Rollenbasierte Zugriffssteuerung (Übersicht)“ auf Seite 190. Weitere Informationen finden Sie in Kapitel 10, „Rollenbasierte Zugriffssteuerung (Übersicht)“. Informationen zu Berechtigungen mit oder ohne RBAC finden Sie in Kapitel 11, „Berechtigungen (Aufgaben)“.

Verwenden von RBAC (Übersicht der Schritte)

RBAC erfordert sorgfältige Planung und Konfiguration, sowie Kenntnisse zur Annahme einer Rolle. Sobald Sie mit Rollen vertraut sind, können Sie RBAC weiter abwandeln und an neue Vorgänge anpassen. Die folgende Übersicht der Schritte enthält Verweise auf diese wichtigen Aufgaben.

Aufgabe	Beschreibung	Anweisungen
Planen und Konfigurieren von RBAC	Konfigurieren Sie RBAC an Ihrem Standort.	„Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214

Aufgabe	Beschreibung	Anweisungen
Benutzerrollen	Nehmen Sie Rollen an, indem Sie die Befehlszeile und Solaris Management Console-GUI verwenden.	„Verwenden von Rollen (Übersicht der Schritte)“ auf Seite 229
Anpassen von RBAC	Passen Sie RBAC für Ihren Standort an.	„Verwalten von RBAC (Übersicht der Schritte)“ auf Seite 233

Konfigurieren von RBAC (Übersicht der Schritte)

Die effiziente Verwendung von RBAC erfordert sorgfältige Planung. Die folgende Übersicht der Schritte hilft Ihnen bei der Planung und Implementierung von RBAC an Ihrem Standort.

Aufgabe	Beschreibung	Anweisungen
1. Planen von RBAC	Umfasst das Feststellen der Sicherheitsanforderungen an Ihrem Standort und die Entscheidung, wie RBAC verwendet werden soll	„So planen Sie die RBAC-Implementierung“ auf Seite 215
2. Erlernen der Verwendung der Solaris Management Console	Umfasst das Kennenlernen der Solaris Management Console	Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*
3. Konfigurieren des ersten Benutzers und der ersten Rolle	Umfasst das Erstellen eines Benutzers und einer Rolle sowie die Zuweisung der Rolle zum Benutzer mit den RBAC-Konfigurationstools in der Solaris Management Console	„Using the Solaris Management Tools With RBAC (Task Map)“ in *System Administration Guide: Basic Administration*
4. (Optional) Erstellen anderer Benutzer, die Rollen annehmen können	Stellt sicher, dass Benutzer, die administrative Rollen annehmen können, vorhanden sind	„Using the Solaris Management Tools With RBAC (Task Map)“ in *System Administration Guide: Basic Administration*
5. (Empfohlen) Erstellen anderer Rollen und Zuweisen dieser Rollen zu Benutzern	Umfasst das Erstellen von Rollen für bestimmte administrative Bereiche und das Zuweisen dieser Rollen zu Benutzern mit den RBAC-Tools	„So können Sie eine Rolle mit der GUI erstellen und zuweisen“ auf Seite 218
		Beispiel 9–5
	Umfasst die Erstellung und Zuweisung von Rollen zu Benutzern über die Befehlszeile	„So erstellen Sie eine Rolle über die Befehlszeile“ auf Seite 221
		„So weisen Sie eine Rolle einem lokalen Benutzer zu“ auf Seite 224
6. (Empfohlen) Prüfen von Rollenaktionen	Umfasst die Vorauswahl einer Prüfklasse, die das Prüfereignis zur Aufzeichnung der Rollenaktionen enthält	„So prüfen Sie Rollen“ auf Seite 225

Aufgabe	Beschreibung	Anweisungen
7. (Optional) Erstellen einer Rolle für den `root`-Benutzer	Verhindert anonyme `root`-Anmeldungen, die eine Sicherheitslücke darstellen	„So wandeln Sie den `root`-Benutzer in eine Rolle um“ auf Seite 226

Konfigurieren von RBAC

RBAC kann mit den folgenden Dienstprogrammen konfiguriert werden:

- **Solaris Management Console-GUI**: Mit RBAC verbundene Aufgaben sollten bevorzugt über die GUI ausgeführt werden. Die Konsolen-Tools zur Verwaltung von RBAC-Elementen sind in der "User Tool Collection" enthalten.
- **Solaris Management Console-Befehle**: Mit den Solaris Management Console-Befehlszeilenschnittstellen wie z. B. `smrole` können Sie Vorgänge für jeden Name Service ausführen. Die Solaris Management Console-Befehle erfordern eine Authentifizierung, um eine Verbindung zum Server herzustellen. Daher eignen sich diese Befehle nicht besonders gut für Skripten.
- **Lokale Befehle**: Mit den Befehlszeilenschnittstellensätzen `user*` und `role*`, zu denen beispielsweise auch `useradd` zählt, können Sie nur lokale Dateien bearbeiten. Die Befehle zur Bearbeitung lokaler Dateien müssen vom Superuser oder einer Rolle mit den geeigneten Berechtigungen ausgeführt werden.

▼ So planen Sie die RBAC-Implementierung

RBAC kann ein wesentlicher Teil der Informationsressourcen-Verwaltung eines Unternehmens sein. Für die Planung müssen Sie sowohl mit den Fähigkeiten von RBAC vertraut sein als auch die Sicherheitsanforderungen Ihres Unternehmens kennen.

1 Erlernen Sie die grundlegenden RBAC-Konzepte.

Lesen Sie die Informationen unter „Rollenbasierte Zugriffssteuerung (Übersicht)“ auf Seite 190. Die Verwendung von RBAC zur Verwaltung eines Systems unterscheidet sich wesentlich von herkömmlichen UNIX-Administrationspraktiken. Sie sollten sich vor der Implementierung mit RBAC-Konzepten vertraut machen. Weitere Informationen finden Sie in Kapitel 10, „Rollenbasierte Zugriffssteuerung (Übersicht)“.

2 Untersuchen Sie die Sicherheitsrichtlinien Ihres Unternehmens.

Diese sollten nähere Informationen zu den potenziellen Bedrohungen des Systems, wie hoch das Risiko der einzelnen Bedrohungen ist und eine Strategie zur Bekämpfung dieser Bedrohungen enthalten. Die Isolierung der sicherheitsrelevanten Aufgaben durch RBAC kann Teil der Strategie sein. Auch wenn Sie die empfohlenen Rollen und ihre Konfigurationen unverändert installieren können, müssen Sie möglicherweise Ihre RBAC-Konfiguration zur Einhaltung Ihrer Sicherheitsrichtlinien anpassen.

3 Legen Sie den Umfang von RBAC für Ihr Unternehmen fest.

Abhängig von Ihren Sicherheitsanforderungen können Sie verschiedene RBAC-Stufen einsetzen:

- **Kein RBAC**: Sie können alle Aufgaben als `root`-Benutzer ausführen. Bei dieser Konfiguration melden Sie sich mit Ihrem eigenen Benutzernamen an. Dann geben Sie `root` als Benutzer ein, wenn Sie ein Solaris Management Console-Tool auswählen.
- **Nur eine Rolle**: Bei dieser Methode wird eine Rolle hinzugefügt. Der Rolle wird das Berechtigungsprofil "Primary Administrator" zugewiesen. Diese Methode ist dem Superuser-Modell ähnlich, da die Rolle über Superuser-Fähigkeiten verfügt. Mit dieser Methode können Sie jedoch nachverfolgen, wer die Rolle angenommen hat.
- **Empfohlene Rollen**: Bei dieser Methode werden drei Rollen erstellt, die auf den Berechtigungsprofilen "Primary Administrator", "System Administrator" und "Operator" basieren. Die Rollen sind für Unternehmen geeignet, in denen es Administratoren mit verschiedenen Stufen der Verantwortung gibt.
- **Angepasste Rollen**: Sie können eigene Rollen erstellen, entsprechend den Sicherheitsanforderungen Ihres Unternehmens. Die neuen Rollen können auf vorhandenen oder angepassten Berechtigungsprofilen basieren. Informationen zur Anpassung von Berechtigungsprofilen, um eine Aufgabentrennung durchzusetzen, finden Sie unter „Creating Roles and Users in Trusted Extensions“ in *Oracle Solaris Trusted Extensions Configuration Guide*.
- **Root-Benutzer als Rolle**: Diese Methode verhindert, dass sich Benutzer als `root` anmelden. Sie müssen sich stattdessen zuerst als normale Benutzer anmelden, und dann die `root`-Rolle annehmen. Informationen finden Sie unter „So wandeln Sie den `root`-Benutzer in eine Rolle um“ auf Seite 226.

4 Entscheiden Sie, welche empfohlenen Rollen für Ihr Unternehmen geeignet sind.

Überprüfen Sie die Fähigkeiten der empfohlenen Rollen und der Standardberechtigungsprofile. Standardberechtigungsprofile ermöglichen Administratoren, eine empfohlene Rolle mithilfe eines einzelnen Profils zu konfigurieren.

Drei Standardberechtigungsprofile sind zur Konfiguration der empfohlenen Rollen verfügbar:

- **Berechtigungsprofil "Primary Administrator"**: Zur Konfiguration einer Rolle, die alle administrativen Aufgaben ausführt, anderen Personen Berechtigungen gewährt und mit administrativen Rollen verbundene Berechtigungen bearbeiten kann. Ein Benutzer mit dieser Rolle kann anderen Benutzern diese Rolle sowie Berechtigungen zuweisen.
- **Berechtigungsprofil "System Administrator"**: Zur Konfiguration einer Rolle, die die meisten administrativen Aufgaben ausführen kann, die sich nicht auf die Sicherheit beziehen. Beispielsweise kann die Rolle "System Administrator" neue Benutzerkonten hinzufügen, jedoch keine Passwörter einstellen und auch anderen keine Berechtigungen gewähren.

- **Berechtigungsprofil "Operator"**: Zur Konfiguration einer Rolle, die einfache administrative Aufgaben ausführen kann, wie z. B. Datenträger-Backup und Druckerverwaltung.

Weitere Informationen zu Berechtigungsprofilen finden Sie hier:

- Sehen Sie sich im Verzeichnis `/etc/security` den Inhalt der Datenbanken `prof_attr` und `exec_attr` an.
- Zeigen Sie in der Solaris Management Console mit dem Tool "Rights" (Berechtigungen) den Inhalt eines Berechtigungsprofils an.
- In diesem Dokument finden Sie unter „Inhalt der Berechtigungsprofile“ auf Seite 247 Zusammenfassungen typischer Berechtigungsprofile.

5 Entscheiden Sie, ob zusätzliche Rollen oder Berechtigungsprofile für Ihr Unternehmen definiert werden müssen.

Suchen Sie nach anderen Anwendungen und Anwendungsfamilien an Ihrem Standort, für die ein beschränkter Zugriff vorteilhaft wäre. RBAC empfiehlt sich bei Anwendungen, die sich auf die Sicherheit auswirken und Denial-of-Service-Probleme verursachen können oder spezielle Administratorkenntnisse erfordern. Sie können Rollen und Berechtigungsprofile an die Sicherheitsanforderungen Ihres Unternehmens anpassen.

a. Legen Sie fest, welche Befehle für die neue Aufgabe erforderlich sind.

b. Entscheiden Sie, welche Berechtigungsprofile für diese Aufgabe geeignet sind.

Überprüfen Sie, ob ein vorhandenes Berechtigungsprofil für diese Aufgabe geeignet ist oder ein separates Berechtigungsprofil erstellt werden muss.

c. Legen Sie fest, welche Rolle für dieses Berechtigungsprofil geeignet ist.

Entscheiden Sie, ob das Berechtigungsprofil für diese Aufgabe einer vorhandenen Rolle zugewiesen werden muss oder eine neue Rolle erstellt werden muss. Wenn Sie eine vorhandene Rolle verwenden, überprüfen Sie, ob andere Berechtigungsprofile für Benutzer geeignet sind, die dieser Rolle zugewiesen sind.

6 Entscheiden Sie, welche Benutzer den verfügbaren Rollen zugewiesen werden sollen.

Nach dem Prinzip der geringsten Berechtigung sollten Sie Benutzern Rollen zuweisen, die ihren Vertraulichkeitsstufen entsprechen. Sie vermeiden unnötige Probleme, indem Sie Benutzern keinen Zugriff auf Aufgaben geben, die sie nicht ausführen müssen.

▼ So können Sie eine Rolle mit der GUI erstellen und zuweisen

Als Superuser oder mit der Rolle "Primary Administrator" können Sie eine neue Rolle erstellen. Bei diesem Verfahren hat der Ersteller der neuen Rolle die Rolle "Primary Administrator" angenommen.

Bevor Sie beginnen

- Sie haben bereits Benutzer erstellt, die diese Rolle an Ihrem Standort annehmen können. Wenn Sie noch keine Benutzer erstellt haben, führen Sie diesen Vorgang durch, indem Sie den Anweisungen unter „Using the Solaris Management Tools With RBAC (Task Map)“ in *System Administration Guide: Basic Administration* folgen.
- Ihnen wurde die Rolle "Primary Administrator" zugewiesen, indem die Verfahren unter „Using the Solaris Management Tools With RBAC (Task Map)“ in *System Administration Guide: Basic Administration* durchgeführt wurden.

1 Starten Sie die Solaris Management Console.

```
# /usr/sbin/smc &
```

Eine Anleitung zum Anmelden finden Sie unter „So nehmen Sie eine Rolle in der Solaris Management Console an“ auf Seite 232.

2 Klicken Sie auf das Symbol "Administrative Roles" (Administrative Rollen).

3 Wählen Sie im Menü "Action" (Aktion) den Befehl "Add Administrative Role" (Administrative Rollen hinzufügen).

4 Erstellen Sie eine neue Rolle, indem Sie eine Reihe von Dialogfeldern ausfüllen.

Mögliche Rollen finden Sie in Beispiel 9–1 bis Beispiel 9–4.

Tipp – Alle Tools in der Solaris Management Console zeigen Informationen im unteren Seitenbereich oder auf der linken Seite des Assistentenfensters an. Sie können in dieser Schnittstelle jederzeit die Hilfefunktion aufrufen, um zusätzliche Informationen zur Durchführung von Aufgaben zu erhalten.

---

5 Weisen Sie die Rolle einem Benutzer zu.

Tipp – Nachdem Sie die Eigenschaften der Rolle festgelegt haben, werden Sie im letzten Dialogfeld aufgefordert, der Rolle einen Benutzer zuzuweisen.

---

6 Starten Sie den Name Service-Cache-Dämon in einem Terminalfenster neu.

```
# svcadm restart system/name-service-cache
```

Weitere Informationen finden Sie auf den Manpages `svcadm(1M)` und `nscd(1M)`.

Beispiel 9–1 Erstellen einer Rolle für das Berechtigungsprofil "System Administrator"

In diesem Beispiel kann die neue Rolle Systemverwaltungsaufgaben ausführen, die sich nicht auf die Sicherheit beziehen. Die Rolle wird erstellt, indem das vorhergehende Verfahren mit den folgenden Parametern ausgeführt wird:

- Rollenname: `sysadmin`
- Vollständiger Rollenname: `System Administrator`
- Rollenbeschreibung: `Performs non-security admin tasks`
- Berechtigungsprofil: `System Administrator`

  Dieses Berechtigungsprofil befindet sich an oberster Stelle in der Liste der Profile, die in der Rolle enthalten sind.

Beispiel 9–2 Erstellen einer Rolle für das Berechtigungsprofil "Operator"

Das Berechtigungsprofil "Operator" enthält Berechtigungen zum Verwalten von Druckern und Backup des Systems auf Offline-Datenträgern. Diese Rolle können Sie einem Benutzer pro Schicht zuweisen. Dazu wählen Sie im Dialogfeld "Step 1: Enter a Role Name" (Schritt 1: Rollennamen eingeben) die Option für die Rollenverteilerliste aus. Die Rolle wird erstellt, indem das vorhergehende Verfahren mit den folgenden Parametern ausgeführt wird:

- Rollenname: `operadm`
- Vollständiger Rollenname: `Operator`
- Rollenbeschreibung: `Backup operator`
- Berechtigungsprofil: `Operator`

  Dieses Berechtigungsprofil muss sich an oberster Stelle in der Liste der Profile befinden, die in der Rolle enthalten sind.

Beispiel 9–3 Erstellen einer Rolle für ein sicherheitsbezogenes Berechtigungsprofil

Standardmäßig bietet nur das Profil "Primary Administrator" sicherheitsbezogene Befehle und Berechtigungen. Wenn Sie eine Rolle benötigen, die über weniger Berechtigungen als die Rolle "Primary Administrator" verfügt, jedoch einige sicherheitsbezogene Aufgaben ausführen kann, müssen Sie die Rolle erstellen.

Mit der Rolle in dem folgenden Beispiel werden Geräte geschützt. Die Rolle wird erstellt, indem das vorhergehende Verfahren mit den folgenden Parametern ausgeführt wird:

- Rollenname: `devicesec`
- Vollständiger Rollenname: `Device Security`
- Rollenbeschreibung: `Configures Devices`
- Berechtigungsprofil: `Device Security`

Mit der Rolle in dem folgenden Beispiel werden Systeme und Hosts im Netzwerk geschützt. Die Rolle wird erstellt, indem das vorhergehende Verfahren mit den folgenden Parametern ausgeführt wird:

- Rollenname: `netsec`
- Vollständiger Rollenname: `Network Security`
- Rollenbeschreibung: `Handles IPsec, IKE, and SSH`
- Berechtigungsprofil: `Network Security`

Beispiel 9–4 Erstellen einer Rolle für ein Berechtigungsprofil mit einem beschränkten Bereich

Eine Reihe von Berechtigungsprofilen verfügen über einen beschränkten Bereich. In diesem Beispiel besteht die einzige Aufgabe der Rolle in der Verwaltung von DHCP. Die Rolle wird erstellt, indem das vorhergehende Verfahren mit den folgenden Parametern ausgeführt wird:

- Rollenname: `dhcpmgt`
- Vollständiger Rollenname: `DHCP Management`
- Rollenbeschreibung: `Manages Dynamic Host Config Protocol`
- Berechtigungsprofil: `DHCP Management`

Beispiel 9–5 Ändern der Rollenzuweisung eines Benutzers

In diesem Beispiel wird eine Rolle einem vorhandenen Benutzer hinzugefügt. Sie können die Rollenzuweisung eines Benutzers ändern, indem Sie in der Solaris Management Console im Tool "Users" (Benutzer) auf das Symbol "User Accounts" (Benutzerkonten) klicken, auf den Benutzer doppelklicken und die Anweisungen in der Onlinehilfe zum Hinzufügen einer Rolle zu den Benutzerfähigkeiten befolgen.

Allgemeine Fehler

Überprüfen Sie Folgendes, wenn die Rolle nicht die gewünschten Fähigkeiten aufweist:

- Werden die Berechtigungsprofile der Rolle in der GUI vom stärksten bis zum schwächsten aufgeführt?

  Wenn beispielsweise das Berechtigungsprofil `All` sich in der Liste an erster Stelle befindet, werden keine Befehle mit Sicherheitsattributen ausgeführt. Ein Profil, das Befehle mit Sicherheitsattributen enthält, muss in der Liste vor dem Berechtigungsprofil `All` aufgeführt werden.

- Verfügen die Befehle in den Berechtigungsprofilen der Rolle über geeignete Sicherheitsattribute?

  Für die Richtlinie `suser` benötigen beispielsweise einige Befehle `uid=0` statt `euid=0`.

- Wurde das Berechtigungsprofil in dem geeigneten Name Service-Bereich definiert? Funktioniert die Rolle in dem Name Service-Bereich, in dem das Berechtigungsprofil definiert wurde?

- Wurde der Name Service-Cache `svc:/system/name-service-cache` neu gestartet?

Der Dämon `nscd` kann über eine längere Aktivitätszeit verfügen. Durch einen Neustart des Dämons wird der Name Service mit den neuesten Daten aktualisiert.

▼ So erstellen Sie eine Rolle über die Befehlszeile

Die Solaris Management Console-GUI ist die bevorzugte Methode zur Verwaltung von RBAC. Informationen zur Verwendung der GUI finden Sie unter „So können Sie eine Rolle mit der GUI erstellen und zuweisen“ auf Seite 218. Sie können auch die Befehlszeilenschnittstelle verwenden, wie in diesem Verfahren beschrieben.

Hinweis – Versuchen Sie nicht, RBAC über die Befehlszeile und die grafische Benutzeroberfläche gleichzeitig zu verwalten. Dies könnte zu widersprüchlichen Änderungen an der Konfiguration und zu unvorhergesehenem Verhalten führen. Sie können beide Tools zur Verwaltung von RBAC verwenden, jedoch nicht gleichzeitig.

Bevor Sie beginnen Um eine Rolle zu erstellen, müssen Sie entweder eine Rolle annehmen, die das Berechtigungsprofil "Primary Administrator" enthält, oder zum Benutzer `root` wechseln.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Wählen Sie einen der folgenden Befehle aus, um eine Rolle über die Befehlszeile zu erstellen.

- **Für Rollen im Bereich des lokalen Name Service verwenden Sie den Befehl `roleadd`.**

Hinweis – Der Befehl `roleadd` unterliegt mehr Beschränkungen als die Solaris Management Console-GUI oder die Befehlszeilenschnittstellen. Im Anschluss an den Befehl `roleadd` müssen Sie den Befehl `usermod` ausführen, um die Rolle einem Benutzer zuzuweisen. Außerdem muss der Benutzer ein Passwort für die Rolle festlegen, wie unter „So weisen Sie eine Rolle einem lokalen Benutzer zu“ auf Seite 224 gezeigt.

```
# roleadd -c comment \
-g group -m homedir -u UID -s shell \
-P profile rolename
```

`-c` *comment*	Kommentar zur Beschreibung von *rolename*
`-g` *group*	Gruppenzuweisung für *rolename*
`-m` *homedir*	Pfad zum Home-Verzeichnis für *rolename*

`-u` *UID*	UID für *rolename*
`-s` *shell*	Anmelde-Shell für *rolename*. Diese Shell muss eine Profil-Shell sein.
`-P` *profile*	Mindestens ein Berechtigungsprofil für *rolename*
rolename	Name der neuen lokalen Rolle

- **Verwenden Sie den Befehl `smrole add`.**

  Dieser Befehl erstellt eine Rolle in einem verteilten Name Service wie NIS, NIS+ oder LDAP. Dieser Befehl wird als Client des Solaris Management Console-Servers ausgeführt.

  ```
  $ /usr/sadm/bin/smrole -D domain-name \
  -r admin-role -l <Type admin-role password> \
  add -- -n rolename -a rolename -d directory\
  -F full-description -p profile
  ```

`-D` *domain-name*	Name der zu ändernden Domain
`-r` *admin-role*	Name der administrativen Rolle, von der die Rolle geändert werden kann. Die administrative Rolle muss über die Autorisierung `solaris.role.assign` verfügen. Wenn Sie Ihre angenommene Rolle ändern, muss die Rolle über die Autorisierung `solaris.role.delegate` verfügen.
`-l`	Eingabeaufforderung für das Passwort von *admin-role*
`--`	Trennzeichen zwischen Authentifizierungsoptionen und Unterbefehlsoptionen
`-n` *rolename*	Name der neuen Rolle
`-c` *comment*	Kommentar, der die Fähigkeiten der Rolle beschreibt
`-a` *username*	Name des Benutzers, der *rolename* annehmen kann
`-d` *directory*	Home-Verzeichnis für *rolename*
`-F` *full-description*	Vollständige Beschreibung für *rolename*. Diese Beschreibung wird in der Solaris Management Console-GUI angezeigt.
`-p` *profile*	Berechtigungsprofil, das in den Fähigkeiten von *rolename* enthalten ist. Diese Option stellt Befehle mit administrativen Fähigkeiten für die Rolle zur Verfügung. Sie können mehrere Optionen des Typs `-p` *profile* angeben.

3. **Damit die Änderungen wirksam werden, führen Sie die Anweisungen unter „So weisen Sie eine Rolle einem lokalen Benutzer zu“ auf Seite 224 aus.**

Beispiel 9–6 Erstellen der Rolle "Custom Operator" mit dem Befehl `smrole`

Der Befehl `smrole` gibt eine neue Rolle und ihre Attribute in einem Name Service an. In dem folgenden Beispiel wird mit der Rolle "Primary Administrator" eine neue Version der Rolle "Media Backup" erstellt. Die Rolle schließt das Standardberechtigungsprofil "Media Backup" und das Berechtigungsprofil "FTP Management" ein. Beachten Sie, dass Sie aufgefordert werden, ein Passwort für die neue Rolle einzugeben.

```
% su - primaryadm
Password:      <Type primaryadm password>
$ /usr/sadm/bin/smrole add -H myHost -- -c "FTP and Backup Operator" \
-n operadm2 -a janedoe -d /export/home/operadm \
-F "Backup/FTP Operator" -p "Media Backup" -p "FTP Management"
Authenticating as user: primaryadm

Type /? for help, pressing <enter> accepts the default denoted by [ ]
Please enter a string value for: password ::     <Type primaryadm password>

Loading Tool: com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost
Login to myHost as user primaryadm was successful.
Download of com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost was successful.

Type /? for help, pressing <enter> accepts the default denoted by [ ]
Please enter a string value for: password ::    <Type operadm2 password>

$ svcadm restart system/name-service-cache
```

Der Befehl `smrole` mit dem Unterbefehl `list` zeigt die neue Rolle an:

```
$ /usr/sadm/bin/smrole list --
Authenticating as user: primaryadm

Type /? for help, pressing <enter> accepts the default denoted by [ ]
Please enter a string value for: password ::     <Type primaryadm password>

Loading Tool: com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost
Login to myHost as user primaryadm was successful.
Download of com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost was successful.
root                    0            Superuser
primaryadm            100            Most powerful role
sysadmin              101            Performs non-security admin tasks
operadm               102            Backup Operator
operadm2              103            Backup/FTP Operator
```

Beachten Sie, dass Berechtigungsprofile, die "Media Backup" oder "Media Restore" enthalten, dazu führen, dass die Rolle über Zugriff auf das gesamte Root-Dateisystem verfügt. Daher muss der Administrator diese Berechtigungsprofile vertrauenswürdigen Benutzern zuweisen.

Alternativ kann der Administrator auch darauf verzichten, diese Berechtigungsprofile zuzuweisen. In diesem Fall kann nur der Superuser Backups und Wiederherstellungen durchführen.

▼ So weisen Sie eine Rolle einem lokalen Benutzer zu

Mit diesem Verfahren wird einem lokalen Benutzer eine lokale Rolle zugewiesen und der Name Service-Cache-Dämon neu gestartet. Dann wird gezeigt, wie der Benutzer die Rolle annehmen kann.

Informationen zum Zuweisen einer Rolle zu einem Benutzer in einem verteilten Name Service finden Sie unter „So erstellen Sie eine Rolle über die Befehlszeile“ auf Seite 221 und „So ändern Sie die Eigenschaften einer Rolle“ auf Seite 236.

Bevor Sie beginnen Sie haben eine lokale Rolle, wie in „So erstellen Sie eine Rolle über die Befehlszeile“ auf Seite 221 beschrieben, hinzugefügt. Sie müssen entweder eine Rolle annehmen, die das Berechtigungsprofil "Primary Administrator" enthält, oder zum Benutzer `root` wechseln.

1. **Weisen Sie die Rolle einem lokalen Benutzer zu.**

   Wenn Sie eine lokale Rolle mit dem Befehl `roleadd` hinzugefügt haben, ist dieser Schritt erforderlich. Dieser Schritt ist optional, wenn Sie die Rolle mit dem Befehl `smrole` und der Solaris Management Console erstellt haben.

   ```
   # usermod -u UID -R rolename login-name
   ```

`-u` *UID*	UID des Benutzers
`-R` *rolename*	Rolle, die dem Benutzer zugewiesen wird
login-name	Anmeldename des Benutzers

2. **Damit die Änderungen angewendet werden, starten Sie den Name Service-Cache-Dämon neu.**

   ```
   # svcadm restart system/name-service-cache
   ```

   Wenn Sie eine Rolle mit einer Solaris Management Console-Schnittstelle hinzugefügt haben, gehen Sie wie unter „Verwenden von Rollen (Übersicht der Schritte)“ auf Seite 229 beschrieben vor. Andernfalls fahren Sie mit dem nächsten Schritt fort.

3. **(Optional) Um das Rollenkonto freizugeben, muss der Benutzer ein Passwort erstellen.**

   Wenn Sie eine lokale Rolle mit dem Befehl `roleadd` hinzugefügt haben, ist dieser Schritt erforderlich.

   ```
   % su - rolename
   Password:       <Type rolename password>
   Confirm Password:       <Retype rolename password>
   $
   ```

Beispiel 9–7 Erstellen und Zuweisen einer lokalen Rolle über die Befehlszeile

In diesem Beispiel wird eine Rolle zur Verwaltung von Oracle Solaris Cryptographic Framework erstellt. Das Berechtigungsprofil "Crypto Management" enthält den Befehl `cryptoadm` zur Verwaltung von kryptografischen Hardware- und Softwareservices auf einem lokalen System.

```
# roleadd -c "Cryptographic Services manager" \
-g 14 -m /export/home/cryptoadm -u 104 -s pfksh \
-P "Crypto Management" cryptomgt
# usermod -u 1111 -R cryptomgt
# svcadm restart system/name-service-cache
% su - cryptomgt
Password:      <Type cryptomgt password>
Confirm Password:      <Retype cryptomgt password>
$ /usr/ucb/whoami
cryptomgt
$
```

Informationen zu Oracle Solaris Cryptographic Framework finden Sie in Kapitel 13, „Oracle Solaris Cryptographic Framework (Übersicht)“. Informationen zur Verwaltung des Frameworks finden Sie unter „Verwalten von Cryptographic Framework (Übersicht der Schritte)“ auf Seite 309.

▼ So prüfen Sie Rollen

Die von einer Rolle durchgeführten Aktionen können geprüft werden. Der Prüfdatensatz enthält den Anmeldenamen des Benutzers, der die Rolle angenommen hat, den Rollennamen und die Aktion, die die Rolle durchgeführt hat. Die Informationen werden vom Prüfereignis `6180:AUE_prof_cmd:profile command:ua,as` erfasst. Durch Vorauswahl der Klassen `as` oder `ua` können Sie die Rollenaktionen prüfen.

1. **Planen Sie die Prüfung und bearbeiten Sie die Prüfkonfigurationsdateien.**

   Weitere Informationen finden Sie unter „Prüfung bei Oracle Solaris (Übersicht der Schritte)“ auf Seite 637.

2. **Nehmen Sie die Klasse `ua` oder die Klasse `as` in die `flags`-Zeile der Datei `audit_control` auf.**

   ```
   ## audit_control file
   flags:lo,as
   naflags:lo
   plugin:name=audit_binfile.so; p_dir=/var/audit
   ```

   Die Klassen `ua` oder `as` enthalten andere Prüfereignisse. Die in einer Klasse enthaltenen Prüfereignisse können Sie in der Datei `audit_event` anzeigen. Stattdessen können Sie auch den Befehl `bsmrecord` verwenden (siehe Beispiel 30–27).

3 **Schließen Sie die Konfiguration des Prüfservice ab und aktivieren Sie die Prüffunktion.**

Weitere Informationen finden Sie unter „Konfigurieren und Aktivieren des Prüfservice (Aufgaben)“ auf Seite 649.

▼ So wandeln Sie den `root`-Benutzer in eine Rolle um

In diesem Verfahren wird beschrieben, wie der `root` von einem Anmeldungsbenutzer in eine Rolle umgewandelt wird. Nach Abschluss dieses Verfahrens können Sie sich nicht mehr direkt beim System als `root` anmelden, es sei denn der Einzelbenutzermodus wird ausgeführt. Ihnen muss die `root`-Rolle zugewiesen sein und Sie müssen mit `su` zu `root` wechseln.

Durch Umwandeln des `root`-Benutzers in eine Rolle verhindern Sie anonyme `root`-Anmeldungen. Da ein Benutzer sich zuerst anmeldet und *dann* die `root`-Rolle annimmt, wird die Anmelde-ID des Benutzers an den Prüfservice übergeben und in der Datei `sulog` aufgezeichnet.

Mit diesem Verfahren erstellen Sie einen lokalen Benutzer und weisen ihm die `root`-Rolle zu. In Beispiel 9–8 wird beschrieben, wie Sie Benutzer daran hindern, die Rolle anzunehmen.

Bevor Sie beginnen Sie können dieses Verfahren nicht durchführen, wenn Sie direkt als `root` angemeldet sind. Sie müssen sich erst mit Ihrem Benutzernamen anmelden und dann mit `su` zu `root` wechseln.

1 **Melden Sie sich beim Zielsystem als gewöhnlicher Benutzer an.**

2 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie unter „Using the Solaris Management Tools With RBAC (Task Map)“ in *System Administration Guide: Basic Administration*.

3 **Erstellen Sie einen lokalen Benutzer, der die `root`-Rolle annehmen kann.**

Zur Sicherheit sollte mindestens einem lokalen Benutzer die `root`-Rolle zugewiesen werden.

`$ useradd -c` *comment* `-u` *uid* `-d` *homedir username*

`-c` *comment*	Kommentar zur Beschreibung des Benutzers
`-d` *homedir*	Home-Verzeichnis des Benutzers. Dieses Verzeichnis sollte sich auf dem lokalen System befinden.
`-u` *uid*	Benutzer-ID
username	Name des neuen lokalen Benutzers.

```
# useradd -c "JDoe's local account" -u 123 -d /export/home1 jdoe-local
```

4 Weisen Sie dem Benutzer ein Passwort zu.

```
# passwd -r files jdoe-local
New Password:          <Type password>
Re-enter new Password:      <Retype password>
passwd: password successfully changed for jdoe-local
#
```

5 Stellen Sie sicher, dass Sie nicht als `root` angemeldet sind.

```
# who
jdoe    console      May 24 13:51    (:0)
jdoe    pts/5        May 24 13:51    (:0.0)
jdoe    pts/4        May 24 13:51    (:0.0)
jdoe    pts/10       May 24 13:51    (:0.0)
```

6 Wandeln Sie den `root`-Benutzer in eine Rolle um.

```
# usermod -K type=role root
```

7 Stellen Sie sicher, dass `root` eine Rolle ist.

Der `root`-Eintrag in der Datei `user_attr` sollte etwa wie folgt aussehen:

```
# grep root /etc/user_attr
root::::type=role;auths=solaris.*,solaris.grant;profiles=...
```

8 Weisen Sie die `root`-Rolle Ihrem lokalen Konto zu.

```
# usermod -R root jdoe-local
```

Achtung – Wenn Sie die `root`-Rolle keinem Benutzer zuweisen, ist eine Anmeldung als Superuser nur noch im Einzelbenutzermodus möglich. Sie müssen ein Root-Passwort eingeben, um in den Einzelbenutzermodus zu wechseln.

9 Konfigurieren Sie den Name Service, zu dem im Falle eines Fehlers zurückgewechselt werden soll.

a. Öffnen Sie ein neues Terminalfenster und nehmen Sie die `root`-Rolle an.

```
% whoami
jdoe
% su - jdoe-local
Enter password:          <Type jdoe-local password>
% roles
root
% su - root
Enter password:          <Type root password>
#
```

b. Bearbeiten Sie die Datei `nsswitch.conf`.

Folgende Einträge in der Datei `nsswitch.conf` ermöglichen die Rückkehr des Name Service.

```
passwd:  files nis [TRYAGAIN=0 UNAVAIL=return NOTFOUND=return]
group:  files nis [TRYAGAIN=0 UNAVAIL=return NOTFOUND=return]
```

10 (Optional) Weisen Sie die `root`-Rolle den ausgewählten Benutzerkonten im Name Service zu.

Die Vorgehensweise wird unter „So ändern Sie die RBAC-Eigenschaften eines Benutzers“ auf Seite 241 beschrieben.

Beispiel 9–8 Verhindern der Konfiguration eines Systems mit der `root`-Rolle

In diesem Beispiel erfordert eine Standortsicherheitsrichtlinie, dass das System durch mehrere unterschiedliche Rollen konfiguriert wird. Diese unterschiedlichen Rollen wurden erstellt und getestet. Damit das `root`-Konto nicht zur Konfiguration des Systems verwendet wird, wandelt der Sicherheitsadministrator `root` in eine Rolle um, weist diese jedoch nicht zu. Die `root`-Rolle enthält ein Passwort, um das System im Einzelbenutzermodus zu verwenden.

Zunächst überprüft der Administrator, dass `root` keine zugewiesene Rolle ist.

```
% whoami
jdoe-local
% su - root
Password: a!2@3#4$5%6^7
# grep roles /etc/user_attr
jdoe-local::::type=normal;roles=secadmin
kdoe-local::::type=normal;roles=sysadmin
```

Ohne das `root`-Konto zu verlassen, wandelt der Administrator `root` in eine Rolle um.

```
# usermod -K type=role root
```

Dann überprüft der Administrator die Änderung im `root`-Eintrag in der Datei `user_attr`.

```
# grep root /etc/user_attr
root::::type=role;auths=solaris.*,solaris.grant;profiles=...
```

Beispiel 9–9 Umwandeln der `root`-Rolle in einen `root`-Benutzer

In diesem Beispiel setzt der Administrator das System außer Betrieb und möchte sich beim Desktop als Superuser anmelden. Das System wurde vom Netzwerk getrennt.

Zuerst nimmt der Administrator die `root`-Rolle an, um alle `root`-Rollenzuweisungen zu entfernen.

```
% whoami
jdoe-local
```

```
% su - root
Password: a!2@3#4$5%6^7
# grep roles /etc/user_attr
jdoe-local::::type=normal;roles=root
kdoe-local::::type=normal;roles=root
# usermod -R "" jdoe-local
# usermod -R "" kdoe-local
# grep roles /etc/user_attr
#
```

Ohne die root-Rolle zu verlassen, wandelt der Administrator root in einen Benutzer um.

```
# rolemod -K type=normal root
```

Dann überprüft der Administrator die Änderung im root-Eintrag in der Datei user_attr.

```
# grep root /etc/user_attr
root::::type=normal;auths=solaris.*,solaris.grant;profiles=...
```

Allgemeine Fehler

In einer Desktop-Umgebung können Sie sich nicht direkt als root anmelden, wenn root als Rolle definiert ist. Eine diagnostische Meldung gibt an, dass root eine Rolle auf Ihrem System ist. Wenn kein lokales Konto die root-Rolle annehmen kann, müssen Sie eines erstellen. Melden Sie sich im Einzelbenutzermodus als root beim System an, erstellen Sie ein lokales Benutzerkonto und weisen Sie dem neuen Konto die root-Rolle zu. Melden Sie sich als neuer Benutzer an und nehmen Sie die root-Rolle an.

Es ist keine Anmeldung als Superuser möglich, wenn Sie den root-Benutzer in eine Rolle umwandeln und nicht folgende Zuweisungen vornehmen:

- Zuweisen der root-Rolle zu einem gültigen Benutzer
- Zuweisen eines Berechtigungsprofils, das dem root-Berechtigungsprofil entspricht, zu einem gültigen Benutzer. Das Profil "Primary Administrator" entspricht dem root-Berechtigungsprofil.
- Erstellen Sie eine Rolle mit root-Fähigkeiten und weisen Sie diese einem gültigen Benutzer zu. Eine Rolle, der das Profil "Primary Administrator" zugewiesen ist, entspricht der root-Rolle.

Verwenden von Rollen (Übersicht der Schritte)

In der folgenden Übersicht der Schritte wird auf Verfahren zur Verwendung einer Rolle verwiesen, nachdem die Rollen zugewiesen wurden.

Aufgabe	Beschreibung	Anweisungen
Verwenden der Solaris Management Console	Melden Sie sich mit einer Rolle zum Ausführen administrativer Aufgaben in der Solaris Management Console an.	„So nehmen Sie eine Rolle in der Solaris Management Console an“ auf Seite 232
Annehmen einer Rolle in einem Terminalfenster	Führen Sie administrative Aufgaben über die Befehlszeile in einer Profil-Shell aus.	„So nehmen Sie eine Rolle in einem Terminalfenster an“ auf Seite 230

Verwenden von Rollen

Nachdem Sie die Rollen mit den Oracle Solaris-Standardberechtigungsprofilen eingerichtet und Benutzern zugewiesen haben, können die Rollen verwendet werden. Eine Rolle kann über die Befehlszeile angenommen werden. In der Solaris Management Console kann eine Rolle auch zur lokalen Systemverwaltung und über das Netzwerk angenommen werden.

▼ So nehmen Sie eine Rolle in einem Terminalfenster an

Bevor Sie beginnen Die Rolle muss Ihnen bereits zugewiesen sein. Der Name Service muss mit diesen Informationen aktualisiert werden.

1 In einem Terminalfenster können Sie feststellen, welche Rollen Sie annehmen können.

```
% roles
Comma-separated list of role names is displayed
```

2 Verwenden Sie den Befehl `su`, um eine Rolle anzunehmen.

```
% su - rolename
Password:       <Type rolename password>
$
```

Nach Eingabe des Befehls `su -` *rolename* wird eine Profil-Shell für die Rolle angezeigt. Eine Profil-Shell erkennt die Sicherheitsattribute (Autorisierungen, Berechtigungen und festgelegte ID-Bits).

3 Stellen Sie sicher, dass Sie sich wirklich in einer Rolle befinden.

```
$ /usr/ucb/whoami
rolename
```

Nun können Sie Rollenaufgaben in diesem Terminalfenster ausführen.

4 (Optional) Zeigen Sie die Fähigkeiten Ihrer Rolle an.

Informationen zum Vorgang finden Sie unter „So legen Sie die von einer Rolle ausführbaren privilegierten Befehle fest“ auf Seite 278.

Beispiel 9–10 Annehmen der Rolle "Primary Administrator"

In dem folgenden Beispiel nimmt der Benutzer die Rolle "Primary Administrator" an. In der Standardkonfiguration entspricht diese Rolle dem Superuser. Die Rolle überprüft bei jedem Befehl, der in der Profil-Shell für die Rolle eingegeben wird, welche Berechtigungen dafür vorhanden sind.

```
% roles
sysadmin,oper,primaryadm
% su - primaryadm
Password:       <Type primaryadm password>
$ /usr/ucb/whoami       Prompt has changed to role prompt
primaryadm
$ ppriv $$
1200:   pfksh
flags = <none>
        E (Effective): all
        I (Inheritable): basic
        P (Permitted): all
        L (Limit): all
```

Informationen zu Berechtigungen finden Sie unter „Berechtigungen (Übersicht)“ auf Seite 201.

Beispiel 9–11 Annehmen der `root`-Rolle

In dem folgenden Beispiel nimmt der Benutzer die `root`-Rolle an. Die Rolle wurde in „So wandeln Sie den `root`-Benutzer in eine Rolle um“ auf Seite 226 erstellt.

```
% roles
root
% su - root
Password:       <Type root password>
# /usr/ucb/whoami       Prompt has changed to role prompt
root
$ ppriv $$
1200:   pfksh
flags = <none>
        E: all
        I: basic
        P: all
        L: all
```

Informationen zu Berechtigungen finden Sie unter „Berechtigungen (Übersicht)“ auf Seite 201.

Beispiel 9–12 Annehmen der Rolle "System Administrator"

In dem folgenden Beispiel nimmt der Benutzer die Rolle "System Administrator" an. Im Unterschied zur Rolle "Primary Administrator" verfügt die Rolle "System Administrator" über grundlegende Berechtigungen im zugehörigen effektiven Satz.

```
% roles
sysadmin,oper,primaryadm
% su - sysadmin
Password:       <Type sysadmin password>
$ /usr/ucb/whoami       Prompt has changed to role prompt
sysadmin
$ ppriv $$
1200:   pfksh
flags = <none>
        E: basic
        I: basic
        P: basic
        L: all
```

Informationen zu Berechtigungen finden Sie unter „Berechtigungen (Übersicht)“ auf Seite 201. Die Fähigkeiten der Rolle werden unter „Berechtigungsprofil "System Administrator"“ auf Seite 249 kurz beschrieben.

▼ So nehmen Sie eine Rolle in der Solaris Management Console an

Zum Ändern der Informationen in der Solaris Management Console-GUI sind administrative Fähigkeiten erforderlich. Mit einer Rolle erhalten Sie administrative Fähigkeiten. Zum Anzeigen von Informationen benötigen Sie die Autorisierung `solaris.admin.usermgr.read`. Das Berechtigungsprofil "Basic Solaris User" enthält diese Autorisierung.

Bevor Sie beginnen Eine administrative Rolle, die die Eigenschaften von Benutzern oder Rollen ändern kann, muss Ihnen bereits zugewiesen sein. Beispielsweise kann die Rolle "Primary Administrator" die Eigenschaften von Benutzern oder Rollen ändern.

1 Starten Sie die Solaris Management Console.

```
% /usr/sbin/smc &
```

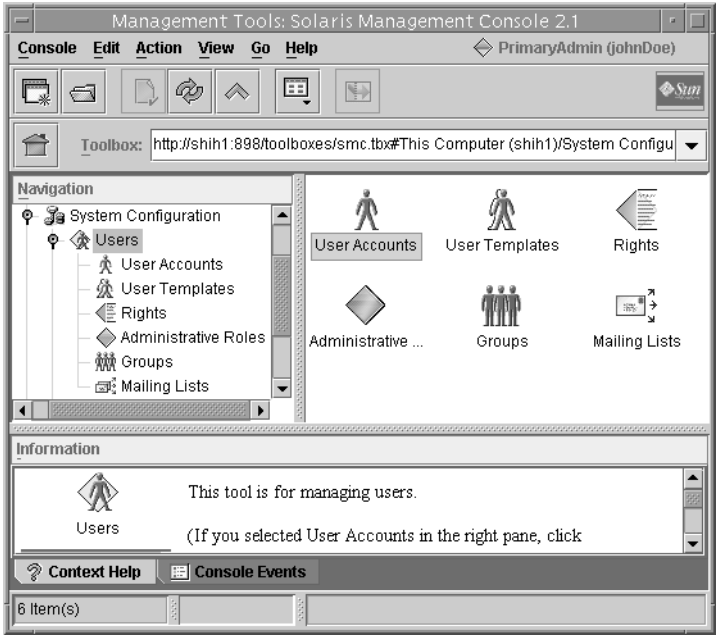
Ausführlichere Anweisungen finden Sie unter „Using the Solaris Management Tools With RBAC (Task Map)“ in *System Administration Guide: Basic Administration*.

2 Wählen Sie die Werkzeugleiste für Ihre Aufgabe aus.

Navigieren Sie im entsprechenden Name Service-Bereich zur Werkzeugleiste mit dem Tool oder der Sammlung von Tools und klicken Sie auf das Symbol. Die Bereiche sind Dateien (lokal), NIS, NIS+ und LDAP. Wenn die entsprechende Werkzeugleiste im Navigationsfenster nicht angezeigt wird, wählen Sie im Menü "Console" (Konsole) den Befehl "Open Toolbox" (Werkzeugleiste öffnen) und laden die gewünschte Werkzeugleiste.

3 **Wählen Sie das Tool, das Sie verwenden möchten.**

Navigieren Sie zu dem Tool oder der Sammlung und klicken Sie auf das Symbol. Die Tools zum Verwalten von RBAC-Elementen befinden sich im Tool "Users" (Benutzer), wie in der folgenden Abbildung gezeigt.



4 **Geben Sie Ihren Benutzernamen und Ihr Passwort im Dialogfeld "Login: User Name" (Anmeldung: Benutzername) ein.**

5 **Authentifizieren Sie sich im Dialogfeld "Login: Role" (Anmeldung: Rolle).**

Das Optionsmenü "Role" im Dialogfeld zeigt die Rollen an, die Ihnen zugewiesen sind. Wählen Sie eine Rolle aus und geben Sie das entsprechende Passwort ein.

Verwalten von RBAC (Übersicht der Schritte)

In der folgenden Übersicht der Schritte wird auf Verfahren zur Änderung der rollenbasierten Zugriffssteuerung (Role-based Access Control, RABC) nach der anfänglichen RBAC-Implementierung verwiesen.

Aufgabe	Beschreibung	Anweisungen
Ändern des Rollenpassworts	Ein autorisierter Benutzer oder eine Rolle ändert das Passwort für eine andere Rolle.	„So ändern Sie das Passwort einer Rolle“ auf Seite 234

Aufgabe	Beschreibung	Anweisungen
Ändern der Eigenschaften einer Rolle	Ändert die Fähigkeiten (Berechtigungen, privilegierte Befehle, Profile oder Autorisierungen) einer Rolle	„So ändern Sie die Eigenschaften einer Rolle“ auf Seite 236
Erstellen oder Ändern von Berechtigungsprofilen	Erstellt ein Berechtigungsprofil oder ändert die Autorisierungen, privilegierten Befehle bzw. zusätzlichen Profile in einem Berechtigungsprofil	„So erstellen oder ändern Sie ein Berechtigungsprofil“ auf Seite 238
Ändern der administrativen Fähigkeiten eines Benutzers	Fügt einem gewöhnlichen Benutzer eine Rolle, ein Berechtigungsprofil, eine Autorisierung oder Berechtigungen zu	„So ändern Sie die RBAC-Eigenschaften eines Benutzers“ auf Seite 241
Sichere Legacy-Anwendungen	Aktiviert die festgelegten ID-Berechtigungen für Legacy-Anwendungen. Skripten können Befehle mit festgelegten IDs enthalten. Legacy-Anwendungen können gegebenenfalls nach Autorisierungen suchen.	„So fügen Sie RBAC-Eigenschaften zu Legacy-Anwendungen hinzu“ auf Seite 243

Dieser Vorgang dient zur Verwaltung der in RBAC verwendeten Elemente. Verfahren zur Benutzerverwaltung finden Sie in Kapitel 5, „Managing User Accounts and Groups (Tasks)“ in *System Administration Guide: Basic Administration*.

Verwalten von RBAC

Die Solaris Management Console-GUI ist die bevorzugte Methode zur Verwaltung von RBAC.

Hinweis – Versuchen Sie nicht, RBAC über die Befehlszeile und die grafische Benutzeroberfläche gleichzeitig zu verwalten. Dies könnte zu widersprüchlichen Änderungen an der Konfiguration und zu unvorhergesehenem Verhalten führen. Sie können beide Tools zur Verwaltung von RBAC verwenden, jedoch nicht gleichzeitig.

▼ So ändern Sie das Passwort einer Rolle

Bevor Sie beginnen

Sie müssen eine Rolle angenommen haben, die das Profil "User Security" beinhaltet, oder sich als Superuser angemeldet haben. Sie können sich nicht die Rolle verwenden, deren Passwort Sie ändern möchten. Eine Rolle kann das eigene Passwort nicht ändern.

- **Verwenden Sie eine der folgenden Methoden, um das Passwort einer Rolle zu ändern.**
  - **Führen Sie den Befehl `passwd` als Superuser oder in einer Rolle aus, die das Berechtigungsprofil "User Security" enthält.**

    ```
    $ passwd -r naming-service target-rolename
    ```

`-r` *naming-service* — Wendet die Passwortänderungen auf eines der folgenden Repositorys an: `files`, `nis`, `nisplus` oder `ldap`. Wenn kein Repository angegeben ist, wird das Passwort in `files` geändert.

target-rolename — Name einer vorhandenen Rolle, die Sie ändern möchten.

Weitere Befehlsoptionen finden Sie auf der Manpage `passwd(1)`.

- **Ändern Sie das Passwort in der Solaris Management Console.**

  Informationen zum Starten der Konsole finden Sie unter „So nehmen Sie eine Rolle in der Solaris Management Console an“ auf Seite 232.

  a. **Melden Sie sich bei der Konsole als Superuser oder mit einer Rolle an, die das Berechtigungsprofil "User Security" enthält.**

     Die Anmelderolle kann nicht auch die Zielrolle sein.

  b. **Wählen Sie den entsprechenden Bereich.**

     Wenn Sie den Bereich `Files` wählen, wird das Rollenpasswort auf dem lokalen System geändert. Wenn Sie den Bereich `LDAP` wählen, wird das Rollenpasswort im LDAP-Naming Service geändert.

  c. **Navigieren Sie zu "Administrative Roles" und führen Sie die Anweisungen im linken Fensterbereich aus.**

     Ausführlichere Informationen finden Sie in der Onlinehilfe.

- **Führen Sie als Superuser oder in einer Rolle, die das Profil "User Security" enthält, den Befehl `smrole` mit dem Unterbefehl `modify` aus.**

  Dieser Befehl wird als Client des Solaris Management Console-Servers ausgeführt.

  ```
  $ /usr/sadm/bin/smrole -D domain-name -r admin-role -l <Type admin-role password> \
  modify -- -n target-rolename  -P password
  ```

  `-D` *domain-name* — Name der zu ändernden Domain

  `-r` *admin-role* — Name der administrativen Rolle, von der die Zielrolle geändert werden kann. Die administrative Rolle muss über die Autorisierung `solaris.admin.usermgr.pswd` verfügen. Die administrative Rolle und die Zielrolle dürfen nicht identisch sein.

  `-l` — Eingabeaufforderung für das Passwort von *admin-role*

  `--` — Trennzeichen zwischen Authentifizierungsoptionen und Unterbefehlsoptionen

  `-n` *target-rolename* — Name der Zielrolle

  `-P` *password* — Neues Passwort für *target-rolename*

Eine vollständige Liste der Befehlsoptionen finden Sie auf der Manpage `smrole(1M)`.

Beispiel 9–13 Ändern des Passworts einer lokalen Rolle mit dem Befehl `passwd`

In diesem Beispiel ändert der Superuser das Passwort der lokalen Rolle `operadm`.

```
# passwd -r files  operadm
New password:       Type new password
Re-enter new password:       Retype new password
```

Beispiel 9–14 Ändern des Passworts einer Rolle in einem LDAP-Repository

In diesem Beispiel ändert die Rolle "Primary Administrator" das Passwort der Rolle `operadm` im LDAP-Directory Service.

```
$ passwd -r ldap operadm
New password:       Type new password
Re-enter new password:       Retype new password
```

Beispiel 9–15 Ändern des Passworts einer Rolle mit dem Befehl `smrole modify`

In diesem Beispiel stellt der Administrator eine Verbindung mit dem Solaris Management Console-Server her, um das `operadm`-Passwort in der NIS-Domain zu ändern. Wenn der Administrator die Eingabetaste drückt, ohne ein Passwort anzugeben, wird die Eingabeaufforderung `New Password:` angezeigt.

```
$ /usr/sadm/bin/smrole -D nis:/examplehost/example.domain \
-r primaryadm -l <Type primaryadm password> \
modify -- -n operadm -P       Press the Return key
New Password: a!2@3#4$5%6*7
$
```

▼ So ändern Sie die Eigenschaften einer Rolle

Bevor Sie beginnen

Um die Eigenschaften einer Rolle ändern zu können, müssen Sie entweder eine Rolle annehmen, die das Berechtigungsprofil "Primary Administrator" enthält, oder zum Benutzer `root` wechseln. Zu den Rolleneigenschaften gehören das Passwort, die Berechtigungsprofile und Autorisierungen.

Hinweis – Informationen zum Ändern der Passworteigenschaft einer Rolle finden Sie unter „So ändern Sie das Passwort einer Rolle“ auf Seite 234.

- **Verwenden Sie eine der folgenden Methoden, um die Eigenschaften einer Rolle zu ändern.**

  - **Verwenden Sie das Tool "Users" (Benutzer) in der Solaris Management Console.**

    Informationen zum Starten der Konsole finden Sie unter „So nehmen Sie eine Rolle in der Solaris Management Console an“ auf Seite 232. Führen Sie die Anweisungen im linken Fensterbereich aus, um eine Rolle in "Administrative Roles" (Administrative Rollen) zu ändern. Ausführlichere Informationen finden Sie in der Onlinehilfe.

  - **Verwenden Sie den Befehl `rolemod`.**

    Mit diesem Befehl werden die Attribute einer Rolle geändert, die im lokalen Name Service definiert ist.

    ```
    $ rolemod -c comment -P profile-list rolename
    ```

`-c` *comment*	Neuer Kommentar, der die Fähigkeiten der Rolle beschreibt
`-P` *profile-list*	Liste der Profile, die in der Rolle enthalten sind. Diese Liste ersetzt die aktuelle Liste der Profile.
rolename	Name einer vorhandenen, lokalen Rolle, die Sie ändern möchten.

    Weitere Befehlsoptionen finden Sie auf der Manpage `rolemod(1M)`.

  - **Verwenden Sie den Befehl `smrole` mit dem Unterbefehl `modify`.**

    Mit diesem Befehl werden die Attribute einer Rolle in einem verteilten Name Service, wie NIS, NIS+ oder LDAP, geändert. Dieser Befehl wird als Client des Solaris Management Console-Servers ausgeführt.

    ```
    $ /usr/sadm/bin/smrole -D domain-name \
    -r admin-role -l <Type admin-role password> \
    modify -- -n rolename  -r username -u username
    ```

`-D` *domain-name*	Name der zu ändernden Domain
`-r` *admin-role*	Name der administrativen Rolle, von der die Rolle geändert werden kann. Die administrative Rolle muss über die Autorisierung `solaris.role.assign` verfügen. Wenn Sie Ihre angenommene Rolle ändern, muss die Rolle über die Autorisierung `solaris.role.delegate` verfügen.
`-l`	Eingabeaufforderung für das Passwort von *admin-role*
`--`	Trennzeichen zwischen Authentifizierungsoptionen und Unterbefehlsoptionen
`-n` *rolename*	Name der neuen Rolle
`-r` *username*	Name des Benutzers, der *rolename* nicht mehr annehmen kann
`-u` *username*	Name des Benutzers, der *rolename* jetzt annehmen kann

Weitere Befehlsoptionen finden Sie auf der Manpage smrole(1M).

Beispiel 9–16 Ändern der Eigenschaften einer lokalen Rolle mit dem Befehl `rolemod`

In diesem Beispiel wird die Rolle `operadm` so geändert, dass das Berechtigungsprofil "FTP Management" enthalten ist.

```
$ rolemod -c "Handles printers, backup, and FTP" \
-P "Operator,FTP Management,All" operadm
```

Diese Berechtigungsprofile werden den Profilen hinzugefügt, die mithilfe der Datei `policy.conf` zugewiesen werden.

Beispiel 9–17 Ändern der Eigenschaften einer lokalen Rolle mit dem Befehl `smrole modify`

In dem folgenden Beispiel wird die Rolle `operadm` so geändert, dass das Berechtigungsprofil "FTP Management" enthalten ist.

```
$ /usr/sadm/bin/smrole -r primaryadm -l <Type primaryadm password> \
modify -- -n operadm -c "Handles printers, backup, and FTP" \
-p "FTP Management"
```

Beispiel 9–18 Ändern einer Rolle in einer Domain mit dem Befehl `smrole modify`

In dem folgenden Beispiel wird die Rolle `clockmgr` geändert. Der NIS-Benutzer mit der ID `108` kann die Rolle nicht mehr annehmen. Der NIS-Benutzer mit der ID `110` kann die Rolle `clockmgr` annehmen.

```
$ /usr/sadm/bin/smrole -D nis:/examplehost/example.domain \
-r primaryadm -l <Type primaryadm password> \
modify -- -n clockmgr -r 108 -u 110
```

▼ So erstellen oder ändern Sie ein Berechtigungsprofil

Bei einem Berechtigungsprofil handelt es sich um die Eigenschaft einer Rolle. Erstellen oder ändern Sie ein Berechtigungsprofil, wenn die Datenbank `prof_attr` kein Berechtigungsprofil enthält, das Ihren Anforderungen entspricht. Weitere Informationen zu Berechtigungsprofilen finden Sie unter „RBAC-Berechtigungsprofile“ auf Seite 198.

Bevor Sie beginnen Um ein Berechtigungsprofil erstellen oder ändern zu können, müssen Sie die Rolle "Primary Administrator" annehmen oder zum Superuser wechseln.

- **Verwenden Sie eine der folgenden Methoden, um ein Berechtigungsprofil zu erstellen oder zu ändern.**

  - **Verwenden Sie das Tool "Users" (Benutzer) in der Solaris Management Console.**

    Informationen zum Starten der Konsole finden Sie unter „So nehmen Sie eine Rolle in der Solaris Management Console an“ auf Seite 232. Führen Sie die Anweisungen im linken Fensterbereich aus, um in "Rights" (Berechtigungen) ein Berechtigungsprofil zu erstellen oder zu ändern. Ausführlichere Informationen finden Sie in der Onlinehilfe.

  - **Verwenden Sie den Befehl `smprofile`.**

    Mit diesem Befehl können Sie ein Berechtigungsprofil hinzufügen, ändern, anzeigen oder löschen. Der Befehl kann auf Dateien und in einem verteilten Name Service, wie NIS, NIS+ oder LDAP verwendet werden. Der Befehl `smprofile` wird als Client des Solaris Management Console-Servers ausgeführt.

    ```
    $ /usr/sadm/bin/smprofile -D domain-name \
    -r admin-role -l <Type admin-role password> \
    add | modify -- -n profile-name \
    -d description  -m help-file -p supplementary-profile
    ```

`-D` *domain-name*	Name der zu ändernden Domain
`-r` *admin-role*	Name der administrativen Rolle, von der die Rolle geändert werden kann. Die administrative Rolle muss über die Autorisierung `solaris.role.assign` verfügen. Wenn Sie Ihre angenommene Rolle ändern, muss die Rolle über die Autorisierung `solaris.role.delegate` verfügen.
`-l`	Eingabeaufforderung für das Passwort von *admin-role*
`--`	Trennzeichen zwischen Authentifizierungsoptionen und Unterbefehlsoptionen
`-n` *profile-name*	Name des neuen Profils
`-d` *description*	Kurze Beschreibung des Profils
`-m` *help-file*	Name der HTML-Hilfedatei, die Sie erstellt und im Verzeichnis `/usr/lib/help/profiles/locale/C` hinzugefügt haben
`-p` *supplementary-profile*	Name eines bestehenden Berechtigungsprofils, das in diesem Berechtigungsprofil enthalten ist. Sie können mehrere Optionen des Typs `-p` *supplementary-profile* angeben.

    Weitere Befehlsoptionen finden Sie auf der Manpage `smprofile(1M)`.

Beispiel 9–19 Ändern eines Berechtigungsprofils über die Befehlszeile

In dem folgenden Beispiel wird das Berechtigungsprofil "Network Management" dem Berechtigungsprofil "Network Security" hinzugefügt. Die Rolle, die das Profil "Network Security" enthält, kann nun das Netzwerk und die Hosts konfigurieren sowie sicherheitsrelevante Befehle ausführen.

```
$ /usr/sadm/bin/smprofile -D nisplus:/example.host/example.domain \
-r primaryadm -l <Type primaryadm password> \
modify -- -n "Network Security" \
-d "Manage network and host configuration and security" \
-m RtNetConfSec.html -p "Network Management"
```

Der Administrator hat vor der Ausführung dieses Befehls die neue Hilfedatei `RtNetConfSec.html` erstellt und im Verzeichnis `/usr/lib/help/profiles/locale/C` abgelegt.

Beispiel 9–20 Erstellen eines neuen Berechtigungsprofils mit dem Tool "Rights"

Die folgende Tabelle enthält Beispieldaten für das hypothetische Berechtigungsprofil "Build Administrator". Dieses Berechtigungsprofil enthält die Befehle im Unterverzeichnis `/usr/local/swctrl/bin`. Diese Befehle verfügen über eine effektive UID von `0`. Das Berechtigungsprofil "Build Administrator" ist für Administratoren nützlich, die Builds und die Versionen bei der Entwicklung von Software verwalten.

Registerkarte	Feld	Beispiel
General	Name	Build Administrator
	Description (Beschreibung)	Zur Verwaltung von Software-Builds und -Versionen
	Help File Name (Hilfedateiname)	`BuildAdmin.html`
Commands (Befehle)	Add Directory (Verzeichnis hinzufügen)	Klicken Sie im Dialogfeld auf "Add Directory" (Verzeichnis hinzufügen), geben Sie `/usr/local/swctrl/bin` im Dialogfeld ein und klicken Sie auf "OK".
	Commands Denied / Commands Permitted (Erlaubte/Nicht erlaubte Befehle)	Verschieben Sie `/usr/local/swctrl/bin` in die Spalte "Commands Permitted" (Erlaubte Befehle).
	Set Security Attributes (Sicherheitsattribute einstellen)	Wählen Sie `/usr/local/swctrl/bin`, klicken Sie auf "Set Security Attributes" (Sicherheitsattribute einstellen) und stellten Sie die effektive UID auf `root` ein.

Registerkarte	Feld	Beispiel
Authorizations (Autorisierungen)	Authorizations Excluded / Authorizations Included (Ausgeschlossene/eingeschlossene Autorisierungen)	*Keine Autorisierungen*
Supplementary Rights (Zusätzliche Berechtigungen)	Rights Excluded / Rights Included (Ausgeschlossene/eingeschlossene Berechtigungen)	*Keine zusätzlichen Berechtigungsprofile.*

Allgemeine Fehler

Überprüfen Sie Folgendes, wenn das Berechtigungsprofil die Rolle mit den erwarteten Fähigkeiten nicht enthält:

- Werden die Berechtigungsprofile der Rolle in der GUI in der richtigen Reihenfolge vom stärksten bis zum schwächsten Profil aufgeführt?

  Wenn beispielsweise das Berechtigungsprofil `All` sich in der Liste an erster Stelle befindet, werden keine Befehle mit Sicherheitsattributen ausgeführt. Ein Profil, das Befehle mit Sicherheitsattributen enthält, muss in der Liste vor dem Berechtigungsprofil `All` aufgeführt werden.

- Ist ein Befehl mehrmals in den Berechtigungsprofilen der Rolle enthalten? Wenn das der Fall ist, hat die erste Instanz des Befehls alle benötigten Sicherheitsattribute?

  Beispielsweise können für bestimmte Befehlsoptionen Berechtigungen erforderlich sein. Damit die Optionen, für die Berechtigungen erforderlich sind, ausgeführt werden können, müssen die Berechtigungen der ersten Instanz im Profil mit den meisten Rechten zugewiesen sein.

- Verfügen die Befehle in den Berechtigungsprofilen der Rolle über geeignete Sicherheitsattribute?

  Wenn die Richtlinie `suser` lautet, benötigen einige Befehle `uid=0` statt `euid=0`, um erfolgreich ausgeführt werden zu können.

- Wurde der Name Service-Cache `svc:/system/name-service-cache` neu gestartet?

  Der Dämon `nscd` kann über eine längere Aktivitätszeit verfügen. Durch einen Neustart des Dämons wird der Name Service mit den neuesten Daten aktualisiert.

▼ So ändern Sie die RBAC-Eigenschaften eines Benutzers

Zu den Benutzereigenschaften gehören Passwort, Berechtigungsprofile, Rollen und Autorisierungen. Die sicherste Methode, einem Benutzer administrative Fähigkeiten zuzuweisen, besteht darin, ihm eine Rolle zuzuordnen. Informationen hierzu finden Sie unter „Sicherheitsüberlegungen bei direkter Zuweisung von Sicherheitsattributen“ auf Seite 201.

Bevor Sie beginnen Sie müssen entweder eine Rolle annehmen, die das Berechtigungsprofil "Primary Administrator" enthält, oder zum Benutzer `root` wechseln.

- **Verwenden Sie eine der folgenden Methoden, um die RBAC-Eigenschaften eines Benutzers zu ändern:**

  - **Verwenden Sie das Tool "Users" (Benutzer) in der Solaris Management Console.**

    Informationen zum Starten der Konsole finden Sie unter „So nehmen Sie eine Rolle in der Solaris Management Console an“ auf Seite 232. Führen Sie die Anweisungen im linken Fensterbereich aus, um in "User Accounts" (Benutzerkonten) einen Benutzer zu ändern. Ausführlichere Informationen finden Sie in der Onlinehilfe.

    Tipp – Es ist nicht empfehlenswert, Benutzern Autorisierungen, Berechtigungen oder Berechtigungsprofile direkt zuzuweisen. Stattdessen sollten Benutzern Rollen zugewiesen werden. Die Benutzer können dann eine Rolle annehmen und privilegierte Vorgänge ausführen.

  - **Verwenden Sie den Befehl `usermod`.**

    Mit diesem Befehl werden die Attribute eines Benutzers geändert, der im lokalen Name Service definiert ist.

    ```
    $ usermod -R rolename username
    ```

`-R` *rolename*	Name der vorhandenen lokalen Rolle
username	Name eines vorhandenen, lokalen Benutzers, den Sie ändern möchten.

    Weitere Befehlsoptionen finden Sie auf der Manpage `usermod(1M)`.

  - **Verwenden Sie den Befehl `smuser` mit dem Unterbefehl `modify`.**

    Dieser Befehl ändert die Attribute eines Benutzers in einem verteilten Name Service wie NIS, NIS+ oder LDAP. Dieser Befehl wird als Client des Solaris Management Console-Servers ausgeführt.

    ```
    $ /usr/sadm/bin/smuser -D domain-name \
    -r admin-role -l <Type admin-role password> \
    modify -- -n username -a rolename
    ```

`-D` *domain-name*	Name der zu ändernden Domain
`-r` *admin-role*	Name der administrativen Rolle, von der die Rolle geändert werden kann. Die administrative Rolle muss über die Autorisierung `solaris.role.assign` verfügen. Wenn Sie Ihre angenommene Rolle ändern, muss die Rolle über die Autorisierung `solaris.role.delegate` verfügen.
`-l`	Eingabeaufforderung für das Passwort von *admin-role*

`--`	Trennzeichen zwischen Authentifizierungsoptionen und Unterbefehlsoptionen
`-n` *username*	Name des Benutzers, dem *rolename* zugewiesen wird
`-a` *rolename*	Name der Rolle, die Sie *username* zuweisen. Sie können mehrere Optionen des Typs `-a` *rolename* angeben.

Weitere Befehlsoptionen finden Sie auf der Manpage `smuser(1M)`.

Beispiel 9–21 Ändern der RBAC-Eigenschaften eines lokalen Benutzers über die Befehlszeile

In diesem Beispiel kann der Benutzer `jdoe` die Rolle "System Administrator" nun annehmen.

```
$ usermod -R sysadmin jdoe
```

Diese Rolle wird den Rollen hinzugefügt, die der Benutzer annehmen kann.

Beispiel 9–22 Ändern der RBAC-Eigenschaften eines Benutzers mit dem Befehl `smuser`

In diesem Beispiel werden dem Benutzer `jdoe` die beiden Rollen "System Administrator" und "Operator" zugewiesen. Da der Benutzer und die Rollen lokal definiert werden, wird die Option `-D` nicht benötigt.

```
$ /usr/sadm/bin/smuser -r primaryadm -l <Type primaryadm password> \
modify -- -n jdoe -a sysadmin -a operadm
```

In dem folgenden Beispiel ist der Benutzer im NIS-Name Service definiert. Daher ist die Option `-D` erforderlich. Zwei Rollen sind im Name Service definiert. Eine Rolle, `root`, ist lokal definiert.

```
$ /usr/sadm/bin/smuser -D nis:/examplehost/example.domain \
-r primaryadm -l <Type primaryadm password> \
modify -- -n jdoe -a sysadmin -a operadm -a root
```

▼ So fügen Sie RBAC-Eigenschaften zu Legacy-Anwendungen hinzu

Eine Legacy-Anwendung ist ein Befehl oder ein Satz von Befehlen. Die Sicherheitsattribute sind für jeden Befehl in einem Berechtigungsprofil eingestellt. Das Berechtigungsprofil wird dann in eine Rolle eingeschlossen. Ein Benutzer, der eine Rolle annimmt, kann die Legacy-Anwendung mit den Sicherheitsattributen ausführen.

Informationen zum Hinzufügen von Legacy-Anwendungen zur Solaris Management Console finden Sie unter „Adding Tools to the Solaris Management Console“ in *System Administration Guide: Basic Administration*.

Bevor Sie beginnen Sie müssen die Rolle "Primary Administrator" annehmen oder Superuser sein, um die Sicherheitsattribute eines Befehls in einem Berechtigungsprofil zu ändern.

1 **Verwenden Sie das Tool "Users" (Benutzer) in der Solaris Management Console.**

Informationen zum Starten der Konsole finden Sie unter „So nehmen Sie eine Rolle in der Solaris Management Console an“ auf Seite 232. Führen Sie die Anweisungen im linken Fensterbereich aus, um in "Rights" (Berechtigungen) ein Berechtigungsprofil zu ändern. Ausführlichere Informationen finden Sie in der Onlinehilfe.

2 **Fügen Sie den Befehlen, mit denen die Legacy-Anwendung implementiert wird, Sicherheitsattribute hinzu.**

Gehen Sie wie bei allen anderen Befehlen vor, um einer Legacy-Anwendung Sicherheitsattribute hinzuzufügen. Fügen Sie den Befehl mit Sicherheitsattributen einem Berechtigungsprofil hinzu. Weisen Sie einem Legacy-Befehl die Sicherheitsattribute `euid=0` oder `uid=0` zu. Ausführliche Informationen zu dem Verfahren finden Sie unter „So erstellen oder ändern Sie ein Berechtigungsprofil“ auf Seite 238.

3 **Nachdem Sie die Legacy-Anwendung einem Berechtigungsprofil hinzugefügt haben, nehmen Sie dieses Profil in die Liste der Profile einer Rolle auf.**

Weitere Informationen zum Hinzufügen von Berechtigungen zu einer Rolle finden Sie unter „So ändern Sie die Eigenschaften einer Rolle“ auf Seite 236.

Beispiel 9–23 Hinzufügen von Sicherheitsattributen zu Befehlen in einem Skript

Wenn zur erfolgreichen Ausführung eines Befehls in einem Skript das `setuid`-Bit oder das `setgid`-Bit eingestellt werden muss, müssen die Sicherheitsattribute für die ausführbare Datei des Skripts *und* für den Befehl einem Berechtigungsprofil hinzugefügt werden. Anschließend wird das Berechtigungsprofil zu einer Rolle hinzugefügt und die Rolle einem Benutzer zugewiesen. Wenn der Benutzer die Rolle annimmt und das Skript ausführt, wird der Befehl mit den Sicherheitsattributen ausgeführt.

Informationen zum Hinzufügen von Sicherheitsattributen zu einem Befehl oder einem Shell-Skript finden Sie unter „So erstellen oder ändern Sie ein Berechtigungsprofil“ auf Seite 238.

Beispiel 9–24 Überprüfen von Autorisierungen mit einem Skript oder Programm

Um ein Skript für Autorisierungen zu erstellen, müssen Sie einen Test hinzufügen, der auf dem Befehl `auths` basiert. Weitere Informationen zu diesem Befehl finden Sie auf der Manpage `auths(1)`.

Mit der folgenden Zeile wird beispielsweise getestet, ob der Benutzer über die als `$1`-Argument angegebene Autorisierung verfügt:

```
if [ `/usr/bin/auths|/usr/xpg4/bin/grep $1` ]; then
        echo Auth granted
else
        echo Auth denied
fi
```

Der Vollständigkeit halber sollte der Test Logik enthalten, die mit Platzhaltern nach anderen Autorisierungen sucht. Um beispielsweise zu testen, ob der Benutzer über die Autorisierung `solaris.admin.usermgr.write` verfügt, müssen Sie nach diesen Zeichenfolgen suchen:

- `solaris.admin.usermgr.write`
- `solaris.admin.usermgr.*`
- `solaris.admin.*`
- `solaris.*`

Wenn Sie ein Programm schreiben, testen Sie die Autorisierung mithilfe der Funktion `getauthattr()`.

◆ ◆ ◆ KAPITEL 10

Rollenbasierte Zugriffssteuerung (Übersicht)

In diesem Kapitel finden Sie Referenzmaterial zur rollenbasierten Zugriffssteuerung (Role-Based Access Control, RBAC). Im Folgenden sind die Informationen zur Referenz in diesem Kapitel aufgeführt:

- „Inhalt der Berechtigungsprofile“ auf Seite 247
- „Autorisierungsbenennung und -delegation“ auf Seite 252
- „Datenbanken, die RBAC unterstützen“ auf Seite 253
- „RBAC-Befehle“ auf Seite 261

Weitere Informationen zum Verwenden von RBAC erhalten Sie unter Kapitel 9, „Rollenbasierte Zugriffssteuerung (Aufgaben)“. Eine Übersicht finden Sie unter „Rollenbasierte Zugriffssteuerung (Übersicht)“ auf Seite 190.

Inhalt der Berechtigungsprofile

In diesem Abschnitt werden einige typische Berechtigungsprofile beschrieben. Berechtigungsprofile können Autorisierungen, Befehle mit Sicherheitsattributen und ergänzende Berechtigungsprofile enthalten. Die Berechtigungsprofile werden entsprechend ihrer Leistungsfähigkeit in absteigender Reihenfolge aufgeführt. Vorschläge, wie Sie Berechtigungsprofile an Ihrem Standort auf Rollen verteilen können, finden Sie unter „So planen Sie die RBAC-Implementierung“ auf Seite 215.

- **Berechtigungsprofil "Primary Administrator"**: Bietet alle Funktionen von Superuser in einem Profil
- **System Administrator (Berechtigungsprofil)**: Bietet ein Profil, das die meisten nicht mit Sicherheit in Zusammenhang stehenden Aufgaben erfüllen kann. Dieses Profil enthält mehrere andere Profile, um eine leistungsstarke Rolle erstellen zu können.
- **Operator (Berechtigungsprofil)**: Bietet begrenzte Funktionen zum Verwalten von Dateien und Offline-Datenträgern. Dieses Profil enthält ergänzende Berechtigungsprofile zum Erstellen einer einfachen Rolle.

- **Printer Management (Berechtigungsprofil)**: Bietet eine begrenzte Anzahl von Befehlen und Autorisierungen zur Druckerverwaltung. Dieses Profil ist eines von mehreren Profilen, die einen einzelnen Verwaltungsbereich abdecken.
- **Basic Solaris User (Berechtigungsprofil)**: Ermöglicht Benutzern die Verwendung des Systems innerhalb der Grenzen der Sicherheitsrichtlinie. Dieses Profil ist standardmäßig in der Datei `policy.conf` aufgeführt.
- **All (Berechtigungsprofil)**: Bietet Rollen Zugriff auf Befehle, die keine Sicherheitsattribute haben

Jedes Berechtigungsprofil hat eine zugehörige Hilfedatei. Die Hilfedateien sind in HTML verfasst und individuell anpassbar. Die Dateien befinden sich im Verzeichnis `/usr/lib/help/profiles/locale/C`.

Berechtigungsprofil "Primary Administrator"

Das Berechtigungsprofil "Primary Administrator" wird der leistungsstärksten Rolle auf dem System zugewiesen. Die Rolle, die das Berechtigungsprofil "Primary Administrator" enthält, verfügt über Superuser-Funktionen.

- Die `solaris.*`-Autorisierung weist alle Autorisierungen, die von der Oracle Solaris-Software zur Verfügung gestellt werden, effektiv zu.
- Die `solaris.grant`-Autorisierung ermöglicht Rollen, beliebige Autorisierungen beliebigen Berechtigungsprofilen, Rollen oder Benutzern zuzuweisen.
- Mithilfe der Befehlszuweisung `*:uid=0;gid=0` kann ein beliebiger Befehl mit `UID=0` und `GID=0` ausgeführt werden.

Sie können die Hilfedatei `RtPriAdmin.html` gegebenenfalls für Ihren Standort anpassen. Die Hilfedateien sind im Verzeichnis `/usr/lib/help/profiles/locale/C` gespeichert.

Beachten Sie, dass das Berechtigungsprofil "Primary Administrator" nicht geändert oder zugewiesen werden kann, wenn es nicht mit der Sicherheitsrichtlinie der Site übereinstimmt. Die Sicherheitsfunktionen im Berechtigungsprofil "Primary Administrator" müssen dann in ein oder mehrere andere Berechtigungsprofile integriert werden. Die anderen Berechtigungsprofile müssen dann Rollen zugewiesen werden.

TABELLE 10–1 Inhalt des Berechtigungsprofils "Primary Administrator"

Zweck	Inhalt
Ausführen aller administrativen Aufgaben	**Befehle**: `*:uid=0;gid=0` **Autorisierungen**: `solaris.*`, `solaris.grant` **Hilfedatei**: `RtPriAdmin.html`

Berechtigungsprofil "System Administrator"

Das Berechtigungsprofil "System Administrator" ist für Systemadministratoren gedacht. Da der Systemadministrator nicht über die umfassenden Funktionen eines Primäradministrators verfügt, werden keine Platzhalter verwendet. Stattdessen besteht dieses Profil aus einem Satz diskreter, zusätzlicher administrativer Berechtigungsprofile, die sich nicht mit Sicherheit befassen. Die Befehle mit Sicherheitsattributen aus einem der zusätzlichen Berechtigungsprofile werden angezeigt.

Beachten Sie, dass das Berechtigungsprofil "All" am Ende der Liste zusätzlicher Berechtigungsprofile zugewiesen wird.

TABELLE 10–2 Inhalt des Berechtigungsprofils "System Administrator"

Zweck	Inhalt
Ausführen der meisten administrativen Aufgaben, die nicht in Zusammenhang mit Sicherheit stehen	**Zusätzliche Berechtigungsprofile**: Audit Review, Printer Management, Cron Management, Device Management, File System Management, Mail Management, Maintenance and Repair, Name Service Management, Network Management, Object Access Management, Process Management, Software Installation, Project Management, User Management, All **Hilfedatei**: `RtSysAdmin.html`
Befehle aus einem der zusätzlichen Profile	**Berechtigungsprofil "Object Access Management"**, `solaris`-Richtlinie: `/usr/bin/chgrp:privs=file_chown`, `/usr/bin/chmod:privs=file_chown`, `/usr/bin/chown:privs=file_chown` , `/usr/bin/setfacl:privs=file_chown` `suser`-Richtlinie: `/usr/bin/chgrp:euid=0`, `/usr/bin/chmod:euid=0`, `/usr/bin/chown:euid=0`, `/usr/bin/getfacl:euid=0`, `/usr/bin/setfacl:euid=0`

Berechtigungsprofil "Operator"

Das Berechtigungsprofil "Operator" ist ein weniger leistungsstarkes Profil, das Funktionen wie Backups und Druckerwartung zur Verfügung stellt. Die Fähigkeit zum Wiederherstellen von Dateien hat weitere Auswirkungen auf die Sicherheit. Daher sieht die Standardeinstellung in diesem Profil vor, diese Funktion nicht mit einzuschließen.

TABELLE 10–3 Inhalt des Berechtigungsprofils "Operator"

Zweck	Inhalt
Ausführen einfacher administrativer Aufgaben	**Zusätzliche Berechtigungsprofile**: Printer Management, Media Backup, All **Hilfedatei**: `RtOperator.html`

Berechtigungsprofil "Printer Management"

"Printer Management" ist ein typisches Berechtigungsprofil, das für einen spezifischen Aufgabenbereich gedacht ist. Dieses Profil umfasst Autorisierungen und Befehle. Die folgende Tabelle zeigt eine Teilliste der Befehle.

TABELLE 10–4 Inhalt des Berechtigungsprofils "Printer Management"

Zweck	Inhalt
Verwalten von Druckern, Dämonen und Spooling	**Autorisierungen**: `solaris.print.*`, `solaris.label.print`, `solaris.admin.printer.delete`, `solaris.admin.printer.modify`, `solaris.admin.printer.read` , `solaris.smf.manage.discovery.printers.*`, `solaris.smf.value.discovery.printers.*` **Befehle**: `/usr/lib/lp/local/lpadmin:uid=lp;gid =lp`, `/usr/sbin/lpfilter:euid=lp;uid=lp`, `/usr/sbin/lpforms:euid=lp`, `/usr/sbin/lpusers:euid=lp`, `/usr/sbin/ppdmgr:euid=0` **Hilfedatei**: `RtPrntMngmnt.html`

Berechtigungsprofil "Basic Solaris User"

Standardmäßig wird das Berechtigungsprofil "Basic Solaris User" automatisch allen Benutzern über die Datei `policy.conf` zugewiesen. Dieses Profil bietet grundlegende Autorisierungen, die bei normalen Vorgängen nützlich sind. Beachten Sie, dass die Benutzerfreundlichkeit, die das Berechtigungsprofil "Basic Solaris User" bietet, gegenüber den Standort-Sicherheitsanforderungen abgewogen werden muss. Für Standorte mit strengeren Sicherheitsanforderungen könnte es nützlich sein, dieses Profil aus der Datei `policy.conf` zu entfernen.

TABELLE 10–5 Inhalt des Berechtigungsprofils "Basic Solaris User"

Zweck	Inhalt
Automatisches Zuweisen von Berechtigungen zu allen Benutzern	**Autorisierungen**: `solaris.profmgr.read`, `solaris.jobs.user`, `solaris.mail.mailq`, `solaris.device.mount.removable`, `solaris.admin.usermgr.read` , `solaris.admin.logsvc.read`, `solaris.admin.fsmgr.read`, `solaris.admin.serialmgr.read`, `solaris.admin.diskmgr.read`, `solaris.admin.procmgr.user`, `solaris.compsys.read` , `solaris.admin.printer.read`, `solaris.admin.prodreg.read`, `solaris.admin.dcmgr.read`, `solaris.snmp.read`, `solaris.project.read`, `solaris.admin.patchmg.read` , `solaris.network.hosts.read`, `solaris.admin.volmgr.read` **Zusätzliche Berechtigungsprofile**: All **Hilfedatei**: `RtDefault.html`

Berechtigungsprofil "All"

Das Berechtigungsprofil "All" verwendet Platzhalter, um alle Befehle einzuschließen. Dieses Profil bietet eine Rolle mit Zugriff auf alle Befehle, die nicht explizit in anderen Berechtigungsprofilen zugewiesen sind. Ohne das Berechtigungsprofil "All" oder andere Berechtigungsprofile, die Platzhalter verwenden, hat eine Rolle nur Zugriff auf explizit zugewiesene Befehle. Ein solcher begrenzter Befehlssatz ist wenig praktisch. Es sind keine Autorisierungen in diesem Profil enthalten.

Bei Verwendung sollte das Berechtigungsprofil "All" als letztes zugewiesen werden. Diese Position stellt sicher, dass explizite Sicherheitsattributzuweisungen in anderen Berechtigungsprofilen angewendet werden.

TABELLE 10–6 Inhalt des Berechtigungsprofils "All"

Zweck	Inhalt
Ausführen eines beliebigen Befehls als Benutzer oder Rolle	**Befehle**: * **Hilfedatei**: `RtAll.html`

Reihenfolge der Berechtigungsprofile

Die Befehle in Berechtigungsprofilen werden der Reihenfolge nach interpretiert. Das erste Vorkommen eines Befehls ist die einzige Version des Befehls, die für diese Rolle oder den Benutzer verwendet wird. Verschiedene Berechtigungsprofile können den gleichen Befehl enthalten. Daher ist die Reihenfolge der Berechtigungsprofile in einer Profilliste relevant. Das Berechtigungsprofil mit den meisten Funktionen sollte an erster Stelle aufgeführt werden.

Berechtigungsprofile werden in der Solaris Management Console-GUI und in der Datei `prof_attr` aufgeführt. In der Solaris Management Console-GUI sollte das Berechtigungsprofil mit den meisten Funktionen das erste Profil in einer Liste zugewiesener Berechtigungsprofile sein. In der Datei `prof_attr` sollte das Berechtigungsprofil mit den meisten Funktionen das erste in einer Liste zusätzlicher Profile sein. Diese Platzierung stellt sicher, dass ein Befehl mit Sicherheitsattributen vor dem gleichen Befehl ohne Sicherheitsattribute aufgelistet wird.

Anzeigen des Inhalts von Berechtigungsprofilen

Das Solaris Management Console-Berechtigungstool stellt eine Methode zum Untersuchen des Inhalts der Berechtigungsprofile zur Verfügung.

Die Dateien `prof_attr` und `exec_attr` bieten eine genauer unterteilte Ansicht. Die Datei `prof_attr` enthält den Namen jedes Berechtigungsprofils, das auf dem System festgelegt ist. Die Datei enthält auch die Autorisierungen, Berechtigungen und zusätzlichen Berechtigungsprofile für jedes Profil. Die Datei `exec_attr` enthält die Namen der Berechtigungsprofile und ihrer zugehörigen Befehle mit Sicherheitsattributen.

Autorisierungsbenennung und -delegation

Eine RBAC-*Autorisierung* ist eine diskrete Berechtigung, die einer Rolle oder einem Benutzer gewährt werden kann. Autorisierungen werden von RBAC-konformen Anwendungen überprüft, bevor ein Benutzer Zugriff auf die Anwendung oder spezifische Vorgänge innerhalb der Anwendung erhält. Diese Überprüfung ersetzt die Tests in konventionellen UNIX-Anwendungen für `UID=0`.

Autorisierungs-Namenskonventionen

Eine Autorisierung hat einen Namen, der intern und in Dateien verwendet wird. `solaris.admin.usermgr.pswd` ist z. B. der Name einer Autorisierung. Eine Autorisierung verfügt über eine kurze Beschreibung, die auf den grafischen Benutzeroberflächen (Graphical User Interfaces, GUIs) angezeigt wird. `Change Passwords` ist beispielsweise die Beschreibung der Autorisierung `solaris.admin.usermgr.pswd`.

Üblicherweise bestehen Autorisierungsnamen aus dem Internetnamen des Anbieters, dem Themenbereich, beliebigen Teilbereichen sowie Funktionen in umgekehrter Reihenfolge. Die einzelnen Teile des Autorisierungsnamen sind durch Punkte getrennt. Ein Beispiel hierfür ist `com.xyzcorp.device.access`. Ausnahmen zu dieser Konvention sind die Autorisierungen von Oracle Corporation, die das Präfix `solaris` anstelle eines Internetnamen verwenden. Die Namenskonvention ermöglicht Administratoren, Autorisierungen auf hierarchische Weise anzuwenden. Ein Platzhalter (`*`) kann eine beliebige Zeichenfolge rechts eines Punkts repräsentieren.

Beispiel für Autorisierungsgranularität

Als Beispiel für die Verwendung von Autorisierungen können Sie sich Folgendes vorstellen: Ein Benutzer in der Rolle "Operator" ist möglicherweise auf die Autorisierung `solaris.admin.usermgr.read` beschränkt, die Lese-, aber keinen Schreibzugriff auf die Benutzerkonfigurationsdateien bietet. Die Rolle "System Administrator" beinhaltet normalerweise die Autorisierungen `solaris.admin.usermgr.read` und `solaris.admin.usermgr.write` zum Durchführen von Änderungen an Benutzerdateien. Ohne die Autorisierung `solaris.admin.usermgr.pswd` kann der Systemadministrator keine Passwörter ändern. Der Primäradministrator verfügt über alle drei dieser Autorisierungen.

Die Autorisierung `solaris.admin.usermgr.pswd` ist erforderlich, um Passwortänderungen im Solaris Management Console-Benutzertool vorzunehmen. Diese Autorisierung ist auch für die Verwendung der Passwortänderungsoptionen in den Befehlen `smuser`, `smmultiuser` und `smrole` erforderlich.

Delegationsautorität in Autorisierungen

Eine Autorisierung, die mit dem Suffix `grant` endet, ermöglicht Benutzern oder Rollen, zugewiesene Autorisierungen, die mit dem gleichen Präfix beginnen, anderen Benutzern zu übertragen.

Eine Rolle mit den Autorisierungen `solaris.admin.usermgr.grant` und `solaris.admin.usermgr.read` kann die Autorisierung `solaris.admin.usermgr.read` einem anderen Benutzer übertragen. Eine Rolle mit den Autorisierungen `solaris.admin.usermgr.grant` und `solaris.admin.usermgr.*` kann alle Autorisierungen mit dem Präfix `solaris.admin.usermgr` anderen Benutzern übertragen.

Datenbanken, die RBAC unterstützen

In den folgenden vier Datenbanken werden die Daten für die RBAC-Elemente gespeichert:

- **Erweiterte Benutzerattributdatenbank** (`user_attr`) : Verbindet Benutzer und Rollen mit Autorisierungen, Berechtigungen und Berechtigungsprofilen
- **Berechtigungsprofil-Attributdatenbank** (`prof_attr`) : Legt Berechtigungsprofile fest, listet die zugewiesenen Autorisierungen und Schüsselwörter des Profils auf und bestimmt die zugehörige Hilfedatei
- **Autorisierungsattributdatenbank** (`auth_attr`) : Legt Autorisierungen und ihre Attribute fest und bestimmt die zugehörige Hilfedatei
- **Ausführungsattributdatenbank** (`exec_attr`) : Bestimmt die Befehle mit Sicherheitsattributen, die spezifischen Berechtigungsprofilen zugewiesen sind

Die Datenbank `policy.conf` enthält Autorisierungen, Berechtigungen und Berechtigungsprofile, die auf alle Benutzer angewendet werden. Weitere Informationen finden Sie unter „Datei `policy.conf`“ auf Seite 260.

RBAC-Datenbankbeziehungen

Jede RBAC-Datenbank verwendet eine *key*=*value*-Syntax zum Speichern von Attributen. Diese Methode ermöglicht spätere Erweiterung der Datenbanken. Durch die Methode kann ein System außerdem weiterhin ausgeführt werden, wenn ein der zugehörigen Richtlinie unbekanntes Schlüsselwort gefunden wird. Der Inhalt von *key*=*value* verknüpft die Dateien. Die folgenden verknüpften Einträge aus den vier Datenbanken zeigen, wie die RBAC-Datenbanken zusammen verwendet werden.

BEISPIEL 10–1 Anzeigen von RBAC-Datenbankverbindungen

Im folgenden Beispiel erhält der Benutzer `jdoe` die Funktionen des Berechtigungsprofils "File System Management" durch die ihm zugewiesene Rolle `filemgr`.

1. Dem Benutzer `jdoe` wird die Rolle `filemgr` im Benutzereintrag `jdoe` in der Datenbank `user_attr` zugewiesen.

   ```
   # user_attr - user definition
   jdoe::::type=normal;roles=filemgr
   ```

2. Die Rolle `filemgr` wird dem Berechtigungsprofil "File System Management" im Eintrag der Rolle in der Datenbank `user_attr` zugewiesen.

   ```
   # user_attr - role definition
   filemgr::::profiles=File System Management;type=role
   ```

   Der Benutzer und die Rolle werden in den Dateien `passwd` und `shadow` auf dem lokalen System oder in äquivalenten Datenbanken in einem verteilten Naming Service eindeutig festgelegt.

3. Das Berechtigungsprofil "File System Management" wird in der Datenbank `prof_attr` festgelegt. Diese Datenbank weist zudem dem Eintrag "File System Management" drei Autorisierungssätze zu.

   ```
   # prof_attr - rights profile definitions and assigned authorizations
   File System Management:::Manage, mount, share file systems:
   help=RtFileSysMngmnt.html;
   auths=solaris.admin.fsmgr.*,solaris.admin.diskmgr.*,solaris.admin.volmgr.*
   ```

4. Die Autorisierungen werden in der Datenbank `auth_attr` festgelegt.

   ```
   # auth_attr - authorization definitions
   solaris.admin.fsmgr.:::Mounts and Shares::help=AuthFsmgrHeader.html
   solaris.admin.fsmgr.read:::View Mounts and Shares::help=AuthFsmgrRead.html
   solaris.admin.fsmgr.write:::Mount and Share Files::help=AuthFsmgrWrite.html
   ```

5. Dem Berechtigungsprofil "File System Management" werden Befehle mit Sicherheitsattributen in der Datenbank `exec_attr` zugewiesen.

BEISPIEL 10–1 Anzeigen von RBAC-Datenbankverbindungen *(Fortsetzung)*

```
# exec_attr - rights profile names with secured commands
File System Management:suser:cmd:::/usr/sbin/mount:uid=0
File System Management:suser:cmd:::/usr/sbin/dfshares:euid=0
...
File System Management:solaris:cmd:::/usr/sbin/mount:privs=sys_mount
...
```

RBAC-Datenbanken und die Naming Services

Der Name Service-Bereich der RBAC-Datenbanken kann nur auf den lokalen Host angewendet werden. Der Bereich kann zudem alle Hosts umfassen, die einen Naming Service wie NIS, NIS+ oder LDAP verwenden. Welcher Naming Service Vorrang hat, wird für alle Datenbanken in der Datei `/etc/nsswitch.conf` festgelegt.

- `auth_attr` **Eintrag**: Legt die Naming Service-Rangordnung für die Datenbank `auth_attr` fest
- `passwd` **Eintrag**: Legt die Naming Service-Rangordnung für die Datenbank `user_attr` fest
- `prof_attr` **Eintrag**: Legt die Naming Service-Rangordnung für die Datenbank `prof_attr` fest. Legt zudem die Naming Service-Rangordnung für die Datenbank `exec_attr` fest.

  Wird z. B. ein Befehl mit Sicherheitsattributen einem Berechtigungsprofil zugewiesen, das in zwei Naming Services vorhanden ist, wird nur der Eintrag im ersten Service verwendet.

Datenbank `user_attr`

Die Datenbank `user_attr` enthält Benutzer- und Rolleninformationen, die die Datenbanken `passwd` und `shadow` ergänzen. Die Datenbank `user_attr` enthält erweiterte Benutzerattribute wie Autorisierungen, Berechtigungsprofile, Berechtigungen und zugewiesene Rollen. Die Felder in der Datenbank `user_attr` sind folgendermaßen durch Doppelpunkte getrennt:

```
user:qualifier:res1:res2:attr
```

Die Felder haben folgende Bedeutung:

`user`
: Der Name des Benutzers oder der Rolle wie in der Datenbank `passwd` angegeben.

`qualifier:res1:res2`
: Diese Felder sind für spätere Verwendung reserviert.

`attr`
: Eine optionale Liste durch Semikola (`;`) getrennter Schlüsselwertpaare, die die anzuwendenden Sicherheitsattribute beschreibt, wenn der Benutzer Befehle ausführt. Die vier gültigen Schlüssel sind `type`, `auths`, `profiles` und `roles`.

- Das `type`-Schlüsselwort kann auf `normal` gesetzt werden, wenn dieses Konto für einen normalen Benutzer gedacht ist. Der `type` ist `role`, wenn das Konto für eine Rolle gedacht ist.
- Das Schlüsselwort `auths` legt eine durch Kommata getrennte Liste mit Autorisierungsnamen fest, die aus in der Datenbank `auth_attr` festgelegten Namen ausgewählt werden. Autorisierungsnamen können Sternchen (*) als Platzhalter enthalten. `solaris.device.*` steht beispielsweise für alle Oracle Solaris-Geräteautorisierungen.
- Das Schlüsselwort `profiles` gibt eine geordnete, durch Kommata getrennte Liste von Berechtigungsprofilnamen aus der Datenbank `prof_attr` an. Die Reihenfolge der Berechtigungsprofile funktioniert ähnlich wie UNIX-Suchpfade. Das erste Profil in der Liste, das den auszuführenden Befehl enthält, legt fest, welche (bzw. ob) Sicherheitsattribute auf den Befehl angewendet werden.
- Das `roles`-Schlüsselwort legt eine durch Kommata getrennte Liste mit Rollennamen fest. Beachten Sie, dass Rollen in der gleichen `user_attr`-Datenbank festgelegt sind. Rollen werden durch Festlegen des Typwert als `role` angegeben. Rollen können keinen anderen Rollen zugewiesen werden.

Das folgende Beispiel zeigt, wie die Rolle "Operator" in einer typischen `user_attr`-Datenbank festgelegt wird. Das Beispiel zeigt, wie die Rolle dem Benutzer `jdoe` zugewiesen wird. Rollen und Benutzer werden durch das `type`-Schlüsselwort unterschieden.

```
% grep operator /etc/user_attr
jdoe::::type=normal;roles=operator
operator::::profiles=Operator;type=role
```

Datenbank `auth_attr`

Alle Autorisierungen werden in der Datenbank `auth_attr` gespeichert. Autorisierungen können Benutzern, Rollen oder Berechtigungsprofilen zugewiesen werden. Die bevorzugte Methode besteht darin, Autorisierungen in einem Berechtigungsprofil zu platzieren, das Profil in die Profilliste einer Rolle aufzunehmen und die Rolle anschließend einem Benutzer zuzuweisen.

Die Felder in der Datenbank `auth_attr` sind folgendermaßen durch Doppelpunkte getrennt:

```
authname:res1:res2:short_desc:long_desc:attr
```

Die Felder haben folgende Bedeutung:

`authname` Eine eindeutige Zeichenfolge, die zum Identifizieren der Autorisierung im Format *prefix* verwendet wird.[*suffix*]. Autorisierungen für Oracle Solaris verwenden `solaris` als Präfix. Alle anderen Autorisierungen sollten ein Präfix verwenden, das mit dem Internetdomainnamen der Organisation, die die

Autorisierung erstellt (z. B. `com.xyzcompany`) in umgekehrter Reihenfolge beginnt. Das Suffix zeigt an, was autorisiert wird; normalerweise ist dies der funktionale Bereich und Vorgang.

Wenn `authname` aus einem Präfix und einem funktionalen Bereich besteht und mit einem Punkt endet, fungiert `authname` als Überschrift, die in den GUIs von Anwendungen verwendet werden kann. Ein zweiteiliger `authname` ist keine tatsächliche Autorisierung. Der `authname` von `solaris.printmgr.` ist ein Beispiel für eine Überschrift.

Wenn `authname` mit dem Wort "grant" (gewähren) endet, fungiert `authname` als Gewährungsautorisierung. Eine Gewährungsautorisierung ermöglicht dem Benutzer, anderen Benutzern Autorisierungen mit dem gleichen Präfix und funktionalen Bereich zu übertragen. Der `authname` von `solaris.printmgr.grant` ist ein Beispiel für eine Gewährungsautorisierung. `solaris.printmgr.grant` verleiht dem Benutzer das Recht, anderen Benutzern Autorisierungen wie `solaris.printmgr.admin` und `solaris.printmgr.nobanner` zu übertragen.

`res1:res2` Für spätere Verwendung reserviert

`short_desc` Ein Kurzname für die Autorisierung. Dieser Kurzname ist für die Anzeige in Benutzeroberflächen geeignet, z. B. in einer Bildlaufliste einer GUI.

`long_desc` Eine lange Beschreibung. Dieses Feld identifiziert den Zweck der Autorisierung, die Anwendungen, in denen die Autorisierung verwendet wird, und den Benutzertyp, der die Autorisierung möglicherweise verwendet. Die lange Beschreibung kann im Hilfetext einer Anwendung angezeigt werden.

`attr` Eine optionale Liste durch Semikola (;) getrennter Schlüsselwertpaare, die die Attribute einer Autorisierung beschreiben. Es können null oder mehr Schlüssel angegeben werden.

Das Schlüsselwort `help` identifiziert eine Hilfedatei in HTML. Auf Hilfedateien kann über die Datei `index.html` im Verzeichnis `/usr/lib/help/auths/locale/C` zugegriffen werden.

Das folgende Beispiel zeigt eine `auth_attr`-Datenbank mit einigen typischen Werten:

```
% grep printer /etc/security/auth_attr
solaris.admin.printer.:::Printer Information::help=AuthPrinterHeader.html
solaris.admin.printer.delete:::Delete Printer Information::help=AuthPrinterDelete.html
solaris.admin.printer.modify:::Update Printer Information::help=AuthPrinterModify.html
solaris.admin.printer.read:::View Printer Information::help=AuthPrinterRead.html
```

Beachten Sie, dass `solaris.admin.printer.` als Überschrift definiert ist, da der Autorisierungsname mit einem Punkt (.) endet. Überschriften werden von den GUIs zum Organisieren von Autorisierungsfamilien verwendet.

Datenbank `prof_attr`

In der Datenbank `prof_attr` werden Name, Beschreibung, Speicherort der Hilfedatei, Berechtigungen und Autorisierungen gespeichert, die den Berechtigungsprofilen zugewiesen werden. Die Befehle und Sicherheitsattribute, die Berechtigungsprofilen zugewiesen werden, werden in der Datenbank `exec_attr` gespeichert. Weitere Informationen erhalten Sie unter „Datenbank `exec_attr`“ auf Seite 259. Die Felder in der Datenbank `prof_attr` sind folgendermaßen durch Doppelpunkte getrennt:

```
profname:res1:res2:desc:attr
```

Die Felder haben folgende Bedeutung:

`profname` Der Name des Berechtigungsprofils. Bei Berechtigungsprofilnamen wird nach Groß- und Kleinschreibung unterschieden. Dieser Name wird auch von der Datenbank `user_attr` verwendet, um die Profile anzuzeigen, die Rollen und Benutzern zugewiesen werden.

`res1:res2` Für spätere Verwendung reserviert

`desc` Eine lange Beschreibung. In diesem Feld sollte der Zweck des Berechtigungsprofils erläutert sowie angegeben werden, welcher Benutzertyp an der Verwendung des Profils interessiert sein könnte. Die lange Beschreibung sollte zur Anzeige im Hilfetext einer Anwendung geeignet sein.

`attr` Eine optionale Liste mit durch Semikola (;) getrennten Schlüsselwertpaaren, die die Sicherheitsattribute beschreibt, die bei der Ausführung auf das Objekt angewendet werden sollen. Es können null oder mehr Schlüssel angegeben werden. Die gültigen Schlüssel sind `help`. `profiles` und `auths`.

Das Schlüsselwort `help` identifiziert eine Hilfedatei in HTML. Auf Hilfedateien kann über die Datei `index.html` im Verzeichnis `/usr/lib/help/profiles/locale/C` zugegriffen werden.

Das Schlüsselwort `profiles` gibt eine durch Kommata getrennte Liste von Berechtigungsprofilen an. Diese Profile werden als *supplementary rights profiles* (zusätzliche Berechtigungsprofile) bezeichnet.

Das Schlüsselwort `auths` gibt eine durch Kommata getrennte Liste mit Autorisierungsnamen an, die aus den in der Datenbank `auth_attr` definierten Namen ausgewählt werden. Autorisierungsnamen können mit einem Sternchen (*) als Platzhalter angegeben werden.

Das Schlüsselwort `privs` gibt eine durch Kommata getrennte Liste mit Berechtigungen an. Diese Berechtigungen gelten für alle Befehle in einer Profil-Shell.

Das folgende Beispiel zeigt zwei typische `prof_attr`-Datenbankeinträge. Beachten Sie, dass das Berechtigungsprofil "Printer Management" ein zusätzliches Berechtigungsprofil des Berechtigungsprofils "Operator" ist. Das Beispiel enthält einen Zeilenumbruch, um eine übersichtlichere Darstellung zu ermöglichen.

```
% grep 'Printer Management' /etc/security/prof_attr
Printer Management:::                   Name of rights profile
Manage printers, daemons, spooling:     Description
help=RtPrntAdmin.html;                  Help file
auths=solaris.admin.printer.read,       Authorizations
solaris.admin.printer.modify,solaris.admin.printer.delete
...
Operator:::                             Name of rights profile
Can perform simple administrative tasks:    Description
profiles=Printer Management,            Supplementary rights profiles
Media Backup,All;
help=RtOperator.html                    Help file
```

Datenbank `exec_attr`

Die Datenbank `exec_attr` legt Befehle fest, die Sicherheitsattribute zur erfolgreichen Ausführung erfordern. Die Befehle sind Teil eines Berechtigungsprofils. Ein Befehl und seine Sicherheitsattribute können von Rollen oder Benutzern ausgeführt werden, denen das Profil zugewiesen ist.

Die Felder in der Datenbank `exec_attr` sind folgendermaßen durch Doppelpunkte getrennt:

```
name:policy:type:res1:res2:id:attr
```

Die Felder haben folgende Bedeutung:

`profname`	Der Name des Berechtigungsprofils. Bei Berechtigungsprofilnamen wird nach Groß- und Kleinschreibung unterschieden. Der Name bezieht sich auf ein Profil in der Datenbank `prof_attr`.
`policy`	Die mit diesem Eintrag verbundene Sicherheitsrichtlinie. Derzeit sind `suser` und `solaris` die gültigen Einträge. Die `solaris`-Richtlinie erkennt Berechtigungen. Die `suser`-Richtlinie kann dies nicht.
`type`	Der Typ der angegebenen Entität. Derzeit ist `cmd` (Befehl) der einzige gültige Entitätstyp.
`res1:res2`	Für spätere Verwendung reserviert

`id` Eine Zeichenfolge, die die Entität identifiziert. Befehle sollten über den vollständigen Pfad oder einen Pfad mit einem Platzhalter (*) verfügen. Um Argumente anzugeben, schreiben Sie ein Skript mit den Argumenten und verweisen mit der `id` auf das Skript.

`attr` Eine optionale Liste durch Semikola (;) getrennter Schlüsselwertpaare, die die Sicherheitsattribute beschreibt, die bei der Ausführung auf die Entität angewendet werden sollen. Es können null oder mehr Schlüssel angegeben werden. Die Liste gültiger Schlüsselwörter hängt von der angewandten Richtlinie ab.

Für die Richtlinie `suser` lauten die vier gültigen Schlüssel `euid`, `uid`, `egid` und `gid`.

- Die Schlüsselwörter `euid` und `uid` enthalten einen einzelnen Benutzernamen oder eine numerische Benutzer-ID (UID). Befehle, die mit `euid` bezeichnet sind, werden mit der angegebenen UID ausgeführt, ähnlich dem Festlegen des `setuid`-Bit in einer ausführbaren Datei. Befehle, die mit `uid` bezeichnet sind, können sowohl mit der realen UID als auch mit der effektiven UID ausgeführt werden.
- Die Schlüsselwörter `egid` und `gid` enthalten einen einzelnen Gruppennamen oder eine numerische Gruppen-ID (GID). Befehle, die mit `egid` bezeichnet sind, werden mit der angegebenen GID ausgeführt, ähnlich dem Festlegen des `setgid`-Bit in einer ausführbaren Datei. Befehle, die mit `gid` bezeichnet sind, können sowohl mit der realen GID als auch mit der effektiven GID ausgeführt werden.

Für die `solaris`-Richtlinie lautet das gültige Schlüsselwort `privs`. Der Wert besteht aus einer Liste durch Kommata getrennter Berechtigungen.

Das folgende Beispiel zeigt einige typische Werte aus einer `exec_attr`-Datenbank:

```
% grep 'File System Management' /etc/security/exec_attr
File System Management:suser:cmd:::/usr/sbin/ff:euid=0
File System Management:solaris:cmd:::/usr/sbin/mount:privs=sys_mount
...
```

Datei `policy.conf`

Die Datei `policy.conf` bietet eine Methode zum Gewähren spezifischer Berechtigungsprofile, Autorisierungen und Berechtigungen für alle Benutzer. Die relevanten Einträge in der Datei bestehen aus *key*=*value*-Paaren:

- `AUTHS_GRANTED`=*authorizations*: Bezieht sich auf eine oder mehrere Autorisierungen
- `PROFS_GRANTED`=*rights profiles*: Bezieht sich auf ein oder mehrere Berechtigungsprofile

- `PRIV_DEFAULT=`*privileges*: Bezieht sich auf eine oder mehrere Berechtigungen
- `PRIV_LIMIT=`*privileges*: Bezieht sich auf alle Berechtigungen

Das folgende Beispiel zeigt einige typische Werte aus einer `policy.conf`-Datenbank:

```
# grep AUTHS /etc/security/policy
AUTHS_GRANTED=solaris.device.cdrw

# grep PROFS /etc/security/policy
PROFS_GRANTED=Basic Solaris User

# grep PRIV /etc/security/policy

#PRIV_DEFAULT=basic
#PRIV_LIMIT=all
```

Weitere Informationen zu Berechtigungen finden Sie unter „Berechtigungen (Übersicht)“ auf Seite 201.

RBAC-Befehle

In diesem Abschnitt werden Befehle aufgeführt, die zum Verwalten von RBAC verwendet werden. Zudem wird eine Liste mit Befehlen zur Verfügung gestellt, deren Zugriff durch Autorisierungen gesteuert werden kann.

Befehle zum Verwalten von RBAC

Auch wenn Sie die lokalen RBAC-Datenbanken manuell bearbeiten können, wird von dieser Vorgehensweise wird nachdrücklich abgeraten. Die folgenden Befehle stehen für die Verwaltung des Zugriffs auf Aufgaben mit RBAC zur Verfügung.

TABELLE 10–7 RBAC-Verwaltungsbefehle

Manpage für Befehl	Beschreibung
`auths(1)`	Zeigt Autorisierungen für einen Benutzer an
`makedbm(1M)`	Erstellt eine `dbm`-Datei
`nscd(1M)`	Name Service-Cache-Dämon, nützlich zum Zwischenspeichern der Datenbanken `user_attr`, `prof_attr` und `exec_attr`. Verwenden Sie den Befehl `svcadm`, um den Dämon neu zu starten.
`pam_roles(5)`	Modul zur Rollenkontoverwaltung für PAM. Sucht nach der Autorisierung, die eine Rolle annehmen soll.

TABELLE 10–7 RBAC-Verwaltungsbefehle *(Fortsetzung)*

Manpage für Befehl	Beschreibung
`pfexec(1)`	Wird von Profil-Shells zum Ausführen von Befehlen mit Sicherheitsattributen verwendet, die in der Datenbank `exec_attr` angegeben sind
`policy.conf(4)`	Konfigurationsdatei für Systemsicherheitsrichtlinie. Listet gewährte Autorisierungen, Berechtigungen und weitere Sicherheitsinformationen auf.
`profiles(1)`	Zeigt Berechtigungsprofile für einen angegebenen Benutzer an
`roles(1)`	Zeigt Rollen an, die ein angegebener Benutzer annehmen kann
`roleadd(1M)`	Fügt eine Rolle zu einem lokalen System hinzu
`roledel(1M)`	Löscht eine Rolle von einem lokalen System
`rolemod(1M)`	Ändert die Eigenschaften einer Rolle auf einem lokalen System
`smattrpop(1M)`	Überführt die Quelldatenbank für Sicherheitsattribute in die Zieldatenbank. Für die Verwendung in Situationen, in denen lokale Datenbanken in einen Naming Service überführt werden müssen. Auch zur Verwendung in Upgrades, in denen keine Konvertierungsskripten zur Verfügung stehen.
`smexec(1M)`	Verwaltet Einträge in der Datenbank `exec_attr`. Erfordert Authentifizierung
`smmultiuser(1M)`	Verwaltet Massenvorgänge in Benutzerkonten. Erfordert Authentifizierung
`smprofile(1M)`	Verwaltet Berechtigungsprofile in den Datenbanken `prof_attr` und `exec_attr`. Erfordert Authentifizierung
`smrole(1M)`	Verwaltet Rollen und Benutzer in Rollenkonten. Erfordert Authentifizierung
`smuser(1M)`	Verwaltet Benutzereinträge. Erfordert Authentifizierung
`useradd(1M)`	Fügt ein Benutzerkonto zum System hinzu. Die Option `-R` weist einem Benutzerkonto eine Rolle zu.
`userdel(1M)`	Löscht eine Benutzeranmeldung vom System.
`usermod(1M)`	Ändert die Kontoeigenschaften eines Benutzers auf dem System.

Befehle, die Autorisierungen erfordern

Die folgende Tabelle bietet Beispiele dazu, wie Autorisierungen zum Begrenzen von Befehlsoptionen auf einem Oracle Solaris-System verwendet werden. Weitere Diskussionen zum Thema Autorisierungen finden Sie unter „Autorisierungsbenennung und -delegation“ auf Seite 252.

TABELLE 10–8 Befehle und zugehörige Autorisierungen

Manpage für Befehl	Autorisierungsanforderungen
at(1)	`solaris.jobs.user` für alle Optionen erforderlich (wenn weder `at.allow`- noch `at.deny`-Dateien vorhanden sind)
atq(1)	`solaris.jobs.admin` für alle Optionen erforderlich
cdrw(1)	`solaris.device.cdrw` ist für alle Optionen erforderlich und wird standardmäßig in der Datei `policy.conf` gewährt
crontab(1)	`solaris.jobs.user` ist für die Option erforderlich, um einen Job einzureichen (wenn weder `crontab.allow`- noch `crontab.deny`-Dateien vorhanden sind)
	`solaris.jobs.admin` ist erforderlich, damit die Optionen die `crontab`-Dateien anderer Benutzer auflisten oder ändern können
allocate(1)	`solaris.device.allocate` (oder eine andere Autorisierung wie in der Datei `device_allocate` angegeben) ist für die Gerätezuordnung erforderlich
	`solaris.device.revoke` (oder eine andere Autorisierung wie in der Datei `device_allocate` angegeben) ist erforderlich, um ein Gerät einem anderen Benutzer zuzuordnen (Option `-F`)
deallocate(1)	`solaris.device.allocate` (oder eine andere Autorisierung wie in der Datei `device_allocate` angegeben) ist zum Aufheben der Zuordnung des Geräts eines anderen Benutzers erforderlich
	`solaris.device.revoke` (oder eine andere Autorisierung wie in der Datei `device_allocate`) ist erforderlich, um die Aufhebung der Zuordnung des angegebenen Geräts (Option `-F`) oder aller Geräte (Option `-I`) zu erzwingen
list_devices(1)	`solaris.device.revoke` ist erforderlich, um die Geräte eines anderen Benutzers aufzulisten (Option `-U`)
sendmail(1M)	`solaris.mail` ist erforderlich, um auf Mail-Subsystemfunktionen zuzugreifen; `solaris.mail.mailq` ist zum Anzeigen der Mailwarteschlange erforderlich

◆ ◆ ◆ KAPITEL 11

Berechtigungen (Aufgaben)

In diesem Kapitel erhalten Sie schrittweise Anleitungen zum Verwalten und Verwenden von Berechtigungen auf Ihrem System. Im Folgenden ist eine Liste der Informationen in diesem Kapitel aufgeführt.

- „Verwalten und Verwenden von Berechtigungen (Übersicht der Schritte)“ auf Seite 265
- „Verwalten von Berechtigungen (Übersicht der Schritte)“ auf Seite 266
- „Festlegen Ihrer Berechtigungen (Übersicht der Schritte)“ auf Seite 275

Eine Berechtigungsübersicht finden Sie unter „Berechtigungen (Übersicht)“ auf Seite 201. Referenzinformationen erhalten Sie in Kapitel 12, „Berechtigungen (Referenz)“.

Verwalten und Verwenden von Berechtigungen (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf Übersichten zum Verwalten und Verwenden von Berechtigungen.

Aufgabe	Beschreibung	Anweisungen
Verwenden von Berechtigungen auf Ihrer Site	Umfasst das Zuweisen, Entfernen, Hinzufügen und die Fehlersuche bei der Verwendung von Berechtigungen	„Verwalten von Berechtigungen (Übersicht der Schritte)“ auf Seite 266
Verwenden von Berechtigungen beim Ausführen eines Befehls	Umfasst das Verwenden der Ihnen zugewiesenen Berechtigungen	„Festlegen Ihrer Berechtigungen (Übersicht der Schritte)“ auf Seite 275

Verwalten von Berechtigungen (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf Vorgänge zum Anzeigen von Berechtigungen, Zuweisen von Berechtigungen und Ausführen eines Skripts, das privilegierte Befehle enthält.

Aufgabe	Beschreibung	Anweisungen
Festlegen der Berechtigungen, die sich in einem Prozess befinden	Führt die effektiven, vererbbaren, zugelassenen und begrenzten Berechtigungssätze für einen Prozess auf	„So legen Sie die Berechtigungen auf einem Prozess fest“ auf Seite 267
Festlegen, welche Berechtigungen bei einem Prozess fehlen	Führt die Berechtigungen auf, die ein fehlgeschlagener Prozess zur erfolgreichen Ausführung erfordert	„So legen Sie die für ein Programm erforderlichen Berechtigungen fest“ auf Seite 268
Hinzufügen von Berechtigungen zu einem Befehl	Fügt Berechtigungen zu einem Befehl in einem Berechtigungsprofil hinzu. Benutzern oder Rollen kann das Berechtigungsprofil zugewiesen werden. Die Benutzer können den Befehl dann mit den zugewiesenen Berechtigungen in einer Profil-Shell ausführen.	„So fügen Sie Berechtigungen zu einem Befehl hinzu“ auf Seite 270
Zuweisen von Berechtigungen zu einem Benutzer	Erweitert den vererbbaren Berechtigungssatz eines Benutzers oder einer Rolle. Verwenden Sie dieses Verfahren mit Vorsicht.	„So weisen Sie Berechtigungen einem Benutzer oder einer Rolle zu“ auf Seite 271
Einschränken der Berechtigungen eines Benutzers	Beschränkt den grundlegenden Berechtigungssatz des Benutzers. Verwenden Sie dieses Verfahren mit Vorsicht.	„So begrenzen Sie die Berechtigungen eines Benutzers oder einer Rolle“ auf Seite 272
Ausführen eines privilegierten Shell-Skripts	Fügt einem Shell-Skript und den darin enthaltenen Befehlen Berechtigungen hinzu. Anschließend wird das Skript in einer Profil-Shell ausgeführt.	„So führen Sie ein Shell-Skript mit privilegierten Befehlen aus“ auf Seite 274

Verwalten von Berechtigungen

Die sicherste Art zum Verwalten von Berechtigungen für Benutzer und Rollen besteht darin, die Verwendung von Berechtigungen auf Befehle in einem Berechtigungsprofil zu beschränken. Das Berechtigungsprofil wird dann in eine Rolle eingeschlossen. Die Rolle wird einem Benutzer zugewiesen. Wenn der Benutzer die ihm zugewiesene Rolle annimmt, stehen die privilegierten Befehle zur Ausführung in einer Profil-Shell zur Verfügung. Die folgenden Verfahren zeigen, wie Sie Berechtigungen zuweisen, entfernen und Fehler bei der Verwendung von Berechtigungen suchen können.

▼ So legen Sie die Berechtigungen auf einem Prozess fest

Dieses Verfahren zeigt, wie Sie festlegen können, welche Berechtigungen Ihren Prozessen zur Verfügung stehen. Die Liste enthält keine Berechtigungen, die bestimmten Befehlen zugewiesen wurden.

- **Listen Sie die Berechtigungen auf, die dem Prozess Ihrer Shell zur Verfügung stehen.**

```
% ppriv pid
$ ppriv -v pid
```

pid Die Prozessnummer. Verwenden Sie ein doppeltes Dollarzeichen (`$$`), um die Prozessnummer der übergeordneten Shell an den Befehl weiterzugeben.

`-v` Stellt eine ausführliche Liste der Berechtigungsnamen zur Verfügung.

Beispiel 11–1 Festlegen der Berechtigungen in Ihrer aktuellen Shell

Im folgenden Beispiel werden die Berechtigungen im übergeordneten Prozess des Shell-Prozesses des Benutzers aufgeführt. Im zweiten Beispiel werden die vollständigen Namen der Berechtigungen aufgeführt. Die einzelnen Buchstaben in der Ausgabe beziehen sich auf die folgenden Berechtigungssätze:

`E` Der effektive Berechtigungssatz

`I` Der vererbbare Berechtigungssatz

`P` Der zugelassene Berechtigungssatz

`L` Der begrenzte Berechtigungssatz.

```
% ppriv $$
1200:   -csh
flags = <none>
        E: basic
        I: basic
        P: basic
        L: all
% ppriv -v $$
1200:   -csh
flags = <none>
        E: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
        I: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
        P: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
        L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

Beispiel 11–2 Festlegen der Berechtigungen einer Rolle, die Sie annehmen können

Rollen verwenden eine administrative Shell oder Profil-Shell. Sie müssen eine Rolle annehmen und die Shell der Rolle verwenden, um die Berechtigungen aufzulisten, die der Rolle direkt zugewiesen wurden. Im folgenden Beispiel hat die Rolle `sysadmin` keine direkt zugewiesenen Berechtigungen.

```
% su - sysadmin
Password:      <Type sysadmin password>
$ /usr/ucb/whoami
sysadmin
$ ppriv -v $$
1400:   pfksh
flags = <none>
        E: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
        I: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
        P: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
        L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

▼ So legen Sie die für ein Programm erforderlichen Berechtigungen fest

Dieser Vorgang legt fest, welche Berechtigungen ein Befehl oder ein Prozess zur erfolgreichen Ausführung benötigt.

Bevor Sie beginnen Der Befehl oder Prozess muss fehlgeschlagen sein, damit dieser Vorgang ausgeführt werden kann.

1 Geben Sie den Befehl, der fehlschlägt, als Argument zum Fehlersuchbefehl `ppriv` ein.

```
% ppriv -eD touch /etc/acct/yearly
touch[11365]: missing privilege "file_dac_write"
     (euid = 130, syscall = 224) needed at ufs_direnter_cm+0x27c
touch: /etc/acct/yearly cannot create
```

2 Bestimmen Sie, welcher Systemaufruf fehlschlägt, indem Sie die `syscall`-Nummer in der Datei `/etc/name_to_sysnum` suchen.

```
% grep 224 /etc/name_to_sysnum
creat64                 224
```

Beispiel 11–3 Verwenden Sie den Befehl `truss` zum Untersuchen der Verwendung von Berechtigungen

Mit dem Befehl `truss` können Sie Fehler bei der Berechtigungsverwendung in einer normalen Shell suchen. Der folgende Befehl durchsucht z. B. den fehlgeschlagenen Prozess `touch` nach Fehlern:

```
% truss -t creat touch /etc/acct/yearly
creat64("/etc/acct/yearly", 0666)
                      Err#13 EACCES [file_dac_write]
touch: /etc/acct/yearly cannot create
```

Die erweiterten `/proc`-Schnittstellen melden die fehlende Berechtigung nach dem Fehlercode in der Ausgabe `truss`.

Beispiel 11–4 Verwenden des Befehls `ppriv` zum Untersuchen der Berechtigungsverwendung in einer Profil-Shell

Mit dem Befehl `ppriv` können Sie die Verwendung von Berechtigungen in einer Profil-Shell nach Fehlern durchsuchen. Wenn Sie einem Benutzer ein Berechtigungsprofil zuweisen und das Berechtigungsprofil Befehle mit Berechtigungen enthält, müssen die Befehle in einer Profil-Shell eingegeben werden. Wenn die privilegierten Befehle in eine normale Shell eingegeben werden, werden die Befehle nicht mit Berechtigung ausgeführt.

In diesem Beispiel kann der Benutzer `jdoe` die Rolle `objadmin` annehmen. Die Rolle `objadmin` enthält das Berechtigungsprofil "Object Access Management". Dieses Berechtigungsprofil ermöglicht der Rolle `objadmin`, Berechtigungen für Dateien zu ändern, über die `objadmin` nicht verfügt.

Im folgenden Auszug kann `jdoe` die Berechtigungen für die Datei `useful.script` nicht ändern:

```
jdoe% ls -l useful.script
-rw-r--r--  1 aloe  staff  2303 Apr 10 10:10 useful.script
jdoe% chown objadmin useful.script
chown: useful.script: Not owner
jdoe% ppriv -eD chown objadmin useful.script
chown[11444]: missing privilege "file_chown"
            (euid = 130, syscall = 16) needed at ufs_setattr+0x258
chown: useful.script: Not owner
```

Wenn `jdoe` die Rolle `objadmin` annimmt, werden die Berechtigungen für die Datei geändert:

```
jdoe% su - objadmin
Password:      <Type objadmin password>
$ ls -l useful.script
-rw-r--r--  1 aloe  staff  2303 Apr 10 10:10 useful.script
$ chown objadmin useful.script
```

```
$ ls -l useful.script
-rw-r--r--  1 objadmin  staff  2303 Apr 10 10:10 useful.script
$ chgrp admin useful.script
$ ls -l objadmin.script
-rw-r--r--  1 objadmin  admin  2303 Apr 10 10:11 useful.script
```

Beispiel 11–5 Ändern einer Datei, die dem `root`-Benutzer gehört

Dieses Beispiel zeigt den Schutz gegen Berechtigungseskalation. Eine Diskussion hierzu finden Sie unter „Verhindern von Berechtigungseskalation“ auf Seite 284. Die Datei gehört dem `root`-Benutzer. Die weniger leistungsstarke Rolle, `objadmin`, benötigt zum Ändern der Eigentümerschaft der Datei alle Berechtigungen; daher schlägt der Vorgang fehl.

```
jdoe% su - objadmin
Password:      <Type objadmin password>
$ cd /etc; ls -l system
-rw-r--r--  1 root  sys   1883 Oct 10 10:20 system
$ chown objadmin system
chown: system: Not owner
$ ppriv -eD chown objadmin system
chown[11481]: missing privilege "ALL"
     (euid = 101, syscall = 16) needed at ufs_setattr+0x258
chown: system: Not owner
```

▼ So fügen Sie Berechtigungen zu einem Befehl hinzu

Sie fügen einem Befehl Berechtigungen hinzu, wenn Sie den Befehl einem Berechtigungsprofil hinzufügen. Die Berechtigungen aktivieren die Rolle, die das Berechtigungsprofil zum Ausführen des administrativen Befehls enthält, erhalten jedoch keine anderen Superuser-Fähigkeiten.

Bevor Sie beginnen Der Befehl oder das Programm muss Berechtigungen erkennen. Eine vollständigere Diskussion hierzu finden Sie unter „Zuweisen von Berechtigungen zu Prozessen“ auf Seite 207.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2. **Öffnen Sie die Solaris Management Console-GUI.**

   Eine Anleitung hierzu finden Sie unter „So nehmen Sie eine Rolle in der Solaris Management Console an“ auf Seite 232.

3 **Verwenden Sie das Berechtigungstool, um ein angemessenes Profil zu aktualisieren.**

Wählen Sie den Befehl, den Sie einschließen möchten. Fügen Sie für jeden enthaltenen Befehl die erforderlichen Berechtigungen hinzu.

Achtung – Wenn Sie Befehle in ein Berechtigungsprofil einschließen und den Befehlen Berechtigungen hinzufügen, werden die Befehle mit diesen Berechtigungen ausgeführt, wenn die Befehle in einer Profil-Shell ausgeführt werden.

Die Reihenfolge der Profile ist relevant. Die Profil-Shell führt einen Befehl oder eine Aktion mit den Sicherheitsattributen aus, die im ersten Profil in der Profilliste des Kontos angegeben sind. Wenn sich z. B. der Befehl `chgrp` im Berechtigungsprofil "Object Access Management" mit Berechtigungen befindet und "Object Access Management" das erste Profil darstellt, in dem der Befehl `chgrp` gefunden wird, wird der Befehl `chgrp` mit den im Profil "Object Access Management" angegebenen Berechtigungen ausgeführt.

▼ So weisen Sie Berechtigungen einem Benutzer oder einer Rolle zu

Sie können einigen Benutzern mit einer bestimmten Berechtigung immer vertrauen. Sehr spezifische Berechtigungen, die einen kleinen Teil des Systems beeinflussen, sind gut für die Zuweisung zu einem Benutzer geeignet. Eine Diskussion zu den Implikationen direkt zugewiesener Berechtigungen finden Sie unter „Sicherheitsüberlegungen bei direkter Zuweisung von Sicherheitsattributen“ auf Seite 201.

Das folgende Verfahren ermöglicht dem Benutzer `jdoe` die Verwendung hochauflösender Timer.

1 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Fügen Sie die Berechtigung hinzu, die hochauflösende Timer zu den ursprünglichen vererbbaren Berechtigungssätzen des Benutzers hinzufügt.**

```
$ usermod -K defaultpriv=basic,proc_clock_highres jdoe
```

Die Werte für das `defaultpriv`-Schlüsselwort ersetzen die vorhandenen Werte. Daher muss der Wert `basic` angegeben werden, damit der Benutzer die `basic`-Rechte beibehalten kann. In der Standardkonfiguration verfügen alle Benutzer über grundlegende Berechtigungen.

3 Lesen Sie den erzeugten `user_attr`-Eintrag.

```
$ grep jdoe /etc/user_attr
jdoe::::type=normal;defaultpriv=basic,proc_clock_highres
```

Beispiel 11–6 Erstellen einer Rolle mit Berechtigungen zum Konfigurieren der Systemzeit

In diesem Beispiel wird eine Rolle erstellt, deren einzige Aufgabe die Verwaltung der Systemzeit ist.

```
$ /usr/sadm/bin/smrole -D nisplus:/examplehost/example.domain \
-r primaryadm -l <Type primaryadm password> \
add -- -n clockmgr \
-c "Role that sets system time" \
-F "Clock Manager" \
-s /bin/pfksh \
-u 108 \
-P <Type clockmgr password> \
-K defaultpriv=basic,proc_priocntl,sys_cpu_config,
proc_clock_highres,sys_time
```

Die Zeile `-K` ist zu Anzeigezwecken eingeschlossen.

Würde die Rolle lokal erstellt, würde der Eintrag `user_attr` für die Rolle ähnlich dem folgenden angezeigt werden:

```
clockmgr:::Role that sets system time:
type=role;defaultpriv=basic,proc_priocntl,sys_cpu_config,
proc_clock_highres,sys_time
```

▼ So begrenzen Sie die Berechtigungen eines Benutzers oder einer Rolle

Sie können die Berechtigungen begrenzen, die einem Benutzer oder einer Rolle zur Verfügung stehen, indem Sie den grundlegenden Satz oder den begrenzten Satz reduzieren. Sie sollten einen triftigen Grund haben, wenn Sie die Berechtigungen des Benutzers auf diese Weise begrenzen, da solche Beschränkungen unerwünschte Nebeneffekte haben können.

Achtung – Sie sollten die Fähigkeiten jedes Benutzers gründlich testen, wenn sein grundlegender Satz oder der begrenzte Satz geändert wurde.

- Wenn der grundlegende Satz weniger als der Standard enthält, können Benutzer daran gehindert werden, das System zu verwenden.
- Wenn der begrenzte Satz weniger als alle Berechtigungen enthält, schlagen Prozesse, die mit einer effektiven `UID=0` ausgeführt werden müssen, möglicherweise fehl.

1. **Legen Sie die Berechtigungen im grundlegenden und im begrenzten Satz eines Benutzers fest.**

   Informationen zu diesem Vorgang finden Sie unter „So legen Sie die Berechtigungen auf einem Prozess fest“ auf Seite 267.

2. **(Optional) Entfernen Sie eine der Berechtigungen aus dem grundlegenden Satz.**

   ```
   $ usermod -K defaultpriv=basic,!priv-name username
   ```

   Durch Entfernen der Berechtigung `proc_session` hindern Sie den Benutzer daran, Prozesse außerhalb seiner aktuellen Sitzung zu untersuchen. Durch Entfernen der Berechtigung `file_link_any` hindern Sie den Benutzer daran, Hard Links zu Dateien herzustellen, die ihm nicht gehören.

Achtung – Entfernen Sie nicht die Berechtigungen `proc_fork` und `proc_exec`. Ohne diese Berechtigungen kann der Benutzer das System nicht verwenden. Tatsächlich werden diese beiden Berechtigungen nur aus gutem Grund von Dämonen entfernt, die nicht `fork()` oder `exec()` auf anderen Prozessen ausführen sollten.

3. **(Optional) Entfernen Sie eine der Berechtigungen aus dem begrenzten Satz.**

   ```
   $ usermod -K limitpriv=all,!priv-name username
   ```

4. **Testen Sie die Funktionen von *username*.**

   Melden Sie sich als *username* an und versuchen Sie, die Aufgaben auszuführen, die *username* auf dem System ausführen muss.

Beispiel 11–7 Entfernen von Berechtigungen aus dem begrenzten Satz eines Benutzers

Im folgenden Beispiel werden alle Sitzungen, die auf der ursprünglichen Anmeldung von `jdoe` basieren, daran gehindert, die Berechtigung `sys_linkdir` zu verwenden. Das bedeutet, dass der Benutzer keine Hard Links zu Verzeichnissen herstellen oder Verbindungen zu Verzeichnissen entfernen kann, selbst wenn er den Befehl `su` ausführt.

```
$ usermod -K limitpriv=all,!sys_linkdir jdoe
$ grep jdoe /etc/user_attr
jdoe::::type=normal;defaultpriv=basic;limitpriv=all,!sys_linkdir
```

Beispiel 11–8 Entfernen von Berechtigungen aus dem grundlegenden Satz eines Benutzers

Im folgenden Beispiel werden alle Sitzungen, die auf der ursprünglichen Anmeldung von `jdoe` basieren, daran gehindert, die Berechtigung `proc_session` zu verwenden. Das bedeutet, dass der Benutzer keine Prozesse außerhalb der Benutzersitzung untersuchen kann, selbst wenn er den Befehl `su` ausführt.

```
$ usermod -K defaultpriv=basic,!proc_session jdoe
```

```
$ grep jdoe /etc/user_attr
jdoe::::type=normal;defaultpriv=basic,!proc_session;limitpriv=all
```

▼ So führen Sie ein Shell-Skript mit privilegierten Befehlen aus

Hinweis – Wenn Sie ein Shell-Skript erstellen, das Befehle mit geerbten Berechtigungen ausführt, muss das geeignete Berechtigungsprofil die Befehle mit ihnen zugewiesenen Berechtigungen enthalten.

1. **Beginnen Sie das Skript mit `/bin/pfsh` oder einer anderen Profil-Shell in der ersten Zeile.**

   ```
   #!/bin/pfsh
   # Copyright (c) 2009, 2011 by Oracle Corporation
   ```

2. **Legen Sie die Berechtigungen fest, die die Befehle im Skript benötigen.**

   ```
   % ppriv -eD script-full-path
   ```

3. **Öffnen Sie die Solaris Management Console-GUI.**

   Eine Anleitung hierzu finden Sie unter „So nehmen Sie eine Rolle in der Solaris Management Console an“ auf Seite 232. Wählen Sie eine Rolle, mit der sie ein Berechtigungsprofil erstellen können, z. B. Primäradministrator.

4. **Verwenden Sie das Berechtigungstool, um ein angemessenes Profil zu erstellen oder zu aktualisieren.**

   Wählen Sie das Skript und schließen Sie im Berechtigungsprofil jeden Befehl im Shell-Skript ein, den Berechtigungen zur Ausführung benötigen. Fügen Sie für jeden enthaltenen Befehl die erforderlichen Berechtigungen hinzu.

Achtung – Die Reihenfolge der Berechtigungsprofile ist relevant. Die Profil-Shell führt die früheste Instanz eines Befehls in der Profilliste aus. Wenn sich z. B. der Befehl `chgrp` im Berechtigungsprofil "Object Access Management" befindet und "Object Access Management" das erste Profil darstellt, in dem der Befehl `chgrp` gefunden wird, wird der Befehl `chgrp` mit den im Profil "Object Access Management" angegebenen Berechtigungen ausgeführt.

5. **Fügen Sie das Berechtigungsprofil einer Rolle hinzu und weisen Sie die Rolle einem Benutzer zu.**

   Um das Profil auszuführen, nimmt der Benutzer die Rolle an und führt das Skript in der Profil-Shell der Rolle aus.

Festlegen Ihrer Berechtigungen (Übersicht der Schritte)

Die folgende Übersicht der Schritte weist auf Vorgänge zur Verwendung der Berechtigungen hin, die Ihnen zugewiesen wurden.

Aufgabe	Beschreibung	Anweisungen
Anzeigen Ihrer Berechtigungen als Benutzer in jeder Shell	Zeigt die Berechtigungen, die Ihnen direkt zugewiesen wurden. Alle Ihre Prozesse werden mit diesen Berechtigungen ausgeführt.	„So legen Sie die Ihnen direkt zugewiesenen Berechtigungen fest“ auf Seite 275
Festlegen, welche Befehle Sie mit Berechtigung ausführen können	Wenn Berechtigungen ausführbaren Dateien in einem Berechtigungsprofil zugewiesen werden, muss die ausführbare Datei in eine Profil-Shell eingegeben werden.	„So legen Sie die ausführbaren privilegierten Befehle fest“ auf Seite 277
Festlegen, welche Befehle eine Rolle mit Berechtigungen ausführen kann	Nimmt die Rolle an, um festzulegen, welche Befehle die Rolle mit Berechtigungen ausführen kann.	„So legen Sie die von einer Rolle ausführbaren privilegierten Befehle fest“ auf Seite 278

Festlegen Ihrer zugewiesenen Berechtigungen

Wenn einem Benutzer direkt Berechtigungen zugewiesen werden, gelten diese in jeder Shell. Wenn einem Benutzer nicht direkt Berechtigungen zugewiesen werden, muss der Benutzer eine Profil-Shell öffnen. Wenn sich z. B. Befehle mit zugewiesenen Berechtigungen in einem Berechtigungsprofil befinden, das in der Liste der Berechtigungsprofile des Benutzers enthalten ist, muss der Benutzer den Befehl in einer Profil-Shell ausführen.

▼ So legen Sie die Ihnen direkt zugewiesenen Berechtigungen fest

Der folgende Vorgang zeigt, wie Sie festlegen können, ob Ihnen Berechtigungen direkt zugewiesen wurden.

Achtung – Unangemessene Verwendung direkt zugewiesener Berechtigungen kann zu unbeabsichtigten Sicherheitsverletzungen führen. Informationen hierzu finden Sie unter „Sicherheitsüberlegungen bei direkter Zuweisung von Sicherheitsattributen“ auf Seite 201.

1 **Listen Sie die Berechtigungen auf, die Ihre Prozesse verwenden können.**

Weitere Informationen zu diesem Vorgang finden Sie unter „So legen Sie die Berechtigungen auf einem Prozess fest“ auf Seite 267.

2 **Rufen Sie Vorgänge auf und führen Sie Befehle in jeder beliebigen Shell aus.**

Die Berechtigungen, die im effektiven Satz aufgelistet sind, gelten während Ihrer gesamten Sitzung. Wenn Ihnen zusätzlich zum grundlegenden Satz Berechtigungen direkt zugewiesen wurden, werden diese im effektiven Satz aufgelistet.

Beispiel 11–9 Festlegen Ihrer direkt zugewiesenen Berechtigungen

Wenn Ihnen Berechtigungen direkt zugewiesen wurden, enthält Ihr grundlegender Satz mehr als der standardmäßige grundlegende Satz. In diesem Beispiel hat der Benutzer stets Zugriff auf die Berechtigung `proc_clock_highres`.

```
% /usr/ucb/whoami
jdoe
% ppriv -v $$
1800:   pfksh
flags = <none>
        E: file_link_any,...,proc_clock_highres,proc_session
        I: file_link_any,...,proc_clock_highres,proc_session
        P: file_link_any,...,proc_clock_highres,proc_session
        L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
% ppriv -vl proc_clock_highres
        Allows a process to use high resolution timers.
```

Beispiel 11–10 Festlegen der direkt zugewiesenen Berechtigungen einer Rolle

Rollen verwenden eine administrative Shell oder Profil-Shell. Benutzer, die eine Rolle annehmen, können die Shell der Rolle verwenden, um die Berechtigungen aufzulisten, die der Rolle direkt zugewiesen wurden. Im folgenden Beispiel wurden der Rolle `realtime` Berechtigungen zum Verarbeiten von Datums- und Zeitprogrammen direkt zugewiesen.

```
% su - realtime
Password:      <Type realtime password>
$ /usr/ucb/whoami
realtime
$ ppriv -v $$
1600:   pfksh
flags = <none>
        E: file_link_any,...,proc_clock_highres,proc_session,sys_time
        I: file_link_any,...,proc_clock_highres,proc_session,sys_time
        P: file_link_any,...,proc_clock_highres,proc_session,sys_time
        L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

▼ So legen Sie die ausführbaren privilegierten Befehle fest

Wenn einem Benutzer nicht direkt Berechtigungen zugewiesen werden, erhält der Benutzer mithilfe eines Berechtigungsprofils Zugriff auf privilegierte Befehle. Befehle in einem Berechtigungsprofil müssen in einer Profil-Shell ausgeführt werden.

Bevor Sie beginnen Der Benutzer oder die Rolle, der/die eine Authentifizierung bei der Solaris Management Console durchführt, muss über die Autorisierung `solaris.admin.usermgr.read` verfügen. Das Berechtigungsprofil "Basic Solaris User" enthält diese Autorisierung.

1 Legen Sie die Berechtigungsprofile fest, die Ihnen zugewiesen wurden.

```
$ /usr/sadm/bin/smuser list -- -n username -l

Authenticating as user: admin
... Please enter a string value for: password ::
...
User name:      username
User ID (UID):  130
Primary group:  staff
Secondary groups:
Comment: object mgt jobs
Login Shell: /bin/sh
Home dir server: system
Home directory: /export/home/username
AutoHome setup: True
Mail server: system
Rights: Object Access Management
Assigned Roles:
```

2 Suchen Sie die Zeile, die mit "Rights" (Rechte) beginnt.

In der Zeile "Rights" (Rechte) werden die Namen der Berechtigungsprofile aufgeführt, die Ihnen direkt zugewiesen wurden.

3 Suchen Sie die Namen der Berechtigungsprofile in der `exec_attr`-Datenbank.

```
$ cd /etc/security
$ grep "Object Access Management" exec_attr
Object Access Management:solaris:cmd:::/usr/bin/chgrp:privs=file_chown
Object Access Management:solaris:cmd:::/usr/bin/chown:privs=file_chown
Object Access Management:suser:cmd:::/usr/bin/chgrp:euid=0
Object Access Management:suser:cmd:::/usr/bin/chmod:euid=0
...
```

Die Befehle mit hinzugefügten Berechtigungen werden am Ende der `solaris`-Richtlinieneinträge aufgeführt.

4 Geben Sie die Befehle ein, die Berechtigungen in einer Profil-Shell erfordern.

Wenn die Befehle in eine normale Shell eingegeben werden, werden die Befehle nicht mit Berechtigung ausgeführt und schlagen fehl.

```
% pfsh
$
```

Beispiel 11–11 Ausführen privilegierter Befehle in einer Profil-Shell

Im folgenden Beispiel kann der Benutzer `jdoe` die Gruppenberechtigungen für eine Datei nicht von seiner normalen Shell aus ändern. `jdoe` kann jedoch die Berechtigungen durch Eingabe des Befehls in eine Profil-Shell ändern.

```
% whoami
jdoe
% ls -l useful.script
-rwxr-xr-- 1 nodoe eng 262 Apr 2 10:52 useful.script
chgrp staff useful.script
chgrp: useful.script: Not owner
% pfksh
$ /usr/ucb/whoami
jdoe
$ chgrp staff useful.script
$ chown jdoe useful.script
$ ls -l useful.script
-rwxr-xr-- 1 jdoe staff 262 Apr 2 10:53 useful.script
```

▼ So legen Sie die von einer Rolle ausführbaren privilegierten Befehle fest

Eine Rolle erhält Zugriff auf privilegierte Befehle durch ein Berechtigungsprofil, das Befehle mit zugewiesenen Berechtigungen enthält. Die sicherste Art, einem Benutzer Zugriff auf privilegierte Befehle zu gewähren, ist, ihm eine Rolle zuzuweisen. Nach dem Annehmen der Rolle kann der Benutzer alle privilegierten Befehle ausführen, die im Berechtigungsprofil für diese Rolle enthalten sind.

Bevor Sie beginnen Der Benutzer oder die Rolle, der/die eine Authentifizierung bei der Solaris Management Console durchführt, muss über die Autorisierung `solaris.admin.usermgr.read` verfügen. Das Berechtigungsprofil "Basic Solaris User" enthält diese Autorisierung.

1 Legen Sie die Rollen fest, die Sie annehmen können.

```
$ /usr/sadm/bin/smuser list -- -n username -l
Authenticating as user: primadmin
...
User name:      username
User ID (UID):  110
Primary group:  staff
```

```
Secondary groups:
Comment: Has admin roles
Login Shell: /bin/sh
...
Rights:
Assigned Roles: primadmin, admin
```

2 Suchen Sie die Zeile, die mit "Assigned Roles:" (Zugewiesene Rollen:) beginnt.

In der Zeile "Assigned Roles" (Zugewiesene Rollen) werden die Rollen aufgeführt, die Sie annehmen können.

3 Bestimmen Sie die Berechtigungsprofile, die in einer Ihrer Rollen enthalten sind.

```
% su - devadmin
Enter password:       Type devadmin password
$ whoami
devadmin
$ profiles
Device Security


$ /usr/sadm/bin/smuser list -- -n admin -l
Authenticating as user: primadmin
...
User name:      admin
User ID (UID):  101
Primary group:  sysadmin
Secondary groups:
Comment: system administrator
Login Shell: /bin/pfksh
...
Rights: System Administrator
Assigned Roles:
```

4 Suchen Sie die Namen der Berechtigungsprofile für die Rolle in der Zeile "Rights" (Rechte).

5 Suchen Sie die Berechtigungsprofile in der Datenbank `prof_attr`.

Da das Systemadministratorprofil eine Sammlung von Profilen ist, müssen Sie die Profile im Systemadministratorprofil auflisten.

```
$ cd /etc/security
$ grep "System Administrator" prof_attr
System Administrator:::Can perform most non-security administrative
tasks:profiles=Audit Review,Printer Management,Cron Management,
Device Management,File System Management,Mail Management,Maintenance
and Repair,Media Backup,Media Restore,Name Service Management,Network
Management,Object Access Management,Process Management,Software
Installation,User Management,All;help=RtSysAdmin.html
```

6 **Suchen Sie für jedes Berechtigungsprofil die Berechtigungsprofile in der Datenbank `exec_attr`.**

Das Netzwerkverwaltungsprofil beispielsweise ist ein ergänzendes Profil im Systemadministratorprofil. Das Netzwerkverwaltungsprofil enthält eine Reihe privilegierter Befehle.

```
$ cd /etc/security
$ grep "Network Management" exec_attr
Network Management:solaris:cmd:::/usr/sbin/ifconfig:privs=sys_net_config
Network Management:solaris:cmd:::/usr/sbin/route:privs=sys_net_config
...
```

Die Befehle und ihre zugewiesenen Berechtigungen befinden sich in den letzten beiden Feldern der `solaris`-Richtlinieneinträge. Sie können diese Befehle in der Profil-Shell Ihrer Rolle ausführen.

Beispiel 11–12 Ausführen der privilegierten Befehle in Ihrer Rolle

Wenn ein Benutzer eine Rolle annimmt, wird die Shell zur Profil-Shell. Daher werden die Befehle mit den Berechtigungen ausgeführt, die den Befehlen zugewiesen wurden. Im folgenden Beispiel kann die Rolle `admin` die Berechtigungen für die Datei `useful.script` ändern.

```
% whoami
jdoe
% ls -l useful.script
-rwxr-xr-- 1 elsee eng 262 Apr 2 10:52 useful.script
chgrp admin useful.script
chgrp: useful.script: Not owner
% su - admin
Password:     <Type admin password>
$ /usr/ucb/whoami
admin
$ chgrp admin useful.script
$ chown admin useful.script
$ ls -l useful.script
-rwxr-xr-- 1 admin admin 262 Apr 2 10:53 useful.script
```

◆ ◆ ◆ KAPITEL 12

Berechtigungen (Referenz)

Im Folgenden sind die Informationen zur Referenz in diesem Kapitel aufgeführt:

- „Administrative Befehle zum Verarbeiten von Berechtigungen“ auf Seite 281
- „Dateien mit Berechtigungsinformationen“ auf Seite 282
- „Berechtigungen und Prüfung“ auf Seite 283
- „Verhindern von Berechtigungseskalation“ auf Seite 284
- „Legacy-Anwendungen und das Berechtigungsmodell“ auf Seite 285

Informationen zur Verwendung von Berechtigungen erhalten Sie in Kapitel 11, „Berechtigungen (Aufgaben)“. Eine Übersicht finden Sie unter „Berechtigungen (Übersicht)“ auf Seite 201.

Administrative Befehle zum Verarbeiten von Berechtigungen

In der folgenden Tabelle werden die Befehle aufgeführt, die zum Verarbeiten von Berechtigungen zur Verfügung stehen.

TABELLE 12–1 Befehle zum Verarbeiten von Berechtigungen

Zweck	Befehl	Manpage
Untersuchen von Prozessberechtigungen	`ppriv -v` *pid*	`ppriv(1)`
Festlegen von Prozessberechtigungen	`ppriv -s` *spec*	
Auflisten der Berechtigungen auf dem System	`ppriv -l`	
Auflisten einer Berechtigung und ihrer Beschreibung	`ppriv -lv` *priv*	
Fehlersuche bei Fehlschlagen der Berechtigung	`ppriv -eD` *failed-operation*	

TABELLE 12–1 Befehle zum Verarbeiten von Berechtigungen *(Fortsetzung)*

Zweck	Befehl	Manpage
Zuweisen von Berechtigungen zu einem neuen lokalen Benutzer	`useradd`	`useradd`(1M)
Hinzufügen von Berechtigungen zu einem vorhandenen lokalen Benutzer	`usermod`	`usermod`(1M)
Zuweisen von Berechtigungen zu einem Benutzer in einem Naming Service	`smuser`	`smuser`(1M)
Zuweisen von Berechtigungen zu einer neuen lokalen Rolle	`roleadd`	`roleadd`(1M)
Hinzufügen von Berechtigungen zu einer vorhandenen lokalen Rolle	`rolemod`	`rolemod`(1M)
Zuweisen von Berechtigungen zu einer Rolle in einem Naming Service	`smrole`	`smrole`(1M)
Anzeigen der Geräterichtlinie	`getdevpolicy`	`getdevpolicy`(1M)
Festlegen der Geräterichtlinie	`devfsadm`	`devfsadm`(1M)
Aktualisieren der Geräterichtlinie auf offenen Geräten	`update_drv -p` *policy driver*	`update_drv`(1M)
Hinzufügen der Geräterichtlinie zu einem Gerät	`add_drv -p` *policy driver*	`add_drv`(1M)

Die Solaris Management Console-GUI ist das bevorzugte Tool zum Zuweisen von Berechtigungen zu Befehlen, Benutzern und Rollen. Weitere Informationen erhalten Sie unter „So nehmen Sie eine Rolle in der Solaris Management Console an“ auf Seite 232.

Dateien mit Berechtigungsinformationen

Die folgenden Dateien enthalten Informationen zu Berechtigungen.

TABELLE 12–2 Dateien mit Berechtigungsinformationen

Datei und Manpage	Schlüsselwort	Beschreibung
`/etc/security/policy.conf` `policy.conf`(4)	`PRIV_DEFAULT`	Vererbbarer Berechtigungssatz für das System
	`PRIV_LIMIT`	Begrenzter Berechtigungssatz für das System

TABELLE 12–2 Dateien mit Berechtigungsinformationen *(Fortsetzung)*

Datei und Manpage	Schlüsselwort	Beschreibung
`/etc/user_attr` `user_attr(4)`	`privs`-Schlüsselwort im Benutzer- oder Rolleneintrag `defaultpriv`-Schlüsselwort im Benutzer- oder Rolleneintrag Wert wird normalerweise in der Solaris Management Console-GUI festgelegt	Vererbbarer Berechtigungssatz für einen Benutzer oder eine Rolle
	`limitpriv`-Schlüsselwort in einem Benutzer- oder Rolleneintrag Wert wird normalerweise in der Solaris Management Console-GUI festgelegt	Begrenzter Berechtigungssatz für einen Benutzer oder eine Rolle
`/etc/security/exec_attr` `exec_attr(4)`	`privs`-Schlüsselwort im Profileintrag für den Befehl Die Richtlinie für den Befehl muss `solaris` sein.	Liste der Berechtigungen, die einem Befehl in einem Berechtigungsprofil zugewiesen sind
`syslog.conf` `syslog.conf(4)`	Systemprotokolldatei für Fehlersuchmeldungen Pfad im `priv.debug`-Eintrag	Protokoll zur Berechtigungsfehlersuche

Hinweis – Bearbeiten Sie die Datenbanken `exec_attr` und `user_attr` nicht direkt. Um Berechtigungen zu verwalten, verwenden Sie die Solaris Management Console oder Befehle wie `smuser`. Weitere Informationen erhalten Sie auf den Manpages `smc(1M)` und `smuser(1M)`. Beispiele für Vorgänge finden Sie unter „Verwalten von Berechtigungen (Übersicht der Schritte)“ auf Seite 266.

Berechtigungen und Prüfung

Die Verwendung von Berechtigungen kann geprüft werden. Wenn ein Prozess eine Berechtigung verwendet, wird die Verwendung der Berechtigung im Prüf-Token `upriv` des Prüfpfads aufgezeichnet. Wenn Berechtigungsnamen ein Teil der Aufzeichnung sind, werden sie als Text dargestellt. Die folgenden Prüfereignisse zeichnen die Verwendung von Berechtigungen auf:

- `AUE_SETPPRIV` **Prüfereignis**: Das Ereignis generiert einen Prüfdatensatz, wenn ein Berechtigungssatz geändert wird. Das Prüfereignis `AUE_SETPPRIV` befindet sich in der `pm`-Klasse.
- `AUE_MODALLOCPRIV` **Prüfereignis**: Das Prüfereignis generiert einen Prüfdatensatz, wenn eine Berechtigung von außerhalb des Kernels hinzugefügt wird. Das Prüfereignis `AUE_MODALLOCPRIV` befindet sich in der `ad`-Klasse.

- `AUE_MODDEVPLCY` **Prüfereignis**: Das Prüfereignis generiert einen Prüfdatensatz, wenn die Geräterichtlinie geändert wird. Das Prüfereignis `AUE_MODDEVPLCY` befindet sich in der `ad`-Klasse.
- `AUE_prof_cmd` **Prüfereignis**: Das Prüfereignis generiert einen Prüfdatensatz, wenn ein Befehl in einer Profil-Shell ausgeführt wird. Das Prüfereignis `AUE_prof_cmd` befindet sich in den `as`- und `ua`-Prüfklassen. Die Namen der Berechtigungen sind im Prüfdatensatz enthalten.

Die erfolgreiche Verwendung von Berechtigungen, die sich im grundlegenden Satz befinden, wird nicht geprüft. Der Versuch, eine grundlegende Berechtigung zu verwenden, die aus dem grundlegenden Satz eines Benutzers entfernt wurde, wird geprüft.

Verhindern von Berechtigungseskalation

Der Oracle Solaris-Kernel verhindert *Berechtigungseskalation*. Berechtigungseskalation findet statt, wenn eine Berechtigung einem Prozess mehr Vorgänge ermöglicht, als der Prozess eigentlich ausführen können sollte. Um zu verhindern, dass ein Prozess mehr Berechtigungen erhält als vorgesehen, ist für kritische Systemänderungen der vollständige Berechtigungssatz erforderlich. Eine Datei oder ein Prozess, die/der `root` gehört (`UID=0`), kann z. B. nur von einem Prozess mit dem vollständigen Berechtigungssatz geändert werden. Das `root`-Konto erfordert keine Berechtigungen zum Ändern einer Datei, die `root` gehört. Ein Nicht-Root-Benutzer muss jedoch über alle Berechtigungen verfügen, um eine Datei zu ändern, die `root` gehört.

Auf ähnliche Weise erfordern Vorgänge, die Zugriff auf Geräte ermöglichen, alle Berechtigungen im effektiven Satz.

Die Berechtigungen `file_chown_self` und `proc_owner` unterliegen der Berechtigungseskalation. Die Berechtigung `file_chown_self` ermöglicht einem Prozess, seine Dateien abzugeben. Die Berechtigung `proc_owner` ermöglicht einem Prozess, Prozesse, die ihm nicht gehören, zu untersuchen.

Die Berechtigung `file_chown_self` ist durch die Systemvariable `rstchown` begrenzt. Wenn die Variable `rstchown` auf Null gesetzt wird, wird die Berechtigung `file_chown_self` aus dem ursprünglichen vererbbaren Satz des Systems und aller Benutzer entfernt. Weitere Informationen zur Systemvariable `rstchown` erhalten Sie auf der Manpage `chown(1)`.

Die Berechtigung `file_chown_self` wird am sichersten einem bestimmten Befehl zugewiesen, in ein Profil platziert und einer Rolle zur Verwendung in einer Profil-Shell zugewiesen.

Die Berechtigung `proc_owner` reicht nicht aus, um eine Prozess-UID auf `0` zu setzen. Um eine beliebige Prozess-UID auf `UID=0` zu setzen, sind alle Berechtigungen erforderlich. Da die Berechtigung `proc_owner` unbeschränkten Lesezugriff auf alle Dateien auf dem System gewährt, wird die Berechtigung am sichersten einem bestimmten Befehl zugewiesen, in ein Profil platziert und einer Rolle zur Verwendung in einer Profil-Shell zugewiesen.

Achtung – Ein Benutzerkonto kann so geändert werden, dass es die Berechtigung `file_chown_self` oder die Berechtigung `proc_owner` im ursprünglichen vererbbaren Satz des Benutzers einschließt. Sie sollten übergeordnete Sicherheitsgründe dafür haben, so leistungsstarke Berechtigungen im vererbbaren Berechtigungssatz eines Benutzers, einer Rolle oder eines Systems zu platzieren.

Weitere Informationen dazu, wie Berechtigungseskalation für Geräte verhindert wird, erhalten Sie unter „Berechtigungen und Geräte“ auf Seite 210.

Legacy-Anwendungen und das Berechtigungsmodell

Um auch für Legacy-Anwendungen geeignet zu sein, können Berechtigungen sowohl im Superuser- als auch im Berechtigungsmodell implementiert werden. Der Kernel erkennt automatisch am `PRIV_AWARE`-Flag, ob ein Programm für Berechtigungen entwickelt wurde. Stellen Sie sich einen untergeordneten Prozess vor, der Berechtigungen nicht erkennt. Alle Berechtigungen, die er von seinem übergeordneten Prozess geerbt hat, stehen in den zugelassenen und effektiven Sätzen des untergeordneten Prozesses zur Verfügung. Wenn der untergeordnete Prozess eine UID auf 0 setzt, hat er möglicherweise keine vollständigen Superuser-Fähigkeiten. Die effektiven und zugelassenen Sätze des Prozesses werden auf die Berechtigungen des begrenzten Satzes des untergeordneten Prozesses beschränkt. Der begrenzte Satz eines Berechtigungen erkennenden Prozesses beschränkt auf diese Weise die nicht Berechtigungen erkennenden Root-Berechtigungen des untergeordneten Prozesses.

TEIL IV

Kryptografische Services

In diesem Abschnitt werden die zentralisierten Services beschrieben, die vom Oracle Solaris-Betriebssystem bereitgestellt werden und auf kryptografischer und Public-Key-Technologie basieren.

- Kapitel 13, „Oracle Solaris Cryptographic Framework (Übersicht)“
- Kapitel 14, „Oracle Solaris Cryptographic Framework (Aufgaben)“
- Kapitel 15, „Oracle Solaris Key Management Framework“

◆ ◆ ◆ KAPITEL 13

Oracle Solaris Cryptographic Framework (Übersicht)

In diesem Kapitel wird Oracle Solaris Cryptographic Framework vorgestellt. Im Folgenden ist eine Liste der Informationen in diesem Kapitel aufgeführt.

- „Neuerungen bei Oracle Solaris Cryptographic Framework“ auf Seite 289
- „Oracle Solaris Cryptographic Framework“ auf Seite 290
- „Terminologie in Oracle Solaris Cryptographic Framework“ auf Seite 291
- „Geltungsbereich von Oracle Solaris Cryptographic Framework“ auf Seite 292
- „Administrative Befehle in Oracle Solaris Cryptographic Framework“ auf Seite 293
- „Befehle auf Benutzerebene in Oracle Solaris Cryptographic Framework“ auf Seite 293
- „Plugins von Oracle Solaris Cryptographic Framework“ auf Seite 294
- „Kryptografische Services und Zonen“ auf Seite 295

Informationen zur Verwaltung und Verwendung von Oracle Solaris Cryptographic Framework finden Sie unter Kapitel 14, „Oracle Solaris Cryptographic Framework (Aufgaben)“.

Neuerungen bei Oracle Solaris Cryptographic Framework

Solaris 10 1/06: Die Framework-Bibliothek (`libpkcs11.so`) enthält eine neue Komponente mit dem Namen *metaslot*. Der Metaslot fungiert als einzelner, virtueller Slot, der die Fähigkeiten aller in diesem Framework installierten Token und Slots zusammenfasst. Der Metaslot ermöglicht es einer Anwendung, über einen einzigen Slot eine transparente Verbindung mit einem beliebigen verfügbaren Kryptografieservice herzustellen.

- Weitere Informationen erhalten Sie in den Definitionen zu Slot, Metaslot und Token unter „Terminologie in Oracle Solaris Cryptographic Framework“ auf Seite 291.
- Informationen zur Verwaltung des Metaslots finden Sie auf der Manpage `cryptoadm`(1M).
- Eine vollständige Liste der neuen Oracle Solaris-Funktionen sowie eine Beschreibung der Oracle Solaris-Versionen finden Sie im Handbuch *Neuerungen in Oracle Solaris 10 8/11*.

Oracle Solaris Cryptographic Framework

Oracle Solaris Cryptographic Framework stellt eine Reihe gängiger Algorithmen und PKCS #11-Bibliotheken bereit, um kryptografische Anforderungen zu verarbeiten. Die PKCS #11-Bibliotheken werden gemäß dem folgenden Standard implementiert: RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki).

Auf Kernel-Ebene verarbeitet das Framework derzeit kryptografische Anforderungen für Kerberos und IPsec. Unter Verbraucher auf Benutzerebene fallen unter anderem `libsasl` und IKE.

Die US-amerikanischen Exportgesetze erfordern die Einschränkung der Verwendung offener kryptografischer Schnittstellen. Oracle Solaris Cryptographic Framework erfüllt die Vorgaben der aktuellen Gesetze, indem es voraussetzt, dass die kryptografischen Provider für Kernel und PKCS #11 signiert werden. Weitere Erläuterungen finden Sie unter „Binäre Signaturen für Drittanbietersoftware“ auf Seite 294.

Das Framework ermöglicht *Provider* kryptografischer Services die Verwendung von deren Services durch eine Vielzahl von *Verbrauchern* im Oracle Solaris-Betriebssystem. Provider werden auch als *Plugins* bezeichnet. Das Framework ermöglicht drei Typen von Plugins:

- **Plugins auf Benutzerebene**: gemeinsam genutzte Objekte, die Services mithilfe von PKCS #11-Bibliotheken wie z. B. `pkcs11_softtoken.so.1` bereitstellen.
- **Plugins auf Kernel-Ebene**: Kernel-Module, die Implementierungen kryptografischer Algorithmen in Software bereitstellen, wie z. B. AES.

  Viele der Algorithmen in dem Framework sind mit dem SSE2-Befehlssatz für x86 sowie für SPARC-Hardware optimiert.
- **Hardware-Plugins**: Gerätetreiber und die dazugehörigen Hardwarebeschleuniger. Ein Beispiel stellen die Niagara-Chips (die Gerätetreiber ncp und n2cp) dar. Ein Hardwarebeschleuniger bietet aufwendige kryptografische Funktionen, um das Betriebssystem zu entlasten. Das Sun Crypto Accelerator 6000-Board ist ein Beispiel.

Das Framework implementiert eine Standardschnittstelle, die PKCS #11-Bibliothek v2.11, für Provider auf Benutzerebene. Die Bibliothek kann von Drittanbieteranwendungen verwendet werden, um Provider zu erreichen. Drittanbieter können zudem dem Framework signierte Bibliotheken, Kernel-Algorithmusmodule und Gerätetreiber hinzufügen. Diese Plugins werden hinzugefügt, wenn das Dienstprogramm `pkgadd` die Drittanbietersoftware installiert. Ein Diagramm mit den Hauptkomponenten des Frameworks finden Sie in Kapitel 8, „Introduction to the Oracle Solaris Cryptographic Framework“ in *Developer's Guide to Oracle Solaris Security*.

Terminologie in Oracle Solaris Cryptographic Framework

Die folgende Liste von Definitionen und Beispielen ist bei der Arbeit mit dem kryptografischen Framework von Nutzen.

- **Algorithmen**: kryptografische Algorithmen. Hierbei handelt es sich um bewährte rekursive Berechnungsverfahren zum Verschlüsseln oder Hashen von Eingabe. Verschlüsselungsalgorithmen können symmetrisch oder asymmetrisch sein. Symmetrische Algorithmen verwenden denselben Schlüssel für die Verschlüsselung und die Entschlüsselung. Asymmetrische Algorithmen, die in der Public-Key-Kryptografie zum Einsatz kommen, erfordern zwei Schlüssel. Hashing-Funktionen sind ebenfalls Algorithmen.

  Es stehen zum Beispiel folgende Algorithmen zur Verfügung:

  - Symmetrische Algorithmen, wie z. B. AES und ARCFOUR
  - Asymmetrische Algorithmen, wie z. B. Diffie-Hellman und RSA
  - Hashing-Funktionen, wie z. B. MD5
- **Verbraucher**: Benutzer kryptografischer Services, die von Providern stammen. Benutzer können Anwendungen, Endbenutzer oder Kernel-Vorgänge sein.

  Folgende Verbraucher stehen beispielsweise zur Verfügung:

  - Anwendungen, wie z. B. IKE
  - Endbenutzer, wie z. B. ein gewöhnlicher Benutzer, der den Befehl `encrypt` ausführt
  - Kernel-Vorgänge, wie z. B. IPsec
- **Mechanismus**: die Anwendung des Modus eines Algorithmus für einen bestimmten Zweck.

  Ein DES-Mechanismus, der auf Authentifizierung angewendet wird, wie z. B. CKM_DES_MAC, ist beispielsweise ein separater Mechanismus aus einem DES-Mechanismus, der auf Verschlüsselung angewendet wird (CKM_DES_CBC_PAD).
- **Metaslot**: ein einziger Slot, der die Funktionen anderer im Framework geladener Slots zusammenfasst. Durch den Metaslot gestaltet sich das Arbeiten mit all diesen Funktionen der im Framework verfügbaren Provider einfacher. Wenn eine Anwendung, die den Metaslot verwendet, einen Vorgang anfordert, stellt der Metaslot fest, welcher Slot den Vorgang tatsächlich ausführen soll. Die Metaslot-Funktionen sind konfigurierbar, auch wenn dies nicht erforderlich ist. Der Metaslot ist standardmäßig aktiviert. Informationen zum Konfigurieren des Metaslots finden Sie auf der Manpage `cryptoadm(1M)`.
- **Modus**: eine Version des kryptografischen Algorithmus. Zum Beispiel ist CBC (Cipher Block Chaining) ein anderer Modus als ECB (Electronic Code Book). Der AES-Algorithmus weist zwei Modi auf: CKM_AES_ECB und CKM_AES_CBC.

- **Richtlinie**: die von einem Administrator getroffene Auswahl, welche Mechanismen für die Verwendung zur Verfügung gestellt werden. Standardmäßig stehen alle Provider und Mechanismen für die Verwendung zur Verfügung. Das Deaktivieren eines Mechanismus entspricht der Anwendung einer Richtlinie. Für das Aktivieren eines deaktivierten Mechanismus gilt das gleiche.
- **Provider**: von Verbrauchern verwendete kryptografische Services. Provider werden in das Framework integriert und daher auch als *Plugins* bezeichnet.

  Folgende Provider stehen beispielsweise zur Verfügung:

  - PKCS #11-Bibliotheken, wie z. B. `pkcs11_softtoken.so`
  - Module kryptografischer Algorithmen, wie z. B. `aes` und `arcfour`
  - Gerätetreiber und die dazugehörigen Hardwarebeschleuniger, wie z. B. der `mca`-Treiber für den Beschleuniger Sun Crypto 6000
- **Slot**: eine Schnittstelle zu mindestens einem kryptografischen Gerät. Jeder Slot, der einem physischen Lesegerät oder einer anderen Geräteschnittstelle entspricht, kann ein Token enthalten. Ein Token bietet eine logische Ansicht eines kryptografischen Geräts im Framework.
- **Token**: Ein Token bietet in einem Slot eine logische Ansicht eines kryptografischen Geräts im Framework.

Geltungsbereich von Oracle Solaris Cryptographic Framework

Das Framework bietet Befehle für Administratoren, Benutzer und Entwickler, die Provider bereitstellen:

- **Administrative Befehle**: Der Befehl `cryptoadm` bietet einen Unterbefehl `list` zum Auflisten der verfügbaren Provider und deren Funktionen. Gewöhnliche Benutzer können die Befehle `cryptoadm list` und `cryptoadm --help` ausführen.

  Für alle anderen Unterbefehle von `cryptoadm` müssen Sie eine Rolle annehmen, die das Berechtigungsprofil von Crypto Management enthält, oder sich als Superuser anmelden. Unterbefehle wie `disable`, `install`, und `uninstall` stehen für die Verwaltung des Frameworks zur Verfügung. Weitere Informationen erhalten Sie auf der Manpage `cryptoadm(1M)`.

  Der Befehl `svcadm` wird zum Verwalten des Dämons `kcfd` und zum Aktualisieren der Kryptografierichtlinie im Kernel verwendet. Weitere Informationen erhalten Sie auf der Manpage `svcadm(1M)`.
- **Befehle auf Benutzerebene**: Die Befehle `digest` und `mac` stellen Services für die Dateiintegrität bereit. Die Befehle `encrypt` und `decrypt` schützen die Dateien vor dem Abhören. Informationen zur Verwendung dieser Befehle finden Sie unter „Schützen von Dateien mit Oracle Solaris Cryptographic Framework (Übersicht der Schritte)“ auf Seite 298.

- **Binäre Signaturen für Provider von Drittanbietern**: Mit dem Befehl `elfsign` können Drittanbieter Binärdateien für die Verwendung im Framework signieren. Bei Binärdateien, die dem Framework hinzugefügt werden können, handelt es sich um PKCS #11-Bibliotheken, Kernel-Algorithmusmodule und Hardware-Gerätetreiber. Informationen zur Verwendung des Befehls `elfsign` finden Sie in Anhang F, „Packaging and Signing Cryptographic Providers“ in *Developer's Guide to Oracle Solaris Security*.

Administrative Befehle in Oracle Solaris Cryptographic Framework

Mit dem Befehl `cryptoadm` wird ein ausgeführtes kryptografisches Framework verwaltet. Der Befehl ist ein Teil des Berechtigungsprofils von Crypto Management. Dieses Profil kann einer Rolle für die sichere Verwaltung des kryptografischen Frameworks zugewiesen werden. Mit dem Befehl `cryptoadm` wird Folgendes verwaltet:

- Anzeigen von Informationen zu kryptografischen Providern
- Deaktivieren oder Aktivieren von Providermechanismen
- Deaktivieren oder Aktivieren des Metaslots in Solaris 10 1/06

Mit dem Befehl `svcadm` wird der Dämon für kryptografische Services (`kcfd`) aktiviert, aktualisiert und deaktiviert. Dieser Befehl ist ein Teil von SMF (Service Management Facility). `svc:/system/cryptosvcs` ist die Serviceinstanz für das kryptografische Framework. Weitere Informationen finden Sie auf den Manpages `smf(5)` und `svcadm(1M)`.

Befehle auf Benutzerebene in Oracle Solaris Cryptographic Framework

Oracle Solaris Cryptographic Framework bietet Befehle auf Benutzerebene zum Überprüfen der Integrität von Dateien sowie zum Verschlüsseln und Entschlüsseln von Dateien. Mit einem separaten Befehl (`elfsign`) können Provider Binärdateien für die Verwendung mit dem Framework signieren.

- `digest` (**Befehl**): berechnet ein Meldungs-Digest für mindestens eine Datei oder für stdin. Ein Digest eignet sich zum Überprüfen der Integrität einer Datei. SHA1 und MD5 sind Beispiele für Digest-Funktionen.
- `mac` (**Befehl**): berechnet einen Message Authentication Code (MAC) für mindestens eine Datei oder für stdin. Ein MAC weist Daten einer authentifizierten Meldung zu. Mithilfe eines MAC kann der Empfänger überprüfen, ob die Meldung von dem Absender stammte und ob sie manipuliert wurde. Mit den Mechanismen `sha1_mac` und `md5_hmac` kann ein MAC berechnet werden.

- `encrypt` (**Befehl**): verschlüsselt Dateien oder stdin mit einer symmetrischen Verschlüsselung. Der Befehl `encrypt -l` listet die verfügbaren Algorithmen auf. In einer Bibliothek auf Benutzerebene aufgeführte Mechanismen sind mit dem Befehl `encrypt` verfügbar. Das Framework bietet die Mechanismen AES, DES, 3DES (Triple-DES) und ARCFOUR für die Benutzerverschlüsselung.
- `decrypt` (**Befehl**): entschlüsselt mit dem Befehl `encrypt` verschlüsselte Dateien oder stdin. Der Befehl `decrypt` verwendet den gleichen Schlüssel und Mechanismus, der zum Verschlüsseln der Originaldatei verwendet wurde.

Binäre Signaturen für Drittanbietersoftware

Der Befehl `elfsign` bietet eine Möglichkeit zum Signieren von Providern für die Verwendung mit Oracle Solaris Cryptographic Framework. Üblicherweise wird der Befehl durch den Entwickler eines Providers ausgeführt.

Der Befehl `elfsign` verfügt über Unterbefehle zum Anfordern eines Zertifikats von Oracle und zum Signieren von Binärdateien. Mit einem weiteren Unterbefehl wird die Signatur überprüft. Unsignierte Binärdateien können nicht von Oracle Solaris Cryptographic Framework verwendet werden. Zum Signieren von einem oder mehreren Providern sind das Zertifikat von Oracle und der zum Anfordern des Zertifikats verwendete private Schlüssel erforderlich. Weitere Informationen finden Sie in Anhang F, „Packaging and Signing Cryptographic Providers“ in *Developer's Guide to Oracle Solaris Security*.

Plugins von Oracle Solaris Cryptographic Framework

Drittanbieter können ihre Provider in OSOL; Cryptographic Framework integrieren. Bei einem Provider eines Drittanbieters kann es sich um eines der folgenden Objekte handeln:

- Gemeinsam genutzte PKCS #11-Bibliothek
- Ladbares Kernel-Softwaremodul, wie z. B. ein Verschlüsselungsalgorithmus, eine MAC-Funktion oder eine Digest-Funktion
- Kernel-Gerätetreiber für einen Hardwarebeschleuniger

Die Objekte von einem Provider müssen mit einem Zertifikat von Oracle signiert werden. Die Zertifikatanforderung basiert auf einem privaten Schlüssel, den der Drittanbieter auswählt, und einem von Oracle bereitgestellten Zertifikat. Die Zertifikatanforderung wird an Oracle gesendet. Oracle registriert daraufhin den Drittanbieter und stellt das Zertifikat aus. Anschließend signiert der Drittanbieter sein Providerobjekt mit dem Zertifikat von Oracle.

Die ladbaren Kernel-Softwaremodule und die Kernel-Gerätetreiber für Hardwarebeschleuniger müssen ebenfalls mit dem Kernel registriert werden. Die Registrierung erfolgt über die SPI (Service Provider Interface) von Oracle Solaris Cryptographic Framework.

Zum Installieren des Providers stellt der Drittanbieter ein Paket bereit, das das signierte Objekt und das Zertifikat von Oracle installiert. Das Paket muss das Zertifikat enthalten und dem Administrator das Ablegen des Zertifikats in einem sicheren Verzeichnis ermöglichen. Weitere Informationen finden Sie in Anhang F, „Packaging and Signing Cryptographic Providers“ in *Developer's Guide to Oracle Solaris Security*.

Kryptografische Services und Zonen

Die globale Zone und alle nicht globalen Zonen verfügen über einen eigenen `/system/cryptosvc`-Service. Beim Aktivieren oder Aktualisieren des kryptografischen Service in der globalen Zone wird der Dämon `kcfd` in der globalen Zone gestartet. Außerdem werden die Richtlinie auf Benutzerebene für die globale Zone und die Kernel-Richtlinie für das System festgelegt. Beim Aktivieren oder Aktualisieren des Service in einer nicht globalen Zone wird der Dämon `kcfd` in der Zone gestartet und die Richtlinie auf Benutzerebene für die Zone festgelegt. Die Kernel-Richtlinie wurde durch die globale Zone festgelegt.

Weitere Informationen zu Zonen finden Sie in Teil II, „Zonen“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*. Weitere Informationen zu SMF (Service Management Facility) für die Verwaltung persistenter Anwendungen finden Sie in Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration* und auf der Manpage `smf(5)`.

◆ ◆ ◆ KAPITEL 14

Oracle Solaris Cryptographic Framework (Aufgaben)

In diesem Kapitel wird beschrieben, wie Sie Oracle Solaris Cryptographic Framework verwenden. Im Folgenden ist eine Liste der Informationen in diesem Kapitel aufgeführt.

- „Verwenden von Cryptographic Framework (Übersicht der Schritte)“ auf Seite 297
- „Schützen von Dateien mit Cryptographic Framework (Aufgaben)“ auf Seite 298
- „Verwalten von Cryptographic Framework (Aufgaben)“ auf Seite 310

Verwenden von Cryptographic Framework (Übersicht der Schritte)

In der folgenden Übersicht sind die wichtigsten Schritte bei der Verwendung des kryptografischen Frameworks aufgeführt.

Aufgabe	Beschreibung	Anweisungen
Schützen von einzelnen Dateien oder Sätzen von Dateien	Stellt sicher, dass der Inhalt der Dateien nicht manipuliert wurde. Verhindert, dass die Dateien von Eindringlingen gelesen werden. Diese Verfahren können von gewöhnlichen Benutzern durchgeführt werden.	„Schützen von Dateien mit Oracle Solaris Cryptographic Framework (Übersicht der Schritte)“ auf Seite 298
Verwalten des Frameworks	Fügt Softwareprovider hinzu und konfiguriert bzw. entfernt sie. Deaktiviert und aktiviert Mechanismen von Hardwareprovidern. Bei diesen Verfahren handelt es sich um administrative Verfahren.	„Verwalten von Cryptographic Framework (Übersicht der Schritte)“ auf Seite 309
Signieren eines Providers	Ermöglicht das Hinzufügen eines Providers zu Oracle Solaris Cryptographic Framework. Bei diesen Verfahren handelt es sich um Entwicklerverfahren.	Anhang F, „Packaging and Signing Cryptographic Providers“ in *Developer's Guide to Oracle Solaris Security*.

Schützen von Dateien mit Oracle Solaris Cryptographic Framework (Übersicht der Schritte)

Oracle Solaris Cryptographic Framework bietet Ihnen Unterstützung beim Schützen Ihrer Dateien. In der folgenden Übersicht sind die wichtigsten Schritte zum Auflisten der verfügbaren Algorithmen und für den kryptografischen Schutz Ihrer Dateien aufgeführt.

Aufgabe	Beschreibung	Anweisungen
Generieren eines symmetrischen Schlüssels	Generiert einen zufallsverteilten Schlüssel für die Verwendung mit Algorithmen, die der Benutzer angibt	„So generieren Sie einen symmetrischen Schlüssel mit dem Befehl `dd`“ auf Seite 298
	Generiert einen Schlüssel mit benutzerspezifischer Länge. Speichert den Schlüssel optional in einer Datei, einem PKCS #11-Schlüsselspeicher oder NSS-Schlüsselspeicher	„So generieren Sie einen symmetrischen Schlüssel mit dem Befehl `pktool`“ auf Seite 301
Bereitstellen einer Prüfsumme, die die Integrität einer Datei sicherstellt	Überprüft, ob die Kopie einer Datei des Empfängers mit der gesendeten Datei identisch ist	„So berechnen Sie den Digest einer Datei“ auf Seite 304
Schützen einer Datei mit einem MAC (Message Authentication Code)	Stellt gegenüber dem Empfänger Ihrer Meldung sicher, dass Sie der Absender sind	„So berechnen Sie den MAC einer Datei“ auf Seite 305
Verschlüsseln einer Datei und anschließendes Entschlüsseln der verschlüsselten Datei	Schützt den Inhalt von Dateien durch Verschlüsseln der Datei. Stellt die Verschlüsselungsparameter zum Entschlüsseln der Datei bereit	„So entschlüsseln und verschlüsseln Sie eine Datei“ auf Seite 307

Schützen von Dateien mit Cryptographic Framework (Aufgaben)

Dieser Abschnitt enthält Beschreibungen zum Generieren symmetrischer Schlüssel, zum Erstellen von Prüfsummen für die Dateiintegrität und zum Schützen von Dateien vor dem Abhören. Die in diesem Abschnitt aufgeführten Befehle können von gewöhnlichen Benutzern ausgeführt werden. Entwickler können Skripten schreiben, die diese Befehle verwenden.

▼ So generieren Sie einen symmetrischen Schlüssel mit dem Befehl `dd`

Zum Verschlüsseln von Dateien und zum Generieren des MAC einer Datei ist ein Schlüssel erforderlich. Der Schlüssel sollte aus einem Zufallspool von Zahlen abgeleitet werden.

Falls Ihr Standort über einen Generator für Zufallszahlen verfügt, verwenden Sie diesen. Andernfalls können Sie den Befehl `dd` mit dem Oracle Solaris-Gerät `/dev/urandom` als Eingabe verwenden. Weitere Informationen erhalten Sie auf der Manpage dd(1M).

1 Bestimmen Sie die für Ihren Algorithmus erforderliche Schlüssellänge.

a. Listen Sie die verfügbaren Algorithmen auf.

```
% encrypt -l
Algorithm       Keysize:  Min   Max (bits)
----------------------------------------
aes                      128   128
arcfour                    8   128
des                       64    64
3des                     192   192

% mac -l
Algorithm       Keysize:  Min   Max (bits)
----------------------------------------
des_mac                   64    64
sha1_hmac                  8   512
md5_hmac                   8   512
sha256_hmac                8   512
sha384_hmac                8  1024
sha512_hmac                8  1024
```

b. Bestimmen Sie die Schlüssellänge in Byte für die Weiterleitung an den Befehl `dd`.

Teilen Sie die minimale und die maximale Schlüsselgröße durch 8. Wenn sich die minimale und die maximale Schlüsselgröße unterscheiden, können dazwischen liegende Schlüsselgrößen verwendet werden. Beispielsweise kann der Wert 8, 16 oder 64 an den Befehl `dd` für die Funktionen `sha1_hmac` und `md5_hmac` weitergeleitet werden.

2 Generieren Sie den symmetrischen Schlüssel.

`% dd if=/dev/urandom of=`*keyfile* `bs=`*n* `count=`*n*

`if=`*file* — Entspricht der Eingabedatei. Verwenden Sie für einen zufallsverteilten Schlüssel die Datei `/dev/urandom`.

`of=`*keyfile* — Entspricht der Ausgabedatei mit dem generierten Schlüssel.

`bs=`*n* — Entspricht der Schlüsselgröße in Byte. Teilen Sie für die Länge in Byte die in Bit angegebene Schlüsselgröße durch 8.

`count=`*n* — Entspricht dem Zähler der Eingabeblöcke. Die Zahl für *n* sollte `1` lauten.

3 Speichern Sie Ihren Schlüssel in einem geschützten Verzeichnis.

Die Schlüsseldatei sollte ausschließlich vom Benutzer gelesen werden können.

`% chmod 400` *keyfile*

Beispiel 14–1 Erstellen eines Schlüssels für den AES-Algorithmus

Im folgenden Beispiel wird ein Geheimschlüssel für den AES-Algorithmus erstellt. Der Schlüssel wird auch für die spätere Entschlüsselung gespeichert. AES-Mechanismen verwenden einen 128-Bit-Schlüssel. Der Schlüssel wird im Befehl dd als 16-Byte-Schlüssel ausgedrückt.

```
% ls -al ~/keyf
drwx------   2 jdoe  staff        512 May 3 11:32 ./
% dd if=/dev/urandom of=$HOME/keyf/05.07.aes16 bs=16  count=1
% chmod 400 ~/keyf/05.07.aes16
```

Beispiel 14–2 Erstellen eines Schlüssels für den DES-Algorithmus

Im folgenden Beispiel wird ein Geheimschlüssel für den DES-Algorithmus erstellt. Der Schlüssel wird auch für die spätere Entschlüsselung gespeichert. DES-Mechanismen verwenden einen 64-Bit-Schlüssel. Der Schlüssel wird im Befehl dd als 8-Byte-Schlüssel ausgedrückt.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.des8 bs=8  count=1
% chmod 400 ~/keyf/05.07.des8
```

Beispiel 14–3 Erstellen eines Schlüssels für den 3DES-Algorithmus

Im folgenden Beispiel wird ein Geheimschlüssel für den 3DES-Algorithmus erstellt. Der Schlüssel wird auch für die spätere Entschlüsselung gespeichert. 3DES-Mechanismen verwenden einen 192-Bit-Schlüssel. Der Schlüssel wird im Befehl dd als 24-Byte-Schlüssel ausgedrückt.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.3des.24 bs=24 count=1
% chmod 400 ~/keyf/05.07.3des.24
```

Beispiel 14–4 Erstellen eines Schlüssels für den MD5-Algorithmus

Im folgenden Beispiel wird ein Geheimschlüssel für den MD5-Algorithmus erstellt. Der Schlüssel wird auch für die spätere Entschlüsselung gespeichert. Der Schlüssel wird im Befehldd als 64-Byte-Schlüssel ausgedrückt.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.mack64 bs=64 count=1
% chmod 400 ~/keyf/05.07.mack64
```

▼ So generieren Sie einen symmetrischen Schlüssel mit dem Befehl `pktool`

Einige Anwendungen erfordern einen symmetrischen Schlüssel für die Verschlüsselung und Entschlüsselung von Kommunikation. In diesem Verfahren erstellen und speichern Sie einen symmetrischen Schlüssel.

- Falls Ihr Standort über einen Generator für Zufallszahlen verfügt, können Sie mithilfe dieses Generators eine Zufallszahl für den Schlüssel erstellen. Im vorliegenden Verfahren wird kein Generator für Zufallszahlen verwendet.
- Stattdessen können Sie auch den Befehl `dd` mit dem Oracle Solaris-Gerät `/dev/urandom` als Eingabe verwenden. Der Befehl `dd` speichert den Schlüssel nicht. Informationen zu diesem Verfahren finden Sie unter „So generieren Sie einen symmetrischen Schlüssel mit dem Befehl `dd`“ auf Seite 298.

1 (Optional) Wenn Sie einen Schlüsselspeicher verwenden möchten, erstellen Sie diesen.

- **Informationen zum Erstellen und Initialisieren eines PKCS #11-Schlüsselspeichers finden Sie unter „So generieren Sie einen Passwortsatz mit dem Befehl `pktool setpin`“ auf Seite 330.**
- **In Beispiel 15–5 wird die Erstellung und Initialisierung einer NSS-Datenbank dargestellt.**

2 Generieren Sie eine Zufallszahl für die Verwendung als symmetrischer Schlüssel.

Verwenden Sie eine der folgenden Methoden:

- **Generieren Sie einen Schlüssel und speichern Sie ihn in einer Datei.**

  Der Vorteil eines in einer Datei gespeicherten Schlüssels liegt darin, dass Sie den Schlüssel aus dieser Datei extrahieren können, um ihn in der Schlüsseldatei einer Anwendung wie z. B. der Datei `/etc/inet/secret/ipseckeys` oder IPsec zu verwenden.

  ```
  % pktool genkey keystore=file outkey=key-fn \
  [keytype=specific-symmetric-algorithm] [keylen=size-in-bits] \
  [dir=directory] [print=n]
  ```

  `keystore`
  Der Wert `file` gibt den Dateityp des Speicherorts für den Schlüssel an.

  `outkey=`*key-fn*
  Dies ist der Dateiname, wenn `keystore=file`

  `keytype=`*specific-symmetric-algorithm*
  Geben Sie `aes`, `arcfour`, `des` oder `3des` für einen bestimmten Algorithmus an.

  `keylen=`*size-in-bits*
  Dies ist die Länge des Schlüssels in Bit. Die Zahl muss durch 8 teilbar sein. Dieser Wert darf *nicht* für `des` oder `3des` angegeben werden.

`dir=`*directory*
: Hierbei handelt es sich um den Verzeichnispfad zu *key-fn*. Standardmäßig ist *directory* das aktuelle Verzeichnis.

`print=n`
: Druckt den Schlüssel zu dem Terminalfenster. Der Standardwert von `print` ist `n`.

- **Generieren Sie einen Schlüssel und speichern Sie ihn in einem PKCS #11-Schlüsselspeicher.**

  Der Vorteil des PKCS #11-Schlüsselspeichers besteht darin, dass Sie den Schlüssel anhand seiner Beschriftung abrufen können. Diese Methode eignet sich für Schlüssel zum Verschlüsseln und Entschlüsseln von Dateien. Bevor Sie diese Methode verwenden, müssen Sie Schritt 1 abschließen.

  ```
  % pktool genkey label=key-label \
  [keytype=specific-symmetric-algorithm] [keylen=size-in-bits] \
  [token=token] [sensitive=n] [extractable=y] [print=n]
  ```

  `label=`*key-label*
  : Eine benutzerdefinierte Beschriftung für den Schlüssel. Der Schlüssel kann anhand seiner Beschriftung aus dem Schlüsselspeicher abgerufen werden.

  `keytype=`*specific-symmetric-algorithm*
  : Geben Sie `aes`, `arcfour`, `des` oder `3des` für einen bestimmten Algorithmus an.

  `keylen=`*size-in-bits*
  : Dies ist die Länge des Schlüssels in Bit. Die Zahl muss durch 8 teilbar sein. Dieser Wert darf *nicht* für `des` oder `3des` angegeben werden.

  `token=`*token*
  : Dies ist der Token-Name. Standardmäßig lautet das Token `Sun Software PKCS#11 softtoken`.

  `sensitive=n`
  : Gibt die Sensitivität des Schlüssels an. Wenn der Wert `y` ist, kann der Schlüssel nicht mit dem Argument `print=y` gedruckt werden. Der Standardwert von `sensitive` ist `n`.

  `extractable=y`
  : Gibt an, dass der Schlüssel aus dem Schlüsselspeicher extrahiert werden kann. Geben Sie `n` an, um zu verhindern, dass der Schlüssel extrahiert wird.

  `print=n`
  : Druckt den Schlüssel zu dem Terminalfenster. Der Standardwert von `print` ist `n`.

- **Generieren Sie einen Schlüssel und speichern Sie ihn in einem NSS-Schlüsselspeicher.**

  Bevor Sie diese Methode verwenden, müssen Sie Schritt 1 abschließen.

  ```
  % pktool keystore=nss genkey label=key-label \
  [keytype=[keytype=specific-symmetric-algorithm] [keylen=size-in-bits] [token=token] \
  [dir=directory-path] [prefix=database-prefix]
  ```

  `keystore`
  : Der Wert `nss` gibt den NSS-Typ des Speicherorts für den Schlüssel an.

`label=`*key-label*
Eine benutzerdefinierte Beschriftung für den Schlüssel. Der Schlüssel kann anhand seiner Beschriftung aus dem Schlüsselspeicher abgerufen werden.

`keytype=`*specific-symmetric-algorithm*
Geben Sie `aes`, `arcfour`, `des` oder `3des` für einen bestimmten Algorithmus an.

`keylen=`*size-in-bits*
Dies ist die Länge des Schlüssels in Bit. Die Zahl muss durch 8 teilbar sein. Dieser Wert darf *nicht* für `des` oder `3des` angegeben werden.

`token=`*token*
Dies ist der Token-Name. Standard-Token ist das interne NSS-Token.

`dir=`*directory*
Hierbei handelt es sich um den Verzeichnispfad zur NSS-Datenbank. Standardmäßig ist *directory* das aktuelle Verzeichnis.

`prefix=`*directory*
Dies ist das Präfix für die NSS-Datenbank. Standardmäßig ist kein Präfix angegeben.

`print=n`
Druckt den Schlüssel zu dem Terminalfenster. Der Standardwert von `print` ist `n`.

3 (Optional) Überprüfen Sie, ob der Schlüssel vorhanden ist.

Verwenden Sie je nach Speicherort des Schlüssels einen der folgenden Befehle.

- **Überprüfen Sie den Schlüssel in der Datei *key-fn*.**

```
% pktool list keystore=file objtype=key infile=key-fn
Found n keys.
Key #1 - keytype:location (keylen)
```

- **Überprüfen Sie den Schlüssel im PKCS #11- oder NSS-Schlüsselspeicher.**

```
$ pktool list objtype=key
Enter PIN for keystore:
Found n keys.
Key #1 - keytype:location (keylen)
```

Beispiel 14–5 Erstellen eines DES-Schlüssels mit dem Befehl `pktool`

Im folgenden Beispiel wird ein Geheimschlüssel für den DES-Algorithmus erstellt. Der Schlüssel wird für die spätere Entschlüsselung in einer lokalen Datei gespeichert. Der Befehl schützt die Datei mit den Berechtigungen `400`. Wenn die Datei erstellt wird, zeigt die Option `print=y` den generierten Schlüssel im Terminalfenster an.

DES-Mechanismen verwenden einen 64-Bit-Schlüssel. Der Benutzer, der über die Schlüsseldatei verfügt, ruft den Schlüssel mit dem Befehl `od` ab.

```
% pktool genkey keystore=file outkey=64bit.file1 keytype=des print=y
        Key Value ="a3237b2c0a8ff9b3"
% od -x 64bit.file1
0000000 a323 7b2c 0a8f f9b3
```

▼ So berechnen Sie den Digest einer Datei

Beim Berechnen des Digest einer Datei können Sie überprüfen, ob die Datei manipuliert wurde, indem Sie Digest-Ausgaben miteinander vergleichen. Ein Digest ändert die Originaldatei nicht.

1 Listen Sie die verfügbaren Digest-Algorithmen auf.

```
% digest -l
md5
sha1
sha256
sha384
sha512
```

2 Berechnen Sie das Digest der Datei und speichern Sie die Digest-Liste.

Geben Sie einen Algorithmus mit dem Befehl `digest` an.

`% digest -v -a` *algorithm input-file* `>` *digest-listing*

`-v`	Zeigt die Ausgabe in folgendem Format an: *algorithm* `(`*input-file*`) =` *digest*
`-a` *algorithm*	Dies ist der Algorithmus für die Berechnung eines Digest der Datei. Geben Sie den Algorithmus so ein, wie er in der Ausgabe in Schritt 1 angezeigt wird.
input-file	Dies ist die Eingabedatei für den Befehl `digest`.
digest-listing	Dies ist die Ausgabedatei für den Befehl `digest`.

Beispiel 14–6 Berechnen eines Digest mit dem MD5-Mechanismus

Im folgenden Beispiel berechnet der Befehl `digest` unter Verwendung des MD5-Mechanismus ein Digest für einen E-Mail-Anhang.

```
% digest -v -a md5 email.attach >>  $HOME/digest.emails.05.07
% cat  ~/digest.emails.05.07
md5 (email.attach) = 85c0a53d1a5cc71ea34d9ee7b1b28b01
```

Wenn die Option `-v` nicht verwendet wird, wird das Digest ohne begleitende Informationen gespeichert:

```
% digest -a md5 email.attach >>  $HOME/digest.emails.05.07
% cat  ~/digest.emails.05.07
85c0a53d1a5cc71ea34d9ee7b1b28b01
```

Beispiel 14–7 Berechnen eines Digest mit dem SHA1-Mechanismus

Im folgenden Beispiel stellt der Befehl `digest` unter Verwendung des SHA1-Mechanismus eine Verzeichnisliste bereit. Die Ergebnisse werden in einer Datei gespeichert.

```
% digest -v -a sha1 docs/* > $HOME/digest.docs.legal.05.07
% more ~/digest.docs.legal.05.07
sha1 (docs/legal1) = 1df50e8ad219e34f0b911e097b7b588e31f9b435
sha1 (docs/legal2) = 68efa5a636291bde8f33e046eb33508c94842c38
sha1 (docs/legal3) = 085d991238d61bd0cfa2946c183be8e32cccf6c9
sha1 (docs/legal4) = f3085eae7e2c8d008816564fdf28027d10e1d983
```

▼ So berechnen Sie den MAC einer Datei

Ein MAC (Message Authentication Code) berechnet ein Digest für die Datei und verwendet einen Geheimschlüssel für den weiteren Schutz des Digest. Ein MAC ändert die Originaldatei nicht.

1 Listen Sie die verfügbaren Mechanismen auf.

```
% mac -l
Algorithm       Keysize:  Min   Max
-----------------------------------
des_mac                   64    64
sha1_hmac                  8   512
md5_hmac                   8   512
sha256_hmac                8   512
sha384_hmac                8  1024
sha512_hmac                8  1024
```

2 Generieren Sie einen symmetrischen Schlüssel in der entsprechenden Länge.

Es sind folgende zwei Möglichkeiten verfügbar. Sie können einen Passwortsatz angeben, aus dem ein Schlüssel generiert wird. Alternativ können Sie auch einen Schlüssel angeben.

- Wenn Sie einen Passwortsatz (Kennsatz) angeben, müssen Sie diesen speichern oder sich merken. Wenn Sie den Passwortsatz online speichern, sollte die Passwortsatzdatei nur von Ihnen gelesen werden können.
- Wenn Sie einen Schlüssel angeben, muss dieser die richtige Größe für den Mechanismus aufweisen. Informationen zu diesem Verfahren finden Sie unter „So generieren Sie einen symmetrischen Schlüssel mit dem Befehl `dd`“ auf Seite 298.

3 Erstellen Sie einen MAC für eine Datei.

Geben Sie einen Schlüssel an und verwenden Sie einen symmetrischen Schlüsselalgorithmus mit dem Befehl `mac`.

`% mac -v -a` *algorithm* `[ -k` *keyfile* `]` *input-file*

`-v` Zeigt die Ausgabe in folgendem Format an:

algorithm (*input-file*) = *mac*

-a *algorithm*	Dies ist der Algorithmus für die Berechnung des MAC. Geben Sie den Algorithmus so ein, wie er in der Ausgabe des Befehls `mac -l` angezeigt wird.
-k *keyfile*	Dies ist die Datei, die einen Schlüssel mit algorithmusspezifischer Länge enthält.
input-file	Hierbei handelt es sich um die Eingabedatei für den MAC.

Beispiel 14–8 Berechnen eines MAC mit DES_MAC und einem Passwortsatz

Im folgenden Beispiel wird der E-Mail-Anhang mit dem DES_MAC-Mechanismus und einem aus einem Passwortsatz abgeleiteten Schlüssel authentifiziert. Die MAC-Liste wird in einer Datei gespeichert. Wenn der Passwortsatz in einer Datei gespeichert wird, sollte die Datei ausschließlich vom Benutzer gelesen werden können.

```
% mac -v -a des_mac email.attach
Enter passphrase:     <Type passphrase>
des_mac (email.attach) = dd27870a
% echo "des_mac (email.attach) = dd27870a" >> ~/desmac.daily.05.07
```

Beispiel 14–9 Berechnen eines MAC mit MD5_HMAC und einer Schlüsseldatei

Im folgenden Beispiel wird der E-Mail-Anhang mit dem MD5_HMAC-Mechanismus und einem Geheimschlüssel authentifiziert. Die MAC-Liste wird in einer Datei gespeichert.

```
% mac -v -a md5_hmac -k $HOME/keyf/05.07.mack64 email.attach
md5_hmac (email.attach) = 02df6eb6c123ff25d78877eb1d55710c
% echo "md5_hmac (email.attach) = 02df6eb6c123ff25d78877eb1d55710c" \
>> ~/mac.daily.05.07
```

Beispiel 14–10 Berechnen eines MAC mit SHA1_HMAC und einer Schlüsseldatei

Im folgenden Beispiel wird das Verzeichnismanifest mit dem SHA1_HMAC-Mechanismus und einem Geheimschlüssel authentifiziert. Die Ergebnisse werden in einer Datei gespeichert.

```
% mac -v -a sha1_hmac \
-k $HOME/keyf/05.07.mack64 docs/* > $HOME/mac.docs.legal.05.07
% more ~/mac.docs.legal.05.07
sha1_hmac (docs/legal1) = 9b31536d3b3c0c6b25d653418db8e765e17fe07a
sha1_hmac (docs/legal2) = 865af61a3002f8a457462a428cdb1a88c1b51ff5
sha1_hmac (docs/legal3) = 076c944cb2528536c9aebd3b9fbe367e07b61dc7
sha1_hmac (docs/legal4) = 7aede27602ef6e4454748cbd3821e0152e45beb4
```

▼ So entschlüsseln und verschlüsseln Sie eine Datei

Beim Verschlüsseln einer Datei wird die Originaldatei nicht entfernt oder geändert. Die Ausgabedatei wird verschlüsselt.

Lösungen zu häufigen Fehlern in Bezug auf den Befehl `encrypt` finden Sie im Abschnitt nach den Beispielen.

1 Erstellen Sie einen symmetrischen Schlüssel in der entsprechenden Länge.

Es stehen zwei Möglichkeiten zur Verfügung. Sie können einen Passwortsatz angeben, aus dem ein Schlüssel generiert wird. Alternativ können Sie auch einen Schlüssel angeben.

- Wenn Sie einen Passwortsatz angeben, müssen Sie diesen speichern oder sich merken. Wenn Sie den Passwortsatz online speichern, sollte die Passwortsatzdatei nur von Ihnen gelesen werden können.
- Wenn Sie einen Schlüssel angeben, muss dieser die richtige Größe für den Mechanismus aufweisen. Informationen zu diesem Verfahren finden Sie unter „So generieren Sie einen symmetrischen Schlüssel mit dem Befehl `dd`“ auf Seite 298.

2 Verschlüsseln Sie eine Datei.

Geben Sie einen Schlüssel an und verwenden Sie einen symmetrischen Schlüsselalgorithmus mit dem Befehl `encrypt`.

```
% encrypt -a algorithm  [ -k keyfile ] -i input-file -o output-file
```

`-a` *algorithm*	Dies ist der Algorithmus für die Verschlüsselung des MAC. Geben Sie den Algorithmus so ein, wie er in der Ausgabe des Befehls `encrypt -l` angezeigt wird.
`-k` *keyfile*	Dies ist die Datei, die einen Schlüssel mit algorithmusspezifischer Länge enthält. Die Schlüssellänge für jeden Algorithmus (in Bit) wird in der Ausgabe des Befehls `encrypt -l` aufgeführt.
`-i` *input-file*	Dies ist die Eingabedatei, die Sie verschlüsseln möchten. Diese Datei wird durch den Befehl nicht geändert.
`-o` *output-file*	Dies ist die Ausgabedatei, bei der es sich um die verschlüsselte Form der Eingabedatei handelt.

Beispiel 14–11 Verschlüsseln und Entschlüsseln mit AES und einem Passwortsatz

Im folgenden Beispiel wird eine Datei mit dem AES-Algorithmus verschlüsselt. Der Schlüssel wird aus dem Passwortsatz generiert. Wenn der Passwortsatz in einer Datei gespeichert wird, sollte die Datei ausschließlich vom Benutzer gelesen werden können.

```
% encrypt -a aes -i ticket.to.ride -o ~/enc/e.ticket.to.ride
Enter passphrase:     <Type passphrase>
Re-enter passphrase:      Type passphrase again
```

Die Eingabedatei (`ticket.to.ride`) ist weiterhin in ihrer ursprünglichen Form vorhanden.

Zum Entschlüsseln der Ausgabedatei verwendet der Benutzer denselben Passwortsatz und Verschlüsselungsmechanismus wie für die Verschlüsselung der Datei.

```
% decrypt -a aes -i ~/enc/e.ticket.to.ride -o ~/d.ticket.to.ride
Enter passphrase:     <Type passphrase>
```

Beispiel 14–12 Verschlüsseln und Entschlüsseln mit AES und einer Schlüsseldatei

Im folgenden Beispiel wird eine Datei mit dem AES-Algorithmus verschlüsselt. AES-Mechanismen verwenden einen Schlüssel von 128 Bit bzw. 16 Byte.

```
% encrypt -a aes -k ~/keyf/05.07.aes16 \
-i ticket.to.ride -o ~/enc/e.ticket.to.ride
```

Die Eingabedatei (`ticket.to.ride`) ist weiterhin in ihrer ursprünglichen Form vorhanden.

Zum Entschlüsseln der Ausgabedatei verwendet der Benutzer denselben Schlüssel und Verschlüsselungsmechanismus wie für die Verschlüsselung der Datei.

```
% decrypt -a aes -k ~/keyf/05.07.aes16  \
-i ~/enc/e.ticket.to.ride -o ~/d.ticket.to.ride
```

Beispiel 14–13 Verschlüsseln und Entschlüsseln mit ARCFOUR und einer Schlüsseldatei

Im folgenden Beispiel wird eine Datei mit dem ARCFOUR-Algorithmus verschlüsselt. Der ARCFOUR-Algorithmus akzeptiert einen Schlüssel von 8 Bit (1 Byte), 64 Bit (8 Byte) oder 128 Bit (16 Byte).

```
% encrypt -a arcfour -i personal.txt \
-k ~/keyf/05.07.rc4.8 -o ~/enc/e.personal.txt
```

Zum Entschlüsseln der Ausgabedatei verwendet der Benutzer denselben Schlüssel und Verschlüsselungsmechanismus wie für die Verschlüsselung der Datei.

```
% decrypt -a arcfour -i ~/enc/e.personal.txt \
-k ~/keyf/05.07.rc4.8 -o ~/personal.txt
```

Beispiel 14–14 Verschlüsseln und Entschlüsseln mit 3DES und einer Schlüsseldatei

Im folgenden Beispiel wird eine Datei mit dem 3DES-Algorithmus verschlüsselt. Der 3DES-Algorithmus erfordert einen Schlüssel von 192 Bit bzw. 24 Byte.

```
% encrypt -a 3des -k ~/keyf/05.07.des24 \
-i ~/personal2.txt -o ~/enc/e.personal2.txt
```

Zum Entschlüsseln der Ausgabedatei verwendet der Benutzer denselben Schlüssel und Verschlüsselungsmechanismus wie für die Verschlüsselung der Datei.

```
% decrypt -a 3des -k ~/keyf/05.07.des24 \
-i ~/enc/e.personal2.txt -o ~/personal2.txt
```

Allgemeine Fehler

Die folgenden Meldungen geben an, dass der von Ihnen für den Befehl `encrypt` angegebene Schlüssel nicht von dem verwendeten Algorithmus zugelassen wird.

- `encrypt: unable to create key for crypto operation: CKR_ATTRIBUTE_VALUE_INVALID`
- `encrypt: failed to initialize crypto operation: CKR_KEY_SIZE_RANGE`

Wenn Sie einen Schlüssel weiterleiten, der nicht den Anforderungen des Algorithmus entspricht, müssen Sie einen besser geeigneten Schlüssel angeben.

- Dazu können Sie beispielweise einen Passwortsatz angeben. Das Framework stellt dann einen Schlüssel bereit, der den Anforderungen entspricht.
- Die zweite Option besteht darin, bei der Weiterleitung eine Schlüsselgröße zu verwenden, die der Algorithmus akzeptiert. So erfordert der DES-Algorithmus beispielsweise einen Schlüssel von 64 Bit. Für den 3DES-Algorithmus ist dagegen ein Schlüssel von 192 Bit erforderlich.

Verwalten von Cryptographic Framework (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf Verfahren zur Verwaltung von Software- und Hardwareprovidern in Oracle Solaris Cryptographic Framework.

Aufgabe	Beschreibung	Anweisungen
Auflisten der Provider in Oracle Solaris Cryptographic Framework	Listet die für die Verwendung in Oracle Solaris Cryptographic Framework zur Verfügung stehenden Algorithmen, Bibliotheken und Hardwaregeräte auf	„So listen Sie verfügbare Provider auf“ auf Seite 310
Hinzufügen eines Softwareproviders	Fügt eine PKCS #11-Bibliothek oder ein Kernel-Modul zu Oracle Solaris Cryptographic Framework hinzu. Der Provider muss signiert werden.	„So fügen Sie einen Softwareprovider hinzu“ auf Seite 313

Aufgabe	Beschreibung	Anweisungen
Verhindern der Verwendung eines Mechanismus auf Benutzerebene	Deaktiviert die Verwendung eines Softwaremechanismus. Der Mechanismus kann erneut aktiviert werden.	„So verhindern Sie die Verwendung eines Mechanismus auf Benutzerebene“ auf Seite 314
Vorübergehendes Deaktivieren von Mechanismen eines Kernel-Moduls	Deaktiviert vorübergehend die Verwendung eines Mechanismus. Wird üblicherweise zu Testzwecken verwendet	„So verhindern Sie die Verwendung eines Kernel-Modul-Softwareproviders“ auf Seite 316
Deinstallieren eines Providers	Deaktiviert die Verwendung eines Kernel-Softwareproviders	Beispiel 14–22
Auflisten verfügbarer Hardwareprovider	Zeigt die angeschlossene Hardware, die von der Hardware bereitgestellten Mechanismen und die für die Verwendung aktivierten Mechanismen an	„So listen Sie Hardwareprovider auf“ auf Seite 318
Deaktivieren von Mechanismen eines Hardwareproviders	Stellt sicher, dass ausgewählte Mechanismen auf einem Hardwarebeschleuniger nicht verwendet werden	„So deaktivieren Sie Mechanismen und Funktionen eines Hardwareproviders“ auf Seite 319
Neustarten oder Aktualisieren kryptografischer Services	Stellt sicher, dass kryptografische Services zur Verfügung stehen	„So führen Sie eine Aktualisierung oder einen Neustart aller kryptografischen Services durch“ auf Seite 321

Verwalten von Cryptographic Framework (Aufgaben)

In diesem Abschnitt wird beschrieben, wie die Software- und Hardwareprovider in Oracle Solaris Cryptographic Framework verwaltet werden. Bei Bedarf kann die Verwendung von Software- und Hardwareprovidern deaktiviert werden. So können Sie zum Beispiel die Implementierung des Algorithmus eines bestimmten Softwareproviders deaktivieren. Anschließend können Sie die Verwendung des Algorithmus eines anderen Softwareproviders durch das System erzwingen.

▼ So listen Sie verfügbare Provider auf

Oracle Solaris Cryptographic Framework stellt Algorithmen für verschiedene Typen von Verbrauchern bereit:

- Provider auf Benutzerebene stellen eine kryptografische PKCS #11-Schnittstelle für Anwendungen bereit, die mit der `libpkcs11`-Bibliothek verknüpft sind.
- Kernel-Softwareprovider stellen Algorithmen für IPsec, Kerberos und weitere Oracle Solaris-Kernel-Komponenten bereit.
- Kernel-Hardwareprovider stellen verfügbare Algorithmen für Kernel-Verbraucher und Anwendungen über die Bibliothek `pkcs11_kernel` bereit.

1 Listen Sie die Provider in Kurzformat auf.

Hinweis – Inhalt und Format der Providerliste unterscheiden sich je nach Oracle Solaris-Version. Führen Sie den Befehl `cryptoadm list` auf Ihrem System aus, um die vom System unterstützten Provider anzuzeigen.

Nur die Mechanismen auf Benutzerebene stehen gewöhnlichen Benutzern für die Verwendung zur Verfügung.

```
% cryptoadm list
user-level providers:
    /usr/lib/security/$ISA/pkcs11_kernel.so
    /usr/lib/security/$ISA/pkcs11_softtoken.so

kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa

kernel hardware providers:
    ncp/0
```

2 Listen Sie die Provider und die dazugehörigen Mechanismen in Oracle Solaris Cryptographic Framework auf.

Alle Mechanismen werden in der nachfolgenden Ausgabe aufgeführt. Dennoch können einige der aufgelisteten Mechanismen möglicherweise nicht verwendet werden. In Beispiel 14–16 wird die Liste auf diejenigen Mechanismen reduziert, die der Administrator für die Verwendung zugelassen hat.

Die Ausgabe wird zu Anzeigezwecken neu formatiert.

```
% cryptoadm list -m
user-level providers:
====================
/usr/lib/security/$ISA/pkcs11_kernel.so: CKM_MD5,CKM_MD5_HMAC,
CKM_MD5_HMAC_GENERAL,CKM_SHA_1,CKM_SHA_1_HMAC,CKM_SHA_1_HMAC_GENERAL,
...
/usr/lib/security/$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
CKM_AES_CBC,CKM_AES_CBC_PAD,CKM_AES_ECB,CKM_AES_KEY_GEN,
...
kernel software providers:
==========================
des: CKM_DES_ECB,CKM_DES_CBC,CKM_DES3_ECB,CKM_DES3_CBC
aes: CKM_AES_ECB,CKM_AES_CBC
blowfish: CKM_BF_ECB,CKM_BF_CBC
arcfour: CKM_RC4
sha1: CKM_SHA_1,CKM_SHA_1_HMAC,CKM_SHA_1_HMAC_GENERAL
md5: CKM_MD5,CKM_MD5_HMAC,CKM_MD5_HMAC_GENERAL
rsa: CKM_RSA_PKCS,CKM_RSA_X_509,CKM_MD5_RSA_PKCS,CKM_SHA1_RSA_PKCS
```

```
swrand: No mechanisms presented.

kernel hardware providers:
==========================
ncp/0: CKM_DSA,CKM_RSA_X_509,CKM_RSA_PKCS,CKM_RSA_PKCS_KEY_PAIR_GEN,
CKM_DH_PKCS_KEY_PAIR_GEN,CKM_DH_PKCS_DERIVE,CKM_EC_KEY_PAIR_GEN,
CKM_ECDH1_DERIVE,CKM_ECDSA
```

Beispiel 14–15 Suchen der vorhandenen kryptografischen Mechanismen

Im folgenden Beispiel werden alle von der Bibliothek auf Benutzerebene (`pkcs11_softtoken`) bereitgestellten Mechanismen aufgeführt.

```
% cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
Mechanisms:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
...
CKM_SSL3_KEY_AND_MAC_DERIVE,CKM_TLS_KEY_AND_MAC_DERIVE
```

Beispiel 14–16 Suchen der verfügbaren kryptografischen Mechanismen

Eine Richtlinie bestimmt, welche Mechanismen für die Verwendung zur Verfügung stehen. Der Administrator legt die Richtlinie fest. Ein Administrator kann Mechanismen eines bestimmten Providers nach Bedarf deaktivieren. Die Option `-p` zeigt die Liste der Mechanismen an, die von der vom Administrator festgelegten Richtlinie zugelassen werden.

```
% cryptoadm list -p
user-level providers:
=====================
/usr/lib/security/$ISA/pkcs11_kernel.so: all mechanisms are enabled.
random is enabled.
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.

kernel software providers:
==========================
des: all mechanisms are enabled.
aes: all mechanisms are enabled.
blowfish: all mechanisms are enabled.
arcfour: all mechanisms are enabled.
sha1: all mechanisms are enabled.
md5: all mechanisms are enabled.
rsa: all mechanisms are enabled.
swrand: random is enabled.

kernel hardware providers:
==========================
ncp/0: all mechanisms are enabled.
```

▼ So fügen Sie einen Softwareprovider hinzu

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Listen Sie die Softwareprovider auf, die dem System zur Verfügung stehen.

```
% cryptoadm list
user-level providers:
    /usr/lib/security/$ISA/pkcs11_kernel.so
    /usr/lib/security/$ISA/pkcs11_softtoken.so

kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa

kernel hardware providers:
    ncp/0
```

3 Fügen Sie das Paket des Providers mit dem Befehl `pkgadd` hinzu.

```
# pkgadd -d /path/to/package pkginst
```

Das Paket muss Software enthalten, die durch ein Zertifikat von Oracle signiert wurde. Informationen zum Anfordern eines Zertifikats von Oracle und zum Signieren eines Providers finden Sie in Anhang F, „Packaging and Signing Cryptographic Providers“ in *Developer's Guide to Oracle Solaris Security*.

Das Paket sollte Skripten aufweisen, die das kryptografische Framework benachrichtigen, dass ein weiterer Provider mit einer Gruppe von Mechanismen verfügbar ist. Weitere Informationen zu Packaging-Anforderungen finden Sie in Anhang F, „Packaging and Signing Cryptographic Providers“ in *Developer's Guide to Oracle Solaris Security*.

4 Aktualisieren Sie die Provider.

Sie müssen Provider aktualisieren, wenn Sie einen Softwareprovider hinzugefügt haben oder Hardware und eine angegebene Richtlinie für die Hardware hinzugefügt haben.

```
# svcadm refresh svc:/system/cryptosvc
```

5 Suchen Sie den neuen Provider in der Liste.

In diesem Fall wurde ein neuer Kernel-Softwareprovider installiert.

```
# cryptoadm list
...
```

```
kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa
    swrand
    ecc      <-- added provider
...
```

Beispiel 14–17 Hinzufügen eines Softwareproviders auf Benutzerebene

Im folgenden Beispiel ist eine signierte PKCS #11-Bibliothek installiert.

```
# pkgadd -d /cdrom/cdrom0/SolarisNew
    Answer the prompts
# svcadm refresh system/cryptosvc
# cryptoadm list
user-level providers:
=========================
    /usr/lib/security/$ISA/pkcs11_kernel.so
    /usr/lib/security/$ISA/pkcs11_softtoken.so
    /opt/SUNWconn/lib/$ISA/libpkcs11.so.1      <-- added provider
```

Entwickler, die eine Bibliothek mit dem kryptografischen Framework testen, können die Bibliothek manuell installieren.

```
# cryptoadm install provider=/opt/SUNWconn/lib/\$ISA/libpkcs11.so.1
```

Informationen zum Abrufen Ihres signierten Providers finden Sie unter „Binäre Signaturen für Drittanbietersoftware“ auf Seite 294.

▼ So verhindern Sie die Verwendung eines Mechanismus auf Benutzerebene

Wenn einige der kryptografischen Mechanismen eines Bibliotheksproviders nicht verwendet werden sollen, können Sie ausgewählte Mechanismen entfernen. In diesem Beispielverfahren werden DES-Mechanismen in der Bibliothek `pkcs11_softtoken` verwendet.

1 **Melden Sie sich als Superuser an oder nehmen Sie eine Rolle an, die das Berechtigungsprofil von Crypto Management enthält.**

In Beispiel 9–7 werden die Erstellung einer Rolle mit dem Crypto Management-Berechtigungsprofil und die Zuweisung der Rolle zu einem Benutzer dargestellt.

2. **Listen Sie die Mechanismen auf, die von einem bestimmten Softwareprovider auf Benutzerebene bereitgestellt werden.**

```
% cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
CKM_AES_CBC,CKM_AES_CBC_PAD,CKM_AES_ECB,CKM_AES_KEY_GEN,
...
```

3. **Listen Sie die für die Verwendung zur Verfügung stehenden Mechanismen auf.**

```
$ cryptoadm list -p
user-level providers:
=====================
...
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.
...
```

4. **Deaktivieren Sie die Mechanismen, die nicht verwendet werden sollen.**

```
$ cryptoadm disable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so \
> mechanism=CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB
```

5. **Listen Sie die für die Verwendung zur Verfügung stehenden Mechanismen auf.**

```
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_ECB,CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
```

Beispiel 14–18 Aktivieren eines Mechanismus eines Softwareproviders auf Benutzerebene

Im folgenden Beispiel wird ein deaktivierter DES-Mechanismus erneut für die Verwendung verfügbar gemacht.

```
$ cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
...
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_ECB,CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
$ cryptoadm enable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so \
> mechanism=CKM_DES_ECB
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
```

Beispiel 14–19 Aktivieren aller Mechanismen eines Softwareproviders auf Benutzerebene

Im folgenden Beispiel werden alle Mechanismen der Bibliothek auf Benutzerebene aktiviert.

```
$ cryptoadm enable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so all
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.
```

Beispiel 14–20 Dauerhaftes Entfernen der Verfügbarkeit von Softwareprovidern auf Benutzerebene

Im folgenden Beispiel wird die Bibliothek `libpkcs11.so.1` entfernt.

```
$ cryptoadm uninstall provider=/opt/SUNWconn/lib/\$ISA/libpkcs11.so.1
$ cryptoadm list
user-level providers:
    /usr/lib/security/$ISA/pkcs11_kernel.so
    /usr/lib/security/$ISA/pkcs11_softtoken.so

kernel software providers:
...
```

▼ So verhindern Sie die Verwendung eines Kernel-Modul-Softwareproviders

Stellt das kryptografische Framework verschiedene Modi eines Providers wie z. B. AES bereit, können Sie die Verwendung eines langsamen oder beschädigten Mechanismus deaktivieren. In diesem Beispielverfahren wird der AES-Algorithmus verwendet.

1 Melden Sie sich als Superuser an oder nehmen Sie eine Rolle an, die das Berechtigungsprofil von Crypto Management enthält.

In Beispiel 9–7 werden die Erstellung einer Rolle mit dem Crypto Management-Berechtigungsprofil und die Zuweisung der Rolle zu einem Benutzer dargestellt.

2 Listen Sie die Mechanismen auf, die von einem bestimmten Kernel-Softwareprovider bereitgestellt werden.

```
$ cryptoadm list -m provider=aes
aes: CKM_AES_ECB,CKM_AES_CBC
```

3 Listen Sie die für die Verwendung zur Verfügung stehenden Mechanismen auf.

```
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled.
```

4 Deaktivieren Sie den Mechanismus, der nicht verwendet werden soll.

```
$ cryptoadm disable provider=aes mechanism=CKM_AES_ECB
```

5 Listen Sie die für die Verwendung zur Verfügung stehenden Mechanismen auf.

```
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled, except CKM_AES_ECB.
```

Beispiel 14–21 Aktivieren eines Mechanismus eines Kernel-Softwareproviders

Im folgenden Beispiel wird ein deaktivierter AES-Mechanismus erneut für die Verwendung verfügbar gemacht.

```
cryptoadm list -m provider=aes
aes: CKM_AES_ECB,CKM_AES_CBC
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled, except CKM_AES_ECB.
$ cryptoadm enable provider=aes mechanism=CKM_AES_ECB
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled.
```

Beispiel 14–22 Vorübergehendes Entfernen des Kernel-Softwareproviders

Im folgenden Beispiel wird die Verwendung des AES-Providers vorübergehend deaktiviert. Der Unterbefehl `unload` ist hilfreich, wenn verhindert werden soll, dass ein Provider während des Deinstallierens automatisch geladen wird. Beispielsweise wird der Unterbefehl `unload` verwendet, wenn Sie ein sich auf den Provider auswirkendes Patch installieren.

```
$ cryptoadm unload provider=aes

$ cryptoadm list
...
kernel software providers:
    des
    aes (inactive)
    blowfish
    arcfour
    sha1
    md5
    rsa
    swrand
```

Der AES-Provider steht erst nach Aktualisierung des kryptografischen Frameworks zur Verfügung.

```
$ svcadm refresh system/cryptosvc

$ cryptoadm list
...
kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa
    swrand
```

Verwendet ein Kernel-Verbraucher den Kernel-Softwareprovider, wird die Software nicht entfernt. Es wird eine Fehlermeldung angezeigt und der Provider steht weiterhin für die Verwendung zur Verfügung.

Beispiel 14–23 Dauerhaftes Entfernen der Verfügbarkeit von Softwareprovidern

Im folgenden Beispiel wird die Verwendung des AES-Providers dauerhaft deaktiviert. Danach wird der AES-Provider nicht mehr in der Richtlinienliste der Kernel-Softwareprovider angezeigt.

```
$ cryptoadm uninstall provider=aes

$ cryptoadm list
...
kernel software providers:
    des
    blowfish
    arcfour
    sha1
    md5
    rsa
    swrand
```

Verwendet ein Kernel-Verbraucher den Kernel-Softwareprovider, wird eine Fehlermeldung angezeigt und der Provider steht weiterhin für die Verwendung zur Verfügung.

Beispiel 14–24 Neuinstallieren eines entfernten Kernel-Softwareproviders

Im folgenden Beispiel wird der Kernel-Softwareprovider AES neu installiert.

```
$ cryptoadm install provider=aes mechanism=CKM_AES_ECB,CKM_AES_CBC

$ cryptoadm list
...
kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa
    swrand
```

▼ So listen Sie Hardwareprovider auf

Hardwareprovider werden automatisch gesucht und geladen. Weitere Informationen finden Sie auf der Manpage `driver.conf(4)`.

Bevor Sie beginnen

Wenn Sie über Hardware verfügen, die voraussichtlich in Oracle Solaris Cryptographic Framework zum Einsatz kommt, wird die Hardware mit der SPI im Kernel registriert. Das Framework überprüft, ob der Hardwaretreiber signiert ist. Insbesondere prüft es, ob die Objektdatei des Treibers mit einem von Oracle ausgestellten Zertifikat signiert ist.

Zum Beispiel werden Hardwaremechanismen über das Sun Crypto Accelerator 6000-Board (`mca`), den ncp-Treiber für den kryptografischen Beschleuniger auf den UltraSPARC T1- und T2-Prozessoren (`ncp`) und den n2cp-Treiber für die UltraSPARC T2-Prozessoren (`n2cp`) an das Framework angeschlossen.

Informationen zum Abrufen Ihres signierten Providers finden Sie unter „Binäre Signaturen für Drittanbietersoftware“ auf Seite 294.

1 Listen Sie die Hardwareprovider auf, die auf dem System zur Verfügung stehen.

```
% cryptoadm list
...
kernel hardware providers:
   ncp/0
```

2 Listen Sie die Mechanismen auf, die der Chip oder das Board bereitstellt.

```
% cryptoadm list -m provider=ncp/0
ncp/0: CKM_DSA,CKM_RSA_X_509,CKM_RSA_PKCS,CKM_RSA_PKCS_KEY_PAIR_GEN,
CKM_DH_PKCS_KEY_PAIR_GEN,CKM_DH_PKCS_DERIVE,CKM_EC_KEY_PAIR_GEN,
CKM_ECDH1_DERIVE,CKM_ECDSA
```

3 Listen Sie die Mechanismen auf, die auf dem Chip oder Board für die Verwendung zur Verfügung stehen.

```
% cryptoadm list -p provider=ncp/0
ncp/0: all mechanisms are enabled.
```

▼ So deaktivieren Sie Mechanismen und Funktionen eines Hardwareproviders

Sie können Mechanismen sowie die Zufallszahlfunktion eines Hardwareproviders selektiv deaktivieren. In Beispiel 14–25 wird dargestellt, wie sie erneut aktiviert werden. Die in diesem Beispiel verwendete Hardware, das Sun Crypto Accelerator 1000-Board, stellt einen Generator für Zufallszahlen bereit.

1 Melden Sie sich als Superuser an oder nehmen Sie eine Rolle an, die das Berechtigungsprofil von Crypto Management beinhaltet.

In Beispiel 9–7 werden die Erstellung einer Rolle mit dem Crypto Management-Berechtigungsprofil und die Zuweisung der Rolle zu einem Benutzer dargestellt.

2 Wählen Sie die Mechanismen oder die Funktion, die Sie deaktivieren möchten.

Listen Sie den Hardwareprovider auf.

```
# cryptoadm list
...
```

```
Kernel hardware providers:
    dca/0
```

- **Deaktivieren Sie ausgewählte Mechanismen.**

```
# cryptoadm list -m provider=dca/0
dca/0: CKM_RSA_PKCS, CKM_RSA_X_509, CKM_DSA, CKM_DES_CBC, CKM_DES3_CBC
random is enabled.
# cryptoadm disable provider=dca/0 mechanism=CKM_DES_CBC,CKM_DES3_CBC
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_CBC,CKM_DES3_CBC.
random is enabled.
```

- **Deaktivieren Sie den Generator für Zufallszahlen.**

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 random
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is disabled.
```

- **Deaktivieren Sie alle Mechanismen. Deaktivieren Sie nicht den Generator für Zufallszahlen.**

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 mechanism=all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are disabled. random is enabled.
```

- **Deaktivieren Sie sämtliche Funktionen und Mechanismen der Hardware.**

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are disabled. random is disabled.
```

Beispiel 14–25 Aktivieren von Mechanismen und Funktionen auf einem Hardwareprovider

In den folgenden Beispielen werden deaktivierte Mechanismen einer Hardwarekomponente selektiv aktiviert.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_ECB,CKM_DES3_ECB


.
random is enabled.
# cryptoadm enable provider=dca/0 mechanism=CKM_DES3_ECB
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_ECB.
random is enabled.
```

Im folgenden Beispiel wird nur der Zufallsgenerator aktiviert.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,....
random is disabled.
```

```
# cryptoadm enable provider=dca/0 random
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,....
random is enabled.
```

Im folgenden Beispiel werden nur die Mechanismen aktiviert. Der Zufallsgenerator ist weiterhin deaktiviert.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,....
random is disabled.
# cryptoadm enable provider=dca/0 mechanism=all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is disabled.
```

Im folgenden Beispiel werden sämtliche Funktionen und Mechanismen auf dem Board aktiviert.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_DES_ECB,CKM_DES3_ECB.
random is disabled.
# cryptoadm enable provider=dca/0 all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
```

▼ So führen Sie eine Aktualisierung oder einen Neustart aller kryptografischen Services durch

Standardmäßig ist Oracle Solaris Cryptographic Framework aktiviert. Schlägt der Dämon `kcfd` aus irgendeinem Grund fehl, kann SMF (Service Management Facility) zum Neustarten kryptografischer Services verwendet werden. Weitere Informationen finden Sie auf den Manpages `smf(5)` und `svcadm(1M)`. Informationen zur Auswirkung des Neustarts kryptografischer Services auf Zonen finden Sie unter „Kryptografische Services und Zonen“ auf Seite 295.

1 Überprüfen Sie den Status kryptografischer Services.

```
% svcs cryptosvc
 STATE          STIME    FMRI
offline         Dec_09   svc:/system/cryptosvc:default
```

2 Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an, um kryptografische Services zu aktivieren.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

```
# svcadm enable svc:/system/cryptosvc
```

Beispiel 14–26 Aktualisieren kryptografischer Services

Im folgenden Beispiel werden kryptografische Services in der globalen Zone aktualisiert. Infolgedessen wird die Kryptografierichtlinie auf Kernel-Ebene in allen nicht globalen Zonen ebenfalls aktualisiert.

```
# svcadm refresh system/cryptosvc
```

◆ ◆ ◆ KAPITEL 15

15 Oracle Solaris Key Management Framework

Ab der Version Solaris 10 8/07 stellt KMF (Key Management Framework) Tools und Programmierschnittstellen für die Verwaltung von Public-Key-Objekten bereit. Public-Key-Objekte enthalten X.509-Zertifikate und Paare aus öffentlichem und privatem Schlüssel. Die Formate für die Speicherung dieser Objekte können variieren. KMF bietet ebenfalls ein Tool für die Verwaltung von Richtlinien, die die Verwendung von X.509-Zertifikaten durch Anwendungen bestimmen.

- „Verwalten von Public-Key-Technologien“ auf Seite 323
- „Dienstprogramme von Key Management Framework“ auf Seite 324
- „Verwenden von Key Management Framework (Aufgaben)“ auf Seite 326

Verwalten von Public-Key-Technologien

KMF (Key Management Framework) bietet einen einheitlichen Ansatz für die Verwaltung von Publik-Key-Technologien (PKI). Oracle Solaris umfasst mehrere verschiedene Anwendungen, in denen PKI-Technologien zum Einsatz kommen. Jede Anwendung verfügt über eigene Programmierschnittstellen, Schlüsselspeichermechanismen und administrative Dienstprogramme. Stellt eine Anwendung einen Mechanismus zur Durchsetzung von Richtlinien bereit, so gilt dieser Mechanismus nur für die entsprechende Anwendung. Mit KMF verwenden Anwendungen einen einheitlichen Satz administrativer Tools, einen einzelnen Satz von Programmierschnittstellen sowie einen einzelnen Mechanismus zur Durchsetzung von Richtlinien. Mit diesen Funktionen werden die Anforderungen hinsichtlich PKI aller Anwendungen verwaltet, die diese Schnittstellen übernehmen.

KMF vereinheitlicht die Verwaltung von Public-Key-Technologien mit folgenden Schnittstellen:

- **pktool-Befehl**: Mit diesem Befehl werden PKI-Objekte wie z. B. Zertifikate in verschiedenen Schlüsselspeichern verwaltet.
- **kmfcfg-Befehl**: Mit diesem Befehl wird die Datenbank für PKI-Richtlinien verwaltet.

  Unter Entscheidungen hinsichtlich PKI-Richtlinien fallen Vorgänge wie zum Beispiel die Validierungsmethode für einen Vorgang. Außerdem kann eine PKI-Richtlinie den Geltungsbereich eines Zertifikats begrenzen. So kann eine PKI-Richtlinie beispielsweise durchsetzen, dass ein Zertifikat nur für bestimmte Zwecke verwendet werden kann. Durch eine solche Richtlinie würde verhindert, dass das Zertifikat für andere Anforderungen verwendet wird.
- **KMF-Bibliothek**: Diese Bibliothek enthält Programmierschnittstellen, die den zugrunde liegenden Schlüsselspeichermechanismus abstrahieren.

  Anwendungen müssen keinen bestimmten Schlüsselspeichermechanismus auswählen, können jedoch von einem Mechanismus zu einem anderen migriert werden. Die unterstützten Schlüsselspeicher sind PKCS #11, NSS und OpenSSL. Die Bibliothek umfasst ein plugfähiges Framework, sodass neue Schlüsselspeichermechanismen hinzugefügt werden können. Daher wären bei Anwendungen, die die neuen Mechanismen verwenden, nur geringfügige Änderungen erforderlich, damit ein neuer Schlüsselspeicher verwendet werden kann.

Dienstprogramme von Key Management Framework

KMF bietet Methoden zur Verwaltung des Schlüsselspeichers und stellt die Gesamtrichtlinie für die Verwendung der darin enthaltenen Schlüssel bereit. KMF verwaltet die Richtlinie, die Schlüssel und die Zertifikate für drei Publik-Key-Technologien:

- Token von PKCS #11-Providern, d. h. von Oracle Solaris Cryptographic Framework
- NSS (Network Security Services)
- OpenSSL, ein dateibasierter Schlüsselspeicher

Mit dem Tool `kmfcfg` können KMF-Richtlinieneinträge erstellt, geändert oder gelöscht werden. KMF verwaltet Schlüsselspeicher über den Befehl `pktool`. Weitere Informationen finden Sie auf den Manpages `kmfcfg(1)` und `pktool(1)` sowie in den folgenden Abschnitten.

KMF-Richtlinienverwaltung

Die KMF-Richtlinie wird in einer Datenbank gespeichert. Auf diese Richtliniendatenbank wird intern von allen Anwendungen zugegriffen, die die KMF-Programmierschnittstellen verwenden. Die Datenbank kann die Verwendung der von der KMF-Bibliothek verwalteten Schlüssel und Zertifikate einschränken. Wenn eine Anwendung versucht, ein Zertifikat zu überprüfen, prüft sie die Richtliniendatenbank. Der Befehl `kmfcfg` ändert die Richtliniendatenbank.

KMF-Schlüsselspeicherverwaltung

KMF verwaltet die Schlüsselspeicher für drei Public-Key-Technologien: PKCS #11, Token, NSS und OpenSSL. Für alle diese Technologien können Sie mithilfe des Befehls `pktool` folgende Aktionen ausführen:

- Generieren eines selbstsignierten Zertifikats
- Generieren einer Zertifikatanforderung
- Importieren von Objekten in den Schlüsselspeicher
- Auflisten der Objekte im Schlüsselspeicher
- Löschen von Objekten aus dem Schlüsselspeicher
- Herunterladen einer CRL

Für die Technologien PKCS #11 und NSS können Sie mit dem Befehl `pktool` außerdem durch Generieren eines Passwortsatzes eine PIN festlegen:

- Generieren eines Passwortsatzes für den Schlüsselspeicher
- Generieren eines Passwortsatzes für ein Objekt im Schlüsselspeicher

Beispiele für die Verwendung des Dienstprogramms `pktool` finden Sie auf der Manpage `pktool(1)` und unter „Verwenden von Key Management Framework (Übersicht der Schritte)“ auf Seite 325.

Verwenden von Key Management Framework (Übersicht der Schritte)

KMF (Key Management Framework) ermöglicht Ihnen die zentrale Verwaltung von Public-Key-Technologien.

Aufgabe	Beschreibung	Anweisungen
Erstellen eines Zertifikats	Erstellt ein Zertifikat für die Verwendung durch PKCS #11, NSS oder SSL	„So erstellen Sie ein Zertifikat mit dem Befehl `pktool gencert`“ auf Seite 326

Aufgabe	Beschreibung	Anweisungen
Exportieren eines Zertifikats	Erstellt eine Datei mit dem Zertifikat und den dazugehörigen unterstützenden Schlüsseln. Die Datei kann mit einem Passwort geschützt werden.	„So exportieren Sie ein Zertifikat und einen privaten Schlüssel im PKCS #12-Format“ auf Seite 329
Importieren eines Zertifikats	Importiert ein Zertifikat aus einem anderen System	„So importieren Sie ein Zertifikat in den Schlüsselspeicher“ auf Seite 327
	Importiert ein Zertifikat im PKCS #12-Format aus einem anderen System	Beispiel 15–2
Generieren eines Passwortsatzes	Generiert einen Passwortsatz für den Zugriff auf einen PKCS #11- oder NSS-Schlüsselspeicher	„So generieren Sie einen Passwortsatz mit dem Befehl `pktool setpin`“ auf Seite 330

Verwenden von Key Management Framework (Aufgaben)

In diesem Abschnitt wird beschrieben, wie Sie mithilfe des Befehls `pktool` Ihre Public-Key-Objekte wie z. B. Passwörter, Passwortsätze, Dateien, Schlüsselspeicher, Zertifikate und CRLs verwalten.

▼ So erstellen Sie ein Zertifikat mit dem Befehl `pktool gencert`

Mit diesem Verfahren wird ein selbstsigniertes Zertifikat erstellt und im PKCS #11-Schlüsselspeicher gespeichert. Als Teil dieses Vorgangs wird ebenfalls ein Paar aus öffentlichem und privatem RSA-Schlüssel erstellt. Der private Schlüssel wird in dem Schlüsselspeicher mit dem Zertifikat gespeichert.

1 Generieren eines selbstsignierten Zertifikats

```
% pktool gencert [keystore=keystore] label=label-name \
subject=subject-DN serial=hex-serial-number
```

`keystore=`*keystore* — Gibt den Schlüsselspeicher nach Typ des Public-Key-Objekts an. Der Wert kann `nss`, `pkcs11` oder `ssl` sein. Dieses Schlüsselwort ist optional.

`label=`*label-name* — Gibt einen eindeutigen Namen an, den der Aussteller an das Zertifikat weitergibt

`subject=`*subject-DN* — Gibt den Distinguished Name für das Zertifikat an

`serial=`*hex-serial-number* — Gibt die Seriennummer im hexadezimalen Format an. Der Aussteller des Zertifikats wählt die Nummer aus, z. B. `0x0102030405`.

2 Überprüfen Sie den Inhalt des Schlüsselspeichers.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
      Label:  label-name
      ID: Fingerprint that binds certificate to private key
      Subject: subject-DN
      Issuer:  distinguished-name
      Serial:  hex-serial-number
n. ...
```

Dieser Befehl listet alle Zertifikate im Schlüsselspeicher auf. Im folgenden Beispiel enthält der Schlüsselspeicher nur ein Zertifikat.

Beispiel 15–1 Erstellen eines selbstsignierten Zertifikats mit `pktool`

Im folgenden Beispiel erstellt ein Benutzer bei `My Company` ein selbstsigniertes Zertifikat und speichert dieses in einem Schlüsselspeicher für PKCS #11-Objekte. Zu Beginn ist der Schlüsselspeicher leer. Wenn der Schlüsselspeicher nicht initialisiert wurde, lautet die PIN für das Softtoken `changeme`.

```
% pktool gencert keystore=pkcs11 label="My Cert" \
subject="C=US, O=My Company, OU=Security Engineering Group, CN=MyCA" \
serial=0x000000001
Enter pin for Sun Software PKCS#11 softtoken:     Type PIN for token
```

```
% pktool list
Found 1 certificates.
1. (X.509 certificate)
      Label: My Cert
      ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
      Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
      Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
      Serial: 0x01
```

▼ So importieren Sie ein Zertifikat in den Schlüsselspeicher

In diesem Verfahren wird beschrieben, wie eine Datei mit PKI-Informationen, die mit PEM oder Raw-DER verschlüsselt wurde, in Ihren Schlüsselspeicher importiert wird. In Beispiel 15–4 wird ein Exportverfahren dargestellt.

1 Importieren Sie das Zertifikat.

```
% pktool import keystore=keystore infile=infile-name label=label-name
```

2 Wenn Sie private PKI-Objekte importieren, geben Sie Passwörter an, sofern Sie dazu aufgefordert werden.

a. Geben Sie bei Aufforderung das Passwort für die Datei an.

Wenn Sie private PKI-Informationen importieren, wie z. B. eine Exportdatei im PKCS #12-Format, ist für die entsprechende Datei ein Passwort erforderlich. Der Ersteller der importierten Datei stellt Ihnen das PKCS #12-Passwort zur Verfügung.

```
Enter password to use for accessing the PKCS12 file:      Type PKCS #12 password
```

b. Geben Sie bei Aufforderung das Passwort für Ihren Schlüsselspeicher ein.

```
Enter pin for Sun Software PKCS#11 softtoken:      Type PIN for token
```

3 Überprüfen Sie den Inhalt des Schlüsselspeichers.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
      Label:  label-name
      ID:  Fingerprint that binds certificate to private key
      Subject:  subject-DN
      Issuer:  distinguished-name
      Serial:  hex-serial-number
2. ...
```

Beispiel 15–2 Importieren einer PKCS #12-Datei in den Schlüsselspeicher

Im folgenden Beispiel importiert der Benutzer eine PKCS #12-Datei eines anderen Erstellers. Der Befehl `pktool import` extrahiert den privaten Schlüssel und das Zertifikat aus der Datei `gracedata.p12` und speichert beides in dem bevorzugten Schlüsselspeicher des Benutzers.

```
% pktool import keystore=pkcs11 infile=gracedata.p12 label=GraceCert
Enter password to use for accessing the PKCS12 file:      Type PKCS #12 password
Enter pin for Sun Software PKCS#11 softtoken:      Type PIN for token
Found 1 certificate(s) and 1 key(s) in gracedata.p12
% pktool list
Found 1 certificates.
1. (X.509 certificate)
        Label: GraceCert
        ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
        Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
        Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
        Serial: 0x01
```

Beispiel 15–3 Importieren eines X.509-Zertifikats in den Schlüsselspeicher

Im folgenden Beispiel importiert der Benutzer ein X.509-Zertifikat im PEM-Format in den bevorzugten Schlüsselspeicher des Benutzers. Dieses öffentliche Zertifikat wird nicht mit einem Passwort geschützt. Der öffentliche Schlüsselspeicher des Benutzers ist ebenfalls nicht passwortgeschützt.

```
% pktool import keystore=pkcs11 infile=somecert.pem label="TheirCompany Root Cert"
% pktool list
Found 1 certificates.
1. (X.509 certificate)
        Label: TheirCompany Root Cert
        ID: 21:ae:83:98:24:d1:1f:cb:65:5b:48:75:7d:02:47:cf:98:1f:ec:a0
        Subject: C=US, O=TheirCompany, OU=Security, CN=TheirCompany Root CA
        Issuer: C=US, O=TheirCompany, OU=Security, CN=TheirCompany Root CA
        Serial: 0x01
```

▼ So exportieren Sie ein Zertifikat und einen privaten Schlüssel im PKCS #12-Format

Sie können eine Datei im PKCS #12-Format erstellen, um private Schlüssel und das dazugehörige X.509-Zertifikat auf andere Systeme zu exportieren. Der Zugriff auf die Datei wird durch ein Passwort geschützt.

1 Suchen Sie das zu exportierende Zertifikat.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
      Label:  label-name
      ID: Fingerprint that binds certificate to private key
      Subject: subject-DN
      Issuer:  distinguished-name
      Serial:  hex-serial-number
2. ...
```

2 Exportieren Sie die Schlüssel und das Zertifikat.

Verwenden Sie den Schlüsselspeicher und die Beschriftung aus dem Befehl `pktool list`. Geben Sie einen Dateinamen für die Exportdatei an. Wenn der Name ein Leerzeichen enthält, setzen Sie ihn in doppelte Anführungszeichen.

```
% pktool export keystore=keystore outfile=outfile-name label=label-name
```

3 Schützen Sie die Exportdatei mit einem Passwort.

Geben Sie bei Aufforderung das aktuelle Passwort für den Schlüsselspeicher ein. An diesem Punkt erstellen Sie ein Passwort für die Exportdatei. Der Empfänger muss dieses Passwort beim Importieren der Datei angeben.

```
Enter pin for Sun Software PKCS#11 softtoken:      Type PIN for token
Enter password to use for accessing the PKCS12 file:     Create PKCS #12 password
```

Tipp – Senden Sie das Passwort separat von der Exportdatei. Gemäß der Best Practices empfiehlt es sich, das Passwort außerbandig anzugeben, z. B. während eines Telefonanrufs.

Beispiel 15–4 Exportieren eines Zertifikats und eines privaten Schlüssels im PKCS #12-Format

Im folgenden Beispiel exportiert ein Benutzer die privaten Schlüssel mit dem dazugehörigen X.509-Zertifikat in eine standardmäßige PKCS #12-Datei. Diese Datei kann in andere Schlüsselspeicher importiert werden. Das PKCS #11-Passwort schützt den Quellschlüsselspeicher. Das PKCS #12-Passwort wird zum Schützen privater Daten in der PKCS #12-Datei verwendet. Dieses Passwort wird zum Importieren der Datei benötigt.

```
% pktool list
Found 1 certificates.
1. (X.509 certificate)
      Label: My Cert
      ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
      Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
      Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
      Serial: 0x01

% pktool export keystore=pkcs11 outfile=mydata.p12 label="My Cert"
Enter pin for Sun Software PKCS#11 softtoken:      Type PIN for token
Enter password to use for accessing the PKCS12 file:     Create PKCS #12 password
```

Der Benutzer telefoniert dann mit dem Empfänger und stellt das PKCS #12-Passwort bereit.

▼ So generieren Sie einen Passwortsatz mit dem Befehl `pktool setpin`

Sie können einen Passwortsatz für ein Objekt in einem Schlüsselspeicher sowie für den Schlüsselspeicher selbst generieren. Der Passwortsatz ist für den Zugriff auf das Objekt oder den Schlüsselspeicher erforderlich. In Beispiel 15–4 wird die Generierung eines Passwortsatzes für ein Objekt in einem Schlüsselspeicher dargestellt.

1 Generieren Sie einen Passwortsatz für den Zugriff auf einen Schlüsselspeicher.

```
% pktool setpin keystore=nss|pkcs11 dir=directory
```

2 Beantworten Sie die Eingabeaufforderungen.

Wenn für den Schlüsselspeicher noch kein Passwort festgelegt wurde, drücken Sie die Eingabetaste, um das Passwort zu erstellen.

```
Enter current token passphrase:      Press the Return key
Create new passphrase:      Type the passphrase that you want to use
Re-enter new passphrase:      Retype the passphrase
Passphrase changed.
```

Der Schlüsselspeicher wird jetzt durch *passphrase* geschützt. Wenn Sie den Passwortsatz verlieren, können Sie nicht mehr auf die Objekte im Schlüsselspeicher zugreifen.

Beispiel 15–5 Schützen eines Schlüsselspeichers mit einem Passwortsatz

Im folgenden Beispiel wird dargestellt, wie der Passwortsatz für eine NSS-Datenbank festgelegt wird. Da kein Passwortsatz erstellt wurde, drückt der Benutzer die Eingabetaste bei der ersten Aufforderung.

```
% pktool setpin keystore=nss dir=/var/nss
Enter current token passphrase:      Press the Return key
Create new passphrase:    has8n0NdaH
Re-enter new passphrase:  has8n0NdaH
Passphrase changed.
```

TEIL V

Authentifizierungsservices und sichere Kommunikation

In diesem Abschnitt werden Authentifizierungsservices beschrieben, die auf einem nicht vernetzten System oder zwischen zwei Systemen konfiguriert werden können.

- Kapitel 16, „Verwenden von Authentifizierungsservices (Aufgaben)“
- Kapitel 17, „Verwenden von PAM“
- Kapitel 18, „Verwenden von SASL“
- Kapitel 19, „Verwenden von Oracle Solaris Secure Shell (Aufgaben)“
- Kapitel 20, „Oracle Solaris Secure Shell (Referenz)“

Weitere Informationen zum Konfigurieren eines Netzwerks von authentifizierten Benutzern und Systemen finden Sie unter Teil VI.

◆ ◆ ◆ KAPITEL 16

Verwenden von Authentifizierungsservices (Aufgaben)

In diesem Kapitel wird beschrieben, wie Sie mit Secure RPC einen Host und einen Benutzer über eine NFS-Einhängung authentifizieren. Im Folgenden sind die Themen in diesem Kapitel aufgeführt.

- „Übersicht zu Secure RPC“ auf Seite 335
- „Verwalten von Secure RPC (Übersicht der Schritte)“ auf Seite 340

Übersicht zu Secure RPC

Durch Secure RPC (Remote Procedure Call) werden Remote-Verfahren durch einen Authentifizierungsmechanismus geschützt. Durch den Diffie-Hellman-Authentifzierungsmechanismus werden sowohl der Host als auch der Benutzer, der eine Anforderung für einen Service stellt, authentifiziert. Der Authentifizierungsmechanismus verwendet eine DES-Verschlüsselung (Data Encryption Standard). Zu den Anwendungen, die Secure RPC verwenden, zählen NFS und die Naming Services NIS und NIS+.

NFS-Services und Secure RPC

Durch NFS können mehrere Hosts Dateien über das Netzwerk gemeinsam verwenden. Bei einem NFS-Service speichert ein Server die Daten und Ressourcen für mehrere Clients. Die Clients verfügen über Zugriff auf die Dateisysteme, die der Server gemeinsam mit den Clients verwendet. Benutzer, die an den Clientsystemen angemeldet sind, können auf die Dateisysteme zugreifen, indem sie die Dateisysteme über den Server einhängen. Für den Benutzer im Clientsystem sieht es aus, als ob die Dateien lokal auf dem Client vorhanden wären. Bei einer der häufigsten Verwendungen von NFS können Systeme in Büros installiert werden, während alle Benutzerdateien an einem zentralen Ort gespeichert werden. Durch einige Funktionen des NFS-Service, wie der Option `-nosuid` für den Befehl `mount`, kann verhindert werden, dass Geräte und Dateisysteme durch unberechtigte Benutzer geöffnet werden.

Der NFS-Service verwendet Secure RPC für die Authentifizierung der Benutzer, die Anforderungen über das Netzwerk stellen. Dieser Prozess wird als *Secure NFS* bezeichnet. Der Diffie-Hellman-Authentifizierungsmechanismus (`AUTH_DH`) verwendet DES-Verschlüsselung, um einen berechtigten Zugriff zu ermöglichen. Der `AUTH_DH`-Mechanismus kann auch als `AUTH_DES` bezeichnet werden. Weitere Informationen finden Sie hier:

- Einrichten und Verwalten von Secure NFS: „Verwalten des Secure NFS-Systems“ in *Systemverwaltungshandbuch: Netzwerkdienste*
- Einrichten von NIS+-Tabellen und Eingeben von Namen in der Tabelle `cred`: *System Administration Guide: Naming and Directory Services (NIS+)*
- Übersicht der Transaktionen bei der RPC-Authentifizierung: „Implementierung der Diffie-Hellman-Authentifizierung“ auf Seite 337

DES-Verschlüsselung mit Secure NFS

Die Funktionen der DES-Verschlüsselung (Data Encryption Standard) verwenden einen 56-Bit-Schlüssel zum Verschlüsseln der Daten. Wenn zwei Benutzer mit Berechtigungen oder zwei Hauptelemente denselben DES-Schlüssel kennen, können sie eine private Kommunikation durchführen, indem sie mit dem Schlüssel Text verschlüsseln und entschlüsseln. DES ist ein relativ schneller Verschlüsselungsmechanismus. Ein DES-Chip ermöglicht eine weitere Beschleunigung der Verschlüsselung. Wenn der Chip jedoch nicht vorhanden ist, wird er durch eine Softwareimplementierung ersetzt.

Wenn nur der DES-Schlüssel verwendet wird, besteht das Risiko, dass ein Eindringling einen ausreichenden Umfang an Verschlüsselungstextmeldungen erfassen kann, die mit dem gleichen Schlüssel verschlüsselt wurden, und so den Schlüssel feststellen und die Meldungen entschlüsseln kann. Daher müssen Sicherheitssysteme wie Secure NFS die Schlüssel häufig ändern.

Kerberos-Authentifizierung

Kerberos ist ein Authentifizierungssystem, das vom MIT entwickelt wurde. Die Verschlüsselung in Kerberos basiert in einigen Fällen auf DES. Die Unterstützung für Kerberos V4 wird im Rahmen von Secure RPC nicht mehr zur Verfügung gestellt. Eine client- und serverseitige Implementierung von Kerberos V5, die RPCSEC_GSS verwendet, ist jedoch in dieser Version enthalten. Weitere Informationen erhalten Sie unter Kapitel 21, „Einführung zum Kerberos-Service“.

Diffie-Hellman-Authentifizierung und Secure RPC

Die DH-Methode (Diffie-Hellman) zur Authentifizierung eines Benutzers ist nicht trivial und für einen Eindringling nur schwer zu entschlüsseln. Der Client und Server verfügen über einen eigenen privaten Schlüssel, der zusammen mit dem öffentlichen Schlüssel zum Erstellen eines

allgemeinen Schlüssels verwendet wird. Der private Schlüssel wird auch als der *geheime Schlüssel* bezeichnet. Der Client und Server verwenden den allgemeinen Schlüssel für die gemeinsame Kommunikation. Der allgemeine Schlüssel wird durch eine vereinbarte Verschlüsselungsfunktion (z. B. DES) verschlüsselt.

Bei der Authentifizierung kann das sendende System mit dem allgemeinen Schlüssel die aktuelle Uhrzeit verschlüsseln. Anschließend kann das empfangende System den Schlüssel entschlüsseln und mit der eigenen aktuellen Uhrzeit vergleichen. Die Uhrzeiten auf dem Client und Server müssen synchronisiert sein. Weitere Informationen erhalten Sie unter „Verwalten von Network Time Protocol (Aufgaben)“ in *Systemverwaltungshandbuch: Netzwerkdienste*.

Die öffentlichen und privaten Schlüssel werden in einer NIS- oder NIS+-Datenbank gespeichert. Bei NIS werden die Schlüssel in der Map `publickey` gespeichert. Bei NIS+ werden die Schlüssel in der Tabelle `cred` gespeichert. Diese Dateien enthalten den öffentlichen und privaten Schlüssel für alle potenziellen Benutzer.

Der Systemadministrator ist verantwortlich für die Einrichtung der NIS-Maps oder NIS+-Tabellen und für das Generieren eines öffentlichen und privaten Schlüssels für die einzelnen Benutzer. Der private Schlüssel wird zusammen mit dem Passwort des Benutzers in verschlüsselter Form gespeichert. Dadurch kennt nur der Benutzer den privaten Schlüssel.

Implementierung der Diffie-Hellman-Authentifizierung

Im diesem Abschnitt werden eine Reihe von Transaktionen in einer Client-Server-Sitzung beschrieben, in der die Diffie-Hellman-Authentifizierung (`AUTH_DH`) verwendet wird.

Generieren der öffentlichen und geheimen Schlüssel für Secure RPC

In einigen Fällen führt der Administrator vor einer Transaktion entweder den Befehl `newkey` oder `nisaddcred` aus, um einen öffentlichen und geheimen Schlüssel zu generieren. Jeder Benutzer erhält einen eindeutigen öffentlichen und geheimen Schlüssel. Der öffentliche Schlüssel wird in einer öffentlichen Datenbank gespeichert. Der geheime Schlüssel wird in der gleichen Datenbank in verschlüsselter Form gespeichert. Durch den Befehl `chkey` wird das Schlüsselpaar geändert.

Ausführen des Befehls keylogin für Secure RPC

Normalerweise entspricht das Passwort für die Anmeldung dem Passwort für Secure RPC. In diesem Fall ist der Befehl `keylogin` nicht erforderlich. Wenn die Passwörter jedoch unterschiedlich sind, müssen sich die Benutzer anmelden und anschließend den Befehl `keylogin` ausführen.

Durch den Befehl `keylogin` wird der Benutzer zur Eingabe eines Passworts für Secure RPC aufgefordert. Der Befehl verwendet anschließend das Passwort zum Entschlüsseln des geheimen Schlüssels. Anschließend leitet der Befehl `keylogin` den entschlüsselten geheimen Schlüssel an das Programm *keyserver* weiter. Der Schlüsselserver (Keyserver) ist ein

RPC-Service mit einer lokalen Instanz auf jedem Computer. Der Schlüsselserver speichert den entschlüsselten geheimen Schlüssel und wartet, bis der Benutzer eine Secure RPC-Transaktion mit einem Server startet.

Wenn das Passwort für die Anmeldung und das Passwort für RPC identisch sind, leitet der Anmeldeprozess den geheimen Schlüssel an den Schlüsselserver weiter. Wenn die Passwörter unterschiedlich sein müssen, muss der Benutzer jedes Mal den Befehl `keylogin` ausführen. Wenn der Befehl `keylogin` in der Konfigurationsdatei der Benutzerumgebung enthalten ist (z. B. Datei `~/.login`, `~/.cshrc` oder `~/.profile`), wird der Befehl `keylogin` bei jeder Anmeldung des Benutzers automatisch ausgeführt.

Generieren des Dialogschlüssels für Secure RPC

Wenn der Benutzer eine Transaktion mit einem Server startet, geschieht Folgendes:

1. Der Schlüsselserver generiert einen zufällig erzeugten Dialogschlüssel.
2. Der Kernel verwendet den Dialogschlüssel sowie weiteres Material, um den Zeitstempel des Clients zu verschlüsseln.
3. Der Schlüsselserver sucht den öffentlichen Schlüssel des Servers in der Datenbank für öffentliche Schlüssel. Weitere Informationen erhalten Sie auf der Manpage `publickey(4)`.
4. Der Schlüsselserver verwendet den geheimen Schlüssel des Clients und den öffentlichen Schlüssel des Servers, um einen gemeinsamen Schlüssel zu erstellen.
5. Der Schlüsselserver verschlüsselt den Dialogschlüssel mit dem allgemeinen Schlüssel.

Anfängliche Kontaktaufnahme des Servers mit Secure RPC

Die Übertragung, die den verschlüsselten Zeitstempel und den verschlüsselten Dialogschlüssel enthält, wird anschließend an den Server gesendet. Die Übertragung enthält einen Berechtigungsnachweis und Verifikator. Der Berechtigungsnachweis weist drei Bestandteile auf:

- Den Netzwerknamen des Clients
- Den Dialogschlüssel, der durch den allgemeinen Schlüssel verschlüsselt wird
- Ein "Fenster", das durch den Dialogschlüssel verschlüsselt wird

Das Fenster ist der Zeitunterschied, den der Client zwischen dem Takt des Servers und dem Zeitstempel des Clients zulässt. Wenn der Unterschied zwischen dem Takt des Servers und dem Zeitstempel größer als das Fenster ist, weist der Server die Clientanforderung zurück. Unter normalen Umständen geschieht keine Zurückweisung, da der Client zuerst eine Synchronisierung mit dem Server durchführt, bevor die RPC-Sitzung gestartet wird.

Der Verifikator des Clients enthält Folgendes:

- Den verschlüsselten Zeitstempel
- Einen verschlüsselten Verifikator des angegebenen Fensters, der dekremental um den Wert von 1 verringert wird

Der Fensterverifikator wird benötigt, falls ein Benutzer einen anderen Benutzer imitieren möchte. Der Imitator kann ein Programm schreiben, das nicht die verschlüsselten Felder des Berechtigungsnachweises und Verifikators ausfüllt, sondern nur zufällige Bits einfügt. Der Server entschlüsselt den Dialogschlüssel in einen zufällig erzeugten Schlüssel. Der Server verwendet anschließend den Schlüssel, um das Fenster und den Zeitstempel zu entschlüsseln. Das Ergebnis sind zufällig erzeugte Zahlen. Nach einigen tausend Versuchen erreicht das zufällig erzeugte Fenster/Zeitstempel-Paar möglicherweise einen Zugriff am Authentifizierungssystem. Durch den Fensterverifikator verringert sich die Möglichkeit, dass ein gefälschter Berechtigungsnachweis authentifiziert wird.

Entschlüsseln des Dialogschlüssels mit Secure RPC

Wenn der Server die Übertragung vom Client erhält, geschieht Folgendes:

1. Der Schlüsselserver, der sich lokal am Server befindet, sucht den öffentlichen Schlüssel des Clients in der Datenbank für öffentliche Schlüssel.
2. Der Schlüsselserver verwendet den öffentlichen Schlüssel des Clients und den geheimen Schlüssel des Servers, um den allgemeinen Schlüssel abzuleiten. Der allgemeine Schlüssel ist der gleiche allgemeine Schlüssel, der vom Client berechnet wird. Nur der Server und Client können den allgemeinen Schlüssel berechnen, da für die Berechnung einer der geheimen Schlüssel bekannt sein muss.
3. Der Kernel verwendet den allgemeinen Schlüssel zum Entschlüsseln des Dialogschlüssels.
4. Der Kernel ruft den Schlüsselserver auf, um den Zeitstempel des Clients mit dem entschlüsselten Dialogschlüssel zu entschlüsseln.

Speichern der Informationen auf dem Server mit Secure RPC

Nachdem der Server den Zeitstempel des Clients entschlüsselt hat, speichert der Server vier Arten von Informationen in einer Berechtigungsnachweistabelle:

- Den Computernamen des Clients
- Den Dialogschlüssel
- Das Fenster
- Den Zeitstempel des Clients

Der Server speichert die ersten drei Elemente, um sie zu einem späteren Zeitpunkt zu verwenden. Der Server speichert den Zeitstempel des Clients, um Wiederholungen zu vermeiden. Der Server akzeptiert nur Zeitstempel, die chronologisch nach dem letzten angezeigten Zeitstempel liegen. Daher werden wiederholte Transaktionen auf jeden Fall zurückgewiesen.

Hinweis – Bei diesen Transaktionen ist außerdem implizit der Name des Aufrufers enthalten, der auf eine bestimmte Art authentifiziert werden muss. Der Schlüsselserver kann für die Authentifizierung des Aufrufers keine DES-Authentifizierung verwenden, da ansonsten eine gegenseitige Sperrung (Deadlock) entstehen würde. Um dies zu vermeiden, speichert der Schlüsselserver die geheimen Schlüssel nach Benutzer-ID (UID) und gewährt Anfragen nur den lokalen `root`-Prozessen.

Zurückgeben des Verifikators an den Client mit Secure RPC

Der Server gibt einen Verifikator an den Client zurück, der Folgendes enthält:

- Die Index-ID, die der Server im zugehörigen Berechtigungsnachweis-Cache aufzeichnet
- Den Zeitstempel des Clients abzüglich des Werts von 1, der durch den Dialogschlüssel verschlüsselt wird

Der Wert 1 wird deshalb vom Zeitstempel des Clients abgezogen, um sicherzustellen, dass der Zeitstempel veraltet ist. Ein veralteter Zeitstempel kann nicht erneut als Clientverifikator verwendet werden.

Authentifizieren des Servers mit Secure RPC

Der Client erhält den Verifikator und authentifiziert den Server. Der Client ist darüber informiert, dass nur der Server den Verifikator gesendet haben kann, da nur der Server darüber informiert ist, welchen Zeitstempel der Client gesendet hat.

Verarbeiten von Transaktionen mit Secure RPC

Bei jeder Transaktion nach der ersten Transaktion gibt der Client die Index-ID an den Server zurück. Der Client sendet ebenfalls einen anderen verschlüsselten Zeitstempel. Der Server sendet den Zeitstempel des Clients abzüglich des Werts von 1 zurück, der durch den Dialogschlüssel verschlüsselt wird.

Verwalten von Secure RPC (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf Verfahren zum Konfigurieren von Secure RPC für NIS, NIS+ und NFS.

Aufgabe	Beschreibung	Anweisungen
1. Starten des Schlüsselservers	Stellt sicher, dass Schlüssel für die Authentifizierung der Benutzer erstellt werden können	„So starten Sie den Schlüsselserver mit Secure RPC neu“ auf Seite 341

Aufgabe	Beschreibung	Anweisungen
2. Einrichten von Berechtigungsnachweisen auf einem NIS+-Host	Stellt sicher, dass der Benutzer `root` auf einem Host in einer NIS+-Umgebung authentifiziert werden kann	„So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS+-Host ein“ auf Seite 342
3. Übergeben eines Schlüssels an einen NIS+-Benutzer	Ermöglicht die Authentifizierung eines Benutzers in einer NIS+-Umgebung	„So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS+-Benutzer ein“ auf Seite 343
4. Einrichten von Berechtigungsnachweisen auf einem NIS-Host	Stellt sicher, dass der Benutzer `root` auf einem Host in einer NIS-Umgebung authentifiziert werden kann	„So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS-Host ein“ auf Seite 344
5. Übergeben eines Schlüssels an einen NIS-Benutzer	Ermöglicht die Authentifizierung eines Benutzers in einer NIS-Umgebung	„So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS-Benutzer ein“ auf Seite 344
6. Gemeinsame Nutzung von NFS-Dateien mit Authentifizierung	Ermöglicht, dass ein NFS-Server mithilfe von Authentifizierung gemeinsam genutzte Dateisysteme sicher schützen kann	„So können Sie NFS-Dateien mit Diffie-Hellman-Authentifizierung gemeinsam nutzen“ auf Seite 346

Verwalten von Authentifizierung mit Secure RPC (Aufgaben)

Indem Sie eine Authentifizierung für die Verwendung eingehängter NFS-Dateisysteme fordern, können Sie die Sicherheit im Netzwerk erhöhen.

▼ So starten Sie den Schlüsselserver mit Secure RPC neu

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Vergewissern Sie sich, dass der Dämon `keyserv` ausgeführt wird.

```
# svcs \*keyserv\*
STATE    STIME   FMRI
disabled Dec_14  svc:/network/rpc/keyserv
```

3 Aktivieren Sie den Schlüsselserver-Service, wenn der Service nicht online ist.

```
# svcadm enable network/rpc/keyserv
```

▼ So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS+-Host ein

Führen Sie dieses Verfahren auf jedem Host in der NIS+-Domain aus. Nachdem durch den `root` der Befehl `keylogin` ausgeführt wurde, verfügt der Server über GSS-API-Verarbeiter-Berechtigungsnachweise für `mech_dh` und der Client über GSS-API-Initiator-Berechtigungsnachweise.

Eine ausführliche Beschreibung der NIS+-Sicherheit erhalten Sie unter *System Administration Guide: Naming and Directory Services (NIS+)*.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Aktivieren Sie die Tabelle `publickey` im Naming Service.

Fügen Sie folgende Zeile zur Datei `/etc/nsswitch.conf` hinzu:

```
publickey: nisplus
```

3 Initialisieren Sie den NIS+-Client.

```
# nisinit -cH hostname
```

Ersetzen Sie *hostname* durch den Namen eines vertrauenswürdigen NIS+-Servers, der einen Eintrag in den zugehörigen Tabellen für das Clientsystem enthält.

4 Fügen Sie den Client zur Tabelle `cred` hinzu.

Geben Sie die folgenden Befehle ein:

```
# nisaddcred local
# nisaddcred des
```

5 Überprüfen Sie die Einrichtung, indem Sie den Befehl `keylogin` verwenden.

Wenn Sie zur Eingabe eines Passworts aufgefordert werden, wurde das Verfahren erfolgreich durchgeführt.

```
# keylogin
Password:
```

Beispiel 16–1 Einrichten eines neuen Schlüssels für `root` auf einem NIS+-Client

Im folgenden Beispiel wird der Host `pluto` für die Einrichtung von `earth` als ein NIS+-Client verwendet. Sie können die Warnungen ignorieren. Durch Akzeptieren des Befehls `keylogin` wird sichergestellt, dass `earth` als sicherer NIS+-Client ordnungsgemäß eingerichtet wurde.

```
# nisinit -cH pluto
NIS Server/Client setup utility.
This system is in the example.com. directory.
Setting up NIS+ client ...
All done.
# nisaddcred local
# nisaddcred des
DES principal name : unix.earth@example.com
Adding new key for unix.earth@example.com (earth.example.com.)
Network password:    <Type password>
Warning, password differs from login password.
Retype password:     <Retype password>
# keylogin
Password:            <Type password>
#
```

▼ So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS+-Benutzer ein

Führen Sie dieses Verfahren für jeden Benutzer in der NIS+-Domain aus.

1. **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

   Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Fügen Sie den Benutzer zur Tabelle `cred` auf dem Root-Master-Server hinzu.**

   Geben Sie folgenden Befehl ein:

   # nisaddcred -p unix.*UID@domain-name* **-P** *username.domain-name***. des**

   Beachten Sie, dass in diesem Fall *username.domain-name* auf einen Punkt (.) enden muss.

3. **Überprüfen Sie die Einrichtung, indem Sie sich als Client anmelden und den Befehl `keylogin` eingeben.**

Beispiel 16–2 Einrichten eines neuen Schlüssel für einen NIS+-Benutzer

Im folgenden Beispiel wird ein Schlüssel für die Diffie-Hellman-Authentifizierung an den Benutzer `jdoe` übergeben.

```
# nisaddcred -p unix.1234@example.com -P jdoe.example.com. des
DES principal name : unix.1234@example.com
Adding new key for unix.1234@example.com (jdoe.example.com.)
Password:            <Type password>
Retype password:     <Retype password>
```

```
# rlogin rootmaster -l jdoe
% keylogin
Password:           <Type password>
%
```

So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS-Host ein

Führen Sie dieses Verfahren auf jedem Host in der NIS-Domain aus.

1. **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

   Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Aktivieren Sie die Map `publickey` im Naming Service.**

   Fügen Sie folgende Zeile zur Datei `/etc/nsswitch.conf` hinzu:

   ```
   publickey: nis
   ```

3. **Erstellen Sie mit dem Befehl `newkey` ein neues Schlüsselpaar.**

   ```
   # newkey -h hostname
   ```

   Ersetzen Sie *hostname* durch den Namen des Clients.

Beispiel 16–3 Einrichten eines neuen Schlüssels für `root` auf einem NIS-Client

Im folgenden Beispiel wird `earth` als ein sicherer NIS-Client eingerichtet.

```
# newkey -h earth
Adding new key for unix.earth@example.com
New Password:       <Type password>
Retype password:    <Retype password>
Please wait for the database to get updated...
Your new key has been successfully stored away.
#
```

So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS-Benutzer ein

Führen Sie dieses Verfahren für jeden Benutzer in der NIS-Domain aus.

Bevor Sie beginnen Nur Systemadministratoren, die am NIS-Master-Server angemeldet sind, können einen neuen Schlüssel für einen Benutzer generieren.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Erstellen Sie einen neuen Schlüssel für einen Benutzer.

```
# newkey -u username
```

Ersetzen Sie *username* durch den Namen des Benutzers. Das System fordert Sie zur Eingabe eines Passworts auf. Sie können ein allgemeines Passwort eingeben. Der private Schlüssel wird in verschlüsselter Form durch ein allgemeines Passwort gespeichert.

3 Weisen Sie den Benutzer an, sich anzumelden und den Befehl `chkey -p` einzugeben.

Durch diesen Befehl können Benutzer ihre privaten Schlüssel durch ein nur dem Benutzer bekanntes Passwort erneut verschlüsseln.

Hinweis – Mit dem Befehl `chkey` kann ein neues Schlüsselpaar für einen Benutzer erstellt werden.

Beispiel 16–4 Einrichten und Verschlüsseln eines neuen Benutzerschlüssels in NIS

In diesem Beispiel richtet der Superuser den Schlüssel ein.

```
# newkey -u jdoe
Adding new key for unix.12345@example.com
New Password:       <Type password>
Retype password:    <Retype password>
Please wait for the database to get updated...
Your new key has been successfully stored away.
#
```

Anschließend verschlüsselt der Benutzer `jdoe` den Schlüssel mit einem privaten Passwort erneut.

```
% chkey -p
Updating nis publickey database.
Reencrypting key for unix.12345@example.com
Please enter the Secure-RPC password for jdoe:     <Type password>
Please enter the login password for jdoe:          <Type password>
Sending key change request to centralexample...
```

▼ So können Sie NFS-Dateien mit Diffie-Hellman-Authentifizierung gemeinsam nutzen

Durch dieses Verfahren werden gemeinsam genutzte Dateisysteme auf einem NFS-Server geschützt, indem eine Authentifizierung für den Zugriff benötigt wird.

Bevor Sie beginnen Die Diffie-Hellman-Authentifizierung mit öffentlichen Schlüsseln muss auf dem Netzwerk aktiviert sein. Führen Sie eines der folgenden Verfahren durch, um die Authentifizierung auf dem Netzwerk zu aktivieren:

- „So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS+-Host ein“ auf Seite 342
- „So richten Sie einen Diffie-Hellman-Schlüssel für einen NIS-Host ein“ auf Seite 344

1 Melden Sie sich als Superuser an oder nehmen Sie eine Rolle an, die das File System Management-Profil beinhaltet.

Beispielsweise beinhaltet die Rolle des Systemadministrators das File System Management-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2 Auf dem NFS-Server können Sie ein Dateisystem mit der Diffie-Hellman-Authentifizierung gemeinsam nutzen.

```
# share -F nfs -o sec=dh /filesystem
```

Ersetzen Sie *filesystem* durch das Dateisystem, das gemeinsam genutzt werden soll.

Die Option `-o sec=dh` bedeutet, dass die Authentifizierung `AUTH_DH` für den Zugriff auf das Dateisystem erforderlich ist.

3 Auf einem NFS-Client können Sie ein Dateisystem mit der Diffie-Hellman-Authentifizierung einhängen.

```
# mount -F nfs -o sec=dh server:filesystem mount-point
```

server	Entspricht dem Namen des Systems, auf dem *filesystem* gemeinsam genutzt wird
filesystem	Entspricht dem Namen des Dateisystems, das gemeinsam genutzt wird, beispielsweise `opt`
mount-point	Entspricht dem Namen des Einhängepunkts, beispielsweise `/opt`

Durch die Option `-o sec=dh` wird das Dateisystem mit der Authentifizierung `AUTH_DH` eingehängt.

◆ ◆ ◆ KAPITEL 17

Verwenden von PAM

In diesem Kapitel wird das PAM-Framework (Pluggable Authentication Module) behandelt. PAM stellt eine Methode zur Verfügung, mit der Authentifizierungsservices in Oracle Solaris-Betriebssystem integriert werden können. PAM bietet Unterstützung für mehrere Authentifizierungsservices beim Zugriff auf ein System.

- „PAM (Übersicht)“ auf Seite 347
- „PAM (Aufgaben)“ auf Seite 350
- „PAM-Konfiguration (Referenz)“ auf Seite 353

PAM (Übersicht)

Mit dem PAM-Framework (Pluggable Authentication Module) können Sie neue Authentifizierungsservices integrieren, ohne Systemzugangsservices wie `login`, `ftp` und `telnet` zu ändern. Sie können PAM auch verwenden, um die UNIX-Anmeldung mit anderen Sicherheitsmechanismen, z. B. Kerberos, zu integrieren. Mechanismen für Konto-, Berechtigungsnachweis-, Sitzungs- und Passwortverwaltung können ebenfalls mithilfe dieses Frameworks integriert werden.

Vorteile der Verwendung von PAM

Das PAM-Framework ermöglicht Ihnen das Konfigurieren der Verwendung von Systemzugangsservices (z. B. `ftp`, `login`, `telnet` oder `rsh`) zur Benutzerauthentifizierung. Im Folgenden finden Sie einige der Vorteile von PAM:

- Flexible Konfigurationsrichtlinie
  - Authentifizierungsrichtlinie pro Anwendung
  - Die Möglichkeit zur Auswahl eines Standardauthentifizierungsmechanismus
  - Die Möglichkeit zum Anfordern mehrerer Autorisierungen für Hochsicherheitssysteme
- Einfache Verwendung für den Endbenutzer

  - Keine erneute Passworteingabe, wenn die Passwörter für verschiedene Authentifizierungsservices gleich sind
  - Die Möglichkeit, Passwörter für mehrere Authentifizierungsservices vom Benutzer anzufordern, ohne dass der Benutzer mehrere Befehle eingeben muss
- Die Möglichkeit, auswählbare Optionen an die Benutzerauthentifizierungsservices weiterzuleiten
- Die Möglichkeit, eine standortspezifische Sicherheitsrichtlinie zu implementieren, ohne die Systemzugangsservices ändern zu müssen

Einführung zum PAM-Framework

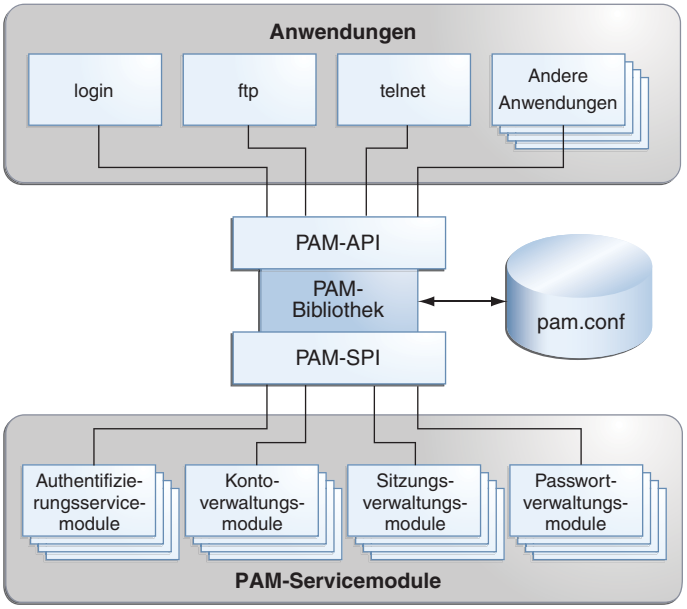
Das PAM-Framework besteht aus vier Teilen:

- PAM-Verbraucher
- PAM-Bibliothek
- Konfigurationsdatei `pam.conf(4)`
- PAM-Servicemodule, auch als Provider bezeichnet

Das Framework stellt eine einheitliche Methode für die Ausführung authentifizierungsbezogener Aktivitäten zur Verfügung. Dieser Ansatz ermöglicht Anwendungsentwicklern die Verwendung von PAM-Services, ohne die Semantik der Richtlinie kennen zu müssen. Algorithmen werden zentral zur Verfügung gestellt. Die Algorithmen können unabhängig von den individuellen Applikationen geändert werden. Mit PAM können Administratoren den Authentifizierungsprozess auf die Anforderungen eines bestimmten Systems abstimmen, ohne Anwendungen ändern zu müssen. Anpassungen werden über die PAM-Konfigurationsdatei `pam.conf` vorgenommen.

Die folgende Abbildung zeigt die PAM-Architektur. Anwendungen kommunizieren mit der PAM-Bibliothek über die Anwendungsprogrammierschnittstelle (Application Programming Interface, API) des PAM. PAM-Module kommunizieren mit der PAM-Bibliothek über die SPI (Service Provider Interface) des PAM. Auf diese Weise ermöglicht die PAM-Bibliothek die Kommunikation zwischen Anwendungen und Modulen.

ABBILDUNG 17–1 PAM-Architektur



Änderungen am PAM in der Version Solaris 10

Die Version Solaris 10 umfasst die folgenden Änderungen am PAM-Framework:

- Das Modul `pam_authtok_check` ermöglicht nun strikte Passwortüberprüfungen mithilfe neuer, abstimmbarer Parameter in der Datei `/etc/default/passwd`. Die neuen Parameter legen Folgendes fest:
  - Eine Liste durch Kommata getrennter Wörterbuchdateien, die zur Überprüfung von Passwörtern anhand normaler Wörterbucheinträge verwendet werden
  - Die mindestens erforderlichen Unterschiede zwischen einem alten und einem neuen Passwort
  - Die für ein neues Passwort erforderliche Mindestanzahl alphabetischer oder nicht alphabetischer Zeichen
  - Die für ein neues Passwort erforderliche Mindestanzahl an Groß- oder Kleinbuchstaben
  - Die zulässige Anzahl aufeinander folgender gleicher Zeichen
- Das Modul `pam_unix_auth` implementiert die Kontosperre für lokale Benutzer. Die Kontosperre wird durch den Parameter `LOCK_AFTER_RETRIES` in `/etc/security/policy.conf` und den Schlüssel `lock_after-retries` in `/etc/user_attr` aktiviert. Weitere Informationen erhalten Sie auf den Manpages `policy.conf(4)` und `user_attr(4)`.

- Das neue Steuer-Flag `binding` wurde definiert. Dieses Steuer-Flag ist auf der Manpage `pam.conf(4)` und in „Funktionsweise von PAM-Stacking“ auf Seite 354 dokumentiert.
- Das Modul `pam_unix` wurde entfernt und durch verschiedene Servicemodule mit einem gleichwertigen oder größeren Funktionsumfang ersetzt. Viele dieser Module wurden in der Version Solaris 9 eingeführt. Im Folgenden wird eine Liste der Ersatzmodule aufgeführt:
  - `pam_authtok_check`
  - `pam_authtok_get`
  - `pam_authtok_store`
  - `pam_dhkeys`
  - `pam_passwd_auth`
  - `pam_unix_account`
  - `pam_unix_auth`
  - `pam_unix_cred`
  - `pam_unix_session`
- Der Funktionsumfang des Moduls `pam_unix_auth` wurde auf zwei Module aufgeteilt. Das Modul `pam_unix_auth` überprüft jetzt die Richtigkeit des eingegebenen Passworts für den jeweiligen Benutzer. Das neue Modul `pam_unix_cred` bietet Funktionen zum Einrichten von Berechtigungsinformationen für Benutzer.
- Neue Erweiterungen des Moduls `pam_krb5` verwalten den Cache für Kerberos-Berechtigungsnachweise. Dabei stützen sie sich auf das PAM-Framework.
- Es wurde ein neues `pam_deny`-Modul hinzugefügt. Das Modul kann zur Verweigerung des Zugriffs auf Services verwendet werden. Das Modul `pam_deny` wird standardmäßig nicht eingesetzt. Weitere Informationen finden Sie auf der Manpage `pam_deny(5)`.

PAM (Aufgaben)

In diesem Abschnitt werden einige Aufgaben beschrieben, die erforderlich sein können, um die Verwendung einer bestimmten Sicherheitsrichtlinie durch das PAM-Framework zu veranlassen. Beachten Sie die Sicherheitsprobleme, die mit der PAM-Konfigurationsdatei in Verbindung stehen. Weitere Informationen zu Sicherheitsproblemen finden Sie unter „Planen Ihrer PAM-Implementierung“ auf Seite 351.

PAM (Übersicht der Schritte)

Aufgabe	Beschreibung	Anweisungen
Planen Ihrer PAM-Installation	Prüfen Sie vor Beginn des Softwarekonfigurationsprozesses Konfigurationsprobleme und treffen Sie entsprechende Entscheidungen.	„Planen Ihrer PAM-Implementierung“ auf Seite 351

Aufgabe	Beschreibung	Anweisungen
Hinzufügen neuer PAM-Module	Manchmal müssen standortspezifische Module geschrieben und installiert werden, um Anforderungen zu erfüllen, die nicht Teil der generischen Software sind. In diesem Verfahren wird erklärt, wie diese neuen PAM-Module installiert werden.	„So fügen Sie ein PAM-Modul hinzu“ auf Seite 352
Blockieren des Zugriffs über `~/.rhosts`	Erhöhen Sie die Sicherheit, indem Sie den Zugriff über `~/.rhosts` verhindern.	„So verhindern Sie mit PAM den Zugriff von Remote-Systemen im Rhost-Stil“ auf Seite 353
Initiieren der Fehlerprotokollierung	Starten Sie die Protokollierung von PAM-Fehlermeldungen mithilfe von `syslog`.	„So protokollieren Sie PAM-Fehlerberichte“ auf Seite 353

Planen Ihrer PAM-Implementierung

Im Lieferzustand implementiert die Konfigurationsdatei `pam.conf` die Standardsicherheitsrichtlinie. Diese Richtlinie ist normalerweise für viele verschiedene Situationen geeignet. Wenn Sie eine andere Sicherheitsrichtlinie implementieren möchten, sollten Sie folgende Punkte besonders beachten:

- Legen Sie fest, welche Anforderungen Sie haben, insbesondere, welche PAM-Servicemodule Sie wählen sollten.
- Identifizieren Sie die Services, die spezielle Konfigurationsoptionen erfordern. Verwenden Sie gegebenenfalls `other`.
- Bestimmen Sie die Reihenfolge, in der die Module ausgeführt werden sollten.
- Wählen Sie das Steuer-Flag für jedes Modul. Weitere Informationen zu allen Steuer-Flags finden Sie unter „Funktionsweise von PAM-Stacking“ auf Seite 354.
- Wählen Sie alle erforderlichen Optionen für jedes Modul. Auf der Manpage für jedes Modul sollten alle speziellen Optionen aufgeführt werden.

Im Folgenden werden einige Vorschläge gemacht, die Sie vor dem Ändern der PAM-Konfigurationsdatei beachten sollten:

- Verwenden Sie `other`-Einträge für jeden Modultyp, sodass nicht jede Anwendung in `/etc/pam.conf` erfasst werden muss.
- Berücksichtigen Sie die Sicherheitsimplikationen der Steuer-Flags `binding`, `sufficient` und `optional`.
- Sehen Sie sich die Manpages zu den Modulen an. Auf diesen Manpages wird erläutert, wie die einzelnen Module funktionieren, welche Optionen verfügbar sind sowie welche Interaktionen zwischen gestapelten Modulen stattfinden.

Achtung – Wenn die PAM-Konfigurationsdatei falsch konfiguriert oder fehlerhaft ist, kann sich möglicherweise kein Benutzer mehr anmelden. Da der Befehl `sulogin` PAM nicht verwendet, ist dann das Root-Passwort erforderlich, um den Rechner im Einzelbenutzermodus zu starten und das Problem zu beheben.

Überprüfen Sie die Datei `/etc/pam.conf` nach dem Ändern so umfassend wie möglich, solange Sie noch Zugriff auf das System haben und Probleme beheben können. Testen Sie alle Befehle, die von Ihren Änderungen betroffen sein können. Ein Beispiel ist das Hinzufügen eines neuen Moduls zum Service `telnet`. In diesem Beispiel geben Sie den Befehl `telnet` ein und überprüfen, ob Ihre Änderungen zu dem gewünschten Verhalten des Service führen.

▼ So fügen Sie ein PAM-Modul hinzu

Dieses Verfahren zeigt, wie Sie ein neues PAM-Modul hinzufügen. Neue Module können erstellt werden, um standortspezifische Sicherheitsrichtlinien abzudecken oder Anwendungen Dritter zu unterstützen.

1. **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2. **Legen Sie fest, welche Steuer-Flags und anderen Optionen zu verwenden sind.**

   Informationen zu Steuer-Flags erhalten Sie unter „Funktionsweise von PAM-Stacking“ auf Seite 354.

3. **Stellen Sie sicher, dass `root` der Eigentümer der Moduldatei ist und die Berechtigungen `555` sind.**

4. **Bearbeiten Sie die PAM-Konfigurationsdatei `/etc/pam.conf` und fügen Sie dieses Modul den entsprechenden Services hinzu.**

5. **Überprüfen Sie, ob das Modul korrekt hinzugefügt wurde.**

   Testen Sie dies für den Fall, dass die Konfigurationsdatei falsch konfiguriert ist, *vor* dem Neustart des Systems. Melden Sie sich mithilfe eines direkten Service wie `ssh` an und führen Sie vor dem Neustart des Systems den Befehl `su` aus. Der Service ist möglicherweise ein Dämon, der nur einmal beim Systemstart ausgeführt wird. Sie müssen das System dann neu starten, bevor Sie überprüfen können, ob das Modul hinzugefügt wurde.

▼ So verhindern Sie mit PAM den Zugriff von Remote-Systemen im Rhost-Stil

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2 **Entfernen Sie alle Zeilen, die `rhosts_auth.so.1` enthalten, aus der PAM-Konfigurationsdatei.**

Dieser Schritt verhindert, dass die `~/.rhosts`-Dateien während einer `rlogin`-Sitzung gelesen werden. So wird nicht authentifizierter Zugriff von Remote-Systemen auf das lokale System verhindert. Jeglicher `rlogin`-Zugriff erfordert unabhängig von Vorhandensein und Inhalt von `~/.rhosts`- oder `/etc/hosts.equiv` -Dateien ein Passwort.

3 **Deaktivieren Sie den Service `rsh`.**

Um weiteren nicht authentifizierten Zugriff auf die `~/.rhosts`-Dateien zu verhindern, deaktivieren Sie den Service `rsh`.

```
# svcadm disable network/shell
```

▼ So protokollieren Sie PAM-Fehlerberichte

1 **Melden Sie sich als Superuser an oder nehmen Sie eine entsprechende Rolle an.**

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2 **Konfigurieren Sie die Datei `/etc/syslog.conf` für die Protokollierungsstufe, die Sie benötigen.**

Weitere Informationen zu Protokollierungsstufen finden Sie unter `syslog.conf(4)`.

3 **Aktualisieren Sie die Konfigurationsinformationen für den Dämon `syslog`.**

```
# svcadm refresh system/system-log
```

PAM-Konfiguration (Referenz)

Die PAM-Konfigurationsdatei `pam.conf(4)` wird verwendet, um PAM-Servicemodule für Systemservices wie `login`, `rlogin`, `su` und `cron` zu konfigurieren. Diese Datei wird vom Systemadministrator verwaltet. Eine falsche Reihenfolge der Einträge in `pam.conf` kann unvorhersehbare Nebeneffekte haben. Durch falsche Konfiguration von `pam.conf` können z. B. Benutzer blockiert werden, sodass der Einzelbenutzermodus zur Reparatur erforderlich ist. Eine Beschreibung für die Festlegung der Reihenfolge finden Sie unter „Funktionsweise von PAM-Stacking“ auf Seite 354.

PAM-Konfigurationsdateisyntax

Die Einträge in der Konfigurationsdatei haben das folgende Format:

service-name module-type control-flag module-path module-options

service-name Name des Service, z. B. `ftp`, `login` oder `passwd`. Eine Anwendung kann verschiedene Namen für die Services verwenden, die sie bereitstellt. Der Secure Shell-Dämon Oracle Solaris verwendet die folgenden Servicenamen: `sshd-none`, `sshd-password`, `sshd-kbdint`, `sshd-pubkey` und `sshd-hostbased` . Der Servicename *other* ist ein vordefinierter Name, der als Platzhalter-Servicename verwendet wird. Wenn ein bestimmter Servicename in der Konfigurationsdatei nicht gefunden wird, wird die Konfiguration für *other* verwendet.

module-type Der Servicetyp, d. h. `auth`, `account`, `session` oder `password`.

control-flag Gibt die Rolle des Moduls durch Bestimmen des integrierten Erfolgs- oder Fehlerwerts für den Service an. Gültige Steuer-Flags sind `binding`, `include`, `optional`, `required`, `requisite` und `sufficient`. Informationen zur Verwendung dieser Flags erhalten Sie unter „Funktionsweise von PAM-Stacking“ auf Seite 354.

module-path Der Pfad zu dem Bibliotheksobjekt, das der Service implementiert. Wenn der Pfadname nicht absolut ist, wird angenommen, dass der Pfadname relativ zu `/usr/lib/security/$ISA/` ist. Verwenden Sie das architekturabhängige Makro $ISA, um zu veranlassen, dass `libpam` im Verzeichnis nach der spezifischen Architektur der Anwendung sucht.

module-options Optionen, die an die Servicemodule weitergegeben werden. Auf der Manpage eines Moduls werden die Optionen beschrieben, die von diesem Modul akzeptiert werden. Zu den typischen Moduloptionen gehören `nowarn` und `debug`.

Funktionsweise von PAM-Stacking

Wenn eine Anwendung die folgenden Funktionen aufruft, liest `libpam` die Konfigurationsdatei `/etc/pam.conf`, um zu bestimmen, welche Module an der Ausführung dieses Service beteiligt sind:

- `pam_authenticate`(3PAM)
- `pam_acct_mgmt`(3PAM)
- `pam_setcred`(3PAM)
- `pam_open_session`(3PAM)
- `pam_close_session`(3PAM)
- `pam_chauthtok`(3PAM)

Wenn `/etc/pam.conf` nur ein Modul für die Ausführung dieses Service enthält, z. B. Authentifizierung oder Kontoverwaltung, bestimmt das Ergebnis dieses Moduls den Ausgang der Ausführung. Die Standardauthentifizierungsoperation für die Anwendung `passwd` enthält z. B. ein Modul, `pam_passwd_auth.so.1` :

```
passwd  auth required           pam_passwd_auth.so.1
```

Falls jedoch mehrere Module für die Ausführung des Service festgelegt sind, werden diese Module als *gestapelt* angesehen und davon ausgegangen, dass ein *PAM-Stack* für diesen Service vorhanden ist. Betrachten Sie z. B. den Fall, in dem `pam.conf` die folgenden Einträge enthält:

```
login   auth requisite          pam_authtok_get.so.1
login   auth required           pam_dhkeys.so.1
login   auth required           pam_unix_cred.so.1
login   auth required           pam_unix_auth.so.1
login   auth required           pam_dial_auth.so.1
```

Diese Einträge stellen ein Beispiel für den `auth`-Stack des `login`-Service dar. Um das Ergebnis dieses Stacks zu bestimmen, erfordern die Ergebniscodes der individuellen Module einen *Integrationsprozess*. In diesem Integrationsprozess werden die Module der Reihe nach wie in `/etc/pam.conf` angegeben ausgeführt. Jeder Erfolgs- oder Fehlercode wird abhängig vom Steuer-Flag des Moduls in das Gesamtergebnis integriert. Das Steuer-Flag kann zur vorzeitigen Beendigung des Stacks führen. Ein `requisite`-Modul kann beispielsweise fehlschlagen, und ein `sufficient`- oder `binding`-Modul erfolgreich ausgeführt werden. Wenn der Stack verarbeitet wurde, werden die einzelnen Ergebnisse in einem einzigen Gesamtergebnis zusammengefasst, das an die Anwendung geliefert wird.

Ein Steuer-Flag gibt die Rolle an, die ein PAM-Modul beim Festlegen des Zugriffs auf den Service spielt. Im Folgenden werden die Steuer-Flags und ihre jeweiligen Effekte aufgelistet:

- **binding** (Bindung): Wenn die Anforderungen eines Bindungsmoduls erfolgreich erfüllt wurden, wird der Erfolg direkt an die Anwendung zurückgegeben, falls keine zuvor erforderlichen Module fehlgeschlagen sind. Bei Erfüllung dieser Bedingungen werden keine weiteren Module ausgeführt. Bei Fehlschlagen wird ein optionaler Fehler aufgezeichnet und die Verarbeitung der Module fortgesetzt.
- **include** (einschließen): Fügt Zeilen aus einer separaten PAM-Konfigurationsdatei zur Verwendung an diesem Punkt im PAM-Stack hinzu. Dieses Flag kontrolliert nicht das Erfolgs- oder Fehlerverhalten. Wenn eine neue Datei gelesen wird, wird der PAM-Einschließungs-Stack um 1 erhöht. Wenn die Stack-Prüfung in der neuen Datei beendet ist, wird der Einschließungs-Stack-Wert um 1 verringert. Wenn das Ende der Datei erreicht wird und der PAM-Einschließungs-Stack 0 beträgt, wird die Stack-Verarbeitung beendet. Der Höchstwert für den PAM-Einschließungs-Stack beträgt 32.
- **optional**: Das erfolgreiche Erfüllen der Anforderungen eines optionalen Moduls ist für die Verwendung des Service nicht erforderlich. Bei Fehlschlagen wird ein optionaler Fehler aufgezeichnet.

- **required** (erforderlich): Das erfolgreiche Erfüllen der Anforderungen eines erforderlichen Moduls ist für die Verwendung des Service erforderlich. Bei Fehlschlagen wird ein Fehler zurückgegeben, nachdem die verbleibenden Module für diesen Service ausgeführt wurden. Abschließender Erfolg für den Service wird nur zurückgegeben, wenn keine bindenden oder erforderlichen Module Fehler gemeldet haben.
- **requisite** (obligatorisch): Das erfolgreiche Erfüllen der Anforderungen eines obligatorischen Moduls ist für die Verwendung des Service erforderlich. Fehlschlagen führt zu einer sofortigen Fehlerrückgabe ohne weitere Ausführung von Modulen. Alle obligatorischen Module für einen Service müssen einen Erfolg zurückgeben, damit die Funktion einen Erfolg an die Anwendung zurückgeben kann.
- **sufficient** (ausreichend): Wenn zuvor keine Fehler für erforderliche Module aufgetreten sind, wird ein Erfolg in einem ausreichenden Modul sofort an die Anwendung zurückgegeben, ohne dass weitere Module ausgeführt werden. Bei Fehlschlagen wird ein optionaler Fehler aufgezeichnet.

Die folgenden beiden Diagramme zeigen, wie Zugriff während des Integrationsprozesses festgelegt wird. Das erste Diagramm zeigt, wie Erfolg oder Fehlschlagen für die einzelnen Arten von Steuer-Flags aufgezeichnet werden. Das zweite Diagramm zeigt, wie der integrierte Wert festgelegt wird.

ABBILDUNG 17–2 PAM-Stacking: Auswirkungen von Steuer-Flags

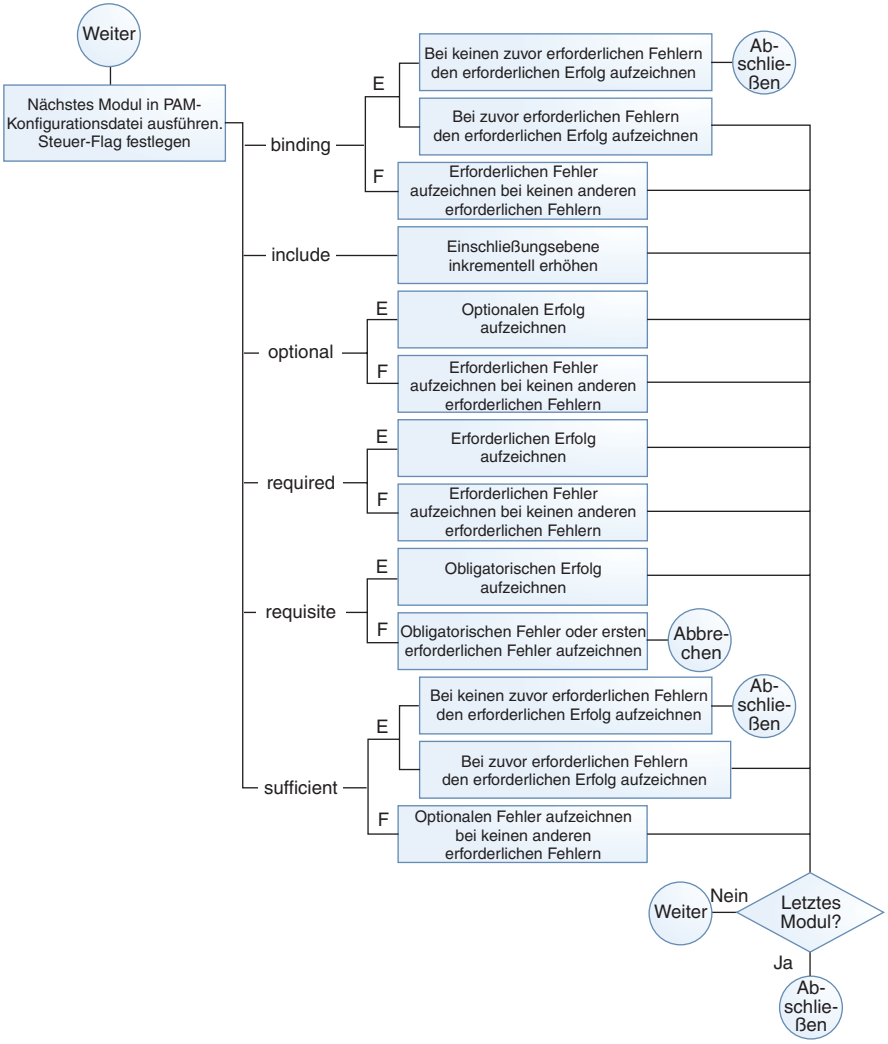
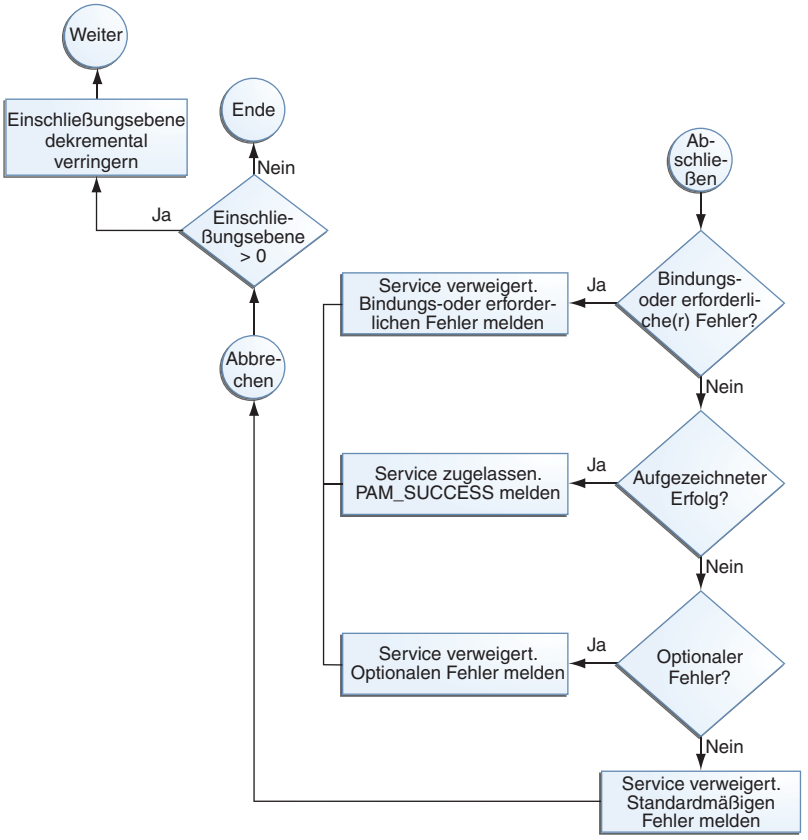


ABBILDUNG 17–3 PAM-Stacking: Vorgehensweise zum Bestimmen integrierter Werte



Beispiel für PAM-Stacking

Berücksichtigen Sie das folgende Beispiel für einen `rlogin`-Service, der Authentifizierung erfordert.

BEISPIEL 17–1 Teilinhalte einer typischen PAM-Konfigurationsdatei

Die Datei `pam.conf` in diesem Beispiel enthält Folgendes für `rlogin`-Services:

```
# Authentication management
...
# rlogin service
rlogin  auth sufficient         pam_rhosts_auth.so.1
rlogin  auth requisite          pam_authtok_get.so.1
rlogin  auth required           pam_dhkeys.so.1
rlogin  auth required           pam_unix_auth.so.1
...
```

BEISPIEL 17–1 Teilinhalte einer typischen PAM-Konfigurationsdatei *(Fortsetzung)*

Wenn der Service `rlogin` eine Authentifizierung erfordert, führt `libpam` zuerst das Modul `pam_rhosts_auth(5)` aus. Das Steuer-Flag wird für das Modul `pam_rhosts_auth` auf `sufficient` gesetzt. Wenn das Modul `pam_rhosts_auth` den Benutzer authentifizieren kann, wird die Verarbeitung angehalten und Erfolg an die Anwendung zurückgegeben.

Wenn das Modul `pam_rhosts_auth` den Benutzer nicht authentifizieren kann, wird das nächste PAM-Modul, `pam_authtok_get(5)`, ausgeführt. Das Steuer-Flag für dieses Modul wird auf `requisite` gesetzt. Wenn `pam_authtok_get` fehlschlägt, wird der Authentifizierungsprozess beendet und der Fehler an `rlogin` zurückgegeben.

Wenn `pam_authtok_get` Erfolg hat, werden die beiden nächsten Module, `pam_dhkeys(5)` und `pam_unix_auth(5)`, ausgeführt. Beide Module haben zugeordnete Steuer-Flags, die auf `required` gesetzt sind, sodass der Prozess unabhängig von der Rückgabe eines einzelnen Fehlers weiter ausgeführt wird. Nach der Ausführung von `pam_unix_auth` verbleiben keine Module für die Authentifizierung von `rlogin`. Wenn entweder `pam_dhkeys` oder `pam_unix_auth` einen Fehler zurückgegeben haben, wird dem Benutzer an dieser Stelle der Zugriff über `rlogin` verweigert.

◆ ◆ ◆ KAPITEL 18

18 Verwenden von SASL

Dieses Kapitel enthält Information zu SASL (Simple Authentication and Security Layer).

- „SASL (Übersicht)“ auf Seite 361
- „SASL (Referenz)“ auf Seite 362

SASL (Übersicht)

Simple Authentication and Security Layer (SASL) ist ein Framework, das von Netzwerkprotokollen zur Authentifizierung verwendet wird und optionale Sicherheitsservices bietet. Eine Anwendung ruft die SASL-Bibliothek (`/usr/lib/libsasl.so`) auf, die eine Glue-Schicht zwischen der Anwendung und den verschiedenen SASL-Mechanismen zur Verfügung stellt. Die Mechanismen werden im Authentifizierungsprozess und bei der Bereitstellung optionaler Sicherheitsservices verwendet. Die Version von SASL leitet sich von Cyrus SASL ab, wobei einige Änderungen implementiert wurden.

SASL stellt die folgenden Services bereit:

- Laden beliebiger Plugins
- Bestimmen der erforderlichen Sicherheitsoptionen aus der Anwendung, um die Auswahl eines Sicherheitsmechanismus zu erleichtern
- Auflisten von Plugins, die für die Anwendung zur Verfügung stehen
- Auswählen des für einen bestimmten Authentifizierungsversuch am besten geeigneten Mechanismus aus einer Liste verfügbarer Mechanismen
- Weiterleiten der Authentifizierungsdaten zwischen der Anwendung und dem ausgewählten Mechanismus
- Bereitstellen von Informationen zur SASL-Aushandlung zurück zur Anwendung

SASL (Referenz)

Der folgende Abschnitt enthält Informationen zur Implementierung von SASL.

SASL-Plugins

SASL-Plugins bieten Unterstützung für Sicherheitsmechanismen, die Standardisierung von Benutzern und das Abrufen von Hilfseigenschaften. Standardmäßig werden die dynamisch geladenen 32-Bit-Plugins in `/usr/lib/sasl` und die 64-Bit-Plugins in `/usr/lib/sasl/` *$ISA* installiert. Folgende Plugins für Sicherheitsmechanismen stehen zur Verfügung:

`crammd5.so.1`	CRAM-MD5: unterstützt Authentifizierung, aber keine Autorisierung
`digestmd5.so.1`	DIGEST-MD5: unterstützt Authentifizierung, Integrität, Vertraulichkeit sowie Autorisierung
`gssapi.so.1`	GSSAPI: unterstützt Authentifizierung, Integrität, Vertraulichkeit sowie Autorisierung. Die GSSAPI-Sicherheitsmechanismen erfordern eine funktionierende Kerberos-Infrastruktur.
`plain.so.1`	PLAIN: unterstützt Authentifizierung und Autorisierung

Das Sicherheitsmechanismus-Plugin EXTERNAL und das Benutzerstandardisierungs-Plugin INTERNAL sind außerdem in `libsasl.so.1` integriert. Der EXTERNAL-Mechanismus unterstützt Authentifizierung und Autorisierung. Die Mechanismen unterstützen Integrität und Vertraulichkeit, sofern von der externen Sicherheitsquelle bereitgestellt. Das INTERNAL-Plugin fügt den Bereichsnamen bei Bedarf dem Benutzernamen hinzu.

Die Oracle Solaris-Version stellt derzeit keine `auxprop`-Plugins bereit. Damit die CRAM-MD5- und DIGEST-MD5-Mechanismus-Plugins serverseitig voll funktionsfähig sind, muss der Benutzer ein `auxprop`-Plugin zum Abrufen von Klartextpasswörtern angeben. Das PLAIN-Plugin erfordert zusätzliche Unterstützung zum Überprüfen des Passworts. Die Passwortüberprüfung kann durch Folgendes unterstützt werden: ein Callback zur Serveranwendung, ein `auxprop`-Plugin, `saslauthd` oder `pwcheck`. Die Dämonen`salauthd` und `pwcheck` stehen in den Oracle Solaris-Versionen nicht zur Verfügung. Beschränken Sie der besseren Interoperabilität halber die Serveranwendungen mit der SASL-Option `mech_list` auf die voll funktionsfähigen Mechanismen.

SASL-Umgebungsvariable

Standardmäßig ist der Client-Authentifizierungsname auf `getenv("LOGNAME")` eingestellt. Diese Variable kann vom Client oder vom Plugin zurückgesetzt werden.

SASL-Optionen

Das Verhalten von `libsasl` und den Plugins lässt sich mithilfe von Optionen, die in der Datei `/etc/sasl/`*app*`.conf` festgelegt werden können, serverseitig ändern. Die Variable *app* ist der vom Server definierte Name für die Anwendung. Der Anwendungsname sollte in der Dokumentation für die *app* des Servers angegeben sein.

Die folgenden Optionen werden unterstützt:

`auto_transition`	Automatischer Übergang des Benutzers zu anderen Mechanismen, wenn dieser eine erfolgreiche Nur-Text-Authentifizierung durchführt
`auxprop_login`	Listet den Namen der zu verwendenden Plugins für Hilfseigenschaften auf
`canon_user_plugin`	Wählt das Plugin canon_user für die Verwendung aus
`mech_list`	Listet die Mechanismen auf, die von der Serveranwendung verwendet werden dürfen
`pwcheck_method`	Listet die Mechanismen auf, die zum Überprüfen von Passwörtern verwendet werden. Derzeit ist `auxprop` der einzige zugelassene Wert.
`reauth_timeout`	Legt die Dauer (in Minuten) fest, während der Authentifizierungsinformationen für eine schnelle Neuauthentifizierung im Cache gespeichert werden. Diese Option wird vom DIGEST-MD5-Plugin verwendet. Durch Einstellen dieser Option auf 0 wird die Neuauthentifizierung deaktiviert.

Die folgenden Optionen werden nicht unterstützt:

`plugin_list`	Listet verfügbare Mechanismen auf. Wird nicht verwendet, da die Option das Verhalten des dynamischen Ladens von Plugins ändert.
`saslauthd_path`	Definiert den Speicherort von saslauthd-Door (Verweis), der für die Kommunikation mit dem Dämon `saslauthd` verwendet wird. Der Dämon `saslauthd` ist nicht in der Oracle Solaris-Version enthalten. Demzufolge ist auch die Option nicht verfügbar.
`keytab`	Definiert den Speicherort der vom GSSAPI-Plugin verwendeten Datei `keytab`. Verwenden Sie stattdessen die Umgebungsvariable `KRB5_KTNAME`, um den standardmäßigen `keytab`-Speicherort festzulegen.

Die nachfolgenden Optionen sind nicht in Cyrus SASL enthalten. Sie wurden jedoch für die Oracle Solaris-Version hinzugefügt:

`use_authid`	Ruft die Berechtigungsnachweise des Clients ab anstatt die Standardberechtigungsnachweise zum Erstellen des Sicherheitskontexts für den GSS-Client zu verwenden. Standardmäßig wird die Kerberos-Identität des Standardclients verwendet.
`log_level`	Legt die gewünschte Protokollierungsstufe für einen Server fest

◆ ◆ ◆ KAPITEL 19

Verwenden von Oracle Solaris Secure Shell (Aufgaben)

Die Secure Shell-Funktion ermöglicht einen sicheren Zugriff auf einen Remote-Host über ein ungesichertes Netzwerk. Die Shell bietet Befehle für Remote-Anmeldung und Remote-Dateiübertragung. Dieses Kapitel umfasst die folgenden Themen.

- „Oracle Solaris Secure Shell (Übersicht)“ auf Seite 365
- „Oracle Solaris Secure Shell und das OpenSSH-Projekt“ auf Seite 368
- „Konfigurieren von Oracle Solaris Secure Shell (Übersicht der Schritte)“ auf Seite 370
- „Verwenden von Oracle Solaris Secure Shell (Übersicht der Schritte)“ auf Seite 375

Referenzinformationen finden Sie in Kapitel 20, „Oracle Solaris Secure Shell (Referenz)“. Informationen zur Verbindung zwischen Oracle Solaris Secure Shell und dem OpenSSH-Projekt finden Sie unter „Oracle Solaris Secure Shell und das OpenSSH-Projekt“ auf Seite 368.

Oracle Solaris Secure Shell (Übersicht)

Bei der Secure Shell-Funktion erfolgt die Authentifizierung mithilfe von Passwörtern, öffentlichen Schlüsseln oder beidem. Der gesamte Netzwerkverkehr wird verschlüsselt. So verhindert Secure Shell, dass potenzielle Eindringlinge eine abgefangene Mitteilung lesen. Secure Shell verhindert auch Spoofing.

Secure Shell kann außerdem bedarfsgesteuert als Virtuelles privates Netzwerk (VPN) verwendet werden. Ein VPN kann X Window-Systemverkehr weiterleiten oder einzelne Portnummern zwischen lokalen und Remote-Rechnern über verschlüsselte Netzwerklinks verbinden.

Mit Secure Shell können Sie Folgendes ausführen:

- Sicheres Anmelden bei einem anderen Host über ein ungesichertes Netzwerk
- Sicheres Übertragen kopierter Dateien zwischen zwei Hosts
- Sicheres Ausführen von Befehlen auf dem Remote-Host

Secure Shell unterstützt zwei Versionen des Secure Shell-Protokolls. Version 1 ist die ursprüngliche Version des Protokolls. Version 2 bietet mehr Sicherheit und behebt einige grundlegende Entwurfsfehler von Version 1. Version 1 wird nur bereitgestellt, um Benutzern bei der Migration auf Version 2 zu helfen. Benutzern wird abgeraten, Version 1 zu verwenden.

Hinweis – Im Folgenden wird v1 für Version 1 und v2 für Version 2 verwendet.

Oracle Solaris Secure Shell-Authentifizierung

Secure Shell ermöglicht die Authentifizierung der Verbindung zum Remote-Host mithilfe von öffentlichen Schlüsseln und Passwörtern. Die Authentifizierung mithilfe von öffentlichen Schlüsseln ist ein stärkerer Authentifizierungsmechanismus als die Passwortauthentifizierung, da private Schlüssel nie über das Netzwerk versendet werden.

Die Authentifizierungsmethoden werden in der folgenden Reihenfolge getestet. Wenn die Konfiguration eine Authentifizierungsmethode nicht unterstützt, wird die nächste Methode getestet.

- **GSS-API**: Verwendet GSS-API-Mechanismen wie `mech_krb5` (Kerberos V) und `mech_dh` (AUTH_DH) zur Authentifizierung von Clients und Servern. Weitere Informationen zu GSS-API finden Sie in „Introduction to GSS-API“ in *Developer's Guide to Oracle Solaris Security* .
- **Hostbasierte Authentifizierung**: Verwendet Host-Schlüssel und rhosts-Dateien. Verwendet die öffentlichen/privaten RSA- und DSA-Hostschlüssel zur Authentifizierung des Clients. Verwendet die rhosts-Dateien zur Autorisierung des Clients für Benutzer
- **Authentifizierung mittels öffentlicher Schlüssel**: Authentifiziert Benutzer mit ihren öffentlichen/privaten RSA- und DSA-Schlüsseln
- **Passwortauthentifizierung**: Verwendet PAM zur Authentifizierung von Benutzern. Die Tastaturauthentifizierungsmethode in v2 ermöglicht willkürliche Eingabeaufforderungen durch PAM. Weitere Informationen finden Sie im Abschnitt `SECURITY` auf der Manpage `sshd(1M)`.

Die folgende Tabelle enthält die Anforderungen zur Authentifizierung eines Benutzers, der versucht, sich bei einem Remote-Host anzumelden. Der Benutzer ist beim lokalen Host (Client) angemeldet. Der Remote-Host (Server) führt den Dämon `sshd` aus. Die Tabelle enthält die Secure Shell-Authentifizierungsmethoden, die kompatiblen Protokollversionen und die Hostanforderungen.

TABELLE 19–1 Authentifizierungsmethoden für Secure Shell

Authentifizierungsmethode (Protokollversion)	Lokaler Host (Client) – Anforderungen	Remote-Host (Server) – Anforderungen
GSS-API (v2)	Initiator-Berechtigungsnachweise für GSS-Mechanismen	Verarbeiter-Berechtigungsnachweise für GSS-Mechanismen. Weitere Informationen finden Sie unter „Erhalt von GSS-Berechtigungsnachweisen in Secure Shell“ auf Seite 391.

Hostbasiert (v2)	Benutzerkonto
	Privater Schlüssel von lokalem Host in `/etc/ssh/ssh_host_rsa_key` oder `/etc/ssh/ssh_host_dsa_key`
	`HostbasedAuthentication yes` in `/etc/ssh/ssh_config`
		Benutzerkonto
		Öffentlicher Schlüssel von lokalem Host in `/etc/ssh/known_hosts` oder `~/.ssh/known_hosts`
		`HostbasedAuthentication yes` in `/etc/ssh/sshd_config`
		`IgnoreRhosts no` in `/etc/ssh/sshd_config`
		Lokaler Hosteintrag in `/etc/ssh/shosts.equiv`, `/etc/hosts.equiv`, `~/.rhosts` oder `~/.shosts`

Öffentlicher RSA- oder DSA-Schlüssel (v2)	Benutzerkonto Privater Schlüssel in `~/.ssh/id_rsa` oder `~/.ssh/id_dsa` Öffentlicher Schlüssel des Benutzers in `~/.ssh/id_rsa.pub` oder `~/.ssh/id_dsa.pub`	Benutzerkonto Öffentlicher Schlüssel des Benutzers in `~/.ssh/authorized_keys`
Öffentlicher RSA-Schlüssel (v1)	Benutzerkonto Privater Schlüssel in `~/.ssh/identity` Öffentlicher Schlüssel des Benutzers in `~/.ssh/identity.pub`	Benutzerkonto Öffentlicher Schlüssel des Benutzers in `~/.ssh/authorized_keys`
Interaktiv mit Tastatur (v2)	Benutzerkonto	Benutzerkonto Unterstützt PAM einschließlich willkürlicher Eingabeaufforderungen und Passwortänderungen, wenn die Passwortdatierungsfunktion ausgelöst wird
Passwort-basiert (v1 oder v2)	Benutzerkonto	Benutzerkonto Unterstützt PAM
Nur `.rhosts` (v1)	Benutzerkonto	Benutzerkonto `IgnoreRhosts no` in `/etc/ssh/sshd_config` Lokaler Hosteintrag in `/etc/ssh/shosts.equiv`, `/etc/hosts.equiv`, `~/.shosts` oder `~/.rhosts`

TABELLE 19–1 Authentifizierungsmethoden für Secure Shell *(Fortsetzung)*

Authentifizierungsmethode (Protokollversion)	Lokaler Host (Client) – Anforderungen	Remote-Host (Server) – Anforderungen
Nur `.rhosts` mit RSA (v1) auf dem Server	Benutzerkonto Öffentlicher Schlüssel von lokalem Host in `/etc/ssh/ssh_host_rsa1_key`	Benutzerkonto Öffentlicher Schlüssel von lokalen Host in `/etc/ssh/ssh_known_hosts` oder `~/.ssh/known_hosts` `IgnoreRhosts no` in `/etc/ssh/sshd_config` Lokaler Hosteintrag in `/etc/ssh/shosts.equiv`, `/etc/hosts.equiv`, `~/.shosts` oder `~/.rhosts`

Secure Shell in the Enterprise

Eine umfassende Beschreibung von Secure Shell auf einem Oracle Solaris-System finden Sie in *Secure Shell in the Enterprise* von Jason Reid, ISBN 0-13-142900-0, Juni 2003. Dieses Buch ist Teil der Sun BluePrints Series, die von Sun Microsystems Press veröffentlicht wird.

Oracle Solaris Secure Shell und das OpenSSH-Projekt

Die Oracle Solaris Secure Shell ist ein Zweig des OpenSSH (`http://www.openssh.com`)-Projekts. Korrekturen für Sicherheitslücken, die in späteren Versionen von OpenSSH erkannt wurden, wurden in Oracle Solaris Secure Shell integriert, sowie Fehlerkorrekturen und Funktionen. Der Oracle Solaris Secure Shell-Zweig wird intern weiterentwickelt.

Zusammen mit den Fehlerkorrekturen wurden auch folgende Funktionen in den Oracle Solaris-Zweig von Secure Shell integriert:

- PAM: Oracle Solaris Secure Shell verwendet PAM. Die OpenSSH-Konfigurationsoption `UsePAM` wird nicht unterstützt.
- Privilegienteilung: Oracle Solaris Secure Shell verwendet nicht den Privilegienteilungscode aus dem OpenSSH-Projekt. Oracle Solaris Secure Shell trennt die Verarbeitung der Prüfung, Datensatzerhaltung und erneute Tastatureingabe von der Verarbeitung der Sitzungsprotokolle.

  Der Oracle Solaris Secure Shell-Privilegienteilungscode ist immer aktiviert und kann nicht deaktiviert werden. Die OpenSSH-Option `UsePrivilegeSeparation` wird nicht unterstützt.
- Gebietsschema: Oracle Solaris Secure Shell bietet volle Unterstützung für die Aushandlung der Sprache wie in RFC 4253, *Secure Shell Transfer Protocol* definiert. Nach der Anmeldung kann die Anmelde-Shell des Benutzers die von Secure Shell ausgehandelten Gebietsschemaeinstellungen überschreiben.

- Prüfung: Oracle Solaris Secure Shell ist vollständig in das Subsystem für die Oracle Solaris-Prüfung integriert. Weitere Informationen zur Prüfung finden Sie in Teil VII.
- GSS-API-Unterstützung: Die GSS-API kann zur Benutzerauthentifizierung *und* zum anfänglichen Schlüsselaustausch verwendet werden. Die GSS-API ist in RFC4462, *Generic Security Service Application Program Interface* definiert.
- Proxy-Befehle: Oracle Solaris Secure Shell bietet Proxy-Befehle für die Protokolle SOCKS5 und HTTP. Ein Beispiel finden Sie unter „So richten Sie Standardverbindungen mit Hosts außerhalb einer Firewall ein“ auf Seite 385.

In Version Solaris 9 wurden folgende Änderungen an Oracle Solaris Secure Shell eingeführt:

- Oracle Solaris Secure Shell wurde von OpenSSH 3.5p1 getrennt.
- Der Standardwert für `X11Forwarding` in der Datei `/etc/ssh/sshd_config` lautet `yes`
- Die folgenden Schlüsselwörter wurden eingeführt:
  - `GSSAPIAuthentication`
  - `GSSAPIKeyExchange`
  - `GSSAPIDelegateCredentials`
  - `GSSAPIStoreDelegatedCredentials`
  - `KbdInteractiveAuthentication`

  Die `GSSAPI`-Schlüsselwörter ermöglichen Oracle Solaris Secure Shell die Verwendung von GSS-Berechtigungsnachweisen zur Authentifizierung. Das Schlüsselwort `KbdInteractiveAuthentication` unterstützt willkürliche Eingabeaufforderungen und Passwortänderungen in PAM. Eine vollständige Liste der Schlüsselwörter und ihrer Standardwerte finden Sie unter „Schlüsselwörter in Secure Shell“ auf Seite 393.
- Die Codes ARCFOUR und AES128-CTR sind jetzt verfügbar. ARCFOUR ist auch unter dem Namen RC4 bekannt. Beim AES-Cipher handelt es sich um AES im Zählermodus.
- Der `sshd`-Dämon verwendet die Variablen in `/etc/default/login` und den Befehl `login`. Die `/etc/default/login`-Variablen können durch Werte in der Datei `sshd_config` überschrieben werden. Weitere Informationen finden Sie unter „Secure Shell und Variablen für die Anmeldeumgebung“ auf Seite 397 und auf der Manpage `sshd_config(4)`.
- Die Option `ChrootDirectory` auf dem Server ermöglicht dem Server, nach Authentifizierung der Verbindung mit `chroot` das Root-Verzeichnis der verbundenen Clients entsprechend der angegebenen Option zu ändern. Diese Option unterstützt einen internen SFTP-Server, dessen Konfiguration mit der Option `ChrootDirectory` vereinfacht wurde.

Oracle Solaris Secure Shell (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf andere Übersichten zur Konfiguration von Secure Shell und zur Verwendung der Secure Shell-Funktion in Oracle Solaris.

Aufgabe	Beschreibung	Anweisungen
Konfigurieren von Secure Shell	Enthält Anweisungen für Administratoren zur Konfiguration von Secure Shell für Benutzer	„Konfigurieren von Oracle Solaris Secure Shell (Übersicht der Schritte)“ auf Seite 370
Verwenden von Secure Shell	Enthält Anweisungen für Benutzer zur Verwendung von Secure Shell	„Verwenden von Oracle Solaris Secure Shell (Übersicht der Schritte)“ auf Seite 375

Konfigurieren von Oracle Solaris Secure Shell (Übersicht der Schritte)

In der folgenden Übersicht der Schritte wird auf Verfahren zur Konfiguration von Secure Shell verwiesen.

Aufgabe	Beschreibung	Anweisungen
Konfigurieren von hostbasierter Authentifizierung	Konfiguriert hostbasierte Authentifizierung auf Client und Server	„So richten Sie eine hostbasierte Authentifizierung für Secure Shell ein“ auf Seite 371
Konfigurieren eines Hosts zur Verwendung von v1 und v2	Erstellt öffentliche Schlüsseldateien für Hosts, die v1- und v2-Protokolle verwenden	„So aktivieren Sie Secure Shell v1“ auf Seite 373
Konfigurieren von Port-Weiterleitung	Ermöglicht Benutzern die Verwendung der Port-Weiterleitung	„So konfigurieren Sie die Port-Weiterleitung in Secure Shell“ auf Seite 374

Konfigurieren von Oracle Solaris Secure Shell (Aufgaben)

Standardmäßig ist die hostbasierte Authentifizierung und Verwendung beider Protokolle in Secure Shell nicht aktiviert. Das Ändern dieser Standards erfordert einige administrative Maßnahmen. Auch zur Port-Weiterleitung sind administrativen Maßnahmen notwendig.

▼ So richten Sie eine hostbasierte Authentifizierung für Secure Shell ein

Mit dem folgenden Verfahren wird ein öffentliches Schlüsselsystem eingerichtet, in dem der öffentliche Schlüssel des Clients zur Authentifizierung auf dem Server verwendet wird. Der Benutzer muss außerdem ein Paar aus öffentlichem und privatem Schlüssel erstellen.

In diesem Verfahren beziehen sich die Begriffe *Client* und *lokaler Host* auf den Rechner, auf dem ein Benutzer den Befehl `ssh` eingibt. Die Begriffe *Server* und *Remote-Host* beziehen sich auf den Rechner, mit dem der Client eine Verbindung herzustellen versucht.

1 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Aktivieren Sie die hostbasierte Authentifizierung auf dem Client.**

Geben Sie in der Clientkonfigurationsdatei `/etc/ssh/ssh_config` den folgenden Eintrag ein:

```
HostbasedAuthentication yes
```

Informationen zur Syntax der Datei finden Sie auf der Manpage `ssh_config(4)`.

3 **Aktivieren Sie die hostbasierte Authentifizierung auf dem Server.**

Geben Sie in der Serverkonfigurationsdatei `/etc/ssh/ssh_config` den gleichen Eintrag ein:

```
HostbasedAuthentication yes
```

Informationen zur Syntax der Datei finden Sie auf der Manpage `sshd_config(4)`.

4 **Konfigurieren Sie auf dem Server eine Datei, durch die der Client als vertrauenswürdiger Host erkannt wird.**

Weitere Informationen finden Sie im Abschnitt `FILES` auf der Manpage `sshd(1M)`.

- **Fügen Sie den Client als Eintrag in der Datei `/etc/ssh/shosts.equiv` des Servers ein.**

  client-host

- **Sie können auch die Benutzer bitten, einen Eintrag für den Client ihrer Datei `~/.shosts` auf dem Server hinzuzufügen.**

  client-host

5 **Vergewissern Sie sich, dass der Dämon `sshd` auf dem Server Zugriff auf die Liste der vertrauenswürdigen Hosts hat.**

Stellen Sie `IgnoreRhosts` in der Datei `/etc/ssh/sshd_config` auf `no` ein.

```
## sshd_config
IgnoreRhosts no
```

6 **Vergewissern Sie sich, dass die Benutzer von Secure Shell an Ihrem Standort über Konten auf beiden Hosts verfügen.**

7 **Führen Sie einen der folgenden Schritte aus, um den öffentlichen Schlüssel des Clients auf den Server zu übertragen.**

- **Ändern Sie die Datei `sshd_config` auf dem Server, bitten Sie dann die Benutzer, die öffentlichen Hostschlüssel des Clients der zugehörigen Datei `~/.ssh/known_hosts` hinzuzufügen.**

  ```
  ## sshd_config
  IgnoreUserKnownHosts no
  ```

  Benutzeranweisungen finden Sie unter „So generieren Sie ein Paar aus öffentlichem und privatem Schlüssel für Secure Shell“ auf Seite 376.

- **Kopieren Sie den öffentlichen Schlüssel des Clients auf den Server.**

  Die Hostschlüssel werden im Verzeichnis `/etc/ssh` gespeichert. Die Schlüssel werden üblicherweise vom Dämon `sshd` beim ersten Starten erstellt.

  a. **Fügen Sie den Schlüssel der Datei `/etc/ssh/ssh_known_hosts` auf dem Server hinzu.**

  Geben Sie auf dem Client den Befehl in einer Zeile ohne umgekehrten Schrägstrich ein.

  ```
  # cat /etc/ssh/ssh_host_dsa_key.pub | ssh RemoteHost \
  'cat >> /etc/ssh/ssh_known_hosts && echo "Host key copied"'
  ```

  b. **Geben Sie bei Aufforderung Ihr Anmeldepasswort ein.**

  Sobald die Datei kopiert ist, wird die Meldung "Host key copied" (Hostschlüssel kopiert) angezeigt.

  Die einzelnen Zeilen der Datei `/etc/ssh/ssh_known_hosts` bestehen aus Feldern, die durch Leerzeichen getrennt sind:

  hostnames algorithm-name publickey comment

  c. **Bearbeiten Sie die Datei `/etc/ssh/ssh_known_hosts` und fügen Sie *RemoteHost* als erstes Feld in den kopierten Eintrag ein.**

  ```
  ## /etc/ssh/ssh_known_hosts File
  RemoteHost  <copied entry>
  ```

Beispiel 19–1 Einrichten von hostbasierter Authentifizierung

In dem folgenden Beispiel wird jeder Host als Server und als Client konfiguriert. Ein Benutzer auf einem der beiden Hosts kann eine `ssh`-Verbindung zu dem anderen Host initiieren. In der folgenden Konfiguration ist jeder Host gleichzeitig Server und Client:

- Auf jedem Host enthalten die Secure Shell-Konfigurationsdateien die folgenden Einträge:

```
## /etc/ssh/ssh_config
HostBasedAuthentication yes
#
## /etc/ssh/sshd_config
HostBasedAuthentication yes
IgnoreRhosts no
```

- Die Datei `shosts.equiv` auf jedem Host enthält einen Eintrag für den anderen Host:

```
## /etc/ssh/shosts.equiv on machine2
machine1

## /etc/ssh/shosts.equiv on machine1
machine2
```

- Der öffentliche Schlüssel für jeden Host befindet sich in der Datei `/etc/ssh/ssh_known_hosts` auf dem anderen Host:

```
## /etc/ssh/ssh_known_hosts on machine2
... machine1

## /etc/ssh/ssh_known_hosts on machine1
... machine2
```

- Benutzer verfügen nur über ein Konto auf beiden Hosts:

```
## /etc/passwd on machine1
jdoe:x:3111:10:J Doe:/home/jdoe:/bin/sh

## /etc/passwd on machine2
jdoe:x:3111:10:J Doe:/home/jdoe:/bin/sh
```

▼ So aktivieren Sie Secure Shell v1

Dieses Verfahren ist hilfreich, wenn ein Host mit anderen Hosts interagiert, die v1 und v2 ausführen.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Konfigurieren Sie den Host zur Verwendung beider Secure Shell-Protokolle.

Bearbeiten Sie die Datei `/etc/ssh/sshd_config`.

```
# Protocol 2
Protocol 2,1
```

3 Stellen Sie eine separate Datei für den Hostschlüssel für v1 bereit.

Fügen Sie der Datei `/etc/ssh/sshd_config` einen `HostKey`-Eintrag hinzu.

```
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_rsa1_key
```

4 Generieren Sie einen Hostschlüssel für v1.

```
# ssh-keygen -t rsa1 -f /etc/ssh/ssh_host_rsa1_key -N ''
```

`-t rsa1`	Gibt den RSA-Algorithmus für v1 an
`-f`	Gibt die Datei an, die den Hostschlüssel enthält
`-N ''`	Gibt an, dass kein Passwortsatz erforderlich ist.

5 Starten Sie den Dämon `sshd` neu.

```
# svcadm restart network/ssh:default
```

Stattdessen können Sie auch das System neu booten.

▼ So konfigurieren Sie die Port-Weiterleitung in Secure Shell

Mithilfe der Port-Weiterleitung kann ein lokaler Port an einen Remote-Host weitergeleitet werden. Tatsächlich wird ein Socket zugewiesen, das auf Anfragen vom Port auf der lokalen Seite wartet. Ähnlich kann ein Port auf der Remote-Seite angegeben werden.

Hinweis – Zur Secure Shell-Port-Weiterleitung muss eine TCP-Verbindung verwendet werden. Secure Shell unterstützt keine Port-Weiterleitung für UDP-Verbindungen.

---

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Konfigurieren Sie eine Secure Shell-Einstellung auf dem Remote-Server, um die Port-Weiterleitung zu ermöglichen.**

Ändern Sie den Wert von `AllowTcpForwarding` in der Datei `/etc/ssh/sshd_config` in `yes`.

```
# Port forwarding
AllowTcpForwarding yes
```

3 **Starten Sie den Secure Shell-Service neu.**

```
remoteHost# svcadm restart network/ssh:default
```

Informationen zum Verwalten von persistenten Services finden Sie in Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration* und auf der Manpage `svcadm`(1M).

4 **Vergewissern Sie sich, dass die Port-Weiterleitung verwendet werden kann.**

```
remoteHost# /usr/bin/pgrep -lf sshd
 1296 ssh -L 2001:remoteHost:23 remoteHost
```

Verwenden von Oracle Solaris Secure Shell (Übersicht der Schritte)

In der folgenden Übersicht der Schritte wird auf Verfahren zur Verwendung von Secure Shell für Benutzer verwiesen.

Aufgabe	Beschreibung	Anweisungen
Erstellen eines Paars aus öffentlichem und privatem Schlüssel	Ermöglicht an Standorten, an denen die Authentifizierung mithilfe von öffentlichen Schlüsseln erfolgt, den Zugriff auf Secure Shell	„So generieren Sie ein Paar aus öffentlichem und privatem Schlüssel für Secure Shell“ auf Seite 376
Ändern des Passwortsatzes	Ändert den Passwortsatz, der zur Authentifizierung des privaten Schlüssels dient	„So ändern Sie den Passwortsatz für einen privaten Secure Shell-Schlüssel“ auf Seite 378
Anmelden mit Secure Shell	Bietet verschlüsselte Secure Shell-Kommunikation bei einer Remote-Anmeldung. Der Prozess ist dem Befehl `rsh` ähnlich.	„So melden Sie sich bei einem Remote-Host mithilfe von Secure Shell an“ auf Seite 379
Anmelden bei Secure Shell ohne Eingabe eines Passworts	Ermöglicht die Anmeldung mithilfe eines Agenten, der Ihr Passwort für Secure Shell bereitstellt	„So reduzieren Sie die Aufforderungen zur Passworteingabe in Secure Shell“ auf Seite 380
		„So richten Sie den Befehl `ssh-agent` zur automatischen Ausführung in CDE ein“ auf Seite 381

Aufgabe	Beschreibung	Anweisungen
Verwenden der Port-Weiterleitung in Secure Shell	Gibt einen lokalen oder Remote-Port an, der für eine Secure Shell-Verbindung über TCP verwendet werden soll	„So verwenden Sie die Port-Weiterleitung in Secure Shell“ auf Seite 382
Kopieren von Dateien mit Secure Shell	Kopiert Dateien sicher von einem Host auf den anderen	„So kopieren Sie Dateien mit Secure Shell“ auf Seite 384
Sicheres Verbinden zwischen Hosts innerhalb und außerhalb der Firewall	Verwendet mit HTTP oder SOCKS5 kompatible Secure Shell-Befehle zur Verbindung von Hosts, die durch eine Firewall getrennt sind	„So richten Sie Standardverbindungen mit Hosts außerhalb einer Firewall ein“ auf Seite 385

Verwenden von Oracle Solaris Secure Shell (Aufgaben)

Secure Shell bietet sicheren Zugriff zwischen einer lokalen und einer Remote-Shell. Weitere Informationen finden Sie auf den Manpages `ssh_config(4)` und `ssh(1)`.

▼ So generieren Sie ein Paar aus öffentlichem und privatem Schlüssel für Secure Shell

Benutzer müssen ein Paar aus öffentlichem und privatem Schlüssel generieren, wenn an ihrem Standort eine hostbasierte Authentifizierung oder eine Authentifizierung anhand öffentlicher Benutzerschlüssel implementiert wird. Zusätzliche Optionen finden Sie auf der Manpage `ssh-keygen(1)`.

Bevor Sie beginnen Fragen Sie Ihren Systemadministrator, ob eine hostbasierte Authentifizierung konfiguriert wurde.

1 Starten Sie das Schlüsselgenerierungsprogramm.

```
myLocalHost% ssh-keygen -t rsa
Generating public/private rsa key pair.
...
```

Dabei gilt: `-t` ist der Algorithmustyp, entweder `rsa`, `dsa` oder `rsa1`.

2 Geben Sie den Pfad zu der Datei ein, die den Schlüssel enthält.

Standardmäßig wird der Dateiname `id_rsa`, in diesem Fall für einen RSA v2-Schlüssel, in Klammern eingeschlossen. Sie können die Datei auswählen, indem Sie die Eingabetaste drücken. Stattdessen können Sie auch einen alternativen Dateinamen eingeben.

```
Enter file in which to save the key (/home/jdoe/.ssh/id_rsa):     <Press Return>
```

Der Dateiname des öffentlichen Schlüssels wird automatisch erstellt, indem die Zeichenfolge `.pub` an den Dateinamen für den privaten Schlüssel angehängt wird.

3 Geben Sie einen Passwortsatz zur Verwendung des Schlüssels ein.

Dieser Passwortsatz wird zur Verschlüsselung des privaten Schlüssels verwendet. Von einem Nulleintrag wird *dringend abgeraten*. Beachten Sie, dass der Passwortsatz bei der Eingabe nicht angezeigt wird.

```
Enter passphrase (empty for no passphrase):      <Type passphrase>
```

4 Geben Sie den Passwortsatz zur Bestätigung erneut ein.

```
Enter same passphrase again:      <Type passphrase>
Your identification has been saved in /home/jdoe/.ssh/id_rsa.
Your public key has been saved in /home/jdoe/.ssh/id_rsa.pub.
The key fingerprint is:
0e:fb:3d:57:71:73:bf:58:b8:eb:f3:a3:aa:df:e0:d1 jdoe@myLocalHost
```

5 Überprüfen Sie die Ergebnisse.

Überprüfen Sie, ob der Pfad zur Schlüsseldatei korrekt ist.

```
% ls ~/.ssh
id_rsa
id_rsa.pub
```

Jetzt haben Sie ein Paar aus öffentlichem und privatem Schlüssel erstellt.

6 Wählen Sie die geeignete Option:

- **Wenn Ihr Administrator eine hostbasierte Authentifizierung konfiguriert hat, müssen Sie möglicherweise den öffentlichen Schlüssel des lokalen Hosts auf den Remote-Host kopieren.**

  Jetzt können Sie sich beim Remote-Host anmelden. Details finden Sie unter „So melden Sie sich bei einem Remote-Host mithilfe von Secure Shell an“ auf Seite 379.

  a. Geben Sie den Befehl in einer Zeile ohne umgekehrten Schrägstrich ein.

  ```
  % cat /etc/ssh/ssh_host_dsa_key.pub | ssh RemoteHost \
  'cat >> ~./ssh/known_hosts && echo "Host key copied"'
  ```

  b. Geben Sie bei Aufforderung Ihr Anmeldepasswort ein.

  ```
  Enter password:      <Type password>
  Host key copied
  %
  ```

- **Wenn an Ihrem Standort Benutzer mithilfe von öffentlichen Schlüsseln authentifiziert werden, nehmen Daten in die Datei `authorized_keys` auf dem Remote-Host auf.**

  a. Kopieren Sie den öffentlichen Schlüssel auf den Remote-Host.

  Geben Sie den Befehl in einer Zeile ohne umgekehrten Schrägstrich ein.

  ```
  myLocalHost% cat $HOME/.ssh/id_rsa.pub | ssh myRemoteHost \
  'cat >> .ssh/authorized_keys && echo "Key copied"'
  ```

b. Geben Sie bei Aufforderung Ihr Anmeldepasswort ein.

Sobald die Datei kopiert ist, wird die Meldung "Key copied" (Schlüssel kopiert) angezeigt.

```
Enter password:       Type login password
Key copied
myLocalHost%
```

7 (Optional) Reduzieren Sie die Eingabeaufforderung für Passwortsätze.

Anweisungen finden Sie unter „So reduzieren Sie die Aufforderungen zur Passworteingabe in Secure Shell“ auf Seite 380. Weitere Informationen finden Sie auf den Manpages `ssh-agent(1)` und `ssh-add(1)`.

Beispiel 19–2 Einrichten eines v1 RSA-Schlüssels für einen Benutzer

In dem folgenden Beispiel kann der Benutzer Hosts aufrufen, die v1 des Secure Shell-Protokolls ausführen. Um von v1-Hosts authentifiziert zu werden, erstellt der Benutzer einen v1-Schlüssel und kopiert den öffentlichen Schlüsselteil auf den Remote-Host.

```
myLocalHost% ssh-keygen -t rsa1 -f /home/jdoe/.ssh/identity
Generating public/private rsa key pair.
...
Enter passphrase (empty for no passphrase):      <Type passphrase>
Enter same passphrase again:      <Type passphrase>
Your identification has been saved in /home/jdoe/.ssh/identity.
Your public key has been saved in /home/jdoe/.ssh/identity.pub.
The key fingerprint is:
...
myLocalHost% ls ~/.ssh
id_rsa
id_rsa.pub
identity
identity.pub
myLocalHost% cat $HOME/.ssh/identity.pub | ssh myRemoteHost \
'cat >> .ssh/authorized_keys && echo "Key copied"'
```

▼ So ändern Sie den Passwortsatz für einen privaten Secure Shell-Schlüssel

Mit dem folgenden Verfahren wird der private Schlüssel nicht geändert. Das Verfahren ändert den Authentifizierungsmechanismus für den privaten Schlüssel, d. h. den Passwortsatz. Informationen finden Sie auf der Manpage `ssh-keygen(1)`.

- **Ändern Sie Ihren Passwortsatz.**

  Führen Sie den Befehl `ssh-keygen` mit der Option `-p` aus und geben Sie an den Eingabeaufforderungen die entsprechenden Informationen ein.

  ```
  myLocalHost% ssh-keygen -p
  Enter file which contains the private key (/home/jdoe/.ssh/id_rsa):     <Press Return>
  Enter passphrase (empty for no passphrase):     <Type passphrase>
  Enter same passphrase again:      <Type passphrase>
  ```

  Dabei gilt: `-p` fordert an, dass der Passwortsatz einer Datei mit einem privaten Schlüssel geändert wird.

▼ So melden Sie sich bei einem Remote-Host mithilfe von Secure Shell an

1. **Starten Sie eine Secure Shell-Sitzung.**

   Geben Sie den Befehl `ssh` ein sowie den Namen des Remote-Hosts.

   ```
   myLocalHost% ssh myRemoteHost
   ```

   Es wird eine Eingabeaufforderung zur Authentizität des Remote-Hosts angezeigt:

   ```
   The authenticity of host 'myRemoteHost' can't be established.
   RSA key fingerprint in md5 is: 04:9f:bd:fc:3d:3e:d2:e7:49:fd:6e:18:4f:9c:26
   Are you sure you want to continue connecting(yes/no)?
   ```

   Diese Eingabeaufforderung ist bei der ersten Verbindung zu einem Remote-Host normal.

2. **Überprüfen Sie bei Aufforderung die Authentizität des Schlüssels vom Remote-Host.**

   - **Wenn Sie die Authentizität des Remote-Hosts nicht bestätigen können, geben Sie `no` ein und wenden sich an Ihren Systemadministrator.**

     ```
     Are you sure you want to continue connecting(yes/no)? no
     ```

     Der Administrator ist für die Aktualisierung der globalen Datei `/etc/ssh/ssh_known_hosts` zuständig. Wenn die Datei `ssh_known_hosts` auf dem neuesten Stand ist, wird diese Eingabeaufforderung nicht angezeigt.

   - **Wenn Sie die Authentizität des Remote-Hosts bestätigen können, geben Sie die entsprechende Antwort ein und fahren mit dem nächsten Schritt fort.**

     ```
     Are you sure you want to continue connecting(yes/no)? yes
     ```

3. **Authentifizieren Sie sich bei Secure Shell.**

   a. **Geben Sie bei Aufforderung Ihren Passwortsatz ein.**

      ```
      Enter passphrase for key '/home/jdoe/.ssh/id_rsa':     <Type passphrase>
      ```

b. Geben Sie bei Aufforderung das Passwort für Ihr Konto ein.

```
jdoe@myRemoteHost's password:      <Type password>
Last login: Fri Jul 20 14:24:10 2001 from myLocalHost
myRemoteHost%
```

4 Führen Sie Transaktionen auf dem Remote-Host aus.

Die gesendeten Befehle sind verschlüsselt. Alle Antworten, die Sie erhalten sind verschlüsselt.

5 Trennen Sie die Secure Shell-Verbindung.

Geben Sie zum Abschluss **exit** ein oder verwenden Sie die gewohnte Methode zum Schließen der Shell.

```
myRemoteHost% exit
myRemoteHost% logout
Connection to myRemoteHost closed
myLocalHost%
```

▼ So reduzieren Sie die Aufforderungen zur Passworteingabe in Secure Shell

Wenn Sie Ihren Passwortsatz und Ihr Passwort zur Verwendung von Secure Shell nicht jedes Mal eingeben möchten, können Sie den Agentendämon verwenden. Starten Sie den Dämon zu Beginn der Sitzung. Fügen Sie dem Agentendämon Ihre privaten Schlüssel hinzu, indem Sie den Befehl `ssh-add` eingeben. Wenn Sie verschiedene Konten auf unterschiedlichen Hosts besitzen, fügen Sie die für die Sitzung benötigten Schlüssel hinzu.

Sie können den Agentendämon bei Bedarf manuell starten, wie im folgenden Verfahren beschrieben. Sie können den Agentendämon auch automatisch zu Beginn jeder Sitzung ausführen, wie in „So richten Sie den Befehl `ssh-agent` zur automatischen Ausführung in CDE ein“ auf Seite 381 beschrieben.

1 Starten Sie den Agentendämon.

```
myLocalHost% eval 'ssh-agent'
Agent pid 9892
```

2 Überprüfen Sie, ob der Agentendämon gestartet wurde.

```
myLocalHost% pgrep ssh-agent
9892
```

3 Fügen Sie Ihren privaten Schlüssel dem Agentendämon hinzu.

Geben Sie den Befehl `ssh-add` ein.

```
myLocalHost% ssh-add
Enter passphrase for /home/jdoe/.ssh/id_rsa:      <Type passphrase>
Identity added: /home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa)
myLocalHost%
```

4 Starten Sie eine Secure Shell-Sitzung.

```
myLocalHost% ssh myRemoteHost
```

Sie müssen keinen Passwortsatz eingeben.

Beispiel 19–3 Verwenden von `ssh-add`-Optionen

In diesem Beispiel fügt `jdoe` dem Agentendämon zwei Schlüssel hinzu. Die Option `-l` wird zum Auflisten aller Schlüssel des Dämons verwendet. Am Ende der Sitzung werden mit der Option `-D` alle Schlüssel des Agentendämons entfernt.

```
myLocalHost% ssh-agent
myLocalHost% ssh-add
Enter passphrase for /home/jdoe/.ssh/id_rsa:      <Type passphrase>
Identity added: /home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa)
myLocalHost% ssh-add /home/jdoe/.ssh/id_dsa
Enter passphrase for /home/jdoe/.ssh/id_dsa:      <Type passphrase>
Identity added:
/home/jdoe/.ssh/id_dsa(/home/jdoe/.ssh/id_dsa)

myLocalHost% ssh-add -l
md5 1024 0e:fb:3d:53:71:77:bf:57:b8:eb:f7:a7:aa:df:e0:d1
/home/jdoe/.ssh/id_rsa(RSA)
md5 1024 c1:d3:21:5e:40:60:c5:73:d8:87:09:3a:fa:5f:32:53
/home/jdoe/.ssh/id_dsa(DSA)
```

User conducts Oracle Solaris Secure Shell transactions

```
myLocalHost% ssh-add -D
Identity removed:
/home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa.pub)
/home/jdoe/.ssh/id_dsa(DSA)
```

▼ So richten Sie den Befehl `ssh-agent` zur automatischen Ausführung in CDE ein

In CDE können Sie vermeiden, dass Sie bei jeder Verwendung von Secure Shell zur Eingabe Ihres Passwortsatzes und Passworts aufgefordert werden, indem Sie den Agentendämon `ssh-agent` automatisch starten. Sie können den Agentendämon über das `.dtprofile`-Skript starten. Informationen zum Hinzufügen Ihres Passwortsatzes und Passworts finden Sie in Beispiel 19–3.

Achtung – Wenn Sie Sun Java Desktop System (Java DS) verwenden, richten Sie den Befehl `ssh-agent` nicht zur automatischen Ausführung ein. Da das Beenden des `ssh-agent`-Prozesses durch eine CDE-Schnittstelle gesteuert wird, wird der Dämon nach dem Beenden von Java DS weiter ausgeführt. Wenn Sie den Dämon beispielsweise in einer CDE-Sitzung starten, dann zu einer Java DS-Sitzung wechseln und sich anschließend abmelden, wird der Dämon weiter ausgeführt.

Die Ausführung des Dämons beansprucht Systemressourcen. Auch wenn keine Probleme in Verbindung mit der fortgesetzten Ausführung des Dämons `ssh-agent` bekannt sind, enthält der Dämon ein Passwort, was ein Sicherheitsrisiko bedeuten kann.

1 Starten Sie den Agentendämon automatisch in einem Benutzer-Startskript.

Fügen Sie folgenden Zeilen am Ende des Skripts `$HOME/.dtprofile` hinzu:

```
if [ "$SSH_AUTH_SOCK" = "" -a -x /usr/bin/ssh-agent ]; then
                eval `/usr/bin/ssh-agent`
fi
```

2 Beenden Sie den Agentendämon, wenn Sie die CDE-Sitzung beenden.

Fügen Sie dem Skript `$HOME/.dt/sessions/sessionexit` folgende Zeilen hinzu:

```
if [ "$SSH_AGENT_PID" != "" -a -x /usr/bin/ssh-agent ]; then
                /usr/bin/ssh-agent -k
fi
```

Dieser Eintrag gewährleistet, dass keiner den Secure Shell-Agenten nach Beendigung der CDE-Sitzung verwenden kann. Da das Skript eine CDE-spezifische Schnittstelle (`sessionexit`) verwendet, wird der Agentendämon in einer Sun Java Desktop System-Sitzung mit diesem Verfahren nicht beendet.

▼ So verwenden Sie die Port-Weiterleitung in Secure Shell

Sie können angeben, dass ein lokaler Port an einen Remote-Host weitergeleitet wird. Tatsächlich wird ein Socket zugewiesen, das auf Anfragen vom Port auf der lokalen Seite wartet. Die Verbindung von diesem Port wird über einen sicheren Kanal zum Remote-Host eingerichtet. Beispielsweise können Sie Port 143 angeben, um an einem entfernten Standort E-Mails über IMAP4 zu erhalten. Ähnlich kann ein Port auf der Remote-Seite angegeben werden.

Bevor Sie beginnen Zur Weiterleitung von Ports muss der Administrator die Port-Weiterleitung auf dem Secure Shell-Remote-Server aktiviert haben. Weitere Informationen finden Sie unter „So konfigurieren Sie die Port-Weiterleitung in Secure Shell“ auf Seite 374.

- **Zur sicheren Weiterleitung von Ports wählen Sie eine der folgenden Optionen:**

  - **Um Mitteilungen sicher von einem Remote-Port an einen lokalen Port zu senden, geben Sie beide Ports an.**

    Geben Sie den lokalen Port an, der auf Mitteilungen vom Remote-Port wartet. Geben Sie außerdem den Remote-Host und den Remote-Port an, von denen die Mitteilung weiterleitet wird.

    ```
    myLocalHost% ssh -L localPort:remoteHost:remotePort
    ```

  - **Um eine sichere Verbindung von einem Remote-Port zu einem lokalen Port einzurichten, geben Sie beide Ports an.**

    Geben Sie den Remote-Port an, der auf Mitteilungen wartet. Geben Sie außerdem den lokalen Host und den lokalen Port an, von denen die Mitteilung weiterleitet wird.

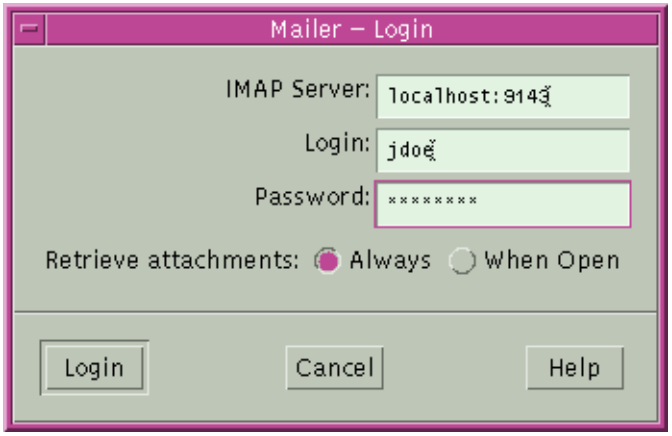
    ```
    myLocalHost% ssh -R remotePort:localhost:localPort
    ```

Beispiel 19–4 Verwenden der lokalen Port-Weiterleitung für den Empfang von E-Mails

Das folgende Beispiel zeigt, wie Sie die lokale Port-Weiterleitung verwenden, um Mails von einem Remote-Server sicher empfangen zu können.

```
myLocalHost% ssh -L 9143:myRemoteHost:143 myRemoteHost
```

Mit diesem Befehl werden Verbindungen von Port `9143` auf `myLocalHost` an Port `143` weitergeleitet. Port `143` ist der Port für den IMAP v2-Server auf `myRemoteHost`. Wenn der Benutzer eine Mailanwendung startet, muss er die lokale Portnummer angeben, wie im folgenden Dialogfeld gezeigt.



Verwechseln Sie `localhost` in dem Dialogfeld nicht mit `myLocalHost`. `myLocalHost` ist ein hypothetischer Hostname. `localhost` ist ein Schlüsselwort zur Identifizierung des lokalen Systems.

Beispiel 19–5 Verwendung der Remote-Port-Weiterleitung zur Kommunikation außerhalb einer Firewall

In diesem Beispiel wird gezeigt, wie ein Benutzer in einer Unternehmensumgebung Verbindungen von einem Host in einem externen Netzwerk an einen Host innerhalb der unternehmenseigenen Firewall weiterleiten kann.

```
myLocalHost% ssh -R 9022:myLocalHost:22 myOutsideHost
```

Mit diesem Befehl werden Verbindungen von Port `9022` auf `myOutsideHost` an Port `22`, dem `sshd`-Server, auf dem lokalen Host weitergeleitet.

```
myOutsideHost% ssh -p 9022 localhost
myLocalHost%
```

▼ So kopieren Sie Dateien mit Secure Shell

Im folgenden Verfahren wird gezeigt, wie Sie den Befehl `scp` verwenden, um verschlüsselte Dateien zwischen Hosts zu kopieren. Sie können verschlüsselte Dateien zwischen einem lokalen und einem Remote-Host oder zwei Remote-Hosts kopieren. Der Befehl funktioniert ähnlich wie der Befehl `rcp`, mit dem Unterschied, dass der Befehl `scp` zur Authentifizierung auffordert. Weitere Informationen finden Sie auf der Manpage `scp(1)`.

Sie können auch den Befehl `sftp`, eine sichere Form des Befehls `ftp`, verwenden. Weitere Informationen finden Sie auf der Manpage `sftp(1)`. Ein Beispiel erhalten Sie unter Beispiel 19–6.

1 Starten Sie das Programm zum sicheren Kopieren.

Geben Sie die Quelldatei, den Benutzernamen am Remote-Ziel und das Zielverzeichnis an.

```
myLocalHost% scp myfile.1 jdoe@myRemoteHost:~
```

2 Geben Sie bei Aufforderung Ihren Passwortsatz ein.

```
Enter passphrase for key '/home/jdoe/.ssh/id_rsa':      <Type passphrase>
myfile.1       25% |*******                      |    640 KB  0:20 ETA
myfile.1
```

Nach der Eingabe des Passwortsatzes ist eine Fortschrittsanzeige zu sehen. Sie ist in der zweiten Zeile der oben stehenden Ausgabe enthalten. Die Fortschrittsanzeige enthält folgende Informationen:

- Dateiname
- Prozentsatz der Datei, der bisher übertragen wurde
- Sternchen, die den übertragenen Prozentsatz der Datei kennzeichnen
- Menge der übertragenen Daten
- Geschätzte Zeit für den Empfang der gesamten Datei (ETA, Estimated Time of Arrival). Dies entspricht der verbleibenden Übertragungszeit.

Beispiel 19–6 Angeben eines Ports bei Verwendung des Befehls `sftp`

In diesem Beispiel möchte der Benutzer, dass der Befehl `sftp` einen bestimmten Port verwendet. Der Benutzer gibt den Port mithilfe der Option `-o` an.

```
% sftp -o port=2222 guest@RemoteFileServer
```

▼ So richten Sie Standardverbindungen mit Hosts außerhalb einer Firewall ein

Mit Secure Shell können Sie eine Verbindung von einem Host innerhalb der Firewall zu einem Host außerhalb der Firewall herstellen. Dazu muss ein Proxy-Befehl für `ssh` entweder in einer Konfigurationsdatei oder als Option in der Befehlszeile angegeben werden. Informationen zur Befehlszeilenoption finden Sie unter Beispiel 19–7.

Im Allgemeinen können Sie Ihre `ssh`-Interaktionen über eine Konfigurationsdatei anpassen.

- Sie können Ihre persönliche Datei in `~/.ssh/config` anpassen.
- Sie können auch die Einstellungen in der administrativen Konfigurationsdatei `/etc/ssh/ssh_config` verwenden.

Die Dateien können mit zwei Arten von Proxy-Befehlen angepasst werden. Ein Proxy-Befehl ist für HTTP-Verbindungen geeignet. Der andere Proxy-Befehl ist für SOCKS5-Verbindungen geeignet. Weitere Informationen finden Sie auf der Manpage `ssh_config(4)`.

1 Geben Sie die Proxy-Befehle und Hosts in einer Konfigurationsdatei an.

Fügen Sie die benötigten Zeilen mit der folgenden Syntax hinzu:

```
[Host outside-host]
ProxyCommand proxy-command [-h proxy-server] \
[-p proxy-port] outside-host|%h outside-port|%p
```

`Host` *outside-host*
: Beschränkt die Proxy-Befehlsspezifikation auf Instanzen, wenn ein Remote-Hostname in der Befehlszeile angegeben wird. Mit einem Platzhalter für *outside-host* wird die Proxy-Befehlsspezifikation auf mehrere Hosts angewendet.

proxy-command
: Gibt den Proxy-Befehl an.

  Für den Befehl gibt es eine der folgenden zwei Möglichkeiten:

  - `/usr/lib/ssh/ssh-http-proxy-connect` für HTTP-Verbindungen
  - `/usr/lib/ssh/ssh-socks5-proxy-connect` für SOCKS5-Verbindungen

`-h` *proxy-server* und `-p` *proxy-port*
: Diese Optionen geben einen Proxy-Server bzw. einen Proxy-Port an. Wenn vorhanden, überschreiben die Proxys alle Umgebungsvariablen, die Proxy-Server und Proxy-Ports angeben, wie z. B. `HTTPPROXY`, `HTTPPROXYPORT`, `SOCKS5_PORT`, `SOCKS5_SERVER` und `http_proxy`. Die Variable `http_proxy` gibt eine URL an. Wenn die Optionen nicht verwendet werden, müssen die entsprechenden Umgebungsvariablen festgelegt werden. Weitere Informationen finden Sie auf den Manpages `ssh-socks5-proxy-connect(1)` und `ssh-http-proxy-connect(1)`.

outside-host
: Gibt den Host an, zu dem eine Verbindung hergestellt werden soll. Geben Sie den Host mithilfe des Substitutionsarguments `%h` in der Befehlszeile an.

outside-port
: Gibt den Port an, zu dem eine Verbindung hergestellt werden soll. Geben Sie den Port mithilfe des Substitutionsarguments `%h` in der Befehlszeile an. Durch Angabe von `%h` und `%p` ohne Verwendung der Option `Host` *outside-host* wird der Proxy-Befehl auf das Hostargument angewendet, sobald der Befehl `ssh` aufgerufen wird.

2 Führen Sie Secure Shell unter Angabe des externen Hosts aus.

Geben Sie zum Beispiel Folgendes ein:

```
myLocalHost% ssh myOutsideHost
```

Dieser Befehl sucht nach einer Proxy-Befehlsspezifikation für `myOutsideHost` in Ihrer persönlichen Konfigurationsdatei. Wenn die Spezifikation nicht gefunden wird, sucht der Befehl in der systemweiten Konfigurationsdatei `/etc/ssh/ssh_config`. Der Befehl `ssh` wird durch den Proxy-Befehl ersetzt.

Beispiel 19–7 Erstellen einer Verbindung zu Hosts außerhalb einer Firewall über die Befehlszeile

Unter „So richten Sie Standardverbindungen mit Hosts außerhalb einer Firewall ein“ auf Seite 385 wird erläutert, wie Sie einen Proxy-Befehl in einer Konfigurationsdatei angeben. In diesem Beispiel wird ein Proxy-Befehl in der `ssh`-Befehlszeile angegeben.

```
% ssh -o'Proxycommand=/usr/lib/ssh/ssh-http-proxy-connect \
-h myProxyServer -p 8080 myOutsideHost 22' myOutsideHost
```

Die Option `-o` des Befehls `ssh` ermöglicht die Eingabe eines Proxy-Befehls in der Befehlszeile. Dieser Beispielbefehl bewirkt Folgendes:

- Ersetzt `ssh` durch den HTTP-Proxy-Befehl
- Verwendet Port `8080` und `myProxyServer` als Proxy-Server
- Verbindet Port `22` auf `myOutsideHost`

◆ ◆ ◆ KAPITEL 20

20 Oracle Solaris Secure Shell (Referenz)

In diesem Kapitel werden die Konfigurationsoptionen der Secure Shell-Funktion von Oracle Solaris beschrieben. In der folgenden Liste sind die Referenzinformationen in diesem Kapitel aufgeführt.

- „Eine typische Secure Shell-Sitzung“ auf Seite 389
- „Client- und Serverkonfiguration in Secure Shell“ auf Seite 392
- „Schlüsselwörter in Secure Shell“ auf Seite 393
- „Verwalten bekannter Hosts in Secure Shell“ auf Seite 398
- „Secure Shell-Pakete und Initialisierung“ auf Seite 398
- „Secure Shell-Dateien“ auf Seite 399
- „Secure Shell-Befehle“ auf Seite 401

Die Verfahren zur Konfiguration von Secure Shell werden in Kapitel 19, „Verwenden von Oracle Solaris Secure Shell (Aufgaben)“ beschrieben.

Eine typische Secure Shell-Sitzung

Der Secure Shell-Dämon (`sshd`) wird normalerweise beim Neustart zusammen mit den Netzwerkdiensten gestartet. Der Dämon wartet auf Verbindungen von Clients. Eine Secure Shell-Sitzung beginnt, sobald ein Benutzer den Befehl `ssh`, `scp` oder `sftp` ausführt. Für jede eingehende Verbindung wird ein neuer `sshd`-Dämon gestartet. Diese Dämonen übernehmen den Schlüsselaustausch, die Verschlüsselung, Authentifizierung, Befehlsausführung und den Datenaustausch mit dem Client. Die Sitzungsmerkmale werden von clientseitigen und serverseitigen Konfigurationsdateien bestimmt. Befehlszeilenargumente können die Einstellungen in den Konfigurationsdateien überschreiben.

Der Client und der Server müssen sich gegenseitig authentifizieren. Nach einer erfolgreichen Authentifizierung kann der Benutzer Remote-Befehle ausführen und Daten zwischen Hosts kopieren.

Sitzungsmerkmale in Secure Shell

Das serverseitige Verhalten des `sshd`-Dämons wird durch Schlüsselworteinstellungen in der Datei `/etc/ssh/sshd_config` gesteuert. Die Datei `sshd_config` steuert, welche Arten der Authentifizierung für den Zugriff auf den Server zulässig sind. Das serverseitige Verhalten kann auch durch Befehlszeilenoptionen gesteuert werden, wenn der `sshd`-Dämon gestartet wird.

Das clientseitige Verhalten wird durch Secure Shell-Schlüsselwörter mit folgender Prioritätsreihenfolge gesteuert:

- Befehlszeilenoptionen
- Konfigurationsdatei `~/.ssh/config` des Benutzers
- Systemweite Konfigurationsdatei `/etc/ssh/ssh_config`

Beispielsweise kann ein Benutzer eine systemweite `Ciphers`-Konfigurationseinstellung überschreiben, die `aes128–ctr` bevorzugt, indem er `-c aes256–ctr,aes128-ctr,arcfour` in der Befehlszeile angibt. Die erste Verschlüsselung, `aes256–ctr`, wird nun bevorzugt.

Authentifizierung und Schlüsselaustausch in Secure Shell

Die Secure Shell-Protokolle v1 und v2 unterstützen Client-Benutzer/Host-Authentifizierung und Server-Host-Authentifizierung. Bei beiden Protokollen werden kryptografische Sitzungsschlüssel zum Schutz von Secure Shell-Sitzungen ausgetauscht. Jedes Protokoll bietet verschiedene Methoden zur Authentifizierung und zum Austausch von Schlüsseln. Einige Methoden sind optional Secure Shell unterstützt eine Reihe von Client-Authentifizierungsmechanismen, die in Tabelle 19–1 aufgeführt werden. Server werden mithilfe von bekannten öffentlichen Hostschlüsseln authentifiziert.

In Version 1 des Protokolls unterstützt Secure Shell Benutzerauthentifizierung mit Passwörtern. Das Protokoll unterstützt außerdem öffentliche Benutzerschlüssel und die Authentifizierung mit öffentlichen Schlüsseln vertrauenswürdiger Hosts. Die Serverauthentifizierung erfolgt mit einem öffentlichen Hostschlüssel. In Version 1 des Protokolls sind alle öffentlichen Schlüssel RSA-Schlüssel. Um Sitzungsschlüssel auszutauschen, wird ein temporärer Serverschlüssel benötigt, der regelmäßig neu generiert wird.

In Version 2 des Protokolls unterstützt Secure Shell die Benutzerauthentifizierung und eine generische interaktive Authentifizierung, die normalerweise Passwörter umfasst. Das Protokoll unterstützt außerdem die Authentifizierung mit öffentlichen Benutzerschlüsseln und öffentlichen Schlüsseln vertrauenswürdiger Hosts. Bei den Schlüsseln kann es sich um RSA- oder DSA-Schlüssel handeln. Der Austausch von Sitzungsschlüsseln besteht darin, dass temporäre Diffie-Hellman-Schlüssel ausgetauscht werden, die bei der Serverauthentifizierung signiert werden. Außerdem kann Secure Shell GSS-Berechtigungsnachweise zur Authentifizierung verwenden.

Erhalt von GSS-Berechtigungsnachweisen in Secure Shell

Um die GSS-API zur Authentifizierung in Secure Shell zu verwenden, muss der Server über GSS-API-Verarbeiter-Berechtigungsnachweise und der Client über GSS-API-Initiator-Berechtigungsnachweise verfügen. Unterstützt werden `mech_dh` und `mech_krb5`.

Für `mech_dh` verfügt der Server über GSS-API-Verarbeiter-Berechtigungsnachweise, wenn `root` den Befehl `keylogin` ausgeführt hat.

Für `mech_krb5` verfügt der Server über GSS-API-Verarbeiter-Berechtigungsnachweise, wenn das Host-Hauptelement, das dem Server entspricht, über einen gültigen Eintrag in `/etc/krb5/krb5.keytab` verfügt.

Der Client verfügt über Initiator-Berechtigungsnachweise für `mech_dh`, wenn eine der folgenden Aktionen ausgeführt wurde:

- Der Befehl `keylogin` wurde ausgeführt.
- Das Modul `pam_dhkeys` wird in der Datei `pam.conf` verwendet.

Der Client verfügt über Initiator-Berechtigungsnachweise für `mech_krb5`, wenn eine der folgenden Aktionen ausgeführt wurde:

- Der Befehl `kinit` wurde ausgeführt.
- Das Modul `pam_krb5` wird in der Datei `pam.conf` verwendet.

Informationen zur Verwendung von `mech_dh` in Secure RPC finden Sie unter Kapitel 16, „Verwenden von Authentifizierungsservices (Aufgaben)“. Informationen zur Verwendung von `mech_krb5` finden Sie in Kapitel 21, „Einführung zum Kerberos-Service“. Weitere Informationen zu Mechanismen finden Sie auf den Manpages `mech(4)` und `mech_spnego(5)`.

Befehlsausführung und Datenweiterleitung in Secure Shell

Nachdem die Authentifizierung abgeschlossen ist, kann der Benutzer Secure Shell verwenden, normalerweise durch Anfordern einer Shell oder Ausführen eines Befehls. Mithilfe der `ssh`-Befehlsoptionen kann der Benutzer Anforderungen stellen. Zu den Anforderungen kann die Zuordnung einer Pseudo-TTY, die Weiterleitung von X11-Verbindungen oder TCP/IP-Verbindungen oder das Aktivieren eines `ssh-agent`-Authentifizierungsprogramms über eine sichere Verbindung gehören.

Eine Benutzersitzung besteht aus folgenden grundlegenden Komponenten:

1. Der Benutzer fordert eine Shell oder die Ausführung eines Befehls an, wodurch der Sitzungsmodus gestartet wird.

   In diesem Modus sendet oder empfängt das Client-Terminal Daten. Der Server sendet Daten über die Shell oder mithilfe eines Befehls.

2. Wenn die Datenübertragung abgeschlossen ist, wird das Benutzerprogramm geschlossen.
3. Jegliche X11- und TCP/IP-Weiterleitung wird beendet, ausgenommen für die bereits vorhandenen Verbindungen. Vorhandene X11- und TCP/IP-Verbindungen bleiben geöffnet.
4. Der Server sendet eine Statusmeldung an den Client. Wenn alle Verbindungen, wie noch offene weitergeleitete Ports, geschlossen sind, trennt der Client die Verbindung zum Server. Dann wird der Client beendet.

Client- und Serverkonfiguration in Secure Shell

Die Merkmale einer Secure Shell-Sitzung werden durch Konfigurationsdateien gesteuert. Die Konfigurationsdateien können bis zu einem gewissen Grad durch Befehlszeilenoptionen überschrieben werden.

Clientkonfiguration in Secure Shell

In den meisten Fällen werden die clientseitigen Merkmale einer Secure Shell-Sitzung von der systemweiten Konfigurationsdatei `/etc/ssh/ssh_config` gesteuert. Die Einstellungen in der Datei `ssh_config` können von der Konfigurationsdatei des Benutzers, `~/.ssh/config`, überschrieben werden. Zusätzlich kann der Benutzer beide Konfigurationsdateien über die Befehlszeile überschreiben.

Die Einstellungen in der Datei `/etc/ssh/sshd_config` auf dem Server bestimmen, welche Clientanforderungen vom Server zugelassen werden. Eine Liste der Serverkonfigurationseinstellungen finden Sie unter „Schlüsselwörter in Secure Shell“ auf Seite 393. Ausführliche Informationen finden Sie auf der Manpage `sshd_config(4)`.

Die Schlüsselwörter in der Clientkonfigurationsdatei werden unter „Schlüsselwörter in Secure Shell“ auf Seite 393 aufgeführt. Wenn das Schlüsselwort über einen Standardwert verfügt, wird der Wert angegeben. Diese Schlüsselwörter werden ausführlich auf den Manpages `ssh(1)`, `scp(1)`, `sftp(1)` und `ssh_config(4)` beschrieben. Eine Liste der Schlüsselwörter in alphabetischer Reihenfolge und der entsprechenden Befehlszeilenüberschreibungen finden Sie in Tabelle 20–8.

Serverkonfiguration in Secure Shell

Die serverseitigen Merkmale einer Secure Shell-Sitzung werden von der Datei `/etc/ssh/sshd_config` gesteuert. Die Schlüsselwörter in der Serverkonfigurationsdatei werden unter „Schlüsselwörter in Secure Shell“ auf Seite 393 aufgeführt. Wenn das Schlüsselwort über einen Standardwert verfügt, wird der Wert angegeben. Eine vollständige Beschreibung der Schlüsselwörter finden Sie auf der Manpage `sshd_config(4)`.

Schlüsselwörter in Secure Shell

In der folgenden Tabelle werden die Schlüsselwörter und, falls vorhanden, ihre Standardwerte angegeben. Die Schlüsselwörter sind alphabetisch geordnet. Sie befinden sich auf dem Client in der Datei `ssh_config`. Schlüsselwörter für den Server befinden sich in der Datei `sshd_config`. Einige Schlüsselwörter sind in beiden Dateien enthalten. Wenn ein Schlüsselwort nur für eine Version des Protokolls anwendbar ist, wird die Version angegeben.

TABELLE 20–1 Schlüsselwörter in Secure Shell-Konfigurationsdateien (A bis Escape)

Schlüsselwort	Standardwert	Speicherort	Protokoll
`AllowGroups`	Kein Standardwert	Server	
`AllowTcpForwarding`	`yes`	Server	
`AllowUsers`	Kein Standardwert	Server	
`AuthorizedKeysFile`	`~/.ssh/authorized_keys`	Server	
`Banner`	`/etc/issue`	Server	
`Batchmode`	`no`	Client	
`BindAddress`	Kein Standardwert	Client	
`CheckHostIP`	`yes`	Client	
`ChrootDirectory`	`no`	Server	v2
`Cipher`	`blowfish`, `3des`	Client	v1
`Ciphers`	`aes128-ctr, aes128-cbc, 3des-cbc, blowfish-cbc, arcfour`	Beide	v2
`ClearAllForwardings`	`no`	Client	
`ClientAliveCountMax`	`3`	Server	v2
`ClientAliveInterval`	`0`	Server	v2
`Compression`	`no`	Beide	
`CompressionLevel`	Kein Standardwert	Client	v1
`ConnectionAttempts`	`1`	Client	
`DenyGroups`	Kein Standardwert	Server	
`DenyUsers`	Kein Standardwert	Server	
`DynamicForward`	Kein Standardwert	Client	
`EscapeChar`	`~`	Client	

TABELLE 20–2 Schlüsselwörter in Secure Shell-Konfigurationsdateien (Fall bis Local)

Schlüsselwort	Standardwert	Speicherort	Protokoll
`FallBackToRsh`	`no`	Client	
`ForwardAgent`	`no`	Client	
`ForwardX11`	`no`	Client	
`GatewayPorts`	`no`	Beide	
`GlobalKnownHostsFile`	`/etc/ssh/ssh_known_hosts`	Client	
`GSSAPIAuthentication`	`yes`	Beide	v2
`GSSAPIDelegateCredentials`	`no`	Client	v2
`GSSAPIKeyExchange`	`yes`	Beide	v2
`GSSAPIStoreDelegateCredentials`	`yes`	Server	v2
`Host`	* Weitere Informationen finden Sie unter „Hostspezifische Parameter in Secure Shell“ auf Seite 396.	Client	
`HostbasedAuthentication`	`no`	Beide	v2
`HostbasedUsesNameFromPacketOnly`	`no`	Server	v2
`HostKey`	`/etc/ssh/ssh_host_key`	Server	v1
`HostKey`	`/etc/ssh/host_rsa_key`, `/etc/ssh/host_dsa_key`	Server	v2
`HostKeyAlgorithms`	`ssh-rsa, ssh-dss`	Client	v2
`HostKeyAlias`	Kein Standardwert	Client	v2
`HostName`	Kein Standardwert	Client	v2
`IdentityFile`	`~/.ssh/identity`	Client	v1
`IdentityFile`	`~/.ssh/id_dsa, ~/.ssh/id_rsa`	Client	v2
`IgnoreRhosts`	`yes`	Server	
`IgnoreUserKnownHosts`	`yes`	Server	
`KbdInteractiveAuthentication`	`yes`	Beide	
`KeepAlive`	`yes`	Beide	
`KeyRegenerationInterval`	`3600` (Sekunden)	Server	
`ListenAddress`	Kein Standardwert	Server	

TABELLE 20–2 Schlüsselwörter in Secure Shell-Konfigurationsdateien (Fall bis Local) *(Fortsetzung)*

Schlüsselwort	Standardwert	Speicherort	Protokoll
`LocalForward`	Kein Standardwert	Client	

TABELLE 20–3 Schlüsselwörter in Secure Shell-Konfigurationsdateien (Login bis R)

Schlüsselwort	Standardwert	Speicherort	Protokoll
`LoginGraceTime`	`600` (Sekunden)	Server	
`LogLevel`	`info`	Beide	
`LookupClientHostnames`	`yes`	Server	
`MACs`	`hmac-sha1,hmac-md5`	Beide	v2
`MaxAuthTries`	`6`	Server	
`MaxAuthTriesLog`	3	Server	
`MaxStartups`	`10:30:60`	Server	
`NoHostAuthenticationForLocalHost`	`no`	Client	
`NumberOfPasswordPrompts`	`3`	Client	
`PAMAuthenticationViaKBDInt`	`yes`	Server	v2
`PasswordAuthentication`	`yes`	Beide	Beide
`PermitEmptyPasswords`	`no`	Server	
`PermitRootLogin`	`no`	Server	
`PermitUserEnvironment`	`no`	Server	
`PidFile`	`/var/run/sshd.pid`	Server	
`Port`	`22`	Beide	
`PreferredAuthentications`	`hostbased,publickey,keyboard-interactive,passwor`	Client	v2
`PrintLastLog`	`yes`	Server	v2
`PrintMotd`	`no`	Server	
`Protocol`	`2,1`	Beide	
`ProxyCommand`	Kein Standardwert	Client	
`PubkeyAuthentication`	`yes`	Beide	v2
`RemoteForward`	Kein Standardwert	Client	

TABELLE 20–3 Schlüsselwörter in Secure Shell-Konfigurationsdateien (Login bis R) *(Fortsetzung)*

Schlüsselwort	Standardwert	Speicherort	Protokoll
`RhostsAuthentication`	`no`	Beide	v1
`RhostsRSAAuthentication`	`no`	Beide	v1
`RSAAuthentication`	`no`	Beide	v1

TABELLE 20–4 Schlüsselwörter in Secure Shell-Konfigurationsdateien (S bis X)

Schlüsselwort	Standardwert	Speicherort	Protokoll
`StrictHostKeyChecking`	`ask`	Client	
`StrictModes`	`yes`	Server	
`Subsystem`	`sftp /usr/lib/ssh/sftp-server`	Server	
`SyslogFacility`	`auth`	Server	
`UseLogin`	`no` (veraltet und ignoriert)	Server	
`UseOpenSSLEngine`	`yes`	Beide	v2
`UsePrivilegedPort`	`no`	Beide	v2
`User`	Kein Standardwert	Client	
`UserKnownHostsFile`	`~/.ssh/known_hosts`	Client	
`UseRsh`	`no`	Client	
`VerifyReverseMapping`	`no`	Server	
`X11DisplayOffset`	`10`	Server	
`X11Forwarding`	`yes`	Server	
`X11UseLocalHost`	`yes`	Server	
`XAuthLocation`	`/usr/openwin/bin/xauth`	Beide	

Hostspezifische Parameter in Secure Shell

Wenn sich verschiedene Secure Shell-Merkmale für unterschiedliche lokale Hosts als nützlich erweisen, kann der Administrator unterschiedliche Gruppen von Parametern in der Datei `/etc/ssh/ssh_config` definieren, die abhängig vom Host oder entsprechend einem regulären Ausdruck angewendet werden. Dazu werden Einträge in der Datei nach `Host`-Schlüsselwort gruppiert. Wenn das `Host`-Schlüsselwort nicht verwendet wird, werden die Einträge in der Clientkonfigurationsdatei auf den lokalen Host angewendet, auf dem der Benutzer gerade arbeitet.

Secure Shell und Variablen für die Anmeldeumgebung

Wenn die folgenden Secure Shell-Schlüsselwörter in der Datei `sshd_config` nicht eingestellt sind, wird ihr Wert aus entsprechenden Einträgen in der Datei `/etc/default/login` abgeleitet:

Eintrag in `/etc/default/login`	Schlüsselwort und Wert in `sshd_config`
`CONSOLE=*`	`PermitRootLogin=without-password`
`#CONSOLE=*`	`PermitRootLogin=yes`
`PASSREQ=YES`	`PermitEmptyPasswords=no`
`PASSREQ=NO`	`PermitEmptyPasswords=yes`
`#PASSREQ`	`PermitEmptyPasswords=no`
`TIMEOUT=`*secs*	`LoginGraceTime=`*secs*
`#TIMEOUT`	`LoginGraceTime=300`
`RETRIES` und `SYSLOG_FAILED_LOGINS`	Nur auf die Authentifizierungsmethoden `password` und `keyboard-interactive` anwenden

Wenn die folgenden Variablen von den Initialisierungsskripten der Anmelde-Shell des Benutzers eingestellt werden, verwendet der `sshd`-Dämon diese Werte. Wenn die Variablen nicht eingestellt sind, verwendet der Dämon den Standardwert.

`TIMEZONE` Steuert die Einstellung der Umgebungsvariablen `TZ`. Wenn die Variable nicht eingestellt ist, verwendet der `sshd`-Dämon den Wert, den `TZ` bei seinem Start hatte.

`ALTSHELL` Steuert die Einstellung der Umgebungsvariablen `SHELL`. Der Standardwert lautet `ALTSHELL=YES`, wobei der `sshd`-Dämon den Wert der Shell des Benutzers verwendet. Bei `ALTSHELL=NO` wird der Wert für `SHELL` nicht eingestellt.

`PATH` Steuert die Einstellung der Umgebungsvariablen `PATH`. Wenn der Wert nicht eingestellt ist, lautet der Standardpfad `/usr/bin`.

`SUPATH` Steuert die Einstellung der Umgebungsvariablen `PATH` für `root`. Wenn der Wert nicht eingestellt ist, lautet der Standardpfad `/usr/sbin:/usr/bin` .

Weitere Informationen finden Sie auf den Manpages `login(1)` und `sshd(1M)`.

Verwalten bekannter Hosts in Secure Shell

Jeder Host, der mit einem anderen Host sicher kommunizieren muss, benötigt den öffentlichen Schlüssel des Servers, der in der `/etc/ssh/ssh_known_hosts`-Datei des lokalen Hosts gespeichert ist. Auch wenn ein Skript zur Aktualisierung der `/etc/ssh/ssh_known_hosts` -Dateien verwendet werden kann, wird davon nachdrücklich abgeraten, da hierdurch eine wesentliche Sicherheitsschwachstelle entstehen kann.

Die `/etc/ssh/ssh_known_hosts`-Datei sollte nur durch einen sicheren Mechanismus wie folgt verteilt werden:

- Über eine sichere Verbindung wie Secure Shell, IPsec oder kerberisiertes `ftp` von einem bekannten und vertrauenswürdigen Rechner
- Zum Zeitpunkt der Installation

Um zu vermeiden, dass sich Unberechtigte durch falsche öffentliche Schlüssel Zugriff auf eine `known_hosts`-Datei verschaffen können, sollten Sie einen JumpStart-Server als bekannte und vertrauenswürdige Quelle für die `ssh_known_hosts` -Datei verwenden. Die `ssh_known_hosts`-Datei kann während der Installation verteilt werden. Später kann die neueste Version mit Skripten, die den Befehl `scp` verwenden, abgerufen werden. Dieser Ansatz ist sicher, da jeder Host bereits über den öffentlichen Schlüssel vom JumpStart-Server verfügt.

Secure Shell-Pakete und Initialisierung

Secure Shell hängt von Solaris-Kernpaketen und folgenden Paketen ab:

- `SUNWgss`: Enthält die Software Generic Security Service (GSS)
- `SUNWtcpd`: Enthält TCP-Wrappers
- `SUNWopenssl-libraries`: Enthält OpenSSL-Bibliotheken
- `SUNWzlib`: Enthält die zip-Komprimierungsbibliothek

Secure Shell wird durch folgende Pakete installiert:

- `SUNWsshr`: Enthält Clientdateien und Dienstprogramme für das Root-Verzeichnis (`/`)
- `SUNWsshdr`: Enthält Serverdateien und Dienstprogramme für das Root-Verzeichnis (`/`)
- `SUNWsshcu`: Enthält allgemeine Quelldateien für das Verzeichnis `/usr`
- `SUNWsshdu`: Enthält Serverdateien für das Verzeichnis `/usr`
- `SUNWsshu`: Enthält Clientdateien und Dienstprogramme für das Verzeichnis `/usr`

Beim Neustart nach der Installation wird der `sshd`-Dämon ausgeführt. Der Dämon erstellt Hostschlüssel auf dem System. Ein Oracle Solaris-System, auf dem der `sshd`-Dämon ausgeführt wird, stellt einen Secure Shell-Server dar.

Secure Shell-Dateien

Die folgende Tabelle enthält die wichtigen Secure Shell-Dateien und vorgeschlagene Dateiberechtigungen.

TABELLE 20–5 Secure Shell-Dateien

Dateiname	Description (Beschreibung)	Vorgeschlagene Berechtigungen und Eigentümer
`/etc/ssh/sshd_config`	Enthält Konfigurationsdaten für `sshd`, den Secure Shell-Dämon	`-rw-r--r-- root`
`/etc/ssh/ssh_host_key`	Enthält den privaten Hostschlüssel (v1)	`-rw------- root`
`/etc/ssh/ssh_host_dsa_key` oder `/etc/ssh/ssh_host_rsa_key`	Enthält den privaten Hostschlüssel (v2)	`-rw------- root`
host-private-key `.pub`	Enthält den öffentlichen Hostschlüssel, beispielsweise `/etc/ssh/ssh_host_rsa_key.pub`. Wird zum Kopieren des Hostschlüssels in die lokale Datei `known_hosts` verwendet	`-rw-r--r-- root`
`/var/run/sshd.pid`	Enthält die Prozess-ID des Secure Shell-Dämons `sshd`. Wenn mehrere Dämonen ausgeführt werden, enthält die Datei den zuletzt gestarteten Dämon.	`-rw-r--r-- root`
`~/.ssh/authorized_keys`	Enthält die öffentlichen Schlüssel des Benutzers, der sich bei dem Benutzerkonto anmelden darf	`-rw-r--r--` *username*
`/etc/ssh/ssh_known_hosts`	Enthält die öffentlichen Hostschlüssel der Hosts, mit denen der Client sicher kommunizieren kann. Die Daten in der Datei werden vom Administrator eingegeben.	`-rw-r--r-- root`
`~/.ssh/known_hosts`	Enthält die öffentlichen Hostschlüssel der Hosts, mit denen der Client sicher kommunizieren kann. Die Datei wird automatisch verwaltet. Sobald ein Benutzer eine Verbindung mit einem unbekannten Host herstellt, wird der Remote-Hostschlüssel der Datei hinzugefügt.	`-rw-r--r--` *username*
`/etc/default/login`	Enthält Standardwerte, die vom `sshd`-Dämon verwendet werden, wenn die entsprechenden `sshd_config`-Parameter nicht eingestellt sind	`-r--r--r-- root`
`/etc/nologin`	Wenn diese Datei vorhanden ist, lässt der `sshd`-Dämon nur eine Anmeldung durch den `root`-Benutzer zu. Der Inhalt dieser Datei wird Benutzern angezeigt, die versuchen, sich anzumelden.	`-rw-r--r-- root`
`~/.rhosts`	Enthält Paare aus Host- und Benutzernamen, die die Hosts angeben, bei denen sich der Benutzer ohne Passwort anmelden kann. Diese Datei wird auch von den Dämonen `rlogind` und `rshd` verwendet.	`-rw-r--r--` *username*

TABELLE 20–5 Secure Shell-Dateien *(Fortsetzung)*

Dateiname	Description (Beschreibung)	Vorgeschlagene Berechtigungen und Eigentümer
`~/.shosts`	Enthält Paare aus Host- und Benutzernamen, die die Hosts angeben, bei denen sich der Benutzer ohne Passwort anmelden kann. Diese Datei wird nicht von anderen Dienstprogrammen verwendet. Weitere Informationen finden Sie auf der Manpage `sshd(1M)` im Abschnitt `FILES`.	`-rw-r--r--` *username*
`/etc/hosts.equiv`	Enthält die Hosts, die bei der `.rhosts`-Authentifizierung verwendet werden. Diese Datei wird auch von den Dämonen `rlogind` und `rshd` verwendet.	`-rw-r--r-- root`
`/etc/ssh/shosts.equiv`	Enthält die Hosts, die bei einer hostbasierten Authentifizierung verwendet werden. Diese Datei wird nicht von anderen Dienstprogrammen verwendet.	`-rw-r--r-- root`
`~/.ssh/environment`	Enthält die anfänglichen Zuweisungen bei der Anmeldung. Diese Datei wird standardmäßig nicht gelesen. Damit sie gelesen wird, muss das Schlüsselwort `PermitUserEnvironment` in der Datei `sshd_config` auf `yes` eingestellt werden.	`-rw-r--r--` *username*
`~/.ssh/rc`	Enthält Initialisierungsroutinen, die vor dem Start der Benutzer-Shell ausgeführt werden. Ein Beispiel für eine Initialisierungsroutine finden Sie auf der Manpage `sshd(1M)`.	`-rw-r--r--` *username*
`/etc/ssh/sshrc`	Enthält hostspezifische Initialisierungsroutinen, die vom Administrator definiert werden	`-rw-r--r-- root`
`/etc/ssh/ssh_config`	Konfiguriert die Systemeinstellungen auf dem Clientsystem	`-rw-r--r-- root`
`~/.ssh/config`	Konfiguriert Benutzereinstellungen. Überschreibt Systemeinstellungen	`-rw-r--r--` *username*

In der folgenden Tabelle werden Secure Shell-Dateien aufgeführt, die durch Schlüsselwörter oder Befehlsoptionen überschrieben werden können.

TABELLE 20–6 Überschreibungen für die Position der Secure Shell-Dateien

Dateiname	Schlüsselwortüberschreibung	Befehlszeilenüberschreibung
`/etc/ssh/ssh_config`		`ssh -F` *config-file* `scp -F` *config-file*
`~/.ssh/config`		`ssh -F` *config-file*
`/etc/ssh/host_rsa_key` `/etc/ssh/host_dsa_key`	`HostKey`	

TABELLE 20–6 Überschreibungen für die Position der Secure Shell-Dateien *(Fortsetzung)*

Dateiname	Schlüsselwortüberschreibung	Befehlszeilenüberschreibung
`~/.ssh/identity`	`IdentityFile`	`ssh -i` *id-file*
`~/.ssh/id_dsa`, `~/.ssh/id_rsa`		`scp -i` *id-file*
`~/.ssh/authorized_keys`	`AuthorizedKeysFile`	
`/etc/ssh/ssh_known_hosts`	`GlobalKnownHostsFile`	
`~/.ssh/known_hosts`	`UserKnownHostsFile`	
	`IgnoreUserKnownHosts`	

Secure Shell-Befehle

In der folgenden Tabelle werden die wichtigsten Secure Shell-Befehle zusammengefasst.

TABELLE 20–7 Befehle in Secure Shell

Befehl	Beschreibung	Manpage
`ssh`	Meldet einen Benutzer bei einem Remote-Rechner an und führt Befehle auf einem Remote-Rechner sicher aus. Dieser Befehl in Secure Shell ist ein Ersatz für `rlogin` und `rsh`. Der Befehl `ssh` ermöglicht eine sichere, verschlüsselte Kommunikation zwischen zwei nicht vertrauenswürdigen Hosts über ein unsicheres Netzwerk. X11-Verbindungen und willkürliche TCP/IP-Ports können auch über den sicheren Kanal weitergeleitet werden.	`ssh(1)`
`sshd`	Secure Shell-Dämon. Dieser Dämon wartet auf Verbindungen von Clients und ermöglicht eine sichere, verschlüsselte Kommunikation zwischen zwei nicht vertrauenswürdigen Hosts über ein unsicheres Netzwerk.	`sshd(1M)`
`ssh-add`	Fügt dem Authentifizierungsagenten `ssh-agent` RSA- oder DSA-Identitäten hinzu. Die Identitäten werden auch als *Schlüssel* bezeichnet.	`ssh-add(1)`
`ssh-agent`	Enthält private Schlüssel, die zur Authentifizierung öffentlicher Schlüssel verwendet werden. Das Programm `ssh-agent` wird zu Beginn einer X- oder Anmeldesitzung gestartet. Alle anderen Fenster und Programme werden als Clients des Programms `ssh-agent` gestartet. Mithilfe von Umgebungsvariablen kann der Agent gefunden und zur Authentifizierung verwendet werden, wenn Benutzer den Befehl `ssh` zur Anmeldung bei anderen Systemen verwenden.	`ssh-agent(1)`
`ssh-keygen`	Generiert und verwaltet Authentifizierungsschlüssel für Secure Shell	`ssh-keygen(1)`
`ssh-keyscan`	Sammelt die öffentlichen Schlüssel von mehreren Secure Shell-Hosts. Hilft bei der Erstellung und Überprüfung von `ssh_known_hosts`-Dateien.	`ssh-keyscan(1)`

TABELLE 20–7 Befehle in Secure Shell *(Fortsetzung)*

Befehl	Beschreibung	Manpage
`ssh-keysign`	Wird vom Befehl `ssh` für den Zugriff auf Hostschlüssel auf dem lokalen Host verwendet. Generiert die digitale Signatur, die bei einer hostbasierten Authentifizierung mit Secure Shell v2 benötigt wird. Der Befehl wird vom Befehl `ssh` aufgerufen und nicht vom Benutzer.	`ssh-keysign`(1M)
`scp`	Kopiert die Dateien zwischen Hosts in einem Netzwerk sicher durch eine verschlüsselte `ssh`-Übertragung. Im Unterschied zum Befehl `rcp` fordert der Befehl `scp` zur Eingabe von Passwörtern oder Passwortsätzen auf, wenn Passwörter für die Authentifizierung benötigt werden.	`scp`(1)
`sftp`	Ein interaktives Dateiübertragungsprogramm, das dem Befehl `ftp` ähnlich ist. Im Unterschied zum Befehl `ftp` führt der Befehl `sftp` alle Vorgänge mithilfe einer verschlüsselten `ssh`-Übertragung durch. Mit dem Befehl stellen Sie eine Verbindung zu dem angegebenen Host her, melden sich an und wechseln in den interaktiven Befehlsmodus.	`sftp`(1)

Die folgende Tabelle enthält die Befehlsoptionen zum Überschreiben von Secure Shell-Schlüsselwörtern. Die Schlüsselwörter werden in den Dateien `ssh_config` und `sshd_config` angegeben.

TABELLE 20–8 Befehlszeilenäquivalente für Secure Shell

Schlüsselwort	ssh-Befehlszeilenüberschreibung	scp-Befehlszeilenüberschreibung
`BatchMode`		`scp -B`
`BindAddress`	`ssh -b` *bind-addr*	`scp -a` *bind-addr*
`Cipher`	`ssh -c` *cipher*	`scp -c` *cipher*
`Ciphers`	`ssh -c` *cipher-spec*	`scp -c` *cipher-spec*
`Compression`	`ssh -C`	`scp -C`
`DynamicForward`	`ssh -D` *SOCKS4-port*	
`EscapeChar`	`ssh -e` *escape-char*	
`ForwardAgent`	`ssh -A` zum Aktivieren `ssh -a` zum Deaktivieren	
`ForwardX11`	`ssh -X` zum Aktivieren `ssh -x` zum Deaktivieren	
`GatewayPorts`	`ssh -g`	
`IPv4`	`ssh -4`	`scp -4`

TABELLE 20–8 Befehlszeilenäquivalente für Secure Shell *(Fortsetzung)*

Schlüsselwort	ssh-Befehlszeilenüberschreibung	scp-Befehlszeilenüberschreibung
`IPv6`	`ssh -6`	`scp -6`
`LocalForward`	`ssh -L` *localport:remotehost:remoteport*	
`MACS`	`ssh -m` *mac-spec*	
`Port`	`ssh -p` *port*	`scp -P` *port*
`Protokoll`	`ssh -1` nur für v1 `ssh -2` nur für v2	
`RemoteForward`	`ssh -R` *remoteport:localhost:localport*	

TEIL VI

Kerberos-Service

Dieser Abschnitt enthält Informationen über die Konfiguration, Verwaltung und Verwendung des Kerberos-Service in folgenden Kapiteln:

- Kapitel 21, „Einführung zum Kerberos-Service“
- Kapitel 22, „Planen des Kerberos-Service“
- Kapitel 23, „Konfigurieren des Kerberos-Service (Aufgaben)“
- Kapitel 24, „Kerberos-Fehlermeldungen und -Fehlerbehebung“
- Kapitel 25, „Verwalten von Kerberos-Hauptelementen und Richtlinien (Aufgaben)“
- Kapitel 26, „Verwenden von Kerberos-Anwendungen (Aufgaben)“
- Kapitel 27, „Der Kerberos-Service (Referenz)“

◆ ◆ ◆ KAPITEL 21

Einführung zum Kerberos-Service

Dieses Kapitel bietet eine Einführung zum Kerberos-Service. Im Folgenden ist eine Übersicht der Informationen in diesem Kapitel aufgeführt.

- „Allgemeine Informationen zum Kerberos-Service“ auf Seite 407
- „Funktionsweise des Kerberos-Service“ auf Seite 408
- „Kerberos-Sicherheitsservices“ auf Seite 415
- „Die Komponenten verschiedener Kerberos-Versionen“ auf Seite 416

Allgemeine Informationen zum Kerberos-Service

Der *Kerberos-Service* stellt eine Client-Server-Architektur dar, die sichere Netzwerktransaktionen ermöglicht. Der Service bietet starke Benutzerauthentifizierung sowie Integrität und Vertraulichkeit. Durch die *Authentifizierung* wird die Echtheit sowohl der Identität des Senders als auch der des Empfängers einer Netzwerktransaktion gewährleistet. Dieser Service kann auch die Gültigkeit zurück- und weitergesendeter Daten überprüfen (*Integrität*) und die Daten während der Übertragung verschlüsseln (*Vertraulichkeit*). Mit dem Kerberos-Service können Sie sich sicher bei anderen Rechnern anmelden, Befehle ausführen, Daten austauschen und Dateien übertragen. Außerdem bietet der Service *Autorisierungsservices*, die es Administratoren ermöglichen, den Zugriff auf Services und Rechner einzuschränken. Überdies können Sie als Kerberos-Benutzer den Zugriff anderer Personen auf Ihr Konto regulieren.

Der Kerberos-Service ist ein *Single Sign-On*-System, d. h. Sie müssen sich nur einmal pro Sitzung beim Service authentifizieren und alle während der Sitzung folgenden Transaktionen werden automatisch gesichert. Nachdem Sie der Service authentifiziert hat, müssen Sie sich nicht jedes Mal neu authentifizieren, wenn Sie einen Kerberos-basierten Befehl wie z. B. `ftp` oder `rsh` verwenden oder wenn Sie auf ein NFS-Dateisystem zugreifen möchten. Demzufolge müssen Sie Ihr Passwort nicht bei jeder Verwendung dieser Services über das Netzwerk versenden, wo es abgefangen werden kann.

Der Oracle Solaris Kerberos-Service basiert auf dem Kerberos V5-Netzwerkauthentifizierungsprotokoll, das am MIT (Massachusetts Institute of Technology) entwickelt wurde. Personen, die das Kerberos V5-Produkt verwendet haben, sollte die Oracle Solaris-Version daher bekannt vorkommen. Da es sich beim Kerberos V5-Protokoll *de facto* um einen Industriestandard für Netzwerksicherheit handelt, bietet die Oracle Solaris-Version Interoperabilität mit anderen Systemen. In anderen Worten ermöglicht der Oracle Solaris Kerberos-Service sichere Transaktionen auch über heterogene Netzwerke, da er mit Systemen arbeitet, die das Kerberos V5-Protokoll verwenden. Darüber hinaus bietet der Service Authentifizierung und Sicherheit sowohl zwischen Domains als auch innerhalb einer einzelnen Domain.

Der Kerberos-Service bietet Flexibilität bei der Ausführung von Oracle Solaris-Anwendungen. Sie können den Service so konfigurieren, dass er sowohl Kerberos-basierte als auch andere Anforderungen für Netzwerkdienste wie beispielsweise den NFS-Service, `telnet` und `ftp` ermöglicht. Infolgedessen laufen aktuelle Anwendungen weiterhin, auch wenn sie auf Systemen ausgeführt werden, auf denen der Kerberos-Service nicht aktiviert ist. Selbstverständlich können Sie den Kerberos-Service auch so konfigurieren, dass er nur Kerberos-basierte Netzwerkanforderungen ermöglicht.

Der Kerberos-Service bietet einen Sicherheitsmechanismus, der die Verwendung von Kerberos für die Authentifizierung, Integrität und Vertraulichkeit ermöglicht, wenn Sie mit Anwendungen arbeiten, die die GSS-API (Generic Security Service Application Programming Interface) verwenden. Dennoch sind Anwendungen nicht an den Kerberos-Service gebunden, wenn andere Sicherheitsmechanismen entwickelt werden. Da der Service so ausgelegt ist, dass er sich modular in die GSS-API integrieren lässt, können Anwendungen, die die GSS-API verwenden, je nach Anforderungen einen beliebigen Sicherheitsmechanismus verwenden.

Funktionsweise des Kerberos-Service

Im Folgenden ist eine Übersicht des Kerberos-Authentifizierungssystems aufgeführt. Eine detailliertere Beschreibung finden Sie unter „Funktionsweise des Kerberos-Authentifizierungssystems“ auf Seite 598.

Für den Benutzer ist der Kerberos-Service nach dem Starten der Kerberos-Sitzung weitgehend unsichtbar. Bei Befehlen wie `rsh` oder `ftp` verhält es sich ähnlich. Das Initialisieren einer Kerberos-Sitzung umfasst häufig nur eine Anmeldung und die Angabe eines Kerberos-Passworts.

Das Konzept eines *Tickets* bildet den Mittelpunkt des Kerberos-Systems. Bei einem Ticket handelt es sich um einen Satz elektronischer Informationen, die einen Benutzer oder einen Service wie z. B. den NFS-Service identifizieren. Ein Ticket identifiziert Sie und Ihre Netzwerkzugriffsberechtigungen. Dies ist vergleichbar mit einem Führerschein, der Sie ebenfalls identifiziert und angibt, welche Fahrzeuge Sie fahren dürfen. Beim Ausführen einer Kerberos-basierten Transaktion (beispielsweise einer Remote-Anmeldung bei einem anderen

Rechner) senden Sie transparent eine Anforderung für ein Ticket an ein *Key Distribution Center* oder KDC. Das KDC greift auf eine Datenbank zu, um Ihre Identität zu authentifizieren, und gibt ein Ticket zurück, das Sie für den Zugriff auf den anderen Rechner berechtigt. "Transparent" bedeutet, dass Sie ein Ticket nicht explizit anfordern müssen. Die Anforderung erfolgt über den Befehl `rlogin`. Da nur ein authentifizierter Client ein Ticket für einen bestimmten Service erhalten kann, kann kein anderer Benutzer `rlogin` unter einer angenommenen Identität verwenden.

Tickets sind bestimmte Attribute zugewiesen. Ein Ticket kann beispielsweise *weiterleitbar* sein, d. h. es kann auf einem anderen Rechner verwendet werden, ohne dass ein neuer Authentifizierungsvorgang erforderlich ist. Ebenfalls kann ein Ticket *nachdatiert* sein, was bedeutet, dass es erst nach einer bestimmten Zeit gültig ist. Die Art der Verwendung von Tickets (beispielsweise zur Angabe, welche Benutzer welche Arten von Tickets erhalten dürfen) wird von *Richtlinien* bestimmt. Richtlinien werden bei der Installation oder Verwaltung des Kerberos-Service festgelegt.

Hinweis – Die Begriffe *Berechtigungsnachweis* und *Ticket* kommen im Folgenden sehr häufig vor. In Bezug auf Kerberos werden diese Begriffe häufig synonym verwendet. Technisch gesehen entspricht ein Berechtigungsnachweis jedoch einem Ticket und dem *Sitzungsschlüssel* für die entsprechende Sitzung. Dieser Unterschied wird unter „Erhalten von Zugriff auf einen Service mit Kerberos“ auf Seite 598 im Detail erläutert.

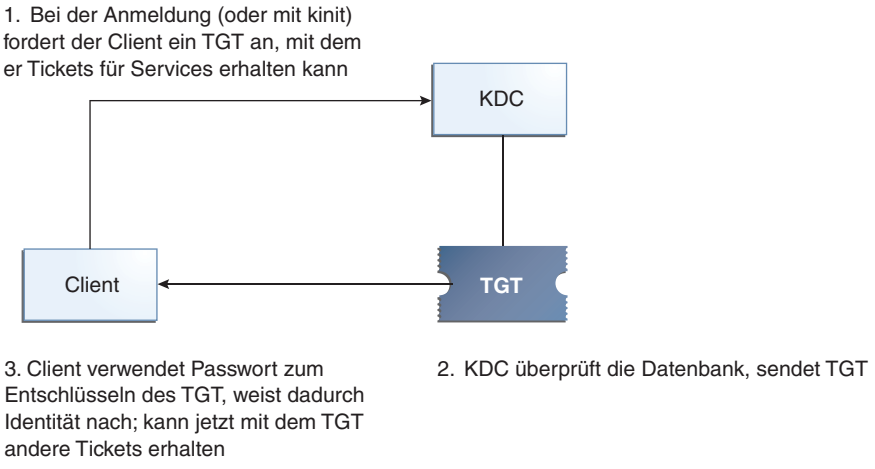
In den folgenden Abschnitten wird näher auf den Kerberos-Authentifizierungsprozess eingegangen.

Erstauthentifizierung: das Ticket-gewährende Ticket

Die Kerberos-Authentifizierung umfasst zwei Phasen: eine Erstauthentifizierung, die alle nachfolgenden Authentifizierungen ermöglicht, und die nachfolgenden Authentifizierungen selbst.

Die folgende Abbildung zeigt den Vorgang der Erstauthentifizierung.

ABBILDUNG 21–1 Erstauthentifizierung für eine Kerberos-Sitzung



TGT = Ticket-gewährendes Ticket (Ticket-Granting Ticket)
KDC = Key Distribution Center

1. Ein Client (ein Benutzer oder ein Service wie NFS) beginnt eine Kerberos-Session durch Anfordern eines *Ticket-gewährenden Tickets* (TGT) vom Key Distribution Center (KDC). Diese Anforderung erfolgt häufig automatisch bei der Anmeldung.

   Ein Ticket-gewährendes Ticket ist erforderlich, um andere Tickets für bestimmte Services zu erhalten. Das Ticket-gewährende Ticket lässt sich mit einem Pass vergleichen. Wie ein Pass identifiziert das Ticket-gewährende Ticket Sie und ermöglicht Ihnen, zahlreiche "Visa" zu erhalten, wobei die "Visa" (Tickets) hier nicht für andere Länder, sondern für Remote-Rechner oder Netzwerkdienste bestimmt sind. Ebenso wie Pässe und Visa sind das Ticket-gewährende Ticket und die anderen Tickets nur für eine begrenzte Zeit gültig. Der Unterschied besteht darin, dass "kerberisierte" Befehle erkennen, dass Sie über einen Pass verfügen, und die Visa für Sie besorgen. Sie müssen die Transaktionen nicht selbst ausführen.

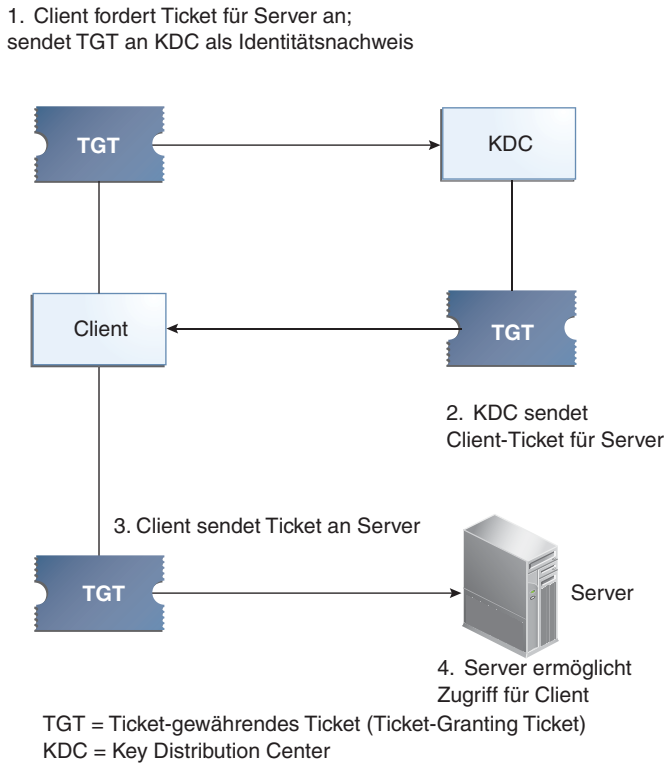
   Weiterhin ist das Ticket-gewährende Ticket mit einem dreitägigen Skipass vergleichbar, der für vier verschiedene Skistationen gültig ist. Sie zeigen den Pass bei einer der Skistationen vor und erhalten für diese Station ein Liftticket, solange der Pass noch nicht abgelaufen ist. Sobald Sie das Liftticket erhalten haben, können Sie diese Station zum Skifahren nutzen. Wenn Sie am nächsten Tag zu einer anderen Skistation gehen und dort erneut Ihren Pass vorzeigen, bekommen Sie ein weiteres Liftticket für jene Station. Der Unterschied liegt darin, dass die Kerberos-basierten Befehle erkennen, dass Sie über einen Wochenend-Skipass verfügen, und das Liftticket für Sie besorgen. Dies bedeutet abermals, dass Sie die Transaktionen nicht selbst ausführen müssen.
2. Das KDC erstellt ein Ticket-gewährendes Ticket und sendet es in verschlüsselter Form an den Client zurück. Der Client entschlüsselt das Ticket-gewährende Ticket unter Verwendung des Passworts des Clients.

3. Da der Client jetzt über ein Ticket-gewährendes Ticket verfügt, kann er Tickets für alle Arten von Netzwerkvorgängen wie etwa `rlogin` oder `telnet` anfordern, bis das Ticket-gewährende Ticket abläuft. Die Lebensdauer dieses Tickets beträgt normalerweise ein paar Stunden. Jedes Mal, wenn der Client einen eindeutigen Netzwerkvorgang ausführt, fordert er ein Ticket für diesen Vorgang vom KDC an.

Nachfolgende Kerberos-Authentifizierungen

Nachdem der Client die Erstauthentifizierung erhalten hat, läuft jede nachfolgende Authentifizierung nach dem in der folgenden Abbildung dargestellten Muster ab.

ABBILDUNG 21–2 Erhalten von Zugriff auf einen Service mit Kerberos-Authentifizierung



1. Der Client fordert vom KDC ein Ticket für einen bestimmten Service an, um z. B. entfernt auf einen anderen Rechner zuzugreifen, indem er sein Ticket-gewährendes Ticket als Identitätsnachweis an das KDC sendet.
2. Das KDC sendet das Ticket für den bestimmten Service an den Client zurück.

Beispiel: Der Benutzer `joe` möchte auf ein freigegebenes NFS-Dateisystem zugreifen, für das `krb5`-Authentifizierung erforderlich ist. Da er zum Zeitpunkt des Zugriffs auf die Dateien bereits authentifiziert ist (d. h. bereits über ein Ticket-gewährendes Ticket verfügt), ruft das NFS-Clientsystem automatisch und transparent ein Ticket vom KDC für den NFS-Service ab.

Beispiel: Der Benutzer `joe` verwendet `rlogin` auf dem Server `boston`. Da er bereits authentifiziert ist (d. h. bereits über ein Ticket-gewährendes Ticket verfügt), erhält er über den Befehl `rlogin` automatisch und transparent ein Ticket. Mit diesem Ticket kann er sich beliebig oft entfernt bei `boston` anmelden, bis das Ticket abläuft. Wenn `joe` sich entfernt beim Rechner `denver` anmelden möchte, erhält er ein anderes Ticket, wie in Schritt 1 beschrieben.

3. Der Client sendet das Ticket an den Server.

   Wenn der NFS-Service verwendet wird, sendet der NFS-Client das Ticket für den NFS-Service automatisch und transparent an den NFS-Server.

4. Der Server erteilt dem Client Zugriff.

Diese Schritte erwecken den Anschein, dass der Server zu keiner Zeit mit dem KDC kommuniziert. Dies tut er jedoch, indem er sich wie der erste Client beim KDC registriert. Der Einfachheit halber wurde dieser Teil ausgelassen.

Die Kerberos-Remote-Anwendungen

Die Kerberos-basierten bzw. kerberisierte Befehle, die ein Benutzer wie z. B. `joe` verwenden kann, sind Folgende:

- `ftp`
- `rcp`
- `rdist`
- `rlogin`
- `rsh`
- `ssh`
- `telnet`

Diese Anwendungen sind dieselben wie die gleichnamigen Solaris-Anwendungen. Sie wurden jedoch dahingehend erweitert, dass sie Kerberos-Hauptelemente zur Authentifizierung von Transaktionen verwenden und dadurch Kerberos-basierte Sicherheit bieten. Informationen zu Hauptelementen finden Sie unter „Kerberos-Hauptelemente“ auf Seite 413.

Weitere Informationen zu diesen Befehlen erhalten Sie unter „Kerberos-Benutzerbefehle“ auf Seite 578.

Kerberos-Hauptelemente

Ein Client im Kerberos-Service wird durch sein *Hauptelement* identifiziert. Ein Hauptelement stellt eine eindeutige Identität dar, der das KDC Tickets zuweisen kann. Bei einem Hauptelement kann es sich um einen Benutzer, wie beispielsweise `joe`, oder einen Service wie `nfs` oder `telnet` handeln.

Üblicherweise wird ein Hauptelementname in drei Komponenten aufgeteilt: den *primären Namen*, die *Instanz* und den *Bereich*. Ein typisches Kerberos-Hauptelement ist beispielsweise `joe/admin@ENG.EXAMPLE.COM`. In diesem Beispiel gilt Folgendes:

- `joe` ist der primäre Name. Der primäre Name kann wie in diesem Fall ein Benutzername oder ein Service wie z. B. `nfs` sein. Der primäre Name kann auch durch das Wort `host` dargestellt werden, was bedeutet, dass es sich bei diesem Hauptelement um ein Service-Hauptelement handelt, das verschiedene Netzwerkdienste bereitstellt (`ftp`, `rcp`, `rlogin` und so weiter).
- `admin` ist die Instanz. Bei Benutzer-Hauptelementen ist eine Instanz optional, für Service-Hauptelemente ist sie dagegen erforderlich. Beispiel: Wenn der Benutzer `joe` gelegentlich als Systemadministrator fungiert, kann er sich mithilfe von `joe/admin` von seiner üblichen Identität als Benutzer unterscheiden. Ebenso kann `joe` , wenn er über Konten auf zwei verschiedenen Hosts verfügt, zwei Hauptelementnamen mit unterschiedlichen Instanzen verwenden, z. B. `joe/denver.example.com` und `joe/boston.example.com`. Beachten Sie, dass der Kerberos-Service `joe` und `joe/admin` wie zwei vollständig verschiedene Hauptelemente behandelt.

  Bei Service-Hauptelementen ist die Instanz der voll qualifizierte Hostname. `bigmachine.eng.example.com` ist ein Beispiel für eine derartige Instanz. Der primäre Name bzw. die Instanz für dieses Beispiel könnte `ftp/bigmachine.eng.example.com` oder `host/bigmachine.eng.example.com` sein.
- `ENG.EXAMPLE.COM` ist der Kerberos-Bereich. Informationen zu Bereichen finden Sie unter „Kerberos-Bereiche“ auf Seite 413.

Folgende Namen sind gültige Hauptelementnamen:

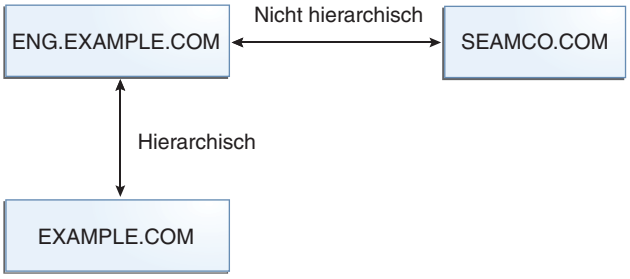
- `joe`
- `joe/admin`
- `joe/admin@ENG.EXAMPLE.COM`
- `nfs/host.eng.example.com@ENG.EXAMPLE.COM`
- `host/eng.example.com@ENG.EXAMPLE.COM`

Kerberos-Bereiche

Ein *Bereich* ist ein logisches Netzwerk (ähnlich einer Domain), das eine Gruppe von Systemen unter dem Namen *Master-KDC* definiert. Abbildung 21–3 zeigt die möglichen Beziehungen zwischen Bereichen. Einige Bereiche sind hierarchisch, wobei ein Bereich eine Obergruppe des

anderen Bereichs darstellt. Andernfalls sind die Bereiche nicht hierarchisch (oder auch "direkt") und die Zuordnung zwischen den beiden Bereichen muss definiert werden. Eine Funktion des Kerberos-Service besteht in der bereichsübergreifenden Erteilung von Authentifizierung. Jeder Bereich erfordert lediglich einen Hauptelementeintrag für den anderen Bereich im dazugehörigen KDC. Diese Kerberos-Funktion nennt sich *bereichsübergreifende Authentifizierung*.

ABBILDUNG 21–3 Kerberos-Bereiche



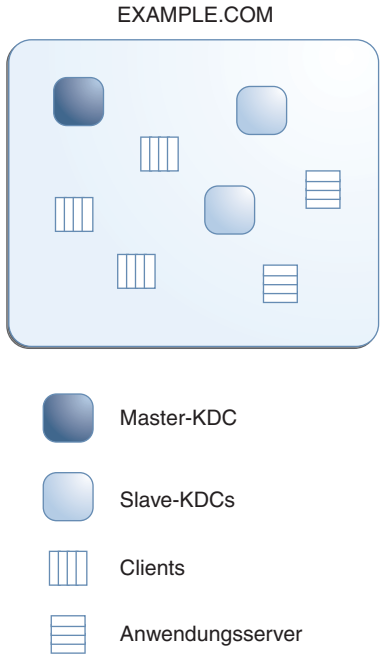
Kerberos-Server

Jeder Bereich muss einen Server zur Verwaltung der Masterkopie der Hauptelement-Datenbank umfassen. Dieser Server wird als der *Master-KDC-Server* bezeichnet. Außerdem sollte in jedem Bereich mindestens ein *Slave-KDC-Server* vorhanden sein, der doppelte Kopien der Hauptelement-Datenbank enthält. Sowohl der Master- als auch der Slave-KDC-Server erstellen Tickets zum Einrichten einer Authentifizierung.

Der Bereich kann auch einen Kerberos-*Anwendungsserver* umfassen. Dieser Server bietet Zugriff auf kerberisierte Services (wie z. B. `ftp`, `telnet`, `rsh` und NFS). Wenn Sie SEAM 1.0 oder 1.0.1 installiert haben, kann der Bereich einen Kerberos-Netzwerkanwendungsserver umfassen. Diese Software wurde jedoch nicht mit diesen Versionen mitgeliefert.

Die folgende Abbildung zeigt, was ein hypothetischer Bereich umfassen kann.

ABBILDUNG 21–4 Ein typischer Kerberos-Bereich



Kerberos-Sicherheitsservices

Zusätzlich zu der sicheren Authentifizierung von Benutzern stellt der Kerberos-Service zwei Sicherheitsservices bereit:

- **Integrität**: Ebenso, wie die Authentifizierung die richtige Identität von Clients im Netzwerk sicherstellt, gewährleistet die Integrität, dass die von den Clients gesendeten Daten gültig sind und während der Übertragung nicht manipuliert wurden. Integrität wird durch Versehen der Daten mit kryptografischen Prüfsummen erreicht. Sie schließt auch die Benutzerauthentifizierung mit ein.
- **Vertraulichkeit**: Die Vertraulichkeit stellt ein zusätzliches Maß an Sicherheit dar. Hierunter fällt nicht nur die Überprüfung der Integrität übertragener Daten, sondern auch die Verschlüsselung der Daten vor der Übertragung. Auf diese Weise werden Daten vor dem Abhören geschützt. Im Rahmen der Vertraulichkeit werden Benutzer ebenfalls authentifiziert.

Entwickler können ihre RPC-basierten Anwendungen so entwerfen, dass sie unter Verwendung der Programmierschnittstelle RPCSEC_GSS einen Sicherheitsservice auswählen.

Die Komponenten verschiedener Kerberos-Versionen

Komponenten des Kerberos-Service wurden in zahlreiche Versionen integriert. Ursprünglich wurden der Kerberos-Service sowie Änderungen, die zur Unterstützung des Kerberos-Service am Basisbetriebssystem vorgenommen wurden, unter dem Produktnamen "Sun Enterprise Authentication Mechanism" (kurz: SEAM) veröffentlicht. Da immer mehr Komponenten des SEAM-Produkts in die Oracle Solaris-Software integriert wurden, verringerte sich der Inhalt der SEAM-Version. Die Oracle Solaris-Versionen enthalten sämtliche Komponenten des SEAM-Produkts, sodass das SEAM-Produkt nicht mehr erforderlich ist. Der Name des SEAM-Produkts wird aus "historischen Gründen" in der Dokumentation verwendet.

In der folgenden Tabelle wird beschrieben, welche Komponenten in den einzelnen Versionen des Produkts enthalten sind. Die Versionen werden in chronologischer Reihenfolge aufgeführt. Sämtliche Komponenten werden in den nachfolgenden Abschnitten beschrieben.

TABELLE 21–1 Inhalt der Kerberos-Versionen

Versionsname	Inhalt
SEAM 1.0 in Solaris Easy Access Server 3.0	Vollständige Version des Kerberos-Service für die Versionen Solaris 2.6 und 7
Der Kerberos-Service in der Version Solaris 8	Nur Kerberos-Clientsoftware
SEAM 1.0.1 im Solaris 8-Administrationspaket	Kerberos-KDC und Remote-Anwendungen für die Version Solaris 8
Der Kerberos-Service in der Version Solaris 9	Nur Kerberos-KDC und Clientsoftware
SEAM 1.0.2	Kerberos-Remote-Anwendungen für die Version Solaris 9
Der Kerberos-Service in der Version Solaris 10	Vollständige Version des Kerberos-Service mit Erweiterungen

Kerberos-Komponenten

Ebenso wie die MIT-Distribution des Kerberos V5-Produkts umfasst der Oracle Solaris Kerberos-Service folgende Komponenten:

- Key Distribution Center (KDC):
  - Dämon für die Verwaltung der Kerberos-Datenbank: `kadmind`
  - Dämon für die Verarbeitung von Kerberos-Tickets: `krb5kdc`
  - Programme für die Datenbankverwaltung: `kadmin` (nur Master), `kadmin.local` und `kdb5_util`
  - Software für die Datenbankweitergabe: `kprop` (nur Slave) und `kpropd`

- Benutzerprogramme für die Verwaltung von Berechtigungsnachweisen: `kinit` , `klist` und `kdestroy`
- Benutzerprogramm zum Ändern Ihres Kerberos-Passworts: `kpasswd`
- Remote-Anwendungen: `ftp`, `rcp`, `rdist`, `rlogin` , `rsh`, `ssh` und `telnet`
- Dämonen für Remote-Anwendungen: `ftpd`, `rlogind`, `rshd`, `sshd` und `telnetd`
- Dienstprogramm für die Schlüsseltabellenverwaltung: `ktutil`
- Die GSS-API (Generic Security Service Application Programming Interface): ermöglicht Anwendungen die Verwendung mehrerer Sicherheitsmechanismen, ohne dass Sie die Anwendung nach jedem Hinzufügen eines neuen Mechanismus neu kompilieren müssen. Die GSS-API verwendet Standardschnittstellen, dank derer Anwendungen sich auf viele Betriebssysteme portieren lassen. GSS-API stellt Anwendungen bereit, die die Sicherheitsservices der Integrität und der Vertraulichkeit sowie Authentifizierung umfassen. Sowohl `ftp` als auch `ssh` verwenden die GSS-API.
- Die RPCSEC_GSS-API (Application Programming Interface): ermöglicht NFS-Services die Verwendung der Kerberos-Authentifizierung. RPCSEC_GSS ist eine Sicherheitsvariante, die Sicherheitsservices bereitstellt, die unabhängig von den verwendeten Mechanismen sind. RPCSEC_GSS befindet sich in der GSS-API-Schicht ganz oben. Alle plugfähigen GSS_API-basierten Sicherheitsmechanismen können von Anwendungen verwendet werden, die RPCSEC_GSS verwenden.

Darüber hinaus umfasst der Oracle Solaris Kerberos-Service Folgendes:

- Graphical Kerberos Administration Tool (`gkadmin`): ermöglicht Ihnen die Verwaltung von Hauptelementen und Hauptelementrichtlinien. Diese auf Java-Technologie basierende GUI stellt eine Alternative zum Befehl `kadmin` dar.
- Ein Kerberos V5-Servicemodul für PAM: bietet Authentifizierung sowie Konto-, Sitzungs- und Passwortverwaltung für den Kerberos-Service. Mithilfe des Moduls kann die Kerberos-Authentifizierung dem Benutzer transparent gemacht werden.
- Kernel-Module: bieten Kernel-basierte Implementierungen des Kerberos-Service für die Verwendung durch den NFS-Service, was zu einer erheblichen Verbesserung der Leistung beiträgt.

Kerberos-Ergänzungen für die Version Solaris 10 5/08

Folgende Erweiterungen sind ab der Version Solaris 10 5/08 enthalten:

- Die Kerberos-Software von Solaris wurde mit der Version MIT 1.4 synchronisiert. Insbesondere die Software für das KDC, der Befehl `kinit` und der Kerberos-Mechanismus wurden aktualisiert.
- Zudem wurde Unterstützung für den Zugriff auf Datensätze von Kerberos-Hauptelementen und Richtlinien mit LDAP über einen Verzeichnisserver hinzugefügt. Je nach Bereitstellung der KDCs und der DSs erleichtert diese Änderung die Verwaltung und bietet höhere Verfügbarkeit. Eine Liste der auf LDAP bezogenen Verfahren finden Sie unter „Verwalten eines KDC auf einem LDAP-Verzeichnisserver“ auf Seite 504.
- Dieser Version wurde Unterstützung für Solaris-Clients hinzugefügt, die keine zusätzliche Einrichtung erfordern. Am Kerberos-Service sowie an einigen Standardeinstellungen wurden Änderungen vorgenommen. Kerberos-Clients von Solaris funktionieren ohne clientseitige Konfiguration in Umgebungen, die ordnungsgemäß konfiguriert sind. Weitere Informationen finden Sie unter „Optionen zur Clientkonfiguration“ auf Seite 431.

Kerberos-Ergänzungen für die Version Solaris 10 8/07

Die MIT Kerberos V5-API (krb5-api) wird in der Version Solaris 10 8/07 unterstützt. Weitere Informationen finden Sie auf den Manpages `libkrb5`(3LIB) und `krb5-config`(1). Eine detailliertere Dokumentation finden Sie zudem auf den Webseiten des MIT Kerberos V5-Projekts unter mit.edu, sobald diese verfügbar ist.

Obwohl die krb5-api inzwischen verfügbar ist, empfiehlt Oracle nachdrücklich die Verwendung der GSS-API für die Netzwerkauthentifizierung, Integrität und Vertraulichkeit, da es sich bei der GSS-API um einen unabhängigen Sicherheitsmechanismus und um einen IETF-Standard handelt. Weitere Informationen finden Sie auf der Manpage `libgss`(3LIB).

Kerberos-Ergänzungen für die Version Solaris 10 6/06

In der Version Solaris 10 6/06 kann der Dämon `ktkt_warnd` automatisch Berechtigungsnachweise erneuern, anstatt bloß den Benutzer kurz vor Ablauf des Berechtigungsnachweises zu benachrichtigen. Der Benutzer muss angemeldet sein, damit der Berechtigungsnachweis automatisch erneuert werden kann.

Kerberos-Erweiterungen in der Version Solaris 10 3/05

Diese Kerberos-Erweiterungen sind in der Version Oracle Solaris enthalten. Einige der Erweiterungen wurden in früheren Software Express-Versionen eingeführt und in den Betaversionen von Solaris 10 aktualisiert.

- Für Remote-Anwendungen wie `ftp`, `rcp`, `rlogin`, `rsh`, `ssh` und `telnet` steht Kerberos-Protokollunterstützung zur Verfügung. Weitere Informationen finden Sie auf den Manpages für die einzelnen Befehle bzw. Dämonen und auf der Manpage `krb5_auth_rules(5)`.
- Die Hauptelement-Datenbank für Kerberos muss nicht mehr jedes Mal vollständig übertragen werden, sondern kann inkrementell aktualisiert werden. Die inkrementelle Weitergabe bietet folgende Vorteile:
  - Bessere Konsistenz der Datenbanken auf den verschiedenen Servern
  - Niedrigerer Bedarf an Ressourcen (Netzwerk, CPU usw.)
  - Bedeutend schnellere Weitergabe von Aktualisierungen
  - Automatisiertes Weitergabeverfahren
- Ein neues Skript zur Erleichterung der automatischen Konfiguration eines Kerberos-Clients ist mittlerweile verfügbar. Mit dessen Hilfe können Administratoren schnell und problemlos Kerberos-Clients einrichten. Informationen zu Verfahren, die das neue Skript verwenden, finden Sie unter „Konfigurieren von Kerberos-Clients“ auf Seite 468. Weitere Informationen finden Sie außerdem auf der Manpage `kclient(1M)`.
- Der Kerberos-Service wurde um mehrere neue Verschlüsselungstypen erweitert. Diese sorgen für mehr Sicherheit und eine verbesserte Kompatibilität mit anderen Kerberos-Implementierungen, die diese Verschlüsselungstypen unterstützen. Weitere Informationen finden Sie unter „Verwenden von Kerberos-Verschlüsselungstypen“ auf Seite 602. Es stehen folgende Verschlüsselungstypen zur Verfügung:
  - Der Verschlüsselungstyp AES kann zur Verschlüsselung von Kerberos-Sitzungen mit hoher Geschwindigkeit und Sicherheit verwendet werden.
  - ARCFOUR-HMAC sorgt für eine bessere Kompatibilität mit anderen Kerberos-Implementierungen.
  - Triple DES (3DES) mit SHA1 erhöht die Sicherheit. Außerdem bewirkt dieser Verschlüsselungstyp eine bessere Interoperabilität mit anderen Kerberos-Implementierungen, die diesen Verschlüsselungstyp unterstützen.
- Die Verschlüsselungstypen werden über das kryptografische Framework aktiviert. Das Framework kann für hardwarebeschleunigte Kryptografie für den Kerberos-Service sorgen.
- Die KDC-Software, die Benutzerbefehle und Benutzeranwendungen unterstützen jetzt die Verwendung des TCP-Netzwerkprotokolls. Diese Erweiterung sorgt für einen stabileren Betrieb und verbesserte Interoperabilität mit anderen Kerberos-Implementierungen, einschließlich Active Directory von Microsoft. Das KDC überwacht nun sowohl die traditionellen UDP- als auch die TCP-Ports und kann folglich auf Anforderungen in beiden Protokollen reagieren. Beim Senden einer Anforderung an das KDC verwenden die Benutzerbefehle und -anwendungen zuerst den UDP-Port. Schlägt dies fehl, versuchen sie es über den TCP-Port.

- Unter anderem mit den Befehlen `kinit` , `klist` und `kprop` wurde die KDC-Software um IPv6-Unterstützung erweitert. IPv6-Adressen werden standardmäßig unterstützt. Zum Aktivieren der IPv6-Unterstützung müssen keine Konfigurationsparameter geändert werden. Für die Befehle`kadmin` und `kadmind` steht keine IPv6-Unterstützung zur Verfügung.
- Mehrere Unterbefehle des Befehls `-kadmin` wurden um die Option `e` erweitert. Mit dieser neuen Option kann bei der Erstellung von Hauptelementen der Verschlüsselungstyp ausgewählt werden. Weitere Informationen finden Sie auf der Manpage `kadmin(1M)`.
- Ergänzungen des Moduls `pam_krb5` verwalten den Cache für Kerberos-Berechtigungsnachweise. Dabei stützen sie sich auf das PAM-Framework. Weitere Informationen finden Sie auf der Manpage `pam_krb5(5)`.
- Es besteht Unterstützung für die automatische Erkennung von Kerberos-KDC, admin server, kpasswd-Server und auf DNS-Abfragen basierenden Zuordnungen von Host- oder Domänennamen zu Bereichen. Durch diese Erweiterung fallen einige der zur Installation eines Kerberos-Clients erforderlichen Schritte weg. Anstatt eine Konfigurationsdatei lesen zu müssen, kann der Client einen KDC-Server mithilfe von DNS ausfindig machen. Weitere Informationen finden Sie auf der Manpage `krb5.conf(4)`.
- Eine weitere Neuerung stellt das PAM-Modul `pam_krb5_migrate` dar. Das neue Modul unterstützt die automatische Migration von Benutzern, die noch nicht über ein Kerberos-Konto verfügen, in den lokalen Kerberos-Bereich. Weitere Informationen finden Sie auf der Manpage `pam_krb5_migrate(5)`.
- Die Datei `~/.k5login` kann jetzt mit den GSS-Anwendungen `ftp` und `ssh` verwendet werden. Weitere Informationen finden Sie auf der Manpage `gss_auth_rules(5)`.
- Das Dienstprogramm `kproplog` wurde aktualisiert. Es gibt jetzt alle Attributnamen pro Protokolleintrag aus. Weitere Informationen finden Sie auf der Manpage `kproplog(1M)`.
- Die strenge TGT-Überprüfung kann jetzt mithilfe einer Konfigurationsoption in der Datei `krb5.conf` deaktiviert werden. Weitere Informationen finden Sie auf der Manpage `krb5.conf(4)`.
- Mit den Erweiterungen der Dienstprogramme zum Ändern von Passwörtern kann der Oracle Solaris Kerberos V5-Administrationsserver Anforderungen für Passwortänderungen von Clients akzeptieren, auf denen die Oracle Solaris-Software nicht ausgeführt wird. Weitere Informationen finden Sie auf der Manpage `kadmind(1M)`.
- Der Wiedergabe-Cache wird jetzt standardmäßig nicht mehr in arbeitsspeicherabhängigen Dateisystemen gespeichert, sondern dauerhaft unter `/var/krb5/rcache/`. Dieser neue Speicherort bietet Schutz vor Wiedergaben bei Systemneustarts. Die Leistung des rcache-Codes wurde verbessert. Da sich der Wiedergabe-Cache jetzt aber im Dauerspeicher befindet, kann es sein, dass er trotzdem insgesamt langsamer arbeitet.

- Der Wiedergabe-Cache kann jetzt für die Speicherung in Dateien oder ausschließlich im Arbeitsspeicher konfiguriert werden. Weitere Informationen zu Umgebungsvariablen, die hinsichtlich der Typen und Speicherpositionen für Schlüsseltabelle und Berechtigungsnachweis-Cache konfiguriert werden können, finden Sie auf der Manpage `krb5envvar(5)`.
- Der Kerberos-GSS-Mechanismus kommt nunmehr ohne GSS-Berechtigungstabelle aus. Weitere Informationen finden Sie unter „Zuordnen von GGS-Berechtigungsnachweisen zu UNIX-Berechtigungsnachweisen“ auf Seite 430 oder auf den Manpages `gsscred(1M)`, `gssd(1M)` und `gsscred.conf(4)`.
- Die Kerberos-Dienstprogramme `kinit` und `ktutil` beruhen neuerdings auf MIT Kerberos Version 1.2.1. Durch diese Änderung wurde der Befehl `kinit` um neue Optionen und der Befehl `ktutil` um neue Unterbefehle bereichert. Weitere Informationen finden Sie auf den Manpages `kinit(1)` und `ktutil(1)`.
- Solaris Kerberos Key Distribution Center (KDC) und `kadmind` bauen jetzt auf MIT Kerberos Version 1.2.1 auf. Das KDC verwendet nun standardmäßig eine btree-basierte Datenbank, die zuverlässiger ist als die aktuelle Hash-basierte Datenbank. Weitere Informationen finden Sie auf der Manpage `kdb5_util(1M)`
- Die Dämonen `kpropd`, `kadmind`, `krb5kdc` und `ktkt_warnd` werden von Service Management Facility verwaltet. Administrative Maßnahmen an diesem Service, z. B. Aktivieren, Deaktivieren oder Neustarten, können mithilfe des Befehls `svcadm` vorgenommen werden. Der Status des Service kann für alle Dämonen mit dem Befehl `svcs` abgefragt werden. Eine Übersicht zur Service Management Facility finden Sie in Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration*.

Kerberos-Komponenten in der Version Solaris 9

Die Version Solaris 9 umfasst alle in „Kerberos-Komponenten“ auf Seite 416 enthaltenen Komponenten, mit Ausnahme derjenigen für die Remote-Anwendungen.

SEAM 1.0.2-Komponenten

Die Version SEAM 1.0.2 umfasst die Remote-Anwendungen. Diese Anwendungen stellen den einzigen Teil von SEAM 1.0 dar, der nicht in die Version Solaris 9 integriert wurde. Folgendes sind die Komponenten für die Remote-Anwendungen:

- Clientanwendungen: `ftp`, `rcp`, `rlogin`, `rsh` und `telnet`
- Serverdämonen: `ftpd`, `rlogind`, `rshd` und `telnetd`

Kerberos-Komponenten in der Version Solaris 8

Die Version Solaris 8 umfasst nur die clientseitigen Teile des Kerberos-Service, sodass zahlreiche Komponenten nicht enthalten sind. Mithilfe dieses Produkts können Systeme, auf denen die Version Solaris 8 ausgeführt wird, zu Kerberos-Clients werden, ohne dass SEAM 1.0.1 separat installiert werden muss. Zur Verwendung dieser Funktionen müssen Sie ein KDC installieren, der entweder Solaris Easy Access Server 3.0, das Solaris 8-Administrationspaket, die MIT-Distribution oder Windows 2000 verwendet. Die clientseitigen Komponenten erfüllen nicht ihren Zweck, wenn kein KDC zum Verteilen von Tickets installiert ist. Die folgenden Komponenten sind in dieser Version enthalten:

- Benutzerprogramme zum Abrufen, Anzeigen und Löschen von Tickets: `kinit`, `klist` und `kdestroy`
- Benutzerprogramm zum Ändern Ihres Kerberos-Passworts: `kpasswd`
- Dienstprogramm für die Verwaltung der Schlüsseltabelle: `ktutil`
- Ergänzungen zu PAM (Pluggable Authentication Module): ermöglicht Anwendungen die Verwendung verschiedener Authentifizierungsmechanismen. Mithilfe von PAM können An- und Abmeldungen dem Benutzer transparent gemacht werden.
- GSS_API-Plugins: bieten Kerberos-Protokoll- und kryptografische Unterstützung.
- Unterstützung für NFS-Clients und -Server

SEAM 1.0.1-Komponenten

Die Version SEAM 1.0.1 umfasst alle Komponenten der Version SEAM 1.0, die noch nicht in der Version Solaris 8 enthalten sind. Folgende Komponenten stehen zur Verfügung:

- Key Distribution Center (KDC) (Master):
  - Dämon für die Verwaltung der Kerberos-Datenbank: `kadmind`
  - Dämon für die Verarbeitung von Kerberos-Tickets: `krb5kdc`
- Slave-KDCs
- Programme für die Datenbankverwaltung: `kadmin` und `kadmin.local`
- Software für die Datenbankweitergabe: `kprop`
- Remote-Anwendungen: `ftp`, `rcp`, `rlogin`, `rsh` und `telnet`
- Dämonen für Remote-Anwendungen: `ftpd`, `rlogind`, `rshd` und `telnetd`
- Dienstprogramm für die Verwaltung: `kdb5_util`
- Graphical Kerberos Administration Tool (`gkadmin`): ermöglicht Ihnen die Verwaltung von Hauptelementen und Hauptelementrichtlinien. Diese auf Java-Technologie basierende GUI stellt eine Alternative zum Befehl `kadmin` dar.

- Ein Verfahren zur Vorkonfiguration: ermöglicht Ihnen das Festlegen der Parameter für die Installation und Konfiguration von SEAM 1.0.1. Auf diese Weise können Sie die SEAM-Installation automatisieren. Dieses Verfahren eignet sich insbesondere für mehrere Installationen.
- Mehrere Bibliotheken

SEAM 1.0-Komponenten

Die Version SEAM 1.0 umfasst neben sämtlichen in „Kerberos-Komponenten“ auf Seite 416 enthaltenen Elementen folgende weitere Elemente:

- Ein Dienstprogramm (`gsscred`) und einen Dämon (`gssd`): Diese Programme erleichtern die Zuordnung von UNIX-Benutzer-IDs (UIDs) zu Hauptelementnamen. Diese Programme sind erforderlich, da NFS-Server UNIX-UIDs zum Identifizieren von Benutzern verwenden, und nicht von Hauptelementnamen, die in einem anderen Format gespeichert sind.
- Die GSS-API (Generic Security Service Application Programming Interface): ermöglicht Anwendungen die Verwendung mehrerer Sicherheitsmechanismen, ohne dass Sie die Anwendung nach jedem Hinzufügen eines neuen Mechanismus neu kompilieren müssen. Da die GSS-API rechnerunabhängig ist, eignet sie sich für Anwendungen im Internet. GSS-API stellt Anwendungen bereit, die die Sicherheitsservices der Integrität und der Vertraulichkeit sowie Authentifizierung umfassen.
- Die RPCSEC_GSS-API (Application Programming Interface): ermöglicht NFS-Services die Verwendung der Kerberos-Authentifizierung. RPCSEC_GSS ist eine Sicherheitsvariante, die Sicherheitsservices bereitstellt, die unabhängig von den verwendeten Mechanismen sind. RPCSEC_GSS befindet sich in der GSS-API-Schicht ganz oben. Alle plugfähigen GSS_API-basierten Sicherheitsmechanismen können von Anwendungen verwendet werden, die RPCSEC_GSS verwenden.
- Ein Verfahren zur Vorkonfiguration: ermöglicht Ihnen das Festlegen der Parameter für die Installation und Konfiguration von SEAM 1.0. Auf diese Weise können Sie die Installation automatisieren. Dieses Verfahren eignet sich insbesondere für mehrere Installationen.

◆ ◆ ◆ KAPITEL 22

Planen des Kerberos-Service

Dieses Kapitel sollte von Administratoren gelesen werden, die für die Installation und Verwaltung des Kerberos-Service zuständig sind. In dem Kapitel werden mehrere Installations- und Konfigurationsoptionen erläutert, mit denen sich Administratoren vor dem Installieren und Konfigurieren des Service vertraut machen sollten.

Nachfolgend werden die Themen aufgelistet, mit denen sich Systemadministratoren und andere zuständige Mitarbeiter befassen sollten:

- „Notwendigkeit des Planens von Kerberos-Bereitstellungen“ auf Seite 425
- „Planen von Kerberos-Bereichen“ auf Seite 426
- „Zuordnen von Hostnamen zu Bereichen“ auf Seite 427
- „Client- und Service-Hauptelementnamen“ auf Seite 428
- „Ports für die KDC- und Admin-Services“ auf Seite 429
- „Die Anzahl der Slave-KDCs“ auf Seite 429
- „Entscheidung über das zu verwendende System für die Datenbankweitergabe“ auf Seite 431
- „Synchronisierung von Uhren innerhalb eines Bereichs“ auf Seite 431
- „Optionen zur Clientkonfiguration“ auf Seite 431
- „Verbessern der Sicherheit bei der Clientanmeldung“ auf Seite 432
- „Optionen zur KDC-Konfiguration“ auf Seite 433
- „Kerberos-Verschlüsselungstypen“ auf Seite 433
- „Onlinehilfe-URL im Graphical Kerberos Administration Tool“ auf Seite 434

Notwendigkeit des Planens von Kerberos-Bereitstellungen

Bevor Sie den Kerberos-Service installieren, müssen Sie verschiedene Konfigurationsprobleme lösen. Obwohl die Konfiguration nach der Erstinstallation geändert werden kann, lassen sich bestimmte Änderungen eventuell schwer implementieren. Zudem muss für manche Änderungen das KDC neu eingerichtet werden, sodass sich hinsichtlich der Kerberos-Konfiguration eine langfristige Planung empfiehlt.

Die Bereitstellung einer Kerberos-Infrastruktur umfasst Aufgaben wie die Installation von KDCs, die Erstellung von Schlüsseln für Ihre Hosts und die Migration von Benutzern. Die erneute Konfiguration einer Kerberos-Bereitstellung kann sich ebenso schwierig gestalten wie die erstmalige Bereitstellung. Planen Sie Bereitstellungen deshalb sorgfältig, um Neukonfigurationen zu vermeiden.

Planen von Kerberos-Bereichen

Ein *Bereich* ist ein logisches Netzwerk (ähnlich einer Domain), das eine Gruppe von Systemen unter dem Namen Master-KDC definiert. Ebenso wie beim Einrichten eines DNS-Domainnamens sollten Probleme bezüglich des Bereichsnamens, der Anzahl und Größe jedes Bereichs sowie der Beziehung eines Bereichs zu anderen Bereichen für die bereichsübergreifende Authentifizierung vor der Konfiguration des Kerberos-Service gelöst werden.

Bereichsnamen

Bereichsnamen können aus einer beliebigen ASCII-Zeichenfolge bestehen. Üblicherweise entspricht der Bereichsname Ihrem DNS-Domainnamen, mit dem Unterschied, dass der Bereichsname in Großbuchstaben geschrieben ist. Mithilfe dieser Konvention lassen sich Probleme mit dem Kerberos-Service von Problemen mit dem DNS-Namespace unterscheiden, während ein bekannter Name verwendet wird. Wenn Sie DNS nicht verwenden oder sich für eine andere Zeichenfolge entscheiden, können Sie eine beliebige Zeichenfolge verwenden. Der Konfigurationsvorgang erfordert jedoch mehr Arbeitsaufwand. Es empfiehlt sich die Verwendung von Bereichsnamen, die der standardmäßigen Naming-Struktur für das Internet folgen.

Anzahl der Bereiche

Die Anzahl der für Ihre Installation erforderlichen Bereiche hängt von mehreren Faktoren ab:

- Die Anzahl der zu unterstützenden Clients. Durch eine zu hohe Anzahl an Clients in einem Bereich wird die Verwaltung erschwert und der Bereich muss möglicherweise aufgeteilt werden. Die primären Faktoren zur Bestimmung der Anzahl der möglichen zu unterstützenden Clients sind folgende:
  - Die Menge des Kerberos-Verkehrs, den jeder Client generiert
  - Die Bandbreite des physischen Netzwerks
  - Die Geschwindigkeit der Hosts

  Da jede Installation verschiedene Grenzen aufweist, gibt es für die Bestimmung der maximalen Anzahl an Clients keine allgemein gültige Regel.

- Zum einen spielt die Entfernung der Clients eine Rolle. Es bietet sich an, mehrere kleine Bereiche einzurichten, wenn sich die Clients in verschiedenen geografischen Regionen befinden.
- Zum anderen kommt es auch auf die Anzahl der Hosts an, die als KDC installiert werden können. Jeder Bereich sollte mindestens zwei KDC-Server umfassen: einen Master-Server und einen Slave-Server.

Es wird empfohlen, die Kerberos-Bereiche an administrativen Domains auszurichten. Beachten Sie, dass ein Kerberos V-Bereich mehrere Subdomains der DNS-Domain umfassen kann, der der Bereich entspricht.

Bereichshierarchie

Beim Konfigurieren mehrerer Bereiche für die bereichsübergreifende Authentifizierung müssen Sie die Beziehung zwischen diesen Bereichen bestimmen. Sie können eine hierarchische Beziehung zwischen den Bereichen festlegen, wodurch automatische Pfade zu den zugehörigen Domains bestimmt werden. Selbstverständlich müssen alle Bereiche in der hierarchischen Kette ordnungsgemäß konfiguriert werden. Die automatischen Pfade stellen eine Erleichterung bei der Verwaltung dar. Wenn jedoch viele Ebenen von Domains vorhanden sind, sollten Sie nicht den Standardpfad verwenden, da zu viele Transaktionen erforderlich sind.

Sie können die vertrauensvolle Beziehung auch direkt einrichten. Eine direkte vertrauensvolle Beziehung eignet sich besonders dann, wenn zwischen zwei hierarchischen Bereichen zu viele Ebenen vorhanden sind oder wenn keine hierarchische Beziehung festgelegt ist. Die Verbindung muss in der Datei `/etc/krb5/krb5.conf` auf allen Hosts definiert werden, die die Verbindung verwenden. Dies erfordert etwas zusätzliche Arbeit. Die direkte vertrauensvolle Beziehung wird auch als transitive Beziehung bezeichnet. Eine Einführung hierzu finden Sie unter „Kerberos-Bereiche“ auf Seite 413. Informationen zu den Konfigurationsverfahren für mehrere Bereiche finden Sie unter „Konfigurieren von bereichsübergreifender Authentifizierung“ auf Seite 456.

Zuordnen von Hostnamen zu Bereichen

Die Zuordnung von Hostnamen zu Bereichsnamen wird im Abschnitt `domain_realm` der Datei `krb5.conf` definiert. Je nach Anforderungen können diese Zuordnungen für eine ganze Domain und für einzelne Hosts definiert werden.

Informationen über die KDCs können auch mithilfe von DNS abgefragt werden. Mit DNS lassen sich die Information leichter ändern, da Sie die Datei `krb5.conf` nicht für jede Änderung auf allen Clients bearbeiten müssen. Weitere Informationen finden Sie auf der Manpage `krb5.conf(4)`.

Ab den Versionen Solaris Express Developer Edition 1/08 und Solaris 10 5/08 können Solaris Kerberos-Clients besser mit Active Directory-Servern interagieren. Die Active Directory-Server können für die Zuordnung von Bereichen zu Hosts konfiguriert werden.

Client- und Service-Hauptelementnamen

Wenn Sie den Kerberos-Service verwenden, muss DNS auf allen Hosts aktiviert sein. Bei aktiviertem DNS sollten die Hauptelemente den vollständig qualifizierten Domainnamen (FQDN, Fully Qualified Domain Name) jedes Hosts enthalten. Beispiel: Wenn der Hostname `boston` , der DNS-Domainname `example.com` und der Bereichsname `EXAMPLE.COM` sind, sollte der Hauptelementname für den Host `host/boston.example.com@EXAMPLE.COM` lauten. Die in diesem Buch aufgeführten Beispiele setzen die Konfiguration von DNS und die Verwendung des FQDN für jeden Host voraus.

Der Kerberos-Service standardisiert Alias-Namen von Hosts über DNS und verwendet die standardisierte Form (cname) beim Erstellen des Service-Hauptelements für den zugewiesenen Service. Daher sollte bei der Erstellung eines Service-Hauptelements die Hostnamen-Komponente von Service-Hauptelementen die kanonische Form des Hostnamens des Systems sein, das den Service hostet.

Im Folgenden sehen Sie ein Beispiel für die Standardisierung des Hostnamens durch den Kerberos-Service. Ein Benutzer führt den Befehl "ssh alpha.example.com" aus, wobei `alpha.example.com` ein DNS-Host-Alias für den standardisierten Namen (cname) `beta.example.com` ist. Wenn ssh Kerberos aufruft und ein Hostservice-Ticket für `alpha.example.com` anfordert, standardisiert der Kerberos-Service `alpha.example.com` auf `beta.example.com` und fordert vom KDC ein Ticket für das Service-Hauptelement "host/beta.example.com" an.

Bei den Hauptelementnamen, die den FQDN eines Hosts enthalten, muss eine Übereinstimmung mit der Zeichenfolge bestehen, die den DNS-Domainnamen in der Datei `/etc/resolv.conf` beschreibt. Beim Kerberos-Service muss der DNS-Domainname in Kleinbuchstaben geschrieben sein, wenn Sie den FQDN für ein Hauptelement angeben. Der DNS-Domainname kann Groß- und Kleinbuchstaben enthalten; bei der Erstellung eines Host-Hauptelements dürfen Sie jedoch nur Kleinbuchstaben verwenden. So ist es beispielsweise egal, ob der DNS-Domainname `example.com`, `Example.COM` usw. lautet. Der Hauptelementname für den Host ist weiterhin `host/boston.example.com@EXAMPLE.COM`.

Darüber hinaus wurde Service Management Facility so konfiguriert, dass eine Vielzahl der Dämonen und Befehle erst gestartet wird, wenn der DNS-Clientservice ausgeführt wird. Die Dämonen `kdb5_util`, `kadmind` und `kpropd` sowie der Befehl `kprop` sind so konfiguriert, dass sie vom DNS-Service abhängen. Um die mit dem Kerberos-Service und SMF verfügbaren Funktionen voll nutzen zu können, müssen Sie den DNS-Clientservice auf allen Hosts aktivieren.

Ports für die KDC- und Admin-Services

Standardmäßig werden die Ports `88` und `750` für das KDC und Port `749` für den KDC-Verwaltungsdämon verwendet. Es können auch andere Portnummern verwendet werden. Wenn Sie die Portnummern ändern, müssen die Dateien `/etc/services` und `/etc/krb5/krb5.conf` auf jedem Client geändert werden. Außerdem muss die Datei `/etc/krb5/kdc.conf` auf jedem KDC aktualisiert werden.

Die Anzahl der Slave-KDCs

Ebenso wie das Master-KDC generieren Slave KDCs Berechtigungsnachweise für Clients. Slave-KDCs bieten ein Backup, wenn der Master nicht verfügbar ist. Jeder Bereich sollte mindestens ein Slave-KDC umfassen. In Abhängigkeit der folgenden Faktoren sind möglicherweise weitere Slave-KDCs erforderlich:

- Die Anzahl der physischen Segmente im Bereich. Normalerweise sollte das Netzwerk so eingerichtet werden, dass jedes Segment (zumindest minimal) ohne den Rest des Bereichs funktionieren kann. Dazu muss von jedem Segment aus auf ein KDC zugegriffen werden können. In diesem Fall könnte das KDC entweder ein Master oder ein Slave sein.
- Die Anzahl der Clients im Bereich. Durch Hinzufügen weiterer Slave-KDC-Server können Sie die Auslastung der aktuellen Server verringern.

Es können auch zu viele Slave-KDCs hinzugefügt werden. Bedenken Sie, dass die KDC-Datenbank an jeden Server weitergegeben werden muss, d. h. je mehr KDC-Server installiert sind, desto länger kann es dauern, die Daten innerhalb des gesamten Bereichs zu aktualisieren. Zudem erhöht sich bei einer größeren Anzahl von Slaves das Risiko einer Sicherheitsverletzung, da auf jedem Slave eine Kopie der KDC-Datenbank verbleibt.

Außerdem kann mindestens ein Slave-KDC für den Austausch mit dem Master-KDC konfiguriert werden. Der Vorteil einer derartigen Konfiguration bei mindestens einem Slave-KDC liegt darin, dass im Falle eines Ausfalls des Master-KDC ein vorkonfiguriertes System vorliegt, das auf einfache Weise als Master-KDC ausgetauscht werden kann. Anweisungen zur Konfiguration eines austauschbaren Slave-KDC finden Sie unter „Austauschen von Master-KDC und Slave-KDC“ auf Seite 484.

Zuordnen von GGS-Berechtigungsnachweisen zu UNIX-Berechtigungsnachweisen

Der Kerberos-Service bietet eine Standardzuordnung von Namen für GSS-Berechtigungsnachweise zu UNIX-Benutzer-IDs (UIDs) für GSS-Anwendungen, die diese Zuordnung erfordern, wie z. B. NFS. Bei der Verwendung des Kerberos-Service entsprechen die Namen von GSS-Berechtigungsnachweisen den Kerberos-Hauptelementnamen. Der standardmäßige Zuordnungsalgorithmus besteht darin, einen Kerberos-Hauptelementnamen zu verwenden, der aus einer Komponente besteht, und mithilfe dieser Komponente, die dem primären Namen des Hauptelements entspricht, die UID abzurufen. Das Abrufen erfolgt im Standardbereich oder in einem beliebigen durch den Parameter `auth_to_local_realm` in `/etc/krb5/krb5.conf` zugelassenen Bereich. Zum Beispiel wird der Benutzer-Hauptelementname `bob@EXAMPLE.COM` der UID des UNIX-Benutzers `bob` unter Verwendung der Passworttabelle zugeordnet. Der Benutzer-Hauptelementname `bob/admin@EXAMPLE.COM` würde nicht zugeordnet, da der Hauptelementname eine Instanzkomponente von `admin` enthält. Wenn die Standardzuordnungen für die Berechtigungsnachweise des Benutzers ausreichen, muss die Tabelle der GGS-Berechtigungsnachweise nicht gefüllt werden. In früheren Versionen war das Füllen der Tabelle der GSS-Berechtigungsnachweise für den Betrieb des NFS-Service erforderlich. Wenn die Standardzuordnungen nicht ausreichen (z. B. wenn Sie einen Hauptelementnamen mit einer Instanzkomponente zuordnen möchten), sollten andere Methoden verwendet werden. Weitere Informationen finden Sie unter:

- „So erstellen Sie eine Berechtigungsnachweistabelle“ auf Seite 463
- „So fügen Sie der Berechtigungstabelle einen einzelnen Eintrag hinzu“ auf Seite 464
- „So ordnen Sie Berechtigungsnachweise zwischen Bereichen zu“ auf Seite 465
- „Überwachen der Zuordnungen von GSS-Berechtigungsnachweisen zu UNIX-Berechtigungsnachweisen“ auf Seite 525

Automatische Benutzermigration in einen Kerberos-Bereich

UNIX-Benutzer, die über keine gültigen Benutzerkonten im standardmäßigen Kerberos-Bereich verfügen, können mit dem PAM-Framework automatisch migriert werden. Insbesondere das Modul `pam_krb5_migrate` kommt im Authentifizierungs-Stack des PAM-Service zum Einsatz. Services werden so eingerichtet, dass für einen Benutzer ohne Kerberos-Hauptelement automatisch ein Kerberos-Hauptelement erstellt wird, sobald er sich beim System mit seinem Passwort anmeldet. Das Passwort für das neue Hauptelement entspricht dem UNIX-Passwort. Anweisungen zur Verwendung des Moduls `pam_krb5_migrate` finden Sie unter „So konfigurieren Sie eine automatische Migration von Benutzern in einem Kerberos-Bereich“ auf Seite 480.

Entscheidung über das zu verwendende System für die Datenbankweitergabe

Die auf dem Master-KDC gespeicherte Datenbank muss regelmäßig an die Slave-KDCs weitergegeben werden. Sie können eine inkrementelle Weitergabe der Datenbank konfigurieren. Hierbei werden anstatt der gesamten Datenbank nur aktualisierte Informationen an die Slave-KDCs weitergegeben. Weitere Informationen zur Datenbankweitergabe finden Sie unter „Verwalten der Kerberos-Datenbank“ auf Seite 489.

Wenn Sie die inkrementelle Weitergabe nicht verwenden, müssen Sie zunächst festlegen, wie häufig die Slave-KDCs aktualisiert werden sollen. Der Bedarf an aktualisierten Informationen, die jedem Client zur Verfügung stehen, muss gegenüber der Zeit abgewogen werden, die die Durchführung der Aktualisierung in Anspruch nimmt.

Bei großen Installationen mit vielen KDCs in einem Bereich können die Daten von einem oder mehreren Slaves weitergegeben werden, sodass der Vorgang parallel erfolgt. Durch diese Strategie wird die Zeit für die Aktualisierung verringert. Auf der anderen Seite gestaltet sich die Verwaltung des Bereichs komplexer. Eine vollständige Beschreibung dieser Strategie finden Sie unter „Einrichten von paralleler Weitergabe“ auf Seite 502.

Synchronisierung von Uhren innerhalb eines Bereichs

Auf allen Hosts des Kerberos-Authentifizierungssystems müssen die internen Uhren innerhalb eines angegebenen maximalen Zeitraums synchronisiert werden. Diese als *Uhrdifferenz* bezeichnete Funktion stellt eine weitere Kerberos-Sicherheitsprüfung dar. Wenn die Uhrdifferenz zu einem der Hosts überschritten wird, werden Anforderungen abgewiesen.

Ein Möglichkeit zur Synchronisierung aller Uhren besteht in der Verwendung der NTP-Software (Network Time Protocol). Weitere Informationen finden Sie unter „Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients“ auf Seite 482. Es gibt noch andere Methoden zur Synchronisierung von Uhren. Die Verwendung von NTP ist daher nicht obligatorisch. Es sollte jedoch irgendeine Form der Synchronisierung gewählt werden, um Zugriffsfehler aufgrund von Uhrdifferenz zu verhindern.

Optionen zur Clientkonfiguration

Eine neue Funktion in der Version Solaris 10 ist das Konfigurationsdienstprogramm `kclient`. Das Dienstprogramm kann im interaktiven oder im nicht interaktiven Modus ausgeführt werden. Im interaktiven Modus wird der Benutzer zur Angabe Kerberos-spezifischer Parameterwerte aufgefordert. Auf diese Weise kann er während der Konfiguration des Clients Änderungen an der vorhandenen Installation vornehmen. Im nicht interaktiven Modus wird eine Datei mit vorher festgelegten Parameterwerten verwendet. Außerdem stehen im nicht

interaktiven Modus Befehlszeilenoptionen zur Verfügung. Sowohl der interaktive als auch der nicht interaktive Modus erfordern weniger Schritte als der manuelle Vorgang. Dadurch wird der Konfigurationsvorgang beschleunigt und ist insgesamt weniger fehleranfällig.

An der Version Solaris 10 5/08 wurden Änderungen vorgenommen, um einen Kerberos-Client zu ermöglichen, der keinerlei Konfiguration bedarf. Werden die hier beschriebenen Regeln in Ihrer Umgebung befolgt, ist kein explizites Konfigurationsverfahren für den Solaris Kerberos-Client erforderlich.

- DNS wird zur Rückgabe von SRV-Datensätzen für KDCs konfiguriert.
- Der Bereichsname entspricht dem DNS-Domainnamen oder das KDC unterstützt Verweise.
- Für den Kerberos-Client ist keine `keytab`-Datei erforderlich.

In manchen Fällen empfiehlt es sich eher, den Kerberos-Client explizit zu konfigurieren.

- Werden keine Verweise verwendet, hängt die Logik der nicht erforderlichen Konfiguration vom DNS-Domainnamen des Hosts zur Bestimmung des Bereichs ab. Dies birgt ein gewisses Sicherheitsrisiko. Das Risiko ist jedoch wesentlich geringer als beim Aktivieren von `dns_lookup_realm`.
- Das Modul `pam_krb5` verwendet einen Hostschlüsseleintrag in der Datei `keytab`. Diese Anforderung kann in der Datei `krb5.conf` deaktiviert werden. Aus Sicherheitsgründen wird dies jedoch nicht empfohlen. Weitere Informationen finden Sie auf der Manpage `krb5.conf(4)`.
- Der Vorgang ohne erforderliche Konfiguration ist weniger effizient als die direkte Konfiguration und weist eine größere Abhängigkeit von DNS auf. Auch werden mehr DNS-Abfragen ausgeführt als bei einem direkt konfigurierten Client.

Eine Beschreibung aller Vorgänge zur Clientkonfiguration finden Sie unter „Konfigurieren von Kerberos-Clients“ auf Seite 468.

Verbessern der Sicherheit bei der Clientanmeldung

In der Version Solaris 10 11/06 überprüft ein Client mithilfe des Moduls `pam_krb5` bei der Anmeldung, ob es sich bei dem KDC, das das letzte TGT ausgestellt hat, um dasselbe KDC handelt, das das in `/etc/krb5/krb5.keytab` gespeicherte Client-Host-Hauptelement ausgestellt hat. Das Modul `pam_krb5` überprüft das KDC, wenn das Modul im Authentifizierungs-Stack konfiguriert ist. Für einige Konfigurationen muss diese Prüfung deaktiviert werden. Dies gilt beispielsweise für DHCP-Clients, auf denen kein Client-Host-Hauptelement gespeichert wird. Zum Deaktivieren dieser Prüfung müssen Sie die Option `verify_ap_req_nofail` in der Datei `krb5.conf` auf "false" setzen. Weitere Informationen finden Sie unter „So deaktivieren Sie die Überprüfung des TGT (Ticket Granting Ticket)“ auf Seite 478.

Optionen zur KDC-Konfiguration

Ab der Version Solaris 10 5/08 steht Unterstützung für die Verwendung von LDAP zum Verwalten der Datenbankdateien für Kerberos zur Verfügung. Anweisungen finden Sie unter „So konfigurieren Sie ein KDC zur Verwendung eines LDAP-Datenservers“ auf Seite 443. LDAP vereinfacht die Verwaltung für Standorte, die eine bessere Koordination zwischen den Solaris Kerberos-Datenbanken und der vorhandenen DS-Einrichtung erfordern.

Kerberos-Verschlüsselungstypen

Ein *Verschlüsselungstyp* ist ein Bezeichner, der den Verschlüsselungsalgorithmus, den Verschlüsselungsmodus und die Hash-Algorithmen angibt, die im Kerberos-Service verwendet werden. Den Schlüsseln im Kerberos-Service ist ein Verschlüsselungstyp zur Identifizierung des kryptografischen Algorithmus und Modus für die Verwendung bei durch den Service ausgeführten kryptografischen Vorgängen mit dem Schlüssel zugewiesen. Folgende Verschlüsselungstypen werden unterstützt:

- `des-cbc-md5`
- `des-cbc-crc`
- `des3-cbc-sha1-kd`
- `arcfour-hmac-md5`
- `arcfour-hmac-md5-exp`
- `aes128-cts-hmac-sha1-96`
- `aes256-cts-hmac-sha1-96`

Hinweis – In Versionen vor Solaris 10 8/07 kann der Verschlüsselungstyp `aes256-cts-hmac-sha1-96` mit dem Kerberos-Service verwendet werden, wenn die ungebündelten Strong Cryptographic-Pakete installiert sind.

Wenn Sie den Verschlüsselungstyp ändern möchten, sollten Sie dies bei der Erstellung einer neuen Hauptelementdatenbank tun. Aufgrund der Interaktion zwischen KDC, Server und Client gestaltet sich das Ändern des Verschlüsselungstyps in einer vorhandenen Datenbank schwierig. Legen Sie diese Parameter nicht fest, außer wenn Sie die Datenbank neu erstellen. Weitere Informationen finden Sie unter „Verwenden von Kerberos-Verschlüsselungstypen“ auf Seite 602.

Hinweis – Wenn Sie ein Master-KDC installiert haben, das die Version Solaris 10 nicht ausführt, müssen Sie die Slave-KDCs vor der Aktualisierung des Master-KDC auf die Version Solaris 10 aktualisieren. Ein Master-KDC für Solaris 10 verwendet die neuen Verschlüsselungstypen, die von einem älteren Slave nicht verarbeitet werden können.

Onlinehilfe-URL im Graphical Kerberos Administration Tool

Die Onlinehilfe-URL wird vom Graphical Kerberos Administration Tool (`gkadmin`) verwendet, sodass die URL ordnungsgemäß für die Aktivierung des Menüs "Help Contents" (Inhalt der Hilfe) definiert werden sollte. Die HTML-Version dieses Handbuchs kann auf jedem geeigneten Server installiert werden. Alternativ können Sie auch die Sammlungen unter `http://www.oracle.com/technetwork/indexes/documentation/index.html` verwenden.

Bei der Konfiguration eines Hosts für die Verwendung des Kerberos-Service wird die URL in der Datei krb5.conf angegeben. Die URL sollte auf den Abschnitt "Graphical Kerberos Administration Tool" im Kapitel "Verwalten von Hauptelementen und Richtlinien (Aufgaben)" in diesem Buch verweisen. Sie können eine andere HTML-Seite auswählen, wenn Ihnen ein anderer Ort geeigneter erscheint.

◆ ◆ ◆ KAPITEL 23

Konfigurieren des Kerberos-Service (Aufgaben)

In diesem Kapitel werden Konfigurationsverfahren für KDC-Server, Netzwerkanwendungsserver, NFS-Server und Kerberos-Clients beschrieben. Viele dieser Verfahren erfordern Superuser-Zugriff. Deshalb sollten sie von Systemadministratoren oder erfahrenen Benutzern verwendet werden. Bereichsübergreifende Konfigurationsverfahren und andere Themen in Verbindung mit KDC-Servern sind ebenfalls enthalten.

In diesem Kapitel werden folgende Themen behandelt.

- „Konfigurieren des Kerberos-Service (Übersicht der Schritte)“ auf Seite 435
- „Konfigurieren von KDC-Servern“ auf Seite 437
- „Konfigurieren von Kerberos-Clients“ auf Seite 468
- „Konfigurieren von bereichsübergreifender Authentifizierung“ auf Seite 456
- „Konfigurieren von Kerberos-Netzwerkanwendungsservern“ auf Seite 458
- „Konfigurieren von Kerberos-NFS-Servern“ auf Seite 461
- „Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients“ auf Seite 482
- „Austauschen von Master-KDC und Slave-KDC“ auf Seite 484
- „Verwalten der Kerberos-Datenbank“ auf Seite 489
- „Erhöhen der Sicherheit auf Kerberos-Servern“ auf Seite 506

Konfigurieren des Kerberos-Service (Übersicht der Schritte)

Einige Teile des Konfigurationsprozesses hängen von anderen Teilen ab und müssen in einer bestimmten Reihenfolge ausgeführt werden. Mit diesen Verfahren werden oft Services eingerichtet, die zur Verwendung des Kerberos-Service erforderlich sind. Andere Verfahren sind nicht von einer bestimmten Reihenfolge abhängig und können bei Bedarf durchgeführt werden. In der folgenden Übersicht der Schritte wird eine Reihenfolge für eine Kerberos-Installation vorgeschlagen.

Aufgabe	Description (Beschreibung)	Anweisungen
1. Planen der Kerberos-Installation	Ermöglicht Ihnen, Konfigurationsprobleme zu lösen, bevor Sie die Softwarekonfiguration beginnen. Durch Planen sparen Sie langfristig Zeit und andere Ressourcen.	Kapitel 22, „Planen des Kerberos-Service“
2. (Optional) Installieren von NTP	Konfiguriert die NTP-Software (Network Time Protocol) oder ein anderes Protokoll zur Synchronisierung von Uhren. Damit der Kerberos-Service ordnungsgemäß funktioniert, müssen die Uhren auf allen Systemen im Bereich synchronisiert sein.	„Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients“ auf Seite 482
3. Konfigurieren von KDC-Servern	Konfiguriert und erstellt die Master-KDC- und Slave-KDC-Server sowie die KDC-Datenbank für einen Bereich	„Konfigurieren von KDC-Servern“ auf Seite 437
4. (Optional) Erhöhen der Sicherheit auf KDC-Servern	Verhindert Sicherheitsverletzungen auf KDC-Servern	„So beschränken Sie den Zugriff auf KDC-Server“ auf Seite 506
5. (Optional) Konfigurieren von austauschbaren KDC-Servern	Erleichtert das Austauschen von Master-KDC und Slave-KDC	„So konfigurieren Sie ein austauschbares Slave-KDC“ auf Seite 484

Konfigurieren zusätzlicher Kerberos-Services (Übersicht der Schritte)

Im Anschluss an die erforderlichen Schritte können folgende optionale Verfahren durchgeführt werden.

Aufgabe	Description (Beschreibung)	Anweisungen
Konfigurieren von bereichsübergreifender Authentifizierung	Ermöglicht die Kommunikation zwischen Bereichen	„Konfigurieren von bereichsübergreifender Authentifizierung“ auf Seite 456
Konfigurieren von Kerberos-Anwendungsservern	Ermöglicht einem Server, Services wie `ftp`, `telnet` und `rsh` mit Kerberos-Authentifizierung zu unterstützen	„Konfigurieren von Kerberos-Netzwerkanwendungsservern“ auf Seite 458
Konfigurieren von Kerberos-Clients	Ermöglicht einem Client, Kerberos-Services zu nutzen	„Konfigurieren von Kerberos-Clients“ auf Seite 468
Konfigurieren des Kerberos-NFS-Servers	Ermöglicht einem Server die gemeinsame Nutzung eines Dateisystems, das eine Kerberos-Authentifizierung erfordert	„Konfigurieren von Kerberos-NFS-Servern“ auf Seite 461

Aufgabe	Description (Beschreibung)	Anweisungen
Erhöhen der Sicherheit auf einem Anwendungsserver	Erhöht die Sicherheit auf einem Anwendungsserver, indem der Zugriff auf authentifizierte Transaktionen beschränkt wird	„So aktivieren Sie nur kerberisierte Anwendungen“ auf Seite 506

Konfigurieren von KDC-Servern

Nach der Installation der Kerberos-Software müssen Sie die KDC-Server konfigurieren. Durch Konfiguration eines Master-KDC und mindestens eines Slave-KDC wird der Service zur Ausgabe von Berechtigungsnachweisen bereitgestellt. Diese Berechtigungsnachweise bilden die Grundlage für den Kerberos-Service. Daher müssen die KDCs vor der Durchführung anderer Aufgaben installiert werden.

Der wichtigste Unterschied zwischen einem Master-KDC und einem Slave-KDC ist, dass nur das Master-KDC Datenbankverwaltungsanforderungen verarbeiten kann. So muss z. B. das Ändern eines Passworts oder das Hinzufügen eines neuen Hauptelements auf dem Master-KDC erfolgen. Diese Änderungen können dann an die Slave-KDCs weitergegeben werden. Sowohl Slave-KDC als auch Master-KDC generieren Berechtigungsnachweise. Diese Funktionsweise bietet Redundanz, falls das Master-KDC nicht verfügbar ist.

TABELLE 23–1 Konfigurieren von KDC-Servern (Übersicht der Schritte)

Aufgabe	Description (Beschreibung)	Anweisungen
Konfigurieren eines Master-KDC-Servers	Konfiguriert und erstellt Master-KDC-Server und -Datenbank für einen Bereich mithilfe eines manuellen Prozesses, der für komplexere Installationen benötigt wird	„So konfigurieren Sie ein Master-KDC manuell“ auf Seite 438
	Konfiguriert und erstellt Master-KDC-Server und -Datenbank für einen Bereich mithilfe eines manuellen Prozesses und LDAP für das KDC	„So konfigurieren Sie ein KDC zur Verwendung eines LDAP-Datenservers“ auf Seite 443
Konfigurieren eines Slave-KDC-Servers	Konfiguriert und erstellt einen Slave-KDC-Server für einen Bereich mithilfe eines manuellen Prozesses, der für komplexere Installationen benötigt wird	„So konfigurieren Sie ein Slave-KDC manuell“ auf Seite 451
Aktualisieren von Hauptelementschlüsseln auf einem KDC-Server	Aktualisiert einen Sitzungsschlüssel auf einem KDC-Server zur Verwendung neuer Verschlüsselungstypen	„So aktualisieren Sie die Ticket Granting Service-Schlüssel auf einem Master-Server“ auf Seite 455

▼ So konfigurieren Sie ein Master-KDC manuell

Bei diesem Verfahren wird eine inkrementelle Weitergabe konfiguriert. Zusätzlich werden folgende Konfigurationsparameter verwendet:

- Bereichsname = `EXAMPLE.COM`
- DNS-Domainname = `example.com`
- Master-KDC = `kdc1.example.com`
- `admin`-Hauptelement = `kws/admin`
- Onlinehilfe-URL = `http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956`

Hinweis – Passen Sie die URL an, sodass sie auf den Bereich "Graphical Kerberos Administration Tool" verweist, wie in „Onlinehilfe-URL im Graphical Kerberos Administration Tool“ auf Seite 434 beschrieben.

Bevor Sie beginnen Für dieses Verfahren muss der Host zur Verwendung von DNS konfiguriert sein. Wenn dieser Master austauschbar sein soll, beachten Sie die Naming-Anweisungen unter „Austauschen von Master-KDC und Slave-KDC“ auf Seite 484.

1. **Melden Sie sich als Superuser beim Master-KDC an.**

2. **Bearbeiten Sie die Kerberos-Konfigurationsdatei (`krb5.conf`).**

   Sie müssen die Bereichsnamen und Servernamen ändern. Eine vollständige Beschreibung dieser Datei finden Sie auf der Manpage `krb5.conf(4)`.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = EXAMPLE.COM

[realms]
        EXAMPLE.COM = {
        kdc = kdc1.example.com
        admin_server = kdc1.example.com
        }

[domain_realm]
        .example.com = EXAMPLE.COM
#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
        default = FILE:/var/krb5/kdc.log
        kdc = FILE:/var/krb5/kdc.log

[appdefaults]
    gkadmin = {
        help_url = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956
        }
```

In diesem Beispiel wurden die Zeilen für `default_realm`, `kdc`, `admin_server` und alle Einträge von `domain_realm` geändert. Außerdem wurde die Zeile zur Definition der `help_url` bearbeitet.

Hinweis – Um die Verschlüsselungstypen zu beschränken, können Sie die Zeilen `default_tkt_enctypes` oder `default_tgs_enctypes` einstellen. Eine Beschreibung der Probleme beim Beschränken der Verschlüsselungstypen finden Sie unter „Verwenden von Kerberos-Verschlüsselungstypen“ auf Seite 602.

---

3 Bearbeiten Sie die KDC-Konfigurationsdatei (`kdc.conf`).

Sie müssen den Bereichsnamen ändern. Eine vollständige Beschreibung dieser Datei finden Sie auf der Manpage `kdc.conf(4)`.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM = {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
                sunw_dbprop_master_ulogsize = 1000
                }
```

In diesem Beispiel wurde die Bereichsnamendefinition im Abschnitt `realms` geändert. Im Abschnitt `realms` wurden außerdem Zeilen zum Aktivieren der inkrementellen Weitergabe und für die Anzahl der Aktualisierungen, die der KDC-Master in der Protokolldatei beibehält, hinzugefügt.

Hinweis – Um die Verschlüsselungstypen zu beschränken, können Sie die Zeilen `permitted_enctypes`, `supported_enctypes` oder `master_key_type` einstellen. Eine Beschreibung der Probleme beim Beschränken der Verschlüsselungstypen finden Sie unter „Verwenden von Kerberos-Verschlüsselungstypen“ auf Seite 602.

---

4 Erstellen Sie die KDC-Datenbank mithilfe des Befehls `kdb5_util`.

Der Befehl `kdb5_util` erstellt die KDC-Datenbank. In Verbindung mit der Option `-s` erstellt dieser Befehl eine Stash-Datei, die zur Authentifizierung des KDC dient, bevor die Dämonen `kadmind` und `krb5kdc` gestartet werden.

```
kdc1 # /usr/sbin/kdb5_util create -s
Initializing database '/var/krb5/principal' for realm 'EXAMPLE.COM'
master key name 'K/M@EXAMPLE.COM'
You will be prompted for the database Master Password.
```

```
It is important that you NOT FORGET this password.
Enter KDC database master key:     <Type the key>
Re-enter KDC database master key to verify:     <Type it again>
```

5 Bearbeiten Sie die Kerberos-Zugriffssteuerungsliste (`kadm5.acl`).

Nach der Datenaufnahme sollte die Datei `/etc/krb5/kadm5.acl` alle Hauptelementnamen enthalten, die zur Verwaltung des KDC berechtigt sind.

```
kws/admin@EXAMPLE.COM   *
```

Der Eintrag ermöglicht dem Hauptelement `kws/admin` im Bereich `EXAMPLE.COM` Hauptelemente oder Richtlinien im KDC zu ändern. Die Standardinstallation enthält ein Sternchen (*) zur Übereinstimmung mit allen `admin`-Hauptelementen. Diese Standardeinstellung kann ein Sicherheitsrisiko darstellen. Es ist sicherer, eine Liste aller `admin`-Hauptelemente einzuschließen. Weitere Informationen finden Sie auf der Manpage `kadm5.acl(4)`.

6 Starten Sie den Befehl `kadmin.local` und fügen Sie Hauptelemente hinzu.

Mit den nächsten Teilschritten erstellen Sie Hauptelemente, die vom Kerberos-Service verwendet werden.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local:
```

a. Fügen Sie der Datenbank Admin-Hauptelemente hinzu.

Sie können so viele `admin`-Hauptelemente hinzufügen, wie Sie benötigen. Sie müssen mindestens ein `admin`-Hauptelement zum Abschließen des KDC-Konfigurationsprozesses hinzufügen. In diesem Beispiel wird ein `kws/admin`-Hauptelement hinzugefügt. Ersetzen Sie `kws` durch einen geeigneten Hauptelementnamen.

```
kadmin.local: addprinc kws/admin
Enter password for principal kws/admin@EXAMPLE.COM:     <Type the password>
Re-enter password for principal kws/admin@EXAMPLE.COM:     <Type it again>
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

b. Erstellen Sie die `kiprop`-Hauptelemente.

Das `kiprop`-Hauptelement dient dazu, Aktualisierungen vom Master-KDC zu autorisieren.

```
kadmin.local: addprinc -randkey kiprop/kdc1.example.com
Principal "kiprop/kdc1.example.com@EXAMPLE.COM" created.
kadmin.local:
```

c. Erstellen Sie eine Schlüsseltabellendatei für den `kadmind`-Service.

Diese Befehlssequenz erstellt eine spezielle Schlüsseltabellendatei mit Hauptelementeinträgen für `kadmin/<FQDN>` und `changepw/<FQDN>`. Diese Hauptelemente werden für den `kadmind`-Service und zum Ändern von Passwörtern verwendet. Wenn die Hauptelementinstanz ein Hostname ist, muss der FQDN unabhängig von der Schreibung des Domainnamens in der Datei `/etc/resolv.conf` in Kleinbuchstaben angegeben

werden. Das `kadmin/changepw`-Hauptelement dient zum Ändern der Passwörter von Clients, auf denen keine Solaris-Version ausgeführt wird.

```
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc1.example.com
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab changepw/kdc1.example.com
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/changepw
Entry for principal kadmin/changepw with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local:
```

d. Fügen Sie das `kiprop`-Hauptelement für den Master-KDC-Server der Schlüsseltabellendatei `kadmind` hinzu.

Da Sie das `kiprop`-Hauptelement der Datei `kadm5.keytab` hinzugefügt haben, kann sich der Befehl `kadmind` beim Start der inkrementellen Weitergabe authentifizieren.

```
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc1.example.com
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local:
```

e. Beenden Sie `kadmin.local`.

Sie haben alle erforderlichen Hauptelemente für die nächsten Schritte hinzugefügt.

```
kadmin.local: quit
```

7 Starten Sie die Kerberos-Dämonen.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

8 Starten Sie `kadmin` und fügen Sie weitere Hauptelemente hinzu.

Zu diesem Zeitpunkt können Sie Hauptelemente mit dem Graphical Kerberos Administration Tool hinzufügen. Dazu müssen Sie sich mit einem der zuvor in diesem Verfahren erstellten `admin`-Hauptelementnamen anmelden. Der Einfachheit halber wird hier das folgende Befehlszeilenbeispiel gezeigt.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Erstellen Sie das `host`-Hauptelement für das Master-KDC.

Das Host-Hauptelement wird von kerberisierten Anwendungen wie `kprop` zur Weitergabe von Änderungen an Slave-KDCs verwendet. Dieses Hauptelement dient auch dazu, sicheren Remote-Zugriff auf den KDC-Server für Anwendungen wie `ssh` zu bieten. Wenn die Hauptelementinstanz ein Hostname ist, muss der FQDN unabhängig von der Schreibung des Domainnamens in der Datei `/etc/resolv.conf` in Kleinbuchstaben angegeben werden.

```
kadmin: addprinc -randkey host/kdc1.example.com
Principal "host/kdc1.example.com@EXAMPLE.COM" created.
kadmin:
```

b. (Optional) Erstellen Sie das `kclient`-Hauptelement.

Dieses Hauptelement wird vom Dienstprogramm `kclient` während der Installation eines Kerberos-Clients verwendet. Sie müssen das Hauptelement nur hinzufügen, wenn Sie dieses Dienstprogramm verwenden möchten. Die Benutzer des Dienstprogramms `kclient` müssen dieses Passwort verwenden.

```
kadmin: addprinc clntconfig/admin
Enter password for principal clntconfig/admin@EXAMPLE.COM:     <Type the password>
Re-enter password for principal clntconfig/admin@EXAMPLE.COM:      <Type it again>
Principal "clntconfig/admin@EXAMPLE.COM" created.
kadmin:
```

c. Fügen Sie das `host`-Hauptelement des Master-KDC der Schlüsseltabellendatei des Master-KDC hinzu.

Durch Hinzufügen des Host-Hauptelements zur Schlüsseltabellendatei kann es von Anwendungsservern wie `sshd` automatisch verwendet werden.

```
kadmin: ktadd host/kdc1.example.com
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
```

```
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

d. Beenden Sie `kadmin`.

```
kadmin: quit
```

9 (Optional) Synchronisieren Sie die Uhr des Master-KDC mit NTP oder einem anderen Synchronisierungsmechanismus für Uhren.

Die Installation und Verwendung des Network Time Protocol (NTP) ist nicht obligatorisch. Alle Uhren müssen sich innerhalb der im Abschnitt `libdefaults` der Datei `krb5.conf` definierten Standardzeit befinden. Informationen zu NTP finden Sie unter „Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients“ auf Seite 482.

10 Konfigurieren Sie Slave-KDCs.

Um für Redundanz zu sorgen, installieren Sie mindestens ein Slave-KDC. Genaue Anweisungen finden Sie unter „So konfigurieren Sie ein Slave-KDC manuell“ auf Seite 451.

▼ So konfigurieren Sie ein KDC zur Verwendung eines LDAP-Datenservers

Ab der Version Solaris 10 5/08 kann ein KDC mit folgendem Verfahren zur Verwendung eines LDAP-Datenservers konfiguriert werden.

In diesem Verfahren werden die folgenden Konfigurationsparameter verwendet:

- Realm name = `EXAMPLE.COM`
- DNS-Domainname = `example.com`
- Master-KDC = `kdc1.example.com`
- Verzeichnisserver = `dsserver.example.com`
- `admin`-Hauptelement = `kws/admin`
- FMRI für den LDAP-Service = `svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1`
- Onlinehilfe-URL = `http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956`

Hinweis – Passen Sie die URL an, sodass sie auf den Bereich "Graphical Kerberos Administration Tool" verweist, wie in „Onlinehilfe-URL im Graphical Kerberos Administration Tool“ auf Seite 434 beschrieben.

Bevor Sie beginnen Für dieses Verfahren muss der Host außerdem zur Verwendung von DNS konfiguriert sein. Um die Leistung zu verbessern, installieren Sie das KDC und den LDAP-Directory Service auf dem gleichen Server. Außerdem muss ein Verzeichnisserver ausgeführt werden. Das unten beschriebene Verfahren funktioniert mit Servern, die über die Sun Java Directory Server Enterprise Edition-Version verfügen.

1. **Melden Sie sich als Superuser beim KDC an.**

2. **Erstellen Sie ein Zertifikat für den Verzeichnisserver und importieren Sie es.**

   Mit den folgenden Schritten konfigurieren Sie ein S10-KDC zur Verwendung des selbstsignierten Zertifikats von Directory Server 6.1. Wenn das Zertifikat abgelaufen ist, führen Sie die Anweisungen zum Erneuern von Zertifikaten unter „To Manage Self-Signed Certificates“ in *Sun Java System Directory Server Enterprise Edition 6.2 Administration Guide* aus.

   a. **Exportieren Sie das selbstsignierte Verzeichnisserverzertifikat.**

      ```
      # /usr/sfw/bin/certutil -L -n defaultCert -d /export/sun-ds6.1/directory/alias \
              -P 'slapd-' -a > /var/tmp/ds_cert.pem
      ```

   b. **Erstellen Sie eine lokale Zertifikatdatenbank.**

      ```
      # /usr/sfw/bin/certutil -N -d /var/ldap
      ```

   c. **Fügen Sie das Verzeichnisserverzertifikat der lokalen Zertifikatdatenbank hinzu.**

      ```
      # /usr/sfw/bin/certutil -A -n defaultCert -i /var/tmp/ds_cert -a -t CT -d /var/ldap
      ```

   d. **Importieren Sie das Verzeichnisserverzertifikat.**

```
# pktool setpin keystore=nss dir=/var/ldap
# chmod a+r /var/ldap/*.db
# pktool import keystore=nss objtype=cert trust="CT" infile=/tmp/defaultCert.certutil.der \
        label=defaultCert dir=/var/ldap
```

3. **Nehmen Sie Daten in das LDAP-Verzeichnis auf, falls nötig.**

4. **Fügen Sie das Kerberos-Schema dem vorhandenen Schema hinzu.**

```
# ldapmodify -h dsserver.example.com -D "cn=directory manager" -f /usr/share/lib/ldif/kerberos.ldif
```

5 Erstellen Sie den Kerberos-Container im LDAP-Verzeichnis.

Fügen Sie die folgenden Einträge der Datei `krb5.conf` hinzu.

a. Definieren Sie den Datenbanktyp.

Fügen Sie einen Eintrag zum Definieren des `database_module` im Abschnitt `realms` hinzu.

```
database_module = LDAP
```

b. Definieren Sie das Datenbankmodul.

```
[dbmodules]
    LDAP = {
        ldap_kerberos_container_dn = "cn=krbcontainer,dc=example,dc=com"
        db_library = kldap
        ldap_kdc_dn = "cn=kdc service,ou=profile,dc=example,dc=com"
        ldap_kadmind_dn = "cn=kadmin service,ou=profile,dc=example,dc=com"
        ldap_cert_path = /var/ldap
        ldap_servers = ldaps://dsserver.example.com
    }
```

c. Erstellen Sie das KDC im LDAP-Verzeichnis.

Dieser Befehl erstellt `krbcontainer` und mehrere andere Objekte. Er erstellt auch die `/var/krb5/.k5.EXAMPLE.COM`-Stash-Datei mit dem Master-Schlüssel.

```
# kdb5_ldap_util -D "cn=directory manager" create -P abcd1234 -r EXAMPLE.COM -s
```

6 Nehmen Sie die Distinguished Name (DN)-Passwörter für die KDC-Bindung in der Stash-Datei auf.

Mit diesen Passwörtern stellt das KDC eine Verbindung zum Verzeichnisserver her. Das KDC verwendet verschiedene Rollen, abhängig vom entsprechenden Zugriffstyp.

```
# kdb5_ldap_util stashsrvpw "cn=kdc service,ou=profile,dc=example,dc=com"
# kdb5_ldap_util stashsrvpw "cn=kadmin service,ou=profile,dc=example,dc=com"
```

7 Fügen Sie KDC-Servicerollen hinzu.

a. Erstellen Sie die Datei `kdc_roles.ldif` mit dem folgenden oder einem ähnlichen Inhalt:

```
dn: cn=kdc service,ou=profile,dc=example,dc=com
cn: kdc service
sn: kdc service
objectclass: top
objectclass: person
userpassword: test123

dn: cn=kadmin service,ou=profile,dc=example,dc=com
cn: kadmin service
sn: kadmin service
objectclass: top
objectclass: person
userpassword: test123
```

b. Erstellen Sie die Rolleneinträge im LDAP-Verzeichnis.

```
# ldapmodify -a -h dsserver.example.com -D "cn=directory manager" -f kdc_roles.ldif
```

8 Stellen Sie die ACLs für die KDC-Rollen ein.

```
# cat << EOF | ldapmodify -h dsserver.example.com -D "cn=directory manager"
# Set kadmin ACL for everything under krbcontainer.
dn: cn=krbcontainer,dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///cn=krbcontainer,dc=example,dc=com")(targetattr="krb*")(version 3.0;\
      acl kadmin_ACL; allow (all)\
      userdn = "ldap:///cn=kadmin service,ou=profile,dc=example,dc=com";)

# Set kadmin ACL for everything under the people subtree if there are
# mix-in entries for krb princs:
dn: ou=people,dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///ou=people,dc=example,dc=com")(targetattr="krb*")(version 3.0;\
      acl kadmin_ACL; allow (all)\
      userdn = "ldap:///cn=kadmin service,ou=profile,dc=example,dc=com";)
EOF
```

9 Bearbeiten Sie die Kerberos-Konfigurationsdatei (`krb5.conf`).

Sie müssen die Bereichsnamen und Servernamen ändern. Eine vollständige Beschreibung dieser Datei finden Sie auf der Manpage `krb5.conf`(4).

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = EXAMPLE.COM

[realms]
        EXAMPLE.COM = {
        kdc = kdc1.example.com
        admin_server = kdc1.example.com
        }

[domain_realm]
        .example.com = EXAMPLE.COM
#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
        default = FILE:/var/krb5/kdc.log
        kdc = FILE:/var/krb5/kdc.log

[appdefaults]
    gkadmin = {
        help_url = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956
        }
```

In diesem Beispiel wurden die Zeilen für `default_realm`, `kdc`, `admin_server` und alle Einträge von `domain_realm` geändert. Außerdem wurde die Zeile zur Definition der `help_url` bearbeitet.

Hinweis – Um die Verschlüsselungstypen zu beschränken, können Sie die Zeilen `default_tkt_enctypes` oder `default_tgs_enctypes` einstellen. Eine Beschreibung der Probleme beim Beschränken der Verschlüsselungstypen finden Sie unter „Verwenden von Kerberos-Verschlüsselungstypen“ auf Seite 602.

10 Bearbeiten Sie die KDC-Konfigurationsdatei (`kdc.conf`).

Sie müssen den Bereichsnamen ändern. Eine vollständige Beschreibung dieser Datei finden Sie auf der Manpage `kdc.conf(4)`.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM = {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
                sunw_dbprop_master_ulogsize = 1000
                }
```

In diesem Beispiel wurde die Bereichsnamendefinition im Abschnitt `realms` geändert. Im Abschnitt `realms` wurden außerdem Zeilen zum Aktivieren der inkrementellen Weitergabe und für die Anzahl der Aktualisierungen, die der KDC-Master in der Protokolldatei beibehält, hinzugefügt.

Hinweis – Um die Verschlüsselungstypen zu beschränken, können Sie die Zeilen `permitted_enctypes`, `supported_enctypes` oder `master_key_type` einstellen. Eine Beschreibung der Probleme beim Beschränken der Verschlüsselungstypen finden Sie unter „Verwenden von Kerberos-Verschlüsselungstypen“ auf Seite 602.

11 Bearbeiten Sie die Kerberos-Zugriffssteuerungsliste (`kadm5.acl`).

Nach der Datenaufnahme sollte die Datei `/etc/krb5/kadm5.acl` alle Hauptelementnamen enthalten, die zur Verwaltung des KDC berechtigt sind.

```
kws/admin@EXAMPLE.COM    *
```

Der Eintrag ermöglicht dem Hauptelement `kws/admin` im Bereich `EXAMPLE.COM` Hauptelemente oder Richtlinien im KDC zu ändern. Die Standardinstallation enthält ein Sternchen (*) zur Übereinstimmung mit allen `admin`-Hauptelementen. Diese Standardeinstellung kann ein Sicherheitsrisiko darstellen. Es ist sicherer, eine Liste aller `admin`-Hauptelemente einzuschließen. Weitere Informationen finden Sie auf der Manpage `kadm5.acl(4)`.

12 Starten Sie den Befehl `kadmin.local` und fügen Sie Hauptelemente hinzu.

Mit den nächsten Teilschritten erstellen Sie Hauptelemente, die vom Kerberos-Service verwendet werden.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local:
```

a. Fügen Sie der Datenbank Admin-Hauptelemente hinzu.

Sie können so viele `admin`-Hauptelemente hinzufügen, wie Sie benötigen. Sie müssen mindestens ein `admin`-Hauptelement zum Abschließen des KDC-Konfigurationsprozesses hinzufügen. In diesem Beispiel wird ein `kws/admin`-Hauptelement hinzugefügt. Ersetzen Sie `kws` durch einen geeigneten Hauptelementnamen.

```
kadmin.local: addprinc kws/admin
Enter password for principal kws/admin@EXAMPLE.COM:     <Type the password>
Re-enter password for principal kws/admin@EXAMPLE.COM:      <Type it again>
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

b. Erstellen Sie eine Schlüsseltabellendatei für den `kadmind`-Service.

Diese Befehlssequenz erstellt eine spezielle Schlüsseltabellendatei mit Hauptelementeinträgen für `kadmin` und `changepw`. Diese Hauptelemente werden für den `kadmind`-Service benötigt. Wenn die Hauptelementinstanz ein Hostname ist, muss der FQDN unabhängig von der Schreibung des Domainnamens in der Datei `/etc/resolv.conf` in Kleinbuchstaben angegeben werden.

```
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc1.example.com
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab changepw/kdc1.example.com
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/changepw
Entry for principal kadmin/changepw with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type Triple DES cbc
```

```
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local:
```

c. Beenden Sie `kadmin.local`.

Sie haben alle erforderlichen Hauptelemente für die nächsten Schritte hinzugefügt.

```
kadmin.local: quit
```

13 (Optional) Konfigurieren Sie die LDAP-Abhängigkeit für Kerberos-Services.

Wenn die LDAP- und KDC-Server auf demselben Host ausgeführt werden und der LDAP-Service mit einem SMF-FMRI konfiguriert ist, fügen Sie dem LDAP-Service eine Abhängigkeit für die Kerberos-Dämonen hinzu. Dadurch wird der KDC-Service beim Neustart des LDAP-Service gestartet.

a. Fügen Sie die Abhängigkeit dem krb5kdc-Service hinzu.

```
# svccfg -s security/krb5kdc
svc:/network/security/krb5kdc> addpg dsins1 dependency
svc:/network/security/krb5kdc> setprop dsins1/entities = \
    fmri: "svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1"
svc:/network/security/krb5kdc> setprop dsins1/grouping = astring: "require_all"
svc:/network/security/krb5kdc> setprop dsins1/restart_on = astring: "restart"
svc:/network/security/krb5kdc> setprop dsins1/type = astring: "service"
svc:/network/security/krb5kdc> exit
```

b. Fügen Sie die Abhängigkeit dem kadmin-Service hinzu.

```
# svccfg -s security/kadmin
svc:/network/security/kadmin> addpg dsins1 dependency
svc:/network/security/kadmin> setprop dsins1/entities =\
    fmri: "svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1"
svc:/network/security/kadmin> setprop dsins1/grouping = astring: "require_all"
svc:/network/security/kadmin> setprop dsins1/restart_on = astring: "restart"
svc:/network/security/kadmin> setprop dsins1/type = astring: "service"
svc:/network/security/kadmin> exit
```

14 Starten Sie die Kerberos-Dämonen.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

15 Starten Sie `kadmin` und fügen Sie weitere Hauptelemente hinzu.

Zu diesem Zeitpunkt können Sie Hauptelemente mit dem Graphical Kerberos Administration Tool hinzufügen. Dazu müssen Sie sich mit einem der zuvor in diesem Verfahren erstellten `admin`-Hauptelementnamen anmelden. Der Einfachheit halber wird hier das folgende Befehlszeilenbeispiel gezeigt.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Erstellen Sie das `host`-Hauptelement für das Master-KDC.

Das Host-Hauptelement wird von kerberisierten Anwendungen wie `klist` und `kprop` verwendet. Clients verwenden dieses Hauptelement beim Einhängen eines authentifizierten NFS-Dateisystems. Wenn die Hauptelementinstanz ein Hostname ist, muss der FQDN unabhängig von der Schreibung des Domainnamens in der Datei `/etc/resolv.conf` in Kleinbuchstaben angegeben werden.

```
kadmin: addprinc -randkey host/kdc1.example.com
Principal "host/kdc1.example.com@EXAMPLE.COM" created.
kadmin:
```

b. (Optional) Erstellen Sie das `kclient`-Hauptelement.

Dieses Hauptelement wird vom Dienstprogramm `kclient` während der Installation eines Kerberos-Clients verwendet. Sie müssen das Hauptelement nur hinzufügen, wenn Sie dieses Dienstprogramm verwenden möchten. Die Benutzer des Dienstprogramms `kclient` müssen dieses Passwort verwenden.

```
kadmin: addprinc clntconfig/admin
Enter password for principal clntconfig/admin@EXAMPLE.COM:     <Type the password>
Re-enter password for principal clntconfig/admin@EXAMPLE.COM:      <Type it again>
Principal "clntconfig/admin@EXAMPLE.COM" created.
kadmin:
```

c. Fügen Sie das `host`-Hauptelement des Master-KDC der Schlüsseltabellendatei des Master-KDC hinzu.

Durch Hinzufügen des Host-Hauptelements zur Schlüsseltabellendatei kann es automatisch verwendet werden.

```
kadmin: ktadd host/kdc1.example.com
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

d. Beenden Sie `kadmin`.

```
kadmin: quit
```

16 (Optional) Synchronisieren Sie die Uhr des Master-KDC mit NTP oder einem anderen Synchronisierungsmechanismus für Uhren.

Die Installation und Verwendung des Network Time Protocol (NTP) ist nicht obligatorisch. Alle Uhren müssen sich innerhalb der im Abschnitt `libdefaults` der Datei `krb5.conf` definierten Standardzeit befinden. Informationen zu NTP finden Sie unter „Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients“ auf Seite 482.

17 Konfigurieren Sie Slave-KDCs.

Um für Redundanz zu sorgen, installieren Sie mindestens ein Slave-KDC. Genaue Anweisungen finden Sie unter „So konfigurieren Sie ein Slave-KDC manuell“ auf Seite 451.

▼ So konfigurieren Sie ein Slave-KDC manuell

Mit diesem Verfahren wird ein neues Slave-KDC namens `kdc2` konfiguriert. Außerdem wird die inkrementelle Weitergabe konfiguriert. In diesem Verfahren werden die folgenden Konfigurationsparameter verwendet:

- Realm name = `EXAMPLE.COM`
- DNS-Domainname = `example.com`
- Master-KDC = `kdc1.example.com`
- Slave-KDC = `kdc2.example.com`
- `admin`-Hauptelement = `kws/admin`

Bevor Sie beginnen Das Master-KDC muss konfiguriert sein. Wenn dieser Slave austauschbar ist, finden Sie spezielle Anweisungen unter „Austauschen von Master-KDC und Slave-KDC“ auf Seite 484.

1 Melden Sie sich auf dem Master-KDC als Superuser an.

2 Starten Sie `kadmin` auf dem Master-KDC.

Sie müssen sich mit einem der zuvor bei der Konfiguration des Master-KDC erstellten `admin`-Hauptelementnamen anmelden.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Fügen Sie auf dem Master-KDC der Datenbank Slave-Host-Hauptelemente hinzu, falls noch nicht geschehen.

Damit der Slave ordnungsgemäß funktioniert, muss er über ein Host-Hauptelement verfügen. Wenn die Hauptelementinstanz ein Hostname ist, muss der FQDN unabhängig von der Schreibung des Domainnamens in der Datei `/etc/resolv.conf` in Kleinbuchstaben angegeben werden.

```
kadmin: addprinc -randkey host/kdc2.example.com
Principal "host/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

b. Erstellen Sie das `kiprop`-Hauptelement auf dem Master-KDC.

Das `kiprop`-Hauptelement dient zur Autorisierung der inkrementellen Weitergabe vom Master-KDC.

```
kadmin: addprinc -randkey kiprop/kdc2.example.com
Principal "kiprop/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

c. Beenden Sie `kadmin`.

```
kadmin: quit
```

3 Bearbeiten Sie die Kerberos-Konfigurationsdatei (`krb5.conf`) auf dem Master-KDC.

Sie müssen einen Eintrag pro Slave hinzufügen. Eine vollständige Beschreibung dieser Datei finden Sie auf der Manpage `krb5.conf(4)`.

```
kdc1 # cat /etc/krb5/krb5.conf
 .
 .
[realms]
                EXAMPLE.COM = {
                kdc = kdc1.example.com
                kdc = kdc2.example.com
                admin_server = kdc1.example.com
        }
```

4 Fügen Sie auf dem Master-KDC der Datei `kadm5.acl` einen `kiprop`-Eintrag hinzu.

Durch diesen Eintrag erhält das Master-KDC Anforderungen zur inkrementellen Weitergabe für den `kdc2`-Server.

```
kdc1 # cat /etc/krb5/kadm5.acl
*/admin@EXAMPLE.COM *
kiprop/kdc2.example.com@EXAMPLE.COM p
```

5 Starten Sie `kadmind` auf dem Master-KDC neu, um die neuen Einträge in der Datei `kadm5.acl` zu verwenden.

```
kdc1 # svcadm restart network/security/kadmin
```

6 Kopieren Sie die KDC-Administrationsdateien vom Master-KDC-Server auf alle Slave-KDCs.

Dieser Schritt ist für alle Slave-KDCs obligatorisch, da der Master-KDC-Server über aktualisierte Informationen verfügt, die auf den KDC-Servern benötigt werden. Sie können `ftp` oder einen ähnlichen Transfermechanismus verwenden, um Kopien der folgenden Dateien vom Master-KDC zu übertragen:

- `/etc/krb5/krb5.conf`
- `/etc/krb5/kdc.conf`

7 Fügen Sie auf allen Slave-KDCs einen Eintrag für das Master-KDC hinzu und fügen Sie jedes Slave-KDC in die Konfigurationsdatei zur Weitergabe der Datenbank (`kpropd.acl`) ein.

Diese Informationen müssen auf allen Slave-KDC-Servern aktualisiert werden.

```
kdc2 # cat /etc/krb5/kpropd.acl
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
```

8 Stellen Sie auf allen Slave-KDCs sicher, dass die Kerberos-Zugriffssteuerungsliste `kadm5.acl` nicht mit Daten angefüllt ist.

In unverändertem Zustand sieht die Datei `kadm5.acl` etwa folgendermaßen aus:

```
kdc2 # cat /etc/krb5/kadm5.acl
*/admin@___default_realm___ *
```

Wenn die Datei `kiprop`-Einträge enthält, entfernen Sie diese.

9 Ändern Sie auf einem neuen Slave einen Eintrag in `kdc.conf`.

Ersetzen Sie den Eintrag `sunw_dbprop_master_ulogsize` durch einen Eintrag zur Definition von `sunw_dbprop_slave_poll`. Dieser Eintrag stellt eine Abfragezeit von 2 Minuten ein.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM= {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
                sunw_dbprop_slave_poll = 2m
        }
```

10 Starten Sie den Befehl `kadmin` auf dem neuen Slave.

Sie müssen sich mit einem der zuvor bei der Konfiguration des Master-KDC erstellten `admin`-Hauptelementnamen anmelden.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Fügen Sie mithilfe von `kadmin` das Host-Hauptelement des Slaves der Schlüsseltabellendatei des Slaves hinzu.

Dieser Eintrag stellt die ordnungsgemäße Funktion von `kprop` und anderen kerberisierten Anwendungen sicher. Wenn die Hauptelementinstanz ein Hostname ist, muss der FQDN unabhängig von der Schreibung des Domainnamens in der Datei `/etc/resolv.conf` in Kleinbuchstaben angegeben werden.

```
kadmin: ktadd host/kdc2.example.com
Entry for principal host/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

b. Fügen Sie das `kiprop`-Hauptelement der Schlüsseltabellendatei des Slave-KDC hinzu.

Durch Hinzufügen des `kiprop`-Hauptelements zur Datei `krb5.keytab` kann sich der Befehl `kpropd` beim Start der inkrementellen Weitergabe authentifizieren.

```
kadmin: ktadd kiprop/kdc2.example.com
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

c. Beenden Sie `kadmin`.

```
kadmin: quit
```

11 Starten Sie den Kerberos-Weitergabedämon auf dem neuen Slave.

```
kdc2 # /usr/lib/krb5/kpropd
```

12 Erstellen Sie mit `kdb5_util` auf dem neuen Slave eine Stash-Datei.

```
kdc2 # /usr/sbin/kdb5_util stash
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key

Enter KDC database master key:      <Type the key>
```

13 Brechen Sie den Kerberos-Weitergabedämon ab.

```
kdc2 # pkill kpropd
```

14 (Optional) Synchronisieren Sie die Uhr des neuen Slave-KDC mit derjenigen des Master-KDC, indem Sie NTP oder einen anderen Synchronisierungsmechanismus für Uhren verwenden.

Die Installation und Verwendung des Network Time Protocol (NTP) ist nicht obligatorisch. Alle Uhren müssen sich innerhalb der im Abschnitt `libdefaults` der Datei `krb5.conf` definierten Standardzeit befinden. Informationen zu NTP finden Sie unter „Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients“ auf Seite 482.

15 Starten Sie den KDC-Dämon (`krb5kdc`) auf dem neuen Slave.

Wenn der `krb5kdc`-Service aktiviert ist, wird `kpropd` ebenfalls gestartet, sofern das System als Slave konfiguriert ist.

```
kdc2 # svcadm enable network/security/krb5kdc
```

▼ So aktualisieren Sie die Ticket Granting Service-Schlüssel auf einem Master-Server

Wenn das TGS-Hauptelement (Ticket Granting Service) nur über einen DES-Schlüssel verfügt, was bei KDC-Servern vor Solaris 10 der Fall ist, beschränkt der Schlüssel den Verschlüsselungstyp des TGT-Sitzungsschlüssels (Ticket Granting Ticket) auf DES. Wenn ein KDC auf eine Version aktualisiert wird, die zusätzliche stärkere Verschlüsselungstypen unterstützt, wird erwartungsgemäß die stärkere Verschlüsselung für alle vom KDC generierten Sitzungsschlüssel verwendet. Wenn das vorhandene TGS-Hauptelement nicht mit den neuen Verschlüsselungstypen aktualisiert wird, ist der TGT-Sitzungsschlüssel weiterhin auf DES beschränkt. Das folgende Verfahren aktualisiert den Schlüssel, sodass zusätzliche Verschlüsselungstypen verwendet werden können.

- **Aktualisieren Sie den Hauptelementschlüssel des TGS-Service.**

```
kdc1 % /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin: cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

Beispiel 23–1 Aktualisieren der Hauptelementschlüssel von einem Master-Server

Wenn Sie auf dem KDC-Master als `root` angemeldet sind, können Sie das Hauptelement für den TGS-Service mit dem folgenden Befehl aktualisieren:

```
kdc1 # kadmin.local -q 'cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM'
```

Konfigurieren von bereichsübergreifender Authentifizierung

Es gibt verschiedene Möglichkeiten zum Verknüpfen von Bereichen, sodass Benutzer aus einem Bereich in einem anderen Bereich authentifiziert werden können. Eine bereichsübergreifende Authentifizierung wird durch Einrichtung eines Geheimschlüssels erreicht, der von beiden Bereichen ausgetauscht wird. Die Beziehung zwischen den Bereichen kann entweder hierarchisch oder gerichtet sein (siehe „Bereichshierarchie“ auf Seite 427).

▼ So richten Sie eine hierarchische bereichsübergreifende Authentifizierung ein

In diesem Beispiel werden die beiden Bereiche `ENG.EAST.EXAMPLE.COM` und `EAST.EXAMPLE.COM` verwendet. Die bereichsübergreifende Authentifizierung wird für beide Richtungen eingerichtet. Dieses Verfahren muss auf dem Master-KDC in beiden Bereichen ausgeführt werden.

Bevor Sie beginnen Das Master-KDC der einzelnen Bereiche muss konfiguriert sein. Für einen vollständigen Test des Authentifizierungsprozesses müssen mehrere Kerberos-Clients konfiguriert sein.

1. **Melden Sie sich beim ersten Master-KDC als Superuser an.**

2. **Erstellen Sie TGT-Service-Hauptelemente für beide Bereiche.**

   Sie müssen sich mit einem der zuvor bei der Konfiguration des Master-KDC erstellten `admin`-Hauptelementnamen anmelden.

```
# /usr/sbin/kadmin -p kws/admin
Enter password:     <Type kws/admin password>
kadmin: addprinc krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM
Enter password for principal krgtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM:      <Type password>
kadmin: addprinc krbtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM
Enter password for principal krgtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM:      <Type password>
kadmin: quit
```

Hinweis – Das für die Service-Hauptelemente angegebene Passwort muss auf beiden KDCs identisch sein. Daher muss das Passwort für das Service-Hauptelement `krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM` in beiden Bereiche gleich sein.

3 Fügen Sie der Kerberos-Konfigurationsdatei (`krb5.conf`) Einträge hinzu, um die Domainnamen für die Bereiche zu definieren.

```
# cat /etc/krb5/krb5.conf
[libdefaults]
 .
 .
[domain_realm]
        .eng.east.example.com = ENG.EAST.EXAMPLE.COM
        .east.example.com = EAST.EXAMPLE.COM
```

In diesem Beispiel werden Domainnamen für die Bereiche `ENG.EAST.EXAMPLE.COM` und `EAST.EXAMPLE.COM` definiert. Die Subdomain muss unbedingt zuerst aufgeführt werden, da die Datei von oben nach unten durchsucht wird.

4 Kopieren Sie die Kerberos-Konfigurationsdatei auf alle Clients in diesem Bereich.

Damit die bereichsübergreifende Authentifizierung funktioniert, muss auf allen Systemen (einschließlich des Slave-KDCs und anderer Server) die neue Version der Kerberos-Konfigurationsdatei (`/etc/krb5/krb5.conf`) installiert sein.

5 Wiederholen Sie diese Schritte im zweiten Bereich.

▼ So richten Sie eine direkte bereichsübergreifende Authentifizierung ein

In diesem Beispiel werden die beiden Bereiche `ENG.EAST.EXAMPLE.COM` und `SALES.WEST.EXAMPLE.COM` verwendet. Die bereichsübergreifende Authentifizierung wird für beide Richtungen eingerichtet. Dieses Verfahren muss auf dem Master-KDC in beiden Bereichen ausgeführt werden.

Bevor Sie beginnen Das Master-KDC der einzelnen Bereiche muss konfiguriert sein. Für einen vollständigen Test des Authentifizierungsprozesses müssen mehrere Kerberos-Clients konfiguriert sein.

1 Melden Sie sich als Superuser bei einem der Master-KDC-Server an.

2 Erstellen Sie TGT-Service-Hauptelemente für beide Bereiche.

Sie müssen sich mit einem der zuvor bei der Konfiguration des Master-KDC erstellten `admin`-Hauptelementnamen anmelden.

```
# /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
```

```
kadmin: addprinc krbtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM
Enter password for principal
  krgtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM:       <Type the password>
kadmin: addprinc krbtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM
Enter password for principal
  krgtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM:       <Type the password>
kadmin: quit
```

Hinweis – Das für die Service-Hauptelemente angegebene Passwort muss auf beiden KDCs identisch sein. Daher muss in beiden Bereichen das gleiche Passwort für das Service-Hauptelement `krbtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM` verwendet werden.

3 Fügen Sie in der Kerberos-Konfigurationsdatei Einträge hinzu, um den direkten Pfad zum Remote-Bereich zu definieren.

In diesem Beispiel werden die Clients im Bereich `ENG.EAST.EXAMPLE.COM` gezeigt. Um die entsprechenden Definitionen im Bereich `SALES.WEST.EXAMPLE.COM` zu erhalten, müssen Sie die Bereichsnamen austauschen.

```
# cat /etc/krb5/krb5.conf
[libdefaults]
 .
 .
[capaths]
    ENG.EAST.EXAMPLE.COM = {
        SALES.WEST.EXAMPLE.COM = .
    }

    SALES.WEST.EXAMPLE.COM = {
         ENG.EAST.EXAMPLE.COM = .
    }
```

4 Kopieren Sie die Kerberos-Konfigurationsdatei auf alle Clients im aktuellen Bereich.

Damit die bereichsübergreifende Authentifizierung funktioniert, muss auf allen Systemen (einschließlich des Slave-KDCs und anderer Server) die neue Version der Kerberos-Konfigurationsdatei (`/etc/krb5/krb5.conf`) installiert sein.

5 Wiederholen Sie diese Schritte im zweiten Bereich.

Konfigurieren von Kerberos-Netzwerkanwendungsservern

Netzwerkanwendungsserver sind Hosts, die Zugriff auf eine oder mehrere der folgenden Netzwerkanwendungen bieten: `ftp`, `rcp`, `rlogin`, `rsh`, `ssh` und `telnet`. Die Kerberos-Version dieser Befehle kann mit wenigen Schritten auf einem Server aktiviert werden.

So konfigurieren Sie einen Kerberos-Netzwerkanwendungsserver

In diesem Verfahren werden die folgenden Konfigurationsparameter verwendet:

- Anwendungsserver = `boston`
- `admin`-Hauptelement = `kws/admin`
- DNS-Domainname = `example.com`
- Realm name = `EXAMPLE.COM`

Bevor Sie beginnen Für dieses Verfahren muss das Master-KDC konfiguriert sein. Für einen vollständigen Test des Prozesses müssen mehrere Kerberos-Clients konfiguriert sein.

1 (Optional) Installieren Sie den NTP-Client oder einen anderen Synchronisierungsmechanismus für Uhren.

Informationen zu NTP finden Sie unter „Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients“ auf Seite 482.

2 Fügen Sie Hauptelemente für den neuen Server hinzu und aktualisieren Sie die Schlüsseltabelle des Servers.

Mit dem folgenden Befehl stellen Sie fest, ob das Host-Hauptelement vorhanden ist:

```
boston # klist -k |grep host
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
```

Wenn der Befehl kein Hauptelement zurückgibt, erstellen Sie mit folgenden Schritten neue Hauptelemente.

Die Verwendung des Graphical Kerberos Administration-Tools wird unter „So erstellen Sie ein neues Kerberos-Hauptelement“ auf Seite 538 erläutert. In den folgenden Schritten wird anhand eines Beispiels erläutert, wie die erforderlichen Hauptelemente mithilfe der Befehlszeile hinzugefügt werden. Sie müssen sich mit einem der zuvor bei der Konfiguration des Master-KDC erstellten `admin`-Hauptelementnamen anmelden.

```
boston # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Erstellen Sie das `host`-Hauptelement des Servers.

Das `host`-Hauptelement wird zu folgenden Zwecken verwendet:

- Authentifizieren des Datenverkehrs bei Verwendung von Remote-Befehlen wie `rsh` und `ssh`
- Ermöglicht `pam_krb5` KDC-Spoofing-Angriffe zu verhindern, indem mithilfe des `host`-Hauptelements sichergestellt wird, dass der Kerberos-Berechtigungsnachweis von einem vertrauenswürdigen KDC stammt.
- Ermöglicht dem `root`-Benutzer, automatisch einen Kerberos-Berechtigungsnachweis zu erhalten, ohne dass ein `root`-Hauptelement vorhanden sein muss. Dies kann beim manuellen Einhängen einer NFS-Komponente nützlich sein, wenn für die Komponente ein Kerberos-Berechtigungsnachweis erforderlich ist.

Dieses Hauptelement ist erforderlich, wenn der Datenverkehr über die Remote-Anwendung mithilfe des Kerberos-Service authentifiziert werden soll. Wenn dem Server mehrere Hostnamen zugewiesen sind, erstellen Sie ein Hauptelement für jeden Hostnamen unter Verwendung der FQDN-Form des Hostnamens.

```
kadmin: addprinc -randkey host/boston.example.com
Principal "host/boston.example.com" created.
kadmin:
```

b. Fügen Sie das `host`-Hauptelement der Schlüsseltabelle des Servers hinzu.

Wenn der Befehl `kadmin` noch nicht ausgeführt wird, starten Sie ihn mit einem Befehl ähnlich dem folgenden: `/usr/sbin/kadmin -p` *kws*`/admin`

Wenn dem Server mehrere Hostnamen zugewiesen sind, fügen Sie der Schlüsseltabelle für jeden Hostnamen ein Hauptelement hinzu.

```
kadmin: ktadd host/boston.example.com
Entry for principal host/boston.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

c. Beenden Sie `kadmin`.

```
kadmin: quit
```

Konfigurieren von Kerberos-NFS-Servern

NFS-Services identifizieren Benutzer anhand von UNIX-Benutzer-IDs (UIDs) und können GSS-Berechtigungsnachweise nicht direkt verwenden. Um Berechtigungsnachweise in UIDs umzuwandeln, muss möglicherweise eine Tabelle erstellt werden, in der Berechtigungsnachweise von Benutzern den entsprechenden UNIX-UIDs zugeordnet werden. Weitere Informationen zur Standardzuordnung von Berechtigungsnachweisen finden Sie unter „Zuordnen von GGS-Berechtigungsnachweisen zu UNIX-Berechtigungsnachweisen“ auf Seite 430. Bei den Verfahren in diesem Abschnitt liegt der Schwerpunkt auf den Aufgaben, die zur Konfiguration eines Kerberos-NFS-Servers, zur Verwaltung der Berechtigungsnachweistabelle und zum Starten der Kerberos-Sicherheitsmodi für über NFS eingehängte Dateisysteme notwendig sind. In der folgenden Übersicht der Schritte werden die Aufgaben in diesem Abschnitt beschrieben.

TABELLE 23–2 Konfigurieren von Kerberos-NFS-Servern (Übersicht der Schritte)

Aufgabe	Description (Beschreibung)	Anweisungen
Konfigurieren eines Kerberos-NFS-Servers	Ermöglicht einem Server die gemeinsame Nutzung eines Dateisystems, das eine Kerberos-Authentifizierung erfordert	„So konfigurieren Sie Kerberos-NFS-Server“ auf Seite 462
Erstellen einer Berechtigungsnachweistabelle	Generiert eine Berechtigungsnachweistabelle, mit der GSS-Berechtigungsnachweise den entsprechenden UNIX-Benutzer-IDs zugeordnet werden, wenn die Standardzuordnung nicht ausreicht	„So erstellen Sie eine Berechtigungsnachweistabelle“ auf Seite 463
Ändern der Berechtigungsnachweistabelle, in der die Benutzerberechtigungsnachweise den entsprechenden UNIX-UIDs zugeordnet werden	Aktualisiert die Informationen in der Berechtigungsnachweistabelle	„So fügen Sie der Berechtigungstabelle einen einzelnen Eintrag hinzu“ auf Seite 464
Erstellen von Berechtigungsnachweisen zwischen ähnlichen Bereichen	Bietet Anweisungen zur Zuordnung von UIDs zwischen zwei Bereichen, wenn die Bereiche über eine gemeinsame Passwortdatei verfügen	„So ordnen Sie Berechtigungsnachweise zwischen Bereichen zu“ auf Seite 465
Gemeinsames Nutzen eines Dateisystems mit Kerberos-Authentifizierung	Ermöglicht die gemeinsame Nutzung eines Dateisystems unter Verwendung von Sicherheitsmodi, sodass eine Kerberos-Authentifizierung erforderlich ist	„So richten Sie eine sichere NFS-Umgebung mit mehreren Kerberos-Sicherheitsmodi ein“ auf Seite 466

▼ So konfigurieren Sie Kerberos-NFS-Server

In diesem Verfahren werden die folgenden Konfigurationsparameter verwendet:

- Realm name = `EXAMPLE.COM`
- DNS-Domainname = `example.com`
- NFS-Server = `denver.example.com`
- `admin`-Hauptelement = `kws/admin`

1 Sorgen Sie dafür, dass die Voraussetzungen für die Konfiguration eines Kerberos-NFS-Servers erfüllt sind.

Das Master-KDC muss konfiguriert sein. Für einen vollständigen Test des Prozesses sind mehrere Clients erforderlich.

2 (Optional) Installieren Sie den NTP-Client oder einen anderen Synchronisierungsmechanismus für Uhren.

Die Installation und Verwendung des Network Time Protocol (NTP) ist nicht obligatorisch. Damit die Authentifizierung erfolgreich ist, müssen alle Uhren mit der Uhrzeit auf dem KDC-Server synchronisiert sein, wobei die maximale Abweichung durch die `clockskew`-Beziehung in der Datei `krb5.conf` definiert wird. Informationen zu NTP finden Sie unter „Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients“ auf Seite 482.

3 Konfigurieren Sie den NFS-Server als Kerberos-Client.

Befolgen Sie die Anweisungen unter „Konfigurieren von Kerberos-Clients“ auf Seite 468.

4 Starten Sie `kadmin`.

Sie können das Graphical Kerberos Administration Tool verwenden, wie unter „So erstellen Sie ein neues Kerberos-Hauptelement“ auf Seite 538 erläutert. Dazu müssen Sie sich mit einem der zuvor bei der Konfiguration des Master-KDC erstellten `admin`-Hauptelementnamen anmelden. In dem folgenden Beispiel wird gezeigt, wie die erforderlichen Hauptelemente mithilfe der Befehlszeile hinzufügt werden.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Erstellen Sie das NFS-Service-Hauptelement des Servers.

Wenn die Hauptelementinstanz ein Hostname ist, muss der FQDN unabhängig von der Schreibung des Domainnamens in der Datei `/etc/resolv.conf` in Kleinbuchstaben angegeben werden.

Wiederholen Sie diesen Schritt für jede eindeutige Schnittstelle im System, die für den Zugriff auf NFS-Daten verwendet werden könnte. Wenn ein Host mehrere Schnittstellen mit eindeutigen Namen aufweist, muss jeder eindeutige Name über ein eigenes NFS-Service-Hauptelement verfügen.

```
kadmin: addprinc -randkey nfs/denver.example.com
Principal "nfs/denver.example.com" created.
kadmin:
```

b. Fügen Sie das NFS-Service-Hauptelement der Schlüsseltabellendatei des Servers hinzu.

Wiederholen Sie diesen Schritt für jedes eindeutige in Schritt a erstellte Service-Hauptelement.

```
kadmin: ktadd nfs/denver.example.com
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs denver.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

c. Beenden Sie `kadmin`.

```
kadmin: quit
```

5 (Optional) Erstellen Sie bei Bedarf besondere GSS-Berechtigungsnachweistabellen.

Normalerweise generiert der Kerberos-Service geeignete Zuordnungen zwischen den GSS-Berechtigungsnachweisen und den UNIX-UIDs. Die Standardzuordnung wird in „Zuordnen von GGS-Berechtigungsnachweisen zu UNIX-Berechtigungsnachweisen“ auf Seite 430 beschrieben. Wenn die Standardzuordnung nicht ausreicht, finden Sie weitere Informationen unter „So erstellen Sie eine Berechtigungsnachweistabelle“ auf Seite 463.

6 Geben Sie das NFS-Dateisystem zur gemeinsamen Nutzung unter Verwendung von Kerberos-Sicherheitsmodi frei.

Weitere Informationen finden Sie unter „So richten Sie eine sichere NFS-Umgebung mit mehreren Kerberos-Sicherheitsmodi ein“ auf Seite 466.

▼ So erstellen Sie eine Berechtigungsnachweistabelle

Die Berechtigungsnachweistabelle `gsscred` wird von einem NFS-Server verwendet, um Kerberos-Berechtigungsnachweise UIDs zuzuordnen. Standardmäßig wird der Primärteil des Hauptelementnamens einem UNIX-Anmeldenamen zugeordnet. Diese Tabelle muss erstellt werden, wenn die Standardzuordnung nicht ausreicht, damit NFS-Clients Dateisysteme von einem NFS-Server mit Kerberos-Authentifizierung einhängen können.

1. **Bearbeiten Sie `/etc/gss/gsscred.conf` und ändern Sie den Sicherheitsmechanismus.**

   Ändern Sie den Mechanismus in `files`.

2. **Erstellen Sie die Berechtigungsnachweistabelle mit dem Befehl `gsscred`.**

   ```
   # gsscred -m kerberos_v5 -a
   ```

   Der Befehl `gsscred` sammelt Informationen aus allen Quellen, die für den `passwd`-Eintrag in der Datei `/etc/nsswitch.conf` angegeben sind. Möglicherweise müssen Sie den Eintrag `files` vorübergehend entfernen, wenn die lokalen Passworteinträge nicht in die Berechtigungsnachweistabelle eingeschlossen werden sollen. Weitere Informationen finden Sie auf der Manpage `gsscred(1M)`.

▼ So fügen Sie der Berechtigungstabelle einen einzelnen Eintrag hinzu

Bevor Sie beginnen Voraussetzung für dieses Verfahren ist, dass die Tabelle `gsscred` bereits auf dem NFS-Server erstellt wurde. Anweisungen finden Sie unter „So erstellen Sie eine Berechtigungsnachweistabelle“ auf Seite 463.

1. **Melden Sie sich als Superuser beim NFS-Server an.**

2. **Fügen Sie der Berechtigungsnachweistabelle mit dem Befehl `gsscred` einen Eintrag hinzu.**

   ```
   # gsscred -m mech [ -n name [ -u uid ]] -a
   ```

mech	Definiert den zu verwendenden Sicherheitsmechanismus
name	Definiert den Hauptelementnamen des Benutzers, wie im KDC angegeben
uid	Definiert die UID des Benutzers, wie in der Passwortdatenbank angegeben
`-a`	Fügt die UID der Hauptelement-Zuordnung zu

Beispiel 23–2 Hinzufügen eines Hauptelements mit mehreren Komponenten zur Berechtigungsnachweistabelle

In dem folgenden Beispiel wird ein Eintrag für ein Hauptelement namens `sandy/admin` hinzugefügt, das UID 3736 zugeordnet wird.

```
# gsscred -m kerberos_v5 -n sandy/admin -u 3736 -a
```

Beispiel 23–3 Hinzufügen eines Hauptelements in einer anderen Domain zur Berechtigungsnachweistabelle

In dem folgenden Beispiel wird ein Eintrag für ein Hauptelement namens `sandy/admin@EXAMPLE.COM` hinzugefügt, das UID `3736` zugeordnet wird.

```
# gsscred -m kerberos_v5 -n sandy/admin@EXAMPLE.COM -u 3736 -a
```

▼ So ordnen Sie Berechtigungsnachweise zwischen Bereichen zu

Dieses Verfahren ermöglicht die Zuordnung der Berechtigungsnachweise von zwei Bereichen, die die gleiche Passwortdatei verwenden. In diesem Beispiel verwenden `CORP.EXAMPLE.COM` und `SALES.EXAMPLE.COM` die gleiche Passwortdatei. Die Berechtigungsnachweise für `bob@CORP.EXAMPLE.COM` und `bob@SALES.EXAMPLE.COM` werden der gleichen UID zugewiesen.

1. **Melden Sie sich als Superuser an.**

2. **Fügen Sie auf dem Clientsystem der Datei `krb5.conf` Einträge hinzu.**

```
# cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = CORP.EXAMPLE.COM
 .
[realms]
    CORP.EXAMPLE.COM = {
        .
        auth_to_local_realm = SALES.EXAMPLE.COM
        .
    }
```

Beispiel 23–4 Zuweisen von Berechtigungsnachweisen zwischen Bereichen mithilfe der gleichen Passwortdatei

Dieses Beispiel zeigt eine geeignete Zuordnung von Berechtigungsnachweisen zweier Bereiche, die die gleiche Passwortdatei verwenden. In diesem Beispiel verwenden `CORP.EXAMPLE.COM` und `SALES.EXAMPLE.COM` die gleiche Passwortdatei. Die Berechtigungsnachweise für `bob@CORP.EXAMPLE.COM` und `bob@SALES.EXAMPLE.COM` werden der gleichen UID zugewiesen. Fügen Sie auf dem Clientsystem der Datei `krb5.conf` Einträge hinzu.

```
# cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = CORP.EXAMPLE.COM
 .
[realms]
    CORP.EXAMPLE.COM = {
        .
```

```
        auth_to_local_realm = SALES.EXAMPLE.COM
        .
    }
```

Allgemeine Fehler Informationen zur Fehlerbehebung bei der Zuordnung von Berechtigungsnachweisen finden Sie unter „Überwachen der Zuordnungen von GSS-Berechtigungsnachweisen zu UNIX-Berechtigungsnachweisen“ auf Seite 525.

▼ So richten Sie eine sichere NFS-Umgebung mit mehreren Kerberos-Sicherheitsmodi ein

Durch dieses Verfahren kann ein NFS-Server sicheren NFS-Zugriff unter Verwendung verschiedener Sicherheitsmodi oder -varianten bieten. Wenn ein Client eine Sicherheitsvariante mit dem NFS-Server aushandelt, wird die erste vom Server angebotene Variante, auf die der Client Zugriff hat, verwendet. Diese Variante wird für alle nachfolgenden Clientanforderungen des Dateisystems verwendet, das vom NFS-Server zur gemeinsamen Nutzung freigegeben wird.

1 Melden Sie sich als Superuser beim NFS-Server an.

2 Stellen Sie sicher, dass die Schlüsseltabellendatei ein NFS-Service-Hauptelement enthält.

Mit dem Befehl `klist` stellen Sie fest, ob eine Schlüsseltabellendatei vorhanden ist und zeigen die Hauptelemente an. Wenn keine Schlüsseltabellendatei oder kein NFS-Service-Hauptelement vorhanden ist, müssen Sie überprüfen, ob alle unter „So konfigurieren Sie Kerberos-NFS-Server“ auf Seite 462 beschriebenen Schritte ausgeführt wurden.

```
# klist -k
Keytab name: FILE:/etc/krb5/krb5.keytab
KVNO Principal
---- --------------------------------------------------------
   3 nfs/denver.example.com@EXAMPLE.COM
   3 nfs/denver.example.com@EXAMPLE.COM
   3 nfs/denver.example.com@EXAMPLE.COM
   3 nfs/denver.example.com@EXAMPLE.COM
```

3 Aktivieren Sie die Kerberos-Sicherheitsmodi in der Datei `/etc/nfssec.conf`.

Bearbeiten Sie die Datei `/etc/nfssec.conf` und entfernen Sie das "#" vor den Kerberos-Sicherheitsmodi.

```
# cat /etc/nfssec.conf
 .
 .
#
# Uncomment the following lines to use Kerberos V5 with NFS
#
krb5            390003  kerberos_v5     default -               # RPCSEC_GSS
```

```
krb5i           390004  kerberos_v5     default integrity       # RPCSEC_GSS
krb5p           390005  kerberos_v5     default privacy         # RPCSEC_GSS
```

4 Bearbeiten Sie die Datei `/etc/dfs/dfstab` und fügen Sie den entsprechenden Einträgen die Option `sec=` mit den erforderlichen Sicherheitsmodi hinzu.

`share -F nfs -o sec=`*mode file-system*

mode Gibt die zu verwendenden Sicherheitsmodi an, wenn das Dateisystem freigegeben wird. Wenn Sie mehrere Sicherheitsmodi verwenden, ist der erste Modus in der Liste der Standardmodus.

file-system Definiert den Pfad des Dateisystems, das gemeinsam genutzt werden soll.

Für alle Clients, die auf Dateien des genannten Dateisystems zugreifen, ist eine Kerberos-Authentifizierung erforderlich. Um auf die Dateien zuzugreifen, muss das Benutzer-Hauptelement auf dem NFS-Client authentifiziert werden.

5 Stellen Sie sicher, dass der NFS-Service auf dem Server ausgeführt wird.

Wenn dieser Befehl der erste `share`-Befehl oder Satz von `share`-Befehlen ist, den Sie initiiert haben, werden die NFS-Dämonen wahrscheinlich nicht ausgeführt. Die Dämonen werden mit dem folgenden Befehl neu gestartet:

```
# svcadm restart network/nfs/server
```

6 (Optional) Wenn Sie den Automounter verwenden, bearbeiten Sie die Datenbank `auto_master`, um einen anderen Sicherheitsmodus als den Standardmodus auszuwählen.

Sie müssen dieses Verfahren nicht ausführen, wenn Sie den Automounter nicht für den Zugriff auf das Dateisystem verwenden oder der standardmäßige Sicherheitsmodus akzeptabel ist.

file-system `auto_home -nosuid,sec=`*mode*

7 (Optional) Geben Sie den Befehl `mount` manuell ein, um auf das Dateisystem in einem nicht standardmäßigen Modus zuzugreifen.

Sie können den Befehl `mount` auch zur Angabe des Sicherheitsmodus verwenden, in diesem Fall wird jedoch der Automounter nicht genutzt.

`# mount -F nfs -o sec=`*mode file-system*

Beispiel 23–5 Freigabe eines Dateisystems mit einem Kerberos-Sicherheitsmodus

In diesem Beispiel bedeutet die Zeile mit der Angabe `dfstab`, dass die Kerberos-Authentifizierung erfolgreich sein muss, bevor über den NFS-Service auf Dateien zugegriffen werden kann.

```
# grep krb /etc/dfs/dfstab
share -F nfs -o sec=krb5 /export/home
```

Beispiel 23–6 Freigabe eines Dateisystems mit mehren Kerberos-Sicherheitsmodi

In diesem Beispiel wurden alle drei Kerberos-Sicherheitsmodi ausgewählt. Welcher Modus verwendet wird, muss zwischen Client und NFS-Server ausgehandelt werden. Wenn der erste Modus im Befehl fehlschlägt, wird der nächste getestet. Weitere Informationen finden Sie auf der Manpage `nfssec(5)`.

```
# grep krb /etc/dfs/dfstab
share -F nfs -o sec=krb5:krb5i:krb5p /export/home
```

Konfigurieren von Kerberos-Clients

Kerberos-Clients schließen in dem Netzwerk, das Kerberos-Services verwenden muss, jeden Host ein, der kein KDC-Server ist. Dieser Abschnitt enthält die Verfahren zum Installieren eines Kerberos-Clients sowie Informationen zur Verwendung der `root`-Authentifizierung zum Einhängen von NFS-Dateisystemen.

Konfigurieren von Kerberos-Clients (Übersicht der Schritte)

In der folgenden Übersicht der Schritte sind alle Verfahren zum Einrichten von Kerberos-Clients aufgeführt. Jede Zeile enthält eine Aufgabenbezeichnung, eine Beschreibung der Gründe für die Aufgabe und einen Link zur Aufgabe.

Aufgabe	Description (Beschreibung)	Anweisungen
Festlegen eines Kerberos-Clientinstallationsprofils	Generiert ein Clientinstallationsprofil, das zur automatischen Installation eines Kerberos-Clients verwendet werden kann	„So erstellen Sie ein Kerberos-Clientinstallationsprofil“ auf Seite 469
Konfigurieren eines Kerberos-Clients	Installiert einen Kerberos-Client manuell. Führen Sie dieses Verfahren aus, wenn jede Clientinstallation eindeutige Installationsparameter benötigt.	„So konfigurieren Sie einen Kerberos-Client manuell“ auf Seite 472
	Installiert einen Kerberos-Client automatisch. Führen Sie dieses Verfahren aus, wenn für jeden Client die gleichen Installationsparameter verwendet werden.	„So konfigurieren Sie einen Kerberos-Client automatisch“ auf Seite 469
	Installiert einen Kerberos-Client interaktiv. Führen Sie dieses Verfahren aus, wenn nur wenige Installationsparameter geändert werden müssen.	„So konfigurieren Sie einen Kerberos-Client interaktiv“ auf Seite 471

Aufgabe	Description (Beschreibung)	Anweisungen
Zulassen, dass Clients auf ein NFS-Dateisystem als `root`-Benutzer zugreifen	Erstellt ein `root`-Hauptelement auf dem Client, sodass der Client ein NFS-Dateisystem einhängen kann, das mit `root`-Zugriff zur gemeinsamen Nutzung freigegeben ist. Ermöglicht dem Client außerdem, nicht interaktiven `root`-Zugriff auf das NFS-Dateisystem einzurichten, sodass cron-Jobs ausgeführt werden können.	„So greifen Sie auf ein durch Kerberos geschütztes NFS-Dateisystem als `root`-Benutzer zu“ auf Seite 478
Deaktivieren der Überprüfung des KDC, das ein Client-TGT (Ticket Granting Ticket) ausgegeben hat	Ermöglicht Clients, in deren lokalen Schlüsseltabellendatei kein Host-Hauptelement gespeichert ist, die Sicherheitsprüfung zu überspringen, die überprüft, ob das KDC, von dem das TGT ausgegeben wurde, dem Server entspricht, von dem das Host-Hauptelement stammt.	„So deaktivieren Sie die Überprüfung des TGT (Ticket Granting Ticket)“ auf Seite 478

▼ So erstellen Sie ein Kerberos-Clientinstallationsprofil

Mit diesem Verfahren wird ein kclient-Profil erstellt, das bei der Installation eines Kerberos-Clients verwendet werden kann. Durch Verwenden des kclient-Profils verringern Sie das Risiko von Schreibfehlern. Außerdem muss der Benutzer im Vergleich zum interaktiven Prozess weniger eingreifen.

1. **Melden Sie sich als Superuser an.**

2. **Erstellen Sie ein kclient-Installationsprofil.**

   Ein kclient-Beispielprofil kann etwa folgendermaßen aussehen:

```
client# cat /net/denver.example.com/export/install/profile
REALM EXAMPLE.COM
KDC kdc1.example.com
ADMIN clntconfig
FILEPATH /net/denver.example.com/export/install/krb5.conf
NFS 1
DNSLOOKUP none
```

▼ So konfigurieren Sie einen Kerberos-Client automatisch

Bevor Sie beginnen

Bei diesem Verfahren wird ein Installationsprofil verwendet. Weitere Informationen finden Sie unter „So erstellen Sie ein Kerberos-Clientinstallationsprofil“ auf Seite 469.

1. **Melden Sie sich als Superuser an.**

2 Führen Sie das Installationsskript `kclient` aus.

Sie müssen das Kennwort für den `clntconfig`-Hauptbenutzer angeben, um den Vorgang durchzuführen.

```
client# /usr/sbin/kclient -p /net/denver.example.com/export/install/profile

Starting client setup
-----------------------------------------------------

kdc1.example.com

Setting up /etc/krb5/krb5.conf.

Obtaining TGT for clntconfig/admin ...
Password for clntconfig/admin@EXAMPLE.COM:      <Type the password>

nfs/client.example.com entry ADDED to KDC database.
nfs/client.example.com entry ADDED to keytab.

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Copied /net/denver.example.com/export/install/krb5.conf.

-----------------------------------------------------
Setup COMPLETE.

client#
```

Beispiel 23–7 Automatisches Konfigurieren eines Kerberos-Client mit Befehlszeilenüberschreibungen

In dem folgenden Beispiel werden die im Installationsprofil eingestellten Parameter `DNSARG` und `KDC` überschrieben.

```
# /usr/sbin/kclient -p /net/denver.example.com/export/install/profile\
-d dns_fallback -k kdc2.example.com

Starting client setup
-----------------------------------------------------

kdc1.example.com

Setting up /etc/krb5/krb5.conf.

Obtaining TGT for clntconfig/admin ...
Password for clntconfig/admin@EXAMPLE.COM:      <Type the password>

nfs/client.example.com entry ADDED to KDC database.
nfs/client.example.com entry ADDED to keytab.
```

```
host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Copied /net/denver.example.com/export/install/krb5.conf.

------------------------------------------------
Setup COMPLETE.

client#
```

▼ So konfigurieren Sie einen Kerberos-Client interaktiv

Dieses Verfahren verwendet das `kclient`-Installationsdienstprogramm ohne Installationsprofil.

1 **Melden Sie sich als Superuser an.**

2 **Führen Sie das Installationsskript `kclient` aus.**

Sie müssen die folgenden Informationen bereitstellen:

- Kerberos-Bereichsname
- KDC-Master-Hostname
- Administrativer Hauptelementname
- Passwort für das administrative Hauptelement

Beispiel 23–8 Ausführen des `kclient`-Installationsdienstprogramms

Die folgende Ausgabe zeigt das Ergebnis nach Ausführung des Befehls `kclient`.

```
client# /usr/sbin/kclient

Starting client setup
------------------------------------------------

Do you want to use DNS for kerberos lookups ? [y/n]: n
        No action performed.
Enter the Kerberos realm: EXAMPLE.COM
Specify the KDC hostname for the above realm: kdc1.example.com

Setting up /etc/krb5/krb5.conf.

Enter the krb5 administrative principal to be used: clntconfig/admin
Obtaining TGT for clntconfig/admin ...
Password for clntconfig/admin@EXAMPLE.COM:      <Type the password>
Do you plan on doing Kerberized nfs ? [y/n]: n

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.
```

```
Do you want to copy over the master krb5.conf file ? [y/n]: y
Enter the pathname of the file to be copied: \
/net/denver.example.com/export/install/krb5.conf

Copied /net/denver.example.com/export/install/krb5.conf.

-----------------------------------------------
Setup COMPLETE !
#
```

▼ So konfigurieren Sie einen Kerberos-Client manuell

In diesem Verfahren werden die folgenden Konfigurationsparameter verwendet:

- Realm name = `EXAMPLE.COM`
- DNS-Domainname = `example.com`
- Master-KDC = `kdc1.example.com`
- Slave-KDC = `kdc2.example.com`
- NFS-Server = `denver.example.com`
- Client = `client.example.com`
- `admin`-Hauptelement = `kws/admin`
- Benutzer-Hauptelement = `mre`
- Onlinehilfe-URL = `http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956`

Hinweis – Passen Sie die URL an, sodass sie auf den Bereich "Graphical Kerberos Administration Tool" verweist, wie in „Onlinehilfe-URL im Graphical Kerberos Administration Tool“ auf Seite 434 beschrieben.

---

1 Melden Sie sich als Superuser an.

2 Bearbeiten Sie die Kerberos-Konfigurationsdatei (`krb5.conf`).

Um die Kerberos-Standardversion der Datei zu ändern, müssen Sie die Bereichsnamen und die Servernamen ändern. Sie müssen auch den Pfad zu den Hilfedateien für `gkadmin` angeben.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = EXAMPLE.COM

[realms]
        EXAMPLE.COM = {
        kdc = kdc1.example.com
        kdc = kdc2.example.com
```

```
        admin_server = kdc1.example.com
        }

[domain_realm]
        .example.com = EXAMPLE.COM
#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
        default = FILE:/var/krb5/kdc.log
        kdc = FILE:/var/krb5/kdc.log

[appdefaults]
    gkadmin = {
        help_url = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956
```

Hinweis – Um die Verschlüsselungstypen zu beschränken, können Sie die Zeilen `default_tkt_enctypes` oder `default_tgs_enctypes` einstellen. Eine Beschreibung der Probleme beim Beschränken der Verschlüsselungstypen finden Sie unter „Verwenden von Kerberos-Verschlüsselungstypen“ auf Seite 602.

3 (Optional) Ändern Sie das Verfahren zum Suchen der KDCs.

Ab Solaris 10 5/08 wird die Zuordnung zwischen Kerberos-Bereich und KDC standardmäßig in der folgenden Reihenfolge bestimmt:

- Durch Definition im Abschnitt `realms` in `krb5.conf`
- Durch Suchen von SRV-Datensätze in DNS

Sie können dieses Verhalten ändern, indem Sie `dns_lookup_kdc` oder `dns_fallback` im Abschnitt `libdefaults` der Datei `krb5.conf` hinzufügen. Weitere Informationen finden Sie auf der Manpage `krb5.conf(4)`. Beachten Sie, dass Verweise immer zuerst getestet werden.

4 (Optional) Ändern Sie das Verfahren zur Bestimmung des Bereichs für einen Host.

Ab Solaris 10 5/08 wird die Zuordnung zwischen Host und Bereich standardmäßig in der folgenden Reihenfolge bestimmt:

- Wenn das KDC Verweise unterstützt, kann es den Client informieren, zu welchem Bereich der Host gehört.
- Durch Definition von `domain_realm` in der Datei `krb5.conf`
- DNS-Domainname des Hosts
- Standardbereich

Sie können dieses Verhalten ändern, indem Sie `dns_lookup_kdc` oder `dns_fallback` im Abschnitt `libdefaults` der Datei `krb5.conf` hinzufügen. Weitere Informationen finden Sie auf der Manpage `krb5.conf(4)`. Beachten Sie, dass Verweise immer zuerst getestet werden.

5 **(Optional) Synchronisieren Sie die Uhr des Clients mit derjenigen des Master-KDC, indem Sie NTP oder einen anderen Synchronisierungsmechanismus für Uhren verwenden.**

Die Installation und Verwendung des Network Time Protocol (NTP) ist nicht obligatorisch. Damit die Authentifizierung erfolgreich ist, müssen alle Uhren mit der Uhrzeit auf dem KDC-Server synchronisiert sein, wobei die maximale Abweichung durch die `clockskew`-Beziehung in der Datei `krb5.conf` definiert wird. Informationen zu NTP finden Sie unter „Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients“ auf Seite 482.

6 **Starten Sie `kadmin`.**

Sie können das Graphical Kerberos Administration Tool verwenden, wie unter „So erstellen Sie ein neues Kerberos-Hauptelement“ auf Seite 538 erläutert. Dazu müssen Sie sich mit einem der zuvor bei der Konfiguration des Master-KDC erstellten `admin`-Hauptelementnamen anmelden. In dem folgenden Beispiel wird gezeigt, wie die erforderlichen Hauptelemente mithilfe der Befehlszeile hinzufügt werden.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. **(Optional) Erstellen Sie ein Benutzer-Hauptelement, falls noch nicht vorhanden.**

Sie müssen ein Benutzer-Hauptelement nur erstellen, wenn dem mit diesem Host verbundenen Benutzer noch kein Hauptelement zugewiesen ist.

```
kadmin: addprinc mre
Enter password for principal mre@EXAMPLE.COM:      <Type the password>
Re-enter password for principal mre@EXAMPLE.COM:      <Type it again>
kadmin:
```

b. **(Optional) Erstellen Sie ein `root`-Hauptelement und fügen Sie das Hauptelement der Schlüsseltabellendatei des Servers hinzu.**

Dieser Schritt muss ausgeführt werden, damit der Client `root`-Zugriff auf Dateisysteme hat, die über den NFS-Service eingehängt wurden. Er ist auch für nicht interaktiven `root`-Zugriff erforderlich, beispielsweise zum Ausführen von cron-Jobs als `root`.

Wenn der Client keinen `root`-Zugriff auf ein Remote-Dateisystem benötigt, das über den NFS-Service eingehängt ist, können Sie diesen Schritt überspringen. Das `root`-Hauptelement muss ein Hauptelement aus zwei Komponenten sein, wobei die zweite Komponente dem Hostnamen des Kerberos-Clientsystems entspricht, um die Erstellung eines `root`-Hauptelements für den ganzen Bereich zu vermeiden. Wenn die Hauptelementinstanz ein Hostname ist, muss der FQDN unabhängig von der Schreibung des Domainnamens in der Datei `/etc/resolv.conf` in Kleinbuchstaben angegeben werden.

```
kadmin: addprinc -randkey root/client.example.com
Principal "root/client.example.com" created.
kadmin: ktadd root/client.example.com
Entry for principal root/client.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
```

```
Entry for principal root/client.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

c. Erstellen Sie ein `host`-Hauptelement und fügen Sie es der Schlüsseltabellendatei des Servers hinzu.

Das `host`-Hauptelement wird von Remote-Zugriffsservices zur Authentifizierung verwendet. Das Hauptelement ermöglicht `root` den Erhalt eines Berechtigungsnachweises, wenn noch keiner in der Schlüsseltabellendatei vorhanden ist.

```
kadmin: addprinc -randkey host/denver.example.com
Principal "host/denver.example.com@EXAMPLE.COM" created.
kadmin: ktadd host/denver.example.com
Entry for principal host/denver.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

d. (Optional) Fügen Sie das NFS-Service-Hauptelement der Schlüsseltabellendatei des Servers hinzu.

Dieser Schritt ist nur erforderlich, wenn der Client auf NFS-Dateisysteme unter Verwendung der Kerberos-Authentifizierung zugreifen muss.

```
kadmin: ktadd nfs/denver.example.com
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

e. Beenden Sie `kadmin`.

```
kadmin: quit
```

7 (Optional) Aktivieren Sie Kerberos mit NFS.

a. Aktivieren Sie Kerberos-Sicherheitsmodi in der Datei `/etc/nfssec.conf`.

Bearbeiten Sie die Datei `/etc/nfssec.conf` und entfernen Sie das "#" vor den Kerberos-Sicherheitsmodi.

```
# cat /etc/nfssec.conf
 .
 .
#
# Uncomment the following lines to use Kerberos V5 with NFS
#
krb5            390003  kerberos_v5     default -               # RPCSEC_GSS
krb5i           390004  kerberos_v5     default integrity       # RPCSEC_GSS
krb5p           390005  kerberos_v5     default privacy         # RPCSEC_GSS
```

b. Aktivieren Sie DNS.

Wenn die Datei `/etc/resolv.conf` noch nicht erstellt wurde, erstellen Sie sie, da die Standardisierung des Service-Hauptelements davon abhängt, dass dies von DNS durchgeführt wird. Weitere Informationen finden Sie auf der Manpage `resolv.conf(4)`.

c. Starten Sie den `gssd`-Service neu.

Nachdem die Datei `/etc/resolv.conf` erstellt oder geändert wurde, müssen Sie den `gssd`-Dämon neu starten, um die Änderungen erneut zu lesen.

```
# svcadm restart network/rpc/gss
```

8 Wenn der Client das TGT automatisch erneuern soll oder Benutzer vor dem Ablauf des Kerberos-Tickets warnen soll, erstellen Sie einen Eintrag in der Datei `/etc/krb5/warn.conf`.

Weitere Informationen finden Sie auf der Manpage `warn.conf(4)`.

Beispiel 23–9 Einrichten eines Kerberos-Clients unter Verwendung eines Nicht-Solaris-KDC

Ein Kerberos-Client kann zur Verwendung eines Nicht-Solaris-KDC eingerichtet werden. In diesem Fall muss der Datei `/etc/krb5/krb5.conf` im Abschnitt `realms` eine Zeile hinzugefügt werden. Die Zeile ändert das Protokoll, das für die Kommunikation zwischen Client und dem Kerberos-Server zur Passwortänderung verwendet wird. Die Zeile hat folgendes Format.

```
[realms]
                EXAMPLE.COM = {
                kdc = kdc1.example.com
                kdc = kdc2.example.com
                admin_server = kdc1.example.com
                kpasswd_protocol = SET_CHANGE
        }
```

Beispiel 23–10 DNS-TXT-Datensätze für die Zuordnung von Host- und Domainnamen zum Kerberos-Bereich

```
@ IN SOA kdc1.example.com root.kdc1.example.com (
                                1989020501   ;serial
                                10800        ;refresh
                                3600         ;retry
                                3600000      ;expire
                                86400 )      ;minimum

                        IN      NS      kdc1.example.com.
kdc1                    IN      A       192.146.86.20
kdc2                    IN      A       192.146.86.21

_kerberos.example.com.              IN      TXT     "EXAMPLE.COM"
_kerberos.kdc1.example.com.         IN      TXT     "EXAMPLE.COM"
_kerberos.kdc2.example.com.         IN      TXT     "EXAMPLE.COM"
```

Beispiel 23–11 DNS-SRV-Datensätze für Kerberos-Serverpositionen

In diesem Beispiel werden die Datensätze für die Position der KDCs, des `admin`-Servers bzw. des `kpasswd`-Servers definiert.

```
@ IN SOA kdc1.example.com root.kdc1.example.com (
                                1989020501   ;serial
                                10800        ;refresh
                                3600         ;retry
                                3600000      ;expire
                                86400 )      ;minimum

                                   IN      NS      kdc1.example.com.
kdc1                               IN      A       192.146.86.20
kdc2                               IN      A       192.146.86.21

_kerberos._udp.EXAMPLE.COM         IN      SRV 0 0 88  kdc2.example.com
_kerberos._tcp.EXAMPLE.COM         IN      SRV 0 0 88  kdc2.example.com
_kerberos._udp.EXAMPLE.COM         IN      SRV 1 0 88  kdc1.example.com
_kerberos._tcp.EXAMPLE.COM         IN      SRV 1 0 88  kdc1.example.com
_kerberos-adm._tcp.EXAMPLE.COM     IN      SRV 0 0 749 kdc1.example.com
_kpasswd._udp.EXAMPLE.COM          IN      SRV 0 0 749 kdc1.example.com
```

So deaktivieren Sie die Überprüfung des TGT (Ticket Granting Ticket)

Mit diesem Verfahren wird die Sicherheitsprüfung deaktiviert, die feststellt, ob das KDC des Host-Hauptelements, das in der lokalen `/etc/krb5/krb5.keytab`-Datei gespeichert ist, mit dem KDC übereinstimmt, von dem das TGT stammt. Mit dieser Überprüfung vermeiden Sie DNS-Spoofingangriffe. Für einige Clientkonfigurationen ist das Host-Hauptelement möglicherweise nicht verfügbar, sodass diese Überprüfung deaktiviert werden muss, damit der Client funktioniert. Die Überprüfung muss in den folgenden Fällen deaktiviert werden:

- Die Client-IP-Adresse wird dynamisch zugewiesen. Beispiel: ein DHCP-Client
- Der Client wurde nicht zum Hosten eines Service konfiguriert, daher wurde kein Host-Hauptelement erstellt.
- Der Hostschlüssel ist nicht auf dem Client gespeichert.

1 Melden Sie sich als Superuser an.

2 Ändern Sie die Datei `krb5.conf`.

Wenn die Option `verify_ap_req_nofail` auf `false` eingestellt ist, ist der TGT-Überprüfungsprozess nicht aktiviert. Weitere Informationen zu dieser Option finden Sie auf der Manpage `krb5.conf(4)`.

```
client # cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = EXAMPLE.COM
        verify_ap_req_nofail = false
  ...
```

Hinweis – Die Option `verify_ap_req_nofail` kann entweder im Abschnitt `[libdefaults]` oder im Abschnitt `[realms]` der Datei `krb5.conf` eingegeben werden. Wenn sich die Option im Abschnitt `[libdefaults]` befindet, wird sie auf alle Bereiche angewendet. Wenn sich die Option im Abschnitt `[realms]` befindet, gilt die Einstellung nur für den definierten Bereich.

So greifen Sie auf ein durch Kerberos geschütztes NFS-Dateisystem als `root`-Benutzer zu

Dieses Verfahren ermöglicht einem Client den Zugriff auf ein NFS-Dateisystem mit Kerberos-Authentifizierung unter Verwendung der `root`-ID-Berechtigung, insbesondere, wenn das NFS-Dateisystem mit Optionen wie `-o sec=krb5,root=client1.sun.com` zur gemeinsamen Nutzung freigegeben ist.

1 Melden Sie sich als Superuser an.

2 Starten Sie `kadmin`.

Sie können das Graphical Kerberos Administration Tool verwenden, wie unter „So erstellen Sie ein neues Kerberos-Hauptelement“ auf Seite 538 erläutert. Dazu müssen Sie sich mit einem der zuvor bei der Konfiguration des Master-KDC erstellten `admin`-Hauptelementnamen anmelden. In dem folgenden Beispiel wird gezeigt, wie die erforderlichen Hauptelemente mithilfe der Befehlszeile hinzufügt werden.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Erstellen Sie ein `root`-Hauptelement für den NFS-Client.

Dieses Hauptelement ermöglicht einen Root-ähnlichen Zugriff auf über NFS eingehängte Dateisysteme, in denen eine Kerberos-Authentifizierung erforderlich ist. Das `root`-Hauptelement muss ein Hauptelement aus zwei Komponenten sein, wobei die zweite Komponente dem Hostnamen des Kerberos-Clientsystems entspricht, um die Erstellung eines root-Hauptelements für den ganzen Bereich zu vermeiden. Wenn die Hauptelementinstanz ein Hostname ist, muss der FQDN unabhängig von der Schreibung des Domainnamens in der Datei `/etc/resolv.conf` in Kleinbuchstaben angegeben werden.

```
kadmin: addprinc -randkey root/client.example.com
Principal "root/client.example.com" created.
kadmin:
```

b. Fügen Sie das `root`-Hauptelement der Schlüsseltabellendatei des Servers hinzu.

Dieser Schritt muss ausgeführt werden, wenn Sie ein `root`-Hauptelement hinzugefügt haben, damit der Client `root`-Zugriff auf Dateisysteme hat, die über den NFS-Service eingehängt wurden. Er ist auch für nicht interaktiven `root`-Zugriff erforderlich, beispielsweise zum Ausführen von cron-Jobs als `root`.

```
kadmin: ktadd root/client.example.com
Entry for principal root/client.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

c. Beenden Sie `kadmin`.

```
kadmin: quit
```

▼ So konfigurieren Sie eine automatische Migration von Benutzern in einem Kerberos-Bereich

Benutzer, die über kein Kerberos-Hauptelement verfügen, können automatisch in einen vorhandenen Kerberos-Bereich migriert werden. Die Migration wird mithilfe des PAM-Framework für den verwendeten Service erzielt, indem das Modul `pam_krb5_migrate` in den Authentifizierungs-Stack des Service in `/etc/pam.conf` übernommen wird.

In diesem Beispiel werden die PAM-Servicenamen `dtlogin` und `other` zur Verwendung der automatischen Migration konfiguriert. Die folgenden Konfigurationsparameter werden verwendet:

- Realm name = `EXAMPLE.COM`
- Master-KDC = `kdc1.example.com`
- Rechner, der den Migrationsservice hostet = `server1.example.com`
- Migrationservice-Hauptelement = `host/server1.example.com`

Bevor Sie beginnen

Richten Sie `server1` als Kerberos-Client des Bereichs `EXAMPLE.COM` ein. Weitere Informationen finden Sie unter „Konfigurieren von Kerberos-Clients“ auf Seite 468.

1 Überprüfen Sie, ob ein Hostservice-Hauptelement für `server1` vorhanden ist.

Das Hostservice-Hauptelement in der Datei `keytab` von `server1` wird verwendet, um den Server beim Master-KDC zu authentifizieren.

```
server1 # klist -k
Keytab name: FILE:/etc/krb5/krb5.keytab
    KVNO Principal
    ---- --------------------------------------------------
       3 host/server1.example.com@EXAMPLE.COM
       3 host/server1.example.com@EXAMPLE.COM
       3 host/server1.example.com@EXAMPLE.COM
       3 host/server1.example.com@EXAMPLE.COM
```

2 Ändern Sie die PAM-Konfigurationsdatei.

a. Fügen Sie Einträge für den Service `dtlogin` hinzu.

```
# cat /etc/pam.conf
 .
 .
#
# dtlogin service (explicit because of pam_krb5_migrate)
#
dtlogin       auth requisite          pam_authtok_get.so.1
dtlogin       auth required           pam_dhkeys.so.1
dtlogin       auth required           pam_unix_cred.so.1
dtlogin       auth sufficient         pam_krb5.so.1
dtlogin       auth requisite          pam_unix_auth.so.1
dtlogin       auth optional           pam_krb5_migrate.so.1
```

b. (Optional) Erzwingen Sie bei Bedarf eine sofortige Passwortänderung.

Der Ablaufzeitpunkt des Passworts für neu erstellte Kerberos-Konten kann auf den aktuellen Zeitpunkt (jetzt) eingestellt werden, um eine sofortige Änderung des Kerberos-Passworts zu erzwingen. Um den Ablaufzeitpunkt auf "jetzt" einzustellen, fügen Sie die Option `expire_pw` den Zeilen hinzu, in denen das Modul `pam_krb5_migrate` verwendet wird. Weitere Informationen finden Sie auf der Manpage `pam_krb5_migrate(5)`.

```
# cat /etc/pam.conf
 .
 .
dtlogin  auth optional           pam_krb5_migrate.so.1 expire_pw
```

c. Fügen Sie das Modul `pam_krb5` dem Konto-Stack hinzu.

Dadurch kann die Passwortablauffunktion von Kerberos den Zugriff sperren.

```
# cat /etc/pam.conf
 .
 .
#
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other   account requisite       pam_roles.so.1
other   account required        pam_krb5.so.1
other   account required        pam_unix_account.so.1
```

d. Fügen Sie das Modul `pam_krb5` dem Passwort-Stack hinzu.

Dadurch können abgelaufene Passwörter aktualisiert werden.

```
# cat /etc/pam.conf
 .
 .
#
# Default definition for Password management
# Used when service name is not explicitly mentioned for password management
#
other   password required       pam_dhkeys.so.1
other   password requisite      pam_authtok_get.so.1
other   password requisite      pam_authtok_check.so.1
other   password sufficient     pam_krb5.so.1
other   password required       pam_authtok_store.so.1
```

3 Aktualisieren Sie die Zugriffssteuerungsdatei im Master-KDC.

Mit den folgenden Einträgen erhält das Service-Hauptelement `host/server1.example.com` Migrations- und Abfragerechte für alle Benutzer, mit Ausnahme des `root`-Benutzers. Es ist wichtig, dass nicht zu migrierende Benutzer unter Verwendung der Berechtigung `U` in der Datei `kadm5.acl` aufgeführt werden. Diese Einträge müssen sich vor dem Eintrag für alle Berechtigungen oder `ui` befinden. Weitere Informationen finden Sie auf der Manpage `kadm5.acl(4)`.

```
kdc1 # cat /etc/krb5/kadm5.acl
host/server1.example.com@EXAMPLE.COM U root
host/server1.example.com@EXAMPLE.COM ui *
*/admin@EXAMPLE.COM *
```

4 **Starten Sie den Kerberos-Verwaltungsdämon auf dem Master-KDC neu.**

Dies ermöglicht dem Dämon `kadmind`, die neuen `kadm5.acl`-Einträge zu verwenden.

```
kdc1 # svcadm restart network/security/kadmin
```

5 **Fügen Sie auf dem Master-KDC der Datei `pam.conf` Einträge hinzu.**

Durch folgende Einträge verwendet der Dämon `kadmind` den PAM-Service `k5migrate` zur Validierung des UNIX-Benutzerpasswortes für zu migrierende Konten.

```
# grep k5migrate /etc/pam.conf
k5migrate       auth    required        pam_unix_auth.so.1
k5migrate       account required        pam_unix_account.so.1
```

Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients

Auf allen Hosts des Kerberos-Authentifizierungssystems müssen die internen Uhren innerhalb eines angegebenen maximalen Zeitraums (der *Uhrdifferenz*) synchronisiert werden. Diese Anforderung ist mit einer weiteren Kerberos-Sicherheitsprüfung verknüpft. Wenn die Uhrdifferenz bei einem der Hosts überschritten wird, werden Clientanforderungen abgewiesen.

Die Uhrdifferenz bestimmt außerdem, wie lange Anwendungsserver alle Kerberos-Protokollmeldungen verfolgen müssen, um wiederholte Anforderungen zu erkennen und abzulehnen. Je größer deshalb die Uhrdifferenz ist, umso mehr Informationen müssen Anwendungsserver erfassen.

Der Standardwert für die maximale Uhrdifferenz ist 300 Sekunden (fünf Minuten). Sie können diesen Standardwert im Bereich `libdefaults` der Datei `krb5.conf` ändern.

Hinweis – Aus Sicherheitsgründen sollte die Uhrdifferenz nie mehr als 300 Sekunden betragen.

Da die Synchronisierung der Uhren zwischen KDCs und Kerberos-Clients wichtig ist, sollten Sie die NTP-Software (Network Time Protocol) zur Synchronisierung verwenden. Die Oracle Solaris-Software enthält die frei verfügbare NTP-Software der University of Delaware.

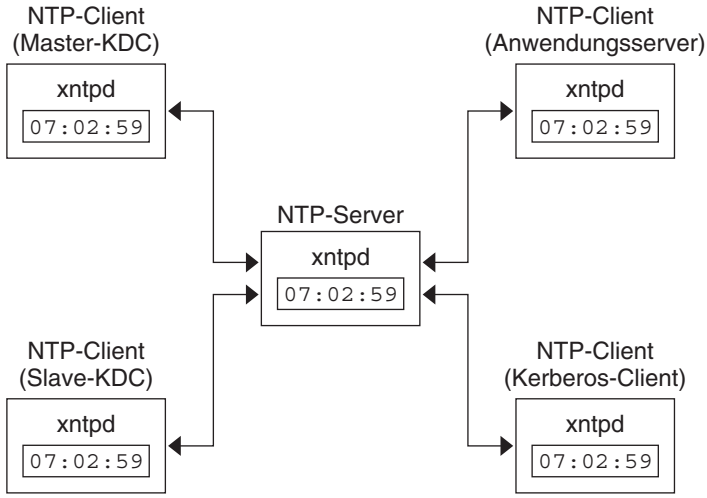
Hinweis – Uhren können auch mit dem `rdate`-Befehl und den `cron`-Jobs synchronisiert werden, was einfacher als die Verwendung von NTP sein kann. In diesem Abschnitt steht jedoch NTP im Vordergrund. Wenn Sie die Uhren über das Netzwerk synchronisieren, muss das Protokoll zur Synchronisierung der Uhren selbst sicher sein.

NTP ermöglicht eine genaue Zeit- oder Netzwerkuhrsynchronisierung (oder beides) in einer Netzwerkumgebung. Im Prinzip ist NTP eine Server-Client-Implementierung. Sie wählen ein

System als Master-Uhr aus (den NTP-Server). Dann richten Sie alle anderen Systeme (die NTP-Clients) zur Synchronisierung der Uhren mit der Master-Uhr ein.

NTP synchronisiert die Uhren mithilfe des Dämons `xntpd`, der eine UNIX-Systemuhrzeit einrichtet und aufrechterhält, die den Internetstandardzeit-Servern entspricht. Die folgende Abbildung zeigt ein Beispiel der NTP-Implementierung mit Server und Client.

ABBILDUNG 23–1 Synchronisieren von Uhren mit NTP



Damit die Uhren von KDCs und Kerberos-Clients synchronisiert sind, müssen Sie folgende Schritte ausführen:

1. Einrichten eines NTP-Servers auf dem Netzwerk. Bei diesem Server kann es sich um ein beliebiges System handeln, mit Ausnahme des Master-KDC. Die NTP-Server-Aufgabe finden Sie unter „Verwalten von Network Time Protocol (Aufgaben)“ in *Systemverwaltungshandbuch: Netzwerkdienste*.
2. KDCs und Kerberos-Clients müssen bei ihrer Konfiguration im Netzwerk als NTP-Clients des NTP-Servers eingerichtet werden. Die NTP-Client-Aufgabe finden Sie unter „Verwalten von Network Time Protocol (Aufgaben)“ in *Systemverwaltungshandbuch: Netzwerkdienste*.

Austauschen von Master-KDC und Slave-KDC

Die Verfahren in diesem Abschnitt vereinfachen das Austauschen eines Master-KDC gegen ein Slave-KDC. Tauschen Sie das Master-KDC nur gegen ein Slave-KDC aus, wenn der Master-KDC-Server ausfällt oder das Master-KDC neu installiert werden muss (beispielsweise wenn neue Hardware installiert wurde).

▼ So konfigurieren Sie ein austauschbares Slave-KDC

Führen Sie dieses Verfahren auf dem Slave-KDC-Server durch, der als Master-KDC verfügbar sein soll. Bei diesem Verfahren wird davon ausgegangen, dass Sie die inkrementelle Weitergabe verwenden.

1 Verwenden Sie während der KDC-Installation Alias-Namen für das Master-KDC und das austauschbare Slave-KDC.

Stellen Sie beim Definieren der Hostnamen für die KDCs sicher, dass jedes System über ein Alias im DNS verfügt. Verwenden Sie die Alias-Namen auch bei der Definition der Hosts in der Datei `/etc/krb5/krb5.conf`.

2 Führen Sie die Schritte zur Installation eines Slave-KDC aus.

Vor dem Austausch sollte dieser Server wie jeder andere Slave-KDC in dem Bereich verwendet werden. Anweisungen finden Sie unter „So konfigurieren Sie ein Slave-KDC manuell“ auf Seite 451.

3 Verschieben Sie die Master-KDC-Befehle.

Um zu verhindern, dass die Master-KDC-Befehle auf diesem Slave-KDC ausgeführt werden, verschieben Sie die Befehle `kprop`, `kadmind` und `kadmin.local` an eine reservierte Position.

```
kdc4 # mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save
kdc4 # mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.save
kdc4 # mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save
```

▼ So tauschen Sie ein Master-KDC gegen ein Slave-KDC aus

Bei diesem Verfahren wird ein Master-KDC-Server namens `kdc1` ausgetauscht. Das Slave-KDC `kdc4` wird zum neuen Master-KDC. Bei diesem Verfahren wird davon ausgegangen, dass Sie die inkrementelle Weitergabe verwenden.

Bevor Sie beginnen Für dieses Verfahren muss der Slave-KDC-Server als austauschbarer Slave eingerichtet sein. Weitere Informationen finden Sie unter „So konfigurieren Sie ein austauschbares Slave-KDC“ auf Seite 484).

1 Starten Sie `kadmin` auf dem neuen Master-KDC.

```
kdc4 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Erstellen Sie neue Hauptelemente für den Service `kadmind`.

In dem folgenden Beispiel wird der Befehl `addprinc` auf zwei Zeilen angezeigt, er sollte jedoch in einer Zeile eingegeben werden.

```
kadmin: addprinc -randkey -allow_tgs_req +password_changing_service -clearpolicy \
       changepw/kdc4.example.com
Principal "changepw/kdc4.example.com@ENG.SUN.COM" created.
kadmin: addprinc -randkey -allow_tgs_req -clearpolicy kadmin/kdc4.example.com
Principal "kadmin/kdc4.example.com@EXAMPLE.COM" created.
kadmin:
```

b. Erstellen Sie eine Schlüsseltabellendatei.

```
kadmin: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc4.example.com
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin: ktadd -k /etc/krb5/kadm5.keytab changepw/kdc4.example.com
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin: ktadd -k /etc/krb5/kadm5.keytab kadmin/changepw
Entry for principal kadmin/changepw with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin:
```

c. Beenden Sie `kadmin`.

```
kadmin: quit
```

2 Erzwingen Sie auf dem neuen Master-KDC eine Synchronisierung.

Durch die folgenden Schritte wird eine vollständige KDC-Aktualisierung auf dem Slave-Server erzwungen.

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulog
```

3 Überprüfen Sie auf dem neuen Master-KDC, ob die Aktualisierung abgeschlossen ist.

```
kdc4 # /usr/sbin/kproplog -h
```

4 Starten Sie auf dem neuen Master-KDC den KDC-Service.

```
kdc4 # svcadm enable -r network/security/krb5kdc
```

5 Löschen Sie das Aktualisierungsprotokoll auf dem neuen Master-KDC.

Durch diese Schritte wird das Aktualisierungsprotokoll für den neuen Master-KDC-Server initialisiert.

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulog
```

6 Beenden Sie die Prozesse `kadmind` und `krb5kdc` auf dem alten Master-KDC.

Wenn Sie den Prozess `kadmind` beenden, verhindern Sie Änderungen an der KDC-Datenbank.

```
kdc1 # svcadm disable network/security/kadmin
kdc1 # svcadm disable network/security/krb5kdc
```

7 Geben Sie auf dem alten Master-KDC die Abfragezeit für Weitergaben an.

Kommentieren Sie den Eintrag `sunw_dbprop_master_ulogsize` in `/etc/krb5/kdc.conf` aus und fügen Sie einen Eintrag zur Definition von `sunw_dbprop_slave_poll` hinzu. Dieser Eintrag stellt eine Abfragezeit von 2 Minuten ein.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM= {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
#               sunw_dbprop_master_ulogsize = 1000
                sunw_dbprop_slave_poll = 2m
        }
```

8 Verschieben Sie die Master-KDC-Befehle und die Datei `kadm5.acl` auf dem alten Master-KDC.

Um zu verhindern, dass die Master-KDC-Befehle ausgeführt werden, verschieben Sie die Befehle `kprop`, `kadmind` und `kadmin.local` an eine reservierte Position.

```
kdc1 # mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save
kdc1 # mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.save
kdc1 # mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save
kdc1 # mv /etc/krb5/kadm5.acl /etc/krb5/kadm5.acl.save
```

9 Ändern Sie die Alias-Namen für das Master-KDC auf dem DNS-Server.

Um die Server zu ändern, bearbeiten Sie die Zonendatei `example.com` und ändern Sie den Eintrag für `masterkdc`.

```
masterkdc IN CNAME kdc4
```

10 Starten Sie den Internet-Domainnamenserver auf dem DNS-Server neu.

Führen Sie den folgenden Befehl zum Laden der neuen Aliasinformationen aus:

```
# svcadm refresh network/dns/server
```

11 Verschieben Sie die Master-KDC-Befehle und die Slave-Datei `kadm.acl` auf dem neuen Master-KDC.

```
kdc4 # mv /usr/lib/krb5/kprop.save /usr/lib/krb5/kprop
kdc4 # mv /usr/lib/krb5/kadmind.save /usr/lib/krb5/kadmind
kdc4 # mv /usr/sbin/kadmin.local.save /usr/sbin/kadmin.local
kdc4 # mv /etc/krb5/kpropd.acl /etc/krb5/kpropd.acl.save
```

12 Erstellen Sie die Kerberos-Zugriffsteuerungsliste (`kadm5.acl`) auf dem neuen Master-KDC.

Nach der Datenaufnahme sollte die Datei `/etc/krb5/kadm5.acl` alle Hauptelementnamen enthalten, die zur Verwaltung des KDC berechtigt sind. Die Datei sollte auch eine Liste aller Slaves enthalten, die inkrementelle Weitergabeanforderungen stellen. Weitere Informationen finden Sie auf der Manpage `kadm5.acl(4)`.

```
kdc4 # cat /etc/krb5/kadm5.acl
kws/admin@EXAMPLE.COM   *
kiprop/kdc1.example.com@EXAMPLE.COM p
```

13 Geben Sie die Aktualisierungsprotokollgröße in der Datei `kdc.conf` auf dem neuen Master-KDC an.

Kommentieren Sie den Eintrag `sunw_dbprop_slave_poll` aus und fügen Sie einen Eintrag zur Definition von `sunw_dbprop_master_ulogsize` hinzu. Dieser Eintrag stellt eine Protokollgröße von 1000 Einträgen ein.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM= {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
```

```
                        acl_file = /etc/krb5/kadm5.acl
                        kadmind_port = 749
                        max_life = 8h 0m 0s
                        max_renewable_life = 7d 0h 0m 0s
                        sunw_dbprop_enable = true
                #       sunw_dbprop_slave_poll = 2m
                        sunw_dbprop_master_ulogsize = 1000
                }
```

14 Fügen Sie auf dem neuen Master-KDC der Datei `kadmind` das Hauptelement `kiprop` hinzu.

```
kdc4 # kadmin.local
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc4.example.com
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: quit
```

15 Starten Sie auf dem neuen Master-KDC die Dämonen `kadmind` und `krb5kdc`.

```
kdc4 # svcadm enable -r network/security/krb5kdc
kdc4 # svcadm enable -r network/security/kadmin
```

16 Fügen Sie auf dem alten Master-KDC das Service-Hauptelement `kiprop` hinzu.

Durch Hinzufügen des Hauptelements `kiprop` in der Datei `krb5.keytab` kann der Dämon `kpropd` sich für den inkrementellen Weitergabeservice authentifizieren.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Authenticating as pricipal kws/admin@EXAMPLE.COM with password.
Enter password:     <Type kws/admin password>
kadmin: ktadd kiprop/kdc1.example.com
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

17 Fügen Sie auf dem alten Master-KDC in der Konfigurationsdatei für die Weitergabe `kpropd.acl` einen Eintrag für jedes KDC in `krb5.conf` hinzu.

```
kdc1 # cat /etc/krb5/kpropd.acl
host/kdc1.example.com@EXAMPLE.COM
```

```
host/kdc2.example.com@EXAMPLE.COM
host/kdc3.example.com@EXAMPLE.COM
host/kdc4.example.com@EXAMPLE.COM
```

18 Starten Sie auf dem alten Master-KDC die Dämonen `kpropd` und `krb5kdc`.

Wenn der Dämon `krb5kdc` gestartet wird, wird `kpropd` ebenfalls gestartet, sofern das System als Slave konfiguriert ist.

```
kdc1 # svcadm enable network/security/krb5kdc
```

Verwalten der Kerberos-Datenbank

Die Kerberos-Datenbank ist der Backbone von Kerberos und muss immer auf dem neuesten Stand sein. Dieser Abschnitt enthält einige Verfahren zur Verwaltung der Kerberos-Datenbank, wie Backup und Wiederherstellen der Datenbank, Einrichten der inkrementellen oder parallelen Weitergabe und Verwalten der Stash-Datei. Die Schritte zur ersten Einrichtung der Datenbank finden Sie in „So konfigurieren Sie ein Master-KDC manuell“ auf Seite 438.

Backup und Weitergabe der Kerberos-Datenbank

Die Weitergabe der Kerberos-Datenbank vom Master-KDC auf die Slave-KDCs ist eine der wichtigsten Konfigurationsaufgaben. Wenn die Weitergabe zu selten erfolgt, stimmen Master-KDC und Slave-KDCs nicht mehr überein. Wenn das Master-KDC ausfällt, verfügen die Slave-KDCs nicht über die neuesten Datenbankinformationen. Wenn außerdem ein Slave-KDC zum Lastenausgleich als Master-KDC konfiguriert wurde, verfügen die Clients, die dieses Slave-KDC als Master-KDC verwenden, nicht über die neuesten Informationen. Daher müssen Sie sicherstellen, dass die Daten oft genug weitergegeben werden oder die Server zur inkrementellen Weitergabe konfigurieren, abhängig davon, wie häufig die Kerberos-Datenbank geändert wird. Die inkrementelle Weitergabe wird der manuellen Weitergabe vorgezogen, da die manuelle Weitergabe mit einem höheren Verwaltungsaufwand verbunden ist. Eine vollständige Weitergabe der Datenbank ist außerdem nicht immer effizient.

Wenn Sie das Master-KDC konfigurieren, richten Sie den Befehl `kprop_script` in einem `cron`-Job ein, um ein Backup der Kerberos-Datenbank in der Abbilddatei `/var/krb5/slave_datatrans` automatisch zu erstellen und an die Slave-KDCs weiterzugeben. Wie jede Datei kann die Kerberos-Datenbank beschädigt werden. Beschädigte Daten auf einem Slave-KDC fallen wahrscheinlich gar nicht weiter auf, da bei der nächsten automatischen Weitergabe eine neue Kopie installiert wird. Wird jedoch die Datenbank auf dem Master-KDC beschädigt, wird sie bei der nächsten Weitergabe auf allen Slave-KDCs installiert. Außerdem wird dann eine nicht beschädigte Backup-Datei auf dem Master-KDC durch eine beschädigte Backup-Datei überschrieben.

Da in diesem Fall keine "sichere" Backup-Kopie vorhanden ist, sollten Sie auch einen `cron`-Job einrichten, um die Dump-Datei `slave_datatrans` regelmäßig an eine andere Position zu

kopieren oder um eine weitere Backup-Kopie zu erstellen, indem Sie den Befehl `dump` des Dienstprogramms `kdb5_util` verwenden. Sollte die Datenbank nun beschädigt werden, können Sie die neueste Backup-Kopie auf dem Master-KDC mit dem Befehl `load` des Dienstprogramms `kdb5_util` wiederherstellen.

Beachten Sie außerdem, dass die Abbilddatei der Datenbank Hauptelementschlüssel enthält und deshalb vor unberechtigtem Zugriff geschützt werden muss. Standardmäßig hat nur der `root` Lese- und Schreibzugriff auf die Abbilddatei der Datenbank. Um die Abbilddatei vor unberechtigtem Zugriff zu schützen, verwenden Sie ausschließlich den Befehl `kprop` zur Weitergabe, der die weitergegebenen Daten verschlüsselt. Außerdem gibt `kprop` die Daten nur an Slave-KDCs weiter und verhindert so, dass die Abbilddatei der Datenbank versehentlich an unberechtigte Hosts gesendet wird.

Achtung – Wenn die Kerberos-Datenbank nach der Weitergabe aktualisiert und vor der nächsten Weitergabe beschädigt wird, werden die Aktualisierungen nicht an die KDC-Slaves weitergegeben. Die Aktualisierungen gehen verloren. Aus diesem Grund sollten Sie bei umfangreichen Aktualisierungen der Kerberos-Datenbank vor einer regelmäßigen, geplanten Weitergabe die Datenbank manuell weitergeben, um Datenverlust zu vermeiden.

Datei `kpropd.acl`

Die Datei `kpropd.acl` auf einem Slave-KDC enthält eine Liste von Host-Hauptelementnamen (ein Name pro Zeile), die die Systeme angibt, von denen das KDC eine aktualisierte Datenbank durch Weitergabe erhalten kann. Wenn das Master-KDC zur Weitergabe aller Slave-KDCs verwendet wird, muss die Datei `kpropd.acl` auf jedem Slave nur den Host-Hauptelementnamen des Master-KDC enthalten.

Die Kerberos-Installation und die nachfolgenden Konfigurationsschritte in diesem Dokument beschreiben, wie Sie diese Datei `kpropd.acl` dem Master-KDC und den Slave-KDCs hinzufügen. Diese Datei enthält alle Hauptelementnamen für den KDC-Host. Diese Konfiguration ermöglicht Ihnen eine Weitergabe von jedem KDC, falls das normalerweise zur Weitergabe verwendete KDC vorübergehend nicht zur Verfügung steht. Durch Beibehalten identischer Kopien auf allen KDCs lässt sich die Konfiguration einfach verwalten.

Befehl `kprop_script`

Der Befehl `kprop_script` gibt die Kerberos-Datenbank mithilfe des Befehls `kprop` an andere KDCs weiter. Wenn der Befehl `kprop_script` auf einem Slave-KDC ausgeführt wird, gibt er die Kerberos-Datenbankkopie des Slave-KDC an andere KDCs weiter. Der Befehl `kprop_script` akzeptiert mehrere durch Leerzeichen getrennte Hostnamen als Argumente, um die KDCs für die Weitergabe anzugeben.

Beim Ausführen von `kprop_script` wird eine Backup-Kopie der Kerberos-Datenbank in der Datei `/var/krb5/slave_datatrans` angelegt und die Datei auf die angegebenen KDCs kopiert. Die Kerberos-Datenbank wird gesperrt, bis die Weitergabe abgeschlossen ist.

▼ So erstellen Sie ein Backup der Kerberos-Datenbank

1 Melden Sie sich als Superuser beim Master-KDC an.

2 Erstellen Sie ein Backup der Kerberos-Datenbank, indem Sie den Befehl `dump` des Dienstprogramms `kdb5_util` verwenden.

```
# /usr/sbin/kdb5_util dump [-verbose] [-d dbname] [filename [principals...]]
```

`-verbose` Gibt den Namen der einzelnen Hauptelemente und die Richtlinie aus, die im Backup enthalten sein sollen

dbname Definiert den Namen der Datenbank, für die das Backup erstellt werden soll. Beachten Sie, dass Sie einen absoluten Pfad für die Datei angeben können. Wenn die Option `-d` nicht angegeben wird, lautet der Standard-Datenbankname `/var/krb5/principal`.

filename Definiert die Datei, die für das Backup der Datenbank verwendet wird. Sie können einen absoluten Pfad für die Datei angeben. Wenn Sie keine Datei angeben, wird die Datenbank in die Standarddatei ausgegeben.

principals Definiert einen oder mehrere durch Leerzeichen getrennte Hauptelemente, die gesichert werden sollen. Verwenden Sie nur vollständig qualifizierte Hauptelementnamen. Wenn Sie keine Hauptelemente angeben, wird die gesamte Datenbank gesichert.

Beispiel 23–12 Backup der Kerberos-Datenbank

In dem folgenden Beispiel wird ein Backup der Kerberos-Datenbank in der Datei `dumpfile` erstellt. Da die Option `-verbose` angegeben ist, wird jedes Hauptelement beim Backup angezeigt.

```
# kdb5_util dump -verbose dumpfile
kadmin/kdc1.eng.example.com@ENG.EXAMPLE.COM
krbtgt/ENG.EXAMPLE.COM@ENG.EXAMPLE.COM
kadmin/history@ENG.EXAMPLE.COM
pak/admin@ENG.EXAMPLE.COM
pak@ENG.EXAMPLE.COM
changepw/kdc1.eng.example.com@ENG.EXAMPLE.COM
```

In dem folgenden Beispiel wird ein Backup der Hauptelemente `pak` und `pak/admin` aus der Kerberos-Datenbank erstellt.

```
# kdb5_util dump -verbose dumpfile pak/admin@ENG.EXAMPLE.COM pak@ENG.EXAMPLE.COM
pak/admin@ENG.EXAMPLE.COM
pak@ENG.EXAMPLE.COM
```

▼ So stellen Sie die Kerberos-Datenbank wieder her

1. **Melden Sie sich als Superuser beim Master-KDC an.**

2. **Halten Sie die KDC-Dämonen auf dem Master an.**

```
kdc1 # svcadm disable network/security/krb5kdc
kdc1 # svcadm disable network/security/kadmin
```

3. **Stellen Sie die Kerberos-Datenbank mithilfe des Befehls `load` des Dienstprogramms `kdb_util` wieder her.**

```
# /usr/sbin/kdb5_util load [-verbose] [-d dbname] [-update] [filename]
```

`-verbose`	Gibt die Namen der einzelnen Hauptelemente und die Richtlinie aus, die wiederhergestellt werden
dbname	Definiert den Namen der Datenbank, die wieder hergestellt werden soll. Beachten Sie, dass Sie einen absoluten Pfad für die Datei angeben können. Wenn die Option `-d` nicht angegeben wird, lautet der Standard-Datenbankname `/var/krb5/principal`.
`-update`	Aktualisiert die vorhandene Datenbank. Andernfalls wird eine neue Datenbank erstellt oder die vorhandene Datenbank überschrieben.
filename	Definiert die Datei, die zur Wiederherstellung der Datenbank verwendet wird. Sie können einen absoluten Pfad für die Datei angeben.

4. **Starten Sie die KDC-Dämonen.**

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

Beispiel 23–13 Wiederherstellen der Kerberos-Datenbank

In dem folgenden Beispiel wird die Datenbank `database1` im aktuellen Verzeichnis mithilfe der Datei `dumpfile` wiederhergestellt. Da die Option `-update` nicht angegeben ist, wird eine neue Datenbank bei der Wiederherstellung erstellt.

```
# kdb5_util load -d database1 dumpfile
```

▼ So konvertieren Sie eine Kerberos-Datenbank nach einem Server-Upgrade

Wenn Ihre KDC-Datenbank auf einem Server mit Solaris 8 oder Solaris 9 erstellt wurde, können Sie durch Konvertieren der Datenbank das verbesserte Datenbankformat nutzen.

Bevor Sie beginnen Stellen Sie sicher, dass die Datenbank ein älteres Format verwendet.

1 Halten Sie die KDC-Dämonen auf dem Master an.

```
kdc1 # svcadm disable network/security/krb5kdc
kdc1 # svcadm disable network/security/kadmin
```

2 Erstellen Sie ein Verzeichnis zum Speichern einer temporären Kopie der Datenbank.

```
kdc1 # mkdir /var/krb5/tmp
kdc1 # chmod 700 /var/krb5/tmp
```

3 Geben Sie die KDC-Datenbank als Abbilddatei aus.

```
kdc1 # kdb5_util dump /var/krb5/tmp/prdb.txt
```

4 Speichern Sie Kopien der aktuellen Datenbankdateien.

```
kdc1 # cd /var/krb5
kdc1 # mv princ* tmp/
```

5 Laden Sie die Datenbank.

```
kdc1 # kdb5_util load /var/krb5/tmp/prdb.txt
```

6 Starten Sie die KDC-Dämonen.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

▼ So konfigurieren Sie ein Master-KDC zur Verwendung der inkrementellen Weitergabe

Mit den Schritten in diesem Verfahren können Sie eine vorhandene Master-KDC neu konfigurieren, um die inkrementelle Weitergabe zu nutzen. In diesem Verfahren werden die folgenden Konfigurationsparameter verwendet:

- Realm name = `EXAMPLE.COM`
- DNS-Domainname = `example.com`
- Master-KDC = `kdc1.example.com`
- Slave-KDC = `kdc2.example.com`
- `admin`-Hauptelement = `kws/admin`

1 Fügen Sie Einträge zu `kdc.conf` hinzu.

Sie müssen die inkrementelle Weitergabe aktivieren und die Anzahl der Aktualisierungen auswählen, die der KDC-Master in der Protokolldatei speichert. Weitere Informationen finden Sie auf der Manpage `kdc.conf(4)`.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
```

```
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM= {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
                sunw_dbprop_master_ulogsize = 1000
        }
```

2 Erstellen Sie das `kiprop`-Hauptelement.

Das `kiprop`-Hauptelement dient zur Authentifizierung des Master-KDC-Servers und zur Autorisierung der Aktualisierungen vom Master-KDC.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin: addprinc -randkey kiprop/kdc1.example.com
Principal "kiprop/kdc1.example.com@EXAMPLE.COM" created.
kadmin: addprinc -randkey kiprop/kdc2.example.com
Principal "kiprop/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

3 Fügen Sie das `kiprop`-Hauptelement der Schlüsseltabellendatei `kadmind` hinzu.

Durch Hinzufügen des `kiprop`-Hauptelements zur Datei `kadm5.keytab` kann sich der Befehl `kadmind` authentifizieren, wenn er gestartet wird.

```
kadmin: ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc1.example.com
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin: quit
```

4 Fügen Sie `kadm5.acl` einen kiprop-Eintrag auf dem Master-KDC hinzu.

Durch diesen Eintrag erhält das Master-KDC Anforderungen zur inkrementellen Weitergabe vom `kdc2`-Server.

```
kdc1 # cat /etc/krb5/kadm5.acl
*/admin@EXAMPLE.COM *
kiprop/kdc2.example.com@EXAMPLE.COM p
```

5 **Kennzeichnen Sie die `kprop`-Zeile in der crontab-Datei im `root` als Kommentar.**

Dieser Schritt verhindert, dass das Master-KDC seine Kopie der KDC-Datenbank weitergibt.

```
kdc1 # crontab -e
#ident  "@(#)root       1.20    01/11/06 SMI"
#
# The root crontab should be used to perform accounting data collection.
#
# The rtc command is run to adjust the real time clock if and when
# daylight savings time changes.
#
10 3 * * * /usr/sbin/logadm
15 3 * * 0 /usr/lib/fs/nfs/nfsfind
1 2 * * * [ -x /usr/sbin/rtc ] && /usr/sbin/rtc -c > /dev/null 2>&1
30 3 * * * [ -x /usr/lib/gss/gsscred_clean ] && /usr/lib/gss/gsscred_clean
#10 3 * * * /usr/lib/krb5kprop_script kdc2.example.sun.com #SUNWkr5ma
```

6 **Starten Sie `kadmind` neu.**

```
kdc1 # svcadm restart network/security/kadmin
```

7 **Konfigurieren Sie alle Slave-KDC-Server, die inkrementelle Weitergabe nutzen.**

Vollständige Anweisungen finden Sie unter „So konfigurieren Sie ein Slave-KDC zur Verwendung der inkrementellen Weitergabe“ auf Seite 495.

▼ So konfigurieren Sie ein Slave-KDC zur Verwendung der inkrementellen Weitergabe

1 **Fügen Sie Einträge zu `krb5.conf` hinzu.**

Die neuen Einträge ermöglichen die inkrementelle Weitergabe und stellen eine Abfragezeit von 2 Minuten ein.

```
kdc2 # cat /etc/krb5/krb5.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM= {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
                sunw_dbprop_slave_poll = 2m
        }
```

2 Fügen Sie das `kiprop`-Hauptelement der Datei `krb5.keytab` hinzu.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin: ktadd kiprop/kdc2.example.com
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

3 Deaktivieren Sie `kpropd`.

```
kdc2 # svcadm disable network/security/krb5_prop
```

4 Starten Sie den KDC-Server neu.

```
kdc2 # svcadm restart network/security/krb5kdc
```

▼ So konfigurieren Sie ein Slave-KDC zur Verwendung der vollständigen Weitergabe

In diesem Verfahren wird beschrieben, wie ein Slave-KDC-Server mit Solaris 10 zur vollständigen Weitergabe konfiguriert wird. Normalerweise muss dieses Verfahren nur durchgeführt werden, wenn auf dem Master-KDC-Server Solaris 9 oder eine frühere Version ausgeführt wird. In diesem Fall kann der Master-KDC-Server keine inkrementelle Weitergabe unterstützen, sodass der Slave konfiguriert werden muss, damit die Daten weitergegeben werden können.

Mit diesem Verfahren wird ein Slave-KDC namens `kdc3` konfiguriert. In diesem Verfahren werden die folgenden Konfigurationsparameter verwendet:

- Realm name = `EXAMPLE.COM`
- DNS-Domainname = `example.com`
- Master-KDC = `kdc1.example.com`
- Slave-KDC = `kdc2.example.com` und `kdc3.example.com`
- `admin`-Hauptelement = `kws/admin`
- Onlinehilfe-URL = `http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956`

Hinweis – Passen Sie die URL an, sodass sie auf den Bereich "Graphical Kerberos Administration Tool" verweist, wie in „Onlinehilfe-URL im Graphical Kerberos Administration Tool“ auf Seite 434 beschrieben.

Bevor Sie beginnen Das Master-KDC muss konfiguriert sein. Wenn dieser Slave austauschbar ist, finden Sie spezielle Anweisungen unter „Austauschen von Master-KDC und Slave-KDC“ auf Seite 484.

1 Melden Sie sich auf dem Master-KDC als Superuser an.

2 Starten Sie `kadmin` auf dem Master-KDC.

Sie müssen sich mit einem der zuvor bei der Konfiguration des Master-KDC erstellten `admin`-Hauptelementnamen anmelden.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Fügen Sie auf dem Master-KDC der Datenbank Slave-Host-Hauptelemente hinzu, falls noch nicht geschehen.

Damit der Slave ordnungsgemäß funktioniert, muss er über ein Host-Hauptelement verfügen. Wenn die Hauptelementinstanz ein Hostname ist, muss der FQDN unabhängig von der Schreibung des Domainnamens in der Datei `/etc/resolv.conf` in Kleinbuchstaben angegeben werden.

```
kadmin: addprinc -randkey host/kdc3.example.com
Principal "host/kdc3@EXAMPLE.COM" created.
kadmin:
```

b. Beenden Sie `kadmin`.

```
kadmin: quit
```

3 Bearbeiten Sie die Kerberos-Konfigurationsdatei (`krb5.conf`) auf dem Master-KDC.

Sie müssen einen Eintrag pro Slave hinzufügen. Eine vollständige Beschreibung dieser Datei finden Sie auf der Manpage `krb5.conf(4)`.

```
kdc1 # cat /etc/krb5/krb5.conf
 .
 .
[realms]
                EXAMPLE.COM = {
                kdc = kdc1.example.com
                kdc = kdc2.example.com
                kdc = kdc3.example.com
                admin_server = kdc1.example.com
        }
```

4 Fügen Sie auf dem Master-KDC einen Eintrag für das Master-KDC hinzu und fügen Sie jedes Slave-KDC in die Datei `kpropd.acl` ein.

Eine vollständige Beschreibung dieser Datei finden Sie auf der Manpage kprop(1M).

```
kdc1 # cat /etc/krb5/kpropd.acl
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
host/kdc3.example.com@EXAMPLE.COM
```

5 Kopieren Sie die KDC-Administrationsdateien vom Master-KDC-Server auf alle Slave-KDCs.

Dieser Schritt ist für alle Slave-KDCs obligatorisch, da der Master-KDC-Server über aktualisierte Informationen verfügt, die auf den KDC-Servern benötigt werden. Sie können `ftp` oder einen ähnlichen Transfermechanismus verwenden, um Kopien der folgenden Dateien vom Master-KDC zu übertragen:

- `/etc/krb5/krb5.conf`
- `/etc/krb5/kdc.conf`
- `/etc/krb5/kpropd.acl`

6 Stellen Sie auf allen Slave-KDCs sicher, dass die Kerberos-Zugriffssteuerungsliste `kadm5.acl` nicht mit Daten angefüllt ist.

In unverändertem Zustand sieht die Datei `kadm5.acl` etwa folgendermaßen aus:

```
kdc2 # cat /etc/krb5/kadm5.acl
*/admin@___default_realm___ *
```

Wenn die Datei `kiprop`-Einträge enthält, entfernen Sie diese.

7 Starten Sie den Befehl `kadmin` auf dem neuen Slave.

Sie müssen sich mit einem der zuvor bei der Konfiguration des Master-KDC erstellten `admin`-Hauptelementnamen anmelden.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Fügen Sie mithilfe von `kadmin` das Host-Hauptelement des Slaves der Schlüsseltabellendatei des Slaves hinzu.

Dieser Eintrag stellt die ordnungsgemäße Funktion von `kprop` und anderen kerberisierten Anwendungen sicher. Wenn die Hauptelementinstanz ein Hostname ist, muss der FQDN unabhängig von der Schreibung des Domainnamens in der Datei `/etc/resolv.conf` in Kleinbuchstaben angegeben werden.

```
kadmin: ktadd host/kdc3.example.com
Entry for principal host/kdc3.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
```

```
Entry for principal host/kdc3.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

b. Beenden Sie `kadmin`.

```
kadmin: quit
```

8 Fügen Sie auf dem Master-KDC den Namen des Slave-KDC dem `cron`-Job zu, der normalerweise die Backups ausführt, indem Sie `crontab -e` verwenden.

Fügen Sie den Namen der einzelnen Slave-KDC-Server am Ende der `kprop_script`-Zeile hinzu.

```
10 3 * * * /usr/lib/krb5/kprop_script kdc2.example.com kdc3.example.com
```

Sie sollten auch den Zeitpunkt der Backups ändern. Mit diesem Eintrag erfolgt das Backup der Daten täglich morgens um 3:10 Uhr.

9 Starten Sie den Kerberos-Weitergabedämon auf dem neuen Slave.

```
kdc3 # svcadm enable network/security/krb5_prop
```

10 Erstellen Sie ein Backup der Datenbank auf dem Master-KDC und geben Sie sie weiter, indem Sie `kprop_script` verwenden.

Wenn bereits eine Backup-Kopie der Datenbank verfügbar ist, muss das Backup kein zweites Mal abgeschlossen werden. Weitere Informationen finden Sie unter „So führen Sie eine manuelle Weitergabe der Kerberos-Datenbank an Slave-KDCs durch“ auf Seite 501.

```
kdc1 # /usr/lib/krb5/kprop_script kdc3.example.com
Database propagation to kdc3.example.com: SUCCEEDED
```

11 Erstellen Sie mit `kdb5_util` auf dem neuen Slave eine Stash-Datei.

```
kdc3 # /usr/sbin/kdb5_util stash
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key

Enter KDC database master key:      <Type the key>
```

12 (Optional) Synchronisieren Sie die Uhr des neuen Slave-KDC mit derjenigen des Master-KDC, indem Sie NTP oder einen anderen Synchronisierungsmechanismus für Uhren verwenden.

Die Installation und Verwendung des Network Time Protocol (NTP) ist nicht obligatorisch. Alle Uhren müssen sich innerhalb der im Abschnitt `libdefaults` der Datei `krb5.conf` definierten Standardzeit befinden. Informationen zu NTP finden Sie unter „Synchronisieren von Uhren zwischen KDCs und Kerberos-Clients“ auf Seite 482.

13 Starten Sie den KDC-Dämon (`krb5kdc`) auf dem neuen Slave.

```
kdc3 # svcadm enable network/security/krb5kdc
```

▼ So überprüfen Sie die Synchronisierung der KDC-Server

Wenn eine inkrementelle Weitergabe konfiguriert wurde, gewährleistet dieses Verfahren, dass die Informationen auf dem Slave-KDC aktualisiert wurden.

1. **Führen Sie auf dem KDC-Master-Server den Befehl `kproplog` aus.**

   ```
   kdc1 # /usr/sbin/kproplog -h
   ```

2. **Führen Sie auf einem KDC-Slave-Server den Befehl `kproplog` aus.**

   ```
   kdc2 # /usr/sbin/kproplog -h
   ```

3. **Überprüfen Sie, ob die letzte Seriennummer und der letzte Zeitstempel übereinstimmen.**

Beispiel 23–14 Überprüfen der Synchronisierung der KDC-Server

In dem folgenden Beispiel werden die Ergebnisse für die Ausführung des Befehls `kproplog` auf dem Master-KDC-Server gezeigt.

```
kdc1 # /usr/sbin/kproplog -h

Kerberos update log (/var/krb5/principal.ulog)
Update log dump:
    Log version #: 1
    Log state: Stable
    Entry block size: 2048
    Number of entries: 2500
    First serial #: 137966
    Last serial #: 140465
    First time stamp: Fri Nov 28 00:59:27 2004
    Last time stamp: Fri Nov 28 01:06:13 2004
```

In dem folgenden Beispiel werden die Ergebnisse für die Ausführung des Befehls `kproplog` auf dem Slave-KDC-Server gezeigt.

```
kdc2 # /usr/sbin/kproplog -h

Kerberos update log (/var/krb5/principal.ulog)
Update log dump:
    Log version #: 1
    Log state: Stable
    Entry block size: 2048
    Number of entries: 0
    First serial #: None
    Last serial #: 140465
    First time stamp: None
    Last time stamp: Fri Nov 28 01:06:13 2004
```

Beachten Sie, dass die Werte für die letzte Seriennummer und den letzten Zeitstempel identisch sind. Das bedeutet, dass Slave- und Master-KDC-Server synchronisiert sind.

Beachten Sie, dass das Aktualisierungsprotokoll des Slave-KDC-Servers keine Aktualisierungseinträge enthält. Das liegt daran, dass der Slave-KDC-Server im Unterschied zum Master-KDC-Server keinen Satz der Aktualisierungen beibehält. Der KDC-Slave-Server bietet auch keine Informationen zu der ersten Seriennummer oder dem ersten Zeitstempel, da dies nicht relevant ist.

▼ So führen Sie eine manuelle Weitergabe der Kerberos-Datenbank an Slave-KDCs durch

In diesem Verfahren wird beschrieben, wie Sie die Kerberos-Datenbank mithilfe des Befehls `kprop` weitergeben. Führen Sie dieses Verfahren aus, um ein Slave-KDC mit dem Master-KDC außerhalb des regelmäßigen `cron`-Jobs zu synchronisieren. Anders als `kprop_script` können Sie mit `kprop` die Backup-Kopie der aktuellen Kerberos-Datenbank weitergeben, ohne zuerst eine neue Backup-Kopie zu erstellen.

Hinweis – Führen Sie dieses Verfahren nicht aus, wenn Sie die inkrementelle Weitergabe nutzen.

1. **Melden Sie sich als Superuser beim Master-KDC an.**

2. **(Optional) Erstellen Sie ein Backup der Datenbank mithilfe des Befehls `kdb5_util`.**

   ```
   # /usr/sbin/kdb5_util dump /var/krb5/slave_datatrans
   ```

3. **Geben Sie die Datenbank mithilfe des Befehls `kprop` an ein Slave-KDC weiter.**

   ```
   # /usr/lib/krb5/kprop -f /var/krb5/slave_datatrans slave-KDC
   ```

Beispiel 23–15 Manuelle Weitergabe der Kerberos-Datenbank an Slave-KDCs mithilfe von `kprop_script`

Wenn Sie ein Backup der Datenbank außerhalb eines routinemäßigen `cron`-Jobs erstellen und an ein Slave-KDC weitergeben möchten, können Sie auch den Befehl `kprop_script` wie folgt verwenden:

```
# /usr/lib/krb5/kprop_script slave-KDC
```

Einrichten von paralleler Weitergabe

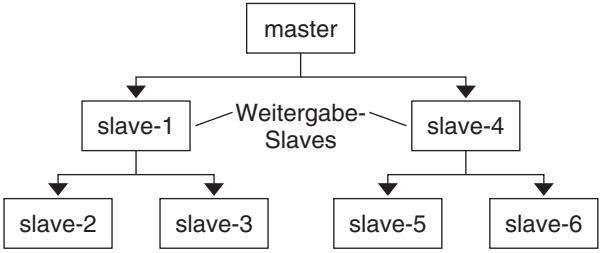
In den meisten Fällen wird das Master-KDC ausschließlich zur Weitergabe der Kerberos-Datenbank an die Slave-KDCs verwendet. Befinden sich jedoch viele Slave-KDCs an einem Standort, empfiehlt sich die *parallele Weitergabe* zur Lastverteilung.

Hinweis – Führen Sie dieses Verfahren nicht aus, wenn Sie die inkrementelle Weitergabe nutzen.

Bei der parallelen Weitergabe geht ein Teil der Aufgaben vom Master-KDC an bestimmte Slave-KDCs über. Diese Arbeitsaufteilung beschleunigt die Weitergabe und entlastet das Master-KDC.

Angenommen, an einem Standort befinden sich ein Master-KDC und sechs Slave-KDCs (siehe Abbildung 23–2), wobei `slave-1` bis `slave-3` eine logische Gruppe und `slave-4` bis `slave-6` eine andere logische Gruppe bilden. Zur Einrichtung einer parallelen Weitergabe kann beispielsweise das Master-KDC die Datenbank an `slave-1` und `slave-4` weitergeben. Diese KDC-Slaves können wiederum die Datenbank an die KDC-Slaves ihrer Gruppe weitergeben.

ABBILDUNG 23–2 Beispiel für die Konfiguration einer parallelen Weitergabe



Konfigurationsschritte zum Einrichten einer parallelen Weitergabe

Der folgende Abschnitt enthält keine ausführliche Beschreibung der einzelnen Verfahrensschritte, sondern eine allgemeine Liste von Schritten zur Konfiguration einer parallelen Weitergabe. Folgende Schritte müssen ausgeführt werden:

1. Ändern Sie auf dem Master-KDC den Eintrag `kprop_script` im entsprechenden `cron`-Job, um nur die Argumente für die KDC-Slaves einzuschließen, die die folgende Weitergabe ausführen (die *Weitergabe-Slaves*).

2. Fügen Sie dem `cron`-Job auf jedem Weitergabe-Slave einen `kprop_script`-Eintrag mit den Argumenten für die Slaves hinzu, an die Daten weitergegeben werden sollen. Für eine erfolgreiche parallele Weitergabe muss der `cron`-Job ausgeführt werden, nachdem der Weitergabe-Slave die neue Kerberos-Datenbank erhalten hat.

   Hinweis – Wie lange die Weitergabe an den Weitergabe-Slave dauert, hängt von Faktoren wie der Netzwerkbandbreite und der Größe der Kerberos-Datenbank ab.

3. Richten Sie die entsprechenden Berechtigungen auf den einzelnen Slave-KDCs für die Weitergabe ein. Fügen Sie dazu den Host-Hauptelementnamen des weitergebenden KDC der Datei `kpropd.acl` hinzu.

BEISPIEL 23–16 Einrichten von paralleler Weitergabe

Unter Verwendung des Beispiels in Abbildung 23–2 sieht der `kprop_script`-Eintrag des Master-KDC etwa folgendermaßen aus:

```
0 3 * * * /usr/lib/krb5/kprop_script slave-1.example.com slave-4.example.com
```

Der `kprop_script`-Eintrag von `slave-1` sieht etwa folgendermaßen aus:

```
0 4 * * * /usr/lib/krb5/kprop_script slave-2.example.com slave-3.example.com
```

Beachten Sie, dass die Weitergabe an die Slaves eine Stunde nach der Weitergabe durch den Master erfolgt.

Die Datei `kpropd.acl` auf den Weitergabe-Slaves enthält folgenden Eintrag:

```
host/master.example.com@EXAMPLE.COM
```

Die Datei `kpropd.acl` auf den KDC-Slaves, die Daten von `slave-1` erhalten, enthält den folgenden Eintrag:

```
host/slave-1.example.com@EXAMPLE.COM
```

Verwalten der Stash-Datei

Die *Stash-Datei* enthält den Master-Schlüssel für die Kerberos-Datenbank, der automatisch zusammen mit der Kerberos-Datenbank erstellt wird. Wenn die Stash-Datei beschädigt wird, können Sie sie mit dem Befehl `stash` des Dienstprogramms `kdb5_util` ersetzen. Eine Stash-Datei sollte nur gelöscht werden, nachdem die Kerberos-Datenbank mit dem Befehl `destroy` des Dienstprogramms `kdb5_util` entfernt wurde. Da die Stash-Datei nicht automatisch zusammen mit der Datenbank gelöscht wird, müssen Sie sie entfernen, um die Bereinigung abzuschließen.

▼ So entfernen Sie eine Stash-Datei

1 **Melden Sie sich als Superuser bei dem KDC an, das die Stash-Datei enthält.**

2 **Entfernen Sie die Stash-Datei.**

```
# rm stash-file
```

stash-file gibt den Pfad der Stash-Datei an. Standardmäßig befindet sich die Stash-Datei unter `/var/krb5/.k5.` *realm*.

Hinweis – Mit der Option `-f` des Befehls `kdb5_util` können Sie die Stash-Datei neu erstellen.

Verwalten eines KDC auf einem LDAP-Verzeichnisserver

Die meisten KDC-Verwaltungsaufgaben für LDAP-Verzeichnisserver sind mit denjenigen für DB2-Server identisch. Es gibt jedoch auch einige spezifische Aufgaben für LDAP.

TABELLE 23–3 Konfigurieren von KDC-Servern zur Verwendung von LDAP (Übersicht der Schritte)

Aufgabe	Description (Beschreibung)	Anweisungen
Konfigurieren eines Master-KDC	Konfiguriert und erstellt Master-KDC-Server und -Datenbank für einen Bereich mithilfe eines manuellen Prozesses und LDAP für das KDC	„So konfigurieren Sie ein KDC zur Verwendung eines LDAP-Datenservers“ auf Seite 443
Kombinieren von Kerberos-Hauptelementattributen mit Objektklassentypen, die nicht zu Kerberos gehören	Ermöglicht die Nutzung der in Kerberos-Datensätzen gespeicherten Informationen in anderen LDAP-Datenbanken	„So kombinieren Sie Kerberos-Hauptelementattribute mit einem nicht zu Kerberos gehörenden Objektklassentyp“ auf Seite 504
Löschen eines Bereichs	Entfernt alle mit einem Bereich verbundenen Daten	„So löschen Sie einen Bereich auf einem LDAP-Verzeichnisserver“ auf Seite 505

▼ So kombinieren Sie Kerberos-Hauptelementattribute mit einem nicht zu Kerberos gehörenden Objektklassentyp

Dieses Verfahren ermöglicht die Zuweisung von Kerberos-Hauptelementattributen zu Objektklassentypen, die nicht zu Kerberos gehören. In diesem Verfahren werden die Attribute `krbprincipalaux`, `krbTicketPolicyAux` und `krbPrincipalName` der Objektklasse "People" zugewiesen.

In diesem Verfahren werden die folgenden Konfigurationsparameter verwendet:

- Verzeichnisserver = `dsserver.example.com`
- Benutzer-Hauptelement = `willf@EXAMPLE.COM`

1. **Melden Sie sich als Superuser an.**

2. **Bereiten Sie die einzelnen Einträge in der Objektklasse "People" vor.**

   Wiederholen Sie diesen Schritt für jeden Eintrag.

   ```
   cat << EOF | ldapmodify -h dsserver.example.com -D "cn=directory manager"
   dn: uid=willf,ou=people,dc=example,dc=com
   changetype: modify
   objectClass: krbprincipalaux
   objectClass: krbTicketPolicyAux
   krbPrincipalName: willf@EXAMPLE.COM
   EOF
   ```

3. **Fügen Sie ein Teilbaumattribut dem Bereichscontainer hinzu.**

   Dieser Schritt ermöglicht das Durchsuchen von Hauptelementeinträgen im Container `ou=people,dc=example,dc=com` sowie im Standardcontainer EXAMPLE.COM.

   ```
   # kdb5_ldap_util -D "cn=directory manager" modify \
               -subtrees 'ou=people,dc=example,dc=com' -r EXAMPLE.COM
   ```

4. **(Optional) Wenn die KDC-Datensätze in DB2 gespeichert sind, migrieren Sie DB2-Einträge.**

   a. **Geben Sie die DB2-Einträge als Abbilddatei aus.**

      ```
      # kdb5_util dump > dumpfile
      ```

   b. **Laden Sie die Datenbank auf den LDAP-Server.**

      ```
      # kdb5_util load -update dumpfile
      ```

5. **(Optional) Fügen Sie die Hauptelementattribute dem KDC hinzu.**

   ```
   # kadmin.local -q 'addprinc willf'
   ```

▼ So löschen Sie einen Bereich auf einem LDAP-Verzeichnisserver

Dieses Verfahren kann ausgeführt werden, wenn ein anderer LDAP-Verzeichnisserver für einen Bereich konfiguriert wurde.

1. **Melden Sie sich als Superuser an.**

2. **Löschen Sie den Bereich.**

   ```
   # kdb5_ldap_util -D "cn=directory manager" destroy
   ```

Erhöhen der Sicherheit auf Kerberos-Servern

Führen Sie diese Schritte aus, um die Sicherheit von Kerberos-Anwendungsservern und KDC-Servern zu erhöhen.

TABELLE 23–4 Erhöhen der Sicherheit auf Kerberos-Servern (Übersicht der Schritte)

Aufgabe	Description (Beschreibung)	Anweisungen
Gewähren von Zugriff mit Kerberos-Authentifizierung	Ermöglicht den Netzwerkzugriff auf einen Server nur mit Kerberos-Authentifizierung	„So aktivieren Sie nur kerberisierte Anwendungen“ auf Seite 506
Einschränken des Zugriffs auf KDC-Server	Erhöht die Sicherheit der KDC-Server und ihrer Daten	„So beschränken Sie den Zugriff auf KDC-Server“ auf Seite 506
Erhöhen der Passwortsicherheit durch Verwendung einer Wörterbuchdatei	Erhöht die Sicherheit neuer Passwörter, indem diese anhand eines Wörterbuchs überprüft werden	„So verwenden Sie eine Wörterbuchdatei zur Erhöhung der Passwortsicherheit“ auf Seite 507

▼ So aktivieren Sie nur kerberisierte Anwendungen

Mit diesem Verfahren wird der Netzwerkzugriff auf den Server, der `telnet`, `ftp`, `rcp`, `rsh` und `rlogin` ausführt, auf Transaktionen mit Kerberos-Authentifizierung beschränkt.

1. **Ändern Sie die Eigenschaft exec für den `telnet`-Service.**

   Fügen Sie die Option `-a user` der Eigenschaft `exec` für `telnet` hinzu, um den Zugriff auf Benutzer mit gültigen Authentifizierungsinformationen zu beschränken.

   ```
   # inetadm -m svc:/network/telnet:default exec="/usr/sbin/in.telnetd -a user"
   ```

2. **(Optional) Wenn noch nicht konfiguriert, ändern Sie die Eigenschaft exec für den `telnet`-Service.**

   Fügen Sie die Option `-a` der Eigenschaft `exec` für `ftp` hinzu, um nur mit Kerberos authentifizierte Verbindungen zuzulassen.

   ```
   # inetadm -m svc:/network/ftp:default exec="/usr/sbin/in.ftpd -a"
   ```

3. **Deaktivieren Sie andere Services.**

   Deaktivieren Sie die Dämonen `in.rshd` und `in.rlogind`.

   ```
   # svcadm disable network/shell
   # svcadm disable network/login:rlogin
   ```

▼ So beschränken Sie den Zugriff auf KDC-Server

Sowohl Master-KDC-Server als auch Slave-KDC-Server verfügen über lokal gespeicherte Kopien der KDC-Datenbank. Für die Sicherheit der gesamten Kerberos-Installation ist es wichtig, dass der Zugriff auf diese Server beschränkt ist und die Datenbanken geschützt sind.

1. **Deaktivieren Sie bei Bedarf Remote-Services.**

   Um den KDC-Server zu schützen, sollten alle unwesentlichen Netzwerkdienste deaktiviert werden. Abhängig von Ihrer Konfiguration können einige dieser Services bereits deaktiviert sein. Überprüfen Sie den Servicestatus mithilfe des Befehls `svcs`. In den meisten Fällen müssen nur die Services `krb5kdc` und `kadmin` ausgeführt werden, wenn es sich um einen KDC-Master handelt. Außerdem können alle Services, die loopback tli (`ticlts`, `ticotsord` und `ticots`) verwenden, aktiviert bleiben.

   ```
   # svcadm disable network/comsat
   # svcadm disable network/dtspc/tcp
   # svcadm disable network/finger
   # svcadm disable network/login:rlogin
   # svcadm disable network/rexec
   # svcadm disable network/shell
   # svcadm disable network/talk
   # svcadm disable network/tname
   # svcadm disable network/uucp
   # svcadm disable network/rpc_100068_2-5/rpc_udp
   ```

2. **Schränken Sie den Zugriff auf die Hardware ein, die das KDC unterstützt.**

   Um den physischen Zugriff einzuschränken, stellen Sie sicher, dass der KDC-Server und dessen Monitor in einem sicheren Gebäude untergebracht sind. Normale Benutzer sollten keinen Zugang zu diesem Server haben.

3. **Speichern Sie die Backups der KDC-Datenbank auf lokalen Festplatten oder auf den KDC-Slaves.**

   Führen Sie Backups auf Bändern für das KDC nur durch, wenn die Bänder sicher verwahrt werden können. Das gilt auch für Kopien von Schlüsseltabellendateien. Am besten sollten diese Dateien in einem lokalen Dateisystem gespeichert werden, das nicht zur gemeinsamen Nutzung mit anderen Systemen freigegeben ist. Das Dateisystem für die Speicherung kann sich entweder auf dem Master-KDC-Server oder auf einem der Slave-KDCs befinden.

▼ So verwenden Sie eine Wörterbuchdatei zur Erhöhung der Passwortsicherheit

Mit einer Wörterbuchdatei kann der Kerberos-Service verhindern, dass bestimmte, darin aufgeführte Wörter bei der Erstellung neuer Berechtigungsnachweise als Passwörter verwendet werden. Dadurch wird es schwieriger, Passwörter zu erraten. Standardmäßig wird die Datei `/var/krb5/kadm5.dict` verwendet, die jedoch leer ist.

1. **Melden Sie sich als Superuser beim Master-KDC an.**

2 Bearbeiten Sie die KDC-Konfigurationsdatei (`kdc.conf`).

Damit der Service eine Wörterbuchdatei verwendet, müssen Sie eine Zeile hinzufügen. In diesem Beispiel wird das Wörterbuch des Dienstprogramms `spell` verwendet. Eine vollständige Beschreibung der Konfigurationsdatei finden Sie auf der Manpage `kdc.conf(4)`.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM = {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
                sunw_dbprop_master_ulogsize = 1000
                dict_file = /usr/share/lib/dict/words
                }
```

3 Starten Sie die Kerberos-Dämonen neu.

```
kdc1 # svcadm restart -r network/security/krb5kdc
kdc1 # svcadm restart -r network/security/kadmin
```

◆ ◆ ◆ KAPITEL 24

Kerberos-Fehlermeldungen und -Fehlerbehebung

In diesem Kapitel erhalten Sie Lösungen zu Fehlermeldungen, die Ihnen bei der Arbeit mit dem Kerberos-Service angezeigt werden können. Außerdem liefert dieses Kapitel Hinweise zur Fehlerbehebung für verschiedene Probleme. Im Folgenden sind die in diesem Kapitel enthaltenen Informationen zu Fehlermeldungen und zur Fehlerbehebung aufgeführt.

- „Fehlermeldungen des SEAM-Tools“ auf Seite 509
- „Häufige Kerberos-Fehlermeldungen (A – M)“ auf Seite 510
- „Häufige Kerberos-Fehlermeldungen (N – Z)“ auf Seite 519
- „Probleme mit dem Format der Datei `krb5.conf` “ auf Seite 523
- „Probleme bei der Weitergabe der Kerberos-Datenbank“ auf Seite 523
- „Probleme beim Einhängen eines kerberisierten NFS-Dateisystems“ auf Seite 523
- „Probleme beim Authentifizieren als `root`“ auf Seite 524
- „Überwachen der Zuordnungen von GSS-Berechtigungsnachweisen zu UNIX-Berechtigungsnachweisen“ auf Seite 525

Kerberos-Fehlermeldungen

Dieser Abschnitt enthält Informationen zu Kerberos-Fehlermeldungen, einschließlich der Ursachen von Fehlern und Möglichkeiten zur Fehlerbehebung.

Fehlermeldungen des SEAM-Tools

`Unable to view the list of principals or policies; use the Name field.`

Grund: Das Hauptelement `admin`, mit dem Sie sich angemeldet haben, verfügt nicht über die Listenberechtigung (`l`) in der ACL-Datei von Kerberos (`kadm5.acl`). Demzufolge können Sie die Hauptelement- oder Richtlinienliste nicht anzeigen.

Lösung: Sie müssen die Namen der Hauptelemente und Richtlinien in das Feld "Name" eingeben, um sie verwenden zu können, oder sich mit einem Hauptelement mit den entsprechenden Berechtigungen anmelden.

`JNI: Java array creation failed`

`JNI: Java class lookup failed`

`JNI: Java field lookup failed`

`JNI: Java method lookup failed`

`JNI: Java object lookup failed`

`JNI: Java object field lookup failed`

`JNI: Java string access failed`

`JNI: Java string creation failed`

Grund: Es besteht ein schwerwiegendes Problem mit der vom SEAM-Tool (`gkadmin`) verwendeten nativen Java-Schnittstelle (Java Native Interface).

Lösung: Beenden Sie den Befehl `gkadmin` und starten Sie ihn neu. Wenn das Problem weiterhin besteht, melden Sie bitte einen Fehler.

Häufige Kerberos-Fehlermeldungen (A – M)

Dieser Abschnitt umfasst eine alphabetische Liste (A – M) häufiger Fehlermeldungen für die Kerberos-Befehle und -Dämonen, das PAM-Framework, die GSS-Schnittstelle, den NFS-Service sowie die Kerberos-Bibliothek.

`All authentication systems disabled; connection refused`

Grund: Diese Version von `rlogind` unterstützt keine Authentifizierungsmechanismen.

Lösung: Stellen Sie sicher, dass `rlogind` mit der Option `-k` aufgerufen wird.

`Another authentication mechanism must be used to access this host`

Grund: Die Authentifizierung konnte nicht durchgeführt werden.

Lösung: Stellen Sie sicher, dass der Client den Kerberos V5-Mechanismus für die Authentifizierung verwendet.

`Authentication negotiation has failed, which is required for encryption. Good bye.`

Grund: Die Authentifizierung konnte nicht mit dem Server ausgehandelt werden.

Lösung: Starten Sie die Fehlersuche für die Authentifizierung, indem Sie den Befehl `telnet` mit dem Befehl `toggle authdebug` ausführen, und lesen Sie die Fehlersuchmeldungen für weitere Hinweise. Vergewissern Sie sich außerdem, dass Sie über gültige Berechtigungsnachweise verfügen.

`Bad krb5 admin server hostname while initializing kadmin interface`
Grund: Für `admin_server` in der Datei `krb5.conf` wurde ein ungültiger Hostname konfiguriert.

Lösung: Geben Sie den richtigen Hostnamen für das Master-KDC in der Zeile `admin_server` der Datei `krb5.conf` an.

`Bad lifetime value`
Grund: Der angegebene Lebensdauerwert ist nicht gültig oder nicht richtig formatiert.

Lösung: Vergewissern Sie sich, dass der angegebene Wert mit den im Abschnitt zu den Zeitformaten auf der Manpage `kinit(1)` enthaltenen Angaben übereinstimmt.

`Bad start time value`
Grund: Der angegebene Wert für die Startzeit ist nicht gültig oder nicht richtig formatiert.

Lösung: Vergewissern Sie sich, dass der angegebene Wert mit den im Abschnitt zu den Zeitformaten auf der Manpage `kinit(1)` enthaltenen Angaben übereinstimmt.

`Cannot contact any KDC for requested realm`
Grund: Im angeforderten Bereich hat kein KDC geantwortet.

Lösung: Stellen Sie sicher, dass mindestens ein KDC (entweder das Master- oder ein Slave-KDC) erreichbar ist oder der Dämon `krb5kdc` auf den KDCs ausgeführt wird. Überprüfen Sie die Datei `/etc/krb5/krb5.conf` auf die Liste der konfigurierten KDCs (`kdc` = *kdc-name*).

`Cannot determine realm for host`
Grund: Kerberos kann den Bereichsnamen für den Host nicht bestimmen.

Lösung: Stellen Sie sicher, dass ein Standardbereichsname vorhanden ist oder die Domainnamenszuordnungen in der Kerberos-Konfigurationsdatei festgelegt sind (`krb5.conf`).

`Cannot find KDC for requested realm`
Grund: Im angeforderten Bereich wurde kein KDC gefunden.

Lösung: Stellen Sie sicher, dass im Abschnitt `realm` der Kerberos-Konfigurationsdatei (`krb5.conf`) ein KDC angegeben ist.

`cannot initialize realm` *realm-name*
Grund: Das KDC weist möglicherweise keine Stash-Datei auf.

Lösung: Vergewissern Sie sich, dass das KDC über eine Stash-Datei verfügt. Ist dies nicht der Fall, erstellen Sie eine Stash-Datei mit dem Befehl `kdb5_util` und versuchen Sie, den Befehl `krb5kdc` neu zu starten.

`Cannot resolve KDC for requested realm`
Grund: Kerberos kann kein KDC für den Bereich bestimmen.

Lösung: Stellen Sie sicher, dass im Abschnitt `realm` der Kerberos-Konfigurationsdatei (`krb5.conf`) ein KDC angegeben ist.

`Cannot reuse password`
Grund: Das von Ihnen angegebene Passwort wurde bereits zuvor von diesem Hauptelement verwendet.

Lösung: Wählen Sie ein Passwort, das nicht zuvor verwendet wurde (zumindest nicht innerhalb der Anzahl der Passwörter, die für jedes Hauptelement in der KDC-Datenbank gespeichert sind). Diese Richtlinie wird von der Richtlinie des Hauptelements durchgesetzt.

`Can't get forwarded credentials`
Grund: Die Weiterleitung der Berechtigungsnachweise konnte nicht eingerichtet werden.

Lösung: Stellen Sie sicher, dass das Hauptelement über weiterleitbare Berechtigungsnachweise verfügt.

`Can't open/find Kerberos configuration file`
Grund: Die Kerberos-Konfigurationsdatei (`krb5.conf`) war nicht verfügbar.

Lösung: Vergewissern Sie sich, dass die Datei `krb5.conf` am richtigen Speicherort verfügbar ist und die richtigen Berechtigungen aufweist. Diese Datei sollte von `root` geschrieben und von allen anderen Benutzern gelesen werden können.

`Client did not supply required checksum--connection rejected`
Grund: Die Authentifizierung mit Prüfsumme wurde nicht mit dem Client ausgehandelt. Der Client verwendet möglicherweise ein altes Kerberos V5-Protokoll, das die anfängliche Verbindungsunterstützung nicht unterstützt.

Lösung: Vergewissern Sie sich, dass der Client ein Kerberos V5-Protokoll verwendet, das die anfängliche Verbindungsunterstützung unterstützt.

`Client/server realm mismatch in initial ticket request`
Grund: In der ersten Ticketanforderung besteht hinsichtlich des Bereichs zwischen Client und Server keine Übereinstimmung.

Lösung: Stellen Sie sicher, dass sich der Server, mit dem Sie kommunizieren, im selbem Bereich wie der Client befindet oder die Bereiche richtig konfiguriert sind.

`Client or server has a null key`
Grund: Das Hauptelement hat einen leeren Schlüssel.

Lösung: Ändern Sie mit dem Befehl `cpw` von `kadmin` das Hauptelement dahingehend, dass dessen Schlüssel ungleich null ist.

`Communication failure with server while initializing kadmin interface`

Grund: Auf dem für den Admin-Server angegebenen Host, auch Master-KDC genannt, wurde der Dämon `kadmind` nicht ausgeführt.

Lösung: Vergewissern Sie sich, dass Sie den richtigen Hostnamen für das Master-KDC angegeben haben. Wenn dies der Fall ist, stellen Sie sicher, dass `kadmind` auf dem von Ihnen angegebenen Master-KDC ausgeführt wird.

`Credentials cache file permissions incorrect`

Grund: Sie verfügen nicht über die richtigen Lese- oder Schreibberechtigungen für den Berechtigungsnachweis-Cache (`/tmp/krb5cc_` *uid*).

Lösung: Stellen Sie sicher, dass Sie über Lese- und Schreibberechtigungen für den Berechtigungsnachweis-Cache verfügen.

`Credentials cache I/O operation failed` *XXX*

Grund: Beim Schreiben in den Berechtigungsnachweis-Cache (`/tmp/krb5cc_`*uid*) durch Kerberos ist ein Problem aufgetreten.

Lösung: Vergewissern Sie sich mit dem Befehl `df`, dass der Berechtigungsnachweis-Cache nicht entfernt wurde und dass freier Speicherplatz auf dem Gerät vorhanden ist.

`Decrypt integrity check failed`

Grund: Sie verfügen möglicherweise über ein ungültiges Ticket.

Lösung: Überprüfen Sie, ob folgende zwei Bedingungen zutreffen:

- Stellen Sie sicher, dass Ihre Berechtigungsnachweise gültig sind. Löschen Sie Ihre Tickets mit `kdestroy` und erstellen Sie neue Tickets mit `kinit`.
- Vergewissern Sie sich, dass der Zielhost eine Schlüsseltabellendatei mit der richtigen Version des Serviceschlüssels aufweist. Verwenden Sie `kadmin`, um die Schlüsselversionsnummer des Service-Hauptelements (z. B. `host/`*FQDN-hostname*) in der Kerberos-Datenbank anzuzeigen. Stellen Sie außerdem mithilfe von `klist -k` auf dem Zielhost sicher, dass jener dieselbe Schlüsselversionsnummer hat.

`Encryption could not be enabled. Goodbye.`

Grund: Die Verschlüsselung konnte nicht mit dem Server ausgehandelt werden.

Lösung: Starten Sie die Fehlersuche für die Authentifizierung, indem Sie den Befehl `telnet` mit dem Befehl `toggle encdebug` ausführen, und lesen Sie die Fehlersuchmeldungen für weitere Hinweise.

`failed to obtain credentials cache`
Grund: Während der `kadmin`-Initialisierung ist ein Fehler aufgetreten, als `kadmin` versuchte, Berechtigungsnachweise für das Hauptelement `admin` abzurufen.

Lösung: Vergewissern Sie sich, dass Sie beim Ausführen von `kadmin` das richtige Hauptelement und Passwort verwendet haben.

`Field is too long for this implementation`
Grund: Die von einer kerberisierten Anwendung gesendete Meldung war zu lang. Dieser Fehler kann in Verbindung mit dem Transportprotokoll UDP auftreten, dessen standardmäßige Maximalgröße für Meldungen 65535 Byte beträgt. Außerdem bestehen in einer Protokollmeldung, die vom Kerberos-Service gesendet wurde, Begrenzungen für einzelne Felder.

Lösung: Überprüfen Sie, ob Sie die UDP-Übertragung in der Datei `/etc/krb5/kdc.conf` des KDC-Servers eingeschränkt haben.

`GSS-API (or Kerberos) error`
Grund: Diese Meldung ist eine generische GSS-API- oder Kerberos-Fehlermeldung und kann durch mehrere verschiedene Probleme ausgelöst werden.

Lösung: Suchen Sie in der Datei `/var/krb5/kdc.log` die genaue Fehlermeldung, die protokolliert wurde, als der Fehler auftrat.

`Hostname cannot be canonicalized`
Grund: Der Kerberos-Client kann den vollständig qualifizierten Hostnamen für den Server nicht finden.

Lösung: Vergewissern Sie sich, dass der Hostname des Servers in DNS definiert ist und die Zuordnungen zwischen Hostname und Adresse bzw. Adresse und Hostname übereinstimmen.

`Illegal cross-realm ticket`
Grund: Das gesendete Ticket verfügte nicht über die richtigen übergreifenden Bereiche. Möglicherweise wurden für die Bereiche nicht die richtigen vertrauensvollen Beziehungen eingerichtet.

Lösung: Stellen Sie sicher, dass die verwendeten Bereiche die richtigen vertrauensvollen Beziehungen aufweisen.

`Improper format of Kerberos configuration file`
Grund: Die Kerberos-Konfigurationsdatei enthält ungültige Einträge.

Lösung: Vergewissern Sie sich, dass auf alle Beziehungen in der Datei `krb5.conf` ein Gleichheitszeichen (=) und ein Wert folgen. Überprüfen Sie außerdem, ob in den Paaren für jeden Unterabschnitt die Klammern vorhanden sind.

`Inappropriate type of checksum in message`
Grund: Die Meldung enthielt einen ungültigen Prüfsummentyp.

Lösung: Überprüfen Sie, welche gültigen Prüfsummentypen in den Dateien `krb5.conf` und `kdc.conf` angegeben werden.

`Incorrect net address`
Grund: Es bestand eine Abweichung bezüglich der Netzwerkadresse. Die Netzwerkadresse im weitergeleiteten Ticket wich von der Netzwerkadresse bei der Verarbeitung des Tickets ab. Diese Meldung kann beim Weiterleiten von Tickets angezeigt werden.

Lösung: Stellen Sie sicher, dass die Netzwerkadressen korrekt sind. Löschen Sie Ihre Tickets mit `kdestroy` und erstellen Sie neue Tickets mit `kinit`.

`Invalid credential was supplied`

`Service key not available`
Grund: Das Service-Ticket im Berechtigungsnachweis-Cache ist möglicherweise nicht korrekt.

Lösung: Leeren Sie den aktuellen Berechtigungsnachweis-Cache und führen Sie `kinit` erneut aus, bevor Sie versuchen, diesen Service zu verwenden.

`Invalid flag for file lock mode`
Grund: Es ist ein interner Kerberos-Fehler aufgetreten.

Lösung: Bitte melden Sie einen Fehler.

`Invalid message type specified for encoding`
Grund: Kerberos konnte den von der kerberisierten Anwendung gesendeten Meldungstyp nicht erkennen.

Lösung: Wenn Sie eine kerberisierte Anwendung verwenden, die an Ihrem Standort oder von einem Hersteller entwickelt wurde, vergewissern Sie sich, dass die Anwendung Kerberos korrekt verwendet.

`Invalid number of character classes`
Grund: Das von Ihnen für das Hauptelement angegebene Passwort enthält nicht genügend Passwortklassen, wie von der Richtlinie des Hauptelements vorgeschrieben.

Lösung: Geben Sie ein Passwort mit der von der Richtlinie vorgeschriebenen Mindestanzahl an Passwortklassen an.

`KADM err: Memory allocation failure`
Grund: Es ist nicht genügend Speicher zum Ausführen von `kadmin` vorhanden.

Lösung: Geben Sie Speicher frei und versuchen Sie, `kadmin` erneut auszuführen.

`kadmin: Bad encryption type while changing host/<FQDN>'s key`
Grund: Weitere standardmäßige Verschlüsselungstypen sind in der Basisversion von Solaris 10 8/07 enthalten. Clients können Verschlüsselungstypen anfordern, die eventuell nicht von einem KDC unterstützt werden, auf dem eine ältere Version der Software ausgeführt wird.

Lösung: Es gibt mehrere Lösungen zur Behebung dieses Problems. Die am leichtesten zu implementierende wird als erstes aufgeführt:

1. Fügen Sie die Pakete SUNWcry und SUNWcryr dem KDC-Server hinzu. Dadurch erhöht sich die Anzahl der vom KDC unterstützten Verschlüsselungstypen.
2. Legen Sie `permitted_enctypes` in `krb5.conf` auf dem Client so fest, dass der Verschlüsselungstyp `aes256` nicht enthalten ist. Dieser Schritt muss auf jedem neuen Client ausgeführt werden.

`KDC can't fulfill requested option`
Grund: Das KDC ließ die angeforderte Option nicht zu. Das Problem besteht eventuell darin, dass Optionen zur Nachdatierung oder weiterleitbare Optionen angefordert wurden und das KDC diese nicht zuließ. Ein weiteres Problem ist möglicherweise, dass Sie die Erneuerung eines TGT angefordert haben, jedoch über kein erneuerbares TGT verfügten.

Lösung: Bestimmen Sie, ob Sie entweder eine vom KDC nicht zugelassene Option oder einen nicht verfügbaren Tickettyp anfordern.

`KDC policy rejects request`
Grund: Die KDC-Richtlinie ließ die Anforderung nicht zu. Dies kann beispielsweise daran liegen, dass die Anforderung an den KDC keine IP-Adresse aufwies. Möglicherweise wurde auch eine Weiterleitung angefordert, die das KDC jedoch nicht zuließ.

Lösung: Stellen Sie sicher, dass Sie den Befehl `kinit` mit den richtigen Optionen verwenden. Ändern Sie bei Bedarf die mit dem Hauptelement verknüpfte Richtlinie oder die Attribute des Hauptelements, um die Anforderung zuzulassen. Sie können die Richtlinie oder das Hauptelement mit dem Befehl `kadmin` ändern.

`KDC reply did not match expectation`
Grund: Die KDC-Antwort enthielt nicht den erwarteten Hauptelementnamen, oder andere Werte in der Antwort waren nicht korrekt.

Lösung: Stellen Sie sicher, dass das KDC, mit dem Sie kommunizieren, mit RFC4120 übereinstimmt, die von Ihnen gesendete Anforderung eine Kerberos V5-Anforderung ist oder das KDC verfügbar ist.

`kdestroy: Could not obtain principal name from cache`
Grund: Der Berechtigungsnachweis-Cache fehlt oder ist beschädigt.

Lösung: Überprüfen Sie, ob der angegebene Cache-Speicherort korrekt ist. Entfernen und fordern Sie bei Bedarf ein neues TGT mit `kinit` an.

`kdestroy: No credentials cache file found while destroying cache`
Grund: Der Berechtigungsnachweis-Cache (`/tmp/krb5c_` *uid*) fehlt oder ist beschädigt.

Lösung: Überprüfen Sie, ob der angegebene Cache-Speicherort korrekt ist. Entfernen und fordern Sie bei Bedarf ein neues TGT mit `kinit` an.

`kdestroy: TGT expire warning NOT deleted`
Grund: Der Berechtigungsnachweis-Cache fehlt oder ist beschädigt.

Lösung: Überprüfen Sie, ob der angegebene Cache-Speicherort korrekt ist. Entfernen und fordern Sie bei Bedarf ein neues TGT mit `kinit` an.

`Kerberos authentication failed`
Grund: Das Kerberos-Passwort ist entweder falsch oder nicht mit dem UNIX-Passwort synchronisiert.

Lösung: Wenn das Passwort nicht synchronisiert ist, müssen Sie ein anderes Passwort angeben, um die Kerberos-Authentifizierung abzuschließen. Es ist möglich, dass der Benutzer das ursprüngliche Passwort vergessen hat.

`Kerberos V5 refuses authentication`
Grund: Die Authentifizierung konnte nicht mit dem Server ausgehandelt werden.

Lösung: Starten Sie die Fehlersuche für die Authentifizierung, indem Sie den Befehl `telnet` mit dem Befehl `toggle authdebug` ausführen, und lesen Sie die Fehlersuchmeldungen für weitere Hinweise. Vergewissern Sie sich außerdem, dass Sie über gültige Berechtigungsnachweise verfügen.

`Key table entry not found`
Grund: Für das Service-Hauptelement ist kein Eintrag in der Schlüsseltabellendatei des Netzwerkanwendungsservers vorhanden.

Lösung: Fügen Sie der Schlüsseltabellendatei des Servers das entsprechende Service-Hauptelement hinzu, damit der kerberisierte Service bereitgestellt werden kann.

`Key version number for principal in key table is incorrect`
Grund: Die Schlüsselversion eines Hauptelements in der Schlüsseltabellendatei weicht von der Version in der Kerberos-Datenbank ab. Entweder wurde der Schlüssel eines Service geändert oder Sie verwenden ein altes Service-Ticket.

Lösung: Wurde der Schlüssel eines Service geändert (z. B. mit `kadmin`), müssen Sie den neuen Schlüssel extrahieren und in der Schlüsseltabellendatei des Hosts speichern, auf dem der Service ausgeführt wird.

Es kann auch sein, dass Sie ein altes Service-Ticket mit einem älteren Schlüssel verwenden. Sie sollten die Befehle `kdestroy` und `kinit` in genannter Reihenfolge erneut ausführen.

`kinit: gethostname failed`
Grund: Aufgrund eines Fehlers in der lokalen Netzwerkkonfiguration schlägt `kinit` fehl.

Lösung: Vergewissern Sie sich, dass der Host ordnungsgemäß konfiguriert ist.

`login: load_modules: can not open module /usr/lib/security/pam_krb5.so.1`
Grund: Das Kerberos-PAM-Modul fehlt entweder oder ist keine gültige ausführbare Binärdatei.

Lösung: Stellen Sie sicher, dass sich das Kerberos-PAM-Module im Verzeichnis `/usr/lib/security` befindet und eine gültige ausführbare Binärdatei ist. Vergewissern Sie sich ebenfalls, dass die Datei `/etc/pam.conf` den richtigen Pfad zu `pam_krb5.so.1` enthält.

`Looping detected inside krb5_get_in_tkt`
Grund: Kerberos versuchte mehrmals, die anfänglichen Tickets abzurufen, aber alle Versuche schlugen fehl.

Lösung: Stellen Sie sicher, dass mindestens ein KDC auf Authentifizierungsanforderungen antwortet.

`Master key does not match database`
Grund: Das geladene Datenbankabbild wurde nicht aus einer Datenbank erstellt, die den Master-Schlüssel enthält. Der Master-Schlüssel befindet sich in `/var/krb5/.k5.`*REALM*.

Lösung: Vergewissern Sie sich, dass der Master-Schlüssel im geladenen Datenbankabbild dem Master-Schlüssel in `/var/krb5/.k5.`*REALM* entspricht.

`Matching credential not found`
Grund: Der entsprechende Berechtigungsnachweis für Ihre Anforderung wurde nicht gefunden. Ihre Anforderung erfordert Berechtigungsnachweise, die im Berechtigungsnachweis-Cache nicht zur Verfügung stehen.

Lösung: Löschen Sie Ihre Tickets mit `kdestroy` und erstellen Sie neue Tickets mit `kinit`.

`Message out of order`
Grund: Meldungen, die unter Verwendung der Vertraulichkeit in fortlaufender Reihenfolge gesendet wurden, wurden in einer anderen Reihenfolge empfangen. Einige Meldungen gingen bei der Übertragung möglicherweise verloren.

Lösung: Sie sollten die Kerberos-Sitzung reinitialisieren.

`Message stream modified`
Grund: Die berechnete Prüfsumme stimmte nicht mit der Prüfsumme der Meldung überein. Die Meldung wurde möglicherweise während der Übertragung geändert, was auf eine Sicherheitslücke hinweisen kann.

Lösung: Stellen Sie sicher, dass die Meldungen korrekt über das Netzwerk übertragen werden. Da diese Meldung auch auf eine mögliche Manipulation von Meldungen während der Übertragung hinweisen kann, löschen Sie Ihre Tickets mit `kdestroy` und reinitialisieren Sie die verwendeten Kerberos-Services.

Häufige Kerberos-Fehlermeldungen (N – Z)

Dieser Abschnitt umfasst eine alphabetische Liste (N – Z) häufiger Fehlermeldungen für die Kerberos-Befehle und -Dämonen, das PAM-Framework, die GSS-Schnittstelle, den NFS-Service sowie die Kerberos-Bibliothek.

`No credentials cache file found`

Grund: Kerberos konnte den Berechtigungsnachweis-Cache (`/tmp/krb5cc_`*uid*) nicht finden.

Lösung: Vergewissern Sie sich, dass die Berechtigungsnachweisdatei vorhanden ist und gelesen werden kann. Ist dies nicht der Fall, versuchen Sie, `kinit` erneut auszuführen.

`No credentials were supplied, or the credentials were unavailable or inaccessible`

`No credential cache found`

Grund: Der Berechtigungsnachweis-Cache des Benutzers ist falsch oder nicht vorhanden.

Lösung: Der Benutzer sollte `kinit` ausführen, bevor er versucht, den Service zu starten.

`No credentials were supplied, or the credentials were unavailable or inaccessible`

`No principal in keytab matches desired name`

Grund: Beim Versuch, den Server zu authentifizieren, ist ein Fehler aufgetreten.

Lösung: Stellen Sie sicher, dass sich der Host oder das Service-Hauptelement in der Schlüsseltabellendatei des Servers befindet.

`Operation requires “`*privilege*`” privilege`

Grund: Das verwendete Hauptelement `admin` verfügt nicht über die entsprechende in der Datei `kadm5.acl` konfigurierte Berechtigung.

Lösung: Verwenden Sie ein Hauptelement, das über die entsprechenden Berechtigungen verfügt. Alternativ können Sie auch das verwendete Hauptelement konfigurieren, um über die entsprechenden Berechtigungen zu verfügen, indem Sie die Datei `kadm5.acl` ändern. Üblicherweise weist ein Hauptelement, dessen Name `/admin` enthält, die jeweiligen Berechtigungen auf.

`PAM-KRB5 (auth): krb5_verify_init_creds failed: Key table entry not found`

Grund: Die Remote-Anwendung versuchte, das Service-Hauptelement des Hosts in der lokalen `/etc/krb5/krb5.keytab`-Datei zu lesen, dieses ist jedoch nicht vorhanden.

Lösung: Fügen Sie der Schlüsseltabellendatei des Hosts dessen Service-Hauptelement hinzu.

`Password is in the password dictionary`

Grund: Das von Ihnen angegebene Passwort befindet sich in einem Passwort-Wörterbuch, das gerade verwendet wird. Ihr angegebenes Passwort ist nicht gut als Passwort geeignet.

Lösung: Wählen Sie ein Passwort mit einer Mischung aus mehreren Passwortklassen.

`Permission denied in replay cache code`

Grund: Der Wiedergabe-Cache des Systems konnte nicht geöffnet werden. Ihr Server wurde möglicherweise zunächst unter einer Benutzer-ID ausgeführt, die sich von Ihrer aktuellen Benutzer-ID unterscheidet.

Lösung: Vergewissern Sie sich, dass der Wiedergabe-Cache die entsprechenden Berechtigungen aufweist. Der Wiedergabe-Cache ist auf dem Host gespeichert, auf dem die kerberisierte Serveranwendung ausgeführt wird. Für Nicht-`root`-Benutzer heißt die Wiedergabe-Cachedatei `/var/krb5/rcache/rc_`*service_name_ uid*. Für Root-Benutzer heißt die Wiedergabe-Cachedatei `/var/krb5/rcache/root/rc_` *service_name*.

`Protocol version mismatch`

Grund: Wahrscheinlich wurde eine Kerberos V4-Anforderung an das KDC gesendet. Der Kerberos-Service unterstützt nur das Kerberos V5-Protokoll.

Lösung: Stellen Sie sicher, dass Ihre Anwendungen das Kerberos V5-Protokoll verwenden.

`Request is a replay`

Grund: Die Anforderung wurde bereits an diesen Server gesendet und verarbeitet. Die Tickets wurden möglicherweise gestohlen und eine andere Person versucht, sie wiederzuverwenden.

Lösung: Warten Sie einige Minuten und übermitteln Sie dann die Anforderung erneut.

`Requested principal and ticket don’t match`

Grund: Das Service-Hauptelement, zu dem Sie eine Verbindung herstellen, und Ihr Service-Ticket stimmen nicht überein.

Lösung: Vergewissern Sie sich, dass DNS ordnungsgemäß funktioniert. Wenn Sie die Software eines anderen Herstellers verwenden, stellen Sie sicher, dass Hauptelementnamen in der Software korrekt verwendet werden.

`Requested protocol version not supported`

Grund: Wahrscheinlich wurde eine Kerberos V4-Anforderung an das KDC gesendet. Der Kerberos-Service unterstützt nur das Kerberos V5-Protokoll.

Lösung: Stellen Sie sicher, dass Ihre Anwendungen das Kerberos V5-Protokoll verwenden.

`Server refused to negotiate authentication, which is required for encryption. Good bye.`

Grund: Die Remote-Anwendung ist entweder nicht fähig, die Kerberos-Authentifizierung vom Client zu akzeptieren oder wurde dementsprechend konfiguriert.

Lösung: Geben Sie eine Remote-Anwendung an, die eine Authentifizierung aushandeln kann, oder konfigurieren Sie die Anwendung so, dass sie die entsprechenden Flags zur Aktivierung der Authentifizierung verwendet.

`Server refused to negotiate encryption. Good bye.`

Grund: Die Verschlüsselung konnte nicht mit dem Server ausgehandelt werden.

Lösung: Starten Sie die Fehlersuche für die Authentifizierung, indem Sie den Befehl `telnet` mit dem Befehl `toggle encdebug` ausführen, und lesen Sie die Fehlersuchmeldungen für weitere Hinweise.

`Server rejected authentication (during sendauth exchange)`

Grund: Der Server, mit dem Sie zu kommunizieren versuchen, hat die Authentifizierung zurückgewiesen. Dieser Fehler tritt meistens während der Weitergabe der Kerberos-Datenbank auf. Die Ursache liegt häufig in Problemen mit der Datei `kpropd.acl`, DNS oder der Schlüsseltabellendatei.

Lösung: Falls Ihnen dieser Fehler angezeigt wird, wenn Sie andere Anwendungen als `kprop` ausführen, überprüfen Sie, ob die Schlüsseltabellendatei des Servers korrekt ist.

`The ticket isn't for us`

`Ticket/authenticator don't match`

Grund: Das Ticket und der Authentifizierer stimmten nicht miteinander überein. Der Hauptelementname in der Anforderung entsprach möglicherweise nicht dem Namen des Service-Hauptelements. Dies liegt entweder daran, dass das Ticket mit einem FQDN-Namen des Hauptelements gesendet wurde, während der Service einen anderen Namen erwartete, oder ein Nicht-FDQN-Name gesendet wurde und der Service einen FQDN-Namen erwartete.

Lösung: Falls Ihnen dieser Fehler angezeigt wird, wenn Sie andere Anwendungen als `kprop` ausführen, überprüfen Sie, ob die Schlüsseltabellendatei des Servers korrekt ist.

`Ticket expired`
Grund: Die Dauer Ihrer Tickets ist abgelaufen.

Lösung: Löschen Sie Ihre Tickets mit `kdestroy` und erstellen Sie neue Tickets mit `kinit`.

`Ticket is ineligible for postdating`
Grund: Das Hauptelement lässt nicht die Nachdatierung aller dazugehörigen Tickets zu.

Lösung: Ändern Sie das Hauptelement mit `kadmin` dahingehend, dass es die Nachdatierung zulässt.

`Ticket not yet valid`
Grund: Das nachdatierte Ticket ist noch nicht gültig.

Lösung: Erstellen Sie ein neues Ticket mit dem richtigen Datum oder warten Sie, bis das aktuelle Ticket gültig ist.

`Truncated input file detected`
Grund: Bei der während des Vorgangs verwendeten Abbilddatei der Datenbank handelt es sich um keine vollständige Abbilddatei.

Lösung: Erstellen Sie die Abbilddatei erneut oder verwenden Sie eine andere Abbilddatei der Datenbank.

`Unable to securely authenticate user ... exit`
Grund: Die Authentifizierung konnte nicht mit dem Server ausgehandelt werden.

Lösung: Starten Sie die Fehlersuche für die Authentifizierung, indem Sie den Befehl `telnet` mit dem Befehl `toggle authdebug` ausführen, und lesen Sie die Fehlersuchmeldungen für weitere Hinweise. Vergewissern Sie sich außerdem, dass Sie über gültige Berechtigungsnachweise verfügen.

`Wrong principal in request`
Grund: Das Ticket enthielt einen ungültigen Hauptelementnamen. Dieser Fehler weist eventuell auf ein DNS- oder FQDN-Problem hin.

Lösung: Vergewissern Sie sich, dass das Hauptelement des Service mit dem Hauptelement im Ticket übereinstimmt.

Kerberos-Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung für die Kerberos-Software.

Probleme mit dem Format der Datei `krb5.conf`

Wenn die Datei `krb5.conf` nicht ordnungsgemäß formatiert wurde, wird auf dem Terminal oder in der Protokolldatei gegebenenfalls folgende Fehlermeldung angezeigt:

```
Improper format of Kerberos configuration file while initializing krb5 library
```

Wenn ein Problem mit dem Format der Datei `krb5.conf` besteht, sind die entsprechenden Services für Angriffe anfällig. Sie sollten dieses Problem beheben, bevor Sie die Verwendung von Kerberos-Funktionen zulassen.

Probleme bei der Weitergabe der Kerberos-Datenbank

Wenn die Weitergabe der Kerberos-Datenbank fehlschlägt, versuchen Sie `/usr/bin/rlogin -x` zwischen dem Slave-KDC und dem Master-KDC sowie vom Master- zum Slave-KDC-Server.

Wurden die KDCs so eingerichtet, dass sie den Zugriff einschränken, ist `rlogin` deaktiviert und kann nicht zur Behebung dieses Problems verwendet werden. Zum Aktivieren von `rlogin` auf einem KDC müssen Sie den Service `eklogin` aktivieren.

```
# svcadm enable svc:/network/login:eklogin
```

Nachdem Sie das Problem behoben haben, müssen Sie den Service `eklogin` deaktivieren.

Wenn `rlogin` nicht funktioniert, hängen die Probleme vermutlich mit den Schlüsseltabellendateien auf den KDCs zusammen. Wenn `rlogin` funktioniert, liegt das Problem nicht in der Schlüsseltabellendatei oder dem Name Service, da `rlogin` und die Software für die Weitergabe dasselbe `host/` *host-name*-Hauptelement verwenden. Stellen Sie in diesem Fall sicher, dass die Datei `kpropd.acl` korrekt ist.

Probleme beim Einhängen eines kerberisierten NFS-Dateisystems

- Schlägt das Einhängen eines kerberisierten NFS-Dateisystems fehl, vergewissern Sie sich, dass die Datei `/var/rcache/root` auf dem NFS-Server vorhanden ist. Wenn `root` nicht Eigentümer des Dateisystems ist, entfernen Sie es und versuchen Sie den Einhängevorgang erneut.

- Tritt beim Zugriff auf ein kerberisiertes NFS-Dateisystem ein Problem auf, stellen Sie sicher, dass der Service `gssd` auf Ihrem System und auf dem NFS-Server aktiviert ist.
- Wird beim Versuch, auf ein kerberisiertes NFS-Dateisystem zuzugreifen, entweder die Fehlermeldung `invalid argument` oder `bad directory` angezeigt, könnte das Problem darin bestehen, dass Sie zum Einhängen des NFS-Dateisystems keinen vollständig qualifizierten DNS-Namen verwenden. Der eingehängte Host entspricht nicht dem Hostnamenteil des Service-Hauptelements in der Schlüsseltabellendatei des Servers.

  Dieses Problem kann auch dann auftreten, wenn Ihr Server über mehrere Ethernet-Schnittstellen verfügt und Sie DNS für die Verwendung eines Schemas eingerichtet haben, das einen Namen pro Schnittstelle vorsieht, anstelle eines Schemas, das auf dem Prinzip mehrerer Adressdatensätze pro Host basiert. Für den Kerberos-Service sollten Sie mehrere Adressdatensätze pro Host einrichten, wie nachfolgend dargestellt[1] :

```
my.host.name.   A       1.2.3.4
                A       1.2.4.4
                A       1.2.5.4

my-en0.host.name.       A       1.2.3.4
my-en1.host.name.       A       1.2.4.4
my-en2.host.name.       A       1.2.5.4

4.3.2.1         PTR     my.host.name.
4.4.2.1         PTR     my.host.name.
4.5.2.1         PTR     my.host.name.
```

In diesem Beispiel ermöglicht das Setup eine Referenz auf die verschiedenen Schnittstellen und ein einziges Service-Hauptelement anstelle von drei Service-Hauptelementen in der Schlüsseltabellendatei des Servers.

Probleme beim Authentifizieren als `root`

Schlägt die Authentifizierung fehl, wenn Sie sich als Superuser bei Ihrem System anmelden und das `root`-Hauptelement bereits der Schlüsseltabellendatei Ihres Hosts hinzugefügt haben, kann dies mit zwei potenziellen Problemen zusammenhängen. Vergewissern Sie sich zunächst, dass das `root`-Hauptelement in der Schlüsseltabellendatei einen vollständig qualifizierten Hostnamen als zugehörige Instanz aufweist. Ist dies der Fall, überprüfen Sie die Datei `/etc/resolv.conf`, um sicherzustellen, dass das System korrekt als DNS-Client eingerichtet ist.

[1] Ken Hornstein, "Kerberos FAQ," [http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#kerbdns], accessed 10 March 2010.

Überwachen der Zuordnungen von GSS-Berechtigungsnachweisen zu UNIX-Berechtigungsnachweisen

Um die Zuordnungen von Berechtigungsnachweisen überwachen zu können, entfernen Sie zunächst die Auskommentierung dieser Zeile in der Datei `/etc/gss/gsscred.conf`.

```
SYSLOG_UID_MAPPING=yes
```

Weisen Sie anschließend den Service `gssd` an, Informationen aus der Datei `/etc/gss/gsscred.conf` abzurufen.

```
# pkill -HUP gssd
```

Jetzt sollten Sie in der Lage sein, die Zuordnungen der Berechtigungsnachweise zu überwachen, wenn `gssd` sie anfordert. Die Zuordnungen werden von `syslogd` aufgezeichnet, wenn die Datei `syslog.conf` für die Systemfunktion `auth` mit dem Schweregrad `debug` konfiguriert ist.

◆ ◆ ◆ KAPITEL 25

Verwalten von Kerberos-Hauptelementen und Richtlinien (Aufgaben)

In diesem Kapitel werden Verfahren für die Verwaltung von Hauptelementen und die damit verbundenen Richtlinien beschrieben. Ebenfalls wird in diesem Kapitel dargestellt, wie die Schlüsseltabellendatei eines Hosts verwaltet wird.

Dieses Kapitel sollte von jedem gelesen werden, der Hauptelemente und Richtlinien verwalten muss. Vor dem Lesen dieses Kapitels sollten Sie sich mit den Hauptelementen und Richtlinien vertraut machen, einschließlich aller Überlegungen bezüglich der Planung. Weitere Informationen finden Sie in Kapitel 21, „Einführung zum Kerberos-Service“ und Kapitel 22, „Planen des Kerberos-Service“.

Im Folgenden sind die Informationen in diesem Kapitel aufgeführt.

- „Möglichkeiten zur Verwaltung von Kerberos-Hauptelementen und -Richtlinien“ auf Seite 527
- „SEAM-Tool“ auf Seite 528
- „Verwalten von Kerberos-Hauptelementen“ auf Seite 532
- „Verwalten von Kerberos-Richtlinien“ auf Seite 546
- „SEAM-Tool-Referenz“ auf Seite 555
- „Verwalten von Schlüsseltabellendateien“ auf Seite 560

Möglichkeiten zur Verwaltung von Kerberos-Hauptelementen und -Richtlinien

Die Kerberos-Datenbank auf dem Master-KDC enthält alle Kerberos-Hauptelemente Ihres Bereichs, die dazugehörigen Passwörter, Richtlinien und weitere Verwaltungsinformationen. Zum Erstellen und Löschen von Hauptelementen und zum Ändern der dazugehörigen Attribute können Sie entweder den Befehl `kadmin` oder `gkadmin` verwenden.

Der Befehl `kadmin` bietet eine interaktive Befehlszeilenschnittstelle, mit der Sie die Hauptelemente und Richtlinien von Kerberos sowie Schlüsseltabellendateien verwalten können. Es sind zwei Versionen des Befehls `kadmin` vorhanden:

- `kadmin`: Verwendet die Kerberos-Authentifizierung für einen sicheren Betrieb im gesamten Netzwerk
- `kadmin.local`: Müssen direkt auf dem Master-KDC ausgeführt werden

Abgesehen davon, dass `kadmin` Kerberos zur Authentifizierung des Benutzers verwendet, sind die Funktionen der beiden Versionen identisch. Die lokale Version ist erforderlich, damit Sie die Datenbank ausreichend einrichten können, um die Remote-Version zu verwenden.

Auch die Oracle Solaris-Version bietet das SEAM-Tool, `gkadmin`, bei dem es sich um eine interaktive grafische Benutzeroberfläche (GUI) handelt, die im Wesentlichen dieselben Funktionen bereitstellt wie der Befehl `kadmin`. Weitere Informationen finden Sie unter „SEAM-Tool“ auf Seite 528.

SEAM-Tool

Das SEAM-Tool (gkadmin) stellt eine interaktive grafische Benutzeroberfläche (GUI) dar, mit der Sie die Kerberos-Hauptelemente und -Richtlinien verwalten können. Es bietet nahezu dieselben Funktionen wie der Befehl `kadmin`. Die Verwaltung von Schlüsseltabellendateien wird jedoch nicht unterstützt. Zum Verwalten von Schlüsseltabellendateien müssen Sie den Befehl `kadmin` verwenden, wie unter „Verwalten von Schlüsseltabellendateien“ auf Seite 560 beschrieben.

Wie auch der Befehl `kadmin` verwendet das SEAM-Tool die Kerberos-Authentifizierung und verschlüsseltes RPC für den sicheren Betrieb im gesamten Netzwerk. Das SEAM-Tool bietet Ihnen folgende Möglichkeiten:

- Erstellen neuer Hauptelemente, die auf Standardwerten oder vorhandenen Hauptelementen basieren
- Erstellen neuer Richtlinien, die auf vorhandenen Richtlinien basieren
- Hinzufügen von Kommentaren für Hauptelemente
- Einrichten von Standardwerten zur Erstellung neuer Hauptelemente
- Anmelden als weiteres Hauptelement ohne Beenden des Tools
- Drucken oder Speichern von Hauptelement- und Richtlinienlisten
- Anzeigen und Suchen von Hauptelement- und Richtlinienlisten

Das SEAM-Tool bietet auch kontextbezogene Hilfe und allgemeine Onlinehilfe.

Die folgende Übersicht der Schritte bietet Zeiger auf die verschiedenen Aufgaben, die Sie mit dem SEAM-Tool: ausführen können.

- „Verwalten von Kerberos-Hauptelementen (Übersicht der Schritte)“ auf Seite 532
- „Verwalten von Kerberos-Richtlinien (Übersicht der Schritte)“ auf Seite 546

Beschreibungen aller Hauptelement- und Richtlinienattribute, die Sie im SEAM-Tool angeben oder anzeigen können, finden Sie unter „Beschreibungen der SEAM-Tool-Fensterbereiche“ auf Seite 555.

Befehlszeilenäquivalente des SEAM-Tools

In diesem Abschnitt werden die `kadmin`-Befehle mit denselben Funktionen wie das SEAM-Tool aufgelistet. Diese Befehle können ohne Ausführung eines X Window-Systems verwendet werden. Auch wenn die meisten in diesem Kapitel beschriebenen Verfahren das SEAM-Tool verwenden, bieten viele Verfahren auch entsprechende Beispiele für die Verwendung der Befehlszeilenäquivalente.

TABELLE 25–1 Befehlszeilenäquivalente des SEAM-Tools

SEAM-Tool-Verfahren	Äquivalent zum Befehl `kadmin`
Anzeigen der Liste der Hauptelemente	`list_principals` oder `get_principals`
Anzeigen der Attribute eines Hauptelements	`get_principal`
Erstellen eines neuen Hauptelements	`add_principal`
Duplizieren eines Hauptelements	Kein Befehlszeilenäquivalent
Ändern eines Hauptelements	`modify_principal` oder `change_password`
Löschen eines Hauptelements	`delete_principal`
Einrichten von Standardwerten zur Erstellung neuer Hauptelemente	Kein Befehlszeilenäquivalent
Anzeigen der Liste der Richtlinien	`list_policies` oder `get_policies`
Anzeigen der Attribute einer Richtlinie	`get_policy`
Erstellen einer neuen Richtlinie	`add_policy`
Duplizieren einer Richtlinie	Kein Befehlszeilenäquivalent
Ändern einer Richtlinie	`modify_policy`
Löschen einer Richtlinie	`delete_policy`

Die einzige vom SEAM-Tool geänderte Datei

Die einzige vom SEAM-Tool geänderte Datei ist die Datei `$HOME/.gkadmin` . Diese Datei enthält die Standardwerte zur Erstellung neuer Hauptelemente. Sie können diese Datei aktualisieren, indem Sie im Menü "Edit" (Bearbeiten) die Option "Properties" (Eigenschaften) auswählen.

Druck- und Onlinehilfefunktionen des SEAM-Tools

Das SEAM-Tool bietet sowohl Druck- als auch Onlinehilfefunktionen. Im Menü "Print" (Drucken) können Sie Folgendes an einen Drucker oder eine Datei senden:

- Liste der verfügbaren Hauptelemente auf dem angegebenen Master-KDC
- Liste der verfügbaren Richtlinien auf dem angegebenen Master-KDC
- Das aktuell ausgewählte oder das geladene Hauptelement
- Die aktuell ausgewählte oder die geladene Richtlinie

Im Menü "Help" (Hilfe) können Sie auf die kontextbezogene Hilfe und auf die allgemeine Hilfe zugreifen. Wenn Sie im Menü "Help" (Hilfe) die Option kontextbezogene Hilfe aufrufen, wird das Fenster für die kontextbezogene Hilfe angezeigt und das Tool wechselt in den Hilfemodus. Wenn Sie im Hilfemodus auf ein Feld, eine Beschriftung oder eine Schaltfläche im Fenster klicken, wird zu diesem Element im Hilfefenster ein Hilfetext angezeigt. Klicken Sie im Hilfefenster auf "Dismiss" (Verlassen), damit das Tool in den normalen Modus zurückkehrt.

Durch Auswahl von "Help Contents" (Inhalt der Hilfe) können Sie außerdem einen HTML-Browser öffnen, der Zeiger auf die allgemeine Übersicht und auf in diesem Kapitel enthaltene aufgabenbezogene Informationen bietet.

Arbeiten mit großen Listen im SEAM-Tool

Je mehr Hauptelemente und Richtlinien Ihre Site aufweist, desto mehr Zeit benötigt das SEAM-Tool zum Laden und Anzeigen der Hauptelemente- und Richtlinienlisten. Dadurch verringert sich die Produktivität bei der Arbeit mit dem Tool. Es gibt verschiedene Möglichkeiten, dieses Problem zu vermeiden.

Als erstes können Sie die Ladezeit für die Listen vollständig eliminieren, indem die Listen nicht vom SEAM-Tool geladen werden. Wählen Sie dazu im Menü "Edit" (Bearbeiten) die Option "Properties" (Eigenschaften) und deaktivieren Sie das Feld "Show Lists" (Listen anzeigen). Wenn das Tool die Listen nicht lädt, kann es die Listen logischerweise nicht anzeigen, sodass Sie die Listenbereiche nicht mehr zur Auswahl von Hauptelementen oder Richtlinien verwenden können. Stattdessen müssen Sie im neu angezeigten Feld "Name" einen Hauptelement- oder Richtlinienamen eingeben und dann den auszuführenden Vorgang auswählen. Die Eingabe eines Namens ist im Grunde gleichbedeutend mit der Auswahl eines Elements aus der Liste.

Eine weitere Möglichkeit besteht darin, die großen Listen im Cache zwischenzuspeichern. Die Zwischenspeicherung der Listen für eine begrenzte Zeit ist als Standardeinstellung für das SEAM-Tool festgelegt. Das SEAM-Tool muss die Listen zu Beginn nach wie vor in den Cache laden. Anschließend kann es jedoch den Cache verwenden, anstatt die Listen erneut abzurufen. Dank dieser Option müssen die Listen nicht mehr vom Server geladen werden, wodurch viel Zeit gespart wird.

Um die Zwischenspeicherung der Listen festzulegen, wählen Sie im Menü "Edit" (Bearbeiten) die Option "Properties" (Eigenschaften). Es stehen zwei Cache-Einstellungen zur Verfügung. Sie können die Liste entweder dauerhaft im Cache speichern oder eine zeitliche Begrenzung angeben, nach der das Tool die Listen erneut vom Server in den Cache laden muss.

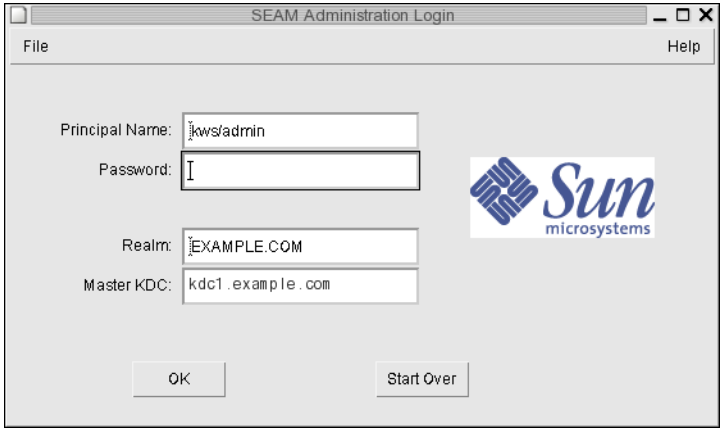
Bei der Zwischenspeicherung der Listen im Cache können Sie Hauptelemente und Richtlinien mithilfe der Listenbereiche auswählen. Die Cache-Speicherung wirkt sich somit im Gegensatz zur ersten Option nicht auf die Verwendung des SEAM-Tools aus. Bei der Zwischenspeicherung werden Ihnen Änderungen anderer Benutzer nicht angezeigt, Sie können jedoch Ihre eigenen Änderungen in den Listen sehen, da die Informationen auf dem Server und im Cache mit Ihren Änderungen aktualisiert werden. Wenn Sie den Cache aktualisieren möchten, um andere Änderungen anzuzeigen und die aktuelle Version der Listen zu erhalten, können mithilfe des Menüs "Refresh" (Aktualisieren) jederzeit den Cache mit Daten vom Server aktualisieren.

▼ So starten Sie das SEAM-Tool

1 Starten Sie das SEAM-Tool mit dem Befehl `gkadmin`.

```
$ /usr/sbin/gkadmin
```

Das Anmeldefenster für die SEAM-Administration wird angezeigt.



2 **Wenn Sie nicht die Standardwerte verwenden möchten, geben Sie neue Standardwerte an.**

Die Standardwerte werden automatisch im Fenster eingefügt. Der standardmäßige Hauptelementname wird bestimmt, indem Ihre aktuelle Identität von der Umgebungsvariable `USER` übernommen und `/admin` daran angehängt wird (*username* `/admin`). Die Felder für den Standardbereich und das Master-KDC werden der Datei `/etc/krb5/krb5.conf` entnommen. Wenn Sie zu den Standardwerten zurückkehren möchten, klicken Sie auf "Start Over" (Erneute Eingabe).

Hinweis – Die Verwaltungsvorgänge, die jeder Hauptelementname ausführen kann, werden durch die ACL-Datei von Kerberos (`/etc/krb5/kadm5.acl`) bestimmt. Informationen über eingeschränkte Berechtigungen finden Sie unter „Verwenden des SEAM-Tools mit eingeschränkten Kerberos-Administratorberechtigungen“ auf Seite 558.

---

3 **Geben Sie ein Passwort für den angegebenen Hauptelementnamen ein.**

4 **Klicken Sie auf "OK".**

Ein Fenster mit allen Hauptelementen wird angezeigt.

Verwalten von Kerberos-Hauptelementen

Dieser Abschnitt enthält schrittweise Anleitungen zur Verwaltung von Hauptelementen mit dem SEAM-Tool. Außerdem werden Beispiele für Befehlszeitenäquivalente aufgeführt (sofern vorhanden).

Verwalten von Kerberos-Hauptelementen (Übersicht der Schritte)

Aufgabe	Beschreibung	Anweisungen
Anzeigen der Liste der Hauptelemente	Zeigen Sie die Liste der Hauptelemente durch Klicken auf die Registerkarte "Principals" (Hauptelemente) an.	„So zeigen Sie die Liste der Kerberos-Hauptelemente an“ auf Seite 534
Anzeigen der Attribute eines Hauptelements	Zeigen Sie die Attribute eines Hauptelements durch Auswählen des Hauptelements in der Hauptelementliste und anschließendes Klicken auf die Schaltfläche "Modify" (Ändern) an.	„So zeigen Sie die Attribute eines Kerberos-Hauptelements an“ auf Seite 536
Erstellen eines neuen Hauptelements	Erstellen Sie ein neues Hauptelement durch Klicken auf die Schaltfläche "Create New" (Neu erstellen) im Fensterbereich "Principal List" (Liste der Hauptelemente).	„So erstellen Sie ein neues Kerberos-Hauptelement“ auf Seite 538

Aufgabe	Beschreibung	Anweisungen
Duplizieren eines Hauptelements	Duplizieren Sie ein Hauptelement durch Auswählen des Elements in der Hauptelementliste und Klicken auf die Schaltfläche "Duplicate" (Duplizieren).	„So duplizieren Sie ein Kerberos-Hauptelement“ auf Seite 541
Ändern eines Hauptelements	Ändern Sie ein Hauptelement durch Auswählen des Elements in der Hauptelementliste und anschließendes Klicken auf die Schaltfläche "Modify" (Ändern). Beachten Sie, dass Sie den Namen eines Hauptelements nicht ändern können. Zum Unbenennen eines Hauptelements müssen Sie das Hauptelement duplizieren, neu benennen, speichern und anschließend das alte Hauptelement löschen.	„So ändern Sie ein Kerberos-Hauptelement“ auf Seite 542
Löschen eines Hauptelements	Löschen Sie ein Hauptelement durch Auswählen des Hauptelements in der Hauptelementliste und anschließendes Klicken auf die Schaltfläche "Delete" (Löschen).	„So löschen Sie ein Kerberos-Hauptelement“ auf Seite 543
Einrichten von Standardwerten zur Erstellung neuer Hauptelemente	Richten Sie Standardwerte zur Erstellung neuer Hauptelemente durch Auswählen von "Properties" (Eigenschaften) im Menü "Edit" (Bearbeiten) ein.	„So richten Sie Standardwerte zur Erstellung neuer Kerberos-Hauptelemente ein“ auf Seite 543
Ändern der Kerberos-Administratorberechtigungen (Datei `kadm5.acl`)	*Nur Befehlszeile.* In den Kerberos-Administratorberechtigungen wird festlegt, welche Vorgänge ein Hauptelement in der Kerberos-Datenbank ausführen kann (zum Beispiel Hinzufügen und Ändern). Zum Ändern der Kerberos-Administratorberechtigungen für jedes Hauptelement müssen Sie die Datei `/etc/krb5/kadm5.acl` bearbeiten.	„So ändern Sie die Kerberos-Administratorberechtigungen“ auf Seite 544

Automatisieren der Erstellung neuer Kerberos-Hauptelemente

Obwohl das SEAM-Tool einfach zu verwenden ist, bietet es keine Möglichkeit zur Automatisierung der Erstellung neuer Hauptelemente. Die Automatisierung ist besonders dann hilfreich, wenn Sie innerhalb kurzer Zeit zehn oder sogar 100 neue Hauptelemente hinzufügen müssen. Dies können Sie durch Ausführen des Befehls `kadmin.local` in einem Bourne-Shell-Skript erreichen.

Die folgende Zeile eines Shell-Skripts ist ein Beispiel für die Automatisierung der Erstellung neuer Hauptelemente:

```
awk '{ print "ank +needchange -pw", $2, $1 }' < /tmp/princnames |
        time /usr/sbin/kadmin.local> /dev/null
```

Zur besseren Lesbarkeit ist dieses Beispiel in zwei Zeilen aufgeteilt. Das Skript liest in einer Datei namens `princnames`, die Hauptelementnamen und die dazugehörigen Passwörter enthält, und fügt diese der Kerberos-Datenbank hinzu. Sie müssen die Datei `princnames` erstellen, die einen Hauptelementnamen und das dazugehörige Passwort in jeder Zeile enthält, getrennt durch mindestens ein Leerzeichen. Die Option `+needchange` konfiguriert das Hauptelement so, dass der Benutzer während der ersten Anmeldung beim Hauptelement zur Angabe eines neuen Passworts aufgefordert wird. Dadurch wird sichergestellt, dass die Passwörter in der Datei `princnames` kein Sicherheitsrisiko darstellen.

Sie können ausführlichere Skripte erstellen. Beispiel: Ihr Skript könnte die Informationen im Name Service verwenden, um die Liste der Benutzernamen für die Hauptelementnamen abzurufen. Welche Schritte Sie ausführen, und auf welche Weise, hängt von den Anforderungen Ihrer Site und Ihren Scripting-Kenntnissen ab.

▼ So zeigen Sie die Liste der Kerberos-Hauptelemente an

Im Anschluss an dieses Verfahren wird ein Beispiel des Befehlszeilenäquivalents gezeigt.

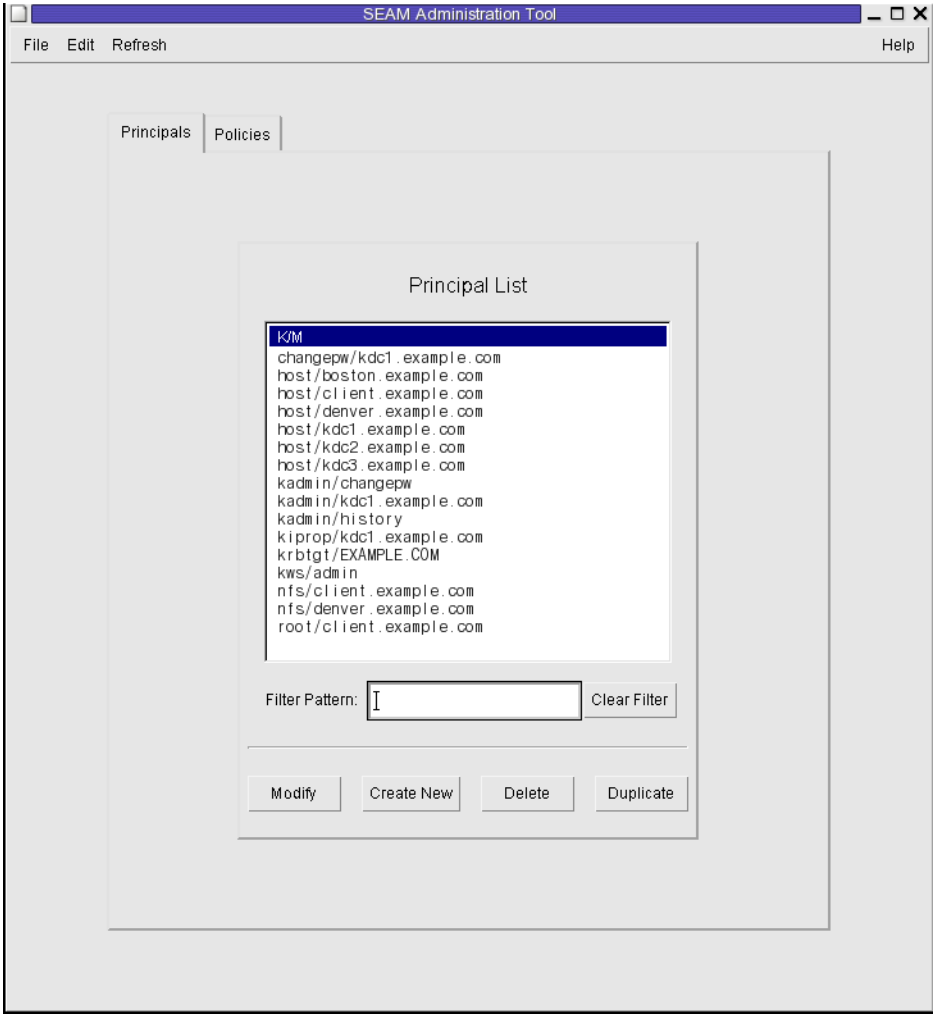
1 Starten Sie bei Bedarf das SEAM-Tool.

Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

```
$ /usr/sbin/gkadmin
```

2 Klicken Sie auf die Registerkarte "Principals" (Hauptelemente).

Die Liste der Hauptelemente wird angezeigt.



3 Zeigen Sie ein bestimmtes Hauptelement oder eine Teilliste von Hauptelementen an.

Geben Sie eine Filterzeichenfolge in das Feld "Filter" ein und drücken Sie die Eingabetaste. Bei erfolgreicher Anwendung des Filters wird die Liste der Hauptelemente angezeigt, die diesem Filter entsprechen.

Die Filterzeichenfolge muss mindestens ein Zeichen umfassen. Da beim Filtermechanismus zwischen Groß- und Kleinschreibung unterschieden wird, müssen Sie die entsprechenden

Groß- und Kleinbuchstaben für den Filter verwenden. Beispiel: Wenn Sie die Filterzeichenfolge ge eingeben, zeigt der Filtermechanismus nur die Hauptelemente an, die die Zeichenfolge ge enthalten (zum Beispiel `george` oder `edge`).

Zum Anzeigen der gesamten Liste der Hauptelemente klicken Sie auf "Clear Filter" (Filter löschen).

Beispiel 25–1 Anzeigen der Liste der Kerberos-Hauptelemente (Befehlszeile)

Im folgenden Beispiel werden mit dem Befehl `list_principals` von `kadmin` alle Hauptelemente aufgelistet, die `kadmin*` entsprechen. In Verbindung mit dem Befehl `list_principals` können auch Platzhalter verwendet werden.

```
kadmin: list_principals kadmin*
kadmin/changepw@EXAMPLE.COM
kadmin/kdc1.example.con@EXAMPLE.COM
kadmin/history@EXAMPLE.COM
kadmin: quit
```

▼ So zeigen Sie die Attribute eines Kerberos-Hauptelements an

Im Anschluss an dieses Verfahren wird ein Beispiel des Befehlszeilenäquivalents gezeigt.

1. **Starten Sie bei Bedarf das SEAM-Tool.**

   Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Klicken Sie auf die Registerkarte "Principals" (Hauptelemente).**

3. **Wählen Sie das anzuzeigende Hauptelement in der Liste und klicken Sie auf "Modify" (Ändern).**

   Der Fensterbereich "Principal Basics" (Grundeinstellungen für Hauptelement) mit einigen Attributen des Hauptelements wird angezeigt.

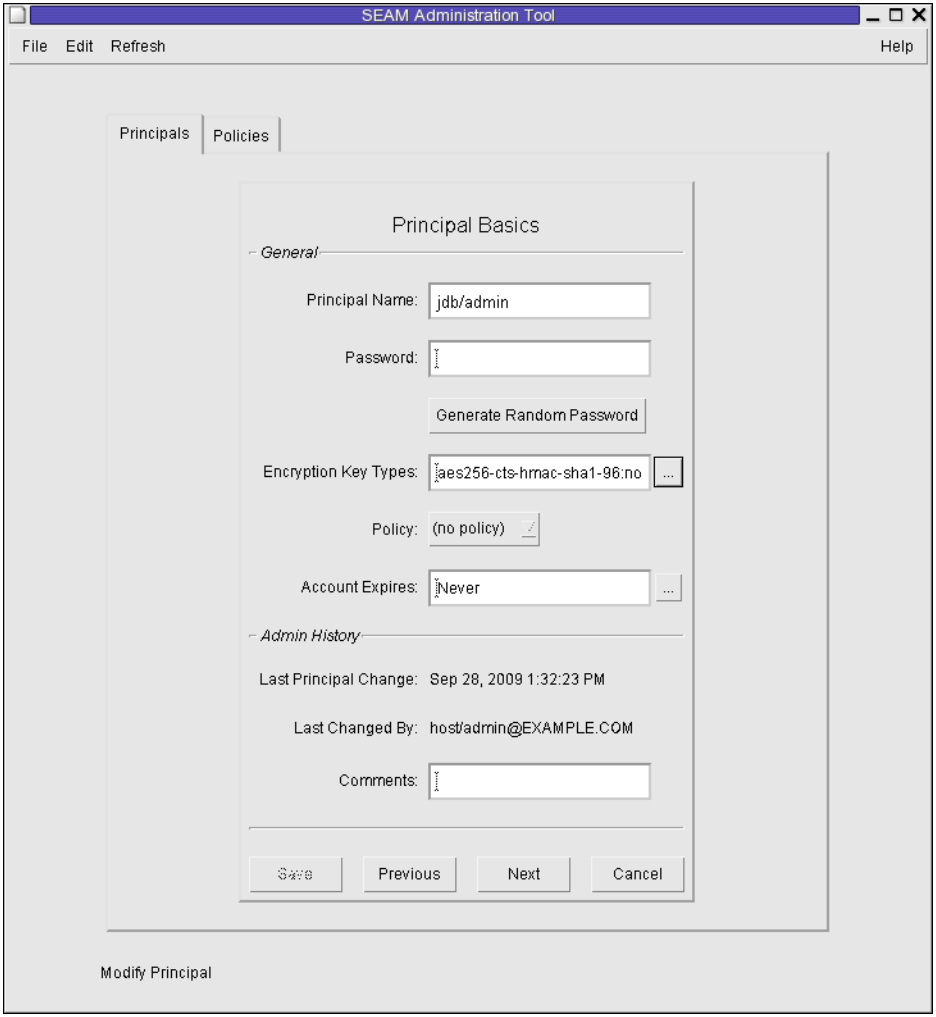
4. **Klicken Sie auf "Next" (Weiter), um alle Attribute des Hauptelements anzuzeigen.**

   Es sind drei Fenster mit Attributinformationen vorhanden. Wählen Sie im Menü "Help" (Hilfe) die Option "Context-Sensitive Help" (Kontextbezogene Hilfe), um Informationen zu den verschiedenen Attributen in jedem Fenster abzurufen. Beschreibungen zu allen Attributen des Hauptelements finden Sie unter „Beschreibungen der SEAM-Tool-Fensterbereiche“ auf Seite 555.

5. **Wenn Sie mit der Anzeige fertig sind, klicken Sie auf "Cancel" (Abbrechen).**

Beispiel 25–2 Anzeigen der Attribute eines Kerberos-Hauptelements

Im folgenden Beispiel sehen Sie das erste Fenster bei Anzeige des Hauptelements `JDB/admin`.



Beispiel 25–3 Anzeigen der Attribute eines Kerberos-Hauptelements (Befehlszeile)

Im folgenden Beispiel werden mit dem Befehl `get_principal` von `kadmin` die Attribute des Hauptelements `jdb/admin` angezeigt.

```
kadmin: getprinc jdb/admin
Principal: jdb/admin@EXAMPLE.COM

Expiration date: [never]
Last password change: [never]

Password expiration date: Wed Apr 14 11:53:10 PDT 2011
Maximum ticket life: 1 day 16:00:00
Maximum renewable life: 1 day 16:00:00
Last modified: Mon Sep 28 13:32:23 PST 2009 (host/admin@EXAMPLE.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 1
Key: vno 1, AES-256 CTS mode with 96-bit SHA-1 HMAC, no salt
Key: vno 1, AES-128 CTS mode with 96-bit SHA-1 HMAC, no salt
Key: vno 1, Triple DES with HMAC/sha1, no salt
Key: vno 1, ArcFour with HMAC/md5, no salt
Key: vno 1, DES cbc mode with RSA-MD5, no salt
Attributes: REQUIRES_HW_AUTH
Policy: [none]
kadmin: quit
```

▼ So erstellen Sie ein neues Kerberos-Hauptelement

Im Anschluss an dieses Verfahren wird ein Beispiel des Befehlszeilenäquivalents gezeigt.

1 Starten Sie bei Bedarf das SEAM-Tool.

Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

Hinweis – Wenn Sie ein neues Hauptelement erstellen, das gegebenenfalls eine neue Richtlinie benötigt, sollten Sie die neue Richtlinie vor dem neuen Hauptelement erstellen. Weitere Informationen finden Sie unter „So erstellen Sie eine neue Kerberos-Richtlinie“ auf Seite 551.

```
$ /usr/sbin/gkadmin
```

2 Klicken Sie auf die Registerkarte "Principals" (Hauptelemente).

3 Klicken Sie auf "New" (Neu).

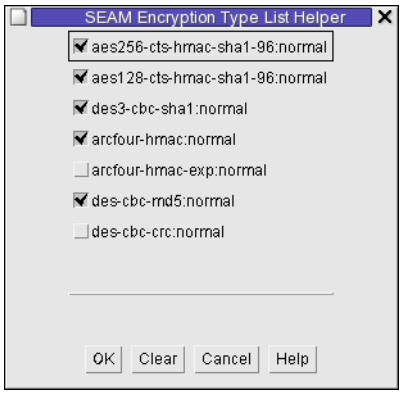
Der Fensterbereich "Principal Basics" (Grundeinstellungen für Hauptelement) mit einigen Attributen für ein Hauptelement wird angezeigt.

4 Geben Sie einen Hauptelementnamen und ein Passwort an.

Die Angabe des Hauptelementnamens und des Passworts ist obligatorisch.

5 **Geben Sie die Verschlüsselungstypen für das Hauptelement an.**

Klicken Sie auf das Kontrollkästchen rechts neben dem Feld der Verschlüsselungsschlüsseltypen, um ein neues Fenster mit allen verfügbaren Verschlüsselungsschlüsseltypen zu öffnen. Klicken Sie nach Auswahl der erforderlichen Verschlüsselungstypen auf "OK".



6 **Geben Sie die Richtlinie für das Hauptelement an.**

7 **Geben Sie Werte für die Attribute des Hauptelements an. Klicken Sie anschließend auf "Next" (Weiter), um weitere Attribute anzugeben.**

Es sind drei Fenster mit Attributinformationen vorhanden. Wählen Sie im Menü "Help" (Hilfe) die Option "Context-Sensitive Help" (Kontextbezogene Hilfe), um Informationen zu den verschiedenen Attributen in jedem Fenster abzurufen. Beschreibungen zu allen Attributen des Hauptelements finden Sie unter „Beschreibungen der SEAM-Tool-Fensterbereiche“ auf Seite 555.

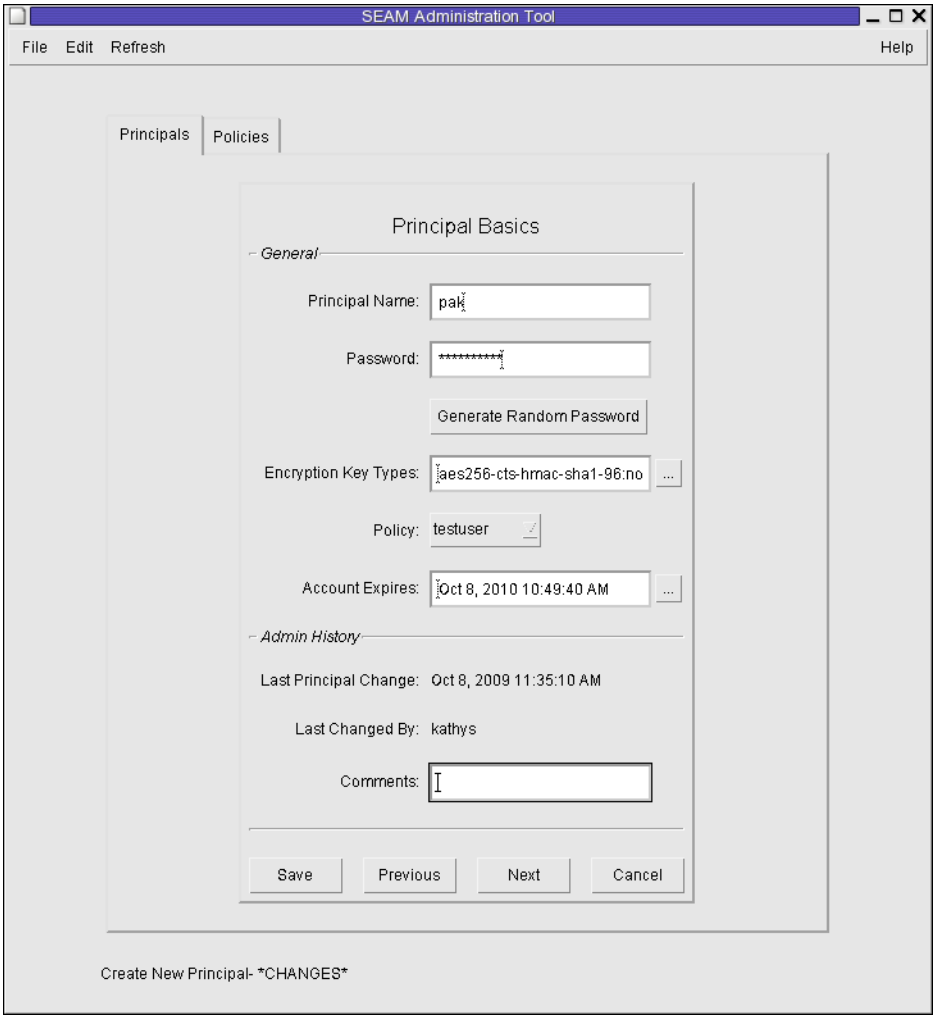
8 **Klicken Sie auf "Save" (Speichern), um das Hauptelement zu speichern, oder im letzten Fensterbereich auf "Done" (Fertig).**

9 **Richten Sie bei Bedarf Kerberos-Administratorberechtigungen für das neue Hauptelement in der Datei `/etc/krb5/kadm5.acl` ein.**

Weitere Informationen finden Sie unter „So ändern Sie die Kerberos-Administratorberechtigungen“ auf Seite 544.

Beispiel 25–4 Erstellen eines neuen Kerberos-Hauptelements

Das folgende Beispiel zeigt den Fensterbereich für die Grundeinstellungen des Hauptelements bei der Erstellung eines neuen Hauptelements namens `pak`. Für die Richtlinie ist `testuser` festgelegt.



Beispiel 25–5 Erstellen eines neuen Kerberos-Hauptelements (Befehlszeile)

Im folgenden Beispiel wird mit dem Befehl `add_principal` von `kadmin` ein neues Hauptelement namens `pak` erstellt. Für die Richtlinie des Hauptelements ist `testuser` festgelegt.

```
kadmin: add_principal -policy testuser pak
Enter password for principal "pak@EXAMPLE.COM": <Type the password>
Re-enter password for principal "pak@EXAMPLE.COM": <Type the password again>
Principal "pak@EXAMPLE.COM" created.
kadmin: quit
```

▼ So duplizieren Sie ein Kerberos-Hauptelement

Dieses Verfahren erläutert, wie mithilfe einiger oder aller Attribute eines vorhandenen Hauptelements ein neues Hauptelement erstellt wird. Für dieses Verfahren ist kein Befehlszeilenäquivalent vorhanden.

1. **Starten Sie bei Bedarf das SEAM-Tool.**

   Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Klicken Sie auf die Registerkarte "Principals" (Hauptelemente).**

3. **Wählen Sie das zu duplizierende Hauptelement in der Liste und klicken Sie auf "Duplicate" (Duplizieren).**

   Der Fensterbereich "Principal Basics" (Grundeinstellungen für Hauptelement) wird angezeigt. Alle Attribute des ausgewählten Hauptelements werden dupliziert, außer den leeren Felder für Hauptelementname und Passwort.

4. **Geben Sie einen Hauptelementnamen und ein Passwort an.**

   Die Angabe des Hauptelementnamens und des Passworts ist obligatorisch. Um ein exaktes Duplikat des ausgewählten Hauptelements zu erstellen, klicken Sie auf "Save" (Speichern) und fahren Sie mit Schritt 7 fort.

5. **Geben Sie verschiedene Werte für die Attribute des Hauptelements an. Klicken Sie anschließend auf "Next" (Weiter), um weitere Attribute anzugeben.**

   Es sind drei Fenster mit Attributinformationen vorhanden. Wählen Sie im Menü "Help" (Hilfe) die Option "Context-Sensitive Help" (Kontextbezogene Hilfe), um Informationen zu den verschiedenen Attributen in jedem Fenster abzurufen. Beschreibungen zu allen Attributen des Hauptelements finden Sie unter „Beschreibungen der SEAM-Tool-Fensterbereiche“ auf Seite 555.

6. **Klicken Sie auf "Save" (Speichern), um das Hauptelement zu speichern, oder im letzten Fensterbereich auf "Done" (Fertig).**

7. **Richten Sie bei Bedarf Kerberos-Administratorberechtigungen für das Hauptelement in der Datei `/etc/krb5/kadm5.acl` ein.**

   Weitere Informationen finden Sie unter „So ändern Sie die Kerberos-Administratorberechtigungen“ auf Seite 544.

▼ So ändern Sie ein Kerberos-Hauptelement

Im Anschluss an dieses Verfahren wird ein Beispiel des Befehlszeilenäquivalents gezeigt.

1. **Starten Sie bei Bedarf das SEAM-Tool.**

   Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Klicken Sie auf die Registerkarte "Principals" (Hauptelemente).**

3. **Wählen Sie das zu ändernde Hauptelement in der Liste und klicken Sie auf "Modify" (Ändern).**

   Der Fensterbereich "Principal Basics" (Grundeinstellungen für Hauptelement) mit einigen Attributen für das Hauptelement wird angezeigt.

4. **Ändern Sie die Attribute des Hauptelements. Klicken Sie anschließend auf "Next" (Weiter), um weitere Attribute zu ändern.**

   Es sind drei Fenster mit Attributinformationen vorhanden. Wählen Sie im Menü "Help" (Hilfe) die Option "Context-Sensitive Help" (Kontextbezogene Hilfe), um Informationen zu den verschiedenen Attributen in jedem Fenster abzurufen. Beschreibungen zu allen Attributen des Hauptelements finden Sie unter „Beschreibungen der SEAM-Tool-Fensterbereiche“ auf Seite 555.

   Hinweis – Der Name eines Hauptelements kann nicht geändert werden. Zum Unbenennen eines Hauptelements müssen Sie das Hauptelement duplizieren, neu benennen, speichern und anschließend das alte Hauptelement löschen.

   ---

5. **Klicken Sie auf "Save" (Speichern), um das Hauptelement zu speichern, oder im letzten Fensterbereich auf "Done" (Fertig).**

6. **Ändern Sie die Kerberos-Administratorberechtigungen für das Hauptelement in der Datei `/etc/krb5/kadm5.acl`.**

   Weitere Informationen finden Sie unter „So ändern Sie die Kerberos-Administratorberechtigungen“ auf Seite 544.

Beispiel 25–6 Ändern des Passworts eines Kerberos-Hauptelements (Befehlszeile)

Im folgenden Beispiel wird mit dem Befehl `change_password` von `kadmin` das Passwort für das Hauptelement `jdb` geändert. Mit dem Befehl `change_password` können Sie das Passwort nicht in ein Passwort ändern, das sich bereits im Passwortverlauf des Hauptelements befindet.

```
kadmin: change_password jdb
Enter password for principal "jdb": <Type the new password>
Re-enter password for principal "jdb": <Type the password again>
```

```
Password for "jdb@EXAMPLE.COM" changed.
kadmin: quit
```

Zum Ändern weiterer Attribute eines Hauptelements müssen Sie den Befehl `modify_principal` von `kadmin` verwenden.

So löschen Sie ein Kerberos-Hauptelement

Im Anschluss an dieses Verfahren wird ein Beispiel des Befehlszeilenäquivalents gezeigt.

1. **Starten Sie bei Bedarf das SEAM-Tool.**

   Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Klicken Sie auf die Registerkarte "Principals" (Hauptelemente).**

3. **Wählen Sie das zu löschende Hauptelement in der Liste und klicken Sie auf "Delete" (Löschen).**

   Nach Bestätigung der Löschung wird das Hauptelement gelöscht.

4. **Entfernen Sie das Hauptelement aus der ACL-Datei (Access Control List, Zugriffssteuerungsliste) von Kerberos (`/etc/krb5/kadm5.acl`).**

   Weitere Informationen finden Sie unter „So ändern Sie die Kerberos-Administratorberechtigungen“ auf Seite 544.

Beispiel 25–7 Löschen eines Kerberos-Hauptelements (Befehlszeile)

Im folgenden Beispiel wird mit dem Befehl `delete_principal` von `kadmin` das Hauptelement `jdb` gelöscht.

```
kadmin: delete_principal pak
Are you sure you want to delete the principal "pak@EXAMPLE.COM"? (yes/no): yes
Principal "pak@EXAMPLE.COM" deleted.
Make sure that you have removed this principal from all ACLs before reusing.
kadmin: quit
```

So richten Sie Standardwerte zur Erstellung neuer Kerberos-Hauptelemente ein

Für dieses Verfahren ist kein Befehlszeilenäquivalent vorhanden.

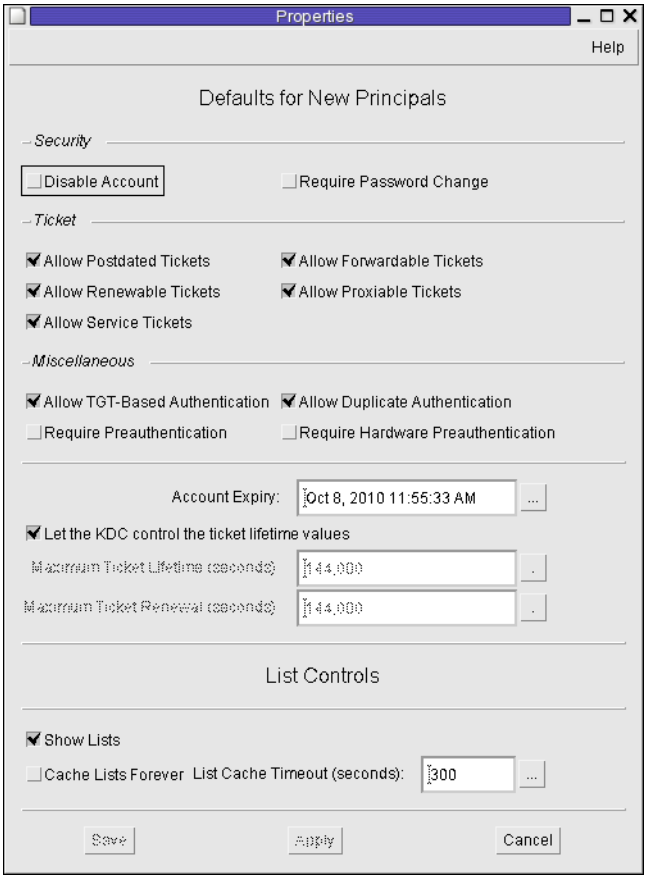
1. **Starten Sie bei Bedarf das SEAM-Tool.**

   Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

   ```
   $ /usr/sbin/gkadmin
   ```

2 **Wählen Sie im Menü "Edit" (Bearbeiten) die Option "Properties" (Eigenschaften).**

Das Fenster "Properties" (Eigenschaften) wird angezeigt.



3 **Wählen Sie die zur Erstellung neuer Hauptelemente zu verwendenden Standardwerte.**

Wählen Sie im Menü "Hilfe" die Option "Kontextbezogene Hilfe", um Informationen zu den verschiedenen Attributen in jedem Fenster abzurufen.

4 **Klicken Sie auf "Speichern".**

▼ So ändern Sie die Kerberos-Administratorberechtigungen

Auch wenn Ihre Site vermutlich viele Benutzer-Hauptelemente aufweist, möchten Sie üblicherweise nur einigen Benutzern ermöglichen, die Kerberos-Datenbank zu verwalten. Die

Berechtigungen für die Verwaltung der Kerberos-Datenbank werden in der ACL-Datei (`.kadm5.acl`) von Kerberos bestimmt. Mithilfe der Datei `kadm5.acl` können Sie Berechtigungen für einzelne Hauptelemente erteilen oder zurücknehmen. Alternativ können Sie mit dem Platzhalter '*' im Hauptelementnamen Berechtigungen für Gruppen von Hauptelementen festlegen.

1 Melden Sie sich als Superuser beim Master-KDC an.

2 Bearbeiten Sie die Datei `/etc/krb5/kadm5.acl`.

Einträge in der Datei `kadm5.acl` müssen folgendes Format aufweisen:

principal privileges [*principal-target*]

principal — Gibt das Hauptelement an, für das die Berechtigungen erteilt werden. Der Platzhalter '*' kann in jedem Teil des Hauptelementnamens enthalten sein. Dies ist bei der Erteilung derselben Berechtigungen für eine Gruppe von Hauptelementen hilfreich. Beispiel: Um alle Hauptelemente mit der Instanz `admin` anzugeben, verwenden Sie `*/admin@`*Bereich*.

Die Instanz `admin` wird häufig verwendet, um separate Berechtigungen (wie beispielsweise Administratorzugriff auf die Kerberos-Datenbank) für ein separates Kerberos-Hauptelement zu erteilen. Beispiel: Der Benutzer `jdb` verfügt möglicherweise über ein Hauptelement namens `jdb/admin` für die administrative Nutzung. In diesem Fall erhält der Benutzer `jdb` nur dann Tickets für `jdb/admin`, wenn er diese Berechtigungen auch tatsächlich verwenden muss.

privileges — Gibt an, welche Vorgänge vom Hauptelement ausgeführt werden können und welche nicht. Dieses Feld besteht aus einer Zeichenfolge aus mindestens einem Zeichen der folgenden Liste oder den jeweiligen Zeichen in Großbuchstaben. Ist das Zeichen ein Großbuchstabe (oder nicht angegeben), wurde der Vorgang abgelehnt. Ist das Zeichen ein Kleinbuchstabe, wurde der Vorgang zugelassen.

`a`	Erlaubt das Hinzufügen von Hauptelementen oder Richtlinien [nicht].
`d`	Erlaubt das Löschen von Hauptelementen oder Richtlinien [nicht].
`m`	Erlaubt das Ändern von Hauptelementen oder Richtlinien [nicht].
`c`	Erlaubt das Ändern von Passwörtern für Hauptelemente [nicht].
`i`	Erlaubt Abfragen in der Kerberos-Datenbank [nicht].
`l`	Erlaubt das Auflisten von Hauptelementen oder Richtlinien in der Kerberos-Datenbank [nicht].
`x` oder `*`	Gewährt alle Berechtigungen (`admcil`).

principal-target — Wenn in diesem Feld ein Hauptelement angegeben ist, werden die *privileges* nur dann dem *principal* zugewiesen, wenn *principal* auf dem *principal-target* aktiv ist. Der Platzhalter '*' kann in jedem Teil des Hauptelementnamens enthalten sein. Dies ist hilfreich für die Gruppierung von Hauptelementen.

Beispiel 25–8 Ändern der Kerberos-Administratorberechtigungen

Mit folgendem Eintrag in der Datei `kadm5.acl` werden jedem Hauptelement im Bereich `EXAMPLE.COM` mit der Instanz `admin` alle Berechtigungen für die Kerberos-Datenbank erteilt:

```
*/admin@EXAMPLE.COM *
```

Mit folgendem Eintrag in der Datei `kadm5.acl` werden dem Hauptelement `jdb@EXAMPLE.COM` die Berechtigungen zum Hinzufügen und Auflisten sowie für Abfragen zu jedem Hauptelement mit der Instanz `root` erteilt.

```
jdb@EXAMPLE.COM ali */root@EXAMPLE.COM
```

Verwalten von Kerberos-Richtlinien

Dieser Abschnitt enthält schrittweise Anleitungen zur Verwaltung von Richtlinien mit dem SEAM-Tool. Außerdem werden Beispiele für Befehlszeitenäquivalente aufgeführt (sofern vorhanden).

Verwalten von Kerberos-Richtlinien (Übersicht der Schritte)

Aufgabe	Beschreibung	Anweisungen
Anzeigen der Liste der Richtlinien	Zeigen Sie die Liste der Richtlinien durch Klicken auf die Registerkarte "Policies" (Richtlinien) an.	„So zeigen Sie die Liste der Kerberos-Richtlinien an“ auf Seite 547
Anzeigen der Attribute einer Richtlinie	Zeigen Sie die Attribute einer Richtlinie durch Auswählen der Richtlinie in der Richtlinienliste und anschließendes Klicken auf die Schaltfläche "Modify" (Ändern) an.	„So zeigen Sie die Attribute einer Kerberos-Richtlinie an“ auf Seite 549
Erstellen einer neuen Richtlinie	Erstellen Sie eine neue Richtlinie durch Klicken auf die Schaltfläche "Create New" (Neu erstellen) des Fensterbereichs "Policy List" (Liste der Richtlinien).	„So erstellen Sie eine neue Kerberos-Richtlinie“ auf Seite 551
Duplizieren einer Richtlinie	Duplizieren Sie eine Richtlinie durch Auswählen der zu duplizierenden Richtlinie in der Richtlinienliste und anschließendes Klicken auf die Schaltfläche "Duplicate" (Duplizieren).	„So duplizieren Sie eine Kerberos-Richtlinie“ auf Seite 553

Aufgabe	Beschreibung	Anweisungen
Ändern einer Richtlinie	Ändern Sie eine Richtlinie durch Auswählen der zu ändernden Richtlinie in der Richtlinienliste und anschließendes Klicken auf die Schaltfläche "Modify" (Ändern). Beachten Sie, dass Sie den Namen einer Richtlinie nicht ändern können. Zum Unbenennen einer Richtlinie müssen Sie die Richtlinie duplizieren, neu benennen, speichern und anschließend die alte Richtlinie löschen.	„So ändern Sie eine Kerberos-Richtlinie“ auf Seite 553
Löschen einer Richtlinie	Löschen Sie eine Richtlinie durch Auswählen der Richtlinie in der Richtlinienliste und anschließendes Klicken auf die Schaltfläche "Delete" (Löschen).	„So löschen Sie eine Kerberos-Richtlinie“ auf Seite 554

▼ So zeigen Sie die Liste der Kerberos-Richtlinien an

Im Anschluss an dieses Verfahren wird ein Beispiel des Befehlszeilenäquivalents gezeigt.

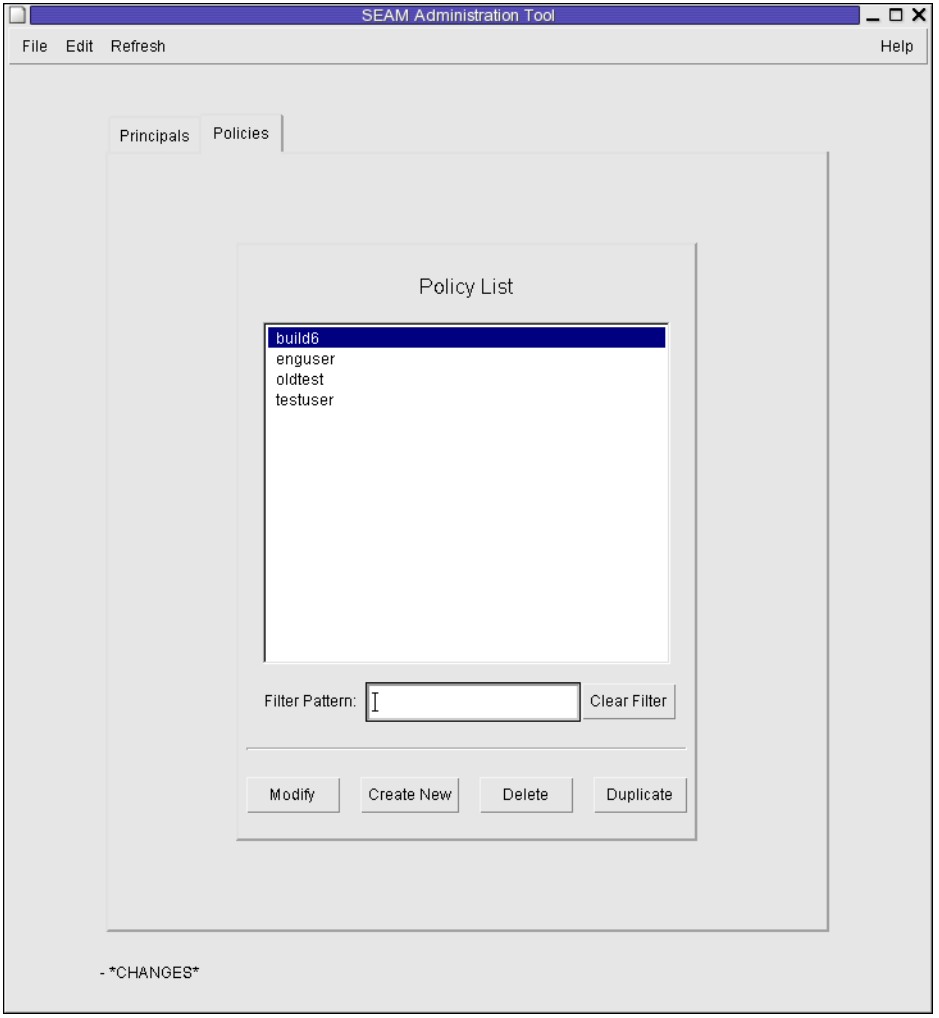
1 **Starten Sie bei Bedarf das SEAM-Tool.**

Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

```
$ /usr/sbin/gkadmin
```

2 **Klicken Sie auf die Registerkarte "Policies" (Richtlinien).**

Die Liste der Richtlinien wird angezeigt.



3 **Zeigen Sie eine bestimmte Richtlinie oder eine Teilliste von Richtlinien an.**

Geben Sie in das Feld "Filter" eine Filterzeichenfolge ein und drücken Sie die Eingabetaste. Bei erfolgreicher Anwendung des Filters wird die Liste der Richtlinien angezeigt, die diesem Filter entsprechen.

Die Filterzeichenfolge muss mindestens ein Zeichen umfassen. Da beim Filtermechanismus zwischen Groß- und Kleinschreibung unterschieden wird, müssen Sie die entsprechenden

Groß- und Kleinbuchstaben für den Filter verwenden. Beispiel: Wenn Sie die Filterzeichenfolge ge eingeben, zeigt der Filtermechanismus nur die Richtlinien an, die die Zeichenfolge ge enthalten (zum Beispiel george oder edge).

Zum Anzeigen der gesamten Liste der Richtlinien klicken Sie auf "Clear Filter" (Filter löschen).

Beispiel 25–9 Anzeigen der Liste der Kerberos-Richtlinien (Befehlszeile)

Im folgenden Beispiel werden mit dem Befehl `list_policies` von `kadmin` alle Richtlinien aufgelistet, die `*user*` entsprechen. In Verbindung mit dem Befehl `list_policies` können auch Platzhalter verwendet werden.

```
kadmin: list_policies *user*
testuser
enguser
kadmin: quit
```

▼ So zeigen Sie die Attribute einer Kerberos-Richtlinie an

Im Anschluss an dieses Verfahren wird ein Beispiel des Befehlszeilenäquivalents gezeigt.

1. **Starten Sie bei Bedarf das SEAM-Tool.**

   Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Klicken Sie auf die Registerkarte "Policies" (Richtlinien).**

3. **Wählen Sie die anzuzeigende Richtlinie in der Liste und klicken Sie auf "Modify" (Ändern).**

   Der Fensterbereich "Policy Details" (Details für Richtlinien) wird angezeigt.

4. **Wenn Sie mit der Anzeige fertig sind, klicken Sie auf "Cancel" (Abbrechen).**

Beispiel 25–10 Anzeigen der Attribute einer Kerberos-Richtlinie

Im folgenden Beispiel sehen Sie den Fensterbereich "Policy Details" (Details für Richtlinien) bei Anzeige der Richtlinie `test`.

Beispiel 25–11 Anzeigen der Attribute einer Kerberos-Richtlinie (Befehlszeile)

Im folgenden Beispiel werden mit dem Befehl `get_policy` von `kadmin` die Attribute der Richtlinie `enguser` angezeigt.

```
kadmin: get_policy enguser
Policy: enguser
Maximum password life: 2592000
Minimum password life: 0
Minimum password length: 8
Minimum number of password character classes: 2
Number of old keys kept: 3
Reference count: 0
kadmin: quit
```

Der Referenzzählwert ist die Anzahl der Hauptelemente, die diese Richtlinie verwenden.

▼ So erstellen Sie eine neue Kerberos-Richtlinie

Im Anschluss an dieses Verfahren wird ein Beispiel des Befehlszeilenäquivalents gezeigt.

1. **Starten Sie bei Bedarf das SEAM-Tool.**

   Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Klicken Sie auf die Registerkarte "Policies" (Richtlinien).**

3. **Klicken Sie auf "New" (Neu).**

   Der Fensterbereich "Policy Details" (Details für Richtlinien) wird angezeigt.

4. **Geben Sie im Feld "Policy Name" (Richtlinienname) einen Namen für die Richtlinie an.**

   Die Angabe des Richtliniennamens ist obligatorisch.

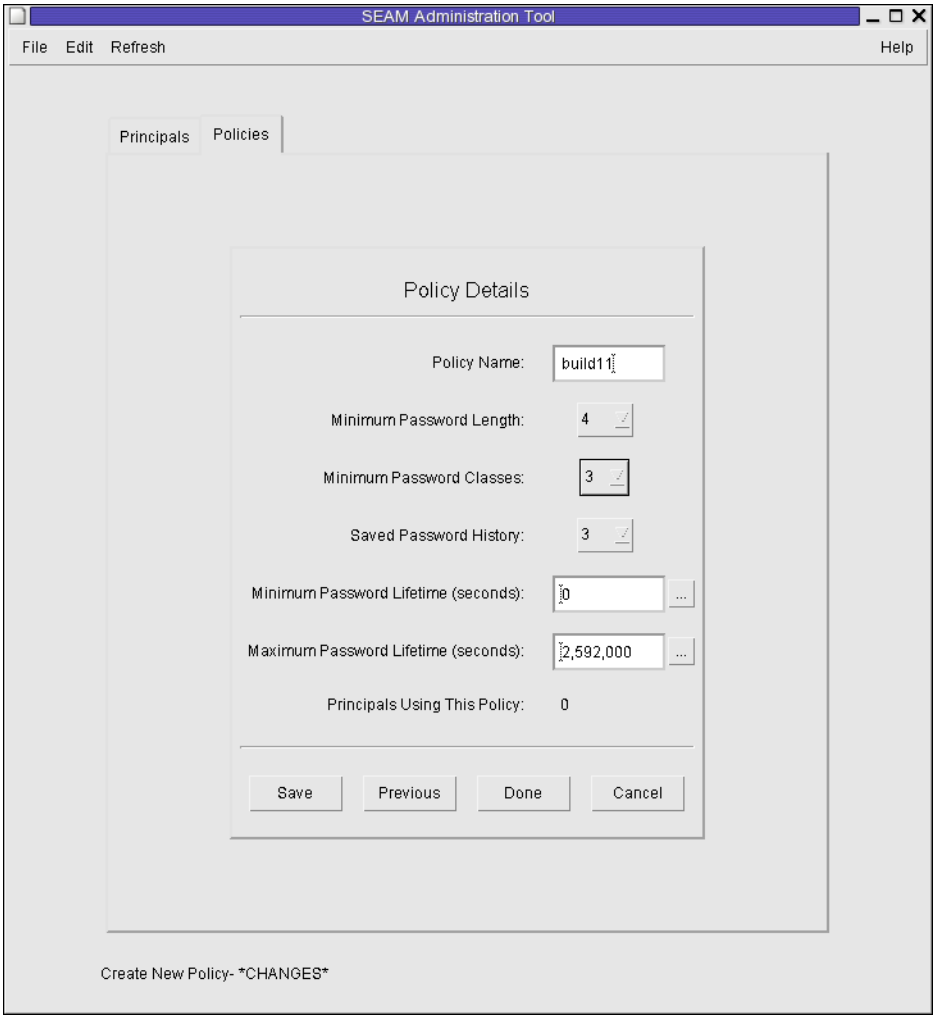
5. **Geben Sie Werte für die Attribute der Richtlinie an.**

   Wählen Sie im Menü "Help" (Hilfe) die Option "Context-Sensitive Help" (Kontextbezogene Hilfe), um Informationen zu den verschiedenen Attributen in diesem Fenster abzurufen. Sämtliche Beschreibungen der Richtlinienattribute finden Sie auch unter Tabelle 25–5.

6. **Klicken Sie auf "Save" (Speichern), um die Richtlinie zu speichern, oder auf "Done" (Fertig).**

Beispiel 25–12 Erstellen einer neuen Kerberos-Richtlinie

Im folgenden Beispiel wird eine neue Richtlinie namens `build11` erstellt. Die Mindestanzahl der Passwortklassen ist auf 3 festgelegt.



Beispiel 25–13 Erstellen einer neuen Kerberos-Richtlinie (Befehlszeile)

Im folgenden Beispiel wird mit dem Befehl `add_policy` von `kadmin` die Richtlinie `build11` erstellt. Diese Richtlinie erfordert mindestens drei Zeichenklassen in einem Passwort.

```
$ kadmin
kadmin: add_policy -minclasses 3 build11
kadmin: quit
```

So duplizieren Sie eine Kerberos-Richtlinie

Dieses Verfahren erläutert, wie mithilfe einiger oder aller Attribute einer vorhandenen Richtlinie eine neue Richtlinie erstellt wird. Für dieses Verfahren ist kein Befehlszeilenäquivalent vorhanden.

1. **Starten Sie bei Bedarf das SEAM-Tool.**

   Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Klicken Sie auf die Registerkarte "Policies" (Richtlinien).**

3. **Wählen Sie die zu duplizierende Richtlinie in der Liste und klicken Sie auf "Duplicate" (Duplizieren).**

   Der Fensterbereich "Policy Details" (Details für Richtlinien) wird angezeigt. Alle Attribute der ausgewählten Richtlinie werden dupliziert, außer dem leeren Feld "Policy Name" (Richtlinienname).

4. **Geben Sie im Feld "Policy Name" (Richtlinienname) einen Namen für die duplizierte Richtlinie an.**

   Die Angabe des Richtliniennamens ist obligatorisch. Um ein exaktes Duplikat der ausgewählten Richtlinie zu erstellen, fahren Sie mit Schritt 6 fort.

5. **Geben Sie verschiedene Werte für die Attribute der Richtlinie an.**

   Wählen Sie im Menü "Help" (Hilfe) die Option "Context-Sensitive Help" (Kontextbezogene Hilfe), um Informationen zu den verschiedenen Attributen in diesem Fenster abzurufen. Sämtliche Beschreibungen der Richtlinienattribute finden Sie auch unter Tabelle 25–5.

6. **Klicken Sie auf "Save" (Speichern), um die Richtlinie zu speichern, oder auf "Done" (Fertig).**

So ändern Sie eine Kerberos-Richtlinie

Im Anschluss an dieses Verfahren wird ein Beispiel des Befehlszeilenäquivalents gezeigt.

1. **Starten Sie bei Bedarf das SEAM-Tool.**

   Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Klicken Sie auf die Registerkarte "Policies" (Richtlinien).**

3. **Wählen Sie die zu ändernde Richtlinie in der Liste und klicken Sie auf "Modify" (Ändern).**

   Der Fensterbereich "Policy Details" (Details für Richtlinien) wird angezeigt.

4. **Ändern Sie die Attribute der Richtlinie.**

   Wählen Sie im Menü "Help" (Hilfe) die Option "Context-Sensitive Help" (Kontextbezogene Hilfe), um Informationen zu den verschiedenen Attributen in diesem Fenster abzurufen. Sämtliche Beschreibungen der Richtlinienattribute finden Sie auch unter Tabelle 25–5.

   Hinweis – Der Name einer Richtlinie kann nicht geändert werden. Zum Unbenennen einer Richtlinie müssen Sie die Richtlinie duplizieren, neu benennen, speichern und anschließend die alte Richtlinie löschen.

5. **Klicken Sie auf "Save" (Speichern), um die Richtlinie zu speichern, oder auf "Done" (Fertig).**

Beispiel 25–14 Ändern einer Kerberos-Richtlinie (Befehlszeile)

Im folgenden Beispiel wird mit dem Befehl `modify_policy` von `kadmin` die Mindestlänge eines Passworts für die Richtlinie `build11` auf fünf Zeichen geändert.

```
$ kadmin
kadmin: modify_policy -minlength 5 build11
kadmin: quit
```

▼ So löschen Sie eine Kerberos-Richtlinie

Im Anschluss an dieses Verfahren wird ein Beispiel des Befehlszeilenäquivalents gezeigt.

Hinweis – Vor dem Löschen einer Richtlinie müssen Sie die Richtlinie von allen Hauptelementen trennen, die sie aktuell verwenden. Dazu müssen Sie das Richtlinienattribut der Hauptelemente ändern. Die Richtlinie kann nicht gelöscht werden, wenn sie noch von einem Hauptelement verwendet wird.

1. **Starten Sie bei Bedarf das SEAM-Tool.**

   Weitere Informationen finden Sie unter „So starten Sie das SEAM-Tool“ auf Seite 531.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Klicken Sie auf die Registerkarte "Policies" (Richtlinien).**

3. **Wählen Sie die zu löschende Richtlinie in der Liste und klicken Sie auf "Delete" (Löschen).**

   Nach Bestätigung der Löschung wird die Richtlinie gelöscht.

Beispiel 25–15 Löschen einer Kerberos-Richtlinie (Befehlszeile)

Im folgenden Beispiel wird mit dem Befehl `delete_policy` des Befehls `kadmin` die Richtlinie `build11` gelöscht.

```
kadmin: delete_policy build11
Are you sure you want to delete the policy "build11"? (yes/no): yes
kadmin: quit
```

Vor dem Löschen einer Richtlinie müssen Sie die Richtlinie von allen Hauptelementen trennen, die sie aktuell verwenden. Dazu müssen Sie den Befehl `modify_principal -policy` von `kadmin` auf die betroffenen Hauptelemente anwenden. Der Befehl `delete_policy` schlägt fehl, wenn die Richtlinie von einem Hauptelement verwendet wird.

SEAM-Tool-Referenz

Dieser Abschnitt enthält Beschreibungen der einzelnen Fensterbereiche des SEAM-Tools. Ebenfalls sind Informationen zur Verwendung eingeschränkter Berechtigungen mit dem SEAM-Tool enthalten.

Beschreibungen der SEAM-Tool-Fensterbereiche

Dieser Abschnitt enthält Beschreibungen zu jedem Hauptelement- und Richtlinienattribut, das Sie im SEAM-Tool entweder angeben oder anzeigen können. Die Attribute sind nach dem Fensterbereich sortiert, in dem sie angezeigt werden.

TABELLE 25–2 Attribute des Fensterbereichs "Principal Basics" (Grundeinstellungen für Hauptelement) des SEAM-Tools

Attribut	Beschreibung
Principal Name (Hauptelementname)	Der Name des Hauptelements (*primary*/*instance*-Teil eines vollständig qualifizierten Hauptelementnamens). Ein Hauptelement stellt eine eindeutige Identität dar, der das KDC Tickets zuweisen kann. Beim Ändern eines Hauptelements können Sie dessen Namen nicht bearbeiten.
Password (Passwort)	Das Passwort für das Hauptelement. Mit der Schaltfläche "Generate Random Password" (Zufälliges Passwort erzeugen) können Sie ein Zufallspasswort für das Hauptelement erstellen.
Policy (Richtlinie)	Ein Menü der für das Hauptelement verfügbarer Richtlinien.
Account Expires (Konto läuft ab)	Datum und Uhrzeit für den Ablauf des Kontos des Hauptelements. Ist das Konto abgelaufen, kann das Hauptelement kein TGT (Ticket-Granting Ticket, Ticket-gewährendes Ticket) mehr erhalten und sich nicht mehr anmelden.
Last Principal Change (Letzte Änderung des Hauptelements)	Das Datum, an dem zuletzt Informationen für das Hauptelement geändert wurden. (Nur Lesen)
Last Changed By (Zuletzt geändert von)	Der Name des Hauptelements, das zuletzt das Konto für dieses Hauptelement geändert hat. (Nur Lesen)
Comments (Kommentare)	Auf das Hauptelement bezogene Kommentare (Beispiel: "Zeitweiliges Konto").

TABELLE 25–3 Attribute des Fensterbereichs "Principal Details" (Details für Hauptelement) des SEAM-Tools

Attribut	Beschreibung
Last Success (Letzter Erfolg)	Datum und Uhrzeit der letzten erfolgreichen Anmeldung des Hauptelements. (Nur Lesen)
Last Failure (Letzter Fehler)	Datum und Uhrzeit des letzten Anmeldefehlers des Hauptelements. (Nur Lesen)
Failure Count (Fehlerzähler)	Die Häufigkeit der Anmeldefehler für das Hauptelement. (Nur Lesen)
Last Password Change (Letzte Änderung des Passworts)	Datum und Uhrzeit der letzten Änderung des Passworts des Hauptelements. (Nur Lesen)
Password Expires (Zeitpunkt des Ablaufens des Passworts)	Datum und Uhrzeit des aktuellen Passworts des Hauptelements.
Key Version (Schlüsselversion)	Die Schlüsselversionsnummer für das Hauptelement. Dieses Attribut wird normalerweise nur dann geändert, wenn das Passwort nicht mehr geheim ist.
Maximum Lifetime (seconds) (Maximale Lebensdauer (Sekunden))	Die maximale Zeit, die für ein Ticket eines Hauptelements gewährt werden kann (ohne Erneuerung).
Maximum Renewal (seconds) (Maximale Erneuerung (Sekunden))	Die maximale Zeit, in der ein vorhandenes Ticket für ein Hauptelement erneuert werden kann.

TABELLE 25–4 Attribute des Fensterbereichs "Principal Flags" (Flags für Hauptelement) des SEAM-Tools

Attribut (Optionsfelder)	Beschreibung
Disable Account (Konto deaktivieren)	Verhindert die Anmeldung des Hauptelements, sofern ausgewählt. Dieses Attribut bietet eine einfache Möglichkeit zum vorübergehenden Sperren eines Hauptelementkontos.
Require Password Change (Änderung des Passworts anfordern)	Wenn ausgewählt, läuft das aktuelle Passwort des Hauptelements ab, sodass der Benutzer mit dem Befehl `kpasswd` ein neues Passwort erstellen muss. Dieses Attribut ist hilfreich, wenn eine Sicherheitsverletzung auftritt und Sie alte Passwörter ersetzen müssen.
Allow Postdated Tickets (Nachdatierte Tickets zulassen)	Wenn ausgewählt, kann das Hauptelement nachdatierte Tickets erhalten. Beispiel: Sie müssen möglicherweise nachdatierte Tickets für `cron` -Jobs verwenden, die nach Feierabend ausgeführt werden müssen, aber Sie können aufgrund der kurzen Lebensdauer des Tickets keine Tickets im Voraus erhalten.
Allow Forwardable Tickets (Weiterleitbare Tickets zulassen)	Wenn ausgewählt, kann das Hauptelement weiterleitbare Tickets erhalten. Hierbei handelt es sich um Tickets, die an den Remote-Host weitergeleitet werden, um eine Single Sign-On-Sitzung bereitzustellen. Beispiel: Wenn Sie weiterleitbare Tickets verwenden und sich über `ftp` oder `rsh` authentifizieren, stehen andere Services wie z. B. NFS-Service zur Verfügung, ohne dass Sie ein anderes Passwort angeben müssen.

TABELLE 25–4 Attribute des Fensterbereichs "Principal Flags" (Flags für Hauptelement) des SEAM-Tools *(Fortsetzung)*

Attribut (Optionsfelder)	Beschreibung
Allow Renewable Tickets (Erneuerbare Tickets zulassen)	Wenn ausgewählt, kann das Hauptelement erneuerbare Tickets erhalten. Ein Hauptelement kann das Ablaufdatum oder die Ablaufzeit eines erneuerbaren Tickets automatisch verlängern. In diesem Fall muss nach Ablauf des ersten Tickets kein neues Ticket abgerufen werden. Derzeit ist der NFS-Service der einzige Service, der Tickets erneuern kann.
Allow Proxiable Tickets (Proxy-fähige Tickets zulassen)	Wenn ausgewählt, kann das Hauptelement Proxy-fähige Tickets erhalten. Ein Proxy-fähiges Ticket ist ein Ticket, das im Auftrag eines Clients von einem Service verwendet werden kann, um einen Vorgang für den Client auszuführen. Mit einem Proxy-fähigen Ticket kann ein Service die Identität eines Clients annehmen und ein Ticket für einen anderen Service erhalten. Der Service kann jedoch kein Ticket-gewährendes Ticket (TGT) erhalten.
Allow Service Tickets (Service-Tickets zulassen)	Wenn ausgewählt, können Service-Tickets für das Hauptelement ausgestellt werden. Service-Tickets sollten nicht für die Hauptelemente `kadmin/`*hostname* und `changepw/` *hostname* ausgestellt werden. Dadurch wird sichergestellt, dass diese Hauptelemente nur die KDC-Datenbank aktualisieren können.
Allow TGT-Based Authentication (TGT-basierte Authentifizierung zulassen)	Wenn ausgewählt, kann das Service-Hauptelement einem anderen Hauptelement Services bereitstellen. Genauer gesagt ermöglicht dieses Attribut dem KDC, ein Service-Ticket für das Service-Hauptelement auszustellen. Dieses Attribut ist nur für Service-Hauptelemente gültig. Ist es nicht ausgewählt, können keine Service-Tickets für das Service-Hauptelement ausgestellt werden.
Allow Duplicate Authentication (Doppelte Authentifizierung zulassen)	Wenn ausgewählt, kann das Benutzer-Hauptelement Service-Tickets für andere Benutzer-Hauptelemente erhalten. Dieses Attribut ist nur für Benutzer-Hauptelemente gültig. Ist es nicht ausgewählt, kann das Benutzer-Hauptelement auch weiterhin Service-Tickets für Service-Hauptelemente, nicht aber für andere Benutzer-Hauptelemente erhalten.
Required Preauthentication (Erforderliche vorgezogene Berechtigungsprüfung)	Wenn ausgewählt, sendet das KDC kein angefordertes Ticket-gewährendes Ticket (TGT) an das Hauptelement, bevor es nicht (mittels Software) bestätigen konnte, dass es sich wirklich um das Hauptelement handelt, das das TGT anfordert. Diese vorgezogene Berechtigungsprüfung erfolgt üblicherweise über ein zusätzliches Passwort, beispielsweise von einer DES-Karte. Ist das Attribut nicht ausgewählt, muss das KDC keine vorgezogene Berechtigungsprüfung für das Hauptelement durchführen, bevor es ein angefordertes TGT an das Hauptelement sendet.
Required Hardware Authentication (Erforderliche Hardware-Authentifizierung)	Wenn ausgewählt, sendet das KDC kein angefordertes Ticket-gewährendes Ticket (TGT) an das Hauptelement, bevor es nicht (mittels Hardware) bestätigen konnte, dass es sich wirklich um das Hauptelement handelt, das das TGT anfordert. Die vorgezogene Berechtigungsprüfung über Hardware kann beispielsweise auf einem Java-Ringleser erfolgen. Ist das Attribut nicht ausgewählt, muss das KDC keine vorgezogene Berechtigungsprüfung für das Hauptelement durchführen, bevor es ein angefordertes TGT an das Hauptelement sendet.

TABELLE 25–5 Attribute des Fensterbereichs "Policy Basics" (Grundeinstellungen für Richtlinie) des SEAM-Tools

Attribut	Beschreibung
Policy Name (Richtlinienname)	Der Name der Richtlinie. Eine Richtlinie stellt eine Reihe von Regeln dar, die das Passwort und die Tickets eines Hauptelements betreffen. Beim Ändern einer Richtlinie können Sie deren Namen nicht bearbeiten.
Minimum Password Length (Mindestlänge für Passwort)	Die minimale Länge des Passworts eines Hauptelements.
Minimum Password Classes (Mindestklassen für Passwort)	Die Mindestanzahl verschiedener Zeichentypen, die im Passwort eines Hauptelements erforderlich sind. Beispiel: Ein Wert für die Mindestanzahl der Klassen von 2 bedeutet, dass ein Passwort mindestens zwei verschiedene Zeichentypen aufweisen muss, wie etwa Buchstaben und Zahlen (hi2mom). Ein Wert von 3 bedeutet, dass ein Passwort mindestens drei verschiedene Zeichentypen aufweisen muss, wie beispielsweise Buchstaben, Zahlen und Satzzeichen (hi2mom!). Und so weiter. Bei einem Wert von 1 ist die Anzahl der Zeichentypen für das Passwort unbegrenzt.
Saved Password History (Verlauf für gespeicherte Passwörter)	Die Anzahl der früher vom Hauptelement verwendeten Passwörter, die nicht wiederverwendet werden können.
Minimum Password Lifetime (seconds) (Minimale Lebensdauer für Passwörter (Sekunden))	Die Mindestzeit, die ein Passwort verwendet werden muss, bevor es geändert werden kann.
Maximum Password Lifetime (seconds) (Maximale Lebensdauer für Passwörter (Sekunden))	Die Höchstzeit, die ein Passwort verwendet werden kann, bevor es geändert werden muss.
Principals Using This Policy (Hauptelemente, die diese Richtlinie verwenden)	Die Anzahl der Hauptelemente, für die diese Richtlinie derzeit gültig ist. (Nur Lesen)

Verwenden des SEAM-Tools mit eingeschränkten Kerberos-Administratorberechtigungen

Alle Funktionen des SEAM-Tools sind verfügbar, wenn das `admin`-Hauptelement über alle Berechtigungen für die Verwaltung der Kerberos-Datenbank verfügt. Es ist jedoch möglich, nur über eingeschränkte Berechtigungen zu verfügen, um beispielsweise nur berechtigt zu sein, die Anzeige der Liste der Hauptelemente anzuzeigen oder das Passwort eines Hauptelements zu ändern. Das SEAM-Tool können Sie trotz eingeschränkter Kerberos-Admininistratorberechtigungen verwenden. Einige Komponenten des SEAM-Tools ändern sich jedoch in Abhängigkeit davon, über welche Kerberos-Administratorberechtigungen Sie nicht verfügen. Tabelle 25–6 zeigt, wie sich das SEAM-Tool in Abhängigkeit von Ihren Kerberos-Administratorberechtigungen ändert.

Die offensichtlichste Änderung des SEAM-Tools erfolgt, wenn Sie nicht über die Berechtigung zum Anzeigen von Listen verfügen. Ohne die Berechtigung zum Anzeigen von Listen werden in den Listenbereichen keine Listen mit den zu bearbeitenden Hauptelementen und Richtlinien angezeigt. Stattdessen müssen Sie im Feld "Name" der Listenbereiche ein Hauptelement oder eine Richtlinie angeben, das bzw. die Sie bearbeiten möchten.

Wenn Sie sich ohne ausreichende Berechtigungen zum Ausführen von Ausgaben beim SEAM-Tool anmelden, wird die folgende Meldung angezeigt und Sie werden zurück zum Anmeldefenster für die SEAM-Administration geführt:

```
Insufficient privileges to use gkadmin: ADMCIL. Please try using another principal.
```

Informationen zum Ändern der Berechtigungen für ein Hauptelement zur Verwaltung der Kerberos-Datenbank finden Sie unter „So ändern Sie die Kerberos-Administratorberechtigungen“ auf Seite 544.

TABELLE 25–6 Verwenden des SEAM-Tools mit eingeschränkten Kerberos-Administratorberechtigungen

Fehlende Berechtigung	Änderung am SEAM-Tool
`a` (hinzufügen)	Die Schaltflächen "Create New" (Neu erstellen) und "Duplicate" (Duplizieren) sind in den Listenbereichen für Hauptelemente und Richtlinien nicht verfügbar. Ohne die Berechtigung zum Hinzufügen können Sie keine neuen Hauptelemente oder Richtlinien erstellen oder duplizieren.
`d` (löschen)	Die Schaltfläche "Delete" (Löschen) ist in den Listenbereichen für Hauptelemente und Richtlinien nicht verfügbar. Ohne die Berechtigung zum Löschen können Sie keine Hauptelemente oder Richtlinien löschen.
`m` (ändern)	Die Schaltfläche "Modify" (Ändern) ist in den Listenbereichen für Hauptelemente und Richtlinien nicht verfügbar. Ohne die Berechtigung zum Ändern können Sie keine Hauptelemente oder Richtlinien ändern. Ebenso können Sie kein Passwort eines Hauptelements ändern, wenn die Schaltfläche "Modify" (Ändern) nicht verfügbar ist, auch wenn Sie über die Berechtigung zum Ändern von Passwörtern verfügen.
`c` (Passwort ändern)	Das Feld "Password" (Passwort) des Fensterbereichs "Principal Basics" (Grundeinstellungen für Hauptelement) ist schreibgeschützt und kann somit nicht geändert werden. Ohne die Berechtigung zum Ändern des Passworts können Sie keine Passwörter von Hauptelementen ändern. Selbst wenn Sie über die Berechtigung zum Ändern des Passworts verfügen, benötigen Sie ebenfalls die Berechtigung zum Ändern der Hauptelemente und Richtlinien, um das Passwort eines Hauptelements zu ändern.

TABELLE 25–6 Verwenden des SEAM-Tools mit eingeschränkten Kerberos-Administratorberechtigungen *(Fortsetzung)*

Fehlende Berechtigung	Änderung am SEAM-Tool
`i` (Datenbankabfrage)	Die Schaltflächen "Modify" (Ändern) und "Duplicate" (Duplizieren) sind in den Listenbereichen für Hauptelemente und Richtlinien nicht verfügbar. Ohne die Berechtigung zum Senden von Abfragen können Sie keine Hauptelemente oder Richtlinien ändern oder duplizieren. Ebenso können Sie kein Passwort eines Hauptelements ändern, wenn die Schaltfläche "Modify" (Ändern) nicht verfügbar ist, auch wenn Sie über die Berechtigung zum Ändern von Passwörtern verfügen.
`l` (Liste)	Die Liste der Hauptelemente und Richtlinien ist in den Listenbereichen nicht verfügbar. Ohne die Berechtigung zum Anzeigen von Listen müssen Sie im Feld "Name" der Listenbereiche das Hauptelement oder die Richtlinie angeben, das bzw. die Sie bearbeiten möchten.

Verwalten von Schlüsseltabellendateien

Jeder Host, der einen Service bereitstellt, muss über eine lokale Datei verfügen, eine sogenannte *Schlüsseltabelle*. Die Schlüsseltabelle enthält das Hauptelement für den entsprechenden Service, einen *Serviceschlüssel*. Mit einem Serviceschlüssel authentifiziert sich ein Service beim KDC. Der Serviceschlüssel ist nur Kerberos und dem Service selbst bekannt. Beispiel: Wenn Sie einen kerberisierten NFS-Server haben, muss dieser Server eine Schlüsseltabellendatei aufweisen, die dessen Service-Hauptelement `nfs` enthält.

Zum Hinzufügen eines Serviceschlüssels zu einer Schlüsseltabellendatei fügen Sie mit dem Befehl `ktadd` von `kadmin` das entsprechende Service-Hauptelement zu einer Schlüsseltabellendatei eines Hosts hinzu. Da Sie ein Service-Hauptelement zu einer Schlüsseltabellendatei hinzufügen, muss das Hauptelement bereits in der Kerberos-Datenbank vorliegen, damit `kadmin` prüfen kann, ob es vorhanden ist. Auf dem Master-KDC befindet sich die Schlüsseltabellendatei standardmäßig unter `/etc/krb5/kadm5.keytab`. Auf Anwendungsservern, die kerberisierte Services bereitstellen, liegt die Schlüsseltabellendatei standardmäßig unter `/etc/krb5/krb5.keytab`.

Eine Schlüsseltabelle entspricht dem Passwort eines Benutzers. Der Schutz der Schüsseltabellendateien ist für Anwendungsserver ebenso wichtig wie für Benutzer der Schutz ihrer Passwörter. Sie sollten Schlüsseltabellendateien immer auf einer lokalen Festplatte speichern und sie nur für den `root`-Benutzer lesbar machen. Zudem sollten Sie eine Schlüsseltabellendatei nie über ein ungesichertes Netzwerk versenden.

Es ist außerdem eine spezielle Instanz vorhanden, in der ein `root`-Hauptelement zu der Schlüsseltabellendatei eines Hosts hinzugefügt wird. Wenn ein Benutzer auf dem Kerberos-Client kerberisierte NFS-Dateisysteme einhängen soll, für die root-äquivalenter Zugriff erforderlich ist, müssen Sie das `root`-Hauptelement des Clients zu der

Schlüsseltabellendatei des Clients hinzufügen. Andernfalls müssen Benutzer zum Einhängen eines kerberisierten NFS-Dateisystems mit `root`-Zugriff den Befehl `kinit` als `root` verwenden, um Berechtigungsnachweise für das `root`-Hauptelement des Clients zu erhalten, auch wenn sie den Automounter verwenden.

Hinweis – Wenn Sie ein Master-KDC einrichten, müssen Sie die Hauptelemente `kadmind` und `changepw` zu der Datei `kadm5.keytab` hinzufügen.

Ein weiterer Befehl zum Verwalten von Schlüsseltabellendateien ist `ktutil`. Mithilfe dieses interaktiven Befehls können Sie die Schlüsseltabellendatei eines lokalen Hosts ohne Kerberos-Administratorberechtigungen verwalten, da `ktutil` nicht wie `kadmin` mit der Kerberos-Datenbank kommuniziert. Somit können Sie nach dem Hinzufügen eines Hauptelements zu einer Schlüsseltabellendatei den Befehl `ktutil` verwenden, um die Schlüsselliste in einer Schlüsseltabellendatei anzuzeigen oder die Authentifizierung für einen Service vorübergehend zu deaktivieren.

Hinweis – Wenn Sie ein Hauptelement in einer Schlüsseltabellendatei mit dem Befehl `ktadd` in `kadmin` ändern, wir ein neuer Schlüssel generiert und der Schlüsseltabellendatei hinzugefügt.

Verwalten von Schlüsseltabellendateien (Übersicht der Schritte)

Aufgabe	Beschreibung	Anweisungen
Hinzufügen eines Service-Hauptelements zu einer Schlüsseltabellendatei	Fügen Sie ein Service-Hauptelement einer Schlüsseltabellendatei mit dem Befehl `ktadd` von `kadmin` zu.	„So fügen Sie ein Service-Hauptelement von Kerberos zu einer Schlüsseltabellendatei hinzu“ auf Seite 562
Entfernen eines Service-Hauptelements aus einer Schlüsseltabellendatei	Entfernen Sie ein Service-Hauptelement aus einer Schlüsseltabellendatei mit dem Befehl `ktremove` von `kadmin`.	„So entfernen Sie ein Service-Hauptelement aus einer Schlüsseltabellendatei“ auf Seite 564
Anzeigen der Schlüsselliste (Liste der Hauptelemente) in einer Schlüsseltabellendatei	Zeigen Sie die Schlüsselliste in einer Schlüsseltabellendatei mit dem Befehl `ktutil` an.	„So zeigen Sie die Schlüsselliste (Hauptelemente) in einer Schlüsseltabellendatei an“ auf Seite 565

Aufgabe	Beschreibung	Anweisungen
Vorübergehendes Deaktivieren der Authentifizierung einen Service auf einem Host	Dieses Verfahren bietet eine schnelle Möglichkeit zum vorübergehenden Deaktivieren der Authentifizierung für einen Service auf einem Host, ohne dass `kadmin`-Berechtigungen erforderlich sind. Kopieren Sie die ursprüngliche Schlüsseltabellendatei an einen temporären Speicherort, bevor Sie das Service-Hauptelement mit `ktutil` aus der Schlüsseltabellendatei des Servers löschen. Wenn Sie den Service wieder aktivieren möchten, kopieren Sie die ursprüngliche Schlüsseltabellendatei zurück an den eigentlichen Speicherort.	„So deaktivieren Sie vorübergehend die Authentifizierung für einen Service auf einem Host“ auf Seite 565

▼ So fügen Sie ein Service-Hauptelement von Kerberos zu einer Schlüsseltabellendatei hinzu

1 Stellen Sie sicher, dass das Hauptelement bereits in der Kerberos-Datenbank vorhanden ist.

Weitere Informationen finden Sie unter „So zeigen Sie die Liste der Kerberos-Hauptelemente an“ auf Seite 534.

2 Melden Sie sich als Superuser bei dem Host an, zu dessen Schlüsseltabellendatei ein Hauptelement hinzugefügt werden muss.

3 Starten Sie den Befehl `kadmin`.

```
# /usr/sbin/kadmin
```

4 Fügen Sie mit dem Befehl `ktadd` ein Hauptelement zu einer Schlüsseltabellendatei hinzu.

`kadmin:` **`ktadd`** `[`**`-e`** *enctype*`] [`**`-k`** *keytab*`] [`**`-q`**`] [`*principal* | **`-glob`** *principal-exp*`]`

`-e` *enctype*	Überschreibt die Liste der in der Datei `krb5.conf` definierten Verschlüsselungstypen.
`-k` *keytab*	Gibt die Schlüsseltabellendatei an. Standardmäßig wird `/etc/krb5/krb5.keytab` verwendet.
`-q`	Zeigt weniger ausführliche Informationen an.
principal	Gibt das der Schlüsseltabellendatei hinzuzufügende Hauptelement an. Sie können folgende Service-Hauptelemente hinzufügen: `host`, `root`, `nfs` und `ftp`.
`-glob` *principal-exp*	Gibt die Hauptelement-Ausdrücke an. Alle Hauptelemente, die *principal-exp* entsprechen, werden der Schlüsseltabellendatei hinzugefügt. Für Hauptelement-Ausdrücke gelten dieselben Regeln

wie für den Befehl `list_principals` von `kadmin`.

5 Beenden Sie den Befehl `kadmin`.

```
kadmin: quit
```

Beispiel 25–16 Hinzufügen eines Service-Hauptelements zu einer Schlüsseltabellendatei

Im folgenden Beispiel werden die Hauptelemente `kadmin/kdc1.example.com` und `changepw/kdc1.example.com` zu der Schlüsseltabellendatei eines Master-KDC hinzugefügt. Für dieses Beispiel muss es sich bei der Schlüsseltabellendatei um die in der Datei `kdc.conf` angegebene Datei handeln.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc1.example.com changepw/kdc1.example.com
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-256 CTS
          mode with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-128 CTS
          mode with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: quit
```

Im folgenden Beispiel wird das Hauptelement `host` von `denver` der Schlüsseltabellendatei von `denver` hinzugefügt, damit das KDC die Netzwerkdienste von `denver` authentifizieren kann.

```
denver # /usr/sbin/kadmin
kadmin: ktadd host/denver.example.com
Entry for principal host/denver.example.com with kvno 3, encryption type AES-256 CTS
          mode with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type Triple DES cbc mode
          with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

▼ So entfernen Sie ein Service-Hauptelement aus einer Schlüsseltabellendatei

1. **Melden Sie sich als Superuser bei dem Host mit einem Service-Hauptelement an, das aus der dazugehörigen Schlüsseltabellendatei entfernt werden muss.**

2. **Starten Sie den Befehl `kadmin`.**

   ```
   # /usr/sbin/kadmin
   ```

3. **(Optional) Zum Anzeigen der aktuellen Liste der Hauptelemente (Schlüssel) in der Schlüsseltabellendatei verwenden Sie den Befehl `ktutil`.**

   Weitere Informationen finden Sie unter „So zeigen Sie die Schlüsselliste (Hauptelemente) in einer Schlüsseltabellendatei an“ auf Seite 565.

4. **Entfernen Sie mit dem Befehl `ktremove` ein Hauptelement aus der Schlüsseltabellendatei.**

   ```
   kadmin: ktremove [-k keytab] [-q] principal [kvno | all | old ]
   ```

`-k` *keytab*	Gibt die Schlüsseltabellendatei an. Standardmäßig wird `/etc/krb5/krb5.keytab` verwendet.
`-q`	Zeigt weniger ausführliche Informationen an.
principal	Gibt das aus der Schlüsseltabellendatei zu entfernende Hauptelement an.
kvno	Entfernt alle Einträge für das angegebene Hauptelement, dessen Schlüsselversionsnummer *kvno* entspricht.
`all`	Entfernt alle Einträge für das angegebene Hauptelement.
`old`	Entfernt alle Einträge für das angegebene Hauptelement, abgesehen von den Einträgen mit der höchsten Schlüsselversionsnummer.

5. **Beenden Sie den Befehl `kadmin`.**

   ```
   kadmin: quit
   ```

Beispiel 25–17 Entfernen eines Service-Hauptelements aus einer Schlüsseltabellendatei

Im folgenden Beispiel wird das Hauptelement `host` von `denver` aus der Schlüsseltabellendatei von `denver` entfernt.

```
denver # /usr/sbin/kadmin
kadmin: ktremove host/denver.example.com@EXAMPLE.COM
kadmin: Entry for principal host/denver.example.com@EXAMPLE.COM with kvno 3
  removed from keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

▼ So zeigen Sie die Schlüsselliste (Hauptelemente) in einer Schlüsseltabellendatei an

1 Melden Sie sich als Superuser bei dem Host mit der Schlüsseltabellendatei an.

Hinweis – Obwohl Sie Schlüsseltabellendateien erstellen können, die Eigentum anderer Benutzern sind, sind für die Verwendung des Standardspeicherorts der Schlüsseltabellendatei `root`-Eigentümerberechtigungen erforderlich.

---

2 Starten Sie den Befehl `ktutil`.

```
# /usr/bin/ktutil
```

3 Lesen Sie mit dem Befehl `read_kt` die Schlüsseltabellendatei in den Schlüssellistenpuffer ein.

```
ktutil: read_kt keytab
```

4 Zeigen Sie mit dem Befehl `list` den Schlüssellistenpuffer an.

```
ktutil: list
```

Der aktuelle Schlüssellistenpuffer wird angezeigt.

5 Beenden Sie den Befehl `ktutil`.

```
ktutil: quit
```

Beispiel 25–18 Anzeigen der Schlüsselliste (Hauptelemente) in einer Schlüssellistendatei

Im folgenden Beispiel wird die Schlüsselliste in der Datei `/etc/krb5/krb5.keytab` auf dem Host `denver` angezeigt.

```
denver # /usr/bin/ktutil
    ktutil: read_kt /etc/krb5/krb5.keytab
    ktutil: list
slot KVNO Principal
---- ---- ---------------------------------------
   1    5 host/denver@EXAMPLE.COM
    ktutil: quit
```

▼ So deaktivieren Sie vorübergehend die Authentifizierung für einen Service auf einem Host

Manchmal müssen Sie gegebenenfalls den Authentifizierungsmechanismus für einen Service, wie zum Beispiel `rlogin` oder `ftp` , auf einem Anwendungsserver im Netzwerk vorübergehend deaktivieren. Beispiel: Möglicherweise möchten Sie Benutzer daran hindern, sich bei einem

System anzumelden, während Sie Verwaltungsvorgänge durchführen Mithilfe des Befehls `ktutil` können Sie dies erreichen, indem Sie das Service-Hauptelement aus der Schlüsseltabellendatei des Servers entfernen, ohne dass dafür `kadmin`-Berechtigungen erforderlich sind. Zum erneuten Aktivieren der Authentifizierung müssen Sie nur die zuvor gespeicherte ursprüngliche Schlüsseltabellendatei zurück an den eigentlichen Speicherort kopieren.

Hinweis – Standardmäßig sind die meisten Services so eingerichtet, dass sie eine Authentifizierung erfordern. Wenn dies nicht der Fall ist, kann der Service auch dann noch ausgeführt werden, wenn Sie die Authentifizierung für diesen Service deaktivieren.

---

1 Melden Sie sich als Superuser bei dem Host mit der Schlüsseltabellendatei an.

Hinweis – Obwohl Sie Schlüsseltabellendateien erstellen können, die Eigentum anderer Benutzern sind, sind für die Verwendung des Standardspeicherorts der Schlüsseltabellendatei `root`-Eigentümerberechtigungen erforderlich.

---

2 Speichern Sie die aktuelle Schlüsseltabellendatei in einer temporären Datei.

3 Starten Sie den Befehl `ktutil`.

```
# /usr/bin/ktutil
```

4 Lesen Sie mit dem Befehl `read_kt` die Schlüsseltabellendatei in den Schlüssellistenpuffer ein.

```
ktutil: read_kt keytab
```

5 Zeigen Sie mit dem Befehl `list` den Schlüssellistenpuffer an.

```
ktutil: list
```

Der aktuelle Schlüssellistenpuffer wird angezeigt. Beachten Sie die Slot-Nummer für den zu deaktivierenden Service.

6 Zum vorübergehenden Deaktivieren des Service eines Hosts entfernen Sie mit dem Befehl `delete_entry` das spezifische Service-Hauptelement aus dem Schlüssellistenpuffer.

```
ktutil: delete_entry slot-number
```

slot-number gibt die Steckplatznummer des zu löschenden Service-Hauptelements an, das vom Befehl `list` angezeigt wird.

7 Schreiben Sie mit dem Befehl `write_kt` den Schlüssellistenpuffer in eine neue Schlüssellistendatei.

```
ktutil: write_kt new-keytab
```

8 Beenden Sie den Befehl `ktutil`.

```
ktutil: quit
```

9 Verschieben Sie die neue Schlüssellistendatei.

```
# mv new-keytab keytab
```

10 Wenn Sie den Service wieder aktivieren möchten, kopieren Sie die temporäre (ursprüngliche) Schlüsseltabellendatei zurück an den ursprünglichen Speicherort.

Beispiel 25–19 Vorübergehendes Deaktivieren eines Service auf einem Host

Im folgenden Beispiel wird der Service `host` auf dem Host `denver` vorübergehend deaktiviert. Zum erneuten Aktivieren des Hostservice auf `denver` kopieren Sie die Datei `krb5.keytab.temp` in die Datei `/etc/krb5/krb5.keytab` .

```
denver # cp /etc/krb5/krb5.keytab /etc/krb5/krb5.keytab.temp
denver # /usr/bin/ktutil
    ktutil:read_kt /etc/krb5/krb5.keytab
    ktutil:list
slot KVNO Principal
---- ---- ---------------------------------------
   1    8 root/denver@EXAMPLE.COM
   2    5 host/denver@EXAMPLE.COM
    ktutil:delete_entry 2
    ktutil:list
slot KVNO Principal
---- ---- ---------------------------------------
   1    8 root/denver@EXAMPLE.COM
    ktutil:write_kt /etc/krb5/new.krb5.keytab
    ktutil: quit
denver # cp /etc/krb5/new.krb5.keytab /etc/krb5/krb5.keytab
```

◆ ◆ ◆ KAPITEL 26

Verwenden von Kerberos-Anwendungen (Aufgaben)

Dieses Kapitel ist für Benutzer bestimmt, die mit einem System arbeiten, auf dem der Kerberos-Service konfiguriert ist. In diesem Kapitel wird erläutert, wie die bereitgestellten kerberisierten Befehle und Services verwendet werden. Wenn Sie die nachfolgenden Informationen lesen, sollten Sie bereits mit den entsprechenden Befehlen in den Nicht-Kerberos-Versionen vertraut sein.

Da sich dieses Kapitel an allgemeine Leser richtet, enthält es Informationen zum Abrufen, Anzeigen und Löschen von Tickets. Außerdem beinhaltet es Informationen zum Auswählen oder Ändern eines Kerberos-Passworts.

Im Folgenden sind die Informationen in diesem Kapitel aufgeführt:

- „Kerberos-Ticketverwaltung“ auf Seite 569
- „Kerberos-Passwortverwaltung“ auf Seite 573
- „Kerberos-Benutzerbefehle“ auf Seite 578

Eine Übersicht über das Oracle Solaris Kerberos-Produkt erhalten Sie in Kapitel 21, „Einführung zum Kerberos-Service“.

Kerberos-Ticketverwaltung

In diesem Abschnitt wird erläutert, wie Tickets abgerufen, angezeigt und gelöscht werden. Eine Einführung zu Tickets finden Sie unter „Funktionsweise des Kerberos-Service“ auf Seite 408.

Automatisches Abrufen von Tickets

Wenn Sie eine SEAM- oder Oracle Solaris-Version installiert haben, ist Kerberos in den Befehl `login` integriert, und Sie rufen Tickets bei der Anmeldung automatisch ab. Die kerberisierten Befehle `rsh`, `rcp`, `rdist`, `telnet` und `rlogin` sind üblicherweise so eingerichtet, dass sie Kopien Ihrer Tickets an die anderen Rechner weiterleiten, damit Sie Tickets für den Zugriff auf diese

Rechner nicht explizit anfordern müssen. Ihre Konfiguration enthält diese automatische Weiterleitung möglicherweise nicht; es handelt sich jedoch um das Standardverhalten. Weitere Informationen zum Weiterleiten von Tickets finden Sie unter „Übersicht über kerberisierte Befehle“ auf Seite 579 und „Weiterleiten von Kerberos-Tickets“ auf Seite 581.

Informationen zur Lebensdauer von Tickets erhalten Sie unter „Lebensdauer von Tickets“ auf Seite 595.

Erstellen eines Kerberos-Tickets

Wenn PAM ordnungsgemäß konfiguriert ist, wird ein Ticket normalerweise automatisch bei der Anmeldung erstellt und es sind keine besonderen Schritte zum Abrufen eines Tickets erforderlich. Sie müssen jedoch gegebenenfalls ein Ticket erstellen, wenn Ihr Ticket abläuft. Außerdem müssen Sie eventuell zusätzlich zu Ihrem Standardhauptelement ein anderes Hauptelement verwenden, wenn Sie sich beispielsweise mit `rlogin -l` als eine andere Person bei einem Rechner anmelden.

Verwenden Sie zum Erstellen eines Tickets den Befehl `kinit`.

```
% /usr/bin/kinit
```

Der Befehl `kinit` fordert Sie zur Angabe Ihres Passworts auf Die vollständige Syntax des Befehls `kinit` finden Sie auf der Manpage `kinit(1)`.

BEISPIEL 26–1 Erstellen eines Kerberos-Tickets

Im folgenden Beispiel erstellt die Benutzerin `jennifer` ein Ticket auf dem eigenen System.

```
% kinit
Password for jennifer@ENG.EXAMPLE.COM:       <Type password>
```

In diesem Beispiel erstellt der Benutzer `david` ein Ticket, das für drei Stunden mit der Option `-l` gültig ist.

```
% kinit -l 3h david@EXAMPLE.ORG
Password for david@EXAMPLE.ORG:       <Type password>
```

Im nächsten Beispiel erstellt der Benutzer `david` mit der Option `-f` ein weiterleitbares Ticket für sich selbst. Mit diesem weiterleitbaren Ticket kann er sich z. B. bei einem zweiten System anmelden und `telnet` auf ein drittes System anwenden.

```
% kinit -f david@EXAMPLE.ORG
Password for david@EXAMPLE.ORG:          <Type password>
```

BEISPIEL 26–1 Erstellen eines Kerberos-Tickets *(Fortsetzung)*

Weitere Informationen zum Weiterleiten von Tickets finden Sie unter „Weiterleiten von Kerberos-Tickets“ auf Seite 581 und „Typen von Tickets“ auf Seite 593.

Anzeigen von Kerberos-Tickets

Nicht alle Tickets sind gleich. So kann beispielsweise ein Ticket *weiterleitbar* sein, während ein anderes Ticket *nachdatiert* ist. Ein drittes Ticket kann z. B. sowohl weiterleitbar als auch nachdatiert sein. Durch Verwenden des Befehls `klist` mit der Option `-f` können Sie anzeigen, über welche Tickets Sie verfügen und welches deren Attribute sind.

```
% /usr/bin/klist -f
```

Die folgenden Symbole geben die mit jedem Ticket verknüpften Attribute an, wie durch `klist` angezeigt:

A Vorauthentifiziert (Preauthenticated)

D Nachdatierbar (Postdatable)

d Nachdatiert (Postdated)

F Weiterleitbar (Forwardable)

f Weitergeleitet (Forwarded)

I Anfänglich (Initial)

i Ungültig (Invalid)

P Proxyfähig (Proxiable)

p Proxy

R Erneuerbar (Renewable)

Unter „Typen von Tickets“ auf Seite 593 werden die verschiedenen möglichen Attribute eines Tickets beschrieben.

BEISPIEL 26–2 Anzeigen von Kerberos-Tickets

In diesem Beispiel verfügt die Benutzerin `jennifer` über ein *anfängliches* Ticket, das *weiterleitbar* (F) und *nachdatiert* (d) ist, aber noch nicht validiert wurde (i).

```
% /usr/bin/klist -f
Ticket cache: /tmp/krb5cc_74287
Default principal: jennifer@EXAMPLE.COM

Valid starting                Expires                Service principal
```

BEISPIEL 26–2 Anzeigen von Kerberos-Tickets *(Fortsetzung)*

```
09 Mar 04 15:09:51  09 Mar 04 21:09:51  nfs/EXAMPLE.COM@EXAMPLE.COM
        renew until 10 Mar 04 15:12:51, Flags: Fdi
```

Im folgenden Beispiel verfügt der Benutzer `david` über zwei Tickets, die von seinem Host an einen anderen Host *weitergeleitet* (f) wurden. Die Tickets sind auch *weiterleitbar* (F).

```
% klist -f
Ticket cache: /tmp/krb5cc_74287
Default principal: david@EXAMPLE.COM

Valid starting                Expires                Service principal
07 Mar 04 06:09:51  09 Mar 04 23:33:51  host/EXAMPLE.COM@EXAMPLE.COM
        renew until 10 Mar 04 17:09:51, Flags: fF

Valid starting                Expires                Service principal
08 Mar 04 08:09:51  09 Mar 04 12:54:51  nfs/EXAMPLE.COM@EXAMPLE.COM
        renew until 10 Mar 04 15:22:51, Flags: fF
```

Das anschließende Beispiel zeigt, wie die Verschlüsselungstypen des Sitzungsschlüssels und des Tickets mit der Option `-e` angezeigt werden. Mit der Option `-a` wird die Hostadresse einem Hostnamen zugeordnet, falls der Name Service die Konvertierung durchführen kann.

```
% klist -fea
Ticket cache: /tmp/krb5cc_74287
Default principal: david@EXAMPLE.COM

Valid starting                Expires                Service principal
07 Mar 04 06:09:51  09 Mar 04 23:33:51  krbtgt/EXAMPLE.COM@EXAMPLE.COM
        renew until 10 Mar 04 17:09:51, Flags: FRIA
        Etype(skey, tkt): DES cbc mode with RSA-MD5, DES cbc mode with CRC-32
        Addresses: client.example.com
```

Löschen von Kerberos-Tickets

Wenn Sie alle während Ihrer aktuellen Sitzung erhaltenen Kerberos-Tickets löschen möchten, verwenden Sie den Befehl `kdestroy`. Der Befehl leert den Berechtigungsnachweis-Cache, wodurch alle Ihre Berechtigungsnachweise und Tickets gelöscht werden. Wenn `kdestroy` ausgeführt wird, verringert sich die Gefahr, dass der Berechtigungsnachweis-Cache beeinträchtigt wird, während Sie nicht angemeldet sind. Dies ist jedoch üblicherweise nicht erforderlich.

Verwenden Sie zum Löschen Ihrer Tickets den Befehl `kdestroy`.

```
% /usr/bin/kdestroy
```

Der Befehl `kdestroy` löscht *alle* Ihre Tickets. Sie können diesen Befehl nicht verwenden, um ein bestimmtes ausgewähltes Ticket zu löschen.

Wenn Sie eine Zeit lang nicht mit dem System arbeiten und besorgt sind, dass ein Eindringling Ihre Berechtigungen verwenden könnte, sollten Sie entweder `kdestroy` oder einen Bildschirmschoner verwenden, der den Bildschirm sperrt.

Kerberos-Passwortverwaltung

Wenn der Kerberos-Service konfiguriert ist, haben Sie zwei Passwörter: das reguläre Solaris-Passwort und ein Kerberos-Passwort. Die beiden Passwörter können gleich lauten oder verschieden sein.

Hinweis zum Auswählen eines Passworts

Ihr Passwort kann fast jedes beliebige Zeichen enthalten. Die wichtigsten Ausnahmen bilden die Strg-Tasten und die Eingabetaste. Ein Passwort sollte in erster Linie leicht zu merken sein, aber von anderen nicht erraten werden können. Folgendes sollten Sie beispielsweise nicht als Passwort verwenden:

- Wörter, die in einem Wörterbuch verzeichnet sind
- Einen gebräuchlichen oder beliebten Namen
- Den Namen einer berühmten Person oder Figur
- Ihren Namen oder Benutzernamen in irgendeiner Form (z. B. rückwärts geschrieben, zweimal wiederholt usw.)
- Den Namen Ihres Ehepartners, Kinds oder Haustiers
- Ihr Geburtsdatum oder das Geburtsdatum eines Angehörigen
- Ihre Sozialversicherungs-, Führerschein-, Ausweis- oder eine ähnliche Identifikationsnummer
- Ein in diesem oder einem anderen Handbuch verwendetes Beispielpasswort

Ein Passwort sollte mindestens acht Zeichen lang sein. Darüber hinaus sollte es eine Mischung aus Zeichen enthalten, wie etwa Groß- und Kleinbuchstaben, Zeilen und Satzzeichen. Nachfolgend sind einige Passwörter aufgeführt, die gut geeignet wären, wenn sie nicht in diesem Handbuch verwendet würden:

- Akronyme, wie z. B. "IVMHAinSF" (was für "Ich verlor mein Herz auch in San Francisco" stehen könnte).
- Leicht auszusprechende Unsinnswörter, wie z. B. "Dumdidum" oder "Bimbambum!".
- Absichtlich falsch geschriebene Begriffe, wie z. B. "Hannnover" oder "Aapfelkkuchen".

Achtung – Verwenden Sie diese Beispiele nicht. Die in Handbüchern verwendeten Passwörter sind die ersten Passwörter, die ein Eindringling ausprobieren würde.

Ändern Ihres Passworts

Wenn PAM ordnungsgemäß konfiguriert ist, können Sie Ihr Kerberos-Passwort auf zwei Arten ändern:

- Mit dem üblichen UNIX-Befehl `passwd`. Wenn der Kerberos-Service konfiguriert ist, fordert Sie der Befehl `passwd` automatisch zur Angabe eines neuen Kerberos-Passworts auf.

  Der Vorteil der Verwendung von `passwd` statt `kpasswd` liegt darin, dass Sie gleichzeitig sowohl UNIX- als auch Kerberos-Passwörter festlegen können. Dennoch *müssen* Sie im Allgemeinen nicht beide Passwörter mit `passwd` ändern. Häufig können Sie auch nur Ihr UNIX-Passwort ändern und am Kerberos-Passwort keine Änderungen vornehmen oder umgekehrt.

  Hinweis – Das Verhalten von `passwd` hängt von der Konfiguration des PAM-Moduls ab. Möglicherweise müssen Sie in bestimmten Konfigurationen beide Passwörter ändern. Bei einigen Standorten ist eine Änderung des UNIX-Passworts erforderlich, während bei anderen das Kerberos-Passwort geändert werden muss.

- Mit dem Befehl `kpasswd`. Der Befehl `kpasswd` ähnelt sehr stark dem Befehl `passwd`. Ein Unterschied besteht jedoch darin, dass `kpasswd` nur Kerberos-Passwörter ändert. Wenn Sie Ihr UNIX-Passwort ändern möchten, müssen Sie `passwd` verwenden.

  Ein weiterer Unterschied liegt darin, dass `kpasswd` ein Passwort für ein Kerberos-Hauptelement ändern kann, bei dem es sich nicht um einen gültigen UNIX-Benutzer handelt. Beispiel: `david/admin` ist ein Kerberos-Hauptelement, aber kein tatsächlicher UNIX-Benutzer, sodass Sie `kpasswd` statt `passwd` verwenden müssen.

Nachdem Sie Ihr Passwort geändert haben, dauert es eine Weile, bis die Änderung über ein System weitergegeben wird. Dies gilt insbesondere für große Netzwerke. Je nach Konfiguration Ihres Systems beträgt die Verzögerung zwischen wenigen Minuten und mehr als einer Stunde. Wenn Sie die neuen Kerberos-Tickets kurz nach Änderung Ihres Passworts erhalten müssen, versuchen Sie es zuerst mit dem neuen Passwort. Funktioniert das neue Passwort nicht, versuchen Sie es erneut mit dem alten Passwort.

Mit dem Kerberos V5-Protokoll können Systemadministratoren Kriterien bezüglich der zulässigen Passwörter für jeden Benutzer festlegen. Derartige Kriterien werden von der für

jeden Benutzer festgelegten *Richtlinie* oder einer Standardrichtlinie definiert. Weitere Informationen zu Richtlinien finden Sie unter „Verwalten von Kerberos-Richtlinien“ auf Seite 546.

Beispiel: Angenommen, die Richtlinie der Benutzerin `jennifer` (hier `jenpol` genannt) schreibt vor, dass Passwörter mindestens acht Zeichen lang sein und eine Mischung von mindestens zwei Arten von Zeichen enthalten müssen. `kpasswd` wird daher den Versuch, "sloth" als Passwort zu verwenden, zurückweisen.

```
% kpasswd
kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.
Old password:        <Jennifer types her existing password>
kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by
the policy jenpol
which requires a minimum of 8 characters from at least 2 classes
(the five classes are lowercase, uppercase, numbers, punctuation,
and all other characters).
New password:      <Jennifer types 'sloth'>
New password (again):       <Jennifer re-types 'sloth'>
kpasswd: New password is too short.
Please choose a password which is at least 4 characters long.
```

In diesem Fall verwendet `jennifer` "slothrop49" als Passwort. Das Passwort "slothrop49" entspricht den Kriterien, da es über acht Zeichen lang ist und zwei verschiedene Arten von Zeichen enthält (Zahlen und Kleinbuchstaben).

```
% kpasswd
kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.
Old password:       <Jennifer types her existing password>
kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by
the policy jenpol
which requires a minimum of 8 characters from at least 2 classes
(the five classes are lowercase, uppercase, numbers, punctuation,
and all other characters).
New password:       <Jennifer types 'slothrop49'>
New password (again):       <Jennifer re-types 'slothrop49'>
Kerberos password changed.
```

BEISPIEL 26–3 Ändern Ihres Passworts

Im folgenden Beispiel ändert der Benutzer `david` sowohl sein UNIX- als auch sein Kerberos-Passwort mit `passwd`.

```
% passwd
    passwd:  Changing password for david
    Enter login (NIS+) password:                    <Type the current UNIX password>
    New password:                                <Type the new UNIX password>
    Re-enter password:                           <Confirm the new UNIX password>
```

BEISPIEL 26–3 Ändern Ihres Passworts *(Fortsetzung)*

```
Old KRB5 password:                  <Type the current Kerberos password>
New KRB5 password:                  <Type the new Kerberos password>
Re-enter new KRB5 password:         <Confirm the new Kerberos password>
```

Bedenken Sie, dass `passwd` sowohl nach dem UNIX- als auch nach dem Kerberos-Passwort fragt. Dieses Verhalten ist in der Standardkonfiguration festgelegt. In diesem Fall muss der Benutzer `david` mit dem Befehl `kpasswd` ein neues Kerberos-Passwort festlegen, wie im Folgenden dargestellt.

Im nachstehenden Beispiel ändert der Benutzer `david` nur sein Kerberos-Passwort mit `kpasswd` .

```
% kpasswd
kpasswd: Changing password for david@ENG.EXAMPLE.COM.
Old password:               <Type the current Kerberos password>
New password:               <Type the new Kerberos password>
New password (again):       <Confirm the new Kerberos password>
Kerberos password changed.
```

In diesem Beispiel ändert der Benutzer `david` das Passwort für das Kerberos-Hauptelement `david/admin` (bei dem es sich nicht um einen gültigen UNIX-Benutzer handelt). Er muss `kpasswd` verwenden.

```
% kpasswd david/admin
kpasswd:  Changing password for david/admin.
Old password:               <Type the current Kerberos password>
New password:               <Type the new Kerberos password>
New password (again):       <Type the new Kerberos password>
Kerberos password changed.
```

Gewähren von Zugriff auf Ihr Konto

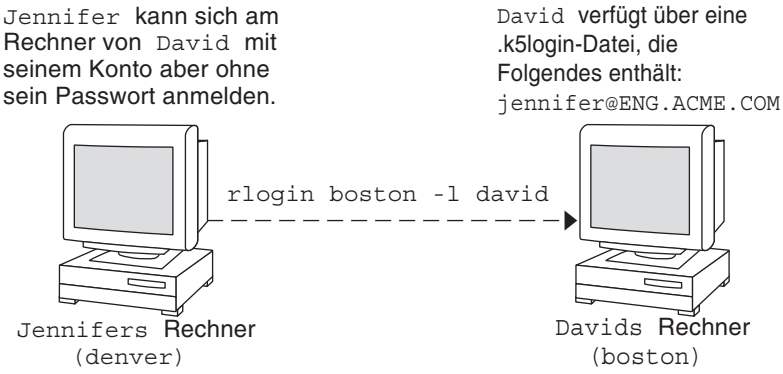
Wenn Sie einem Benutzer Zugriff erteilen müssen, damit er sich (unter Ihrem Namen) bei Ihrem Konto anmelden kann, können Sie dies über Kerberos durchführen, ohne Ihr Passwort bekannt zu geben, indem Sie eine `.k5login`-Datei in Ihrem Home-Verzeichnis ablegen. Eine `.k5login`-Datei ist eine Liste von einem oder mehreren Kerberos-Hauptelementen, die den einzelnen Personen entsprechen, denen Sie Zugriff gewähren möchten. Jedes Hauptelement muss sich in einer separaten Zeile befinden.

Angenommen, der Benutzer `david` hat eine `.k5login`-Datei in seinem Home-Verzeichnis abgelegt, die wie folgt aussieht:

```
jennifer@ENG.EXAMPLE.COM
joe@EXAMPLE.ORG
```

Mit dieser Datei können die Benutzer `jennifer` und `joe` die Identität von `david` annehmen, vorausgesetzt, sie verfügen bereits über Kerberos-Tickets in ihren jeweiligen Bereichen. Zum Beispiel kann jennifer sich entfernt beim Rechner von `david` (`boston`) unter dessen Namen anmelden, ohne dass dieser sein Passwort bekanntgeben muss.

ABBILDUNG 26–1 Verwenden der Datei `.k5login` zum Gewähren von Zugriff auf Ihr Konto



Wenn das Home-Verzeichnis von `david` unter Verwendung von Kerberos V5-Protokolls von einem anderen (dritten) Rechner aus über NFS eingehängt wird, benötigt `jennifer` ein weiterleitbares Ticket, um darauf zuzugreifen. Ein Beispiel für die Verwendung eines weiterleitbaren Tickets finden Sie unter „Erstellen eines Kerberos-Tickets“ auf Seite 570.

Wenn Sie sich bei anderen Rechnern über ein Netzwerk anmelden, möchten Sie vermutlich Ihr eigenes Kerberos-Hauptelement in die `.k5login`-Dateien auf diesen Rechnern einbeziehen.

Aus folgenden Gründen ist es wesentlich sicherer, eine `.k5login`-Datei zu verwenden, als Ihr Passwort bekannt zu geben:

- Sie können den Zugriff jederzeit zurücknehmen, indem Sie das Hauptelement aus Ihrer `.k5login`-Datei entfernen.
- Dennoch verfügen die in der `.k5login`-Datei in Ihrem Home-Verzeichnis aufgelisteten Benutzer-Hauptelemente über vollen Zugriff auf diesen Rechner (oder auf Gruppen von Rechnern, wenn die `.k5login`-Datei gemeinsam genutzt wird, beispielsweise über NFS). Sämtliche kerberisierte Services autorisieren den Zugriff jedoch basierend auf der Identität dieses Benutzers (und nicht auf Ihrer Identität). Somit kann sich `jennifer` beim Rechner von `joe` anmelden und dort Aufgaben ausführen. Wenn sie allerdings ein kerberisiertes Programm wie z. B. `ftp` oder `rlogin` verwendet, kann sie dies unter ihrem Namen tun.

- Kerberos führt ein Protokoll darüber, wer Tickets abruft, sodass ein Systemadministrator bei Bedarf herausfinden kann, wer zu einem bestimmen Zeitpunkt Ihre Benutzeridentität verwenden kann.

Eine gängige Methode zur Verwendung der `.k5login`-Datei besteht darin, sie in dem Home-Verzeichnis `root` abzulegen und den aufgelisteten Kerberos-Hauptelementen somit `root`-Zugriff auf diesen Rechner zu erteilen. Dank dieser Konfiguration können Systemadministrationen lokal die Funktion von `root` übernehmen oder sich entfernt als `root` anmelden, ohne das `root`-Passwort bekanntgeben und ohne das `root`-Passwort über das Netzwerk eingeben zu müssen.

BEISPIEL 26–4 Verwenden der Datei `.k5login` zum Gewähren von Zugriff auf Ihr Konto

Angenommen, `jennifer` möchte sich als `root` bei dem Rechner `boston.example.com` anmelden. Da sie über einen Eintrag für Ihren Hauptelementnamen in der `.k5login`-Datei im Home-Verzeichnis von `root` auf `boston.example.com` verfügt, muss sie erneut ihr Passwort nicht eingeben.

```
% rlogin boston.example.com -l root -x
This rlogin session is using DES encryption for all data transmissions.
Last login: Thu Jun 20 16:20:50 from daffodil
SunOS Release 5.7 (GENERIC) #2: Tue Nov 14 18:09:31 EST 1998
boston[root]%
```

Kerberos-Benutzerbefehle

Das Kerberos V5-Produkt ist ein *Single Sign-On*-System, d. h. Sie müssen Ihr Passwort nur einmal eingeben. Die Kerberos V5-Programme führen die Authentifizierung (und die optionale Verschlüsselung) für Sie durch, da Kerberos in eine Reihe vorhandener bekannter Netzwerkprogramme integriert wurde. Bei den Kerberos V5-Anwendungen handelt es sich um Versionen bestehender UNIX-Netzwerkprogramme mit zusätzlichen Kerberos-Funktionen.

Wenn Sie beispielsweise mit einem kerberisierten Programm eine Verbindung zu einem Remote-Host herstellen, führen das Programm, das KDC und der Remote-Host eine Reihe schneller Aushandlungen aus. Nach Abschluss dieser Aushandlungen hat das Programm Ihre Identität in Ihrem Namen gegenüber dem Remote-Host bewiesen und der Remote-Host hat Ihnen Zugriff gewährt.

Denken Sie daran, dass kerberisierte Befehle zuerst versuchen, die Authentifizierung mit Kerberos durchzuführen. Schlägt die Kerberos-Authentifizierung fehl, tritt je nach den mit dem Befehl verwendeten Optionen ein Fehler auf oder es wird versucht, die UNIX-Authentifizierung durchzuführen. Ausführlichere Informationen finden Sie im Abschnitt `Kerberos Security` auf der Manpage zu jedem Kerberos-Befehl.

Übersicht über kerberisierte Befehle

Die kerberisierten Netzwerkdienste stellen Programme dar, die eine Verbindung zu einem anderen Rechner im Internet herstellen. Dabei handelt es sich um folgende Programme:

- `ftp`
- `rcp`
- `rdist`
- `rlogin`
- `rsh`
- `ssh`
- `telnet`

Diese Programme verfügen über Funktionen, die Ihre Kerberos-Tickets transparent für die Aushandlung von Authentifizierung und optionale Verschlüsselung mit dem Remote-Host verwenden. In den meisten Fällen wird Ihnen lediglich auffallen, dass Sie Ihr Passwort nicht mehr eingeben müssen, um die Tickets zu verwenden, da Kerberos Ihre Identität für Sie überprüft.

Die Kerberos V5-Netzwerkprogramme umfassen Optionen, mit denen Sie die folgenden Aktionen ausführen können:

- Weiterleiten Ihres Tickets an einen anderen Host (sofern Sie zu Beginn weiterleitbare Tickets abgerufen haben)
- Verschlüsseln von Daten, die zwischen Ihnen und dem Remote-Host übertragen wurden

---

Hinweis – In diesem Abschnitt wird vorausgesetzt, dass Sie bereits mit den Nicht-Kerberos-Versionen dieser Programme vertraut sind, und die durch das Kerberos V5-Paket hinzugefügten Kerberos-Funktionen werden hervorgehoben. Ausführliche Beschreibungen zu den hier aufgeführten Befehlen finden Sie auf den jeweiligen Manpages.

Folgende Kerberos-Optionen wurden den Befehlen `ftp`, `rcp`, `rlogin`, `rsh` und `telnet` hinzugefügt:

`-a`	Versucht, die automatische Anmeldung unter Verwendung Ihrer vorhandenen Tickets durchzuführen. Verwendet den von `getlogin()` zurückgegebenen Benutzernamen, es sei denn, der Name weicht von der aktuellen Benutzer-ID ab. Weitere Informationen finden Sie auf der Manpage `telnet`(1).
`-f`	Leitet ein *nicht erneut weiterleitbares* Ticket an einen Remote-Host weiter. Diese Option und die Option `-F` schließen sich gegenseitig aus. Sie können nicht zusammen im selben Befehl verwendet werden.

Wenn Sie Grund haben anzunehmen, dass Sie sich bei anderen Kerberos-basierten Services auf einem dritten Host authentifizieren müssen, sollten Sie ein Ticket weiterleiten. So ist es beispielsweise denkbar, dass Sie sich entfernt bei einem anderen Rechner anmelden möchten, um sich dann über diesen Rechner ebenfalls entfernt bei einem dritten Rechner anzumelden.

Sie sollten definitiv ein weiterleitbares Ticket verwenden, wenn Ihr Home-Verzeichnis auf dem Remote-Host unter Verwendung des Kerberos V5-Mechanismus über NFS eingehängt ist. Andernfalls können Sie nicht auf Ihr Home-Verzeichnis zugreifen. Dies ist der Fall, wenn Sie sich zum Beispiel bei System 1 anmelden. Über System 1 melden Sie sich entfernt bei Ihrem Home-Rechner (System 2) an, der Ihr Home-Verzeichnis über System 3 einhängt. Wenn Sie nicht die Option `-f` oder `-F` mit `rlogin` verwendet haben, können Sie nicht auf Ihr Home-Verzeichnis zugreifen, weil Ihr Ticket nicht an System 3 weitergeleitet werden kann.

Standardmäßig ruft `kinit` weiterleitbare TGTs (Ticket-gewährende Tickets) ab. Es ist dennoch möglich, dass sich Ihre Konfiguration in dieser Hinsicht unterscheidet.

Weitere Informationen zum Weiterleiten von Tickets finden Sie unter „Weiterleiten von Kerberos-Tickets“ auf Seite 581.

`-F` — Leitet eine *erneut weiterleitbare* Kopie Ihres TGT an ein Remote-System weiter. Diese Option ähnelt der Option `-f`, ermöglicht jedoch den Zugriff auf einen weiteren (z. B. vierten oder fünften) Rechner. Die Option `-F` kann daher als Obergruppe der Option `-f` betrachtet werden. Die Option `-F` und die Option `-f` schließen sich gegenseitig aus. Sie können nicht zusammen im selben Befehl verwendet werden.

Weitere Informationen zum Weiterleiten von Tickets finden Sie unter „Weiterleiten von Kerberos-Tickets“ auf Seite 581.

`-k` *realm* — Fordert Tickets für den Remote-Host im angegebenen *realm* an, anstatt den Bereich selbst mithilfe der Datei `krb5.conf` zu bestimmen.

`-K` — Verwendet Ihre Tickets zum Authentifizieren beim Remote-Host, führt aber keine automatische Anmeldung durch.

`-m` *mechanism* — Gibt den zu verwendenden GSS-API-Sicherheitsmechanismus an, wie er in der Datei `/etc/gss/mech` aufgelistet ist. Standardmäßig ist `kerberos_v5` angegeben.

`-x` — Verschlüsselt diese Sitzung.

`-X` *auth-type* — Deaktiviert den Authentifizierungstyp *auth-type*.

Die folgende Tabelle zeigt, welche Befehle über bestimmte Optionen verfügen. "X" gibt an, dass der Befehl über die jeweilige Option verfügt.

TABELLE 26–1 Kerberos-Optionen für Netzwerkbefehle

	ftp	rcp	rlogin	rsh	telnet
-a					X
-f	X		X	X	X
-F			X	X	X
-k		X	X	X	X
-K					X
-m	X				
-x	X	X	X	X	X
-X					X

Außerdem ermöglicht `ftp`, die Schutzebene einer Sitzung an der entsprechenden Eingabeaufforderung festzulegen:

clear Setzt die Schutzebene auf "clear" (kein Schutz). Dies ist die standardmäßige Schutzebene.

private Setzt die Schutzebene auf "private". Die Vertraulichkeit und Integrität von Datenübertragungen werden durch Verschlüsselung geschützt. Dennoch steht der Vertraulichkeitsservice möglicherweise nicht allen Kerberos-Benutzern zur Verfügung.

safe Setzt die Schutzebene auf "safe". Die Integrität von Datenübertragungen wird durch kryptografische Prüfsummen geschützt.

Sie können die Schutzebene auch über die `ftp`-Eingabeaufforderung festlegen, indem Sie `protect` gefolgt von einer der oben dargestellten Sicherheitsebenen eingeben (`clear`, `private` oder `safe`).

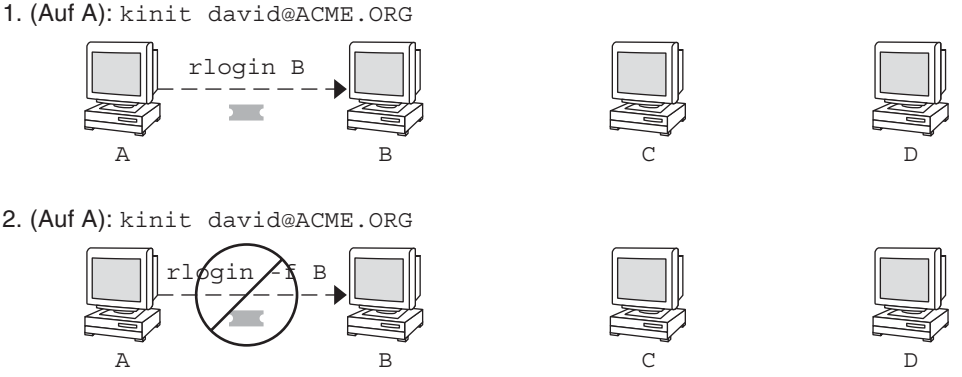
Weiterleiten von Kerberos-Tickets

Wie unter „Übersicht über kerberisierte Befehle“ auf Seite 579 beschrieben, können Sie einige Befehle entweder mit der Option `-f` oder `-F` verwenden, um Tickets weiterzuleiten. Das Weiterleiten von Tickets ermöglicht es Ihnen, Ihre Netzwerktransaktionen zu "verketten". Beispielsweise können Sie sich entfernt bei einem Rechner anmelden, um sich dann über diesen

Rechner ebenfalls entfernt bei einem anderen Rechner anzumelden. Mit der Option `-f` können Sie ein Ticket weiterleiten, während Ihnen die Option `-F` das erneute Weiterleiten eines weitergeleiteten Tickets ermöglicht.

In Abbildung 26–2 ruft der Benutzer `david` ein nicht weiterleitbares TGT (Ticket-gewährendes Ticket) mit `kinit` ab. Das Ticket lässt sich nicht weiterleiten, weil er die Option `-f` nicht angegeben hat. In Szenario 1 kann er sich entfernt bei Rechner B anmelden, aber keine weiteren Schritte ausführen. In Szenario 2 schlägt der Befehl `rlogin -f` fehl, weil der Benutzer versucht, ein nicht weiterleitbares Ticket weiterzuleiten.

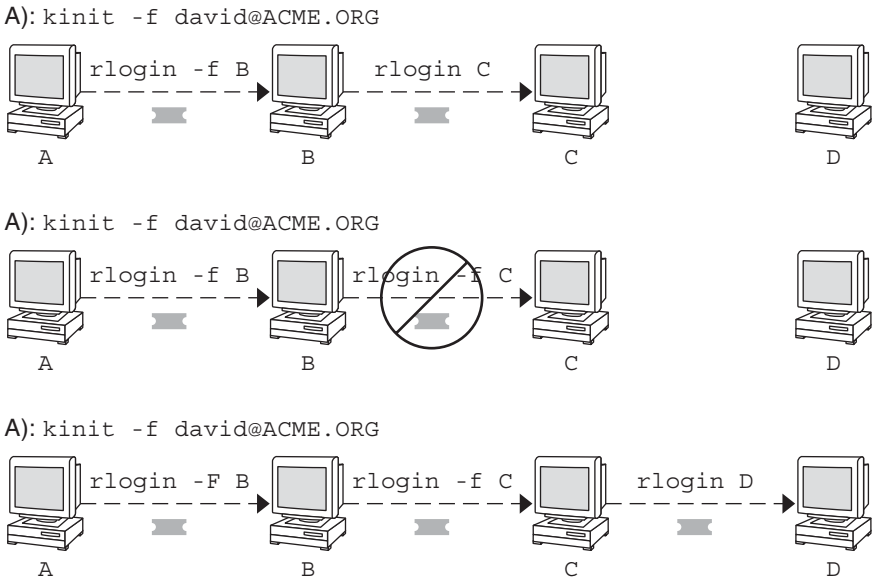
ABBILDUNG 26–2 Verwenden nicht weiterleitbarer Tickets



Faktisch werden Kerberos-Konfigurationsdateien so eingerichtet, dass `kinit` standardmäßig weiterleitbare Tickets abruft. Ihre Konfiguration kann jedoch davon abweichen. Der Anschaulichkeit halber gehen wir davon aus, dass der Befehl `kinit` *keine* weiterleitbaren TGTs abruft, es sei denn, er wird mit der Option `kinit -f` aufgerufen. Beachten Sie auch, dass `kinit` nicht mit der Option `-F` verwendet wird. TGTs sind entweder weiterleitbar oder nicht.

In Abbildung 26–3 ruft der Benutzer `david` weiterleitbare TGTs mit `kinit -f` ab. In Szenario 3 kann er auf Rechner C zugreifen, da er ein weiterleitbares Ticket mit `rlogin` verwendet. In Szenario 4 schlägt der zweite `rlogin`-Befehl fehl, da das Ticket nicht weitergeleitet werden kann. In Szenario 5 wird stattdessen die Option `-F` verwendet. Dadurch ist der zweite `rlogin`-Befehl erfolgreich und das Ticket kann erneut weitergeleitet werden (an Rechner D).

ABBILDUNG 26–3 Verwenden weiterleitbarer Tickets



Verwenden kerberisierter Befehle (Beispiele)

Die folgenden Beispiele zeigen, wie sich die Optionen auf die kerberisierten Befehle auswirken.

BEISPIEL 26–5 Verwenden der Optionen `-a`, `-f` und `-x` mit `telnet`

In diesem Beispiel hat sich der Benutzer `david` bereits angemeldet und möchte `telnet` auf den Rechner `denver.example.com` anwenden. Er verwendet die Option `-f` zum Weiterleiten seiner vorhandenen Tickets, die Option `-x` zum Verschlüsseln der Sitzung und die Option `-a` zum automatischen Ausführen der Anmeldung. Da er nicht vorhat, die Services eines dritten Hosts zu nutzen, kann er `-f` anstelle von `-F` verwenden.

```
% telnet -a -f -x denver.example.com
Trying 128.0.0.5...
Connected to denver.example.com. Escape character is '^]'.
[ Kerberos V5 accepts you as "david@eng.example.com" ]
[ Kerberos V5 accepted forwarded credentials ]
SunOS 5.9: Tue May 21 00:31:42 EDT 2004  Welcome to SunOS
%
```

Bedenken Sie, dass der Rechner von `david` Kerberos verwendet hat, um ihn für `denver.example.com` zu authentifizieren, und ihn automatisch unter seinem Namen angemeldet hat. Er verfügte über eine verschlüsselte Sitzung, Kopien seiner Tickets standen schon für ihn bereit und er musste zu keiner Zeit sein Passwort eingeben. Hätte er eine Nicht-Kerberos-Version von `telnet` verwendet, wäre er aufgefordert worden, sein Passwort

BEISPIEL 26–5 Verwenden der Optionen `-a`, `-f` und `-x` mit `telnet` *(Fortsetzung)*

anzugeben. Das Passwort wäre dann unverschlüsselt über das Netzwerk versendet worden. Hätte ein Eindringling währenddessen den Netzwerkverkehr beobachtet, so hätte dieser das Passwort von `david` erfahren.

Wenn Sie Ihre Kerberos-Tickets weiterleiten, löscht `telnet` diese beim Beenden, sofern vorhanden. Gleiches gilt für die anderen hier erläuterten Befehle.

BEISPIEL 26–6 Verwenden von `rlogin` mit der Option `-F`

In diesem Beispiel möchte sich die Benutzerin `jennifer` beim eigenen Rechner (`boston.example.com`) anmelden. Sie leitet ihre vorhandenen Tickets mit der Option `-F` weiter und verschlüsselt die Sitzung mit der Option `-x`. Sie wählt `-F` anstelle von `-f`, da sie nach der Anmeldung bei `boston` gegebenenfalls weitere Netzwerktransaktionen ausführen möchte, für die Tickets erneut weitergeleitet werden müssen. Da sie ihre vorhandenen Tickets weiterleitet, braucht sie zudem ihr Passwort nicht einzugeben.

```
% rlogin boston.example.com -F -x
This rlogin session is using encryption for all transmissions.
Last login Mon May 19 15:19:49 from daffodil
SunOS Release 5.9 (GENERIC) #2 Tue Nov 14 18:09:3 EST 2003
%
```

BEISPIEL 26–7 Festlegen der Schutzebene in `ftp`

Angenommen, der Benutzer `joe` möchte mit `ftp` über den Rechner `denver.example.com` seine Mail aus dem Verzeichnis `~joe/MAIL` abrufen, indem er die Sitzung verschlüsselt. Der Austausch sähe wie folgt aus:

```
% ftp -f denver.example.com
Connected to denver.example.com
220 denver.example.org FTP server (Version 6.0) ready.
334 Using authentication type GSSAPI; ADAT must follow
GSSAPI accepted as authentication type
GSSAPI authentication succeeded Name (daffodil.example.org:joe)
232 GSSAPI user joe@MELPOMENE.EXAMPLE.COM is authorized as joe
230 User joe logged in.
Remote system type is UNIX.
Using BINARY mode to transfer files.
ftp> protect private
200 Protection level set to Private
ftp> cd ~joe/MAIL
250 CWD command successful.
ftp> get RMAIL
227 Entering Passive Mode (128,0,0,5,16,49)
150 Opening BINARY mode data connection for RMAIL (158336 bytes).
226 Transfer complete. 158336 bytes received in 1.9 seconds (1.4e+02 Kbytes/s)
ftp> quit
%
```

BEISPIEL 26–7 Festlegen der Schutzebene in `ftp` *(Fortsetzung)*

Zum Verschlüsseln der Sitzung setzt `joe` die Schutzebene auf `private`.

◆ ◆ ◆ KAPITEL 27

Der Kerberos-Service (Referenz)

In diesem Kapitel werden zahlreiche Dateien, Befehle und Dämonen des Kerberos-Produkts aufgelistet. Außerdem liefert das Kapitel detaillierte Informationen über die Funktionsweise der Kerberos-Authentifizierung.

Im Folgenden sind die Informationen zur Referenz in diesem Kapitel aufgeführt.

- „Kerberos-Dateien“ auf Seite 587
- „Kerberos-Befehle“ auf Seite 589
- „Kerberos-Dämonen“ auf Seite 590
- „Kerberos-Terminologie“ auf Seite 591
- „Funktionsweise des Kerberos-Authentifizierungssystems“ auf Seite 598
- „Erhalten von Zugriff auf einen Service mit Kerberos“ auf Seite 598
- „Verwenden von Kerberos-Verschlüsselungstypen“ auf Seite 602
- „Verwenden der Tabelle `gsscred`“ auf Seite 604
- „Wesentliche Unterschiede zwischen Oracle Solaris Kerberos und MIT Kerberos“ auf Seite 605

Kerberos-Dateien

TABELLE 27–1 Kerberos-Dateien

Dateiname	Beschreibung
`~/.gkadmin`	Standardwerte für die Erstellung neuer Hauptelemente im SEAM-Tool
`~/.k5login`	Liste der Hauptelemente, die Zugriff auf ein Kerberos-Konto gewähren

TABELLE 27–1 Kerberos-Dateien *(Fortsetzung)*

Dateiname	Beschreibung
`/etc/krb5/kadm5.acl`	ACL-Datei (Access Control List, Zugriffssteuerungsliste) von Kerberos mit Hauptelementnamen von KDC-Administratoren und deren Kerberos-Administratorberechtigungen
`/etc/krb5/kadm5.keytab`	Schlüsseltabellendatei für den `kadmin`-Service auf dem Master-KDC
`/etc/krb5/kdc.conf`	KDC-Konfigurationsdatei
`/etc/krb5/kpropd.acl`	Konfigurationsdatei für die Weitergabe der Kerberos-Datenbank
`/etc/krb5/krb5.conf`	Konfigurationsdatei für den Kerberos-Bereich
`/etc/krb5/krb5.keytab`	Schlüsseltabellendatei für Netzwerkanwendungsserver
`/etc/krb5/warn.conf`	Konfigurationsdatei für die Warnung beim Ablauf von Kerberos-Tickets und die automatische Erneuerung
`/etc/pam.conf`	PAM-Konfigurationsdatei
`/tmp/krb5cc_`*uid*	Standardmäßiger Berechtigungsnachweis-Cache, wobei *uid* die dezimale UID des Benutzers ist
`/tmp/ovsec_adm.`*xxxxxx*	Temporärer Berechtigungsnachweis-Cache für die Lebensdauer des Vorgangs zur Passwortänderung, wobei *xxxxxx* eine zufällige Zeichenfolge ist
`/var/krb5/.k5.`*REALM*	KDC-Stash-Datei, die eine Kopie des KDC-Master-Schlüssels enthält
`/var/krb5/kadmin.log`	Protokolldatei für `kadmind`
`/var/krb5/kdc.log`	Protokolldatei für das KDC
`/var/krb5/principal`	Hauptelement-Datenbank für Kerberos
`/var/krb5/principal.kadm5`	Administrative Datenbank für Kerberos, die Richtlinieninformationen enthält
`/var/krb5/principal.kadm5.lock`	Sperrdatei der administrativen Kerberos-Datenbank
`/var/krb5/principal.ok`	Initialisierungsdatei der Hauptelement-Datenbank für Kerberos, die bei erfolgreicher Initialisierung der Kerberos-Datenbank erstellt wird
`/var/krb5/principal.ulog`	Kerberos-Aktualisierungsprotokoll, das Updates für die inkrementelle Weitergabe enthält
`/var/krb5/slave_datatrans`	Backup-Datei des KDC, die das Skript `kprop_script` für die Weitergabe verwendet

TABELLE 27–1 Kerberos-Dateien *(Fortsetzung)*

Dateiname	Beschreibung
`/var/krb5/slave_datatrans_`*slave*	Temporäre Dump-Datei, die bei vollständigen Updates von *slave* erstellt wird

Kerberos-Befehle

In diesem Abschnitt werden einige Befehle des Kerberos-Produkts aufgeführt.

TABELLE 27–2 Kerberos-Befehle

Befehl	Beschreibung
`/usr/bin/ftp`	FTP-Programm (File Transfer Protocol)
`/usr/bin/kdestroy`	Löschen von Kerberos-Tickets
`/usr/bin/kinit`	Abrufen Ticket-gewährender Tickets für Kerberos und Speichern dieser Tickets im Cache
`/usr/bin/klist`	Anzeigen aktueller Kerberos-Tickets
`/usr/bin/kpasswd`	Ändern eines Kerberos-Passworts
`/usr/bin/ktutil`	Verwalten von Kerberos-Schlüsseltabellendateien
`/usr/bin/rcp`	Programm zum Kopieren von Remote-Dateien
`/usr/bin/rdist`	Programm für die Verteilung von Remote-Dateien
`/usr/bin/rlogin`	Programm für die Remote-Anmeldung
`/usr/bin/rsh`	Programm für Remote-Shells
`/usr/bin/telnet`	Kerberisiertes `telnet`-Programm
`/usr/lib/krb5/kprop`	Programm für die Weitergabe der Kerberos-Datenbank
`/usr/sbin/gkadmin`	GUI-Programm für die Verwaltung der Kerberos-Datenbank, das zum Verwalten von Hauptelementen und Richtlinien verwendet wird
`/usr/sbin/gsscred`	Verwalten von Einträgen der gsscred-Tabelle
`/usr/sbin/kadmin`	Programm für die Remote-Verwaltung der Kerberos-Datenbank (auszuführen mit Kerberos-Authentifizierung), das zum Verwalten von Hauptelementen, Richtlinien und Schlüsseltabellendateien verwendet wird

TABELLE 27–2 Kerberos-Befehle *(Fortsetzung)*

Befehl	Beschreibung
`/usr/sbin/kadmin.local`	Programm für die lokale Verwaltung der Kerberos-Datenbank (auszuführen auf Master-KDC, ohne Kerberos-Authentifizierung), das zum Verwalten von Hauptelementen, Richtlinien und Schlüsseltabellendateien verwendet wird
`/usr/sbin/kclient`	Skript für die Kerberos-Clientinstallation, das mit oder ohne Installationsprofil verwendet wird
`/usr/sbin/kdb5_ldap_util`	Erstellen von LDAP-Containern für Kerberos-Datenbanken
`/usr/sbin/kdb5_util`	Erstellen von Kerberos-Datenbanken und Stash-Dateien
`/usr/sbin/kgcmgr`	Konfigurieren von Master- und Slave-KDCs für Kerberos
`/usr/sbin/kproplog`	Auflisten einer Zusammenfassung der Aktualisierungseinträge im Aktualisierungsprotokoll

Kerberos-Dämonen

In der folgenden Tabelle werden die vom Kerberos-Produkt verwendeten Dämonen aufgeführt.

TABELLE 27–3 Kerberos-Dämonen

Dämon	Beschreibung
`/usr/sbin/in.ftpd`	FTP-Dämon (File Transfer Protocol)
`/usr/lib/krb5/kadmind`	Dämon für die Verwaltung der Kerberos-Datenbank
`/usr/lib/krb5/kpropd`	Dämon für die Weitergabe der Kerberos-Datenbank
`/usr/lib/krb5/krb5kdc`	Dämon für die Verarbeitung von Kerberos-Tickets
`/usr/lib/krb5/ktkt_warnd`	Dämon für die Warnung beim Ablauf von Kerberos-Tickets und die automatische Erneuerung
`/usr/sbin/in.rlogind`	Dämon für die Remote-Anmeldung
`/usr/sbin/in.rshd`	Dämon für Remote-Shells
`/usr/sbin/in.telnetd`	`telnet`-Dämon

Kerberos-Terminologie

Im folgenden Abschnitt werden die Kerberos-Begriffe und die dazugehörigen Definitionen aufgeführt. Diese Begriffe werden in der gesamten Kerberos-Dokumentation verwendet. Zum Nachvollziehen der Kerberos-Konzepte bedarf es eines grundlegenden Verständnisses dieser Begriffe.

Kerberos-spezifische Terminologie

Zur Verwaltung von KDCs müssen Sie die in diesem Abschnitt aufgeführten Begriffe verstehen.

Das *Key Distribution Center* oder *KDC* ist die für die Ausstellung von Berechtigungsnachweisen verantwortliche Komponente von Kerberos. Diese Berechtigungsnachweise werden anhand von in der KDC-Datenbank gespeicherten Informationen erstellt. Jeder Bereich benötigt mindestens zwei KDCs: ein Master- und wenigstens ein Slave-KDC. Alle KDCs generieren Berechtigungsnachweise, aber nur das Master-KDC kann Änderungen an der KDC-Datenbank verarbeiten.

Eine *Stash-Datei* enthält den Master-Schlüssel für das KDC. Dieser Schlüssel wird verwendet, wenn ein Server zur automatischen Authentifizierung des KDC vor dem Starten der Befehle `kadmind` und `krb5kdc` neu gestartet wird. Da diese Datei den Master-Schlüssel enthält, sollten die Datei und die zugehörigen Backups dauerhaft gesichert sein. Die Datei wird mit Leseberechtigungen für `root` erstellt. Ändern Sie die Berechtigungen nicht, damit die Datei dauerhaft gesichert bleibt. Wenn die Datei beeinträchtigt wird, könnte der Schlüssel zum Zugriff auf die KDC-Datenbank oder zum Ändern selbiger verwendet werden.

Authentifizierungsspezifische Terminologie

Das Verständnis des Authentifizierungsprozesses erfordert die Kenntnis der in diesem Abschnitt aufgeführten Begriffe. Programmierer und Systemadministratoren sollten mit diesen Begriffen vertraut sein.

Ein *Client* ist die auf einer Workstation eines Benutzers ausgeführte Software. Die auf dem Client ausgeführte Kerberos-Software erstellt sämtliche Anforderungen während dieses Vorgangs. Demnach ist es wichtig, zwischen den Aktionen dieser Software und denen des Benutzers zu unterscheiden.

Die Begriffe *server* und *service* werden häufig synonym verwendet. Genauer gesagt definiert der Begriff *Server* das physische System, auf dem die Kerberos-Software ausgeführt wird. Der Begriff *Service* bezieht sich dagegen auf eine bestimmte Funktion, die auf einem Server unterstützt wird (zum Beispiel `ftp` oder `nfs`). In der Dokumentation wird häufig von Servern als Teil eines Service gesprochen, aber diese Definition ist hinsichtlich der tatsächlichen Bedeutung der Begriffe sehr vage. Daher bezieht sich der Begriff *server* auf das physische System. Der Begriff *service* bezieht sich dagegen auf die Software.

Das Kerberos-Produkt verwendet zwei Typen von Schlüsseln. Bei einem Schlüsseltyp handelt es sich um einen Schlüssel, der vom Passwort abgeleitet wird. Dieser Schlüssel wird an jedes Benutzer-Hauptelement übergeben und ist nur dem Benutzer und dem KDC bekannt. Der andere vom Kerberos-Produkt verwendete Schlüsseltyp ist ein zufallsverteilter Schlüssel, der keinem Passwort zugewiesen ist und somit nicht für die Verwendung durch Benutzer-Hauptelemente geeignet ist. Zufallsverteilte Schlüssel werden üblicherweise für Service-Hauptelemente mit Einträgen in einer Schlüsseltabelle sowie für vom KDC generierte Sitzungsschlüssel verwendet. Service-Hauptelemente können zufallsverteilte Schlüssel verwenden, da der Service auf den Schlüssel in der Schlüsseltabelle zugreifen kann, wodurch er nicht interaktiv ausgeführt werden kann. Sitzungsschlüssel werden vom KDC generiert (und von Client und Service gemeinsam genutzt), um sichere Transaktionen zwischen einem Client und einem Service zu ermöglichen.

Ein *Ticket* ist ein Informationspaket, das zur sicheren Übergabe der Identität eines Benutzers an einen Server oder Service verwendet wird. Ein Ticket ist nur für einen einzigen Client und einen bestimmten Service auf einem spezifischen Server gültig. Ein Ticket enthält Folgendes:

- Hauptelementnamen des Service
- Hauptelementnamen des Benutzers
- IP-Adresse des Hosts des Benutzers
- Zeitstempel
- Wert, der die Lebensdauer des Tickets definiert
- Kopie des Sitzungsschlüssels

Alle dieser Daten werden im Serviceschlüssel des Servers verschlüsselt. Denken Sie daran, dass das KDC das Ticket eingebettet in einem Berechtigungsnachweis ausstellt, wie nachfolgend beschrieben. Nach der Ausstellung eines Tickets kann dieses solange wiederverwendet werden, bis es abläuft.

Ein *Berechtigungsnachweis* ist ein Paket von Informationen, das ein Ticket und einen passenden Sitzungsschlüssel enthält. Der Berechtigungsnachweis wird mit dem Schlüssel des anfordernden Hauptelements verschlüsselt. Üblicherweise generiert das KDC einen Berechtigungsnachweis als Antwort auf eine Ticketanforderung von einem Client.

Bei einem *Authentifizierer* handelt es sich um vom Server zur Authentifizierung des Benutzer-Hauptelements des Clients verwendete Informationen. Ein Authentifizierer schließt den Hauptelementnamen des Benutzers, einen Zeitstempel und weitere Daten mit ein. Im Unterschied zu einem Ticket kann ein Authentifizierer nur einmal verwendet werden. Dies geschieht normalerweise, wenn Zugriff auf einen Service angefordert wird. Ein Authentifizierer wird unter Verwendung des von Client und Server gemeinsam genutzten Sitzungsschlüssels verschlüsselt. Üblicherweise erstellt der Client den Authentifizierer und versendet ihn mit dem Ticket des Servers oder des Service, um den Server bzw. Service zu authentifizieren.

Typen von Tickets

Tickets haben Eigenschaften, die deren Verwendungsweise festlegen. Diese Eigenschaften werden dem Ticket bei der Erstellung zugewiesen. Sie können jedoch später geändert werden. So kann ein Ticket beispielsweise von einem `weiterleitbaren` zu einem `weitergeleiteten` Ticket geändert werden. Sie können die Eigenschaften eines Tickets mit dem Befehl `klist` anzeigen. Weitere Informationen finden Sie unter „Anzeigen von Kerberos-Tickets“ auf Seite 571.

Tickets können durch mindestens einen der folgenden Begriffe beschrieben werden:

Weiterleitbar/weitergeleitet	Ein weiterleitbares Ticket kann von einem Host an einen anderen gesendet werden, ohne dass sich ein Client erneut authentifizieren muss. Beispiel: Wenn der Benutzer `david` ein weiterleitbares Ticket abruft, während er sich am Rechner von `jennifer` befindet, kann er sich bei seinem eigenen Rechner anmelden, ohne dafür ein neues Ticket zu benötigen (und sich somit erneut authentifizieren zu müssen). Ein Beispiel für ein weiterleitbares Ticket finden Sie unter Beispiel 26–1.
Anfänglich	Ein anfängliches Ticket ist ein Ticket, das direkt und nicht auf Basis eines Ticket-gewährenden Tickets ausgestellt wird. Für einige Services, wie zum Beispiel Anwendungen zum Ändern von Passwörtern, kann es erforderlich sein, dass Tickets als anfängliche Tickets gekennzeichnet werden, um sicherzustellen, dass der Client Kenntnisse über den Geheimschlüssel unter Beweis stellen kann. Ein anfängliches Ticket gibt an, dass der Client sich kürzlich selbst authentifiziert hat, anstatt ein Ticket-gewährendes Ticket zu verwenden, das möglicherweise schon seit längerer Zeit vorhanden ist.
Ungültig	Bei einem ungültigen Ticket handelt es sich um ein nachdatiertes Ticket, das noch nicht verwendet werden kann. Ein ungültiges Ticket wird solange von einem Anwendungsserver abgewiesen, bis es validiert wird. Dazu muss ein Ticket nach Ablauf seiner Startzeit vom Client in einer Anforderung für einen Ticket-gewährenden Service an den KDC gesendet werden, wobei das Flag `VALIDATE` festgelegt sein muss.
Nachdatierbar/nachdatiert	Ein nachdatiertes Ticket ist ein Ticket, das erst eine bestimmte Zeit nach seiner Erstellung gültig wird. Ein solches Ticket eignet sich beispielsweise für Batch-Jobs, die spät nachts ausgeführt werden sollen, da das Ticket im Falle eines Diebstahls nicht verwendet werden kann, bis der Batch-Job

	ausgeführt werden muss. Wenn ein nachdatiertes Ticket ausgestellt wird, wird es als ungültig ausgestellt und bleibt dies auch solange, bis seine Startzeit abgelaufen ist und der Client die Validierung durch das KDC anfordert. Ein nachdatiertes Ticket ist normalerweise bis zur Ablaufzeit des Ticket-gewährenden Tickets gültig. Wenn das Ticket jedoch als erneuerbar gekennzeichnet wird, wird seine Lebensdauer normalerweise so festgelegt, dass sie der vollen Lebensdauer des Ticket-gewährenden Tickets entspricht.
Proxyfähig/Proxy	Gelegentlich ist es für ein Hauptelement erforderlich, einem Service die Ausführung eines Vorgangs in dessen Namen zu ermöglichen. Der Hauptelementname des Proxys muss bei der Erstellung des Tickets angegeben werden. Die Oracle Solaris-Version unterstützt keine proxyfähigen oder Proxy-Tickets. Ein proxyfähiges Ticket ähnelt einem weiterleitbaren Ticket, mit der Ausnahme, dass es nur für einen einzigen Service gültig ist, während ein weiterleitbares Ticket dem Service die vollständige Verwendung der Identität des Clients gewährleistet. Ein weiterleitbares Ticket kann daher als eine Art "Super-Proxy" angesehen werden.
Erneuerbar	Da Tickets mit besonders hoher Lebensdauer ein Sicherheitsrisiko darstellen, können Tickets als erneuerbar festgelegt werden. Ein erneuerbares Ticket hat zwei Ablaufzeiten: die Zeit, zu der die aktuelle Instanz des Tickets abläuft, und die maximale Lebensdauer für jedes Ticket, die eine Woche beträgt. Wenn ein Client ein Ticket weiterhin verwenden möchte, erneuert er es vor Ende der ersten Ablaufzeit. Beispiel: Ein Ticket kann für eine Stunde gültig sein, während alle Tickets eine maximale Lebensdauer von 10 Stunden aufweisen. Wenn der Client das Ticket für mehr als eine Stunde behalten möchte, muss er es innerhalb dieser Stunde erneuern. Erreicht ein Ticket die maximale Lebensdauer für Tickets von 10 Stunden, läuft es automatisch ab und kann nicht erneuert werden.

Informationen zum Anzeigen der Attribute von Tickets finden Sie unter „Anzeigen von Kerberos-Tickets“ auf Seite 571.

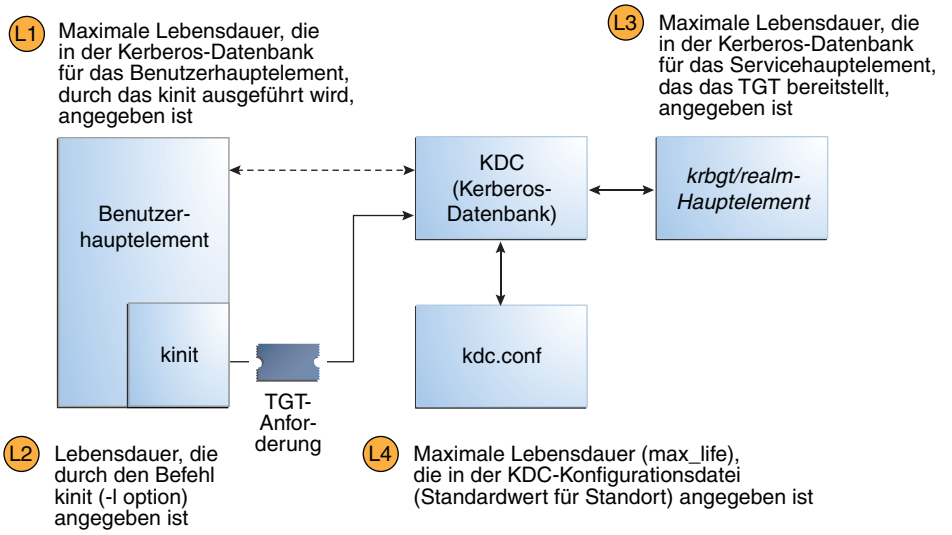
Lebensdauer von Tickets

Jedes Mal, wenn ein Hauptelement ein Ticket abruft, wird für die Lebensdauer des Tickets der kleinste der folgenden Lebensdauerwerte festgelegt (dies gilt auch für Ticket-gewährende Tickets):

- Der von der Option `-l` von `kinit` angegebene Lebensdauerwert, wenn das Ticket mit `kinit` abgerufen wird. Standardmäßig verwendete `kinit` den maximalen Lebensdauerwert.
- Der in der Datei `kdc.conf` angegebene maximale Lebensdauerwert (`max_life`)
- Der maximale Lebensdauerwert, der in der Kerberos-Datenbank für das Service-Hauptelement angegeben ist, das das Ticket bereitstellt. Bei `kinit` lautet das Service-Hauptelement `krbtgt/`*realm*.
- Der maximale Lebensdauerwert, der in der Kerberos-Datenbank für das Benutzer-Hauptelement angegeben ist, das das Ticket anfordert

Abbildung 27–1 zeigt, wie die Lebensdauer eines TGT (Ticket-gewährendes Ticket) bestimmt wird und woher die vier Lebensdauerwerte stammen. Zwar bezieht sich diese Abbildung explizit auf die Bestimmung der Lebensdauer eines TGT; der Vorgang beim Abrufen eines Tickets durch ein beliebiges Hauptelement ist jedoch fast der gleiche. Die einzigen Unterschiede liegen darin, dass `kinit` keinen Lebensdauerwert angibt, und das Service-Hauptelement, welches das Ticket bereitstellt, einen maximalen Lebensdauerwert angibt (anstelle des Hauptelements `krbtgt/` *realm*).

ABBILDUNG 27–1 Bestimmung der Lebensdauer eines TGT



Die erneuerbare Ticket-Lebensdauer wird ebenfalls aus dem Minimum von vier verschiedenen Werten bestimmt, jedoch werden in diesem Fall folgende erneuerbare Lebensdauerwerte verwendet:

- Der von der Option `-r` von `kinit` verwendete erneuerbare Lebensdauerwert, wenn das Ticket mit `kinit` abgerufen oder erneuert wird
- Der in der Datei `kdc.conf` angegebene maximale erneuerbare Lebensdauerwert (`max_renewable_life`)
- Der erneuerbare Wert für die maximale Lebensdauer, der in der Kerberos-Datenbank für das Service-Hauptelement angegeben ist, das das Ticket bereitstellt. Bei `kinit` lautet das Service-Hauptelement `krbtgt/`*realm*.
- Der erneuerbare Wert für die maximale Lebensdauer, der in der Kerberos-Datenbank für das Benutzer-Hauptelement angegeben ist, das das Ticket anfordert

Kerberos-Hauptelementnamen

Jedes Ticket wird durch einen Hauptelementnamen identifiziert. Der Hauptelementname kann einen Benutzer oder einen Service identifizieren. Im Folgenden sind Beispiele für verschiedene Hauptelementnamen aufgeführt.

TABELLE 27–4 Beispiele für Kerberos-Hauptelementnamen

Hauptelementname	Beschreibung
`changepw/kdc1.example.com@EXAMPLE.COM`	Ein Hauptelement für den Master-KDC-Server für den Zugriff auf das KDC, wenn Sie Passwörter ändern
`clntconfig/admin@EXAMPLE.COM`	Ein vom Installationsdienstprogramm `kclient` verwendetes Hauptelement
`ftp/boston.example.com@EXAMPLE.COM`	Ein vom Service `ftp` verwendetes Hauptelement. Dieses Hauptelement kann anstelle eines `host`-Hauptelements verwendet werden.
`host/boston.example.com@EXAMPLE.COM`	Ein von den kerberisierten Anwendungen (z. B. `klist` und `kprop`) und Services (z. B. `ftp` und `telnet`) verwendetes Hauptelement. Dieses Hauptelement wird als `host`- oder Service-Hauptelement bezeichnet. Es wird zur Authentifizierung von NFS-Einhängevorgängen verwendet. Dieses Hauptelement wird auch von einem Client verwendet, um zu überprüfen, ob das an den Client ausgestellte TGT vom richtigen KDC stammt.
`K/M@EXAMPLE.COM`	Das Hauptelement des Master-Schlüsselnamens. Jedem Master-KDC ist eines dieser Hauptelemente zugewiesen.
`kadmin/history@EXAMPLE.COM`	Ein Hauptelement mit einem Schlüssel zum Beibehalten von Passwortverläufen für andere Hauptelemente. Jedes Master-KDC verfügt über eines dieser Hauptelemente.
`kadmin/kdc1.example.com@EXAMPLE.COM`	Ein Hauptelement für den Master-KDC-Server für den Zugriff auf das KDC mit `kadmind`
`kadmin/changepw.example.com@EXAMPLE.COM`	Ein Hauptelement zum Akzeptieren von Anforderungen für Passwortänderungen von Clients, auf denen keine Oracle Solaris-Version ausgeführt wird
`krbtgt/EXAMPLE.COM@EXAMPLE.COM`	Dieses Hauptelement wird beim Generieren eines Ticket-gewährenden Tickets verwendet.
`krbtgt/EAST.EXAMPLE.COM@WEST.EXAMPLE.COM`	Dieses Hauptelement stellt ein Beispiel für ein bereichsübergreifendes Ticket-gewährendes Ticket dar.
`nfs/boston.example.com@EXAMPLE.COM`	Ein vom NFS-Service verwendetes Hauptelement. Dieses Hauptelement kann anstelle eines `host`-Hauptelements verwendet werden.
`root/boston.example.com@EXAMPLE.COM`	Ein dem `root`-Konto auf einem Client zugewiesenes Hauptelement. Dieses Hauptelement wird als `root`-Hauptelement bezeichnet und bietet `root`-Zugriff auf über NFS eingehängte Dateisysteme.
username`@EXAMPLE.COM`	Ein Hauptelement für einen Benutzer

TABELLE 27–4 Beispiele für Kerberos-Hauptelementnamen *(Fortsetzung)*

Hauptelementname	Beschreibung
username/admin@EXAMPLE.COM	Ein admin-Hauptelement zur Verwaltung der KDC-Datenbank

Funktionsweise des Kerberos-Authentifizierungssystems

Mithilfe von Anwendungen können Sie sich bei einem Remote-System anmelden, wenn Sie ein Ticket zum Nachweis Ihrer Identität und einen passenden Sitzungsschlüssel vorweisen können. Der Sitzungsschlüssel enthält Informationen, die speziell für den Benutzer und den Service gelten, auf den zugegriffen wird. Tickets und Sitzungsschlüssel werden vom KDC für alle Benutzer bei der ersten Anmeldung erstellt. Das Ticket und der passende Sitzungsschlüssel bilden einen Berechtigungsnachweis. Bei Verwendung mehrerer Netzwerkdienste kann ein Benutzer zahlreiche Berechtigungsnachweise erhalten. Er benötigt einen Berechtigungsnachweis für jeden Service, der auf einem bestimmten Server ausgeführt wird. Beispiel: Für den Zugriff auf den Service `ftp` auf dem Server `boston` ist ein Berechtigungsnachweis erforderlich. Der Zugriff auf den Service `ftp` auf einem anderen Server erfordert einen weiteren spezifischen Berechtungsnachweis.

Der Vorgang des Erstellens und Speicherns der Berechtigungsnachweise ist transparent. Berechtigungsnachweise werden von dem KDC erstellt, der den Berechtigungsnachweis an den Anforderer sendet. Bei Empfang wird der Berechtigungsnachweis in einem Berechtigungsnachweis-Cache gespeichert.

Interaktion des Kerberos-Service mit DNS und der Datei `nsswitch.conf`

Der Kerberos-Service wird kompiliert, um mithilfe von DNS Hostnamen auflösen zu können. Die Datei `nsswitch.conf` wird nicht konsultiert, wenn die Hostnamenauflösung abgeschlossen ist.

Erhalten von Zugriff auf einen Service mit Kerberos

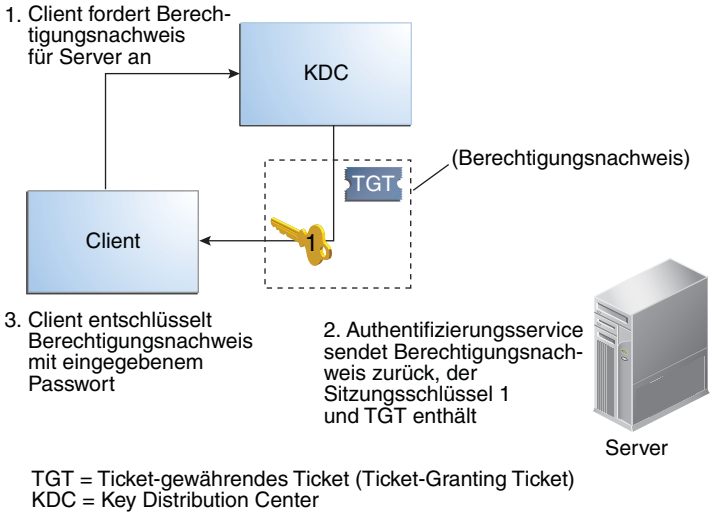
Für den Zugriff auf einen bestimmten Service benötigt der Benutzer zwei Berechtigungsnachweise. Der erste Berechtigungsnachweis ist für das TGT (Ticket-gewährende Ticket). Sobald der Ticket-gewährende Service diesen Berechtigungsnachweis entschlüsselt hat, erstellt er einen zweiten Berechtigungsnachweis für den Server, auf den der Benutzer Zugriff anfordert. Mit diesem zweiten Berechtigungsnachweis kann anschließend Zugriff auf den Service auf dem Server angefordert werden. Nachdem der Server den zweiten Berechtigungsnachweis erfolgreich entschlüsselt hat, erhält der Benutzer den Zugriff. In den folgenden Abschnitten wird dieser Vorgang ausführlicher beschrieben.

Abrufen eines Berechtigungsnachweises für den Ticket-gewährenden Service

1. Zum Starten des Authentifizierungsvorgangs sendet der Client eine Anforderung an den Authentifizierungsserver für ein bestimmtes Benutzer-Hauptelement. Diese Anforderung wird ohne Verschlüsselung gesendet. Da die Anforderung keine gesicherten Informationen enthält, ist eine Verschlüsselung nicht erforderlich.
2. Wenn der Authentifizierungsservice die Anforderung empfängt, wird der Hauptelementname des Benutzers in der KDC-Datenbank abgerufen. Entspricht ein Hauptelement dem Eintrag in der Datenbank, ruft der Authentifizierungsservice den privaten Schlüssel für dieses Hauptelement ab. Anschließend generiert der Authentifizierungsservice einen Sitzungsschlüssel für die Verwendung durch den Client und den Ticket-gewährenden Service (Sitzungsschlüssel 1) sowie ein Ticket für den Ticket-gewährenden Service (Ticket 1). Dieses Ticket wird auch als *Ticket-gewährendes Ticket* (TGT) bezeichnet. Sowohl der Sitzungsschlüssel als auch das Ticket werden mit dem privaten Schlüssel des Benutzers verschlüsselt und die Informationen werden zurück an den Client gesendet.
3. Der Client entschlüsselt mithilfe dieser Informationen Sitzungsschlüssel 1 und Ticket 1 unter Verwendung des privaten Schlüssels für das Benutzer-Hauptelement. Da der private Schlüssel nur dem Benutzer und der KDC-Datenbank bekannt ist, sind die Informationen im Paket sicher. Der Client speichert die Informationen im Berechtigungsnachweis-Cache.

Während dieses Vorgangs wird der Benutzer normalerweise zur Angabe eines Passworts aufgefordert. Wenn das vom Benutzer angegebene Passwort dem zur Erstellung des in der KDC-Datenbank gespeicherten privaten Schlüssels verwendeten Passwort entspricht, kann der Client die vom Authentifizierungsservice gesendeten Informationen erfolgreich entschlüsseln. Jetzt verfügt der Client über einen Berechtigungsnachweis für die Verwendung mit dem Ticket-gewährenden Service. Der Client kann nun einen Berechtigungsnachweis für einen Server anfordern.

ABBILDUNG 27–2 Abrufen eines Berechtigungsnachweises für den Ticket-gewährenden Service

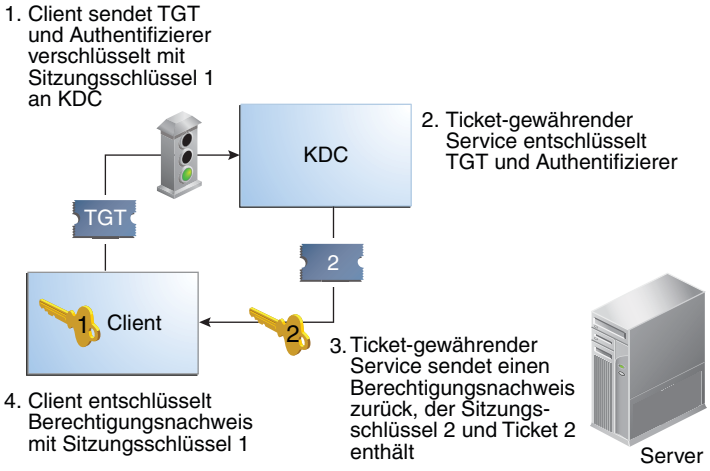


Abrufen eines Berechtigungsnachweises für einen Server

1. Zum Anfordern von Zugriff auf einen bestimmten Server muss ein Client zunächst den Berechtigungsnachweis für diesen Server vom Authentifizierungsservice anfordern. Weitere Informationen finden Sie unter „Abrufen eines Berechtigungsnachweises für den Ticket-gewährenden Service“ auf Seite 599. Der Client sendet dann eine Anforderung an den Ticket-gewährenden Service, die den Service-Hauptelementnamen, Ticket 1 und einen mit Sitzungsschlüssel 1 verschlüsselten Authentifizierer umfasst. Ticket 1 wurde ursprünglich vom Authentifizierungsservice unter Verwendung des Serviceschlüssels des Ticket-gewährenden Service verschlüsselt.
2. Da dem Ticket-gewährenden Service der Serviceschlüssel des Ticket-gewährenden Service bekannt ist, kann Ticket 1 entschlüsselt werden. Die in Ticket 1 enthaltenen Informationen umfassen Sitzungsschlüssel 1, sodass der Ticket-gewährende Service den Authentifizierer entschlüsseln kann. An diesem Punkt wird das Benutzer-Hauptelement mit dem Ticket-gewährenden Service authentifiziert.
3. Nach erfolgreichem Abschluss der Authentifizierung generiert der Ticket-gewährende Service einen Sitzungsschlüssel für das Benutzer-Hauptelement und den Server (Sitzungsschlüssel 2) sowie ein Ticket für den Server (Ticket 2). Sitzungsschlüssel 2 und Ticket 2 werden anschließend mithilfe von Sitzungsschlüssel 1 verschlüsselt. Da Sitzungsschlüssel 1 nur dem Client und dem Ticket-gewährenden Service bekannt ist, sind die entsprechenden Informationen gesichert und können risikofrei über das Netzwerk übertragen werden.

4. Erhält der Client dieses Informationspaket, entschlüsselt er die Informationen mithilfe von Sitzungsschlüssel 1, den er im Berechtigungsnachweis-Cache gespeichert hatte. Der Client hat einen Berechtigungsnachweis zur Verwendung mit dem Server abgerufen. Nun kann der Client Zugriff auf einen bestimmten Service auf diesem Server anfordern.

ABBILDUNG 27–3 Abrufen eines Berechtigungsnachweises für einen Server

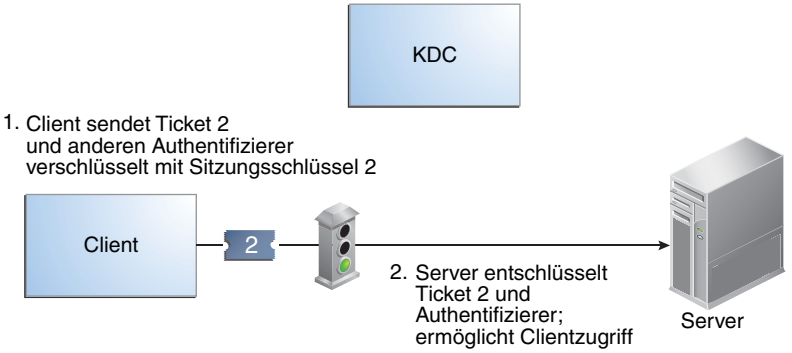


TGT = Ticket-gewährendes Ticket (Ticket-Granting Ticket)
KDC = Key Distribution Center

Abrufen von Zugriff auf einen bestimmten Service

1. Zum Anfordern von Zugriff auf einen bestimmten Service muss der Client zunächst einen Berechtigungsnachweis für den Ticket-gewährenden Service vom Authentifizierungsserver und einen Server-Berechtigungsnachweis vom Ticket-gewährenden Service anfordern. Weitere Informationen finden Sie unter „Abrufen eines Berechtigungsnachweises für den Ticket-gewährenden Service“ auf Seite 599 und „Abrufen eines Berechtigungsnachweises für einen Server“ auf Seite 600. Der Client kann dann eine Anforderung an den Server senden, die Ticket 2 und einen weiteren Authentifizierer umfasst. Der Authentifizierer wird mithilfe von Sitzungsschlüssel 2 verschlüsselt.
2. Ticket 2 wurde durch den Ticket-gewährenden Service mit dem Serviceschlüssel für den Service verschlüsselt. Da der Serviceschlüssel dem Service-Hauptelement bekannt ist, kann der Service Ticket 2 entschlüsseln und Sitzungsschlüssel 2 erhalten. Sitzungsschlüssel 2 kann dann zum Entschlüsseln des Authentifizierers verwendet werden. Wurde der Authentifizierer erfolgreich entschlüsselt, erhält der Client Zugriff auf den Service.

ABBILDUNG 27–4 Abrufen von Zugriff auf einen bestimmten Service



Verwenden von Kerberos-Verschlüsselungstypen

Verschlüsselungstypen identifizieren, welche kryptografischen Algorithmen bei kryptografischen Vorgängen verwendet werden sollen. Die Verschlüsselungstypen `aes` , `des3-cbc-sha1` und `rc4–hmac` ermöglichen die Erstellung von Schlüsseln, die für stärkere kryptografische Vorgänge verwendet werden können. Diese stärkeren Vorgänge erhöhen die Gesamtsicherheit des Kerberos-Service.

Hinweis – In Versionen vor &S10Update4 kann der Verschlüsselungstyp `aes1-cts-hmac-sha-96` mit dem Kerberos-Service verwendet werden, wenn die ungebündelten Strong Cryptographic-Pakete installiert sind.

Wenn ein Client ein Ticket vom KDC anfordert, muss das KDC Schlüssel verwenden, deren Verschlüsselungstyp sowohl mit dem Client als auch mit dem Server kompatibel ist. Während der Client mithilfe des Kerberos-Protokolls anfordern kann, dass das KDC bestimmte Verschlüsselungstypen für den Teil des Clients verwendet, der sich auf die Ticketantwort bezieht, ermöglicht das Protokoll dem Server nicht, Verschlüsselungstypen für das KDC anzugeben.

Hinweis – Wenn Sie ein Master-KDC installiert haben, das die Version Solaris 10 nicht ausführt, müssen Sie die Slave-KDCs vor der Aktualisierung des Master-KDC auf die Version Solaris 10 aktualisieren. Ein Master-KDC für Solaris 10 verwendet die neuen Verschlüsselungstypen, die von einem älteren Slave nicht verarbeitet werden können.

Nachfolgend werden einige der Probleme aufgeführt, die Sie vor dem Ändern der Verschlüsselungstypen berücksichtigen müssen.

- Das KDC geht davon aus, dass der erste dem Server-Hauptelementeintrag in der Hauptelement-Datenbank zugewiesene Schlüssel/Verschlüsselungstyp vom Server unterstützt wird.
- Auf dem KDC sollten Sie sicherstellen, dass die für das Hauptelement generierten Schlüssel mit den Systemen kompatibel sind, auf denen das Hauptelement authentifiziert wird. Standardmäßig erstellt der Befehl `kadmin` Schlüssel für alle unterstützten Verschlüsselungstypen. Wenn die Systeme, auf denen das Hauptelement verwendet wird, diesen Standardsatz von Verschlüsselungstypen nicht unterstützten, sollten Sie die Verschlüsselungstypen beim Erstellen eines Hauptelements einschränken. Sie können die Verschlüsselungstypen unter Verwendung des Flag `-e` in `kadmin addprinc` oder durch Festlegen des Parameters `supported_enctypes` in der Datei `kdc.conf` auf diese Teilmenge beschränken. Der Parameter `supported_enctypes` sollte verwendet werden, wenn die meisten Systeme in einem Kerberos-Bereich eine Teilmenge des Standardsatzes von Verschlüsselungstypen unterstützen. Durch Festlegen von `supported_enctypes` wird der Standardsatz von Verschlüsselungstypen angegeben, den `kadmin addprinc` bei der Erstellung eines Hauptelements für einen bestimmten Bereich verwendet. In der Regel eignen sich diese beiden Methoden am besten zum Festlegen der von Kerberos verwendeten Verschlüsselungstypen.
- Beim Bestimmen der von einem System unterstützten Verschlüsselungstypen müssen Sie sowohl die auf dem System ausgeführte Version von Kerberos als auch die kryptografischen Algorithmen berücksichtigen, die von der Serveranwendung unterstützt werden, für die ein Server-Hauptelement erstellt wird. So sollten Sie z. B. beim Erstellen eines `nfs/hostname`-Service-Hauptelements die Verschlüsselungstypen auf die von dem NFS-Server auf diesem Host unterstützten Typen beschränken. Beachten Sie, dass in der Version Solaris 10 alle unterstützten Kerberos-Verschlüsselungstypen auch vom NFS-Server unterstützt werden.
- Mithilfe des Parameters `master_key_enctype` in der Datei `kdc.conf` kann der Verschlüsselungstyp des Master-Schlüssels festgelegt werden, der die Einträge in der Hauptelement-Datenbank verschlüsselt. Verwenden Sie diesen Parameter nicht, wenn die KDC-Hauptelement-Datenbank bereits erstellt wurde. Mit dem Parameter `master_key_enctype` kann während der Erstellung der Datenbank der standardmäßige Verschlüsselungstyp des Master-Schlüssels `des-cbc-crc` in einen stärkeren Verschlüsselungstyp geändert werden. Stellen Sie beim Konfigurieren der Slave-KDCs sicher, dass alle Slave-KDCs den ausgewählten Verschlüsselungstyp unterstützen und denselben Eintrag für `master_key_enctype` in `kdc.conf` aufweisen. Vergewissern Sie sich außerdem, dass für `master_key_enctype` einer der Verschlüsselungstypen in `supported_enctypes` angegeben ist, wenn `supported_enctypes` in `kdc.conf` festgelegt ist. Eine falsche Vorgehensweise bezüglich dieser Punkte kann zur Folge haben, dass das Master-KDC nicht mit den Slave-KDCs funktioniert.
- Auf dem Client können Sie festlegen, welche Verschlüsselungstypen der Client anfordert, wenn er Tickets vom KDC durch ein Parameterpaar in `krb5.conf` erhält. Der Parameter `default_tkt_enctypes` gibt die Verschlüsselungstypen an, die der Client vorzugsweise beim Anfordern eines TGT (Ticket-gewährendes Ticket) vom KDC verwendet. Das TGT

wird vom Client verwendet, um weitere Servertickets auf effizientere Weise zu erhalten. Durch Festlegen von `default_tkt_enctypes` erhält der Client eine gewisse Kontrolle über die zum Schutz der Kommunikation zwischen Client und KDC verwendeten Verschlüsselungstypen, wenn er mit dem TGT ein Serverticket anfordert (in diesem Fall spricht man von einer TGS-Anforderung). Bedenken Sie, dass die in `default_tkt_enctypes` angegebenen Verschlüsselungstypen mit mindestens einem der Verschlüsselungstypen für Hauptelementschlüssel in der auf dem KDC gespeicherten Hauptelement-Datenbank übereinstimmen müssen. Andernfalls schlägt die TGT-Anforderung fehl. In den meisten Fällen empfiehlt es sich, `default_tkt_enctypes` nicht festzulegen, da dieser Parameter Interoperabilitätsprobleme nach sich ziehen kann. Standardmäßig fordert der Clientcode alle unterstützten Verschlüsselungstypen an und das KDC wählt die Verschlüsselungstypen basierend auf den Schlüsseln, die es in der Hauptelement-Datenbank auffindet.

- Der Parameter `default_tgs_enctypes` beschränkt die von den Clients in TGS-Anforderungen angeforderten Verschlüsselungstypen, mit denen Servertickets erhalten werden. Dieser Parameter schränkt ebenfalls die Verschlüsselungstypen ein, die das KDC beim Erstellen des Sitzungsschlüssels verwendet, den Client und Server gemeinsam nutzen. Wenn ein Client beispielsweise 3DES-Verschlüsselung nur bei sicherem NFS verwenden möchte, sollten Sie `default_tgs_enctypes` = `des3-cbc-sha1` festlegen. Stellen Sie sicher, dass die Client- und Server-Hauptelemente über einen `des-3-cbc-sha1`-Schlüssel in der Hauptelement-Datenbank verfügen. Ebenso wie bei `default_tkt_enctype` empfiehlt es sich meistens, den Parameter nicht festzulegen, da es zu Interoperabilitätsproblemen kommen kann, wenn die Berechtigungsnachweise auf KDC und Server nicht ordnungsgemäß eingerichtet sind.
- Auf dem Server können Sie die akzeptierten Verschlüsselungstypen mit `permitted_enctypes` in `kdc.conf` festlegen. Außerdem können Sie die bei der Erstellung von `keytab`-Einträgen verwendeten Verschlüsselungstypen angeben. Auch hier ist es in den meisten Fällen besser, keine der beiden Methoden zum Festlegen der Verschlüsselungstypen zu verwenden, sondern stattdessen die zu verwendeten Verschlüsselungstypen vom KDC bestimmen zu lassen, da das KDC nicht mit der Serveranwendung kommuniziert, um den zu verwendenden Schlüssel oder Verschlüsselungstyp zu bestimmen.

Verwenden der Tabelle `gsscred`

Wenn die Standardzuordnungen nicht ausreichen, wird die Tabelle `gsscred` von einem NFS-Server verwendet, wenn dieser versucht, einen Kerberos-Benutzer zu identifizieren. Der NFS-Service verwendet UNIX-IDs zum Identifizieren von Benutzern. Diese IDs sind nicht Teil eines Benutzer-Hauptelements oder eines Berechtigungsnachweises. Die Tabelle `gsscred` bietet zusätzliche Zuordnungen von GSS-Berechtigungsnachweisen zu UNIX-UIDs (aus der Passwortdatei). Die Tabelle muss nach dem Füllen der KDC-Datenbank erstellt und verwaltet werden. Weitere Informationen finden Sie unter „Zuordnen von GGS-Berechtigungsnachweisen zu UNIX-Berechtigungsnachweisen“ auf Seite 430.

Bei einer eingehenden Clientanforderung versucht der NFS-Service, den Namen des Berechtigungsnachweises einer UNIX-ID zuzuordnen. Schlägt die Zuordnung fehl, wird die Tabelle `gsscred` überprüft.

Wesentliche Unterschiede zwischen Oracle Solaris Kerberos und MIT Kerberos

Die Version Solaris 10 des Kerberos-Service basiert auf der Version 1.2.1 von MIT Kerberos. Nachfolgend werden die Erweiterungen der Version Solaris 10 aufgeführt, die nicht in MIT 1.2.1 enthalten sind:

- Kerberos-Unterstützung für Remote-Anwendungen von Oracle Solaris
- Inkrementelle Weitergabe für die KDC-Datenbank
- Client-Konfigurationsskript
- Lokalisierte Fehlermeldungen
- Unterstützung für BSM-Prüfdatensätze
- Threadsichere Verwendung von Kerberos mit GSS-API
- Verwendung von Encryption Framework für Kryptografie

Diese Version umfasst auch einige nachträgliche Fehlerbehebungen für MIT 1.2.1. Insbesondere wurden 1.2.5 btree-Fehlerbehebungen und 1.3 TCP-Unterstützung hinzugefügt.

TEIL VII

Prüfung bei Oracle Solaris

Dieser Abschnitt enthält Informationen zur Konfiguration, Verwaltung und Verwendung des Subsystems für die Oracle Solaris-Prüfung.

- Kapitel 28, „Prüfung bei Oracle Solaris (Übersicht)“
- Kapitel 29, „Planen der Oracle Solaris-Prüfung“
- Kapitel 30, „Verwalten der Oracle Solaris-Prüfung (Aufgaben)“
- Kapitel 31, „Prüfung bei Oracle Solaris (Referenz)“

◆ ◆ ◆ KAPITEL 28

Prüfung bei Oracle Solaris (Übersicht)

Bei der Oracle Solaris-Prüfung wird die Verwendung des Systems aufgezeichnet. Der Prüfservice bietet Tools für die Analyse der Prüfdaten.

In diesem Kapitel erhalten Sie eine Einführung zur Verwendung der Prüfung in Oracle Solaris. Im Folgenden ist eine Liste der Informationen in diesem Kapitel aufgeführt.

- „Was ist eine Prüfung?“ auf Seite 609
- „Wie funktioniert eine Prüfung?“ auf Seite 611
- „Welcher Zusammenhang besteht zwischen Prüfung und Sicherheit?“ auf Seite 612
- „Terminologie und Konzepte der Prüfung“ auf Seite 613
- „Prüfung auf Systemen mit Oracle Solaris-Zonen“ auf Seite 620
- „Erweiterungen der Prüffunktionen in der Solaris 10-Version“ auf Seite 621

Vorschläge zur Planung erhalten Sie unter Kapitel 29, „Planen der Oracle Solaris-Prüfung“. Vorgehensweisen zum Konfigurieren der Prüfung an Ihrem Standort finden Sie unter Kapitel 30, „Verwalten der Oracle Solaris-Prüfung (Aufgaben)“. Weitere Referenzinformationen erhalten Sie unter Kapitel 31, „Prüfung bei Oracle Solaris (Referenz)“.

Was ist eine Prüfung?

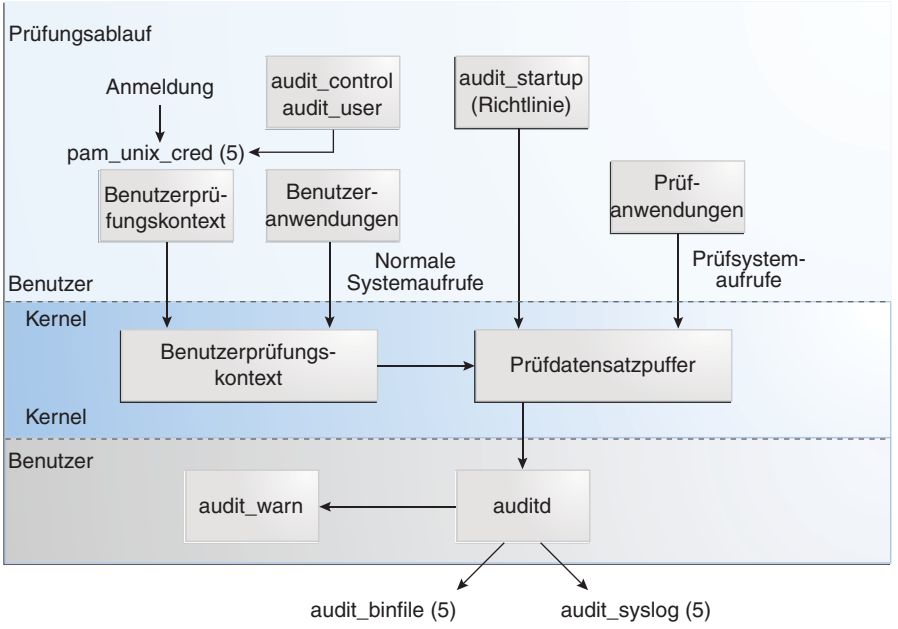
Bei der Prüfung werden Daten zur Nutzung der Systemressourcen erfasst. Die Prüfdaten enthalten einen Datensatz der sicherheitsrelevanten Systemereignisse. Anhand dieser Daten können Sie anschließend Verantwortung für die auf einem Host durchgeführten Aktionen feststellen. Eine erfolgreiche Prüfung beginnt mit zwei Sicherheitsfunktionen: Identifizierung und Authentifizierung. Nachdem ein Benutzer einen Benutzernamen und ein Passwort angegeben hat, wird bei jeder Anmeldung eine eindeutige Prüfsitzungs-ID generiert und dem Benutzerprozess zugewiesen. Die Prüfsitzungs-ID wird von allen während der Anmeldesitzung gestarteten Prozessen übernommen. Auch wenn ein Benutzer die Identität während einer Sitzung ändert, werden alle Aktionen mit der gleichen Prüfsitzungs-ID erfasst. Weitere Informationen zum Ändern der Identität erhalten Sie auf der Manpage su(1M).

Der Prüfservice ermöglicht Folgendes:

- Überwachen der auf einem Host durchgeführten sicherheitsrelevanten Ereignisse
- Aufzeichnen der Ereignisse in einem netzwerkweiten Prüfpfad
- Feststellen von falscher Verwendung oder unberechtigter Aktivität
- Überprüfen der Zugriffsmuster und des Zugriffsverlaufs der Personen und Objekte
- Feststellen von Umgehungsversuchen der Schutzmechanismen
- Festellen der übermäßigen Nutzung von Berechtigungen, wenn ein Benutzer die Identität ändert

Während der Systemkonfiguration legen Sie die zu überwachenden Klassen von Prüfdatensätzen fest. Außerdem können Sie den Grad der für die einzelnen Benutzer durchgeführten Prüfungen einstellen. In der folgenden Abbildung wird der Ablauf der Oracle Solaris-Prüfung ausführlich dargestellt.

ABBILDUNG 28–1 Ablauf der Prüfung



Nach dem Erfassen der Prüfdaten im Kernel werden die Daten durch Plugins an die entsprechenden Standorte verteilt. Anschließend können Sie mithilfe von Tools für die Nachauswahl die interessanten Abschnitte des Prüfpfads auswählen und untersuchen. Beispielsweise können Sie Prüfdatensätze bestimmter Benutzer oder Gruppen überprüfen. Sie

können alle Datensätze eines bestimmten Ereignistyps an einem bestimmten Tag untersuchen. Oder Sie können alle zu einem bestimmten Zeitpunkt des Tages generierten Datensätze auswählen.

Bei Systemen, auf denen nicht globale Zonen installiert sind, wird eine identische Prüfung aller Zonen über die globale Zone durchgeführt. Diese Systeme können so konfiguriert werden, dass sie verschiedene Datensätze in den nicht globalen Zonen erfassen. Weitere Informationen erhalten Sie unter „Prüfung und Oracle Solaris-Zonen“ auf Seite 702.

Wie funktioniert eine Prüfung?

Bei der Prüfung werden Prüfdatensätze generiert, wenn bestimmte Ereignisse auftreten. Normalerweise werden Prüfdatensätze unter anderem durch folgende Ereignisse generiert:

- Starten und Herunterfahren des Systems
- Anmelden und Abmelden
- Erstellen bzw. Löschen von Prozessen oder Erstellen bzw. Löschen von Threads
- Öffnen, Schließen, Erstellen, Löschen oder Umbenennen von Objekten
- Verwenden von Berechtigungsfunktionen oder rollenbasierter Zugriffssteuerung (Role-Based Access Control, RBAC)
- Identifizierungs- und Authentifizierungsaktionen
- Berechtigungsänderungen durch einen Prozess oder Benutzer
- Administrative Aktionen, z. B. Installieren eines Pakets
- Standortspezifische Anwendungen

Prüfdatensätze werden aus drei Quellen generiert:

- Durch eine Anwendung
- Als Ergebnis von Asynchrones Prüfereignis
- Als Ergebnis eines Prozesssystemaufrufs

Nach dem Erfassen werden die entsprechenden Informationen zum Ereignis in einem Prüfdatensatz formatiert. Der Datensatz wird anschließend in Prüfdateien geschrieben. Die abgeschlossenen Prüfdatensätze werden im binären Format gespeichert. Ab der Version Solaris 10 können Prüfdatensätze durch das Dienstprogramm `syslog` protokolliert werden.

Prüfdateien im binären Format können auf einem lokalen Dateisystem gespeichert werden. Die Dateien können ebenfalls auf den über NFS eingehängten Dateiservern gespeichert werden. Der Speicherort kann aus mehreren Partitionen auf dem gleichen System, Partitionen auf unterschiedlichen Systemen oder Partitionen von Systemen auf unterschiedlichen, aber verbundenen Netzwerken bestehen. Die gesamten miteinander verbundenen Prüfdateien werden als ein *Prüfpfad* bezeichnet. In den Prüfdatensätzen werden die Prüfdateien in

chronologischer Reihenfolge erfasst. Ein Prüfdatensatz enthält Informationen zu Identifizierung, Ursache und Zeitpunkt des Ereignisses sowie weitere entsprechende Informationen.

Prüfdatensätze können ebenfalls mithilfe des Dienstprogramms `syslog` überwacht werden. Diese Prüfprotokolle können lokal gespeichert werden. Oder die Protokolle können über das UDP-Protokoll an ein Remote-System gesendet werden. Weitere Informationen erhalten Sie unter „Prüfprotokolle“ auf Seite 617.

Welcher Zusammenhang besteht zwischen Prüfung und Sicherheit?

Die Prüfung von Oracle Solaris erkennt mögliche Sicherheitsverletzungen, indem verdächtige oder nicht ordnungsgemäße Systemnutzungsmuster festgestellt werden. Da durch die Oracle Solaris-Prüfung außerdem verdächtige Aktionen auf bestimmte Benutzer zurückverfolgt werden können, dient dies auch als Abschreckung. Wenn die Benutzer wissen, dass ihre Aktivitäten geprüft werden, vermeiden sie böswillige Aktionen.

Um ein Computersystem, insbesondere ein System in einem Netzwerk, zu schützen, müssen die Aktivitäten durch Mechanismen kontrolliert werden, bevor System- oder Benutzerprozesse gestartet werden. Für die Sicherheit sind Tools erforderlich, die die Aktivitäten während ihrer Ausführung überwachen. Außerdem sind für die Sicherheit Berichte der Aktivitäten erforderlich, nachdem diese aufgetreten sind. Bei der Erstkonfiguration der Oracle Solaris-Prüfung müssen Parameter festgelegt werden, bevor sich Benutzer anmelden oder Systemprozesse beginnen. Bei den Prüfaktivitäten werden normalerweise die aktuellen Ereignisse überwacht und die bestimmten Parametern entsprechenden Ereignisse gemeldet. Ausführliche Informationen zur Überwachung und Berichterstellung dieser Ereignisse durch die Oracle Solaris-Prüfung erhalten Sie unter Kapitel 29, „Planen der Oracle Solaris-Prüfung“ und Kapitel 30, „Verwalten der Oracle Solaris-Prüfung (Aufgaben)“.

Eine Prüfung verhindert jedoch keinen unberechtigten Zugriff durch Hacker. Jedoch kann der Prüfservice beispielsweise in einem Bericht erfassen, dass ein bestimmter Benutzer zu einem bestimmten Zeitpunkt bestimmte Aktionen durchgeführt hat. Im Prüfbericht kann der Benutzer durch Eingangspfad und Benutzernamen festgestellt werden. Diese Informationen können unmittelbar an das Terminal und eine Datei gesendet und zu einem späteren Zeitpunkt für eine Analyse verwendet werden. Durch die vom Prüfservice bereitgestellten Daten können Sie Folgendes feststellen:

- Wie die Systemsicherheit umgangen wurde
- Welche Sicherheitslücken geschlossen werden müssen, um die gewünschte Sicherheitsebene zu gewährleisten

Terminologie und Konzepte der Prüfung

Die folgenden Begriffe werden zur Beschreibung des Prüfservice verwendet. Einige Definitionen enthalten Verweise auf weitere ausführlichere Beschreibungen.

TABELLE 28–1 Begriffe der Oracle Solaris-Prüfung

Begriff	Definition
Prüfklasse	Eine Gruppe von Prüfereignissen. Durch Prüfklassen können Sie eine Gruppe von zu prüfenden Ereignissen auswählen. Weitere Informationen erhalten Sie unter „Prüfklassen und Vorauswahl“ auf Seite 615.
Prüfverzeichnis	Ein Repository der Prüfdateien im binären Format. Eine Beschreibung der Typen von Prüfverzeichnissen erhalten Sie unter „Prüfprotokolle“ auf Seite 617.
Prüfereignis	Eine sicherheitsrelevante Systemaktion, die geprüft wird. Um eine einfachere Auswahl zu ermöglichen, werden Ereignisse in Prüfklassen zusammengefasst. Eine Beschreibung der Systemaktionen, die geprüft werden können, finden Sie unter „Prüfereignisse“ auf Seite 614.
Prüfrichtlinie	Ein Satz von Prüfoptionen, der an Ihrem Standort aktiviert bzw. deaktiviert werden kann. Diese Optionen legen fest, ob bestimmte Prüfdaten aufgezeichnet werden. Außerdem kann durch diese Optionen angegeben werden, ob prüfbare Aktionen nicht aufgezeichnet werden sollen, wenn der Prüfpfad voll ist. Weitere Informationen erhalten Sie unter „Festlegen der Prüfrichtlinien“ auf Seite 629.
Prüfdatensatz	Prüfdaten, die in Prüfdateien gespeichert werden. Durch einen Prüfdatensatz wird ein einzelnes Prüfereignis beschrieben. Jeder Prüfdatensatz besteht aus Prüf-Token. Weitere Informationen zu Prüfdatensätzen erhalten Sie unter „Prüfdatensätze und Prüf-Token“ auf Seite 616.
Prüf-Token	Ein Feld in einem Prüfdatensatz oder -ereignis. Jedes Prüf-Token beschreibt ein Attribut in einem Prüfereignis, beispielsweise einen Benutzer, ein Programm oder anderes Objekt. Beschreibungen aller Prüf-Token erhalten Sie unter „Formate der Prüf-Token“ auf Seite 711.
Prüfpfad	Eine Sammlung von mindestens einer Prüfdatei, in der die Prüfdaten von allen Systemen gespeichert werden, auf denen der Prüfservice ausgeführt wird. Weitere Informationen erhalten Sie unter „Prüfpfad“ auf Seite 707.
Vorauswahl	Bei der Vorauswahl legen Sie die zu überwachenden Prüfklassen fest, bevor Sie den Prüfservice aktivieren. Die Prüfereignisse der im Voraus ausgewählten Prüfklassen werden im Prüfpfad angezeigt. Die nicht bei der Vorauswahl festgelegten Prüfklassen werden nicht geprüft und ihre Ereignisse werden nicht im Prüfpfad aufgezeichnet. Durch ein Tool für die Nachauswahl (Befehl `auditreduce`) werden die Datensätze aus dem Prüfpfad ausgewählt. Weitere Informationen erhalten Sie unter „Prüfklassen und Vorauswahl“ auf Seite 615.

TABELLE 28–1 Begriffe der Oracle Solaris-Prüfung *(Fortsetzung)*

Begriff	Definition
Öffentliche Objekte	Ein öffentliches Objekt ist eine Datei, deren Eigentümer der Benutzer `root` ist und für die öffentlicher Lesezugriff besteht. Beispiele für öffentliche Objekte sind die Dateien in den Verzeichnissen `/etc` und `/usr/bin`. Öffentliche Objekte werden nicht auf schreibgeschützte Ereignisse geprüft. Wenn beispielsweise die `file_read`-Prüfklasse (`fr`) im Voraus ausgewählt wurde, wird der Lesezugriff auf öffentliche Objekte nicht geprüft. Sie können die Standardeinstellung überschreiben, indem Sie die Prüfrichtlinienoption `public` ändern.
Prüf-Plugins	Module, die die Prüfdatensätze in der Kernel-Warteschlange an einen bestimmten Speicherort übertragen. Durch das Plugin `audit_binfile.so` werden binäre Prüfdateien (im Prüfpfad) erstellt. Durch das Plugin `audit_syslog.so` werden ausgewählte Prüfdatensätze für die Protokolle `syslog` gefiltert. Weitere Informationen erhalten Sie unter „Prüf-Plugin-Module“ auf Seite 617.

Prüfereignisse

Sicherheitsrelevante Systemaktionen können geprüft werden. Die prüfbaren Aktionen werden als *Prüfereignisse* bezeichnet. Prüfereignisse werden in der Datei `/etc/security/audit_event` aufgeführt. Jedes Prüfereignis wird in der Datei durch eine Ereignisnummer, einen symbolischen Namen, eine Kurzbeschreibung und den Satz der Prüfklassen, zu denen das Ereignis gehört, definiert. Weitere Informationen zur Datei `audit_event` erhalten Sie auf der Manpage `audit_event(4)`.

Durch den folgenden Eintrag wird beispielsweise das Prüfereignis für den Systemaufruf `exec()` definiert:

```
7:AUE_EXEC:exec(2):ps,ex
```

Wenn Sie für die Prüfung entweder die Prüfklasse `ps` oder `ex` im Voraus auswählen, werden die `exec()`-Systemaufrufe im Prüfpfad aufgezeichnet.

Bei der Oracle Solaris-Prüfung werden *zuweisbare* und *nicht zuweisbare* Ereignisse verarbeitet. Durch die Prüfrichtlinie werden Ereignisse in *synchrone* und *asynchrone* Ereignisse unterteilt. Dies wird im Folgenden beschrieben:

- **Zuweisbare Ereignisse**: Ereignisse, die einem Benutzer zugewiesen werden können. Da der Systemaufruf `exec()` einem Benutzer zugewiesen werden kann, wird er als zuweisbares Ereignis bezeichnet. Alle zuweisbaren Ereignisse werden als synchrone Ereignisse bezeichnet.
- **Nicht zuweisbare Ereignisse**: Ereignisse, die auf der Kernel-Interrupt-Ebene oder vor der Authentifizierung eines Benutzers auftreten. Durch die Prüfklasse `na` werden nicht zuweisbare Prüfereignisse verarbeitet. Das Booten des Systems ist beispielsweise ein nicht zuweisbares Ereignis. Die meisten nicht zuweisbaren Ereignisse sind asynchrone Ereignisse. Nicht zuweisbare Ereignisse, die über zugewiesene Prozesse verfügen, beispielsweise eine fehlgeschlagene Anmeldung, werden als synchrone Ereignisse bezeichnet.
- **Synchrone Ereignisse**: Ereignisse, die einem Prozess im System zugewiesen sind. Synchrone Ereignisse sind die Mehrzahl der Systemereignisse.
- **Asynchrone Ereignisse**: Ereignisse, die keinem Prozess zugewiesen sind. Daher sind keine Prozesse verfügbar, die blockiert oder zu einem späteren Zeitpunkt reaktiviert werden können. Das erstmalige Booten des Systems und Aufrufen bzw. Beenden von PROM sind Beispiele für asynchrone Ereignisse.

Wenn die Klasse, zu der ein Prüfereignis gehört, für die Prüfung im Voraus ausgewählt wird, wird das Ereignis im Prüfpfad aufgezeichnet. Beispiel: Wenn Sie die Prüfklassen `ps` und `na` für die Prüfung im Voraus auswählen, werden unter anderem die Ereignisse der `exec()`-Systemaufrufe und der System-Bootvorgänge im Prüfpfad aufgezeichnet.

Zusätzlich zu den durch den Oracle Solaris-Prüfservice definierten Prüfereignissen können auch Drittanbieteranwendungen Prüfereignisse generieren. Prüfereignisnummern von 32768 bis 65535 sind für Drittanbieteranwendungen verfügbar.

Prüfklassen und Vorauswahl

Jedes Prüfereignis gehört zu mindestens einer *Prüfklasse*. In Prüfklassen kann eine große Anzahl von Prüfereignissen zusammengefasst werden. Bei der *Vorauswahl* einer zu prüfenden Klasse geben Sie an, dass alle Ereignisse in dieser Klasse im Prüfpfad aufgezeichnet werden sollen. Die Vorauswahl kann für Ereignisse auf einem System und für die von einem bestimmten Benutzer eingeleiteten Ereignisse getroffen werden. Nachdem die Ausführung des Prüfservices gestartet wurde, können Sie Prüfklassen zu den im Voraus ausgewählten Klassen dynamisch hinzufügen oder von diesen entfernen.

- **Systemweite Vorauswahl**: Systemweite Standardeinstellungen für die Prüfung können Sie in den Zeilen `flags`, `naflags` und `plugin` der Datei `audit_control` angeben. Die Datei `audit_control` wird unter „Datei `audit_control`“ auf Seite 697 beschrieben. Weitere Informationen erhalten Sie auf der Manpage `audit_control(4)`.

- **Benutzerspezifische Vorauswahl**: Ergänzungen zu den systemweiten Standardeinstellungen für Prüfungen können Sie für bestimmte Benutzer in der Datenbank `audit_user` angeben.

  In der Maske für die Vorauswahl der Prüfung können Sie angeben, welche Klassen von Ereignissen für einen Benutzer geprüft werden. Die Maske für die Vorauswahl der Prüfung ist eine Kombination der systemweiten Standardeinstellungen und den für den Benutzer angegebenen Prüfklassen. Eine ausführliche Beschreibung erhalten Sie unter „Verarbeiten der Prüfungsmerkmale“ auf Seite 707.

  Die Datenbank `audit_user` kann lokal oder durch einen Naming Service verwaltet werden. Die Solaris Management Console bietet eine grafische Benutzeroberfläche für die Verwaltung der Datenbank. Weitere Informationen erhalten Sie auf der Manpage `audit_user(4)`.
- **Dynamische Vorauswahl**: Geben Sie Prüfklassen als Argumente zum Befehl `auditconfig` an, um diese Prüfklassen zu einem Prozess oder einer Sitzung hinzuzufügen oder sie von dort zu entfernen. Weitere Informationen erhalten Sie auf der Manpage `auditconfig(1M)`.

Durch einen Befehl für die Nachauswahl wie `auditreduce` können Sie Datensätze aus den im Voraus ausgewählten Prüfdatensätzen auswählen. Weitere Informationen finden Sie unter „Untersuchen des Prüfpfads“ auf Seite 620 und auf der Manpage `auditreduce(1M)`.

Prüfklassen werden in der Datei `/etc/security/audit_class` definiert. Ein Eintrag gibt für die Klasse die Prüfmaske, den Namen und beschreibenden Namen an. Die Klassendefinitionen `ps` und `na` werden beispielsweise in der Datei `audit_class` wie folgt angezeigt:

```
0x00100000:ps:process start/stop
0x00000400:na:non-attribute
```

Es gibt 32 mögliche Prüfklassen. Zu den Klassen zählen zwei globale Klassen: `all` und `no`. Die Prüfklassen werden auf der Manpage `audit_class(4)` beschrieben.

Die Zuordnung von Prüfereignissen zu Klassen kann konfiguriert werden. Sie können Ereignisse von einer Klasse entfernen, zu einer Klasse hinzufügen und eine neue Klasse für ausgewählte Ereignisse erstellen. Weitere Informationen zur Vorgehensweise erhalten Sie unter „So ändern Sie die Klassenmitgliedschaft eines Prüfereignisses“ auf Seite 647.

Prüfdatensätze und Prüf-Token

In einem *Prüfdatensatz* wird das Auftreten eines geprüften Ereignisses aufgezeichnet. Der Datensatz enthält Informationen wie die Person der durchgeführten Aktion, die betroffenen Dateien, die versuchte Aktion sowie Ort und Zeitpunkt der aufgetretenen Aktion. Das folgende Beispiel zeigt einen `login`-Prüfdatensatz:

```
header,81,2,login - local,,2003-10-13 11:23:31.050 -07:00
subject,root,root,other,root,other,378,378,0 0 example_system
text,successful login
return,success,0
```

Die Art der für ein Prüfereignis gespeicherten Informationen wird durch einen Satz von *Prüf-Token* definiert. Wenn ein Prüfdatensatz für ein Ereignis erstellt wird, enthält der Datensatz einige oder alle der für das Ereignis definierten Token. Der Ereignistyp bestimmt, welche Token aufgezeichnet werden. Im folgenden Beispiel beginnt jede Zeile mit dem Namen des Prüf-Tokens. Der Inhalt des Prüf-Tokens wird nach dem Namen angezeigt. Die vier Prüf-Token bilden zusammen den Prüfdatensatz `login`.

Eine ausführliche Beschreibung der Struktur der einzelnen Prüf-Token sowie ein Beispiel der Ausgabe `praudit` finden Sie unter „Formate der Prüf-Token“ auf Seite 711. Eine Beschreibung des binären Stream von Prüf-Token finden Sie auf der Manpage `audit.log(4)`.

Prüf-Plugin-Module

Sie können Prüf-Plugin-Module für die Verarbeitung der Datensätze angeben, die durch die Vorauswahl in die Prüfwarteschlange gestellt wurden. Die Plugins sind Einträge in der Datei `audit_control`.

- Plugin `audit_binfile.so`: Verarbeitet die Bereitstellung der Prüfwarteschlange an die binären Prüfdateien. Wenn in der Datei `audit_control` kein Plugin und für den Eintrag `dir` ein Wert angegeben wurde, verwendet der Prüfdämon dieses Plugin.
- Plugin `audit_syslog.so`: Verarbeitet die Bereitstellung der ausgewählten Datensätze von der Prüfwarteschlange an die Protokolle `syslog`

Weitere Informationen zur Syntax der Datei `audit_control` finden Sie auf der Manpage `audit_control(4)`. Beispiele erhalten Sie in den Aufgaben unter „Konfigurieren der Prüfdateien (Übersicht der Schritte)“ auf Seite 638.

Weitere Informationen zu den Plugins erhalten Sie auf den Manpages `audit_binfile(5)`, `audit_syslog(5)` und `audit_control(4)`.

Prüfprotokolle

Die Prüfdatensätze werden in Prüfprotokollen erfasst. Die Oracle Solaris-Prüfung bietet zwei Ausgabemethoden für Prüfprotokolle. Protokolle, die als *Prüfdateien* bezeichnet werden, speichern Prüfdatensätze im binären Format. Der Satz an Prüfdateien von einem System oder Standort enthält einen vollständigen Prüfdatensatz. Der vollständige Prüfdatensatz wird als *Prüfpfad* bezeichnet.

Durch das Dienstprogramm `syslog` werden Zusammenfassungen in Textversion des Prüfdatensatzes erfasst und gespeichert. Ein `syslog`-Datensatz ist nicht vollständig. Das folgende Beispiel zeigt einen `syslog`-Eintrag für einen `login`-Prüfdatensatz:

```
Oct 13  11:24:11 example_system auditd: [ID 6472 audit.notice] \
        login - login ok session 378 by root as root:other
```

Die Prüfdatensätze können in beiden Formaten an einem Standort gespeichert werden. Sie können die Systeme an Ihrem Standort so konfigurieren, dass der binäre Modus, der `syslog`-Modus oder beide Modi verwendet werden. In der folgenden Tabelle werden die binären Prüfdatensätze mit den `syslog`-Prüfdatensätzen verglichen.

TABELLE 28–2 Vergleich zwischen binären Prüfdatensätzen und `syslog`-Prüfdatensätzen

Funktion	Binäre Datensätze	`syslog`-Datensätze
Protokoll	Schreibt in Dateisystem	Verwendet UDP für Remote-Protokollierung
Datentyp	Binär	Text
Datensatzlänge	Keine Begrenzung	Bis zu 1024 Zeichen pro Prüfdatensatz
Speicherort	Auf lokaler Festplatte und in den über NFS eingehängten Verzeichnissen	In einem durch die Datei `syslog.conf` angegebenen Speicherort
Konfiguration	Bearbeiten der Datei `audit_control` und Schützen und Einhängen über NFS von Prüfverzeichnissen	Bearbeiten der Dateien `audit_control` und `syslog.conf`
Lesevorgang	Normalerweise im Batch-Modus Browserausgabe in XML	In Echtzeit oder bei Suche durch die für `syslog` erstellten Skripten Nur-Text-Ausgabe
Vollständigkeit	Vollständigkeit und Anzeige in richtiger Reihenfolge wird garantiert	Keine Vollständigkeit garantiert
Zeitstempel	Greenwich Mean Time (GMT)	Zeitpunkt auf dem geprüften System

Die binären Datensätze gewährleisten die höchstmögliche Sicherheit. Die binäre Ausgabe erfüllt die Anforderungen der Sicherheitszertifikate wie CAPP (Common Criteria Controlled Access Protection Profile). Die Datensätze werden in ein Dateisystem geschrieben, das Sie vor Lesezugriff von anderen Personen schützen. Auf einem einzelnen System werden alle binären Datensätze erfasst und in der entsprechenden Reihenfolge angezeigt. Der GMT-Zeitstempel in binären Protokollen ermöglicht einen präzisen Vergleich, wenn Systeme in einem Prüfpfad über verschiedene Zeitzonen verteilt sind. Durch den Befehl `praudit -x` können Sie die Datensätze in einem Browser im XML-Format anzeigen. Außerdem können Sie mithilfe von Skripten die XML-Ausgabe analysieren.

Die `syslog`-Datensätze bieten stattdessen eine höhere Benutzerfreundlichkeit und Flexibilität. Beispielsweise können Sie die `syslog`-Daten aus verschiedenen Quellen erfassen. Wenn Sie die Ereignisse `audit.notice` in der Datei `syslog.conf` überwachen, wird durch das Dienstprogramm `syslog` eine Prüfdatensatz-Zusammenfassung mit dem aktuellen Zeitstempel gespeichert. Sie können die gleichen Tools für die Verwaltung und Analyse verwenden, die Sie

für `syslog`-Meldungen aus verschiedenen Quellen entwickelt haben, beispielsweise Workstations, Server, Firewalls und Router. Die Datensätze können in Echtzeit angezeigt und auf einem Remote-System gespeichert werden.

Indem Sie Prüfdatensätze mithilfe von `syslog.conf` an entfernten Speicherorten speichern, können Sie verhindern, dass die Protokolldaten von Angreifern geändert oder gelöscht werden. Andererseits sind die an einem entfernten Standort gespeicherten Prüfdatensätze anfällig für Netzwerkangriffe wie Denial-of-Service-Angriffe und gefälschte Quelladressen. Außerdem kann UDP Pakete ablegen oder Pakete in einer anderen Reihenfolge übermitteln. Die `syslog`-Einträge sind auf 1024 Zeichen beschränkt, daher können einige Prüfdatensätze im Protokoll abgeschnitten werden. Bei einem einzelnen System werden nicht alle Prüfdatensätze erfasst. Die Datensätze werden möglicherweise nicht in der richtigen Reihenfolge angezeigt. Da jeder Prüfdatensatz mit einem Zeitstempel aus Datum und Uhrzeit des lokalen Systems versehen ist, können Sie durch den Zeitstempel keinen Prüfpfad für mehrere Systeme erstellen.

Weitere Informationen zu Prüfprotokollen erhalten Sie in der folgenden Dokumentation:

- Manpage `audit_syslog`(5)
- Manpage `audit.log`(4)
- „So konfigurieren Sie `syslog`-Prüfprotokolle“ auf Seite 641

Speichern des Prüfpfads

In einem *Prüfverzeichnis* sind die Prüfdateien im binären Format gespeichert. Normalerweise werden bei einer Installation mehrere Prüfverzeichnisse verwendet. Der Inhalt aller Prüfverzeichnisse bildet den *Prüfpfad*. Prüfdatensätze werden in Prüfverzeichnissen in der folgenden Reihenfolge gespeichert:

- **Primäres Prüfverzeichnis**: Ein Verzeichnis, in dem Prüfdateien für ein System normalerweise gespeichert werden
- **Sekundäres Prüfverzeichnis**: Ein Verzeichnis, in dem Prüfdateien für ein System gespeichert werden, wenn das primäre Prüfverzeichnis voll oder nicht verfügbar ist
- **Reserveverzeichnis**: Ein lokales Prüfverzeichnis, das verwendet wird, wenn das primäre Prüfverzeichnis und alle sekundären Prüfverzeichnisse nicht verfügbar sind

Die Verzeichnisse werden in der Datei `audit_control` angegeben. Nur wenn ein in der Liste zuerst genanntes Verzeichnis voll ist, wird das nächste Verzeichnis verwendet. Eine mit Anmerkungen versehene `audit_control`-Datei, die eine Liste der Verzeichniseinträge enthält, finden Sie unter Beispiel 30–3.

Indem Sie die Prüfdateien im standardmäßigen Stammverzeichnis für die Prüfung ablegen, erleichtern Sie die Aufgaben des Prüfers ("Audit Review") beim Prüfen des Prüfpfads. Der Befehl `auditreduce` verwendet das Stammverzeichnis für die Prüfung, um nach allen Dateien im Prüfpfad zu suchen. Das standardmäßige Stammverzeichnis für die Prüfung lautet `/etc/security/audit`. Dieses Verzeichnis ist symbolisch verknüpft mit `/var/audit`.

Prüfdateien in Verzeichnissen mit dem Namen `/var/audit/` *hostname*`/files` können über den Befehl `auditreduce` einfach gefunden werden. Weitere Informationen erhalten Sie unter „Befehl `auditreduce`“ auf Seite 691.

Untersuchen des Prüfpfads

Der Prüfservice bietet Befehle, mit denen Sie die Dateien im Prüfpfad kombinieren und entfernen können. Mit dem Befehl `auditreduce` können Sie Prüfdateien im Prüfpfad kombinieren. Außerdem können Sie mit dem Befehl Dateien filtern, um nach bestimmten Ereignissen zu suchen. Durch den Befehl `praudit` werden die binären Dateien gelesen. Mit den Optionen für den Befehl `praudit` erhalten Sie eine Ausgabe, die sich für Skripten und Browseranzeige eignet.

Prüfung auf Systemen mit Oracle Solaris-Zonen

Eine Zone ist eine virtualisierte Betriebssystemumgebung, die durch eine einzelne Instanz von Oracle Solaris-Betriebssystem erstellt wird. Durch den Prüfservice wird das gesamte System geprüft, einschließlich der Aktivitäten in Zonen. Auf einem System, auf dem nicht globale Zonen installiert sind, kann ein einzelner Prüfservice ausgeführt werden, um eine identische Prüfung für alle Zonen durchzuführen. Stattdessen kann auch ein Prüfservice pro Zone konfiguriert werden, einschließlich der globalen Zone.

Wenn an einem Standort die folgenden Bedingungen erfüllt sind, kann ein einzelner Prüfservice ausgeführt werden:

- An dem Standort ist ein Prüfpfad auf einem einzelnen Image erforderlich.
- Die nicht globalen Zonen werden als Anwendungs-Container verwendet. Die Zonen sind Teil einer administrativen Domain. Das bedeutet, dass nicht globale Zonen über keine angepassten Naming Service-Dateien verfügen.

  Wenn sich alle Zonen in einem System in einer administrativen Domain befinden, können Sie mit der Prüfrichtlinie `zonename` die Prüfereignisse unterscheiden, die in unterschiedlichen Zonen ausgeführt werden.
- Die Administratoren möchten den Aufwand von Prüfungen so gering wie möglich halten. Der Administrator für die globale Zone führt eine identische Prüfung für alle Zonen durch. Außerdem bedient der Prüfdämon der globalen Zone alle Zonen im System.

Wenn an einem Standort die folgenden Bedingungen erfüllt sind, kann ein Prüfservice pro Zone ausgeführt werden:

- Der Standort erfordert keinen Prüfpfad auf einem einzelnen Image.
- Die nicht globalen Zonen verfügen über angepasste Naming Service-Dateien. Diese separaten administrativen Domains dienen normalerweise als Server.

- Die Administratoren der einzelnen Zonen möchten die Prüfung in den von ihnen verwalteten Zonen steuern. Bei einer Prüfung nach Zonen können die Zonenadministratoren entscheiden, ob die Prüfung für die von ihnen verwaltete Zone aktiviert oder deaktiviert werden soll.

Die Vorteile einer Prüfung nach Zonen sind ein angepasster Prüfpfad für jede Zone und die Möglichkeit zum Deaktivieren der Prüfung für einzelne Zonen. Diese Vorteile werden durch einen erhöhten administrativen Aufwand möglicherweise wieder aufgehoben. Der Zonenadministrator passt die einzelnen Prüfkonfigurationsdateien an. Bei jeder Zone wird ein eigener Prüfdämon ausgeführt. Außerdem verfügt jede Zone über eine eigene Prüfwarteschlange und Prüfprotokolle. Die Prüfprotokolldateien der Zone müssen verwaltet werden.

Erweiterungen der Prüffunktionen in der Solaris 10-Version

Ab der Version Solaris 9 sind folgende Funktionen für die Prüfung verfügbar:

- Bei der Prüfung können die Prüfdatensätze mit dem Dienstprogramm `syslog` im Textformat gespeichert werden. Weitere Informationen erhalten Sie unter „Prüfprotokolle“ auf Seite 617. Weitere Informationen zum Einrichten der Datei `audit_control` für die Verwendung des Dienstprogramms `syslog` finden Sie unter „So konfigurieren Sie `syslog`-Prüfprotokolle“ auf Seite 641.
- Für den Befehl `praudit` steht XML als zusätzliches Ausgabeformat zur Verfügung. XML ist ein standardmäßiges, portables, verarbeitbares Format. XML bedeutet, dass die Ausgabe auch in einem Browser gelesen und als Quelle für das XML-Scripting zur Berichterstellung genutzt werden kann. Die Option `-x` für den Befehl `praudit` wird unter „Befehl `praudit`“ auf Seite 693 beschrieben.
- Der Standardsatz der Prüfklassen wurde umstrukturiert. Metaklassen sind übergeordnete Klassen für spezifischere Prüfklassen. Eine Liste des Standardsatzes an Klassen erhalten Sie unter „Definitionen der Prüfklassen“ auf Seite 703.
- Die Verwendung der Tastenkombination Stop-A wird durch den Befehl `bsmconv` nicht mehr deaktiviert. Das Ereignis Stop-A kann geprüft werden.
- Der Zeitstempel in Prüfdatensätzen wird im ISO 8601-Format bereitgestellt. Weitere Informationen zum Standard erhalten Sie unter `http://www.iso.org`.
- Drei Optionen für Prüfrichtlinien sind jetzt verfügbar:
  - **public**: Öffentliche Objekte werden nicht mehr auf schreibgeschützte Ereignisse geprüft. Wenn öffentliche Dateien nicht geprüft werden, verringert sich die Größe des Prüfprotokolls erheblich. Etwaige Versuche, auf wichtige Dateien zuzugreifen, lassen sich folglich leichter überwachen. Weitere Informationen zu öffentlichen Objekten erhalten Sie unter „Terminologie und Konzepte der Prüfung“ auf Seite 613.

- **perzone**: Die Richtlinie `perzone` hat umfangreiche Auswirkungen. Dabei wird in jeder Zone ein separater Prüfdämon ausgeführt. Der Dämon verwendet speziell für die Zone geltende Prüfkonfigurationsdateien. Auch die Prüfwarteschlange gilt speziell für die Zone. Weitere Informationen erhalten Sie auf den Manpages `auditd`(1M) und `auditconfig`(1M). Weitere Informationen zu Zonen erhalten Sie unter „Prüfung und Oracle Solaris-Zonen“ auf Seite 702. Weitere Informationen zu Richtlinien erhalten Sie unter „So planen Sie die Prüfung der Zonen“ auf Seite 624.
- **zonename**: Der Name der Oracle Solaris-Zone, in der ein Prüfereignis aufgetreten ist, kann zu den Prüfdatensätzen hinzugefügt werden. Weitere Informationen zu Zonen erhalten Sie unter „Prüfung und Oracle Solaris-Zonen“ auf Seite 702. Weitere Informationen zur Verwendung der Option erhalten Sie unter „Festlegen der Prüfrichtlinien“ auf Seite 629.

- Es sind jetzt fünf Prüf-Token verfügbar:
  - Das Token `cmd` zeichnet die Liste der Argumente und die Liste der einem Befehl zugewiesenen Umgebungsvariablen auf. Weitere Informationen erhalten Sie unter „Token `cmd`“ auf Seite 715.
  - Das Token `path_attr` zeichnet die Abfolge der Attributdateiobjekte auf, die unterhalb des Token-Objekts `path` angeordnet sind. Weitere Informationen erhalten Sie unter „Token `path_attr`“ auf Seite 722.
  - Das Token `privilege` zeichnet die Verwendung der Berechtigung bei einem Prozess auf. Weitere Informationen erhalten Sie unter „Token `privilege`“ auf Seite 722.
  - Das Token `uauth` zeichnet die Verwendung der Autorisierung bei einem Befehl oder einer Aktion auf. Weitere Informationen erhalten Sie unter „Token `uauth`“ auf Seite 729.
  - Das Token `zonename` zeichnet den Namen der nicht globalen Zone auf, in der ein Prüfereignis aufgetreten ist. Die Option für die Prüfrichtlinie `zonename` bestimmt, ob das Token `zonename` im Prüfdatensatz enthalten sein soll. Weitere Informationen erhalten Sie unter „Token `zonename`“ auf Seite 729.

    Weitere Informationen zur Referenz erhalten Sie unter „Prüfung und Oracle Solaris-Zonen“ auf Seite 702. Weitere Informationen zu Zonen finden Sie in Teil II, „Zonen“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.

◆ ◆ ◆ KAPITEL 29

Planen der Oracle Solaris-Prüfung

In diesem Kapitel wird beschrieben, wie Sie den Prüfservice für die Oracle Solaris-Installation einrichten. Insbesondere werden in diesem Kapitel Themen besprochen, die Sie vor dem Aktivieren des Prüfservice beachten sollten. Im Folgenden sind die Informationen zur Planung in diesem Kapitel aufgeführt:

- „Planen der Oracle Solaris-Prüfung (Übersicht der Schritte)“ auf Seite 623
- „Festlegen der Prüfrichtlinien“ auf Seite 629
- „Steuerung des Prüfungsaufwands“ auf Seite 633
- „Effiziente Prüfung“ auf Seite 635

Eine Übersicht zur Prüfung erhalten Sie unter Kapitel 28, „Prüfung bei Oracle Solaris (Übersicht)“. Vorgehensweisen zum Konfigurieren der Prüfung an Ihrem Standort finden Sie unter Kapitel 30, „Verwalten der Oracle Solaris-Prüfung (Aufgaben)“. Weitere Referenzinformationen erhalten Sie unter Kapitel 31, „Prüfung bei Oracle Solaris (Referenz)“.

Planen der Oracle Solaris-Prüfung (Übersicht der Schritte)

In der folgenden Übersicht sind die wichtigsten Schritte aufgeführt, die für die Planung des Festplattenspeichers und der aufzuzeichnenden Ereignisse erforderlich sind.

Aufgabe	Anweisungen
Festlegen der Prüfstrategie für nicht globale Zonen	„So planen Sie die Prüfung der Zonen“ auf Seite 624
Planen des Speicherplatzes für den Prüfpfad	„So planen Sie Speicherplatz für Prüfdatensätze“ auf Seite 626
Festlegen der zu prüfenden Personen und Objekte	„So planen Sie die zu prüfenden Personen und Objekte“ auf Seite 627

Planen der Oracle Solaris-Prüfung (Aufgaben)

Zwar möchten Sie nur bestimmte Aktivitäten prüfen, aber dennoch nützliche Informationen während der Prüfung erfassen. Der verfügbare Speicherplatz kann durch die steigende Größe der Prüfdateien schnell belegt werden. Ordnen Sie daher ausreichend Festplattenspeicher zu. Gehen Sie bei der Planung der zu prüfenden Personen und Objekte sorgfältig vor.

▼ So planen Sie die Prüfung der Zonen

Wenn das System über implementierte Zonen verfügt, sind für die Konfiguration der Prüfung zwei Möglichkeiten verfügbar:

- Sie können einen Prüfservice in der globalen Zone für alle Zonen konfigurieren.
- Es kann ein Prüfservice pro Zone konfiguriert werden.

Weitere Informationen erhalten Sie unter „Prüfung auf Systemen mit Oracle Solaris-Zonen“ auf Seite 620.

- **Wählen Sie eine der folgenden Methoden.**

  - **OPTION 1 - Konfigurieren eines einzigen Prüfservice für alle Zonen**

    Durch eine identische Prüfung aller Zonen kann ein Prüfpfad auf einem einzelnen Image erstellt werden. Ein Prüfpfad auf einem einzelnen Image ist vorhanden, wenn alle Zonen in einem System Teil einer administrativen Domain sind. Die Prüfdatensätze können dann einfach verglichen werden, da die Datensätze in jeder Zone mit den gleichen Einstellungen im Voraus ausgewählt werden.

    Bei dieser Konfiguration werden alle Zonen als Teil eines Systems behandelt. In der globalen Zone wird der einzige Prüfdämon im System ausgeführt, und es werden Prüfprotokolle für jede Zone erfasst. Die Prüfkonfigurationsdateien werden nur in der globalen Zone angepasst; anschließend werden die Prüfkonfigurationsdateien in jede nicht globale Zone kopiert.

    a. **Kopieren Sie die Datei `audit_control` von der globalen Zone in jede nicht globale Zone.**

    b. **Verwenden Sie die gleiche `audit_user`-Datenbank für jede Zone.**

       Die `audit_user`-Datenbank kann eine lokale Datei darstellen oder über einen gemeinsam genutzten Naming Service zur Verfügung gestellt werden.

    c. **Legen Sie fest, dass die Prüfdatensätze pro Zone ausgewählt werden können.**

       Um den Zonennamen als Teil des Prüfdatensatzes zu verwenden, legen Sie die Richtlinie `zonename` in der globalen Zone fest. Der Befehl `auditreduce` kann anschließend Prüfereignisse pro Zone aus dem Prüfpfad auswählen. Ein Beispiel dazu finden Sie auf der Manpage `auditreduce(1M)`.

Weitere Informationen zur Planung eines Prüfpfads auf einem einzelnen Image finden Sie unter „So planen Sie die zu prüfenden Personen und Objekte“ auf Seite 627. Beginnen Sie mit dem ersten Schritt. Der Administrator der globalen Zone muss ebenfalls Speicherplatz zur Verfügung stellen (siehe Beschreibung unter „So planen Sie Speicherplatz für Prüfdatensätze“ auf Seite 626).

- **OPTION 2 - Konfigurieren eines Prüfservice pro Zone**

  Konfigurieren Sie die Prüfung pro Zone, wenn die verschiedenen Zonen über unterschiedliche Naming Service-Dateien verfügen oder wenn Zonenadministratoren die Prüfung in ihren Zonen steuern möchten.

  - Wenn Sie eine zonenweise Prüfung konfigurieren, müssen Sie eine Konfiguration der globalen Zone für die Prüfung durchführen. Die Prüfrichtlinie `perzone` wird in der globalen Zone eingerichtet. Weitere Informationen zum Einrichten der Prüfrichtlinie finden Sie unter „So konfigurieren Sie eine zonenweise Prüfung“ auf Seite 663.

    Hinweis – Wenn Naming Service-Dateien in nicht globalen Zonen angepasst werden und die Richtlinie `perzone` nicht festgelegt ist, müssen Sie bei der Verwendung der Tools für die Prüfung sorgfältig vorgehen, um die verwendbaren Datensätze auszuwählen. Eine Benutzer-ID in einer Zone kann auf einen anderen Benutzer über die gleiche ID in einer anderen Zone verweisen.

  - Um Datensätze zu generieren, die auf die ursprüngliche Zone zurückverfolgt werden können, legen Sie die Prüfrichtlinie `zonename` in der globalen Zone fest. Führen Sie in der globalen Zone den Befehl `auditreduce` mit der Option `zonename` aus. Führen Sie anschließend in der Zone `zonename` den Befehl `praudit` in der Ausgabe `auditreduce` aus.
  - Die jeweiligen Zonenadministratoren konfigurieren die Prüfdateien für die Zone.

    Ein Administrator für nicht globale Zonen kann alle Richtlinienoptionen mit Ausnahme von `perzone` und `ahlt` festlegen.
  - Die Zonenadministratoren können die Prüfung in der Zone aktivieren oder deaktivieren.

  Wenn Sie die Prüfkonfigurationsdateien in den jeweiligen Zonen anpassen möchten, gehen Sie wie unter „So planen Sie die zu prüfenden Personen und Objekte“ auf Seite 627 beschrieben vor, um die Planung für jede Zone durchzuführen. Sie können den ersten Schritt überspringen. Die jeweiligen Zonenadministratoren müssen ebenfalls Speicherplatz für die einzelnen Zonen bereitstellen (siehe Beschreibung unter „So planen Sie Speicherplatz für Prüfdatensätze“ auf Seite 626).

▼ So planen Sie Speicherplatz für Prüfdatensätze

Für den Prüfpfad ist ein dedizierter Dateibereich erforderlich. Der dedizierte Dateibereich für Prüfdateien muss verfügbar und sicher sein. Jedes System muss über verschiedene Prüfverzeichnisse verfügen, die für Prüfdateien konfiguriert sind. Legen Sie als eine der ersten Aufgaben fest, wie die Prüfverzeichnisse konfiguriert werden sollen, bevor Sie die Prüfung auf einem System aktivieren. Im folgenden Verfahren werden die Schritte für die Planung des Prüfpfad-Speicherplatzes beschrieben.

Bevor Sie beginnen Wenn Sie nicht globale Zonen implementieren, führen Sie zunächst die Schritte unter „So planen Sie die Prüfung der Zonen“ auf Seite 624 aus, bevor Sie dieses Verfahren durchführen.

1. **Legen Sie fest, wie ausführlich die Prüfung an Ihrem Standort durchgeführt werden soll.**

   Wägen Sie die Sicherheitsanforderungen Ihres Standorts mit der Verfügbarkeit des Festplattenspeichers für den Prüfpfad ab.

   Weitere Informationen zur Verringerung der Speicherplatzanforderungen bei gleichzeitiger Gewährleistung der Sicherheit am Standort sowie zum Einrichten von Prüfspeicherplatz finden Sie unter „Steuerung des Prüfungsaufwands“ auf Seite 633 und „Effiziente Prüfung“ auf Seite 635.

2. **Legen Sie fest, welche Systeme geprüft werden sollen.**

   Ordnen Sie auf diesen Systemen Speicherplatz für mindestens ein lokales Prüfverzeichnis zu. Weitere Informationen zum Angeben der Prüfverzeichnisse finden Sie unter Beispiel 30–3.

3. **Legen Sie fest, auf welchen Systemen Prüfdateien gespeichert werden sollen.**

   Geben Sie an, auf welchen Servern die primären und sekundären Prüfverzeichnisse gespeichert werden sollen. Beispiele zum Konfigurieren der Festplatten für Prüfverzeichnisse finden Sie unter „So erstellen Sie Partitionen für Prüfdateien“ auf Seite 649.

4. **Legen Sie die Namen der Prüfverzeichnisse fest.**

   Erstellen Sie eine Liste aller Prüfverzeichnisse, die Sie verwenden möchten. Richtlinien zur Benennung finden Sie unter „Speichern des Prüfpfads“ auf Seite 619 und „Befehl `auditreduce`“ auf Seite 691.

5. **Legen Sie fest, welche Prüfverzeichnisse von welchen Systemen verwendet werden sollen.**

   Erstellen Sie eine Map, auf der dargestellt ist, welches Prüfverzeichnis von welchem System verwendet wird. Mithilfe der Map können Sie die Prüfaktivitäten ausgleichen. Eine Beschreibung finden Sie unter Abbildung 31–1 und Abbildung 31–2.

▼ So planen Sie die zu prüfenden Personen und Objekte

Bevor Sie beginnen Wenn Sie nicht globale Zonen implementieren, führen Sie zunächst die Schritte unter „So planen Sie die Prüfung der Zonen“ auf Seite 624 aus, bevor Sie dieses Verfahren durchführen.

1 Legen Sie fest, ob ein Prüfpfad auf einem einzelnen System-Image verwendet werden soll.

Bei Systemen in einer einzelnen administrativen Domain kann ein Prüfpfad auf einem einzelnen System-Image erstellt werden. Wenn die Systeme unterschiedliche Naming Services verwenden, beginnen Sie mit dem nächsten Schritt. Schließen Sie die restlichen Schritte für die Planung der einzelnen Systeme ab.

Bei einem Prüfpfad auf einem einzelnen System-Image werden die zu prüfenden Systeme als ein Rechner behandelt. Um einen Prüfpfad auf einem einzelnen System-Image für einen Standort zu erstellen, konfigurieren Sie alle Systeme in der Installation wie folgt:

- Verwenden Sie den gleichen Naming Service.

  Für die Interpretierung der Prüfdatensätze werden zwei Befehle verwendet: `auditreduce` und `praudit`. Damit die Prüfdatensätze ordnungsgemäß interpretiert werden, müssen die Dateien `passwd`, `hosts` und `audit_user` einheitlich sein.
- Verwenden Sie die gleichen Dateien `audit_warn`, `audit_event`, `audit_class` und `audit_startup` auf allen Systemen.
- Verwenden Sie die gleiche `audit_user`-Datenbank. Die Datenbank kann sich in einem Naming Service wie NIS oder LDAP befinden.
- Verwenden Sie identische Einträge `flags`, `naflags` und `plugin` in der Datei `audit_control`.

2 Legen Sie die Prüfrichtlinie fest.

Verwenden Sie den Befehl `auditconfig -lspolicy`, um eine kurze Beschreibung der verfügbaren Richtlinienoptionen anzuzeigen. Standardmäßig ist nur die Richtlinie `cnt` aktiviert. Eine ausführliche Beschreibung erhalten Sie unter Schritt 8.

Die Auswirkungen der Richtlinienoptionen werden unter „Festlegen der Prüfrichtlinien“ auf Seite 629 beschrieben. Weitere Informationen zum Festlegen von Prüfrichtlinien finden Sie unter „So konfigurieren Sie die Prüfrichtlinie“ auf Seite 653.

3 Legen Sie fest, ob die Zuordnungen zwischen Ereignissen und Klassen geändert werden sollen.

In vielen Fällen ist die Standardzuordnung ausreichend. Wenn jedoch neue Klassen hinzugefügt, Klassendefinitionen geändert oder der Datensatz eines bestimmten Systemaufrufs als nicht hilfreich eingestuft werden, müssen Sie möglicherweise ein Ereignis in eine andere Klasse verschieben.

Ein Beispiel finden Sie unter „So ändern Sie die Klassenmitgliedschaft eines Prüfereignisses“ auf Seite 647.

4 **Legen Sie fest, welche Prüfklassen im Voraus ausgewählt werden sollen.**

Der optimale Zeitpunkt zum Hinzufügen der Prüfklassen oder Ändern der Standardklassen ist vor dem Starten des Prüfservice.

Die Prüfklassenwerte der Einträge `flags`, `naflags` und `plugin` in der Datei `audit_control` gelten für alle Benutzer und Prozesse. Die im Voraus ausgewählten Klassen bestimmen, ob eine Prüfklasse auf Erfolg, auf Fehler oder beides geprüft wird.

Weitere Informationen zur Vorauswahl der Prüfklassen finden Sie unter „So ändern Sie die Datei `audit_control`“ auf Seite 639.

5 **Legen Sie Benutzerausnahmen für die systemweiten im Voraus ausgewählten Prüfklassen fest.**

Wenn einige Benutzer von den systemweiten im Voraus ausgewählten Prüfklassen unterschiedlich geprüft werden sollen, ändern Sie die Einträge der einzelnen Benutzer in der Datenbank `audit_user`.

Ein Beispiel finden Sie unter „So ändern Sie die Prüfmerkmale eines Benutzers“ auf Seite 644.

6 **Legen Sie den freien Festplattenspeicher fest, der mindestens verfügbar sein soll.**

Wenn der Prozentsatz des Festplattenspeichers eines Prüfdateisystems unterhalb des Wertes `minfree` fällt, wechselt der Dämon `auditd` zum nächsten verfügbaren Prüfverzeichnis. Der Dämon sendet eine Warnung, dass der untere Grenzwert überschritten wurde.

Weitere Informationen zum Festlegen des freien Festplattenspeichers, der mindestens verfügbar sein soll, finden Sie unter Beispiel 30–4.

7 **Legen Sie fest, wie der E-Mail-Alias `audit_warn` verwaltet werden soll.**

Das Skript `audit_warn` wird ausgeführt, wenn Sie das Prüfsystem über eine Situation benachrichtigt, für die administrative Maßnahmen erforderlich sind. Standardmäßig sendet das Skript `audit_warn` eine E-Mail an den Alias `audit_warn` und eine Meldung an die Konsole.

Weitere Informationen zum Einrichten des Alias erhalten Sie unter „So konfigurieren Sie den E-Mail-Alias `audit_warn`“ auf Seite 653.

8 **Legen Sie die durchzuführende Aktion fest, wenn alle Prüfverzeichnisse voll sind.**

Wenn der Prüfpfad voll ist, funktioniert das System weiterhin. Das System zählt die übersprungenen Prüfdatensätze, zeichnet die Ereignisse jedoch nicht auf. Eine höhere Sicherheit erhalten Sie, indem Sie die Richtlinie `cnt` deaktivieren und die Richtlinie `ahlt` aktivieren. Durch die Richtlinie `ahlt` wird das System angehalten, wenn ein asynchrones Ereignis nicht zur Prüfwarteschlange hinzugefügt werden kann.

Eine Beschreibung dieser Richtlinienoptionen erhalten Sie unter „Prüfrichtlinien für asynchrone und synchrone Ereignisse“ auf Seite 632. Weitere Informationen zur Konfiguration dieser Richtlinienoptionen finden Sie unter Beispiel 30–16.

9 **Legen Sie fest, ob Prüfdatensätze im binären Format, im `syslog`-Format oder in beiden Formaten erfasst werden sollen.**

Eine Übersicht der Informationen finden Sie unter „Prüfprotokolle“ auf Seite 617.

Ein Beispiel finden Sie unter „So konfigurieren Sie `syslog`-Prüfprotokolle“ auf Seite 641.

Festlegen der Prüfrichtlinien

Die Prüfrichtlinie bestimmt die Merkmale der Prüfdatensätze für das lokale System. Die Richtlinienoptionen werden vom Startskript festgelegt. Das Skript `bsmconv`, durch das der Prüfservice aktiviert wird, erstellt das Skript `/etc/security/audit_startup`. Das Skript `audit_startup` führt den Befehl `auditconfig` aus, um die Prüfrichtlinie festzulegen. Weitere Informationen zum Skript erhalten Sie auf der Manpage `audit_startup(1M)`.

Die meisten Prüfrichtlinienoptionen sind standardmäßig deaktiviert, damit der Bedarf an Speicherplatz und Systemverarbeitung so gering wie möglich gehalten wird. Mit dem Befehl `auditconfig` können Sie Prüfrichtlinienoptionen dynamisch aktivieren oder deaktivieren. Mit dem Skript `audit_startup` können Sie Richtlinienoptionen dauerhaft aktivieren oder deaktivieren.

Stellen Sie anhand der folgenden Tabelle fest, ob die Anforderungen an Ihrem Standort den zusätzlichen Aufwand rechtfertigen, der durch Aktivieren von mindestens einer Prüfrichtlinienoption entstehen würde.

TABELLE 29–1 Auswirkungen der Prüfrichtlinienoptionen

Richtlinienname	Beschreibung	Warum sollte die Richtlinienoption geändert werden?
`ahlt`	Diese Richtlinie gilt nur für asynchrone Ereignisse. Bei deaktivierter Richtlinie kann das Ereignis abgeschlossen werden, ohne dass ein Prüfdatensatz generiert wird. Bei aktivierter Richtlinie wird das System angehalten, wenn die Prüfdateisysteme voll sind. Administrative Maßnahmen sind erforderlich, um die Prüfwarteschlange zu bereinigen, Speicherplatz für Prüfdatensätze zur Verfügung zu stellen und einen Neustart durchzuführen. Diese Richtlinie kann nur in der globalen Zone aktiviert werden. Die Richtlinie wirkt sich auf alle Zonen aus.	Die Deaktivierung eignet sich, wenn die Systemverfügbarkeit Vorrang vor der Sicherheit hat. Die Aktivierung eignet sich bei einer Umgebung, in der die Sicherheit sehr wichtig ist.

TABELLE 29–1 Auswirkungen der Prüfrichtlinienoptionen *(Fortsetzung)*

Richtlinienname	Beschreibung	Warum sollte die Richtlinienoption geändert werden?
`arge`	Bei deaktivierter Richtlinie sind die Umgebungsvariablen eines ausgeführten Programms nicht im Prüfdatensatz `exec` enthalten. Bei aktivierter Richtlinie werden die Umgebungsvariablen eines ausgeführten Programms zum Prüfdatensatz `exec` hinzugefügt. Der entstandene Prüfdatensatz enthält ausführlichere Informationen als bei deaktivierter Richtlinie.	Bei Deaktivierung werden weniger Informationen erfasst als bei Aktivierung. Die Aktivierung eignet sich, wenn die Prüfung für wenige Benutzer durchgeführt wird. Die Option eignet sich, wenn Sie die in den `exec`-Programmen verwendeten Umgebungsvariablen als nicht vertrauenswürdig betrachten.
`argv`	Bei deaktivierter Richtlinie sind die Argumente eines ausgeführten Programms nicht im Prüfdatensatz `exec` enthalten. Bei aktivierter Richtlinie werden die Argumente eines ausgeführten Programms zum Prüfdatensatz `exec` hinzugefügt. Der entstandene Prüfdatensatz enthält ausführlichere Informationen als bei deaktivierter Richtlinie.	Bei Deaktivierung werden weniger Informationen erfasst als bei Aktivierung. Die Aktivierung eignet sich, wenn die Prüfung für wenige Benutzer durchgeführt wird. Diese Option eignet sich ebenfalls, wenn Sie der Meinung sind, dass ungewöhnliche Programme des Typs `exec` ausgeführt werden.
`cnt`	Wenn diese Richtlinie deaktiviert ist, wird die Ausführung eines Benutzers oder einer Anwendung verhindert. Die Blockierung tritt ein, wenn keine Prüfdatensätze zum Prüfpfad hinzugefügt werden können, da kein freier Festplattenspeicherplatz verfügbar ist. Wenn diese Richtlinie deaktiviert ist, wird dieses Ereignis abgeschlossen, ohne dass ein Prüfdatensatz generiert wird. Die Richtlinie erfasst, wie viele Prüfdatensätze übersprungen wurden.	Die Deaktivierung eignet sich bei einer Umgebung, in der die Sicherheit sehr wichtig ist. Die Aktivierung eignet sich, wenn die Systemverfügbarkeit Vorrang vor der Sicherheit hat.
`group`	Wenn diese Richtlinie deaktiviert ist, wird keine Gruppenliste zu den Prüfdatensätzen hinzugefügt. Wenn die Richtlinie aktiviert ist, wird eine Gruppenliste zu jedem Prüfdatensatz als ein spezielles Token hinzugefügt.	Die Deaktivierung eignet sich normalerweise, um die Sicherheitsanforderungen eines Standorts zu erfüllen. Die Aktivierung eignet sich, wenn Sie prüfen möchten, durch welche Gruppen Prüfereignisse generiert werden.
`path`	Wenn diese Richtlinie deaktiviert ist, erfolgen die Aufzeichnungen in einem Prüfdatensatz in höchstens einem während des Systemaufrufs verwendeten Pfad. Wenn diese Richtlinie aktiviert ist, erfolgen die Aufzeichnungen in jedem mit einem Prüfereignis verwendeten Pfad in allen Prüfdatensätzen.	Durch die Deaktivierung wird höchstens ein Pfad in einem Prüfdatensatz eingefügt. Durch die Aktivierung wird jeder während eines Systemaufrufs verwendete Dateiname oder Pfad im Prüfdatensatz als ein `path`-Token hinzugefügt.

TABELLE 29–1 Auswirkungen der Prüfrichtlinienoptionen *(Fortsetzung)*

Richtlinienname	Beschreibung	Warum sollte die Richtlinienoption geändert werden?
`perzone`	Wenn diese Richtlinie deaktiviert ist, wird eine einzelne Prüfkonfiguration für ein System verwendet. Ein Prüfdämon wird in der globalen Zone ausgeführt. Prüfereignisse in nicht globalen Zonen können im Prüfdatensatz festgestellt werden, indem das Prüf-Token `zonename` im Voraus ausgewählt wird. Wenn diese Richtlinie aktiviert ist, werden separate Prüfkonfiguration, Prüfwarteschlange und Prüfprotokolle für jede Zone verwendet. Eine separate Version des Prüfdämons wird in jeder Zone ausgeführt. Diese Richtlinie kann nur in der globalen Zone aktiviert werden.	Die Deaktivierung eignet sich, wenn kein bestimmter Grund für ein separates Prüfprotokoll, eine Prüfwarteschlange und einen Dämon für die einzelnen Zonen vorliegt. Die Aktivierung eignet sich, wenn Sie das System nicht effizient überwachen können, indem Sie einfach das Prüf-Token `zonename` im Voraus auswählen.
`public`	Bei deaktivierter Richtlinie werden keine schreibgeschützten Ereignisse von öffentlichen Objekten zum Prüfpfad hinzugefügt, wenn der Lesezugriff auf die Dateien im Voraus ausgewählt wurde. Prüfklassen, die schreibgeschützte Ereignisse enthalten, sind beispielsweise `fr`, `fa` und `cl`. Bei aktivierter Richtlinie werden alle schreibgeschützten Prüfereignisse öffentlicher Objekte aufgezeichnet, wenn eine geeignete Prüfklasse im Voraus ausgewählt wurde.	Die Deaktivierung eignet sich normalerweise, um die Sicherheitsanforderungen eines Standorts zu erfüllen. Die Aktivierung ist nur in seltenen Fällen geeignet.
`seq`	Wenn diese Richtlinie deaktiviert ist, wird keine Sequenznummer zu den Prüfdatensätzen hinzugefügt. Wenn diese Richtlinie aktiviert ist, wird eine Sequenznummer zu den Prüfdatensätzen hinzugefügt. Die Sequenznummer ist im Token `sequence` enthalten.	Die Deaktivierung ist ausreichend, wenn die Prüfung problemlos verläuft. Die Aktivierung eignet sich, wenn die Richtlinie `cnt` aktiviert ist. Mit der Richtlinie `seq` können Sie feststellen, ob Daten verworfen wurden.
`trail`	Wenn diese Richtlinie deaktiviert ist, wird kein `trailer`-Token zu den Prüfdatensätzen hinzugefügt. Wenn diese Richtlinie aktiviert ist, wird ein `trailer`-Token zu den Prüfdatensätzen hinzugefügt.	Durch die Deaktivierung verringert sich die Größe des Prüfdatensatzes. Durch die Aktivierung wird das Ende jedes Prüfdatensatzes mit einem `trailer`-Token gekennzeichnet. Das Token `trailer` wird oft im Zusammenhang mit dem Token `sequence` verwendet. Das Token `trailer` ermöglicht eine einfachere und präzisere Neusynchronisierung der Prüfdatensätze.
`zonename`	Wenn diese Richtlinie deaktiviert ist, wird kein `zonename`-Token zu den Prüfdatensätzen hinzugefügt. Wenn diese Richtlinie aktiviert ist, wird ein `zonename`-Token zu allen Prüfdatensätzen von einer nicht globalen Zone hinzugefügt.	Die Deaktivierung eignet sich, wenn Sie das Prüfverhalten der Zonen nicht miteinander vergleichen möchten. Die Aktivierung eignet sich, wenn Sie das Prüfverhalten der Zonen feststellen und vergleichen möchten.

Prüfrichtlinien für asynchrone und synchrone Ereignisse

Durch die Richtlinien `ahlt` und `cnt` werden die durchzuführenden Aktionen festgelegt, wenn die Prüfwarteschlange voll ist und keine weiteren Ereignisse speichern kann. Die Richtlinien sind unabhängig und miteinander verbunden. Die Kombination der Richtlinien hat folgende Auswirkungen:

- `-ahlt +cnt` ist die standardmäßige Richtlinie, die übersprungen wird. Diese Standardwerte ermöglichen die Verarbeitung eines geprüften Ereignisses, auch wenn das Ereignis nicht protokolliert werden kann.

  Die Richtlinie `-ahlt` legt fest, dass, wenn ein Prüfdatensatz eines asynchronen Ereignisses nicht zur Kernel-Prüfwarteschlange hinzugefügt werden kann, das System die Anzahl der Ereignisse zählt und die Verarbeitung fortsetzt. In der globalen Zone wird durch den Zähler `as_dropped` die Anzahl aufgezeichnet.

  Die Richtlinie `+cnt` legt fest, dass, wenn ein synchrones Ereignis eintritt und nicht zur Kernel-Prüfwarteschlange hinzugefügt werden kann, das System das Ereignis zählt und die Verarbeitung fortsetzt. Der Zähler `as_dropped` der Zone erfasst die Anzahl.

  Die Konfiguration `-ahlt +cnt` wird normalerweise an Standorten verwendet, an denen die Verarbeitung fortgesetzt werden muss, auch wenn durch das Fortsetzen der Verarbeitung die Prüfdatensätze verloren gehen könnten. Das Feld `auditstatdrop` zeigt die Anzahl der Prüfdatensätze, die in einer Zone übersprungen wurden.

- Die Richtlinie `+ahlt -cnt` legt fest, dass die Verarbeitung angehalten wird, wenn ein Ereignis nicht zur Kernel-Prüfwarteschlange hinzugefügt werden kann.

  Die Richtlinie `+ahlt` legt fest, dass, wenn ein Prüfdatensatz eines asynchronen Ereignisses nicht zur Kernel-Prüfwarteschlange hinzugefügt werden kann, die gesamte Verarbeitung angehalten wird. Das System wird in einen Alarmzustand versetzt. Das asynchrone Ereignis ist nicht in der Prüfwarteschlange enthalten und muss von den Zeigern im Aufruf-Stack wiederhergestellt werden.

  Die Richtlinie `-cnt` legt fest, dass, wenn ein synchrones Ereignis nicht zur Kernel-Prüfwarteschlange hinzugefügt werden kann, der Thread, der das Ereignis zustellen möchte, blockiert wird. Der Thread wird zu einer Passivwarteschlange hinzugefügt, bis Prüfbereich verfügbar ist. Es wird keine Zählung durchgeführt. Die Programme scheinen blockiert zu sein, bis Prüfbereich verfügbar ist.

  Die Konfiguration `+ahlt -cnt` wird normalerweise an Standorten verwendet, bei denen ein Datensatz der einzelnen Prüfereignisse Vorrang vor der Systemverfügbarkeit hat. Die Programme scheinen blockiert zu sein, bis Prüfbereich verfügbar ist. Das Feld `auditstat wblk` zeigt, wie oft Threads blockiert wurden.

Wenn jedoch ein asynchrones Ereignis eintritt, löst dies den Alarmzustand und Ausfall des Systems aus. Die Kernel-Warteschlange der Prüfereignisse kann aus einem Speicherabzug manuell wiederhergestellt werden. Das asynchrone Ereignis ist nicht in der Prüfwarteschlange enthalten und muss von den Zeigern im Aufruf-Stack wiederhergestellt werden.

- Die Richtlinie `-ahlt -cnt` legt fest, dass, wenn ein asynchrones Ereignis nicht zur Kernel-Prüfwarteschlange hinzugefügt werden kann, das Ereignis gezählt und die Verarbeitung fortgesetzt wird. Wenn ein synchrones Ereignis nicht zur Kernel-Prüfwarteschlange hinzugefügt werden kann, wird der Thread, der das Ereignis zustellen möchte, blockiert. Der Thread wird zu einer Passivwarteschlange hinzugefügt, bis Prüfbereich verfügbar ist. Es wird keine Zählung durchgeführt. Die Programme scheinen blockiert zu sein, bis Prüfbereich verfügbar ist.

  Die Konfiguration `-ahlt -cnt` wird normalerweise an Standorten verwendet, an denen die Aufzeichnung aller synchronen Prüfereignisse Vorrang vor möglichem Verlust asynchroner Prüfdatensätze hat. Das Feld `auditstat wblk` zeigt, wie oft Threads blockiert wurden.
- Die Richtlinie `+ahlt +cnt` legt fest, dass, wenn ein asynchrones Ereignis nicht zur Kernel-Prüfwarteschlange hinzugefügt werden kann, das System in einen Alarmzustand versetzt wird. Wenn ein synchrones Ereignis nicht zur Kernel-Prüfwarteschlange hinzugefügt werden kann, zählt das System das Ereignis und setzt die Verarbeitung fort.

Steuerung des Prüfungsaufwands

Da von einer Prüfung Systemressourcen benötigt werden, müssen Sie den Detaillierungsgrad für die Aufzeichnung festlegen. Bei der Prüfung kann der folgende Aufwand entstehen:

- Höhere Verarbeitungszeit
- Analyse der Prüfungsdaten
- Speicherung der Prüfungsdaten

Höhere Verarbeitungszeit der Prüfungsdaten

Die höhere Verarbeitungszeit ist der geringste Aufwand bei der Prüfung. Der wichtigste Grund ist, dass die Prüfung normalerweise nicht während der rechenintensiven Aufgaben durchgeführt wird, beispielsweise Bildverarbeitung, komplizierte Berechnungen usw. Ein weiterer Grund ist, dass der Aufwand für Systeme mit einem Benutzer normalerweise so gering ist, dass er ignoriert werden kann.

Aufwand für Analyse der Prüfungsdaten

Der Aufwand der Analyse verhält sich ungefähr proportional zur Anzahl der erfassten Prüfungsdaten. Der Analyseaufwand besteht aus der Zeit für das Zusammenfassen und Überprüfen der Prüfdatensätze. Außerdem beinhaltet der Aufwand die Zeit zum Archivieren und Speichern der Datensätze an einem sicheren Speicherort.

Je weniger Datensätze generiert werden, desto weniger Zeit wird zum Analysieren des Prüfpfads benötigt. In den folgenden Abschnitten „Aufwand für Speicherung der Prüfungsdaten“ auf Seite 634 und „Effiziente Prüfung“ auf Seite 635 wird die effiziente Durchführung einer Prüfung beschrieben. Durch eine effiziente Prüfung können Sie die Anzahl der Prüfungsdaten verringern, während die Sicherheit des Standorts weiterhin gewährleistet bleibt.

Aufwand für Speicherung der Prüfungsdaten

Der Speicherungsaufwand ist der größte Aufwand bei der Prüfung. Die Anzahl der Prüfdaten hängt von Folgendem ab:

- Anzahl der Benutzer
- Anzahl der Systeme
- Umfang der Nutzung
- Grad der erforderlichen Rückverfolgbarkeit und Verantwortlichkeit

Da diese Faktoren je nach Standort unterschiedlich sein können, gibt es keine einheitliche Formel, um den Festplattenspeicherplatz für die Speicherung der Prüfdaten vorherzubestimmen. Die folgenden Informationen dienen zur Orientierung:

- Wählen Sie die geeigneten Prüfklassen aus, um den Umfang der generierten Datensätze zu verringern.

  Bei einer vollständigen Prüfung, das heißt mit der Klasse `all`, wird der Speicherplatz auf den Festplatten schnell voll. Sogar durch eine einfache Aufgabe wie Kompilieren eines Programms kann eine umfangreiche Prüfdatei entstehen. Ein kleines Programm kann Tausende von Prüfdatensätzen in weniger als einer Minute generieren.

  Wenn Sie beispielsweise die `file_read`-Prüfklasse `fr` nicht verwenden, können Sie den Speicherplatz für die Prüfung erheblich verringern. Indem Sie nur fehlgeschlagene Operationen prüfen, können Sie in einigen Fällen den Speicherplatz für die Prüfung verringern. Wenn Sie beispielsweise die fehlgeschlagenen `file_read`-Operationen `-fr` prüfen, werden erheblich weniger Datensätze generiert als bei der Prüfung aller `file_read`-Ereignisse.
- Eine effiziente Prüfdateiverwaltung ist ebenfalls wichtig. Nach dem Erstellen der Prüfdatensätze wird durch die Dateiverwaltung der erforderliche Speicherplatz verringert.
- Kenntnis der Prüfklassen

Vor dem Konfigurieren der Prüfung sollte Ihnen die Funktionsweise der in den Klassen enthaltenen Ereignistypen bekannt sein. Sie können die Zuordnungen zwischen Ereignissen und Klassen für die Prüfung ändern, um die Prüfdatensatzerfassung zu optimieren.

- Berücksichtigen Sie bei der Prüfung die Umgebungsbedingungen an Ihrem Standort.

  Führen Sie sinnvolle Maßnahmen durch. Beachten Sie dabei den Grad an Rückverfolgbarkeit an Ihrem Standort und die verwalteten Benutzer.

Effiziente Prüfung

Anhand der folgenden Methoden können Sie die Sicherheitsziele Ihrer Organisation erreichen und gleichzeitig eine effizientere Prüfung durchführen.

- Führen Sie eine zufällige Prüfung nur bei einem bestimmten Prozentsatz der Benutzer gleichzeitig durch.
- Verringern Sie die Speicherplatzanforderungen für Prüfdateien, indem Sie die Dateien kombinieren, deren Größe reduzieren und komprimieren. Entwickeln Sie Verfahren, um die Dateien zu archivieren, an Wechseldatenträger zu übertragen und offline zu speichern.
- Überwachen Sie die Prüfdaten in Echtzeit auf ungewöhnliches Verhalten. Sie können die entwickelten Tools für Verwaltung und Analyse erweitern, um die Prüfdatensätze in den `syslog`-Dateien zu verarbeiten.

  Außerdem können Sie Verfahren einrichten, um den Prüfpfad auf bestimmte Aktivitäten zu überwachen. Sie können ein Skript erstellen, um eine verstärkte Prüfung bestimmter Benutzer oder Systeme automatisch auszulösen, wenn ungewöhnliche Ereignisse festgestellt wurden.

  Beispielsweise können Sie ein Skript erstellen, durch das folgende Vorgänge durchgeführt werden:

  1. Überwachung der Erstellung von Prüfdateien auf allen Prüfdateiservern
  2. Verarbeitung der Prüfdateien mit dem Befehl `tail`

     Die Pipe-Verkettung der Ausgabe vom Befehl `tail -0f` bis zum Befehl `praudit` kann einen Strom an Prüfdatensätzen ergeben, während die Datensätze generiert werden. Weitere Informationen finden Sie auf der Manpage `tail(1)`.
  3. Analyse dieses Stroms an ungewöhnlichen Meldungstypen oder anderen Indikatoren und Zustellen der Analyse an den Prüfer

     Außerdem können mit dem Skript automatische Antworten ausgelöst werden.
  4. Ständige Überwachung der Prüfverzeichnisse auf neue `not_terminated`-Prüfdateien
  5. Beenden ausstehender `tail`-Prozesse, wenn keine weiteren Schreibvorgänge in deren Dateien erfolgen

◆ ◆ ◆ KAPITEL 30

Verwalten der Oracle Solaris-Prüfung (Aufgaben)

In diesem Kapitel werden Verfahren beschrieben, mit denen Sie ein zu prüfendes Oracle Solaris-System einrichten und verwalten können. Außerdem enthält dieses Kapitel Anweisungen zur Verwaltung des Prüfpfads. Im Folgenden ist eine Liste der Informationen in diesem Kapitel aufgeführt.

- „Prüfung bei Oracle Solaris (Übersicht der Schritte)“ auf Seite 637
- „Konfigurieren der Prüfdateien (Übersicht der Schritte)“ auf Seite 638
- „Konfigurieren und Aktivieren des Prüfservice (Übersicht der Schritte)“ auf Seite 648
- „Verwalten der Prüfdatensätze (Übersicht der Schritte)“ auf Seite 665
- „Fehlerbehebung bei der Oracle Solaris-Prüfung (Übersicht der Schritte)“ auf Seite 675

Eine Übersicht zum Prüfservice erhalten Sie unter Kapitel 28, „Prüfung bei Oracle Solaris (Übersicht)“. Vorschläge zur Planung erhalten Sie unter Kapitel 29, „Planen der Oracle Solaris-Prüfung“. Weitere Referenzinformationen erhalten Sie unter Kapitel 31, „Prüfung bei Oracle Solaris (Referenz)“.

Prüfung bei Oracle Solaris (Übersicht der Schritte)

In der folgenden Übersicht der Schritte sind die wichtigsten Aufgaben für die Verwaltung der Prüfung aufgeführt. Die Aufgaben sind geordnet.

Aufgabe	Beschreibung	Anweisungen
1. Planen der Prüfung	Enthält die zu berücksichtigenden Punkte vor dem Konfigurieren des Prüfservice	„Planen der Oracle Solaris-Prüfung (Übersicht der Schritte)“ auf Seite 623
2. Konfigurieren der Prüfdateien	Definiert die zu prüfenden Ereignisse, Klassen und Benutzer	„Konfigurieren der Prüfdateien (Übersicht der Schritte)“ auf Seite 638

Aufgabe	Beschreibung	Anweisungen
3. Konfigurieren und Aktivieren der Prüfung	Konfiguriert auf jedem Host den Festplattenspeicher und andere Prüfserviceanforderungen. Anschließend wird der Prüfservice gestartet.	„Konfigurieren und Aktivieren des Prüfservice (Übersicht der Schritte)“ auf Seite 648
	Konfigurieren Sie auf einem Host, auf dem nicht globale Zonen installiert sind, einen Prüfservice für das System oder einen Prüfservice pro Zone.	„Konfigurieren des Prüfservice in Zonen (Aufgaben)“ auf Seite 660
4. Verwalten der Prüfdatensätze	Erfasst und analysiert die Prüfdaten	„Verwalten der Prüfdatensätze (Übersicht der Schritte)“ auf Seite 665

Konfigurieren der Prüfdateien (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf die Verfahren zum Konfigurieren von Dateien, um die Prüfung an Ihren Standort anzupassen. Die meisten Aufgaben sind optional.

Aufgabe	Beschreibung	Anweisungen
Auswählen von Prüfklassen und Anpassen der Einstellungen von `audit_control`	Inhalt: ■ Vorauswahl der systemweiten Prüfklassen ■ Angeben der Prüfverzeichnisse für jedes System ■ Einstellen der Grenzwerte für den Festplattenspeicher auf Prüfdateisystemen	„So ändern Sie die Datei `audit_control`“ auf Seite 639
(Optional) Protokollieren von Prüfereignissen auf zwei Arten	Ermöglicht das Überwachen von Prüfereignissen in Echtzeit, zusätzlich zum Speichern der Prüfdatensätze im binären Format	„So konfigurieren Sie `syslog`-Prüfprotokolle“ auf Seite 641
(Optional) Ändern der Prüfungsmerkmale der Benutzer	Legt benutzerspezifische Ausnahmen für die systemweiten im Voraus ausgewählten Prüfklassen fest	„So ändern Sie die Prüfmerkmale eines Benutzers“ auf Seite 644
(Optional) Hinzufügen von Prüfklassen	Verringert die Anzahl der Prüfdatensätze durch Erstellen einer neuen Prüfklasse für die Ereignisse	„So fügen Sie eine Prüfklasse hinzu“ auf Seite 646
(Optional) Ändern der Zuordnungen zwischen Ereignissen und Klassen	Verringert die Anzahl der Prüfdatensätze durch Ändern der Zuordnungen zwischen Ereignissen und Klassen	„So ändern Sie die Klassenmitgliedschaft eines Prüfereignisses“ auf Seite 647

Konfigurieren von Prüfdateien (Aufgaben)

Bevor Sie die Prüfung im Netzwerk aktivieren, können Sie die Prüfkonfigurationsdateien an die Prüfungsanforderungen Ihres Standorts anpassen. Außerdem können Sie den Prüfservice erneut starten oder das lokale System erneut booten, um die nach der Aktivierung des Prüfservice geänderten Konfigurationsdateien zu lesen. Es hat sich jedoch bewährt, die Prüfkonfiguration so weit wie möglich anzupassen, bevor der Prüfservice gestartet wird.

Wenn Sie Zonen implementiert haben, können Sie alle Zonen über die globale Zone prüfen. Um die Zonen in der Prüfungsausgabe zu unterscheiden, können Sie die Richtlinienoption `zonename` festlegen. Wenn Sie stattdessen die nicht globalen Zonen einzeln prüfen möchten, können Sie die Richtlinie `perzone` in der globalen Zone einstellen und die Prüfkonfigurationsdateien in den nicht globalen Zonen anpassen. Eine Übersicht finden Sie unter „Prüfung und Oracle Solaris-Zonen“ auf Seite 702. Informationen zur Planung erhalten Sie unter „So planen Sie die Prüfung der Zonen“ auf Seite 624. Informationen zu Verfahren erhalten Sie unter „Konfigurieren des Prüfservice in Zonen (Aufgaben)“ auf Seite 660.

▼ So ändern Sie die Datei `audit_control`

Die Konfiguration der systemweiten Prüfung erfolgt in der Datei `/etc/security/audit_control`. In der Datei werden die zu prüfenden Ereignisse, der Zeitpunkt für die Ausgabe von Prüfungswarnungen und der Speicherort der Prüfdateien festgelegt.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 (Optional) Speichern Sie eine Backup-Kopie der Datei `audit_control`.

```
# cp /etc/security/audit_control /etc/security/audit_control.orig
```

3 Ändern Sie die Datei `audit_control` an Ihrem Standort.

Die Einträge liegen im folgenden Format vor:

keyword:*value*

keyword Definiert den Zeilentyp. Es gibt folgende Typen: `dir`, `flags`, `minfree`, `naflags` und `plugin`. In der Version Solaris 10 sind die Zeilen `dir` und `minfree` veraltet und werden nicht mehr verwendet.

Eine Erläuterung der Schlüsselwörter finden Sie in den folgenden Beispielen.

value Gibt die Daten an, die dem Zeilentyp zugewiesen sind.

Hinweis – Um die Speicherorte der Prüfverzeichnisse anzugeben, verwenden Sie das Attribut `p_dir` des Plugins `audit_binfile.so`. Um den mindestens verfügbaren freien Speicherplatz anzugeben, verwenden Sie das Attribut `p_minfree`.

4 (Optional) Überprüfen Sie die Syntax der Datei.

```
# audit -v /etc/security/audit_control
syntax ok
```

Beispiel 30–1 Vorauswahl der Prüfklassen für alle Benutzer

Die Zeile `flags` in der Datei `audit_control` bestimmt, welche Klassen der zuweisbaren Ereignisse für alle Benutzer im System geprüft werden. Die Klassen werden durch Kommata getrennt. Leerstellen sind zulässig. In diesem Beispiel werden die Ereignisse in den Klassen `lo` und `ap` für alle Benutzer geprüft.

```
## audit_control file
flags:lo,ap
naflags:lo
plugin:name=...
```

Die einer Klasse zugewiesenen Ereignisse können Sie in der Datei `audit_event` anzeigen. Stattdessen können Sie auch den Befehl `bsmrecord` verwenden (siehe Beispiel 30–27).

Beispiel 30–2 Vorauswahl der nicht zuweisbaren Ereignisse

In diesem Beispiel werden alle Ereignisse in der Klasse `na` und alle nicht zuweisbaren `login`-Ereignisse geprüft.

```
## audit_control file
flags:lo
naflags:lo,na
plugin:name=...
```

Beispiel 30–3 Angeben des Speicherorts für binäre Prüfdaten

Durch das Flag `p_dir` des Plugins `audit_binfile.so` wird angegeben, welche Prüfdateisysteme für die binären Prüfdaten verwendet werden sollen. In diesem Beispiel werden drei Speicherorte für binäre Prüfdaten definiert. Die Verzeichnisse sind vom primären Verzeichnis bis zum Reserveverzeichnis der Reihe nach aufgeführt. Die Zeile `plugin` enthält keinen Zeilenumbruch.

```
## audit_control file
##
flags:lo
naflags:lo,na
```

```
plugin:name=audit_binfile.so; p_dir=/var/audit/egret.1/files,
/var/audit/egret.2/files,/var/audit
```

Weitere Informationen zum Einrichten von Dateisystemen für binäre Prüfdaten finden Sie unter „So erstellen Sie Partitionen für Prüfdateien“ auf Seite 649.

Beispiel 30–4 Ändern der unteren Grenzwerte für Warnungen

In diesem Beispiel wird der mindestens verfügbare Speicherplatz für alle Prüfdateisysteme festgelegt, sodass eine Warnung ausgegeben wird, wenn nur 10 Prozent des Dateisystems verfügbar sind.

Die Zeile `plugin` enthält keinen Zeilenumbruch.

```
## audit_control file
#
flags:lo
naflags:lo,na
plugin:name=audit_binfile.so; p_dir=/var/audit/examplehost.1/files,
/var/audit/examplehost.2/files,/var/audit/localhost/files; p_minfree=10
```

Der Alias `audit_warn` erhält die Warnung. Weitere Informationen zum Einrichten des Alias erhalten Sie unter „So konfigurieren Sie den E-Mail-Alias `audit_warn`“ auf Seite 653.

▼ So konfigurieren Sie `syslog`-Prüfprotokolle

Sie können den Prüfservice so anweisen, dass einige oder alle der erfassten Prüfdatensätze in die Prüfwarteschlange für `syslog` kopiert werden. Im folgenden Verfahren wird beschrieben, wie Prüfungsdaten im Text- und binären Format gespeichert werden. Die erfassten Prüfungsdaten im Textformat sind ein untergeordneter Satz der binären Daten.

Bevor Sie beginnen Sie müssen die Prüfklassen im Voraus auswählen. Die im Voraus ausgewählten Prüfklassen werden in der Zeile `flags` und der Zeile `naflags` der Datei `audit_control` angegeben. Außerdem können Sie Klassen für einzelne Benutzer in der Datei `audit_user` im Voraus auswählen und Prüfklassen mit dem Befehl `auditconfig` dynamisch hinzufügen.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 (Optional) Speichern Sie eine Backup-Kopie der Datei `audit_control`.

```
# cp /etc/security/audit_control /etc/security/audit_control.save
```

3 Fügen Sie einen Plugin-Eintrag `audit_syslog.so` hinzu.

```
## audit_control file
flags:lo,ss
naflags:lo,na
plugin:name=audit_binfile.so;p_dir=/var/audit; p_minfree=20;
plugin:name=audit_syslog.so;p_flags=+lo,-ss
```

Ein Eintrag `plugin` weist das folgende Format auf:

`plugin:name=`*name*`; qsize=`*max-queued-records*`;p_*=*value*

- `name=`*name*: Führt den Namen des Plugins auf. Die gültigen Werte sind `audit_binfile.so` und `audit_syslog.so`.
- `qsize=`*max-queued-records*: Gibt die maximale Anzahl der in die Warteschlange zu stellenden Datensätze für Prüfdaten an, die an das Plugin gesendet werden. Dieses Attribut ist optional.
- `p_*=` *value*: Gibt Plugin-spezifische Attribute an. Das Plugin `audit_syslog.so` akzeptiert `p_flags`. Das Plugin `audit_binfile.so` akzeptiert `p_dir`, `p_minfree` und `p_fsize`. Das Attribut `p_fsize` ist seit der Version Solaris 10 10/08 verfügbar.

Weitere Informationen zu Plugin-spezifischen Attributen finden Sie im Abschnitt `OBJECT ATTRIBUTES` der Manpages `audit_binfile(5)` und `audit_syslog(5)`.

4 Fügen Sie einen Eintrag `audit.notice` zur Datei `syslog.conf` hinzu.

Der Eintrag enthält den Speicherort der Protokolldatei.

```
# cat /etc/syslog.conf
...
audit.notice       /var/adm/auditlog
```

Speichern Sie keine Protokolle im Textformat am gleichen Speicherort wie binäre Prüfdateien. Der Befehl `auditreduce`, durch den binäre Prüfdateien gelesen werden, nimmt an, dass alle Dateien in einer Prüfpartition binäre Prüfdateien sind.

5 Erstellen Sie die Protokolldatei.

```
# touch /var/adm/auditlog
```

6 Aktualisieren Sie die Konfigurationsinformationen für den Service `syslog`.

```
# svcadm refresh system/system-log
```

7 Archivieren Sie die `syslog`-Protokolldateien in regelmäßigen Abständen.

Die durch den Prüfservice generierte Ausgabe kann sehr umfangreich sein. Weitere Informationen zum Verwalten der Protokolle finden Sie auf der Manpage `logadm(1M)`.

Beispiel 30–5 Angeben der Prüfklassen für die `syslog`-Ausgabe

Im folgenden Beispiel wird vom Dienstprogramm `syslog` ein untergeordneter Satz der im Voraus ausgewählten Prüfklassen erfasst.

```
## audit_user file
jdoe:pf

## audit_control file
flags:lo,ss
naflags:lo,na
plugin:name=audit_binfile.so; p_dir=/var/audit/host.1/files,
/var/audit/host.2/files,/var/audit/localhost/files; p_minfree=10
plugin:name=audit_syslog.so; p_flags=-lo,-na,-ss,+pf
```

Durch die Einträge `flags` und `naflags` wird das System angewiesen, alle Prüfdatensätze für Anmelden/Abmelden, Nichtzuweisung und Systemstatusänderung im binären Format zu erfassen. Der Plugin-Eintrag `audit_syslog.so` weist das Dienstprogramm `syslog` an, nur fehlgeschlagene Anmeldungen, fehlgeschlagene nicht zuweisbare Ereignisse und fehlgeschlagene Systemstatusänderungen zu erfassen. Für den Benutzer `jdoe` enthält der binäre Prüfdatensatz alle Verwendungen einer die Profile erkennenden Shell. Das Dienstprogramm `syslog` erfasst die erfolgreichen der Profile erkennenden Befehle. Das Erstellen der Klasse `pf` wird unter Beispiel 30–10 beschrieben.

Beispiel 30–6 Einfügen der `syslog`-Prüfdatensätze auf einem Remote-System

Sie können den Eintrag `audit.notice` in der Datei `syslog.conf` so ändern, dass er auf ein Remote-System verweist. In diesem Beispiel lautet der Name des lokalen Systems `example1`. Das Remote-System lautet `remote1`.

```
example1 # cat /etc/syslog.conf
...
audit.notice       @remote1
```

Der Eintrag `audit.notice` in der Datei `syslog.conf` auf dem System `remote1` verweist auf die Protokolldatei.

```
remote1 # cat /etc/syslog.conf
...
audit.notice       /var/adm/auditlog
```

Beispiel 30–7 Verwenden von Plugins in der Datei `audit_control`

Die bevorzugte Methode zum Angeben von Informationen ohne Flags in der Datei `audit_control` ist die Verwendung des Eintrags `plugin`. In diesem Beispiel werden die Prüf-Flags ausgewählt und anschließend die Plugin-Informationen aufgeführt.

```
## audit_control file
flags:lo,ss
naflags:lo,na
plugin:name=audit_binfile.so;p_minfree=10; p_dir=/var/audit
plugin:name=audit_syslog.so; p_flags=+lo
```

▼ So ändern Sie die Prüfmerkmale eines Benutzers

Definitionen für die Benutzer werden in der Datenbank `audit_user` gespeichert. Durch diese Definitionen werden für den jeweiligen Benutzer die im Voraus ausgewählten Klassen in der Datei `audit_control` geändert. In der Datei `nsswitch.conf` wird festgelegt, ob eine lokale Datei oder eine Naming Service-Datenbank verwendet wird. Weitere Informationen zur Berechnung der endgültigen Prüfungsvorauswahlmaske eines Benutzers finden Sie unter „Verarbeiten der Prüfungsmerkmale“ auf Seite 707.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 (Optional) Speichern Sie eine Backup-Kopie der Datenbank `audit_user`.

```
# cp /etc/security/audit_user /etc/security/audit_user.orig
```

3 Fügen Sie neue Einträge zur Datenbank `audit_user` hinzu.

In der lokalen Datenbank weist jeder Eintrag das folgende Format auf:

username:*always-audit*:*never-audit*

username	Wählt den Namen des zu prüfenden Benutzers
always-audit	Wählt die Liste der Prüfklassen, die immer für den angegebenen Benutzer geprüft werden sollen
never-audit	Wählt die Liste der Prüfklassen, die nie für den angegebenen Benutzer geprüft werden sollen

Sie können mehrere Klassen angeben, indem Sie die Prüfklassen durch Kommata trennen.

Die Einträge `audit_user` gelten ab der nächsten Anmeldung des Benutzers.

Beispiel 30–8 Ändern der für einen Benutzer geprüften Ereignisse

In diesem Beispiel enthält die Datei `audit_control` die im Voraus ausgewählten Prüfklassen für das System:

```
## audit_control file
...
flags:lo,ss
naflags:lo,na
```

Die Datei `audit_user` zeigt eine Ausnahme. Wenn der Benutzer `jdoe` eine Profil-Shell verwendet, wird diese Verwendung geprüft:

```
## audit_user file
jdoe:pf
```

Die Prüfungsvorauswahlmaske für `jdoe` ist eine Kombination aus den Einstellungen `audit_user` und `audit_control`. Der Befehl `auditconfig -getaudit` zeigt die Vorauswahlmaske für `jdoe`:

```
# auditconfig -getaudit
audit id = jdoe(1234567)
process preselection mask = ss,pf,lo(0x13000,0x13000)
terminal id (maj,min,host) = 242,511,example1(192.168.160.171)
audit session id = 2138517656
```

Beispiel 30–9 Nur Prüfung von Benutzern und nicht dem System

In diesem Beispiel werden nur Anmelde- und Rollenaktivitäten von vier Benutzern in diesem System geprüft. Durch die Datei `audit_control` werden keine Prüfklassen für das System im Voraus ausgewählt.

```
## audit_control file
...
flags:
naflags:
```

Durch die Datei `audit_user` werden zwei Prüfklassen für vier Benutzer wie folgt im Voraus ausgewählt:

```
## audit_user file
jdoe:lo,pf
kdoe:lo,pf
pdoe:lo,pf
sdoe:lo,pf
```

In der folgenden Datei `audit_control` wird ein unbefugtes Eindringen aufgezeichnet. In Kombination mit der Datei `audit_user` wird durch diese Datei das System besser geschützt als durch die erste Datei `audit_control` in diesem Beispiel.

```
## audit_control file
...
flags:
naflags:lo
plugin:name=...
```

▼ So fügen Sie eine Prüfklasse hinzu

Beim Erstellen einer eigenen Prüfklasse können Sie nur die Prüfereignisse zur Klasse hinzufügen, die Sie an Ihrem Standort prüfen möchten. Wenn Sie die Klasse auf einem System hinzufügen, kopieren Sie die Änderung auf alle zu prüfenden Systeme.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 (Optional) Speichern Sie eine Backup-Kopie der Datei `audit_class`.

```
# cp /etc/security/audit_class /etc/security/audit_class.orig
```

3 Fügen Sie neue Einträge zur Datei `audit_class` hinzu.

Die Einträge liegen im folgenden Format vor:

`0x`*number*`:`*name*`:`*description*

0x	Identifiziert *number* als hexadezimal
number	Definiert eine eindeutige Prüfungsklassenmaske
name	Definiert den Buchstabennamen der Prüfklasse
description	Definiert den beschreibenden Namen der Prüfklasse

Der Eintrag in der Datei muss eindeutig sein. Verwenden Sie keine vorhandenen Prüfklassenmasken.

Beispiel 30–10 Erstellen einer neuen Prüfklasse

In diesem Beispiel wird eine Klasse für einen kleinen Satz an Prüfereignissen erstellt. Der zur Datei `audit_class` hinzugefügte Eintrag lautet wie folgt:

```
0x10000000:pf:profile command
```

Der Eintrag erstellt eine neue Prüfklasse mit dem Namen `pf`. In Beispiel 30–11 wird beschrieben, wie Einträge zur neuen Prüfklasse hinzugefügt werden.

Allgemeine Fehler

Vergewissern Sie sich nach dem Anpassen der Datei `audit_class`, dass die an `audit_user` durchgeführten Änderungen mit den neuen Prüfklassen übereinstimmen. Es treten Fehler auf, wenn die Prüfklassen in `audit_user` kein untergeordneter Satz der Datenbank `audit_class` sind.

▼ So ändern Sie die Klassenmitgliedschaft eines Prüfereignisses

Sie können die Klassenmitgliedschaft eines Prüfereignisses ändern, um die Größe einer vorhandenen Prüfklasse zu verringern oder das Ereignis in eine eigene Klasse hinzuzufügen. Wenn Sie die Zuordnungen zwischen Ereignissen und Klassen in einem System erneut konfigurieren, kopieren Sie die Änderung auf alle zu prüfenden Systeme.

1 **Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.**

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **(Optional) Speichern Sie eine Backup-Kopie der Datei `audit_event`.**

```
# cp /etc/security/audit_event /etc/security/audit_event.orig
```

3 **Ändern Sie die Klasse, zu der bestimmte Ereignisse gehören, indem Sie *class-list* der Ereignisse ändern.**

Die Einträge liegen im folgenden Format vor:

number:*name*:*description*:*class-list*

number	Entspricht der Prüfereignis-ID
name	Entspricht dem Namen des Prüfereignisses
description	Normalerweise der Systemaufruf oder die ausführbare Datei, durch den/die die Erstellung eines Prüfdatensatzes ausgelöst wird
class-list	Entspricht einer durch Kommata getrennten Liste von Prüfklassen

Beispiel 30–11 Zuordnen vorhandener Prüfereignisse zu einer neuen Klasse

In diesem Beispiel wird ein vorhandenes Prüfereignis der neuen Klasse zugewiesen, deren Erstellung unter Beispiel 30–10 beschrieben ist. In der Datei `audit_control` werden vom binären Prüfdatensatz erfolgreiche und fehlerhafte Ereignisse in der Klasse `pf` aufgezeichnet. Das Prüfprotokoll `syslog` enthält nur fehlerhafte Ereignisse in der Klasse `pf`.

```
# grep pf | /etc/security/audit_class
0x10000000:pf:profile command
# vi /etc/security/audit_event
6180:AUE_prof_cmd:profile command:ua,as,pf
# vi audit_control
...
flags:lo,pf
plugin:name=audit_binfile.so; p_dir=/var/audit; p_minfree=10
```

```
plugin:name=audit_syslog.so; p_flags=-lo,-pf
```

Beispiel 30–12 Prüfung der Verwendung von `setuid`-Programmen

In diesem Beispiel wird eine Klasse erstellt, in der Ereignisse gespeichert werden, die Aufrufe der Programme `setuid` und `setgid` überwachen. Im binären Prüfdatensatz werden erfolgreiche und fehlerhafte Ereignisse in den Klassen `lo` und `na` und erfolgreiche Ereignisse in der Klasse `st` erfasst. Das Prüfprotokoll `syslog` enthält nur erfolgreiche Ereignisse in der Klasse `st`.

```
# vi /etc/security/audit_class
0x00000800:st:setuid class
# vi /etc/security/audit_event
26:AUE_SETGROUPS:setgroups(2):st
27:AUE_SETPGRP:setpgrp(2):st
40:AUE_SETREUID:setreuid(2):st
41:AUE_SETREGID:setregid(2):st
214:AUE_SETEGID:setegid(2):st
215:AUE_SETEUID:seteuid(2):st

# vi audit_control
## audit_control file
flags:lo,+st
naflags:lo,na
plugin:name=audit_binfile.so; p_dir=/var/audit; p_minfree=10
plugin:name=audit_syslog.so; p_flags=-lo,+st
```

Konfigurieren und Aktivieren des Prüfservice (Übersicht der Schritte)

Die folgende Übersicht der Schritte verweist auf Verfahren zum Konfigurieren und Aktivieren des Prüfservice. Die Aufgaben sind geordnet.

Aufgabe	Beschreibung	Anweisungen
1. (Optional) Ändern der Prüfkonfigurationsdateien	Wählt die zu prüfenden Ereignisse, Klassen und Benutzer	„Konfigurieren der Prüfdateien (Übersicht der Schritte)“ auf Seite 638
2. Erstellen von Prüfpartitionen	Erstellt Festplattenspeicher für die Prüfdateien und schützt sie durch Dateiberechtigungen	„So erstellen Sie Partitionen für Prüfdateien“ auf Seite 649
3. Erstellen des Alias `audit_warn`	Definiert die Empfänger von E-Mail-Warnungen, wenn Maßnahmen für den Prüfservice erforderlich sind	„So konfigurieren Sie den E-Mail-Alias `audit_warn`“ auf Seite 653
4. (Optional) Ändern der Prüfrichtlinie	Definiert zusätzliche Prüfdaten, die am Standort erforderlich sein können	„So konfigurieren Sie die Prüfrichtlinie“ auf Seite 653

Aufgabe	Beschreibung	Anweisungen
6. Konfigurieren der Prüfung in nicht globalen Zonen	Ermöglicht die Erfassung von Prüfdatensätzen in nicht globalen Zonen	„Konfigurieren des Prüfservice in Zonen (Aufgaben)“ auf Seite 660
7. Aktivieren der Prüfung	Aktiviert den Prüfservice	„So aktivieren Sie den Prüfservice“ auf Seite 656
	Wenn `perzone` für die Prüfung aktiviert ist, ist eine Prüfung in einer nicht globalen Zone möglich.	Beispiel 30–20
8. (Optional) Deaktivieren der Prüfung	Deaktiviert den Prüfservice	„So deaktivieren Sie den Prüfservice“ auf Seite 658
	Wenn `perzone` für die Prüfung aktiviert ist, ist keine Prüfung in einer nicht globalen Zone möglich.	Beispiel 30–25
9. (Optional) Erneutes Lesen der Prüfungskonfigurationsänderungen	Liest Prüfkonfigurationsänderungen in den Kernel, während der Dämon `auditd` ausgeführt wird	„So aktualisieren Sie den Prüfservice“ auf Seite 659

Konfigurieren und Aktivieren des Prüfservice (Aufgaben)

Nach dem Einrichten der Konfigurationsdateien an Ihrem Standort müssen Sie Festplattenspeicher für die Prüfdateien einrichten. Außerdem müssen Sie andere Attribute des Prüfservice einrichten und anschließend den Service aktivieren. In diesem Abschnitt sind ebenfalls Verfahren zum Aktualisieren des Prüfservice beschrieben, wenn die Konfigurationseinstellungen geändert werden.

Wenn eine nicht globale Zone installiert ist, können Sie festlegen, dass die Zone genauso wie die globale Zone geprüft wird. Wenn Sie stattdessen die nicht globale Zone einzeln prüfen möchten, können Sie die Prüfkonfigurationsdateien in der nicht globalen Zone ändern. Weitere Informationen zum Anpassen der Prüfkonfigurationsdateien finden Sie unter „Konfigurieren der Prüfdateien (Übersicht der Schritte)“ auf Seite 638.

▼ So erstellen Sie Partitionen für Prüfdateien

Im folgenden Verfahren wird beschrieben, wie Partitionen für Prüfdateien sowie die entsprechenden Dateisysteme und Verzeichnisse erstellt werden. Überspringen Sie die entsprechenden Schritte, wenn Sie bereits über eine leere Partition verfügen oder ein leeres Dateisystem eingehängt haben.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Legen Sie den erforderlichen Festplattenspeicher fest.

Weisen Sie mindestens 200 MB Festplattenspeicher pro Host zu. Die Anforderungen an den Festplattenspeicher hängen jedoch vom Umfang der erforderlichen Prüfung ab. Deshalb kann Ihr Festplattenspeicherbedarf höher sein. Beachten Sie, eine lokale Partition für ein Reserveverzeichnis festzulegen.

3 Erstellen Sie dedizierte Prüfpartitionen bei Bedarf.

Dieser Schritt kann einfach während der Serverinstallation durchgeführt werden. Außerdem können Sie Partitionen auf Festplatten erstellen, die noch nicht auf dem Server eingehängt sind. Ausführliche Anweisungen zum Erstellen von Partitionen finden Sie unter Kapitel 11, „Administering Disks (Tasks)“ in *System Administration Guide: Devices and File Systems*.

```
# newfs /dev/rdsk/cwtxdysz
```

Dabei gilt: `/dev/rdsk/cwt`*x*`dy`*s z* ist der Raw-Gerätename für die Partition.

Wenn der lokale Host geprüft werden soll, erstellen Sie ebenfalls ein Reserveprüfverzeichnis für den lokalen Host.

4 Erstellen Sie Einhängepunkte für jede neue Partition.

```
# mkdir /var/audit/server-name.n
```

Dabei gilt: *server-name.n* ist der Name des Servers sowie eine Zahl zur Identifizierung der einzelnen Partitionen. Die Zahl ist optional, aber hilfreich, wenn mehrere Prüfverzeichnisse vorhanden sind.

5 Fügen Sie Einträge hinzu, um die neuen Partitionen automatisch einzuhängen.

Fügen Sie eine Zeile ähnlich der folgenden zur Datei `/etc/vfstab` hinzu:

```
/dev/dsk/cwtxdysz /dev/rdsk/cwtxdysz /var/audit/server-name.n   ufs  2  yes
```

6 (Optional) Entfernen Sie den Schwellenwert für den mindestens verfügbaren freien Speicherplatz auf den einzelnen Partitionen.

Bei einer Standardkonfiguration wird eine Warnung generiert, wenn das Verzeichnis zu 80 Prozent voll ist. Durch die Warnung braucht kein freier Speicherplatz für die Partition reserviert werden.

```
# tunefs -m 0 /var/audit/server-name.n
```

7 Hängen Sie die neuen Prüfpartitionen ein.

```
# mount /var/audit/server-name.n
```

8 Erstellen Sie Prüfverzeichnisse auf den neuen Partitionen.

```
# mkdir /var/audit/server-name.n/files
```

9 Korrigieren Sie die Berechtigungen auf den Einhängepunkten und neuen Verzeichnissen.

```
# chmod -R 750 /var/audit/server-name.n/files
```

10 Definieren Sie auf einem Dateiserver die Dateisysteme, die auf anderen Hosts verfügbar sein sollen.

In vielen Fällen werden Festplatten-Farmen zum Speichern von Prüfdatensätzen installiert. Wenn ein Prüfverzeichnis von verschiedenen Systemen verwendet werden soll, muss das Verzeichnis über den NFS-Service gemeinsam genutzt werden. Fügen Sie einen Eintrag ähnlich des folgenden für jedes Verzeichnis zur Datei `/etc/dfs/dfstab` hinzu:

```
share -F nfs /var/audit/server-name.n/files
```

11 Führen Sie auf einem Dateiserver einen Neustart des NFS-Service durch.

Wenn dieser Befehl der erste `share`-Befehl oder Satz von `share`-Befehlen ist, die Sie gestartet haben, werden die NFS-Dämonen möglicherweise nicht ausgeführt.

- **Wenn der NFS-Service offline ist, aktivieren Sie den Service.**

```
% svcs \*nfs\*
disabled       Nov_02   svc:/network/nfs/rquota:default
offline        Nov_02   svc:/network/nfs/server:default
# svcadm enable network/nfs/server
```

- **Wenn der NFS-Service ausgeführt wird, starten Sie den Service neu.**

```
% svcs \*nfs\*
online         Nov_02   svc:/network/nfs/client:default
online         Nov_02   svc:/network/nfs/server:default
# svcadm restart network/nfs/server
```

Weitere Informationen zum NFS-Service erhalten Sie unter „Einrichten von NFS-Services“ in *Systemverwaltungshandbuch: Netzwerkdienste*. Weitere Informationen zum Verwalten von persistenten Services finden Sie in Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration* und auf der Manpage `smf`(5).

Beispiel 30–13 Erstellen eines Reserveprüfverzeichnisses

Alle Systeme, auf denen der Prüfservice ausgeführt wird, müssen über ein lokales Dateisystem verfügen, das verwendet werden kann, wenn kein anderes Dateisystem verfügbar ist. In diesem Beispiel wird ein Dateisystem zu einem System mit dem Namen `egret` hinzugefügt. Da dieses Dateisystem nur lokal verwendet wird, müssen keine der für einen Dateiserver erforderlichen Schritte durchgeführt werden.

```
# newfs /dev/rdsk/c0t2d0
# mkdir /var/audit/egret
# grep egret /etc/vfstab
/dev/dsk/c0t2d0s1  /dev/rdsk/c0t2d0s1  /var/audit/egret ufs  2  yes  -
# tunefs -m 0 /var/audit/egret
# mount /var/audit/egret
# mkdir /var/audit/egret/files
# chmod -R 750 /var/audit/egret/files
```

Beispiel 30–14 Erstellen neuer Prüfpartitionen

In diesem Beispiel wird ein neues Dateisystem auf zwei neuen Festplatten erstellt, die von anderen Systemen im Netzwerk verwendet werden sollen.

```
# newfs /dev/rdsk/c0t2d0
# newfs /dev/rdsk/c0t2d1
# mkdir /var/audit/egret.1
# mkdir /var/audit/egret.2
# grep egret /etc/vfstab
/dev/dsk/c0t2d0s1  /dev/rdsk/c0t2d0s1  /var/audit/egret.1 ufs  2  yes  -
/dev/dsk/c0t2d1s1  /dev/rdsk/c0t2d1s1  /var/audit/egret.2 ufs  2  yes  -
# tunefs -m 0 /var/audit/egret.1
# tunefs -m 0 /var/audit/egret.2
# mount /var/audit/egret.1
# mount /var/audit/egret.2
# mkdir /var/audit/egret.1/files
# mkdir /var/audit/egret.2/files
# chmod -R 750 /var/audit/egret.1/files /var/audit/egret.2/files
# grep egret /etc/dfs/dfstab
 share -F nfs /var/audit/egret.1/files
 share -F nfs /var/audit/egret.2/files
# svcadm enable network/nfs/server
```

Beispiel 30–15 Erstellen von ZFS-Prüfpartitionen

In diesem Beispiel führt der Administrator den Befehl `script` aus, nachdem die ZFS-Prüfpartitionen erstellt wurden. Im Folgenden sehen Sie die Ausgabe des Befehls:

```
# zpool create auditf mirror c0t4d0 c0t5d0
# zfs create -o mountpoint=/audit auditf/audit
# zfs create auditf/audit/noddy
# zfs create auditf/audit/noddy/files
# zfs create auditf/audit/blinken
# zfs create auditf/audit/blinken/files
# zfs set devices=off auditf/audit
# zfs set exec=off auditf/audit
# zfs set setuid=off auditf/audit
# zfs set sharenfs=on auditf/audit
# share
-               /audit/blinken/files   rw   ""
-               /audit/noddy   rw   ""
-               /audit/blinken   rw   ""
-               /audit/noddy/files   rw   ""
-               /audit   rw   ""
# ^D
script done on Fri Apr 10 10:10:20 2009
```

Der Administrator kann anschließend die eingehängten Systeme über das Remote-System `remotesys` anzeigen.

```
# dfshares remotesys
RESOURCE                                SERVER ACCESS    TRANSPORT
remotesys:/audit/blinken/files       remotesys  -         -
```

```
remotesys:/audit/noddy              remotesys  -         -
remotesys:/audit/blinken            remotesys  -         -
remotesys:/audit/noddy/files        remotesys  -         -
remotesys:/audit                    remotesys  -         -
```

Abschließend hängt der Administrator das Dateisystem `/audit` auf `/var/audit` ein.

```
# mount remotesys:/audit /var/audit
# ls /var/audit
blinken  noddy
```

So konfigurieren Sie den E-Mail-Alias `audit_warn`

Das Skript `audit_warn` generiert eine Mail und sendet sie an einen E-Mail-Alias mit dem Namen `audit_warn`. Um diese Mail an eine gültige E-Mail-Adresse zu senden, können Sie eine der unter Schritt 2 beschriebenen Optionen verwenden.

1 Nehmen Sie die Rolle "Primary Administrator" an, oder melden Sie sich als Superuser an.

Die Rolle "Primary Administrator" enthält das gleichnamige Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Konfigurieren Sie den E-Mail-Alias `audit_warn`.

Wählen Sie eine der folgenden Optionen:

- **OPTION 1**: Ersetzen Sie den E-Mail-Alias `audit_warn` durch ein anderes E-Mail-Konto im Skript `audit_warn`.

  Ändern Sie den E-Mail-Alias in der folgenden Zeile des Skripts:

  ```
  ADDRESS=audit_warn            # standard alias for audit alerts
  ```

- **OPTION 2**: Leiten Sie die E-Mail `audit_warn` an ein anderes E-Mail-Konto weiter.

  Fügen Sie in diesem Fall den E-Mail-Alias `audit_warn` zur entsprechenden Mail-Alias-Datei hinzu. Sie können den Alias zur lokalen Datei `/etc/mail/aliases` oder zur Datenbank `mail_aliases` im Namespace hinzufügen. Der neue Eintrag sieht ähnlich des folgenden aus, wenn das E-Mail-Konto `root` zum E-Mail-Alias `audit_warn` hinzugefügt wird:

  ```
  audit_warn: root
  ```

So konfigurieren Sie die Prüfrichtlinie

Die Prüfrichtlinie bestimmt die Merkmale der Prüfdatensätze für den lokalen Host. Wenn die Prüfung aktiviert ist, bestimmt der Inhalt der Datei `/etc/security/audit_startup` die Prüfrichtlinie.

Sie können die aktuellen Prüfrichtlinienoptionen mit dem Befehl `auditconfig` anzeigen und ändern. Außerdem können Sie Richtlinienoptionen für den Befehl `auditconfig` im Skript `audit_startup` ändern, um dauerhaft Änderungen an der Prüfrichtlinie vorzunehmen.

1 **Nehmen Sie eine Rolle an, die das Profil "Audit Control" beinhaltet, oder melden Sie sich als Superuser an.**

Informationen zum Erstellen einer Rolle, die das Profil "Audit Control" beinhaltet und zum Zuweisen dieser Rolle zu einem Benutzer finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2 **Überprüfen Sie die Prüfrichtlinie.**

Bevor die Prüfung aktiviert wird, bestimmt der Inhalt der Datei `audit_startup` die Prüfrichtlinie:

```
#! /bin/sh
...
/usr/bin/echo "Starting BSM services."
/usr/sbin/auditconfig -setpolicy +cnt       Counts rather than drops records
/usr/sbin/auditconfig -conf       Configures event-class mappings
/usr/sbin/auditconfig -aconf      Configures nonattributable events
```

3 **Zeigen Sie die verfügbaren Richtlinienoptionen an.**

```
$ auditconfig -lspolicy
```

Hinweis – Die Richtlinienoptionen `perzone` und `ahlt` können nur in der globalen Zone eingestellt werden.

---

4 **Aktivieren oder deaktivieren Sie die ausgewählten Prüfrichtlinienoptionen.**

```
# auditconfig -setpolicy prefixpolicy
```

prefix Wenn *prefix* den Wert + aufweist, wird die Richtlinienoption aktiviert. Wenn *prefix* den Wert - aufweist, wird die Richtlinienoption deaktiviert.

policy Legt fest, ob die Richtlinie aktiviert oder deaktiviert wird

Die Richtlinie gilt bis zum nächsten Booten oder bis die Richtlinie durch den Befehl `auditconfig -setpolicy` geändert wird.

Eine Beschreibung der einzelnen Richtlinienoptionen erhalten Sie unter „Festlegen der Prüfrichtlinien“ auf Seite 629.

Beispiel 30–16 Einrichten der Prüfrichtlinienoptionen `cnt` und `ahlt`

In diesem Beispiel ist die Richtlinie `cnt` deaktiviert und die Richtlinie `ahlt` aktiviert. Durch diese Einstellungen wird die Verwendung des Systems angehalten, wenn die Prüfpartitionen

voll sind und ein asynchrones Ereignis auftritt. Wenn ein synchrones Ereignis auftritt, wird der Prozess, der den Thread erstellt hat, blockiert. Diese Einstellungen eignen sich, wenn die Sicherheit wichtiger als die Verfügbarkeit ist.

Durch die folgenden `audit_startup`-Einträge wird beim Neubooten die Richtlinienoption `cnt` deaktiviert und die Richtlinienoption `ahlt` aktiviert:

```
# cat /etc/security/audit_startup
#!/bin/sh
/usr/bin/echo "Starting BSM services."
/usr/sbin/deallocate -Is
/usr/sbin/auditconfig -conf
/usr/sbin/auditconfig -aconf
/usr/sbin/auditconfig -setpolicy -cnt
/usr/sbin/auditconfig -setpolicy +ahlt
```

Beispiel 30–17 Vorübergehendes Einrichten der Prüfrichtlinie `seq`

In diesem Beispiel wird der Dämon `auditd` ausgeführt und die Prüfrichtlinie `ahlt` wurde eingerichtet. Die Prüfrichtlinie `seq` wird zur aktuellen Richtlinie hinzugefügt. Durch die Richtlinie `seq` wird ein `sequence`-Token zu jedem Prüfdatensatz hinzugefügt. Dies dient zur Fehlersuche des Prüfservice, wenn die Prüfdatensätze beschädigt sind oder die Datensätze übersprungen wurden.

Durch das Präfix + wird die Option `seq` zur Prüfrichtlinie hinzugefügt und ersetzt nicht die aktuelle Prüfrichtlinie durch `seq`. Durch den Befehl `auditconfig` wird die Richtlinie bis zum nächsten Aufrufen des Befehls oder bis zum nächsten Booten übernommen.

```
$ auditconfig -setpolicy +seq
$ auditconfig -getpolicy
audit policies = ahlt,seq
```

Beispiel 30–18 Einrichten der Prüfrichtlinie `perzone`

In diesem Beispiel wird die Prüfrichtlinie `perzone` im Skript `audit_startup` in der globalen Zone festgelegt. Wenn eine Zone gebootet wird, erfasst die nicht globale Zone die Prüfdatensätze gemäß den Prüfkonfigurationseinstellungen der zugehörigen Zone.

```
$ cat /etc/security/audit_startup
#!/bin/sh
/usr/bin/echo "Starting BSM services."
/usr/sbin/deallocate -Is
/usr/sbin/auditconfig -conf
/usr/sbin/auditconfig -aconf
/usr/sbin/auditconfig -setpolicy +perzone
/usr/sbin/auditconfig -setpolicy +cnt
```

Beispiel 30–19 Ändern einer Prüfrichtlinie

In diesem Beispiel wird der Prüfdämon ausgeführt und die Prüfrichtlinie wurde eingerichtet. Der Befehl `auditconfig` ändert die Richtlinien `ahlt` und `cnt` während der Sitzung. Bei diesen Einstellungen werden die Prüfdatensätze übersprungen, aber gezählt, wenn das Prüfdateisystem voll ist. Weitere Informationen zu Einschränkungen beim Einrichten der Richtlinie `ahlt` finden Sie unter Schritt 3.

```
$ auditconfig -setpolicy +cnt
$ auditconfig -setpolicy -ahlt
$ auditconfig -getpolicy
audit policies = cnt,seq
```

Durch Hinzufügen der Änderungen zur Datei `audit_startup` werden die Richtlinien dauerhaft übernommen:

```
$ cat /etc/security/audit_startup
#!/bin/sh
/usr/bin/echo "Starting BSM services."
/usr/sbin/deallocate -Is
/usr/sbin/auditconfig -conf
/usr/sbin/auditconfig -aconf
/usr/sbin/auditconfig -setpolicy +cnt
```

Die Option `-ahlt` muss nicht in der Datei angegeben werden, da die Richtlinienoption `ahlt` standardmäßig deaktiviert ist. Diese Einstellung eignet sich, wenn die Verfügbarkeit wichtiger als die Sicherheit ist, die durch die Prüfdatensätze bereitgestellt wird.

▼ So aktivieren Sie den Prüfservice

Durch dieses Verfahren wird der Prüfservice für alle Zonen aktiviert. Weitere Informationen zum Starten des Prüfdämons in einer nicht globalen Zone finden Sie unter Beispiel 30–20.

Wenn die Prüfung sicher konfiguriert wurde, bleibt das System im Einzelbenutzermodus, bis die Prüfung aktiviert wird. Sie können die Prüfung auch im Mehrbenutzermodus aktivieren.

Bevor Sie beginnen

Führen Sie dieses Verfahren als Superuser aus, nachdem Sie die folgenden Aufgaben abgeschlossen haben:

- Planen: „Planen der Oracle Solaris-Prüfung (Übersicht der Schritte)“ auf Seite 623
- Anpassen der Prüfdateien: „Konfigurieren der Prüfdateien (Übersicht der Schritte)“ auf Seite 638
- Einrichten von Prüfpartitionen: „So erstellen Sie Partitionen für Prüfdateien“ auf Seite 649
- Einrichten von Prüfwarnungsmeldungen: „So konfigurieren Sie den E-Mail-Alias `audit_warn`“ auf Seite 653
- Einrichten der Prüfrichtlinie: „So konfigurieren Sie die Prüfrichtlinie“ auf Seite 653

Hinweis – Die Übersetzung von Hostnamen muss ordnungsgemäß funktionieren, damit die Prüfung durchgeführt werden kann. Die Datenbank `hosts` in den Naming Services muss ordnungsgemäß konfiguriert sein und verwendet werden können.

Weitere Informationen zur Konfiguration der Hosts-Datenbank finden Sie auf den Manpages `nsswitch.conf`(4) und `netconfig`(4). Weitere Informationen erhalten Sie im *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)* oder *System Administration Guide: Naming and Directory Services (NIS+)*.

1 Führen Sie das Skript aus, durch das der Prüfservice aktiviert wird.

Wechseln Sie in das Verzeichnis `/etc/security` und führen Sie das Skript `bsmconv` aus.

```
# cd /etc/security
# ./bsmconv
This script is used to enable the Basic Security Module (BSM).
Shall we continue with the conversion now? [y/n] y
bsmconv: INFO: checking startup file.
bsmconv: INFO: turning on audit module.
bsmconv: INFO: initializing device allocation.

The Basic Security Module is ready.
If there were any errors, please fix them now.
Configure BSM by editing files located in /etc/security.
Reboot this system now to come up with BSM enabled.
```

Weitere Informationen zu den Auswirkungen des Skripts erhalten Sie auf der Manpage `bsmconv`(1M).

2 Starten Sie das System neu.

```
# reboot
```

Durch die Startdatei `/etc/security/audit_startup` wird der Dämon `auditd` automatisch ausgeführt, wenn das System den Mehrbenutzermodus aufruft.

Eine weitere Auswirkung des Skripts ist die Aktivierung der Gerätezuordnung. Weitere Informationen zum Konfigurieren der Gerätezuordnung finden Sie unter „Verwalten der Gerätezuordnung (Übersicht der Schritte)“ auf Seite 87.

Beispiel 30–20 Aktivieren der Prüfung in einer nicht globalen Zone

Im folgenden Beispiel wurde die Richtlinie `perzone` vom Administrator der globalen Zone aktiviert, nachdem die Prüfung in der globalen Zone aktiviert und die nicht globale Zone gebootet wurde. Der Zonenadministrator der nicht globalen Zone hat die Prüfdateien der Zone konfiguriert und startet anschließend den Prüfdämon in der Zone.

```
zone1# svcadm enable svc:/system/auditd
```

▼ So deaktivieren Sie den Prüfservice

Wenn der Prüfservice nicht mehr benötigt werden sollte, wird durch dieses Verfahren das System in den Status vor dem Aktivieren der Prüfung zurückversetzt. Bei der Prüfung nicht globaler Zonen werden die zugehörigen Prüfservices ebenfalls deaktiviert.

Achtung – Durch diesen Befehl wird die Gerätezuordnung ebenfalls deaktiviert. Führen Sie diesen Befehl nicht aus, wenn Sie Geräte zuordnen möchten. Weitere Informationen zum Deaktivieren der Prüfung und Beibehalten der Gerätezuordnung erhalten Sie unter Beispiel 30–21.

1 Melden Sie sich als Superuser an und schalten Sie das System in den Einzelbenutzermodus.

```
% su
Password:       <Type root password>
# init S
```

Weitere Informationen erhalten Sie auf der Manpage `init(1M)`.

2 Führen Sie das Skript aus, um die Prüfung zu deaktivieren.

Wechseln Sie in das Verzeichnis `/etc/security` und führen Sie das Skript `bsmunconv` aus.

```
# cd /etc/security
# ./bsmunconv
```

Eine weitere Auswirkung des Skripts ist die Deaktivierung der Gerätezuordnung.

Weitere Informationen zu den gesamten Auswirkungen des Skripts `bsmunconv` erhalten Sie auf der Manpage `bsmconv(1M)`.

3 Schalten Sie das System in den Mehrbenutzermodus.

```
# init 6
```

Beispiel 30–21 Deaktivieren der Prüfung und Beibehalten der Gerätezuordnung

In diesem Beispiel hält der Prüfservice die Erfassung der Datensätze an, die Gerätezuordnung wird jedoch fortgesetzt. Alle Werte der Einträge `flags`, `naflags` und `plugin` in der Datei `audit_control` sowie alle Benutzereinträge in der Datei `audit_user` werden entfernt.

```
## audit_control file
flags:
naflags:

## audit_user file
```

Der Dämon `auditd` wird ausgeführt, aber es werden keine Prüfdatensätze gespeichert.

Beispiel 30–22 Deaktivieren der Prüfung für einzelne Zonen

In diesem Beispiel wird die Ausführung des Prüfservice in `zone1` angehalten; in dieser Zone ist der Prüfservice deaktiviert. Die Gerätezuordnung wird beibehalten. Wenn dieser Befehl in der globalen Zone ausgeführt wird und die Prüfrichtlinie `perzone` nicht eingerichtet ist, wird die Prüfung für alle Zonen und nicht nur für die globale Zone deaktiviert.

```
zone1 # audit -t
```

▼ So aktualisieren Sie den Prüfservice

Durch dieses Verfahren wird der Dämon `auditd` erneut gestartet, wenn Sie nach dem Ausführen des Dämons Änderungen an den Prüfkonfigurationsdateien vorgenommen haben.

1. **Nehmen Sie eine Rolle an, die das Berechtigungsprofil "Audit Control" beinhaltet, oder melden Sie sich als Superuser an.**

   Informationen zum Erstellen einer Rolle, die das Berechtigungsprofil "Audit Control" beinhaltet und zum Zuweisen dieser Rolle zu einem Benutzer finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2. **Wählen Sie den entsprechenden Befehl.**

   - **Wenn Sie die Zeile `naflags` in der Datei `audit_control` bearbeiten, ändern Sie die Kernel-Maske für nicht zuweisbare Ereignisse.**

     ```
     $ /usr/sbin/auditconfig -aconf
     ```

     Sie können auch erneut booten.

   - **Wenn Sie andere Zeilen in der Datei `audit_control` ändern, sollte die Datei `audit_control` erneut gelesen werden.**

     Der Prüfdämon führt eine interne Speicherung der Informationen aus der Datei `audit_control` durch. Um die neuen Informationen zu verwenden, booten Sie entweder das System erneut oder weisen Sie das Lesen der geänderten Datei durch den Prüfdämon an.

     ```
     $ /usr/sbin/audit -s
     ```

     Hinweis – Die Prüfdatensätze werden basierend auf der Prüfvorauswahlmaske generiert, die den einzelnen Prozessen zugewiesen ist. Durch Ausführen von `audit -s` werden die Masken in den vorhandenen Prozessen *nicht* geändert. Um die Vorauswahlmaske für einen vorhandenen Prozess zu ändern, müssen Sie den Prozess erneut starten. Sie können auch erneut booten.

Durch den Befehl `audit -s` wird der Prüfdämon angewiesen, das Verzeichnis und die Werte für "minfree" aus der Datei `audit_control` erneut zu lesen. Der Befehl ändert die Generierung der Vorauswahlmaske für Prozesse, die durch nachfolgende Anmeldungen ausgelöst wurden.

- **Wenn Sie die Datei `audit_event` oder `audit_class` während der Ausführung des Prüfdämons ändern, aktualisieren Sie den Prüfservice.**

  Lesen Sie die geänderten Zuordnungen zwischen Ereignissen und Klassen in das System, und stellen Sie sicher, dass die Benutzer, die den Rechner verwenden, ordnungsgemäß geprüft werden.

  ```
  $ auditconfig -conf
  $ auditconfig -setumask auid classes
  ```

  auid Entspricht der Benutzer-ID

  classes Entsprechen den im Voraus ausgewählten Prüfklassen

  Ein Beispiel erhalten Sie unter „So ändern Sie die Vorauswahlmaske eines Benutzers“ auf Seite 683.

- **Weitere Informationen zum Ändern einer Prüfrichtlinie bei einem ausgeführten System finden Sie unter Beispiel 30–17.**

Beispiel 30–23 Neustarten des Prüfdämons

In diesem Beispiel wird das System in den Einzelbenutzermodus und anschließend zurück in den Mehrbenutzermodus geschaltet. Wenn das System zurück in den Mehrbenutzermodus geschaltet wird, werden die geänderten Prüfkonfigurationsdateien in das System gelesen.

```
# init S
# init 6
```

Konfigurieren des Prüfservice in Zonen (Aufgaben)

Durch den Prüfservice wird das gesamte System geprüft, einschließlich der Prüfereignisse in Zonen. Auf einem System, auf dem nicht globale Zonen installiert sind, kann die Prüfung identisch für alle Zonen oder pro Zone durchgeführt werden. Weitere Informationen erhalten Sie unter „Prüfung auf Systemen mit Oracle Solaris-Zonen“ auf Seite 620. Weitere Informationen zur Planung erhalten Sie unter „So planen Sie die Prüfung der Zonen“ auf Seite 624.

▼ So können Sie alle Zonen für die Prüfung identisch konfigurieren

Durch dieses Verfahren können identische Prüfungen für jede Zone durchgeführt werden. Diese Methode erfordert den geringsten Computeraufwand und die geringsten administrativen Ressourcen.

1 Konfigurieren Sie die globale Zone für die Prüfung.

a. Führen Sie die Aufgaben unter „Konfigurieren der Prüfdateien (Übersicht der Schritte)" auf Seite 638 durch.

b. Führen Sie die Aufgaben unter „Konfigurieren und Aktivieren des Prüfservice (Übersicht der Schritte)" auf Seite 648 durch. Beachten Sie dabei folgende Ausnahmen:

- Aktivieren Sie nicht die Prüfrichtlinie `perzone`.
- Aktivieren Sie nicht den Prüfservice. Aktivieren Sie den Prüfservice, nachdem Sie die nicht globalen Zonen für die Prüfung konfiguriert haben.

2 Kopieren Sie die Prüfkonfigurationsdateien von der globalen Zone in alle nicht globalen Zonen.

Kopieren Sie eine der folgenden bearbeiteten Dateien: `audit_class`, `audit_control`, `audit_event` und `audit_user`. Kopieren Sie nicht `audit_startup` oder `audit_warn`. Sie brauchen Dateien, die nicht bearbeitet wurden, nicht zu kopieren.

Es sind folgende zwei Möglichkeiten verfügbar. Als Superuser können Sie die Dateien kopieren oder die Dateien über Loopback einhängen. Die nicht globale Zone muss ausgeführt werden.

- **Kopieren Sie die Dateien.**

  a. Führen Sie über die globale Zone das Verzeichnis `/etc/security` in der nicht globalen Zone auf.

  ```
  # ls /zone/zonename/etc/security/
  ```

  b. Kopieren Sie die Prüfkonfigurationsdateien in das Verzeichnis `/etc/security` der Zone.

  ```
  # cp /etc/security/audit-file /zone/zonename/etc/security/audit-file
  ```

  Wenn Sie zu einem späteren Zeitpunkt eine Prüfkonfigurationsdatei in der globalen Zone ändern, kopieren Sie die Datei erneut in die nicht globalen Zonen.

- **Hängen Sie die Konfigurationsdateien über Loopback ein.**

  a. Halten Sie über die globale Zone die nicht globale Zone an.

  ```
  # zoneadm -z non-global-zone halt
  ```

b. Erstellen Sie ein Loopback-Einhängen mit Lesezugriff für jede Prüfkonfigurationsdatei, die Sie in der globalen Zone geändert haben.

```
# zonecfg -z non-global-zone
 add fs
    set special=/etc/security/audit-file
    set dir=/etc/security/audit-file
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
 exit
```

c. Damit die Änderungen übernommen werden, booten Sie die nicht globale Zone.

```
# zoneadm -z non-global-zone boot
```

Stattdessen können Sie auch das System neu booten.

Wenn Sie zu einem späteren Zeitpunkt eine Prüfkonfigurationsdatei in der globalen Zone ändern, booten Sie das System neu, um die über Loopback eingehängten Dateien in den nicht globalen Zonen zu aktualisieren.

Beispiel 30–24 Loopback-Einhängen der Prüfkonfigurationsdateien

In diesem Beispiel hat der Systemadministrator die Dateien `audit_class`, `audit_event`, `audit_control`, `audit_user`, `audit_startup` und `audit_warn` geändert.

Die Dateien `audit_startup` und `audit_warn` werden nur in der globalen Zone gelesen, sodass kein Loopback-Einhängen in den nicht globalen Zonen erforderlich ist.

In diesem System (`machine1`) hat der Administrator zwei nicht globale Zonen (`machine1–webserver` und `machine1–appserver`) erstellt. Der Administrator hat das Anpassen der Prüfkonfigurationsdateien abgeschlossen. Wenn der Administrator die Dateien zu einem späteren Zeitpunkt ändert, wird das System erneut gebootet, um die Änderungen zu übernehmen.

```
# zoneadm -z machine1-webserver halt
# zoneadm -z machine1-appserver halt
# zonecfg -z machine1-webserver
 add fs
    set special=/etc/security/audit_class
    set dir=/etc/security/audit_class
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
 add fs
    set special=/etc/security/audit_event
    set dir=/etc/security/audit_event
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
 add fs
    set special=/etc/security/audit_control
```

```
    set dir=/etc/security/audit_control
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
add fs
    set special=/etc/security/audit_user
    set dir=/etc/security/audit_user
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
 exit
# zonecfg -z machine1-appserver
 add fs
    set special=/etc/security/audit_class
    set dir=/etc/security/audit_class
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
...
 exit
```

Nach dem Neubooten der Zonen besteht für die Prüfkonfigurationsdateien in den Zonen nur Lesezugriff.

▼ So konfigurieren Sie eine zonenweise Prüfung

Durch dieses Verfahren können die jeweiligen Zonenadministratoren den Prüfservice in ihren Zonen steuern. Eine vollständige Liste der Richtlinienoptionen erhalten Sie auf der Manpage `auditconfig(1M)`.

1 Konfigurieren Sie die Prüfung in der globalen Zone, aktivieren Sie jedoch den Prüfservice nicht.

a. Führen Sie die Aufgaben unter „Konfigurieren der Prüfdateien (Übersicht der Schritte)“ auf Seite 638 durch.

b. Führen Sie die Aufgaben unter „Konfigurieren und Aktivieren des Prüfservice (Übersicht der Schritte)“ auf Seite 648 durch. Beachten Sie dabei folgende Ausnahmen:

- Fügen Sie die Prüfrichtlinie `perzone` hinzu. Ein Beispiel erhalten Sie unter Beispiel 30–18.
- Aktivieren Sie nicht den Prüfservice. Sie aktivieren den Prüfservice, nachdem die nicht globalen Zonen für die Prüfung konfiguriert wurden.

2 Konfigurieren Sie die Prüfdateien in den nicht globalen Zonen.

Hinweis – Wenn Sie die Prüfung in der nicht globalen Zone deaktivieren möchten, können Sie diesen Schritt überspringen. Weitere Informationen zum Deaktivieren der Prüfung erhalten Sie unter Beispiel 30–25.

a. **Führen Sie die Aufgaben unter „Konfigurieren der Prüfdateien (Übersicht der Schritte)“ auf Seite 638 durch.**

b. **Führen Sie die unter „Konfigurieren und Aktivieren des Prüfservice (Übersicht der Schritte)“ auf Seite 648 beschriebenen Verfahren durch.**

c. **Konfigurieren Sie keine systemweiten Prüfeinstellungen.**

   Fügen Sie insbesondere nicht die Richtlinie `perzone` oder `ahlt` zur Datei `audit_startup` der nicht globalen Zone hinzu. Außerdem sollten Sie den Befehl `bsmconv` nicht über die nicht globale Zone ausführen.

d. **Aktivieren Sie die Prüfung in Ihrer Zone.**

   Wenn die globale Zone nach dem Konfigurieren der Prüfung neu gebootet wird, wird die Prüfung in Ihrer Zone automatisch aktiviert.

   Wenn der Administrator der globalen Zone die Prüfrichtlinie `perzone` aktiviert, nachdem das System gebootet wurde, müssen die Administratoren der einzelnen Zonen die Prüfung aktivieren. Einzelheiten finden Sie unter Beispiel 30–20.

3 **Aktivieren Sie den Prüfservice in der globalen Zone.**

Weitere Informationen zu dem Verfahren finden Sie unter „So aktivieren Sie den Prüfservice“ auf Seite 656.

Beispiel 30–25 Deaktivieren der Prüfung in einer nicht globalen Zone

Dieses Beispiel kann verwendet werden, wenn die Prüfrichtlinie `perzone` in der globalen Zone festgelegt wurde. Der Administrator der Zone `noaudit` deaktiviert die Prüfung für diese Zone. Da der Administrator die Prüfung deaktivieren möchte, wurden die Prüfkonfigurationsdateien nicht bearbeitet.

```
noauditzone # svcadm disable svc:/system/auditd
```

Verwalten der Prüfdatensätze (Übersicht der Schritte)

In der folgenden Übersicht der Schritte wird auf Verfahren für die Auswahl, Analyse und Verwaltung der Prüfdatensätze verwiesen.

Aufgabe	Beschreibung	Anweisungen
Anzeigen der Formate von Prüfdatensätzen	Zeigt die Art der Informationen, die für ein Prüfereignis erfasst werden, und die Reihenfolge der dargestellten Informationen	„So zeigen Sie Prüfdatensatzformate an“ auf Seite 665
Zusammenführen von Prüfdatensätzen	Kombiniert Prüfdateien von mehreren Rechnern in einem Prüfpfad	„So führen Sie Prüfdateien aus dem Prüfpfad zusammen“ auf Seite 667
Auswählen der zu untersuchenden Datensätze	Wählt bestimmte zu untersuchende Ereignisse aus	„So wählen Sie Prüfereignisse aus dem Prüfpfad aus“ auf Seite 669
Anzeigen von Prüfdatensätzen	Ermöglicht die Anzeige von binären Prüfdatensätzen	„So zeigen Sie den Inhalt der binären Prüfdateien an“ auf Seite 671
Bereinigen von nicht ordnungsgemäß benannten Prüfdateien	Versieht mit einem Ende-Zeitstempel die Prüfdateien, die vom Prüfservice versehentlich nicht geschlossen wurden	„So bereinigen Sie eine Prüfdatei des Typs `not_terminated`“ auf Seite 673
Verhindern eines Prüfpfadüberlaufs	Verhindert, dass die Prüfdateisysteme voll werden	„So verhindern Sie eine Prüfpfadüberlauf“ auf Seite 674

Verwalten der Prüfdatensätze

Durch Verwalten des Prüfpfads können Sie die Aktionen der Benutzer im Netzwerk überwachen. Bei der Prüfung können umfangreiche Datenmengen generiert werden. In den folgenden Aufgaben erfahren Sie, wie Sie diese Daten verwenden.

▼ So zeigen Sie Prüfdatensatzformate an

Um Skripten zum Suchen der gewünschten Prüfdaten zu schreiben, müssen Sie die Reihenfolge der Token in einem Prüfereignis kennen. Der Befehl `bsmrecord` zeigt die Prüfereignisnummer, Prüfklasse, Auswahlmaske und das Datensatzformat eines Prüfereignisses an.

- **Wandeln Sie das Format aller Prüfereignis-Datensätze in eine HTML-Datei um.**

  Durch die Option `-a` werden alle Formate der Prüfereignis-Datensätze aufgeführt. Durch die Option `-h` wird die Liste in das HTML-Format umgewandelt, das in einem Browser angezeigt werden kann.

  ```
  % bsmrecord -a -h > audit.events.html
  ```

Wenn Sie die Datei `*html` in einem Browser anzeigen, verwenden Sie die Suchfunktion des Browsers, um die entsprechenden Datensätze zu suchen.

Weitere Informationen erhalten Sie auf der Manpage `bsmrecord(1M)`.

Beispiel 30–26 Anzeigen der Prüfdatensatzformate eines Programms

In diesem Beispiel wird das Format aller Prüfdatensätze, die vom Programm `login` generiert wurden, angezeigt. Zu den Anmeldeprogrammen zählen `rlogin`, `telnet`, `newgrp`, Anmeldung für Aufgabenbereich an der Solaris Management Console und Oracle Solaris Secure Shell.

```
% bsmrecord -p login
login: logout
  program     various              See login(1)
  event ID    6153                 AUE_logout
...

newgrp
  program     newgrp               See newgrp login
  event ID    6212                 AUE_newgrp_login
...

rlogin
  program     /usr/sbin/login      See login(1) - rlogin
  event ID    6155                 AUE_rlogin
...

SMC: role login
  program     SMC server           See role login
  event ID    6173                 AUE_role_login
...

/usr/lib/ssh/sshd
  program     /usr/lib/ssh/sshd    See login - ssh
  event ID    6172                 AUE_ssh
...

telnet login
  program     /usr/sbin/login      See login(1) - telnet
  event ID    6154                 AUE_telnet
  ...
```

Beispiel 30–27 Anzeigen der Prüfdatensatzformate einer Prüfklasse

In diesem Beispiel wird das Format aller Prüfdatensätze in der Klasse `fd` angezeigt.

```
% bsmrecord -c fd

rmdir
  system call rmdir                See rmdir(2)
  event ID    48                   AUE_RMDIR
  class       fd                   (0x00000020)
      header
      path
```

```
      [attribute]
      subject
      [use_of_privilege]
      return

unlink
  system call unlink              See unlink(2)
  event ID    6                   AUE_UNLINK
  ...

unlinkat
  system call unlinkat            See openat(2)
  event ID    286                 AUE_UNLINKAT
  ...
```

▼ So führen Sie Prüfdateien aus dem Prüfpfad zusammen

Durch Zusammenführen aller Prüfdateien in allen Prüfverzeichnissen können Sie den Inhalt des gesamten Prüfpfads analysieren. Durch den Befehl `auditreduce` werden alle Datensätze aus den zugehörigen Eingabedateien in eine einzige Ausgabedatei zusammengeführt. Die Eingabedateien können anschließend gelöscht werden. Wenn Sie die Ausgabedatei in ein Verzeichnis mit dem Namen `/etc/security/audit/`*server-name*`/files` hinzufügen, kann durch den Befehl `auditreduce` die Ausgabedatei gefunden werden, ohne dass der vollständige Pfad angegeben werden muss.

Hinweis – Dieses Verfahren gilt nur für binäre Prüfdatensätze.

---

1 Nehmen Sie eine Rolle an, die das Profil "Audit Review" beinhaltet, oder melden Sie sich als Superuser an.

Beispielsweise beinhaltet die Rolle des Systemadministrators das Profil "Audit Review". Außerdem können Sie eine separate Rolle erstellen, die das Profil "Audit Review" enthält. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2 Erstellen Sie ein Verzeichnis zum Speichern der zusammengeführten Prüfdateien.

```
# mkdir audit-trail-directory
```

3 Beschränken Sie den Zugriff auf das Verzeichnis.

```
# chmod 700 audit-trail-directory
# ls -la audit-trail-directory
drwx------   3 root     sys          512 May 12 11:47 .
drwxr-xr-x   4 root     sys         1024 May 12 12:47 ..
```

4 Führen Sie die Prüfdatensätze im Prüfpfad zusammen.

Wechseln Sie in das Verzeichnis *audit-trail-directory* und führen Sie die Prüfdatensätze in eine Datei mit einem benannten Suffix zusammen. Es werden alle Verzeichnisse, die in den Zeilen `dir` der Datei `audit_control` auf dem lokalen System aufgeführt sind, zusammengeführt.

```
# cd audit-trail-directory
# auditreduce -Uppercase-option -O suffix
```

Durch die Optionen in Großbuchstaben des Befehls `auditreduce` werden die Dateien im Prüfpfad bearbeitet. Folgende Optionen in Großbuchstaben sind vorhanden:

`-A` Wählt alle Dateien im Prüfpfad aus

`-C` Wählt nur abgeschlossene Dateien aus. Durch diese Option werden Dateien mit dem Suffix `not_terminated` ignoriert.

`-M` Wählt Dateien mit einem bestimmten Suffix. Das Suffix kann einen Rechnernamen darstellen oder für eine Zusammenfassungsdatei angegeben worden sein.

`-O` Erstellt eine Prüfdatei mit den aus 14 Zeichen bestehenden Zeitstempeln für die Start- und Endezeit mit dem Suffix *suffix* im aktuellen Verzeichnis.

Beispiel 30–28 Kopieren der Prüfdateien in eine Zusammenfassungsdatei

Im folgenden Beispiel werden durch die Rolle "System Administrator" (`sysadmin`) alle Dateien aus dem Prüfpfad in eine zusammengeführte Datei kopiert.

```
$ whoami
sysadmin
$ mkdir /var/audit/audit_summary.dir
$ chmod 700 /var/audit/audit_summary.dir
$ cd /var/audit/audit_summary.dir
$ auditreduce -A -O All
$ ls *All
20100827183214.20100827215318.All
```

Im folgenden Beispiel werden nur abgeschlossene Dateien vom Prüfpfad in eine zusammengeführte Datei kopiert.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -C -O Complete
$ ls *Complete
20100827183214.20100827214217.Complete
```

Im folgenden Beispiel werden nur abgeschlossene Dateien vom Rechner `example1` in eine zusammengeführte Datei kopiert.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -M example1 -O example1summ
$ ls *summ
20100827183214.20100827214217.example1summ
```

Beispiel 30–29 Verschieben der Prüfdateien in eine Zusammenfassungsdatei

Die Option `-D` des Befehls `auditreduce` löscht eine Prüfdatei, wenn Sie sie an einen anderen Speicherort kopieren. Im folgenden Beispiel werden die abgeschlossenen Prüfdateien aus einem System in das Zusammenfassungsverzeichnis kopiert und können zu einem späteren Zeitpunkt untersucht werden.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -C -O daily_example1 -D example1
$ ls *example1
20100827183214.20100827214217.daily_example1
```

Die Prüfdateien aus dem System `example1`, die als Eingabe für die Datei `*daily_example1` verwendet wurden, werden bei erfolgreichem Abschluss dieses Befehls entfernt.

▼ So wählen Sie Prüfereignisse aus dem Prüfpfad aus

Sie können Prüfdatensätze filtern und sie anschließend untersuchen. Eine vollständige Liste der Filterungsoptionen erhalten Sie auf der Manpage `auditreduce(1M)`.

1 Nehmen Sie eine Rolle an, die das Profil "Audit Review" beinhaltet, oder melden Sie sich als Superuser an.

Beispielsweise beinhaltet die Rolle des Systemadministrators das Profil "Audit Review". Außerdem können Sie eine separate Rolle erstellen, die das Profil "Audit Review" enthält. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2 Wählen Sie den gewünschten Datensatztyp aus dem Prüfpfad oder aus der angegebenen Prüfdatei.

`auditreduce` *-lowercase-option argument* [*optional-file*]

argument	Bestimmtes Argument, das für eine Option in Kleinbuchstaben erforderlich ist. Beispiel: Für die Option `-c` ist ein *argument* einer Prüfklasse wie `ua` erforderlich.
`-d`	Wählt alle Ereignisse eines bestimmten Datums aus. Das Datumsformat für *argument* lautet *yyymmdd*. Durch andere Datumsoptionen (`-b` und `-a`) werden Ereignisse vor und nach einem bestimmten Datum ausgewählt.
`-u`	Wählt alle Ereignisse, die einem bestimmten Benutzer zugewiesen werden können. Das *argument* ist ein Benutzername. Durch eine andere Benutzeroption (`-e`) werden alle Ereignisse, die einer effektiven Benutzer-ID zugewiesen werden können, ausgewählt.
`-c`	Wählt alle Ereignisse in einer im Voraus ausgewählten Prüfklasse aus. Das *argument* ist ein Prüfklassenname.

`-m`	Wählt alle Instanzen eines bestimmten Prüfereignisses. Das *argument* ist ein Prüfereignis.
optional-file	Entspricht dem Namen einer Prüfdatei

Beispiel 30–30 Kombinieren und Verringern von Prüfdateien

Durch den Befehl `auditreduce` können Sie die weniger interessanten Datensätze löschen, indem die Eingabedateien kombiniert werden. Beispielsweise können Sie mit dem Befehl `auditreduce` nur die Anmelde- und Abmeldedatensätze in Prüfdateien behalten, die älter als ein Monat sind. Wenn Sie den gesamten Prüfpfad anzeigen möchten, können Sie ihn von einem Backup-Datenträger wiederherstellen.

```
# cd /var/audit/audit_summary.dir
# auditreduce -O lo.summary -b 20100827 -c lo; compress *lo.summary
```

Beispiel 30–31 Kopieren der na-Prüfdatensätze in eine Zusammenfassungsdatei

In diesem Beispiel werden alle Datensätze der nicht zuweisbaren Prüfereignisse im Prüfpfad in einer Datei zusammengefasst.

```
$ whoami
sysadmin
$ cd /var/audit/audit_summary.dir
$ auditreduce -c na -O nasumm
$ ls *nasumm
20100827183214.20100827215318.nasumm
```

Die zusammengeführte Prüfdatei `nasumm` wird mit einem Zeitstempel aus Anfangs- und Enddatum der `na`-Datensätze versehen.

Beispiel 30–32 Suchen der Prüfereignisse in einer angegebenen Prüfdatei

Sie können Prüfdateien manuell auswählen, um nur nach dem benannten Satz von Dateien zu suchen. Beispielsweise können Sie die Datei `*nasumm` im vorherigen Beispiel weiter verarbeiten, um Systemboot-Ereignisse zu suchen. Geben Sie dazu den Dateinamen als letztes Argument für den Befehl `auditreduce` an.

```
$ auditreduce -m 113 -O systemboot 20100827183214.20100827215318.nasumm
20100827183214.20100827183214.systemboot
```

Die Datei `20100827183214.20100827183214.systemboot` enthält nur Systemboot-Prüfereignisse.

Beispiel 30–33 Kopieren der Prüfdatensätze eines Benutzers in eine Zusammenfassungsdatei

In diesem Beispiel werden die Datensätze im Prüfpfad, die den Namen eines bestimmten Benutzers enthalten, zusammengeführt. Durch die Option `-e` wird der effektive Benutzer gesucht. Durch die Option `-u` wird der Prüfungsbenutzer gesucht.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -e tamiko -O tamiko
```

Sie können nach bestimmten Ereignissen in dieser Datei suchen. Im folgenden Beispiel wird der Anmelde- und Abmeldezeitpunkt eines bestimmten Benutzers am 7. September 2010 überprüft. Nur die Dateien mit dem Benutzernamen als Dateisuffix werden überprüft. Die Kurzform des Datums lautet *yyyymmdd*.

```
# auditreduce -M tamiko -O tamikolo -d 20100907 -u tamiko -c lo
```

Beispiel 30–34 Kopieren ausgewählter Datensätze in eine einzelne Datei

In diesem Beispiel werden Anmelde- und Abmeldemeldungen für einen bestimmten Tag aus dem Prüfpfad ausgewählt. Die Meldungen werden in eine Zieldatei zusammengeführt. Die Zieldatei wird in einem anderen Verzeichnis als dem üblichen Stammverzeichnis der Prüfung gespeichert.

```
# auditreduce -c lo -d 20100827 -O /var/audit/audit_summary.dir/logins
# ls /var/audit/audit_summary.dir/*logins
/var/audit/audit_summary.dir/20100827183936.20100827232326.logins
```

▼ So zeigen Sie den Inhalt der binären Prüfdateien an

Mit dem Befehl `praudit` können Sie den Inhalt binärer Prüfdateien anzeigen. Sie können für die Ausgabe des Befehls `auditreduce` eine Pipe-Verkettung durchführen oder eine bestimmte Prüfdatei lesen. Die Option `-x` eignet sich für eine weitere Verarbeitung.

1. **Nehmen Sie eine Rolle an, die das Profil "Audit Review" beinhaltet, oder melden Sie sich als Superuser an.**

   Beispielsweise beinhaltet die Rolle des Systemadministrators das Profil "Audit Review". Außerdem können Sie eine separate Rolle erstellen, die das Profil "Audit Review" enthält. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

2. **Verwenden Sie einen der folgenden `praudit`-Befehle, um die optimale Ausgabe für Ihre Anforderungen zu erstellen.**

   In den folgenden Beispielen sehen Sie eine `praudit`-Ausgabe des gleichen Prüfereignisses. Die Prüfrichtlinie wurde so festgelegt, dass sie die Token `sequence` und `trailer` enthält.

- Durch den Befehl `praudit -s` werden Prüfdatensätze im Kurzformat als ein Token pro Zeile angezeigt. Verwenden Sie die Option `-l`, um die Datensätze auf jeweils einer Zeile anzuzeigen.

  ```
  $ auditreduce -c lo | praudit -s
  header,101,2,AUE_rlogin,,example1,2010-10-13 11:23:31.050 -07:00
  subject,jdoe,jdoe,staff,jdoe,staff,749,749,195 1234 server1
  text,successful login
  return,success,0
  sequence,1298
  ```

- Durch den Befehl `praudit -r` werden Prüfdatensätze im unverarbeiteten Format als ein Token pro Zeile angezeigt. Verwenden Sie die Option `-l`, um die Datensätze auf jeweils einer Zeile anzuzeigen.

  ```
  $ auditreduce -c lo | praudit -r
  21,101,2,6155,0x0000,192.168.60.83,1062021202,64408258
  36,2026700,2026700,10,2026700,10,749,749,195 1234 192.168.60.17
  40,successful login
  39,0,0
  47,1298
  ```

- Durch den Befehl `praudit -x` werden Prüfdatensätze im XML-Format als ein Token pro Zeile angezeigt. Verwenden Sie die Option `-l`, um die XML-Ausgabe für einen Datensatz auf einer Zeile anzuzeigen.

  ```
  $ auditreduce -c lo | praudit -x
  <record version="2" event="login - rlogin" host="example1"
  time="Wed Aug 27 14:53:22 PDT 2010" msec="64">
  <subject audit-uid="jdoe" uid="jdoe" gid="staff" ruid="jdoe"
  rgid="staff" pid="749" sid="749" tid="195 1234 server1"/>
  <text>successful login</text>
  <return errval="success" retval="0"/>
  <sequence seq-num="1298"/>

  </record>
  ```

Beispiel 30–35 Drucken des gesamten Prüfpfads

Durch eine Pipe-Verkettung mit dem Befehl `lp` erfolgt die Ausgabe des gesamten Prüfpfads an den Drucker. Der Drucker sollte über eingeschränkten Zugriff verfügen.

```
# auditreduce | praudit | lp -d example.protected.printer
```

Beispiel 30–36 Anzeigen einer bestimmten Prüfdatei

In diesem Beispiel wird eine Zusammenfassungsdatei für die Anmeldung in einem Terminalfenster untersucht.

```
# cd /var/audit/audit_summary.dir/logins
# praudit 20100827183936.20100827232326.logins | more
```

Beispiel 30–37 Umwandeln der Prüfdatensätze in XML-Format

In diesem Beispiel werden die Prüfdatensätze in das XML-Format konvertiert.

```
# praudit -x 20100827183214.20100827215318.logins > 20100827.logins.xml
```

Die `*xml`-Datei kann in einem Browser angezeigt werden. Der Inhalt der Datei kann durch ein Skript verarbeitet werden, um die entsprechenden Informationen zu extrahieren.

Allgemeine Fehler

Eine Meldung ähnlich der folgenden weist darauf hin, dass Sie nicht über ausreichende Berechtigungen zur Verwendung des Befehls `praudit` verfügen:

```
praudit: Can't assign 20090408164827.20090408171614.example1 to stdin.
```

▼ So bereinigen Sie eine Prüfdatei des Typs `not_terminated`

In einigen Fällen wird ein Prüfdämon beendet, während die zugehörige Prüfdatei noch geöffnet ist, oder der Zugriff auf einen Server ist nicht mehr möglich. Dadurch muss der Rechner zu einem neuen Server wechseln. In diesen Fällen erhält eine Prüfdatei die Zeichenfolge `not_terminated` als Ende-Zeitstempel, obwohl die Datei nicht mehr für Prüfdatensätze verwendet wird. Verwenden Sie den Befehl `auditreduce -O`, damit die Datei den richtigen Zeitstempel erhält.

1. **Führen Sie die Dateien mit der Zeichenfolge `not_terminated` im Prüfdateisystem in der Reihenfolge der Erstellung auf.**

   ```
   # ls -R1t audit-directory*/files/* | grep not_terminated
   ```

   `-R` Führt die Dateien in Unterverzeichnissen auf

   `-t` Führt die Dateien angefangen von der neuesten bis zur ältesten Datei auf

   `-1` Führt die Dateien in einer Spalte auf

2. **Bereinigen Sie die alte `not_terminated`-Datei.**

   Geben Sie den Namen der alten Datei für den Befehl `auditreduce -O` an.

   ```
   # auditreduce -O system-name old-not-terminated-file
   ```

3. **Entfernen Sie die alte `not_terminated`-Datei.**

   ```
   # rm system-name old-not-terminated-file
   ```

Beispiel 30–38 Bereinigen der geschlossenen Prüfdateien des Typs `not_terminated`

Im folgenden Beispiel werden Dateien des Typs `not_terminated` gesucht, umbenannt und die Originale anschließend entfernt.

```
ls -R1t */files/* | grep not_terminated
.../egret.1/20100908162220.not_terminated.egret
.../egret.1/20100827215359.not_terminated.egret
# cd */files/egret.1
# auditreduce -O egret 20100908162220.not_terminated.egret
# ls -1t
20100908162220.not_terminated.egret      Current audit file
20100827230920.20100830000909.egret      Input (old) audit file
20100827215359.not_terminated.egret
# rm 20100827215359.not_terminated.egret
# ls -1t
20100908162220.not_terminated.egret      Current audit file
20100827230920.20100830000909.egret      Cleaned up audit file
```

Der Start-Zeitstempel der neuen Datei gibt den Zeitpunkt des ersten Prüfereignisses in der Datei `not_terminated` an. Der Ende-Zeitstempel gibt den Zeitpunkt des letzten Prüfereignisses in der Datei an.

▼ So verhindern Sie eine Prüfpfadüberlauf

Gehen Sie wie folgt vor, wenn die Sicherheitsrichtlinie ein Speichern aller Prüfdaten erfordert:

1. **Richten Sie einen Zeitplan ein, um die Prüfdateien in regelmäßigen Abständen zu archivieren.**

   Archivieren Sie die Prüfdateien, indem Sie ein Backup der Dateien auf Offline-Datenträgern erstellen. Außerdem können Sie die Dateien auf ein Dateisystem für die Archivierung verschieben.

   Wenn Sie Prüfprotokolle im Textformat mithilfe des Dienstprogramms `syslog` erfassen, archivieren Sie die Textprotokolle. Weitere Informationen erhalten Sie auf der Manpage `logadm(1M)`.

2. **Richten Sie einen Zeitplan ein, um archivierte Prüfdateien aus dem Prüfdateisystem zu löschen.**

3. **Speichern Sie die zusätzlichen Informationen.**

   Archivieren Sie Informationen, die zum Interpretieren der Prüfdatensätze zusammen mit dem Prüfpfad erforderlich sind.

4. **Dokumentieren Sie, welche Prüfdateien archiviert wurden.**

5. **Bewahren Sie die archivierten Datenträger entsprechend auf.**

6 **Verringern Sie den Umfang der gespeicherten Prüfdaten, indem Sie Zusammenfassungsdateien erstellen.**

Sie können Zusammenfassungsdateien aus dem Prüfpfad extrahieren, indem Sie Optionen für den Befehl `auditreduce` verwenden. Die Zusammenfassungsdateien enthalten nur Datensätze für bestimmte Typen von Prüfereignissen. Weitere Informationen zum Extrahieren der Zusammenfassungsdateien erhalten Sie unter Beispiel 30–30 und Beispiel 30–34.

Fehlerbehebung bei der Oracle Solaris-Prüfung (Aufgaben)

In diesem Abschnitt werden verschiedene Fehlermeldungen und Voreinstellungen bei der Oracle Solaris-Prüfung sowie der Prüfung mit anderen Tools vorgestellt. Diese Verfahren dienen zum Aufzeichnen der an Ihrem Standort erforderlichen Prüfereignisse.

Fehlerbehebung bei der Oracle Solaris-Prüfung (Übersicht der Schritte)

In der folgenden Übersicht der Schritte wird auf Verfahren für die Fehlerbehebung bei der Oracle Solaris-Prüfung verwiesen.

Problem	Lösung	Anweisungen
Warum wurden nach dem Konfigurieren der Prüfung keine Prüfdateien erstellt?	Führen Sie eine Fehlerbehebung des Prüfdämons und der Prüfkonfigurationsdateien durch.	„So können Sie die Ausführung der Oracle Solaris-Prüfung feststellen“ auf Seite 676
Wie kann ich den Umfang der bei der Prüfung erfassten Informationen verringern?	Führen Sie die Prüfung nur bei den gewünschten Ereignissen durch.	„So verringern Sie den Umfang der erstellten Prüfdatensätze“ auf Seite 679
Wie kann ich alle Vorgänge eines Benutzers auf dem System prüfen?	Führen Sie die Prüfung bei mindestens einem Benutzer für jeden Befehl durch.	„So prüfen Sie alle Befehle der Benutzer“ auf Seite 680
Wie kann ich die aufgezeichneten Prüfereignisse ändern und die Änderung für die vorhandenen Sitzungen übernehmen?	Aktualisieren Sie die Vorauswahlmaske eines Benutzers.	„So ändern Sie die Vorauswahlmaske eines Benutzers“ auf Seite 683
Wie kann ich Änderungen an bestimmten Dateien suchen?	Prüfen Sie die Dateiänderungen und suchen Sie anschließend mit dem Befehl `auditreduce` die entsprechenden Dateien.	„So suchen Sie nach Prüfdatensätzen der Änderungen an bestimmten Dateien“ auf Seite 683
Wie kann die Größe der Prüfdateien verringert werden?	Beschränken Sie die Größe der binären Prüfdatei.	„So beschränken Sie die Größe binärer Prüfdateien“ auf Seite 686

Problem	Lösung	Anweisungen
Wie kann ich Prüfereignisse von der Datei `audit_event` entfernen?	Aktualisieren Sie die Datei `audit_event`.	„So verhindern Sie die Prüfung bestimmter Ereignisse“ auf Seite 685
Wie kann ich alle Anmeldungen an einem Oracle Solaris-System prüfen?	Prüfen Sie die Anmeldungen von einem beliebigen System.	„So prüfen Sie Anmeldungen von anderen Betriebssystemen“ auf Seite 686
Warum werden Prüfdatensätze nicht für die FTP-Übertragungen gespeichert?	Verwenden Sie das entsprechende Prüfungs-Tool für Dienstprogramme, durch die eigene Protokolle generiert werden.	„So prüfen Sie FTP- und SFTP-Dateiübertragungen“ auf Seite 687

▼ So können Sie die Ausführung der Oracle Solaris-Prüfung feststellen

Wenn Sie annehmen, dass trotz aktivierter Prüfung keine Prüfdatensätze im primären Prüfverzeichnis generiert werden, versuchen Sie den Fehler zu beheben, indem Sie Folgendes durchführen.

Bevor Sie beginnen

Die Datenbank `hosts` im Naming Service wurde ordnungsgemäß konfiguriert und kann einwandfrei verwendet werden. Weitere Informationen zur Behebung von Fehlern beim Naming Service finden Sie in der folgenden Dokumentation:

- Manpage `nsswitch.conf(4)`
- *Systemverwaltungshandbuch: Naming Services und Directory Services (DNS, NIS und LDAP)*
- *System Administration Guide: Naming and Directory Services (NIS+)*

1 Stellen Sie fest, ob die Prüfung ausgeführt wird.

- **Vergewissern Sie sich, dass das Kernel-Modul `c2audit` geladen ist.**

  ```
  # modinfo | grep c2audit
  ```

  Keine Liste weist darauf hin, dass die Prüfung nicht ausgeführt wird. Anhand der folgenden Liste können Sie erkennen, ob die Prüfung ausgeführt wird:

  ```
  40  132ce90  14230 186   1  c2audit (C2 system call)
  ```

- **Vergewissern Sie sich, dass der Prüfdämon ausgeführt wird.**

  Überprüfen Sie den Status des Service `auditd`. Anhand der folgenden Liste können Sie erkennen, dass die Prüfung nicht ausgeführt wird:

  ```
  # svcs -x auditd
  svc:/system/auditd:default (Solaris audit daemon)
   State: disabled since Fri Aug 14 19:02:35 2009
  Reason: Disabled by an administrator.
  ```

```
   See: http://sun.com/msg/SMF-8000-05
   See: auditd(1M)
   See: audit(1M)
Impact: This service is not running.
```

Anhand der folgenden Liste können Sie erkennen, dass der Prüfservice ausgeführt wird:

```
# svcs auditd
STATE          STIME    FMRI
online         10:10:10 svc:/system/auditd:default
```

- **Überprüfen Sie die aktuelle Prüfbedingung.**

  Anhand der folgenden Liste können Sie erkennen, dass die Prüfung nicht ausgeführt wird:

  ```
  # auditconfig -getcond
  auditconfig: auditon(2) failed.
  auditconfig: error = Operation not supported(48)
  ```

  Anhand der folgenden Liste können Sie erkennen, ob die Prüfung ausgeführt wird:

  ```
  # auditconfig -getcond
  audit condition = auditing
  ```

Wenn der Prüfservice nicht ausgeführt wird, aktivieren Sie ihn. Weitere Informationen zu dem Verfahren finden Sie unter „So aktivieren Sie den Prüfservice“ auf Seite 656.

2 Überprüfen Sie die Syntax der Datei `audit_control`.

```
# audit -v /etc/security/audit_control
audit: audit_control must have either a valid "dir:" entry
or a valid "plugin:" entry with "p_dir:" specified.
```

Beheben Sie die Fehler. Die Meldung `syntax ok` gibt an, dass die Syntax der Datei ordnungsgemäß vorhanden ist.

3 Vergewissern Sie sich, dass die Datei `audit_control` über gültige Werte für die Schlüsselwörter `flags` und `naflags` verfügt.

```
# grep flags /etc/security/audit_control
flags:lo
naflags:na,lp
```

Geben Sie gültige Werte an, wenn die Datei `audit_control` ungültige Werte aufweisen sollte. Im vorhergehenden Beispiel stellt `lp` eine ungültige Klasse dar.

4 Vergewissern Sie sich, dass die Datei `audit_user` über gültige Werte für jeden Benutzer verfügt.

```
# tail audit_user
...
# User Level Audit User File
#
# File Format
#
#    username:always:never
#
root:lo:no
admin:lp:no
```

Geben Sie gültige Werte an, wenn die Datei `audit_user` ungültige Werte enthält. Im vorhergehenden Beispiel stellt `lp` eine ungültige Klasse dar.

5 Wenn Sie eine angepasste Prüfklasse erstellt haben, stellen Sie sicher, dass der Klasse Ereignisse zugewiesen wurden.

Beispielsweise enthält die folgende Datei `audit_control` eine Klasse, die von der Oracle Solaris-Software nicht bereitgestellt wird:

```
# grep flags /etc/security/audit_control
flags:lo,pf
naflags:na,lo
```

Eine Beschreibung zur Erstellung der Klasse `pf` erhalten Sie unter „So fügen Sie eine Prüfklasse hinzu“ auf Seite 646.

a. Stellen Sie sicher, dass die Klasse in der Datei `audit_class` definiert ist.

Die Maske der Prüfklasse muss eindeutig sein.

```
# grep pf /etc/security/audit_class
0x10000000:pf:profile command
```

Wenn die Klasse noch nicht definiert ist, definieren Sie sie. Entfernen Sie andernfalls die Klasse aus den Dateien `audit_control` und `audit_user`.

b. Vergewissern Sie sich, dass die Ereignisse zu der Klasse zugewiesen wurden.

```
# grep pf /etc/security/audit_event
6180:AUE_prof_cmd:profile command:ua,as,pf
```

Wenn der Klasse keine Ereignisse zugewiesen wurden, weisen Sie die entsprechenden Ereignisse zu dieser Klasse zu.

6 Wenn durch die vorhergehenden Schritte kein Fehler festgestellt wurde, überprüfen Sie die Systemprotokolldateien `/var/adm/messages` und `/var/log/syslog`.

a. Suchen Sie die Fehler und beheben Sie sie.

b. Wenn der Prüfservice ausgeführt wird, starten Sie ihn erneut.

```
# audit -s
```

c. Wenn der Prüfservice nicht ausgeführt wird, aktivieren Sie ihn.

Weitere Informationen zu dem Verfahren finden Sie unter „So aktivieren Sie den Prüfservice“ auf Seite 656.

▼ So verringern Sie den Umfang der erstellten Prüfdatensätze

Nachdem Sie die zu prüfenden Ereignisse an Ihrem Standort festgestellt haben, erstellen Sie anhand der folgenden Vorschläge einfach zu verwaltende Prüfdateien.

1 Verwenden Sie die standardmäßige Prüfrichtlinie.

Vermeiden Sie insbesondere, Ereignisse und Prüf-Token zum Prüfpfad hinzuzufügen. Die folgenden Richtlinien wirken sich auf die Größe des Prüfpfads aus.

- `arge` (Richtlinie): Fügt Umgebungsvariablen zu den `exec`-Prüfereignissen hinzu
- `argv` (Richtlinie): Fügt Befehlsparameter zu den `exec`-Prüfereignissen hinzu
- `public` (Richtlinie): Beim Prüfen von Dateiereignissen wird ein Ereignis zum Prüfpfad hinzugefügt, wenn ein prüfbares Ereignis in einer öffentlichen Datei auftritt. Zu den Dateiklassen zählen `fa`, `fc`, `fd`, `fm`, `fr`, `fw` und `cl`. Eine Definition der öffentlichen Datei erhalten Sie unter „Terminologie und Konzepte der Prüfung“ auf Seite 613.
- `path` (Richtlinie): Fügt ein `path`-Token zu den Prüfereignissen hinzu, die ein optionales `path`-Token enthalten
- `group` (Richtlinie): Fügt ein group-Token zu den Prüfereignissen hinzu, die ein optionales `newgroups`-Token enthalten
- `seq` (Richtlinie): Fügt ein sequence-Token zu allen Prüfereignissen hinzu
- `trail` (Richtlinie): Fügt ein trailer-Token zu allen Prüfereignissen hinzu
- `windata_down` (Richtlinie): Fügt Ereignisse auf einem System hinzu, das mit Trusted Extensions konfiguriert wurde, wenn Informationen in einem beschrifteten Fenster herabgestuft wurden
- `windata_up` (Richtlinie): Fügt Ereignisse auf einem System hinzu, das mit Trusted Extensions konfiguriert wurde, wenn Informationen in einem beschrifteten Fenster hochgestuft wurden
- `zonename` (Richtlinie): Fügt den Zonennamen zu allen Prüfereignissen hinzu. Wenn nur die globale Zone konfiguriert wurde, wird `zone, global` zu allen Prüfereignissen hinzugefügt.

Im folgenden Prüfdatensatz wird die Verwendung des Befehls `ls` dargestellt. Die Klasse `ex` wird geprüft und die Standardrichtlinie wird verwendet:

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

Der folgenden Datensatz wird verwendet, wenn alle Richtlinien aktiviert sind:

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
attribute,100555,root,bin,136,432,0
```

```
exec_args,1,ls
exec_env,9,HOME=/,HZ=,LANG=C,LOGNAME=root,MAIL=/var/mail/root,PATH=/u
sr/sbin:/usr/bin,SHELL=/sbin/sh,TERM=xterm,TZ=US/Pacific
path,/lib/ld.so.1
attribute,100755,root,bin,136,4289,0
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
group,root,other,bin,sys,adm,uucp,mail,tty,lp,nuucp,daemon
return,success,0
zone,global
sequence,313540
trailer,375
```

2 **Verwenden Sie das Plugin `audit_syslog.so`, um einige Prüfereignisse an `syslog` zu senden.**

Diese Strategie kann nur verwendet werden, wenn keine binären Datensätze der an `syslog`-Protokolle gesendeten Prüfereignisse gespeichert werden müssen. Mithilfe des Befehls `auditreduce` können Sie anschließend diese Datensätze von den binären Dateien entfernen, wodurch sich die Größe der binären Dateien verringert.

3 **Verwenden Sie die Datei `audit_user`, um Ereignisse für bestimmte Benutzer und Rollen zu prüfen.**

Verringern Sie den Umfang der Prüfung für alle Benutzer, indem Sie die Anzahl der Prüfklassen in der Datei `audit_control` reduzieren. Fügen Sie in der Datei `audit_user` Prüfklassen für bestimmte Benutzer und Rollen hinzu.

4 **Erstellen Sie eine eigene angepasste Prüfklasse.**

Sie können Prüfklassen an Ihrem Standort erstellen. Fügen Sie alle zu überwachenden Prüfereignisse zu diesen Klassen hinzu. Eine Beschreibung des Verfahrens erhalten Sie unter „So fügen Sie eine Prüfklasse hinzu“ auf Seite 646.

Hinweis – Wenn Sie vorhandene Prüfklassenzuordnungen ändern, gehen die Änderungen bei einem Upgrade zu einer neuen Version von Oracle Solaris-Betriebssystem möglicherweise verloren. Lesen Sie die Installationsprotokolle sorgfältig durch.

▼ So prüfen Sie alle Befehle der Benutzer

An einigen Standorten erfordern die Sicherheitsrichtlinien möglicherweise, dass die Prüfdatensätze aller Befehle, die vom `root`-Benutzer oder von administrativen Rollen ausgeführt werden, erfasst werden. Andere Standorte erfordern möglicherweise die Erfassung der Prüfdatensätze aller Befehle, die von Benutzern ausgeführt werden.

1 Prüfen Sie die Klassen `lo` und `ex`.

Die Klasse `ex` prüft alle Aufrufe der Funktionen `exec()` und `execve()`. Die Klasse `lo` prüft Anmeldungen, Abmeldungen und Bildschirmsperrungen. Durch die folgende Ausgabe werden alle Ereignisse in den Klassen `ex` und `lo` aufgeführt.

```
7:AUE_EXEC:exec(2):ps,ex
23:AUE_EXECVE:execve(2):ps,ex
...
6152:AUE_login:login - local:lo
6153:AUE_logout:logout:lo
6154:AUE_telnet:login - telnet:lo
6155:AUE_rlogin:login - rlogin:lo
6158:AUE_rshd:rsh access:lo
6159:AUE_su:su:lo
6162:AUE_rexecd:rexecd:lo
6163:AUE_passwd:passwd:lo
6164:AUE_rexd:rexd:lo
6165:AUE_ftpd:ftp access:lo
6171:AUE_ftpd_logout:ftp logout:lo
6172:AUE_ssh:login - ssh:lo
6173:AUE_role_login:role login:lo
6212:AUE_newgrp_login:newgrp login:lo
6213:AUE_admin_authenticate:admin login:lo
6221:AUE_screenlock:screenlock - lock:lo
6222:AUE_screenunlock:screenlock - unlock:lo
6227:AUE_zlogin:login - zlogin:lo
```

- **Um diese Klassen auf Administratoren zu prüfen, ändern Sie die Datei `audit_user`.**

  Im folgenden Beispiel wurden an dem Standort drei Rollen (`sysadm`, `auditadm` und `netadm`) erstellt. Diese Rollen und das `root`-Konto werden auf die Klassen `exec` und `lo` geprüft:

  ```
  ## audit_user file
  root:lo,ex:no
  sysadm:lo,ex:no
  auditadm:lo,ex:no
  netadm:lo,ex:no
  ```

- **Um die Klasse `lo` auf nicht zuweisbare Ereignisse zu prüfen, ändern Sie die Datei `audit_control`.**

  ```
  ## audit_control file
  ...
  naflags:lo
  ...
  ```

- **Um diese Klassen auf alle Benutzer zu prüfen, ändern Sie die Datei `audit_control`.**

  ```
  ## audit_control file
  flags:lo,ex
  naflags:lo
  ...
  ```

  Es wird eine Ausgabe ähnlich der folgenden angezeigt:

  ```
  header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
  path,/usr/bin/ls
  ```

```
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

2 Um die Argumente für Befehle aufzuzeichnen, legen Sie die Richtlinie `argv` fest.

```
## audit_startup script
...
auditconfig -setpolicy +argv
...
```

Durch das Token `exec_args` werden die Befehlsargumente aufgezeichnet:

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
exec_args,1,ls
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

3 Um die Umgebung für die Ausführung des Befehls aufzuzeichnen, legen Sie die Richtlinie `arge` fest.

```
## audit_startup script
...
auditconfig -setpolicy +arge
...
```

Durch das Token `exec_env` wird die Befehlsumgebung aufgezeichnet:

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
exec_env,9,HOME=/,HZ=,LANG=C,LOGNAME=root,MAIL=/var/mail/root,
  PATH=/usr/sbin:/usr/bin,SHELL=/sbin/sh,TERM=xterm,TZ=US/Pacific
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

4 Um die Argumente und die Befehlsumgebung aufzuzeichnen, legen Sie beide Richtlinien fest.

```
## audit_startup script
...
auditconfig -setpolicy +argv
auditconfig -setpolicy +arge
...
```

Es wird eine Ausgabe ähnlich der folgenden angezeigt:

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
exec_args,1,ls
exec_env,9,HOME=/,HZ=,LANG=C,LOGNAME=root,MAIL=/var/mail/root,
  PATH=/usr/sbin:/usr/bin,SHELL=/sbin/sh,TERM=xterm,TZ=US/Pacific
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

So suchen Sie nach Prüfdatensätzen der Änderungen an bestimmten Dateien

Wenn Sie Dateiaufzeichnungen bei einer beschränkten Anzahl von Dateien protokollieren möchten, beispielsweise `/etc/passwd` und die Dateien im Verzeichnis `/etc/default`, suchen Sie die Dateien mithilfe des Befehls `auditreduce`.

1 **Prüfen Sie die Klasse `fw`.**

Indem Sie die Klasse zur Datei `audit_user` anstatt zur Datei `audit_control` hinzufügen, werden weniger Datensätze generiert.

- **Fügen Sie die Klasse `fw` zur Datei `audit_user` hinzu.**

```
## audit_user file
root:fw:no
sysadm:fw:no
auditadm:fw:no
netadm:fw:no
```

- **Fügen Sie die Klasse `fw` zur Datei `audit_control` hinzu.**

```
## audit_control file
flags:lo,fw
...
```

2 **Um die Prüfdatensätze bestimmter Dateien zu suchen, verwenden Sie den Befehl `auditreduce`.**

```
# /usr/sbin/auditreduce -o file=/etc/passwd,/etc/default -O filechg
```

Durch den Befehl `auditreduce` wird der Prüfpfad nach allen Instanzen des Arguments `file` durchsucht. Der Befehl erstellt eine binäre Datei mit dem Suffix `filechg`, die alle Datensätze mit den Pfadnamen der gewünschten Dateien enthält. Weitere Informationen zur Syntax der Option `-o file=`*pathname* erhalten Sie auf der Manpage `auditreduce(1M)`.

3 **Verwenden Sie zum Lesen der Datei `filechg` den Befehl `praudit`.**

```
# /usr/sbin/praudit *filechg
```

So ändern Sie die Vorauswahlmaske eines Benutzers

Wenn Sie die Datei `audit_control` oder `audit_user` ändern, ändert sich die Vorauswahlmaske der bereits angemeldeten Benutzer nicht. Sie müssen das Ändern der Vorauswahlmaske erzwingen.

Bevor Sie beginnen Sie haben die Prüfung aktiviert, die Benutzer sind angemeldet und Sie haben den Wert von `flags` oder `naflags` in der Datei `audit_control` geändert. Sie möchten die bereits angemeldeten Benutzer auf diese neu ausgewählten Prüfklassen prüfen.

1. **Aktualisieren Sie die Vorauswahlmaske der bereits angemeldeten Benutzer.**

   Es sind folgende zwei Möglichkeiten verfügbar. Sie können die vorhandenen Sitzungen beenden oder mit dem Befehl `auditconfig` die Vorauswahlmasken der Benutzer aktualisieren.

   - **Beenden Sie die vorhandenen Sitzungen der Benutzer.**

     Die Benutzer können sich abmelden und anschließend erneut anmelden oder der Administrator kann die aktiven Sitzungen manuell beenden (abbrechen). Die neuen Sitzungen übernehmen die neue Vorauswahlmaske. Das Beenden der Benutzer kann sich jedoch als unpraktisch erweisen.

   - **Ändern Sie dynamisch die Vorauswahlmaske der einzelnen Benutzer.**

     Beispielsweise wurde das Attribut `flags` in der Datei `audit_control` von `lo` in `lo,ex` geändert.

     a. **Stellen Sie die Prüf-ID eines Benutzers und die Prüfsitzungs-ID fest.**

        Suchen Sie zunächst alle gewöhnlichen Benutzer. Im folgenden Beispiel sucht der Administrator nach allen Prozessen, deren Eigentümer nicht `root`, `daemon` oder `lp` ist:

        ```
        # /usr/bin/pgrep -v -u root,daemon,lp | more
        ..
        3941
        3948
        3949
        10640 ...
        ```

        Verwenden Sie anschließend einen der Benutzerprozesse, um die Prüf-ID des Benutzers zu suchen:

        ```
        # auditconfig -getpinfo 3941
        audit id = jdoe(1002)
        process preselection mask = lo(0x1000,0x1000)
        terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
        audit session id = 713
        ```

        Achten Sie darauf, dass die Vorauswahlmaske des Benutzers die Klasse `lo` enthält und die neu hinzugefügte Klasse `ex` nicht enthält.

     Die Prüf-ID des Benutzers lautet `1002`. Die Prüfsitzungs-ID des Benutzers lautet `713`.

2. **Ändern Sie die Vorauswahlmaske des Benutzers.**

   Verwenden Sie eine der folgenden zwei Methoden:

   - **Verwenden Sie die Prüfsitzungs-ID des Benutzers, um die Vorauswahlmaske des Benutzers zu ändern.**

     ```
     # /usr/sbin/auditconfig -setsmask lo,ex 713
     ```

- **Verwenden Sie die Prüf-ID des Benutzers, um die Vorauswahlmaske des Benutzers zu ändern.**

  ```
  # /usr/sbin/auditconfig -setumask lo,ex 1002
  ```

3. **Vergewissern Sie sich, dass die Vorauswahlmaske geändert wurde.**

   ```
   # auditconfig -getpinfo 3941
   audit id = jdoe(1002)
   process preselection mask = ex,lo(0x40001000,0x40001000)
   terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
   audit session id = 713
   ```

▼ So verhindern Sie die Prüfung bestimmter Ereignisse

Aus Wartungsgründen muss an einigen Standorten möglicherweise verhindert werden, dass Prüfereignisse geprüft werden.

1. **Ändern Sie die Klasse des Ereignisses in die Klasse `no`.**

   Beispielsweise gehören die Ereignisse 26 und 27 zur Klasse `pm`.

   ```
   ## audit_event file
   ...
   25:AUE_VFORK:vfork(2):ps
   26:AUE_SETGROUPS:setgroups(2):pm
   27:AUE_SETPGRP:setpgrp(2):pm
   28:AUE_SWAPON:swapon(2):no
   ...
   ```

   Ändern Sie die Klasse dieser Ereignisse in die Klasse `no`.

   ```
   ## audit_event file
   ...
   25:AUE_VFORK:vfork(2):ps
   26:AUE_SETGROUPS:setgroups(2):no
   27:AUE_SETPGRP:setpgrp(2):no
   28:AUE_SWAPON:swapon(2):no
   ...
   ```

   Wenn die Klasse `pm` derzeit geprüft wird, werden die Ereignisse 26 und 27 weiterhin in den vorhandenen Sitzungen geprüft. Damit diese Ereignisse nicht geprüft werden, müssen Sie die Vorauswahlmasken der Benutzer aktualisieren.

Achtung – Setzen Sie die Ereignisse in der Datei `audit_event` niemals in Kommentare. Diese Datei wird vom Befehl `praudit` zum Lesen binärer Prüfdateien verwendet. Archivierte Prüfdateien enthalten möglicherweise Ereignisse, die in der Datei aufgeführt sind.

2. **Anweisungen zum Aktualisieren der Vorauswahlmasken der Benutzer erhalten Sie unter „So ändern Sie die Vorauswahlmaske eines Benutzers“ auf Seite 683.**

▼ So beschränken Sie die Größe binärer Prüfdateien

Für die Größe der binären Prüfdateien gibt es keine Beschränkung. Sie können die Größe beschränken, um die Archivierung und Suche zu erleichtern. Außerdem können Sie auch kleinere binäre Dateien aus der Originaldatei erstellen.

1 **Verwenden Sie ab der Version Solaris 10 10/08 das Attribut `p_fsize`, um die Größe der jeweiligen binären Prüfdateien zu beschränken.**

Durch das Attribut `p_fsize` des Plugins `audit_binfile.so` können Sie die Größe einer Prüfdatei beschränken. Der Standardwert ist Null (0), wodurch keine Beschränkung für die Dateigröße besteht. Der Wert wird in Byte von 512.000 bis 2.147.483.647 angegeben. Wenn die angegebene Größe erreicht wurde, wird die aktuelle Prüfdatei geschlossen und eine neue Datei geöffnet.

Im folgenden Beispiel wird die Größe einer Prüfdatei auf 1 MB begrenzt:

```
plugin:name=audit_binfile.so; p_dir:/var/audit; p_fsize=1024000
```

2 **Wählen Sie mit dem Befehl `auditreduce` die Datensätze aus und zeichnen Sie diese Datensätze in einer Datei auf, um sie für eine weitere Analyse zu verwenden.**

Durch die Optionen `auditreduce` *-lowercase* werden bestimmte Datensätze gesucht.

Durch die Optionen `auditreduce` *-Uppercase* wird die Auswahl in eine Datei geschrieben. Weitere Informationen erhalten Sie auf der Manpage `auditreduce(1M)`.

▼ So prüfen Sie Anmeldungen von anderen Betriebssystemen

Bei Oracle Solaris können alle Anmeldungen unabhängig von der Quelle geprüft werden.

- **Prüfen Sie die Klasse `lo` auf zuweisbare und nicht zuweisbare Ereignisse.**

Durch diese Klasse werden Anmeldungen, Abmeldungen und Bildschirmsperrungen geprüft.

```
## audit_control file
flags:lo
naflags:lo
...
```

Hinweis – Um `ssh`-Anmeldungen zu prüfen, muss auf dem Oracle Solaris-System der `ssh`-Dämon von Oracle Solaris ausgeführt werden. Dieser Dämon wurde für die Oracle Solaris-Prüfung geändert. Weitere Informationen erhalten Sie unter „Oracle Solaris Secure Shell und das OpenSSH-Projekt“ auf Seite 368.

▼ So prüfen Sie FTP- und SFTP-Dateiübertragungen

Der FTP-Service erstellt Protokolle der zugehörigen Dateiübertragungen. Der SFTP-Service, der unter dem SSH-Protokoll ausgeführt wird, kann durch die Oracle Solaris-Prüfung geprüft werden. Die Anmeldungen an beiden Services können durch die Oracle Solaris-Prüfung geprüft werden.

1 Weitere Informationen zum Protokollieren von Befehlen und Dateiübertragungen des FTP-Service erhalten Sie auf der Manpage `ftpaccess(4)`.

Weitere Informationen zu den verfügbaren Protokollierungsoptionen erhalten Sie im Abschnitt zu den Protokollierungsfunktionen. Insbesondere durch die Optionen `log commands` und `log transfers` erhalten Sie hilfreiche Protokolle.

2 Verwenden Sie mindestens eine der beiden folgenden Vorgehensweisen, um `sftp`-Dateiübertragungen zu protokollieren:

- **Prüfen Sie die Dateilesezugriffe.**

  Bei Dateiübertragungen über eine SSH-Verbindung wird der Befehl `sftp` verwendet. Diese Übertragungen können mithilfe des Prüf-Flags `+fr` aufgezeichnet werden. Um fehlgeschlagene `sftp`-Dateiübertragungen zu prüfen, verwenden Sie das Prüf-Flag `-fr`.

  Im Folgenden sehen Sie die Ausgabe einer erfolgreichen `sftp`-Sitzung:

  ```
  header,138,2,open(2) - read,,ma2,2009-08-25 14:48:58.770 -07:00
  path,/home/jdoe/vpn_connect
  attribute,100644,jdoe,staff,391,437,0
  subject,jdoe,jdoe,staff,jdoe,staff,4444,120289379,8457 65558 ma1
  return,success,6
  ```

- **Verwenden Sie die Option für eine ausführliche Ausgabe des Befehls `sftp`.**

  Die Option `-v` (verbose) kann bis zu dreimal wiederholt werden.

  ```
  # sftp -vvv [ other options ] hostname
  ```

3 Um den Zugriff auf die FTP- und SFTP-Services aufzuzeichnen, prüfen Sie die Klasse `lo`.

Wie Sie anhand der folgenden Ausgabe sehen, werden durch das An- und Abmelden beim Dämon `ftpd` Prüfdatensätze generiert.

```
% bsmrecord -c lo | more
...
in.ftpd
  program     /usr/sbin/in.ftpd    See ftp access
  event ID    6165                 AUE_ftpd
  class       lo                   (0x00001000)
      header
      subject
      [text]                       error message
      return

in.ftpd
```

```
  program     /usr/sbin/in.ftpd    See ftp logout
  event ID    6171                 AUE_ftpd_logout
  class       lo                   (0x00001000)
      header
      subject
      return
...
```

Durch die SSH-Anmeldung werden alle Zugriffe auf den Befehl `sftp` aufgezeichnet.

```
...
/usr/lib/ssh/sshd
  program     /usr/lib/ssh/sshd    See login - ssh
  event ID    6172                 AUE_ssh
  class       lo                   (0x00001000)
      header
      subject
      [text]                       error message
      return
```

◆ ◆ ◆ KAPITEL 31

Prüfung bei Oracle Solaris (Referenz)

In diesem Kapitel werden die wichtigsten Komponenten der Oracle Solaris-Prüfung beschrieben. In der folgenden Liste sind die Referenzinformationen in diesem Kapitel aufgeführt.

- „Befehle zur Prüfung“ auf Seite 689
- „Im Prüfservice verwendete Dateien“ auf Seite 695
- „Berechtigungsprofile für Verwalten der Prüfung“ auf Seite 702
- „Prüfung und Oracle Solaris-Zonen“ auf Seite 702
- „Prüfklassen“ auf Seite 703
- „Prüf-Plugins“ auf Seite 706
- „Prüfrichtlinie“ auf Seite 706
- „Verarbeiten der Prüfungsmerkmale“ auf Seite 707
- „Prüfpfad“ auf Seite 707
- „Namenskonventionen für binäre Prüfdateien“ auf Seite 708
- „Struktur von Prüfdatensätzen“ auf Seite 709
- „Formate der Prüf-Token“ auf Seite 711

Eine Übersicht zur Prüfung bei Oracle Solaris finden Sie unter Kapitel 28, „Prüfung bei Oracle Solaris (Übersicht)“. Vorschläge zur Planung erhalten Sie unter Kapitel 29, „Planen der Oracle Solaris-Prüfung“. Vorgehensweisen zum Konfigurieren der Prüfung an Ihrem Standort finden Sie unter Kapitel 30, „Verwalten der Oracle Solaris-Prüfung (Aufgaben)“.

Befehle zur Prüfung

In diesem Abschnitt erhalten Sie Informationen zu den folgenden Befehlen:

- „Dämon `auditd`“ auf Seite 690
- „Befehl `audit`“ auf Seite 691
- „Befehl `bsmrecord`“ auf Seite 691
- „Befehl `auditreduce`“ auf Seite 691
- „Befehl `praudit`“ auf Seite 693

- „Befehl auditconfig“ auf Seite 695

Dämon auditd

In der folgenden Liste sind die Aufgaben des Dämons auditd zusammengefasst:

- Öffnet und schließt Prüfdateien in den Verzeichnissen, die in der Datei audit_control angegeben sind. Die Dateien werden in der angegebenen Reihenfolge geöffnet.
- Lädt mindestens ein Plugin. Oracle bietet zwei Plugins. Durch das Plugin audit_binfile.so werden binäre Prüfdaten in eine Datei geschrieben. Durch das Plugin audit_syslog.so werden ausgewählte Textzusammenfassungen der Prüfdatensätze im Protokoll syslog gespeichert.
- Liest Prüfdaten aus dem Kernel und gibt die Daten durch ein auditd-Plugin aus
- Führt das Skript audit_warn aus, um Warnungen zu verschiedenen Bedingungen auszugeben. Durch das Plugin audit_binfile.so wird das Skript audit_warn ausgeführt. Mithilfe des Skripts werden standardmäßig Warnungen an den E-Mail-Alias audit_warn und an die Konsole gesendet. Durch das Plugin syslog.so wird das Skript audit_warn nicht ausgeführt.
- Wenn alle Prüfverzeichnisse voll sind, werden die Prozesse, die Prüfdatensätze generieren, standardmäßig angehalten. Außerdem sendet der Dämon auditd eine Meldung an die Konsole und den E-Mail-Alias audit_warn. Zu diesem Zeitpunkt kann nur der Systemadministrator Fehler am Prüfservice beheben. Der Administrator kann sich anmelden und Prüfdateien für Offline-Datenträger schreiben, Prüfdateien aus dem System löschen und andere Bereinigungsaufgaben durchführen.

  Die Prüfrichtlinie kann mit dem Befehl auditconfig neu konfiguriert werden.

Der Dämon auditd kann automatisch gestartet werden, wenn das System im Mehrbenutzermodus gebootet wurde. Sie können den Dämon auch über die Befehlszeile starten. Wenn der Dämon auditd gestartet wurde, wird der freie Speicherplatz berechnet, der für die Prüfdateien erforderlich ist.

Der Dämon auditd verwendet eine Liste der Prüfverzeichnisse in der Datei audit_control als mögliche Speicherorte zum Erstellen von Prüfdateien. Der Dämon weist einen Zeiger auf diese Liste der Verzeichnisse auf, wobei das erste Verzeichnis zuerst verwendet wird. Beim Erstellen einer Prüfdatei durch den Dämon auditd wird die Datei zum ersten verfügbaren Verzeichnis der Liste hinzugefügt. Die Liste beginnt am aktuellen Zeiger des Dämons auditd. Sie können den Zeiger an den Anfang der Liste zurücksetzen, indem Sie den Befehl audit -s ausführen. Durch den Befehl audit -n wird der Dämon angewiesen, zu einer neuen Prüfdatei zu wechseln. Die neue Datei wird im gleichen Verzeichnis erstellt wie die aktuelle Datei.

Befehl `audit`

Durch den Befehl `audit` werden die Aktionen des Dämons `auditd` gesteuert. Durch den Befehl `audit` können die folgenden Aufgaben durchgeführt werden:

- Aktivieren und Deaktivieren der Prüfung
- Zurücksetzen des Dämons `auditd`
- Anpassen der Maske für die Vorauswahl der Prüfung auf dem lokalen System
- Schreiben der Prüfdatensätze in eine andere Prüfdatei

Eine Beschreibung der verfügbaren Optionen erhalten Sie auf der Manpage `audit`(1M).

Befehl `bsmrecord`

Durch den Befehl `bsmrecord` wird das Format der Prüfereignisse angezeigt, die in der Datei `/etc/security/audit_event` definiert sind. Die Ausgabe enthält der Reihe nach die Prüf-ID des Ereignisses, die Prüfklasse, das Prüf-Flag und die Prüf-Token des Datensatzes. Wenn keine Option angegeben ist, wird die Ausgabe `bsmrecord` in einem Terminalfenster angezeigt. Wenn die Option `-h` angegeben ist, eignet sich die Ausgabe für die Ansicht in einem Browser. Beispiele zur Verwendung des Befehls `bsmrecord` erhalten Sie unter „So zeigen Sie Prüfdatensatzformate an“ auf Seite 665. Weitere Informationen finden Sie auf der Manpage `bsmrecord`(1M).

Befehl `auditreduce`

Durch den Befehl `auditreduce` werden die im binären Format gespeicherten Prüfdatensätze zusammengefasst. Mit dem Befehl können Prüfdatensätze aus mindestens einer Eingabeprüfdatei zusammengeführt werden. Außerdem können Sie mit dem Befehl eine Nachauswahl der Prüfdatensätze durchführen. Die Datensätze bleiben jedoch im binären Format erhalten. Um den gesamten Prüfpfad zusammenzuführen, führen Sie diesen Befehl auf dem Prüfserver aus. Der Prüfserver ist das System, auf dem alle Prüfdateisysteme für die Installation eingehängt werden. Weitere Informationen erhalten Sie auf der Manpage `auditreduce`(1M).

Mit dem Befehl `auditreduce` können Sie alle geprüften Aktionen auf mehreren Systemen von einem Speicherort aus verfolgen. Durch den Befehl kann die logische Kombination aller Prüfdateien als ein einziger Prüfpfad gelesen werden. Sie müssen alle Systeme an einem Standort für die Prüfung identisch konfigurieren sowie Server und lokale Verzeichnisse für die Prüfdateien erstellen. Durch den Befehl `auditreduce` werden die Generierung oder der Speicherort der Datensätze nicht berücksichtigt. Wenn keine Optionen angegeben sind, werden durch den Befehl `auditreduce` die Prüfdatensätze von allen Prüfdateien in allen Unterverzeichnissen des Stammverzeichnisses für die Prüfung zusammengeführt. Das Stammverzeichnis der Prüfung lautet normalerweise `/etc/security/audit`. Durch den Befehl

`auditreduce` werden die zusammengeführten Ergebnisse an die Standardausgabe gesendet. Außerdem können die Ergebnisse in einer einzelnen Ausgabedatei in chronologischer Reihenfolge hinzugefügt werden. Die Datei enthält binäre Daten.

Durch den Befehl `auditreduce` können außerdem bestimmte Datensatztypen für die Analyse ausgewählt werden. Die Funktionen zum Zusammenführen und Auswählen des Befehls `auditreduce` sind logisch unabhängig voneinander. Durch den Befehl `auditreduce` werden Daten aus den Eingabedateien als die zu lesenden Datensätze erfasst, bevor die Dateien zusammengeführt und anschließend auf die Festplatte geschrieben werden.

Die Angabe von Optionen für den Befehl `auditreduce` ermöglicht Folgendes:

- Anfordern von Prüfdatensätzen, die von bestimmten Prüfklassen generiert wurden
- Anfordern von Prüfdatensätzen, die von einem bestimmten Benutzer generiert wurden
- Anfordern von Prüfdatensätzen, die zu bestimmten Zeitpunkten generiert wurden

Wenn keine Argumente angegeben sind, werden durch den Befehl `auditreduce` die Unterverzeichnisse im Verzeichnis `/etc/security/audit` (dem standardmäßigen Stammverzeichnis für die Prüfung) überprüft. Der Befehl sucht nach einem Verzeichnis `files`, das die Dateien *start-time.end-time.hostname* enthält. Der Befehl `auditreduce` ist sehr hilfreich, wenn die Prüfdaten in separaten Verzeichnissen vorhanden sind. Abbildung 31–1 zeigt Prüfdaten in separaten Verzeichnissen für verschiedene Hosts. Abbildung 31–2 zeigt Prüfdaten in separaten Verzeichnissen für verschiedene Prüfserver.

ABBILDUNG 31–1 Prüfpfad-Speicherplatz sortiert nach Host

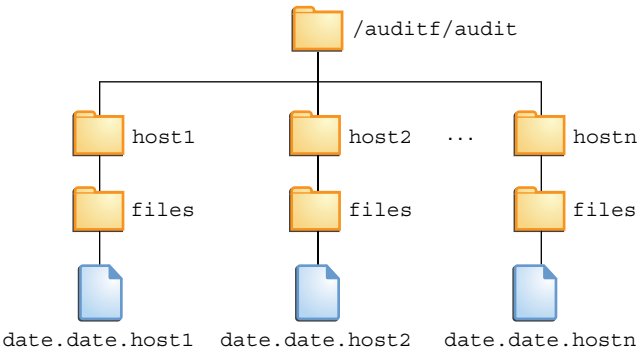
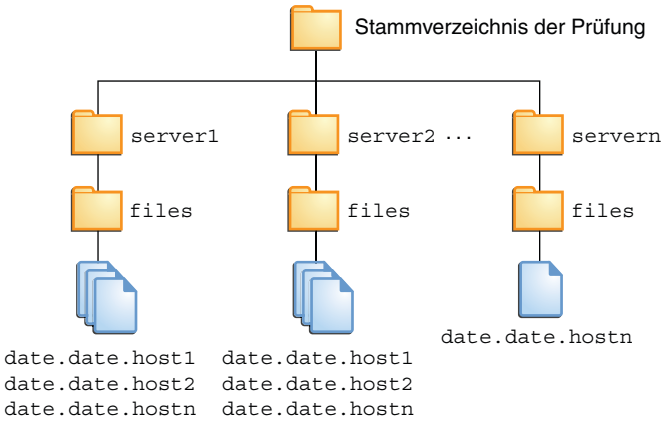


ABBILDUNG 31–2 Prüfpfad-Speicherplatz sortiert nach Server



Wenn die Partition für das Verzeichnis `/etc/security/audit` sehr klein ist, können die Prüfdaten im Standardverzeichnis möglicherweise nicht gespeichert werden. Sie können den Befehl `auditreduce` an ein anderes Verzeichnis weiterleiten, indem Sie die Option `-R` verwenden:

```
# auditreduce -R /var/audit-alt
```

Außerdem können Sie ein bestimmtes Unterverzeichnis angeben, indem Sie die Option `-S` verwenden:

```
# auditreduce -S /var/audit-alt/host1
```

Weitere Informationen zu Optionen und weitere Beispiele erhalten Sie auf der Manpage `auditreduce`(1M).

Befehl `praudit`

Durch den Befehl `praudit` wird die binäre Ausgabe des Befehls `auditreduce` in ein lesbares Format konvertiert. Durch den Befehl `praudit` werden Prüfdatensätze von der Standardeingabe im binären Format gelesen und in einem für die Darstellung geeigneten Format angezeigt. Die Eingabe kann durch eine Pipe-Verkettung über den Befehl `auditreduce` oder eine einzelne Prüfdatei durchgeführt werden. Die Eingabe kann ebenfalls erstellt werden, indem der Befehl `cat` für die Verkettung mehrerer Dateien oder der Befehl `tail` für eine aktuelle Prüfdatei verwendet wird.

Mit dem Befehl `praudit` können vier Ausgabeformate generiert werden. Durch die fünfte Option, `-l` (lang), wird ein Prüfdatensatz pro Ausgabezeile gedruckt. Standardmäßig wird ein Prüf-Token pro Ausgabezeile verwendet. Durch die Option `-d` wird der Begrenzer, der zwischen Token-Feldern und Token verwendet wird, geändert. Der standardmäßige Begrenzer ist ein Komma.

- **Standardwert**: Durch den Befehl `praudit` ohne Angabe von Optionen wird ein Prüf-Token pro Zeile angezeigt. Durch den Befehl wird das Prüfereignis anhand der Beschreibung angezeigt, z. B. Systemaufruf `ioctl(2)`. Die als Text darstellbaren Werte werden im Textformat angezeigt. Beispielsweise wird ein Benutzer mit dem Benutzernamen und nicht mit der Benutzer-ID angezeigt.
- **Option –r**: Die Option für die Ansicht unverarbeiteter Daten zeigt die numerisch darstellbaren Werte als Zahlen an. Beispielsweise wird ein Benutzer durch die Benutzer-ID, Internetadressen im Hexadezimalformat und Modi im oktalen Format dargestellt. Das Prüfereignis wird durch die zugehörige Ereignisnummer angezeigt, beispielsweise `158`.
- **Option –s**: Die Option für die Ansicht im Kurzformat zeigt das Prüfereignis durch den zugehörigen Tabellennamen an, beispielsweise `AUE_IOCTL`. Durch die Option werden die anderen Token so wie von der Standardoption angezeigt.
- **Option –x**: Durch die XML-Option wird der Prüfdatensatz im XML-Format angezeigt. Diese Option eignet sich als Eingabe für Browser oder als Eingabe für die XML verarbeitenden Skripten.

  Das XML wird durch eine DTD beschrieben, die durch den Prüfservice bereitgestellt wird. Von der Oracle Solaris-Software wird ebenfalls ein Stylesheet zur Verfügung gestellt. Die DTD und das Stylesheet sind im Verzeichnis `/usr/share/lib/xml` enthalten.

Im Standardausgabeformat des Befehls `praudit` wird jeder Datensatz durch eine Sequenz von Prüf-Token einfach identifiziert. Jedes Token wird in einer separaten Zeile dargestellt. Am Anfang der Datensätze steht ein `header`-Token. Die Ausgabe können Sie beispielsweise mit dem Befehl `awk` weiterverarbeiten.

Im Folgenden sehen Sie die Ausgabe des Befehls `praudit -l` für ein `header`-Token:

```
header,173,2,settppriv(2),,example1,2010-10-10 10:10:02.020 -07:00
```

Im Folgenden sehen Sie die Ausgabe des Befehls `praudit -r` für das gleiche `header`-Token:

```
121,173,2,289,0x0000,192.168.86.166,1066077962,174352445
```

BEISPIEL 31–1 Verarbeiten der Ausgabe `praudit` mit einem Skript

In einigen Fällen möchten Sie die Ausgabe des Befehls `praudit` als Textzeilen verarbeiten. Beispiel: Sie möchten Datensätze auswählen, die durch den Befehl `auditreduce` nicht ausgewählt werden können. Mit einem einfachen Shell-Skript können Sie die Ausgabe des Befehls `praudit` verarbeiten. Im folgenden Beispiel eines einfachen Skripts wird ein Prüfdatensatz in einer Zeile dargestellt, nach einer benutzerspezifischen Zeichenfolge gesucht und anschließend die Prüfdatei in der ursprünglichen Form zurückgegeben.

```
#!/bin/sh
#
## This script takes an argument of a user-specified string.
#  The sed command prefixes the header tokens with Control-A
#  The first tr command puts the audit tokens for one record
```

BEISPIEL 31–1 Verarbeiten der Ausgabe `praudit` mit einem Skript *(Fortsetzung)*

```
#  onto one line while preserving the line breaks as Control-A
#
praudit | sed -e '1,2d' -e '$s/^file.*$//' -e 's/^header/^aheader/' \\
| tr '\\012\\001' '\\002\\012' \\
| grep "$1" \\       Finds the user-specified string
| tr '\\002' '\\012'       Restores the original newline breaks
```

Beachten Sie, dass `^a` im Skript der Tastenkombination Control-A und nicht den zwei Zeichen `^` und `a` entspricht. Das Präfix unterscheidet das Token `header` von der als Text anzeigbaren Zeichenfolge `header`.

Befehl `auditconfig`

Der Befehl `auditconfig` bietet eine Befehlszeilenschnittstelle, um die Prüfkonfigurationsparameter abzurufen und einzustellen. Durch den Befehl `auditconfig` können die folgenden Aufgaben durchgeführt werden:

- Anzeigen, Überprüfen und Konfigurieren der Prüfrichtlinie
- Feststellen, ob die Prüfung aktiviert oder deaktiviert ist
- Verwalten des Prüfverzeichnisses und der Prüfdatei
- Verwalten der Prüfwarteschlange
- Abrufen und Einstellen von Masken für die Vorauswahl
- Abrufen und Einstellen der Zuordnungen zwischen Prüfereignis und Prüfklasse
- Abrufen und Einstellen von Konfigurationsinformationen wie Sitzungs-ID und Prüf-ID
- Konfigurieren der Prüfungsmerkmale für einen Prozess, eine Shell und eine Sitzung
- Zurücksetzen der Prüfstatistik

Eine Beschreibung der Befehlsoptionen finden Sie auf der Manpage `auditconfig(1M)`.

Im Prüfservice verwendete Dateien

Der Prüfservice verwendet folgende Dateien:

- „Datei `system`“ auf Seite 696
- „Datei `syslog.conf`“ auf Seite 696
- „Datei `audit_class`“ auf Seite 696
- „Datei `audit_control`“ auf Seite 697
- „Datei `audit_event`“ auf Seite 698
- „Skript `audit_startup`“ auf Seite 699
- „Datenbank `audit_user`“ auf Seite 699

- „Skript audit_warn“ auf Seite 700
- „Skript bsmconv“ auf Seite 701

Datei system

Die Datei /etc/system enthält Befehle, die vom Kernel während der Initialisierung gelesen werden, um die Systemvorgänge anzupassen. Durch die Shell-Skripten bsmconv und bsmunconv, die zur Aktivierung und Deaktivierung der Prüfung dienen, wird die Datei /etc/system geändert. Durch das Shell-Skript bsmconv wird die folgende Zeile zur Datei /etc/system hinzugefügt:

```
set c2audit:audit_load=1
```

Durch den Eintrag set c2audit:audit_load=1 wird das Kernel-Modul für die Prüfung geladen, wenn das System gebootet wird. Durch das Shell-Skript bsmunconv wird die Prüfung deaktiviert, wenn das System erneut gebootet wird. Durch den Befehl wird die Zeile c2audit aus der Datei /etc/system entfernt.

Datei syslog.conf

Die Datei /etc/syslog.conf wird zusammen mit dem Plugin audit_syslog.so verwendet, um Prüfdatensätze im Textformat zu speichern. Die Datei syslog.conf kann konfiguriert werden, um das Dienstprogramm syslog für die Speicherung von Prüfdatensätzen zu aktivieren. Ein Beispiel finden Sie unter „So konfigurieren Sie syslog-Prüfprotokolle“ auf Seite 641.

Datei audit_class

Durch die Datei /etc/security/audit_class werden die Prüfklassen definiert. Prüfklassen sind Gruppen von Prüfereignissen. Mit dem Klassennamen in der Datei audit_control können Sie die Klassen im Voraus auswählen, deren Ereignisse geprüft werden sollen. Die Klassen verwenden Präfixe, um nur fehlgeschlagene oder nur erfolgreiche Ereignisse auszuwählen. Weitere Informationen erhalten Sie unter „Syntax der Prüfklassen“ auf Seite 704.

Der Superuser oder ein Administrator mit einer entsprechenden Rolle kann die Definitionen der Prüfklassen ändern. Dieser Administrator kann neue Prüfklassen definieren, vorhandene Klassen umbenennen oder vorhandene Klassen anderweitig ändern, indem die Datei audit_class in einem Texteditor bearbeitet wird. Weitere Informationen erhalten Sie auf der Manpage audit_class(4).

Datei audit_control

Die Datei /etc/security/audit_control auf den einzelnen Systemen enthält Konfigurationsinformationen für den Dämon auditd. Mithilfe der Datei können die Systeme ein Remote-Prüfdateisystem einhängen, um die zugehörigen Prüfdatensätze zu speichern.

Sie können fünf verschiedene Informationstypen in der Datei audit_control speichern. Jede Zeile mit Informationen beginnt mit einem Schlüsselwort.

- flags **(Schlüsselwort)**: Steht am Anfang des Eintrags, durch den die zu prüfenden Ereignisklassen für alle Benutzer im System im Voraus ausgewählt werden. Die hier angegebenen Prüfklassen bestimmen die *systemweite Maske für die Vorauswahl der Prüfung*. Die Prüfklassen werden durch Kommata getrennt.
- naflags **(Schlüsselwort)**: Steht am Anfang des Eintrags, durch den die zu prüfenden Ereignisklassen im Voraus ausgewählt werden, wenn eine Aktion keinem bestimmten Benutzer zugewiesen werden kann. Die Prüfklassen werden durch Kommata getrennt. Die Ereignisklasse na gehört zu diesem Eintrag. Der Eintrag naflags kann zum Protokollieren anderer (normalerweise) zuweisbarer Ereignisklassen verwendet werden, die (in diesem Fall) nicht zugewiesen werden können. Wenn beispielsweise ein Programm einen Boot-Vorgang startet und eine Datei liest, wird durch fr im Eintrag naflags ein Datensatz für dieses Ereignis erstellt.
- minfree **(Schlüsselwort)**: Dieses Schlüsselwort ist veraltet und wird nicht mehr verwendet. Verwenden Sie das Attribut p_minfree für das Plugin audit_binfile.so.

  Durch das Attribut p_minfree wird der Speicherplatz, der mindestens verfügbar sein soll, für alle Prüfdateisysteme als Prozentsatz angegeben. Der Prozentsatz muss größer oder gleich 0 sein. Der Standardwert ist 20 Prozent. Wenn ein Prüfdateisystem zu 80 Prozent voll ist, werden die Prüfdaten im nächsten verfügbaren Prüfverzeichnis gespeichert. Weitere Informationen erhalten Sie auf der Manpage audit_warn(1M).
- dir **(Schlüsselwort)**: Dieses Schlüsselwort ist veraltet und wird nicht mehr verwendet. Verwenden Sie das Attribut p_dir für das Plugin audit_binfile.so.

  Durch das Attribut p_dir werden die Verzeichnisspeicherorte aufgeführt. Durch jeden Zeilenwert werden ein Prüfdateisystem und Verzeichnis definiert, die das System zum Speichern der Prüfdateien verwendet. Sie können mindestens einen Verzeichnisspeicherort angeben. Dabei ist die Reihenfolge der Werte wichtig. Der Dämon auditd erstellt die Prüfdateien in den Verzeichnissen in der angegebenen Reihenfolge. Das erste Verzeichnis entspricht dem *primären Prüfverzeichnis* des Systems. Das zweite Verzeichnis ist das *sekundäre Prüfverzeichnis*, in dem der Dämon auditd die Prüfdateien erstellt, wenn das erste Prüfverzeichnis voll ist. Es wird also das jeweils höhere Verzeichnis verwendet. Weitere Informationen erhalten Sie auf der Manpage audit(1M).
- plugin **(Schlüsselwort)**: Gibt den *Plugin-Pfad* für die Plugin-Module audit_binfile.so und audit_syslog.so an. Durch das Modul audit_binfile.so werden binäre Prüfdateien erstellt. Das Modul audit_syslog.so liefert eine Echtzeitkonvertierung der Oracle

Solaris-Prüfdatensätze in Text. Die Prüfklassen, die im Attribut `p_flags` des Plugins `audit_syslog.so` angegeben sind, müssen ein untergeordneter Satz der im Voraus ausgewählten Prüfklassen sein.

Weitere Informationen zur Datei `audit_control` erhalten Sie auf der Manpage `audit_control(4)`. Weitere Informationen zu Plugins erhalten Sie unter „Prüf-Plugins“ auf Seite 706 und auf den Manpages `audit_binfile(5)` und `audit_syslog(5)`.

BEISPIEL 31–2 Beispiel für Datei `audit_control`

Im Folgenden sehen Sie eine Beispieldatei `audit_control` für das System `noddy`. Von `noddy` werden zwei Prüfdateisysteme auf dem Prüfserver `blinken` und ein drittes Prüfdateisystem, das auf dem zweiten Prüfserver `winken` eingehängt ist, verwendet. Das dritte Dateisystem wird nur verwendet, wenn die Prüfdateisysteme auf `blinken` voll oder nicht verfügbar sind. Ein Wert von 20 Prozent für `minfree` bedeutet, dass das Warnungs-Skript ausgeführt wird, wenn die Dateisysteme zu 80 Prozent voll sind. Die Einstellungen legen fest, dass Anmeldungen und administrative Vorgänge geprüft werden sollen. Die Vorgänge werden auf eine fehlerhafte und erfolgreiche Ausführung geprüft. Es werden Fehler aller Arten, mit Ausnahme von Fehlern beim Erstellen eines Dateisystemobjekts, geprüft. Nicht zuweisbare Ereignisse können ebenfalls geprüft werden. Im Prüfprotokoll `syslog` werden weniger Prüfereignisse aufgezeichnet. Dieses Protokoll enthält Textzusammenfassungen der fehlgeschlagenen Anmeldungen und fehlgeschlagenen administrativen Vorgänge.

In der Version Solaris 10 sind die Zeilen `dir` und `minfree` veraltet und werden nicht mehr verwendet. Im folgenden Beispiel enthalten die `plugin`-Zeilen keinen Zeilenumbruch.

```
flags:lo,am,-all,^-fc
naflags:lo,nt
plugin:name=audit_binfile.so; p_minfree=20; p_dir=/var/audit/blinken/files,
/var/audit/blinken.1/files,/var/audit/winken
plugin:name=audit_syslog.so; p_flags=-lo,-am
```

Datei `audit_event`

Die Datei `/etc/security/audit_event` enthält die standardmäßigen Zuordnungen zwischen Prüfereignis und Prüfklasse. Durch Bearbeiten dieser Datei können Sie die Klassenzuordnungen ändern. Nach dem Ändern der Klassenzuordnungen müssen Sie das System neu booten oder den Befehl `auditconfig -conf` ausführen, um die geänderten Zuordnungen in den Kernel zu übernehmen. Weitere Informationen erhalten Sie auf der Manpage `audit_event(4)`.

Skript `audit_startup`

Durch das Skript `/etc/security/audit_startup` wird der Prüfservice automatisch konfiguriert, wenn das System in den Mehrbenutzermodus wechselt. Der Dämon `auditd` wird gestartet, nachdem vom Skript folgende Aufgaben durchgeführt wurden:

- Konfigurieren der Zuordnungen zwischen Prüfereignis und Prüfklasse
- Einstellen der Prüfrichtlinienoptionen

Weitere Informationen erhalten Sie auf der Manpage `audit_startup(1M)`.

Datenbank `audit_user`

In der Datenbank `/etc/security/audit_user` können die systemweiten im Voraus ausgewählten Klassen für einen bestimmten Benutzer geändert werden. Durch die Klassen, die Sie zu einem Benutzereintrag in der Datenbank `audit_user` hinzugefügt haben, werden die Einstellungen in der Datei `audit_control` auf zwei Arten geändert:

- Angeben von Prüfklassen, die immer für diesen Benutzer geprüft werden sollen
- Angeben von Prüfklassen, die niemals für diesen Benutzer geprüft werden sollen

Jeder Benutzereintrag in der Datenbank `audit_user` enthält drei Felder:

username:*always-audit-classes*:*never-audit-classes*

Die Prüffelder werden in einer Sequenz verarbeitet.

- Durch das Feld *always-audit-classes* wird die Prüfung der Klassen in diesem Feld aktiviert. Verwenden Sie dieses Feld, um systemweite Einstellungen zu ändern. Wenn Sie beispielsweise `all` im Feld *always-audit-classes* angeben, werden alle Daten für einen Benutzer geprüft.
- Durch das Feld *never-audit-classes* wird die Prüfung der Klassen in diesem Feld deaktiviert. Verwenden Sie dieses Feld, um die Systemeinstellungen zu überschreiben. Wenn Sie `all` im Feld *never-audit-classes* angeben, wird die gesamte Prüfung für den Benutzer deaktiviert, sogar die in der Datei `audit_control` angegebenen Prüfklassen.

Beispiel: Sie möchten die systemweiten Prüfeinstellungen auf den Benutzer `tamiko` anwenden, es sei denn der Lesezugriff auf Dateisystemobjekte war erfolgreich. Beachten Sie den zweiten Doppelpunkt (`:`) im folgenden Eintrag `audit_user`:

```
tamiko:^+fr:no          modify system defaults for fr
```

Der vorhergehende Eintrag bedeutet, dass alle Informationen geprüft werden sollen, mit Ausnahme von erfolgreichen Dateilesezugriffen.

Wenn Sie alle Informationen für den Benutzer `tamiko` mit Ausnahme von erfolgreichen Dateilesezugriffen prüfen möchten, können Sie folgenden Eintrag verwenden:

```
tamiko:all,^+fr:no          audit everything except fr
```

Beispiel: Sie möchten Systemstandardwerte für erfolgreiche Dateilesezugriffe für den Benutzer `tamiko` überschreiben. Der folgende Eintrag bedeutet, dass alle Informationen mit Ausnahme von erfolgreichen Dateilesezugriffen geprüft werden.

```
tamiko:all:+fr              override system defaults for fr
```

Hinweis – Erfolgreiche und fehlgeschlagene Ereignisse werden separat behandelt. Bei einem Prozess können mehr Prüfdatensätze für fehlgeschlagene als für erfolgreiche Ereignisse generiert werden.

Skript `audit_warn`

Das Skript `/etc/security/audit_warn` sendet eine Benachrichtigung an einen E-Mail-Alias, wenn der Dämon `auditd` eine ungewöhnliche Bedingung beim Schreiben der Prüfdatensätze feststellt. Sie können dieses Skript Ihrem Standort entsprechend anpassen, um eine Warnung bei Bedingungen auszugeben, die möglicherweise einen Benutzereingriff erfordern. Oder Sie können eine automatische Verarbeitung dieser Bedingungen angeben. Bei allen Fehlerbedingungen wird durch das Skript `audit_warn` eine Meldung in `syslog` mit dem Schweregrad von `daemon.alert` ausgegeben. Mithilfe von `syslog.conf` können Sie die Konsolenansicht von `syslog`-Meldungen konfigurieren. Durch das Skript `audit_warn` wird ebenfalls eine Meldung an den E-Mail-Alias `audit_warn` gesendet. Sie können diesen Alias als Teil der Prüfkonfiguration festlegen.

Wenn der Dämon `auditd` die folgenden Bedingungen feststellt, wird das Skript `audit_warn` aufgerufen. Das Skript sendet eine E-Mail an den Alias `audit_warn`.

- Ein Prüfverzeichnis hat den für `minfree` festgelegten Wert überschritten. Der Wert `minfree` bzw. der untere Grenzwert ist ein Prozentsatz des verfügbaren Speicherplatzes auf einem Prüfdateisystem.

  Das Skript `audit_warn` wird mit der Zeichenfolge `soft` und dem Namen des Verzeichnisses, dessen verfügbarer Speicherplatz unter dem Mindestwert liegt, aufgerufen. Der Dämon `auditd` wechselt automatisch zum nächsten verfügbaren Verzeichnis. Der Dämon schreibt die Prüfdateien in dieses neue Verzeichnis, bis das Verzeichnis den zugehörigen Wert für `minfree` erreicht hat. Der Dämon `auditd` verwendet der Reihenfolge nach das nächste Verzeichnis, das in der Datei `audit_control` aufgeführt ist. Der Dämon zeichnet die Prüfdatensätze auf, bis der Grenzwert für `minfree` des jeweiligen Verzeichnisses erreicht ist.
- Bei allen Prüfverzeichnissen ist der Schwellenwert für `minfree` erreicht.

  Das Skript `audit_warn` wird durch die Zeichenfolge `allsoft` aufgerufen. Eine Meldung wird an die Konsole gesendet. Eine E-Mail wird ebenfalls an den Alias `audit_warn` gesendet.

Wenn alle Prüfverzeichnisse, die in der Datei `audit_control` aufgeführt sind, den zugehörigen Schwellenwert für `minfree` erreicht haben, wechselt der Dämon `auditd` zum ersten Verzeichnis zurück. Der Dämon zeichnet die Prüfdatensätze auf, bis das Verzeichnis vollständig voll ist.

- Ein Prüfverzeichnis ist vollständig voll und es ist kein Speicherplatz verfügbar.

  Das Skript `audit_warn` wird mit der Zeichenfolge `hard` und dem Namen des Verzeichnisses aufgerufen. Eine Meldung wird an die Konsole gesendet. Eine E-Mail wird ebenfalls an den Alias `audit_warn` gesendet.

  Der Dämon `auditd` wechselt automatisch zum nächsten geeigneten Verzeichnis, das über Speicherplatz verfügt. Der Dämon `auditd` verwendet der Reihenfolge nach das nächste Verzeichnis, das in der Datei `audit_control` aufgeführt ist. Der Dämon zeichnet die Prüfdatensätze auf, bis das jeweilige Verzeichnis voll ist.

- Alle Prüfverzeichnisse sind vollständig voll. Das Skript `audit_warn` wird mit der Zeichenfolge `allhard` als Argument aufgerufen.

  Standardmäßig wird eine Meldung an die Konsole gesendet. Eine E-Mail wird ebenfalls an den Alias `audit_warn` gesendet. Prozesse, durch die normalerweise Prüfdatensätze generiert werden, treten zwar weiterhin auf, aber die Prüfdatensätze werden gezählt. Prüfdatensätze werden nicht generiert. Ein Beispiel für diese Situation finden Sie unter Beispiel 30–16 und „So verhindern Sie eine Prüfpfadüberlauf“ auf Seite 674.

- Ein interner Fehler ist aufgetreten. Folgende interne Fehler können auftreten:
  - `ebusy`: Ein anderer `auditd`-Dämonprozess wird bereits ausgeführt.
  - `tmpfile`: Eine temporäre Datei kann nicht verwendet werden.
  - `postsigterm`: Beim Herunterfahren der Prüfung wurde ein Signal erhalten.
  - `plugin` *name*: Ein Fehler ist bei der Ausführung des Plugins aufgetreten.

- Ein Fehler bei der Syntax der Datei `audit_control` wurde festgestellt. Standardmäßig wird eine Meldung an die Konsole gesendet. Eine E-Mail wird ebenfalls an den Alias `audit_warn` gesendet.

Wenn die Prüfrichtlinie `perzone` festgelegt ist, wird durch die `auditd`-Instanz der nicht globalen Zone das `audit_warn`-Skript der Zone aufgerufen. Weitere Informationen erhalten Sie auf der Manpage `audit_warn`(1M).

Skript `bsmconv`

Durch das Skript `/etc/security/bsmconv` wird der Prüfservice aktiviert. Durch den Befehl `bsmunconv` wird der Prüfservice deaktiviert. Nach dem Ausführen des Skripts `bsmconv` konfigurieren Sie die Prüfverzeichnisse und Prüfkonfigurationsdateien. Beim erneuten Booten wird die Prüfung aktiviert.

Weitere Informationen erhalten Sie auf der Manpage `bsmconv`(1M).

Berechtigungsprofile für Verwalten der Prüfung

Oracle Solaris bietet Berechtigungsprofile für das Konfigurieren des Prüfservice und für das Analysieren des Prüfpfads.

- **Audit Control**: Aktiviert eine Rolle zum Konfigurieren der Oracle Solaris-Prüfung. Dieses Berechtigungsprofil gewährt Autorisierungen, um die vom Prüfservice verwendeten Dateien zu konfigurieren. Durch das Profil wird ebenfalls eine Rolle zum Ausführen von Prüfbefehlen aktiviert. Bei einer Rolle mit dem Profil "Audit Control" können folgende Befehle ausgeführt werden: `audit`, `auditd`, `auditconfig`, `bsmconv` und `bsmunconv`.
- **Audit Review**: Aktiviert eine Rolle zum Analysieren der Oracle Solaris-Prüfdatensätze. Dieses Profil gewährt eine Autorisierung zum Lesen der Prüfdatensätze mit den Befehlen `praudit` und `auditreduce`. Bei einer Rolle mit diesem Berechtigungsprofil kann ebenfalls der Befehl `auditstat` ausgeführt werden.
- **System Administrator**: Beinhaltet das Berechtigungsprofil "Audit Review". Bei einer Rolle mit dem Berechtigungsprofil "System Administrator" können Sie Prüfdatensätze analysieren.

Weitere Informationen zum Konfigurieren von Rollen für den Prüfservice erhalten Sie unter „Konfigurieren von RBAC (Übersicht der Schritte)“ auf Seite 214.

Prüfung und Oracle Solaris-Zonen

Nicht globale Zonen können genauso wie die globale Zone geprüft werden. Außerdem ist in nicht globalen Zonen eine eigene Festlegung von Flags, Speicher und Prüfrichtlinien möglich.

Wenn eine identische Prüfung für alle Zonen durchgeführt wird, werden die Einstellungen für die Prüfung in den einzelnen Zonen in den Konfigurationsdateien der globalen Zone vorgenommen. Die Richtlinienoption `+zonename` ist hilfreich. Wenn diese Option festgelegt ist, enthalten die Prüfdatensätze aller Zonen den Namen der Zone. Anschließend können die Prüfdatensätze bei der Nachauswahl nach dem Zonennamen ausgewählt werden. Eine Beschreibung der Prüfrichtlinie finden Sie unter „Festlegen der Prüfrichtlinien“ auf Seite 629. Ein Beispiel finden Sie unter „So konfigurieren Sie die Prüfrichtlinie“ auf Seite 653.

Zonen können auch einzeln geprüft werden. Wenn die Richtlinienoption `perzone` in der globalen Zone festgelegt ist, werden in jeder nicht globalen Zone ein eigener Prüfdämon ausgeführt, eine eigene Prüfwarteschlange verwaltet und der Inhalt und Speicherort der zugehörigen Prüfdatensätze angegeben. In einer nicht globalen Zone können außerdem die meisten Prüfrichtlinienoptionen festgelegt werden. Es kann keine Richtlinie festgelegt werden, die sich auf das gesamte System auswirkt, das heißt von einer nicht globalen Zone können die Richtlinien `ahlt` oder `perzone` nicht festgelegt werden. Eine weitere Beschreibung erhalten Sie unter „Prüfung auf Systemen mit Oracle Solaris-Zonen“ auf Seite 620 und „So planen Sie die Prüfung der Zonen“ auf Seite 624.

Weitere Informationen zur Zonen finden Sie in Teil II, „Zonen“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.

Prüfklassen

Systemweite Standardwerte für die Prüfung bei Oracle Solaris werden im Voraus ausgewählt, indem Sie mindestens eine Klasse der Ereignisse angeben. Die Klassen werden für jedes System in der Datei `audit_control` des Systems im Voraus ausgewählt. Alle Benutzer, die das System verwenden, werden auf diese Ereignisklassen geprüft. Eine Beschreibung der Datei erhalten Sie unter „Datei `audit_control`“ auf Seite 697.

Sie können Prüfklassen konfigurieren und neue Prüfklassen erstellen. Die Namen der Prüfklassen können aus bis zu acht Zeichen bestehen. Für die Beschreibung der Klasse können maximal 72 Zeichen verwendet werden. Numerische und alphanumerische Zeichen sind zulässig.

Sie können die für einen bestimmten Benutzer geprüften Objekte ändern, indem Sie Prüfklassen zu einem Benutzereintrag in der Datenbank `audit_user` hinzufügen. Die Prüfklassen werden außerdem als Argumente für den Befehl `auditconfig` verwendet. Ausführliche Informationen erhalten Sie auf der Manpage `auditconfig`(1M).

Definitionen der Prüfklassen

Die folgende Tabelle zeigt die einzelnen vordefinierten Prüfklassen, den beschreibenden Namen der jeweiligen Prüfklasse und eine Kurzbeschreibung.

TABELLE 31–1 Vordefinierte Prüfklassen

Prüfklasse	Beschreibender Name	Beschreibung
`all`	`all`	Alle Klassen (Metaklasse)
`no`	`no_class`	Nullwert für Deaktivieren der Ereignisvorauswahl
`na`	`non_attrib`	Nicht zuweisbare Ereignisse
`fr`	`file_read`	Lesen von Daten, offen für Lesezugriff
`fw`	`file_write`	Schreiben von Daten, offen für Schreibzugriff
`fa`	`file_attr_acc`	Zugriff der Objektattribute: `stat`, `pathconf`
`fm`	`file_attr_mod`	Ändern der Objektattribute: `chown`, `flock`
`fc`	`file_creation`	Erstellen eines Objekts
`fd`	`file_deletion`	Löschen eines Objekts

TABELLE 31–1 Vordefinierte Prüfklassen *(Fortsetzung)*

Prüfklasse	Beschreibender Name	Beschreibung
cl	file_close	close (Systemaufruf)
ap	application	Anwendungsdefiniertes Ereignis
ad	administrative	Administrative Aktionen (veraltete administrative Metaklasse)
am	administrative	Administrative Aktionen (Metaklasse)
ss	system state	Ändern des Systemstatus
as	system-wide administration	Systemweite Verwaltung
ua	user administration	Benutzerverwaltung
aa	audit administration	Prüfungsauslastung
ps	process start	Prozessbeginn und Prozessende
pm	process modify	Prozessänderung
pc	process	Prozess (Metaklasse)
ex	exec	Programmausführung
io	ioctl	ioctl() (Systemaufruf)
ip	ipc	System V IPC-Vorgänge
lo	login_logout	Anmelde- und Abmeldeereignisse
nt	network	Netzwerkereignisse: bind, connect, accept
ot	other	Verschiedenes wie Gerätezuordnung und memcntl()

Sie können neue Klassen definieren, indem Sie die Datei /etc/security/audit_class ändern. Außerdem können Sie vorhandene Klassen umbenennen. Weitere Informationen erhalten Sie auf der Manpage audit_class(4).

Syntax der Prüfklassen

Ereignisse können auf Erfolg, auf Fehler und auf beides geprüft werden. Ohne eine Präfixangabe wird eine Ereignisklasse auf eine erfolgreiche oder fehlerhafte Durchführung geprüft. Bei einem Pluszeichen (+) als Präfix wird eine Ereignisklasse nur auf eine erfolgreiche Durchführung geprüft. Bei einem Minuszeichen (-) als Präfix wird eine Ereignisklasse nur auf eine fehlerhafte Durchführung geprüft. Die folgende Tabelle enthält einige mögliche Darstellungen von Prüfklassen.

TABELLE 31–2 Prüfklassen mit Plus- und Minuszeichen als Präfix

[*prefix*] *class*	Erläuterung
`lo`	Prüfung aller erfolgreichen An- und Abmeldeversuche und aller fehlerhaften Anmeldeversuche. Ein fehlerhafter Abmeldeversuch eines Benutzers ist nicht möglich.
`+lo`	Prüfung aller erfolgreichen An- und Abmeldeversuche
`-all`	Prüfung aller fehlerhaften Ereignisse
`+all`	Prüfung aller erfolgreichen Ereignisse

Achtung – Durch die Klasse `all` können umfangreiche Datenmengen generiert werden und der Speicherplatz der Prüfdateisysteme schnell belegt werden. Verwenden Sie die Klasse `all` nur, wenn ein wichtiger Grund für die Prüfung aller Aktivitäten vorliegt.

Prüfklassen, die bereits ausgewählt wurden, können durch ein Caret-Präfix (^) weiter angepasst werden. In der folgenden Tabelle sehen Sie, wie durch das Caret-Präfix eine im Voraus ausgewählte Prüfklasse geändert wird.

TABELLE 31–3 Caret-Präfix zum Ändern bereits angegebener Prüfklassen

^[*prefix*]*class*	Erläuterung
`-all,^-fc`	Prüfung aller fehlerhaften Ereignisse, mit Ausnahme von fehlerhaften Versuchen zum Erstellen von Dateiobjekten
`am,^+aa`	Prüfung aller administrativen Ereignisse auf erfolgreiche oder fehlerhafte Durchführung, mit Ausnahme von erfolgreichen Versuchen zur Verwaltung der Prüfung
`am,^ua`	Prüfung aller administrativen Ereignisse auf erfolgreiche und fehlerhafte Durchführung, mit Ausnahme von Benutzeradministrationsereignissen

Die Prüfklassen und die zugehörigen Präfixe können in den folgenden Dateien und Befehlen verwendet werden:

- In der Zeile `flags` der Datei `audit_control`
- In der Zeile `plugin:name=audit_syslog.so; p_flags=` der Datei `audit_control`
- Im Benutzereintrag der Datenbank `audit_user`
- Als Argumente für die `auditconfig`-Befehlsoptionen

Ein Beispiel zur Verwendung der Präfixe in der Datei `audit_control` finden Sie unter „Datei `audit_control`“ auf Seite 697.

Prüf-Plugins

Die Prüf-Plugins geben an, wie die Prüfdatensätze in der Prüfwarteschlange verarbeitet werden. Die Prüf-Plugins werden mit einem Namen in der Datei `audit_control` angegeben: `audit_binfile.so` und `audit_syslog.so`. Durch die Plugins und die zugehörigen Parameter können Sie Folgendes festlegen:

- Ziel, an das binäre Daten gesendet werden sollen, indem das Plugin `audit_binfile.so` mit dem Parameter `p_dir` verwendet wird
- Verbleibender Speicherplatz auf einer Festplatte, bevor eine Warnung an den Administrator gesendet wird, indem das Plugin `audit_binfile.so` mit dem Parameter `p_minfree` verwendet wird
- Maximale Größe einer Prüfdatei, indem das Plugin `audit_binfile.so` mit dem Parameter `p_fsize` verwendet wird

  Das Parameter-Plugin `p_fsize` ist ab der Version Solaris 10 10/08 verfügbar.
- Eine Auswahl an Prüfdatensätzen, die an `syslog` gesendet werden sollen, indem das Plugin `audit_syslog.so` mit dem Parameter `p_flags` verwendet wird
- Maximale Anzahl der Prüfdatensätze, die für das Plugin in der Warteschlange sind, indem der Parameter `qsize` verwendet wird

Weitere Informationen erhalten Sie auf den Manpages `audit_binfile(5)`, `audit_syslog(5)` und `audit_control(4)`.

Prüfrichtlinie

Die Prüfrichtlinie bestimmt, ob zusätzliche Informationen zum Prüfpfad hinzugefügt werden.

Durch die folgenden Richtlinien werden Token zu den Prüfdatensätzen hinzugefügt: `arge`, `argv`, `group`, `path`, `seq`, `trail`, `windata_down`, `windata_up` und `zonename`.

Durch die restlichen Richtlinien werden keine Token hinzugefügt. Die Richtlinien `ahlt` und `cnt` bestimmen die Aktionen, die durchgeführt werden, wenn die Kernel-Prüfdatensätze nicht bereitgestellt werden können. Die Richtlinie `public` schränkt die Prüfung der öffentlichen Dateien ein. Die Richtlinie `perzone` erstellt separate Prüfwarteschlangen für nicht globale Zonen.

Die Auswirkungen der verschiedenen Prüfrichtlinienoptionen werden unter „Festlegen der Prüfrichtlinien“ auf Seite 629 beschrieben. Eine Beschreibung der Prüfrichtlinienoptionen erhalten Sie im Abschnitt zur Option `-setpolicy` auf der Manpage `auditconfig(1M)`. Um eine Liste der verfügbaren Richtlinienoptionen zu erhalten, führen Sie den Befehl `auditconfig -lspolicy` aus.

Verarbeiten der Prüfungsmerkmale

Die folgenden Prüfungsmerkmale werden bei der erstmaligen Anmeldung festgelegt:

- **Prozessvorauswahlmaske**: Eine Kombination der Prüfklassen aus der Datei `audit_control` und der Datenbank `audit_user`. Bei der Anmeldung eines Benutzer werden durch den Anmeldeprozess die im Voraus ausgewählten Klassen zu einer *Prozessvorauswahlmaske* für die Benutzerprozesse kombiniert. In der Prozessvorauswahlmaske wird angegeben, ob durch die Ereignisse in den einzelnen Prüfklassen Prüfdatensätze generiert werden sollen.

  Durch den folgenden Algorithmus wird beschrieben, wie das System die Prozessvorauswahlmaske des Benutzers erhält:

  `(flags` *line* `+` *always-audit-classes*`)` `-` *never-audit-classes*

  Die Prüfklassen aus der Zeile `flags` in der Datei `audit_control` werden zu den Klassen im Feld *always-audit-classes* des Benutzereintrags der Datenbank `audit_user` hinzugefügt. Anschließend werden vom Gesamtwert die Klassen vom Feld *never-audit-classes* des Benutzers abgezogen.
- **Prüf-ID**: Ein Prozess erhält eine Prüf-ID, wenn sich der Benutzer anmeldet. Die Prüf-ID wird von allen untergeordneten Prozessen übernommen, die vom Anfangsprozess des Benutzers gestartet wurden. Mithilfe der Prüf-ID kann die Verantwortlichkeit durchgesetzt werden. Auch wenn ein Benutzer ein `root`-Benutzer wird, bleibt die Prüf-ID gleich. Anhand der Prüf-ID, die in den einzelnen Prüfdatensätzen gespeichert ist, können Sie die Aktionen immer auf den ursprünglich angemeldeten Benutzer zurückführen.
- **Prüfsitzungs-ID**: Die Prüfsitzungs-ID wird bei der Anmeldung zugewiesen. Die Sitzungs-ID wird von allen untergeordneten Prozessen übernommen.
- **Terminal-ID (Port-ID, Rechneradresse)**: Die Terminal-ID besteht aus dem Hostnamen und der Internetadresse, gefolgt von einer eindeutigen Nummer, die für das physische Gerät steht, an dem der Benutzer angemeldet ist. In den meisten Fällen erfolgt die Anmeldung über die Konsole. Die Nummer, die dem Konsolengerät entspricht, lautet `0`.

Prüfpfad

Der *Prüfpfad* enthält binäre Prüfdateien. Das Protokoll wird vom Dämon `auditd` erstellt. Nach dem Aktivieren des Prüfservice durch den Befehl `bsmconv` wird der Dämon `auditd` beim Booten des Systems gestartet. Der Dämon `auditd` erfasst die Prüfpfaddaten und zeichnet die Prüfdatensätze auf.

Die Prüfdatensätze werden im binären Format auf den Dateisystemen gespeichert, die für die Prüfdateien dediziert sind. Obwohl Sie Prüfverzeichnisse auf Dateisystemen physisch verwenden, die nicht für die Prüfung dediziert sind, führen Sie diesen Vorgang *ausschließlich*

für die als Reserve dienenden Verzeichnisse aus. Reserveverzeichnisse sind Verzeichnisse, in denen Prüfdateien nur dann aufgezeichnet werden, wenn kein anderes geeignetes Verzeichnis verfügbar ist.

In dem im Folgenden beschriebenen Szenario kann die Verwendung von Prüfverzeichnissen außerhalb des dedizierten Prüfdateisystems ebenfalls geeignet sein. Dies ist der Fall in einer Softwareentwicklungsumgebung, bei der das Durchführen einer Prüfung optional ist. Die vollständige Ausnutzung des verfügbaren Festplattenspeichers kann wichtiger sein als die Verwaltung eines Prüfpfads. Bei einer Umgebung, in der die Sicherheit jedoch wichtig ist, ist die Verwendung von Prüfverzeichnissen in anderen Dateisystemen nicht zulässig.

Beachten Sie die folgenden Faktoren bei der Verwaltung von Prüfdateisystemen:

- Ein Host muss über mindestens ein lokales Prüfverzeichnis verfügen. Das lokale Verzeichnis kann als ein Reserveverzeichnis verwendet werden, wenn keine Kommunikation zwischen dem Host und dem Prüfserver möglich ist.
- Einhängen der Prüfverzeichnisse mit der Option für Schreib-/Lesezugriff (`rw`). Wenn Sie die Prüfverzeichnisse über ein Remote-System einhängen, können Sie auch die Optionen `intr` und `noac` verwenden.
- Auflisten der Prüfdateisysteme auf dem Prüfserver, auf dem sie vorhanden sind. In der Exportliste sollten alle Systeme enthalten sein, die am Standort geprüft werden.

Namenskonventionen für binäre Prüfdateien

Jede binäre Prüfdatei ist eine in sich abgeschlossene Sammlung von Datensätzen. Der Name der Datei gibt den Zeitraum an, während dessen die Datensätze generiert wurden, sowie das System, von dem sie generiert wurden.

Namen von binären Prüfdateien

Die Namen von abgeschlossenen Prüfdateien liegen im folgenden Format vor:

start-time.end-time.system

start-time	Zeitpunkt, an dem der erste Prüfdatensatz in der Prüfdatei generiert wurde
end-time	Zeitpunkt, an dem der letzte Datensatz in die Datei geschrieben wurde
system	Name des Systems, von dem die Datei generiert wurde

Der Name einer noch aktiven Prüfdatei liegt im folgenden Format vor:

start-time`.not_terminated.`*system*

Beispiele für Namen von Prüfdateien des Typs `not_terminated` und für geschlossene Prüfdateien finden Sie unter „So bereinigen Sie eine Prüfdatei des Typs `not_terminated`“ auf Seite 673.

Zeitstempel für binäre Prüfdateien

Die Zeitstempel in den Dateinamen werden vom Befehl `auditreduce` verwendet, um Datensätze in einem bestimmten Zeitraum zu suchen. Diese Zeitstempel sind wichtig, da Prüfdateien von einem Zeitraum von mindestens einem Monat online vorhanden sein können. Das Durchsuchen aller Dateien nach Datensätzen, die in den letzten 24 Stunden generiert wurden, wäre zu aufwändig.

Die Zeitstempel *start-time* und *end-time* verfügen über eine Auflösung von einer Sekunde. Die Angabe erfolgt in GMT (Greenwich Mean Time). Das Format besteht aus vier Stellen für das Jahr, gefolgt von jeweils zwei Stellen für Monat, Tag, Stunde, Minute und Sekunde:

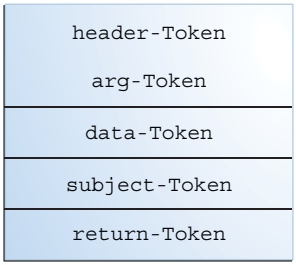
YYYYMMDDHHMMSS

Die Zeitstempel werden in GMT angegeben, um sicherzustellen, dass sie in der richtigen Reihenfolge (auch bei unterschiedlichen Zeitzonen) geordnet werden. Aufgrund der Angabe in GMT müssen das Datum und die Uhrzeit auf die aktuelle Zeitzone übertragen werden, um entsprechende Angaben zu erhalten. Beachten Sie dies, wenn Sie diese Dateien mit den standardmäßigen Dateibefehlen anstatt mit dem Befehl `auditreduce` bearbeiten.

Struktur von Prüfdatensätzen

Ein Prüfdatensatz ist eine Sequenz von Prüf-Token. Jeder Token enthält Ereignisinformationen wie Benutzer-ID, Uhrzeit und Datum. Ein Token `header` steht am Anfang eines Prüfdatensatzes und ein optionales Token `trailer` steht am Ende des Datensatzes. Die anderen Prüf-Token enthalten Informationen, die für das Prüfereignis wichtig sind. In der folgenden Abbildung sehen Sie einen normalerweise verwendeten Prüfdatensatz.

ABBILDUNG 31–3 Struktur eines normalerweise verwendeten Prüfdatensatzes



Analyse von Prüfdatensätzen

Die Analyse von Prüfdatensätzen besteht aus einer Nachauswahl der Datensätze aus dem Prüfpfad. Für die Analyse der erfassten binären Daten können Sie eine der folgenden Methoden verwenden.

- Sie können eine Analyse (ein Parsing) des binären Datenstroms durchführen. Für ein Parsing des Datenstroms müssen Sie die Reihenfolge der Felder in den einzelnen Token kennen sowie die Reihenfolge der Token in den einzelnen Datensätzen. Außerdem müssen Sie die Varianten der Prüfdatensätze kennen. Beispielsweise wird durch den Systemaufruf `ioctl()` ein Prüfdatensatz für "Falscher Dateiname" erstellt, der verschiedene Token aus dem Prüfdatensatz für "Ungültiger Dateideskriptor" enthält.
  - Eine Beschreibung der Reihenfolge binärer Daten in den einzelnen Prüf-Token erhalten Sie auf der Manpage `audit.log(4)`.
  - Eine Beschreibung der Reihenfolge der Token in einem Prüfdatensatz erhalten Sie über den Befehl `bsmrecord`. Die Ausgabe des Befehls `bsmrecord` kann je nach Bedingung in verschiedenen Formaten erfolgen. Eckige Klammern (`[]`) weisen darauf hin, dass ein Prüf-Token optional ist. Weitere Informationen erhalten Sie auf der Manpage `bsmrecord(1M)`. Beispiele finden Sie ebenfalls unter „So zeigen Sie Prüfdatensatzformate an“ auf Seite 665.
- Sie können den Befehl `praudit` verwenden. Durch die Optionen des Befehls erhalten Sie unterschiedliche Textausgaben. Durch den Befehl `praudit -x` erhalten Sie XML für die Eingabe in Skripten und Browsern. Die Ausgaben von `praudit` enthalten keine Felder, die nur zum Parsing der binären Daten dienen. In den Ausgaben wird nicht unbedingt die Reihenfolge der binären Felder eingehalten. Außerdem wird die Reihenfolge und das Format der Ausgabe von `praudit` beim Wechseln zu einer anderen Oracle Solaris-Version nicht gewährleistet.

  Beispiele für die Ausgabe von `praudit` erhalten Sie unter „So zeigen Sie den Inhalt der binären Prüfdateien an“ auf Seite 671 und auf der Manpage `praudit(1M)`.

  Eine Beschreibung der Ausgabe von `praudit` für die einzelnen Prüf-Token erhalten Sie im Abschnitt zu den einzelnen Token unter „Formate der Prüf-Token“ auf Seite 711.

Formate der Prüf-Token

Jedes Prüf-Token verfügt über eine Token-Typ-ID, gefolgt von spezifischen Daten für das Token. Jeder Token-Typ weist ein eigenes Format auf. In der folgenden Tabelle sehen Sie die Namen sowie eine kurze Beschreibung der einzelnen Token. Veraltete Token werden aus Kompatibilitätsgründen mit früheren Solaris-Versionen weiterhin beibehalten.

TABELLE 31–4 Prüf-Token für Prüfung bei Oracle Solaris

Token-Name	Beschreibung	Weitere Informationen
`acl`	ACL-Informationen (Access Control List)	„Token `acl`“ auf Seite 712
`arbitrary`	Daten mit Format- und Typinformationen	„Token `arbitrary` (veraltet)“ auf Seite 713
`arg`	Argumentwert für Systemaufruf	„Token `arg`“ auf Seite 714
`attribute`	Datei-vnode-Token	„Token `attribute`“ auf Seite 714
`cmd`	Befehlsargumente und Umgebungsvariablen	„Token `cmd`“ auf Seite 715
`exec_args`	Exec-Systemaufruf-Argumente	„Token `exec_args`“ auf Seite 715
`exec_env`	Exec-Systemaufruf-Umgebungsvariablen	„Token `exec_env`“ auf Seite 716
`exit`	Informationen zum Programmende	„Token `exit` (veraltet)“ auf Seite 716
`file`	Informationen zur Prüfdatei	„Token `file`“ auf Seite 716
`group`	Informationen zu Prozessgruppen	„Token `group` (veraltet)“ auf Seite 717
`groups`	Informationen zu Prozessgruppen	„Token `groups`“ auf Seite 717
`header`	Gibt Anfang des Prüfdatensatzes an	„Token `header`“ auf Seite 717
`ip_addr`	Internetadresse	„Token `ip_addr`“ auf Seite 718
`ip`	IP-Header-Informationen	„Token `ip` (veraltet)“ auf Seite 719
`ipc`	Informationen zu System V IPC	„Token `ipc`“ auf Seite 719
`ipc_perm`	Objekt-Token von System V IPC	„Token `ipc_perm`“ auf Seite 720
`iport`	Internet-Port-Adresse	„Token `iport`“ auf Seite 720
`opaque`	Unstrukturierte Daten (nicht angegebenes Format)	„Token `opaque` (veraltet)“ auf Seite 721
`path`	Pfadinformationen	„Token `path`“ auf Seite 721
`path_attr`	Zugriffspfadinformationen	„Token `path_attr`“ auf Seite 722
`privilege`	Berechtigungssatzinformationen	„Token `privilege`“ auf Seite 722
`process`	Prozess-Token-Informationen	„Token `process`“ auf Seite 722

TABELLE 31–4 Prüf-Token für Prüfung bei Oracle Solaris *(Fortsetzung)*

Token-Name	Beschreibung	Weitere Informationen
`return`	Status des Systemaufrufs	„Token `return`“ auf Seite 724
`sequence`	Sequenznummer-Token	„Token `sequence`“ auf Seite 725
`socket`	Socket-Typ und -Adressen	„Token `socket`“ auf Seite 725
`subject`	Betreff-Token (gleiches Format wie `process`-Token)	„Token `subject`“ auf Seite 726
`text`	ASCII-Zeichenfolge	„Token `text`“ auf Seite 728
`trailer`	Gibt Ende des Prüfdatensatzes an	„Token `trailer`“ auf Seite 728
`uauth`	Verwendung der Autorisierung	„Token `uauth`“ auf Seite 729
`upriv`	Verwendung der Berechtigung	„Token `upriv`“ auf Seite 729
`zonename`	Name der Zone	„Token `zonename`“ auf Seite 729

Ein Prüfdatensatz beginnt immer mit einem `header`-Token. Das Token `header` gibt an, an welcher Stelle im Prüfpfad der Prüfdatensatz beginnt. Bei zuweisbaren Ereignissen beziehen sich die Token `subject` und `process` auf die Werte des Prozesses, der das Ereignis ausgelöst hat. Bei nicht zuweisbaren Ereignissen bezieht sich das Token `process` auf das System.

Token `acl`

Das Token `acl` zeichnet Informationen zu ACLs (Access Control Lists) auf.

Das Token `acl` besteht aus vier festen Feldern:

- Eine Token-ID, die dieses Token als ein `acl`-Token ausweist
- Ein Feld, das den ACL-Typ angibt
- Ein ACL-Wertfeld
- Ein Feld, in dem die Berechtigungen aufgeführt sind, die dieser ACL zugewiesen sind

Durch den Befehl `praudit -x` werden die Felder des `acl`-Tokens angezeigt:

```
<acl type="1" value="root" mode="6"/>
```

Token `arbitrary` (veraltet)

Das Token `arbitrary` schließt Daten für den Prüfpfad ein. Dieses Token besteht aus vier festen Feldern und einem Array von Daten. Die festen Felder sind im Folgenden aufgeführt:

- Eine Token-ID, die dieses Token als ein `arbitrary`-Token ausweist
- Ein vorgeschlagenes Druckformatfeld, z. B. hexadezimal
- Ein Elementgrößenfeld, das den Umfang der eingeschlossenen Daten angibt, z. B. Kurzform (short)
- Ein Zählerfeld, das die Anzahl der folgenden Elemente angibt

Den weiteren Bestandteil des Tokens bildet *count* des angegeben Typs. Der Befehl `praudit` zeigt das Token `arbitrary` wie folgt an:

```
arbitrary,decimal,int,1
42
```

Die folgende Tabelle zeigt die möglichen Werte des Druckformatfelds.

TABELLE 31–5 Werte für Druckformatfeld des Tokens `arbitrary`

Wert	Aktion
`AUP_BINARY`	Druckt die Daten im binären Format
`AUP_OCTAL`	Druckt die Daten im oktalen Format
`AUP_DECIMAL`	Druckt die Daten im dezimalen Format
`AUP_HEX`	Druckt die Daten im hexadezimalen Format
`AUP_STRING`	Druckt die Daten als Zeichenfolge

Die folgende Tabelle zeigt die möglichen Werte des Elementgrößenfelds.

TABELLE 31–6 Werte für Elementgrößenfeld des Tokens `arbitrary`

Wert	Aktion
`AUR_BYTE`	Daten werden in Byte-Einheiten zu jeweils 1 Byte gedruckt
`AUR_SHORT`	Daten werden im Kurzformateinheiten zu jeweils 2 Byte gedruckt
`AUR_LONG`	Daten werden in Langformateinheiten zu jeweils 4 Byte gedruckt

Token `arg`

Das Token `arg` enthält Informationen zu den Argumenten eines Systemaufrufs: die Argumentnummer des Systemaufrufs, den Argumentwert und eine optionale Beschreibung. Für dieses Token ist ein 32-Bit-Ganzzahl-Systemaufrufargument in einem Prüfdatensatz zulässig.

Das Token `arg` enthält fünf Felder:

- Eine Token-ID, die dieses Token als ein `arg`-Token ausweist
- Eine Argument-ID, die angibt, auf welches Systemaufrufargument das Token verweist
- Der Argumentwert
- Die Länge der beschreibenden Textzeichenfolge
- Die Textzeichenfolge

Durch den Befehl `praudit -x` werden die Felder des `arg`-Tokens angezeigt:

```
<argument arg-num="2" value="0x0" desc="new file uid"/>
```

Token `attribute`

Das Token `attribute` enthält Informationen vom Datei-vnode.

Das Token `attribute` enthält sieben Felder:

- Eine Token-ID, die dieses Token als ein `attribute`-Token ausweist
- Den Dateizugriffsmodus und -typ
- Die Eigentümer-Benutzer-ID
- Die Eigentümer-Gruppen-ID
- Die Dateisystem-ID
- Die Knoten-ID
- Die Geräte-ID, die die Datei darstellt

Weitere Informationen zur Dateisystem-ID und Geräte-ID erhalten Sie auf der Manpage `statvfs(2)`.

Das Token `attribute` wird normalerweise zusammen mit einem `path`-Token verwendet. Das Token `attribute` wird während der Pfadsuchen erstellt. Wenn bei der Pfadsuche ein Fehler auftritt, ist kein vnode verfügbar, um die erforderlichen Dateiinformationen zu erhalten. Daher ist das Token `attribute` nicht im Prüfdatensatz enthalten. Durch den Befehl `praudit -x` werden die Felder des `attribute`-Tokens angezeigt:

```
<attribute mode="100644" uid="adm" gid="adm" fsid="136" nodeid="2040" device="0"/>
```

Token cmd

Das Token cmd zeichnet die Liste der Argumente und die Liste der einem Befehl zugewiesenen Umgebungsvariablen auf.

Das Token cmd enthält die folgenden Felder:

- Eine Token-ID, die dieses Token als ein cmd-Token ausweist
- Ein Zähler der Befehlsargumente
- Die Argumentliste
- Die Länge des nächsten Felds
- Der Inhalt der Argumente
- Ein Zähler der Umgebungsvariablen
- Die Liste der Umgebungsvariablen
- Die Länge des nächsten Felds
- Der Inhalt der Umgebungsvariablen

Durch den Befehl praudit -x werden die Felder des cmd-Tokens angezeigt: Im Folgenden sehen Sie ein abgeschnittenes cmd-Token. Die Zeile enthält einen Zeilenumbruch, um eine übersichtlichere Darstellung zu ermöglichen.

```
<cmd><arge>WINDOWID=6823679</arge>
<arge>COLORTERM=gnome-terminal</arge>
<arge>...LANG=C</arge>...<arge>HOST=machine1</arge>
<arge>LPDEST=printer1</arge>...</cmd>
```

Token exec_args

Das Token exec_args zeichnet Argumente für einen exec()-Systemaufruf auf. Das Token exec_args verfügt über zwei feste Felder:

- Ein Feld mit der Token-ID, die dieses Token als ein attribute-Token ausweist
- Einen Zähler, der die Anzahl der Argumente darstellt, die an den Systemaufruf exec() weitergeleitet werden

Den weiteren Bestandteil dieses Tokens bilden *count*-Zeichenfolgen. Durch den Befehl praudit -x werden die Felder des exec_args-Tokens angezeigt:

```
<exec_args><arg>/usr/bin/sh</arg><arg>/usr/bin/hostname</arg></exec_args>
```

Hinweis – Das Token exec_args wird nur ausgegeben, wenn die Prüfrichtlinienoption argv aktiviert ist.

Token exec_env

Das Token exec_env zeichnet die aktuellen Umgebungsvariablen für einen exec()-Systemaufruf auf. Das Token exec_env verfügt über zwei feste Felder:

- Ein Feld mit der Token-ID, die dieses Token als ein exec_env-Token ausweist
- Einen Zähler, der die Anzahl der Argumente darstellt, die an den Systemaufruf exec() weitergeleitet werden

Den weiteren Bestandteil dieses Tokens bilden *count*-Zeichenfolgen. Durch den Befehl praudit -x werden die Felder des Tokens exec_env angezeigt: Die Zeile enthält einen Zeilenumbruch, um eine übersichtlichere Darstellung zu ermöglichen.

```
<exec_env><env>_=/usr/bin/hostname</env>
<env>DTXSERVERLOCATION=local</env><env>SESSIONTYPE=altDt</env>
<env>LANG=C</env><env>SDT_NO_TOOLTALK=1</env><env>SDT_ALT_HELLO=/bin/true</env>
<env>PATH=/usr/bin:/usr/openwin/bin:/usr/ucb</env>
<env>OPENWINHOME=/usr/openwin</env><env>LOGNAME=jdoe</env><env>USER=jdoe</env>
<env>DISPLAY=:0</env><env>SHELL=/bin/csh</env><env>START_SPECKEYSD=no</env>
<env>SDT_ALT_SESSION=/usr/dt/config/Xsession2.jds</env><env>HOME=/home/jdoe</env>
<env>SDT_NO_DTDBCACHE=1</env><env>PWD=/home/jdoe</env><env>TZ=US/Pacific</env>
</exec_env>
```

Hinweis – Das Token exec_env wird nur ausgegeben, wenn die Prüfrichtlinienoption arge aktiviert ist.

Token exit (veraltet)

Das Token exit zeichnet den Endestatus eines Programms auf. Das Token exit enthält die folgenden Felder:

- Eine Token-ID, die dieses Token als ein exit-Token ausweist
- Ein Programmendestatus, der an den Systemaufruf exit() weitergeleitet wird
- Ein Rückgabewert, der den Endestatus beschreibt oder eine Systemfehlernummer liefert

Der Befehl praudit zeigt das Token exit wie folgt an:

```
exit,Error 0,0
```

Token file

Das Token file ist ein spezielles Token, das vom Dämon auditd generiert wird. Das Token kennzeichnet den Anfang einer neuen Prüfdatei und das Ende einer alten Prüfdatei, wenn die alte Datei deaktiviert wird. Das Anfangs-Token file kennzeichnet die vorhergehende Datei im

Prüfpfad. Das Ende-Token `file` kennzeichnet die nächste Datei im Prüfpfad. Durch den Dämon `auditd` wird ein spezieller Prüfdatensatz erstellt, der dieses Token enthält, um nachfolgende Prüfdateien in einem Prüfpfad miteinander zu verbinden.

Durch den Befehl `praudit -x` werden die Felder des `file`-Tokens angezeigt: Durch dieses Token wird die nächste Datei im Prüfpfad gekennzeichnet. Die Zeile enthält einen Zeilenumbruch, um eine übersichtlichere Darstellung zu ermöglichen.

```
<file iso8601="2009-04-08 14:18:26.200 -07:00">
/var/audit/machine1/files/20090408211826.not_terminated.machine1</file>
```

Token `group` (veraltet)

Dieses Token wurde durch das Token `groups` ersetzt. Weitere Informationen erhalten Sie unter „Token `groups`“ auf Seite 717.

Token `groups`

Das Token `groups` wird durch das Token `group` ersetzt. Das Token `groups` zeichnet die Gruppeneinträge vom Berechtigungsnachweis des Prozesses auf.

Das Token `groups` verfügt über zwei feste Felder:

- Ein Feld mit der Token-ID, die dieses Token als `groups`-Token ausweist
- Ein Zähler, der die Anzahl der Gruppen darstellt, die in diesem Prüfdatensatz enthalten sind

Den weiteren Bestandteil dieses Tokens bilden *count*-Gruppeneinträge.

Durch den Befehl `praudit -x` werden die Felder des `groups`-Tokens angezeigt:

```
<group><gid>staff</gid><gid>other</gid></group>
```

Hinweis – Das Token `groups` wird nur ausgegeben, wenn die Prüfrichtlinienoption `group` aktiviert ist.

Token `header`

Das Token `header` zeichnet sich dadurch aus, dass es den Anfang eines Prüfdatensatzes markiert. Das Token `header` wird in Kombination mit dem Token `trailer` verwendet und schließt alle anderen Token im Datensatz ein.

Das Token `header` verfügt über acht Felder:

- Ein Feld mit der Token-ID, die dieses Token als `header`-Token ausweist
- Ein Byte-Zähler der Gesamtlänge des Prüfdatensatzes, einschließlich der beiden Token `header` und `trailer`
- Eine Versionsnummer, die die Version der Prüfdatensatzstruktur angibt
- Die Prüfereignis-ID, die das vom Datensatz dargestellte Prüfereignis angibt
- Der ID-Modifikator, der bestimmte Merkmale des Prüfereignisses angibt

  Für das ID-Modifikatorfeld sind die folgenden Flags definiert:

```
0x4000          PAD_NOTATTR                     nonattributable event
0x8000          PAD_FAILURE                     failed audit event
```

- Der Adresstyp: entweder IPv4 oder IPv6
- Die Adresse des Rechners
- Die Uhrzeit und das Datum der Datensatzerstellung

Auf 64-Bit-Systemen wird das `header`-Token mit einem 64-Bit- anstatt 32-Bit-Zeitstempel angezeigt.

Der Befehl `praudit` zeigt das Token `header` wie folgt an:

```
header,69,2,su,,machine1,2009-04-08 13:11:58.209 -07:00
```

Der Befehl `praudit -x` zeigt die Felder des Tokens `header` am Anfang des Prüfdatensatzes an. Die Zeile enthält einen Zeilenumbruch, um eine übersichtlichere Darstellung zu ermöglichen.

```
<record version="2" event="su" host="machine1"
iso8601="2009-04-08 13:11:58.209 -07:00">
```

Token `ip_addr`

Das Token `ip_addr` enthält eine IP-Adresse (Internet Protocol). Ab Version Solaris 8 kann die Internetadresse im IPv4- oder IPv6-Format angezeigt werden. Die IPv4-Adresse verwendet 4 Byte. Die IPv6-Adresse verwendet 1 Byte zur Beschreibung des Adresstyps und 16 Byte zur Beschreibung der Adresse.

Das Token `in_addr` enthält drei Felder:

- Eine Token-ID, die dieses Token als ein `in_addr`-Token ausweist
- Ein IP-Adresstyp: entweder IPv4 oder IPv6
- Eine IP-Adresse

Durch den Befehl `praudit -x` wird der Inhalt des Tokens `ip_addr` angezeigt:

```
<ip_address>machine1</ip_address>
```

Token `ip` (veraltet)

Das Token `ip` enthält die Kopie eines IP-Headers (Internet Protocol). Das Token `ip` enthält zwei Felder:

- Eine Token-ID, die dieses Token als ein `ip`-Token ausweist
- Eine Kopie des IP-Headers, d. h. insgesamt 20 Byte

Der Befehl `praudit` zeigt das Token `ip` wie folgt an:

```
ip address,0.0.0.0
```

Die Struktur des IP-Header wird in der Datei `/usr/include/netinet/ip.h` definiert.

Token `ipc`

Das Token `ipc` enthält das System V IPC-Meldungs-Handle, Semaphor-Handle oder Handle mit gemeinsam genutztem Speicher, das vom Aufrufer zum Identifizieren eines bestimmten IPC-Objekts verwendet wird.

Das Token `ipc` enthält drei Felder:

- Eine Token-ID, die dieses Token als ein `ipc`-Token ausweist
- Ein Typfeld, das den Typ des IPC-Objekts angibt
- Das Handle, das das IPC-Objekt angibt

Hinweis – Die IPC-Objekt-IDs verletzen die Kontextfreiheit der Oracle Solaris-Prüf-Token. Es gibt keinen globalen "Namen" zur eindeutigen Identifizierung von IPC-Objekten. IPC-Objekte werden stattdessen durch die zugehörigen Handles identifiziert. Die Gültigkeit der Handles besteht nur während der Zeit, in der die IPC-Objekte aktiviert sind. Die Identifizierung der IPC-Objekte stellt jedoch kein Problem dar. Die System V IPC-Mechanismen werden selten verwendet. Die Mechanismen nutzen gemeinsam die gleiche Prüfklasse.

In der folgenden Tabelle werden die möglichen Werte für das IPC-Objekttypfeld angezeigt. Die Werte werden in der Datei `/usr/include/bsm/audit.h` definiert.

TABELLE 31–7 Werte für das IPC-Objekttypfeld

Name	Wert	Beschreibung
`AU_IPC_MSG`	1	IPC-Meldungsobjekt
`AU_IPC_SEM`	2	IPC-Semaphor-Objekt
`AU_IPC_SHM`	3	IPC-Objekt mit gemeinsam genutztem Speicher

Durch den Befehl `praudit -x` werden die Felder des `ipc`-Tokens angezeigt:

```
<IPC ipc-type="shm" ipc-id="15"/>
```

Token `ipc_perm`

Das Token `ipc_perm` enthält eine Kopie der System V IPC-Zugriffsrechte. Dieses Token wird zu den Prüfdatensätzen hinzugefügt, die von den IPC-Ereignissen mit gemeinsam genutztem Speicher, IPC-Semaphor-Ereignissen und IPC-Meldungsereignissen generiert werden.

Das Token `ipc_perm` enthält acht Felder:

- Eine Token-ID, die dieses Token als ein `ipc_perm`-Token ausweist
- Die Benutzer-ID des IPC-Eigentümers
- Die Gruppen-ID des IPC-Eigentümers
- Die Benutzer-ID des IPC-Erstellers
- Die Gruppen-ID des IPC-Erstellers
- Der Zugriffsmodus von IPC
- Die Sequenznummer von IPC
- Der IPC-Schlüsselwert

Durch den Befehl `praudit -x` werden die Felder des `ipc_perm`-Tokens angezeigt: Die Zeile enthält einen Zeilenumbruch, um eine übersichtlichere Darstellung zu ermöglichen.

```
<IPC_perm uid="jdoe" gid="staff" creator-uid="jdoe"
creator-gid="staff" mode="100600" seq="0" key="0x0"/>
```

Die Werte werden aus der Struktur von `ipc_perm` übernommen, die dem IPC-Objekt zugewiesen ist.

Token `iport`

Das Token `iport` enthält die TCP- oder UDP-Port-Adressen.

Das Token `iport` enthält zwei Felder:

- Eine Token-ID, die dieses Token als ein `iport`-Token ausweist
- Die TCP- oder UDP-Port-Adresse

Der Befehl `praudit` zeigt das Token `iport` wie folgt an:

```
ip port,0xf6d6
```

Token opaque (veraltet)

Das Token opaque enthält unformatierte Daten als eine Byte-Sequenz. Das Token opaque enthält drei Felder:

- Eine Token-ID, die dieses Token als ein opaque-Token ausweist
- Ein Byte-Zähler der Daten
- Ein Array der Byte-Daten

Der Befehl praudit zeigt das Token opaque wie folgt an:

```
opaque,12,0x4f5041515545204441544100
```

Token path

Das Token path enthält Zugriffspfadinformationen für ein Objekt.

Das Token path enthält die folgenden Felder:

- Eine Token-ID, die dieses Token als ein path-Token ausweist
- Die Pfadlänge
- Der absolute Pfad zum Objekt, das auf dem realen Root des Systems basiert

Der Befehl praudit zeigt das Token path ohne das zweite Feld wie folgt an:

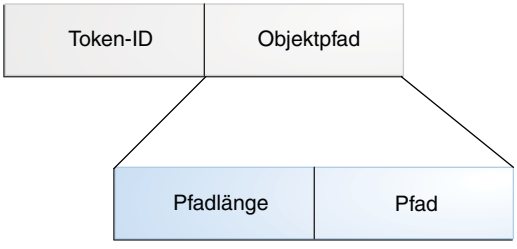
```
path,/etc/security/audit_user
```

Durch den Befehl praudit -x wird der Inhalt des Tokens path angezeigt:

```
<path>/etc/security/prof_attr</path>
```

Die folgende Abbildung zeigt das Format das Tokens path.

ABBILDUNG 31–4 Format des Tokens path



Token path_attr

Das Token path_attr enthält Zugriffspfadinformationen für ein Objekt. Der Zugriffspfad gibt die Sequenz der Attributdateiobjekte unterhalb des Token-Objekts path an. Systemaufrufe wie openat() greifen auf Attributdateien zu. Weitere Informationen zu Attributdateiobjekten finden Sie auf der Manpage fsattr(5).

Das Token path_attr enthält die folgenden Felder:

- Eine Token-ID, die dieses Token als path_attr-Token ausweist
- Einen Zähler, der die Anzahl der Abschnitte von Attributdateipfaden darstellt
- Auf Null endende *count*-Zeichenfolgen

Der Befehl praudit zeigt das path_attr-Token wie folgt an:

```
path_attr,1,attr_file_name
```

Token privilege

Das Token privilege zeichnet die Verwendung von Berechtigungen bei einem Prozess auf. Das Token privilege wird für Berechtigungen im Basissatz nicht aufgezeichnet. Wenn eine Berechtigung durch eine administrative Aktion aus dem Basissatz entfernt wurde, wird die Verwendung dieser Berechtigung aufgezeichnet. Weitere Informationen zu Berechtigungen erhalten Sie unter „Berechtigungen (Übersicht)“ auf Seite 201.

Das Token privilege enthält die folgenden Felder:

- Eine Token-ID, die dieses Token als ein privilege-Token ausweist
- Die Länge des folgenden Felds
- Der Name des Berechtigungssatzes
- Die Länge des folgenden Felds
- Die Liste der Berechtigungen

Durch den Befehl praudit -x werden die Felder des privilege-Tokens angezeigt: Die Zeile enthält einen Zeilenumbruch, um eine übersichtlichere Darstellung zu ermöglichen.

```
<privilege set-type="Effective">file_chown,file_dac_read,
file_dac_write,net_privaddr,proc_exec,proc_fork,proc_setid</privilege>
```

Token process

Das Token process enthält Informationen zu einem Benutzer, der einem Prozess zugewiesen ist, beispielsweise Empfänger eines Signals.

Das Token `process` enthält neun Felder:

- Eine Token-ID, die dieses Token als ein `process`-Token ausweist
- Die Prüf-ID
- Die effektive Benutzer-ID
- Die effektive Gruppen-ID
- Die reale Benutzer-ID
- Die reale Gruppen-ID
- Die Prozess-ID
- Die Prüfsitzungs-ID
- Eine Terminal-ID, die aus einer Geräte-ID und Rechneradresse besteht

Die Prüf-ID, Benutzer-ID, Gruppen-ID, Prozess-ID und Sitzungs-ID, die in der Lang- anstatt Kurzform vorliegen.

Hinweis – Die Felder des Tokens `process` für die Sitzungs-ID, reale Benutzer-ID oder reale Gruppen-ID sind möglicherweise nicht verfügbar. Der Wert wird in diesem Fall auf `-1` festgelegt.

Alle Token, die eine Terminal-ID enthalten, verfügen über mehrere Variationen. Durch den Befehl `praudit` werden diese Variationen ausgeblendet. Daher wird die Terminal-ID auf die gleiche Weise für alle Token verarbeitet, die eine Terminal-ID enthalten. Die Terminal-ID stellt entweder eine IP-Adresse und Portnummer oder eine Geräte-ID dar. Eine Geräte-ID, beispielsweise ein serieller Port, der mit einem Modem verbunden ist, kann einen Wert von Null aufweisen. Die Terminal-ID kann in verschiedenen Formaten angegeben werden.

Die Terminal-ID für Gerätenummern wird wie folgt angegeben:

- **32-Bit-Anwendungen**: 4-Byte-Gerätenummer, 4 Byte nicht verwendet
- **64-Bit-Anwendungen**: 8-Byte-Gerätenummer, 4 Byte nicht verwendet

Bei Versionen vor Solaris 8 wird die Terminal-ID für Portnummern wie folgt angegeben:

- **32-Bit-Anwendungen**: 4-Byte-Portnummer, 4-Byte-IP-Adresse
- **64-Bit-Anwendungen**: 8-Byte-Portnummer, 4-Byte-IP-Adresse

Seit der Version Solaris 8 wird die Terminal-ID für Portnummern wie folgt angegeben:

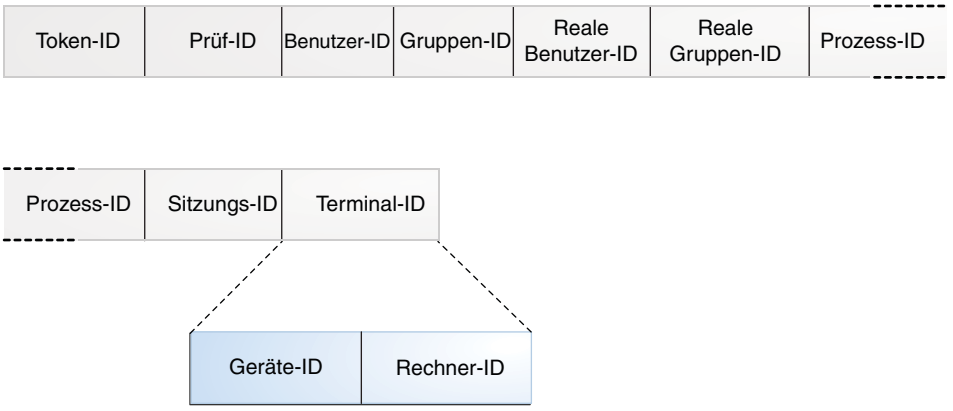
- **32-Bit mit IPv4**: 4-Byte-Portnummer, 4-Byte-IP-Typ, 4-Byte-IP-Adresse
- **32-Bit mit IPv6**: 4-Byte-Portnummer, 4-Byte-IP-Typ, 16-Byte-IP-Adresse
- **64-Bit mit IPv4**: 8-Byte-Portnummer, 4-Byte-IP-Typ, 4-Byte-IP-Adresse
- **64-Bit mit IPv6**: 8-Byte-Portnummer, 4-Byte-IP-Typ, 16-Byte-IP-Adresse

Durch den Befehl `praudit -x` werden die Felder des `process`-Tokens angezeigt: Die Zeile enthält einen Zeilenumbruch, um eine übersichtlichere Darstellung zu ermöglichen.

```
<process audit-uid="-2" uid="root" gid="root" ruid="root"
rgid="root" pid="9" sid="0" tid="0 0 0.0.0.0"/>
```

Die folgende Abbildung zeigt das Format das Tokens `process`.

ABBILDUNG 31–5 Format des Tokens `process`



Token `return`

Das Token `return` enthält den Rückgabestatus des Systemaufrufs (`u_error`) und den Prozessrückgabewert (`u_rval1`).

Das Token `return` enthält drei Felder:

- Eine Token-ID, die dieses Token als ein `return`-Token ausweist
- Der Fehlerstatus des Systemaufrufs
- Der Rückgabewert des Systemaufrufs

Das Token `return` wird als Teil der vom Kernel generierten Prüfdatensätze für Systemaufrufe zurückgegeben. Bei der Anwendungsprüfung gibt dieses Token den Endestatus und andere Rückgabewerte an.

Der Befehl `praudit` zeigt das Token `return` für einen Systemaufruf wie folgt an:

```
return,failure: Operation now in progress,-1
```

Durch den Befehl `praudit -x` werden die Felder des `return`-Tokens angezeigt:

```
<return errval="failure: Operation now in progress" retval="-1/">
```

Token sequence

Das Token sequence enthält eine Sequenznummer. Die Sequenznummer wird inkrementell erhöht, wenn ein Prüfdatensatz zum Prüfpfad hinzugefügt wird. Dieses Token dient zur Fehlersuche.

Das Token sequence enthält zwei Felder:

- Eine Token-ID, die dieses Token als ein sequence-Token ausweist
- Ein 32-Bit-Feld ohne Vorzeichen im Langformat, das die Sequenznummer enthält

Das Token praudit zeigt das Feld des Tokens sequence:

```
sequence,1292
```

Der Befehl praudit -x zeigt den Inhalt des Tokens sequence:

```
<sequence seq-num="1292"/>
```

Hinweis – Das Token sequence wird nur ausgegeben, wenn die Prüfrichtlinienoption seq aktiviert ist.

Token socket

Das Token socket enthält Informationen, die ein Internet-Socket beschreiben. Bei einigen Instanzen enthält das Token vier Felder:

- Eine Token-ID, die dieses Token als ein socket-Token ausweist
- Ein Feld mit dem Socket-Typ, der den Typ des referenzierten Sockets angibt, beispielsweise TCP, UDP oder UNIX
- Der lokale Port
- Die lokale IP-Adresse

Der Befehl praudit zeigt diese Instanz des Tokens socket wie folgt an:

```
socket,0x0002,0x83b1,localhost
```

Bei den meisten Instanzen enthält das Token acht Felder:

- Eine Token-ID, die dieses Token als ein socket-Token ausweist
- Die Socket-Domain
- Ein Feld mit dem Socket-Typ, der den Typ des referenzierten Sockets angibt, beispielsweise TCP, UDP oder UNIX
- Der lokale Port

- Der Adresstyp: entweder IPv4 oder IPv6
- Die lokale IP-Adresse
- Der Remote-Port
- Die Remote-IP-Adresse

Ab Version Solaris 8 kann die Internetadresse im IPv4- oder IPv6-Format angezeigt werden. Die IPv4-Adresse verwendet 4 Byte. Die IPv6-Adresse verwendet 1 Byte zur Beschreibung des Adresstyps und 16 Byte zur Beschreibung der Adresse.

Der Befehl `praudit` zeigt das Token `socket` wie folgt an:

```
socket,0x0002,0x0002,0x83cf,example1,0x2383,server1.Subdomain.Domain.COM
```

Durch den Befehl `praudit -x` werden die Felder des `socket`-Tokens angezeigt: Die Zeile enthält einen Zeilenumbruch, um eine übersichtlichere Darstellung zu ermöglichen.

```
<socket sock_domain="0x0002" sock_type="0x0002" lport="0x83cf"
laddr="example1" fport="0x2383" faddr="server1.Subdomain.Domain.COM"/>
```

Token `subject`

Das Token `subject` beschreibt einen Benutzer, der einen Vorgang durchführt oder durchzuführen versucht. Es wird das gleiche Format wie beim Token `process` verwendet.

Das Token `subject` enthält neun Felder:

- Eine Token-ID, die dieses Token als ein `subject`-Token ausweist
- Die Prüf-ID
- Die effektive Benutzer-ID
- Die effektive Gruppen-ID
- Die reale Benutzer-ID
- Die reale Gruppen-ID
- Die Prozess-ID
- Die Prüfsitzungs-ID
- Eine Terminal-ID, die aus einer Geräte-ID und Rechner-IP-Adresse besteht

Die Prüf-ID, Benutzer-ID, Gruppen-ID, Prozess-ID und Sitzungs-ID, die in der Lang- anstatt Kurzform vorliegen.

Hinweis – Die Felder des Tokens `subject` für die Sitzungs-ID, reale Benutzer-ID oder reale Gruppen-ID sind möglicherweise nicht verfügbar. Der Wert wird in diesem Fall auf `-1` festgelegt.

Alle Token, die eine Terminal-ID enthalten, verfügen über mehrere Variationen. Durch den Befehl `praudit` werden diese Variationen ausgeblendet. Daher wird die Terminal-ID auf die gleiche Weise für alle Token verarbeitet, die eine Terminal-ID enthalten. Die Terminal-ID stellt entweder eine IP-Adresse und Portnummer oder eine Geräte-ID dar. Eine Geräte-ID, beispielsweise ein serieller Port, der mit einem Modem verbunden ist, kann einen Wert von Null aufweisen. Die Terminal-ID kann in verschiedenen Formaten angegeben werden.

Die Terminal-ID für Gerätenummern wird wie folgt angegeben:

- **32-Bit-Anwendungen**: 4-Byte-Gerätenummer, 4 Byte nicht verwendet
- **64-Bit-Anwendungen**: 8-Byte-Gerätenummer, 4 Byte nicht verwendet

Bei Versionen vor Solaris 8 wird die Terminal-ID für Portnummern wie folgt angegeben:

- **32-Bit-Anwendungen**: 4-Byte-Portnummer, 4-Byte-IP-Adresse
- **64-Bit-Anwendungen**: 8-Byte-Portnummer, 4-Byte-IP-Adresse

Seit der Version Solaris 8 wird die Terminal-ID für Portnummern wie folgt angegeben:

- **32-Bit mit IPv4**: 4-Byte-Portnummer, 4-Byte-IP-Typ, 4-Byte-IP-Adresse
- **32-Bit mit IPv6**: 4-Byte-Portnummer, 4-Byte-IP-Typ, 16-Byte-IP-Adresse
- **64-Bit mit IPv4**: 8-Byte-Portnummer, 4-Byte-IP-Typ, 4-Byte-IP-Adresse
- **64-Bit mit IPv6**: 8-Byte-Portnummer, 4-Byte-IP-Typ, 16-Byte-IP-Adresse

Das Token `subject` wird als Teil der vom Kernel generierten Prüfdatensätze für Systemaufrufe zurückgegeben. Der Befehl `praudit` zeigt das Token `subject` wie folgt an:

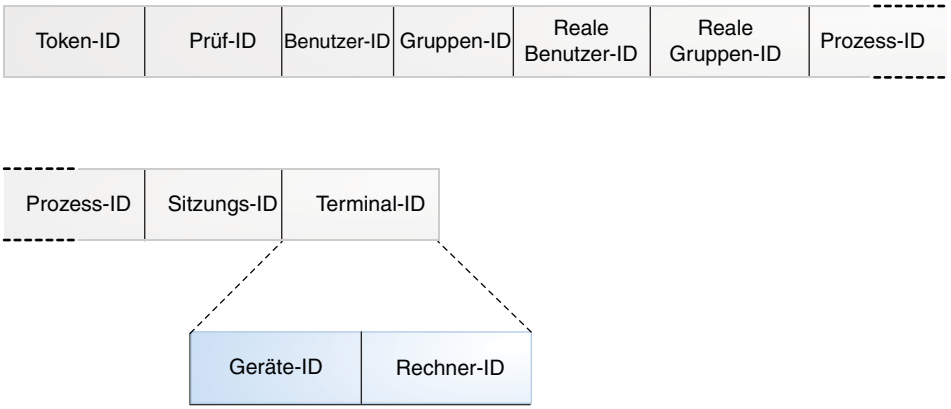
```
subject,jdoe,root,root,root,root,1631,1421584480,8243 65558 machine1
```

Durch den Befehl `praudit -x` werden die Felder des `subject`-Tokens angezeigt: Die Zeile enthält einen Zeilenumbruch, um eine übersichtlichere Darstellung zu ermöglichen.

```
<subject audit-uid="jdoe" uid="root" gid="root" ruid="root"
rgid="root" pid="1631" sid="1421584480" tid="8243 65558 machine1"/>
```

Die folgende Abbildung zeigt das Format des Tokens `subject`.

ABBILDUNG 31–6 Format des Tokens `subject`



Token `text`

Das Token `text` enthält eine Textzeichenfolge.

Das Token `text` enthält drei Felder:

- Eine Token-ID, die dieses Token als ein `text`-Token ausweist
- Die Länge der Textzeichenfolge
- Die Textzeichenfolge selbst

Durch den Befehl `praudit -x` wird der Inhalt des Tokens `text` angezeigt:

```
<text>booting kernel</text>
```

Token `trailer`

Die zwei Token `header` und `trailer` zeichnen sich dadurch aus, dass sie die Endpunkte eines Prüfdatensatzes markieren und alle anderen Token einschließen. Ein `header`-Token steht am Anfang eines Prüfdatensatzes. Ein `trailer`-Token steht am Ende eines Prüfdatensatzes. Das Token `trailer` ist optional. Das Token `trailer` wird als letztes Token eines Datensatzes hinzugefügt, wenn die Prüfrichtlinienoption `trail` festgelegt wurde.

Wenn beim Generieren eines Prüfdatensatzes ein trailer-Token aktiviert ist, können Sie durch den Befehl `auditreduce` überprüfen, ob das trailer-Token ordnungsgemäß auf das header-Token des Datensatzes verweist. Das `trailer`-Token unterstützt rückwärts gerichtete Suchen im Prüfpfad.

Das Token `trailer` enthält drei Felder:

- Eine Token-ID, die dieses Token als ein `trailer`-Token ausweist
- Eine Pad-Nummer für die Markierung des Datensatzendes

- Die Gesamtzahl der Zeichen im Prüfdatensatz, einschließlich der Token `header` und `trailer`

Durch den Befehl `praudit` wird das Token `trailer` wie folgt angezeigt:

```
trailer,136
```

Token `uauth`

Das Token `uauth` zeichnet die Verwendung der Autorisierung bei einem Befehl oder einer Aktion auf.

Das Token `uauth` enthält die folgenden Felder:

- Eine Token-ID, die dieses Token als ein `uauth`-Token ausweist
- Die Länge des Texts im folgenden Feld
- Eine Liste der Autorisierungen

Der Befehl `praudit` zeigt das Token `uauth` wie folgt an:

```
use of authorization,solaris.admin.printer.delete
```

Token `upriv`

Das Token `upriv` zeichnet die Verwendung der Berechtigung bei einem Befehl oder einer Aktion auf.

Durch den Befehl `praudit -x` werden die Felder des `upriv`-Tokens angezeigt:

```
<use_of_privilege result="successful use of priv">proc_setid</use_of_privilege>
```

Token `zonename`

Das Token `zonename` zeichnet die Zone auf, in dem das Prüfereignis aufgetreten ist. Die Zeichenfolge "global" gibt die Prüfereignisse an, die in der globalen Zone auftreten.

Das Token `zonename` enthält die folgenden Felder:

- Eine Token-ID, die dieses Token als ein `zonename`-Token ausweist
- Die Länge des Texts im folgenden Feld
- Der Name der Zone

Durch den Befehl `praudit -x` wird der Inhalt des Tokens `zonename` angezeigt:

```
<zone name="graphzone"/>
```

Glossar

Absicherung Änderung der Standardkonfiguration des Betriebssystems, um die inhärenten Sicherheitsschwachstellen des Hosts zu beheben.

Admin-Hauptelement Ein Benutzer-Hauptelement mit einem Namen in folgender Form: *Benutzername*`/admin` (z. B. `jdoe/admin`). Ein Admin-Hauptelement kann über mehr Berechtigungen verfügen als ein gewöhnliches Benutzer-Hauptelement (z. B. zum Ändern von Richtlinien). Weitere Informationen finden Sie unter Hauptelementname und Benutzer-Hauptelement.

AES Advanced Encryption Standard. Eine symmetrische 128-Bit Blockdaten-Verschlüsselungstechnik. Die US-Regierung hat die Rijndael-Variante des Algorithmus im Oktober 2000 als Verschlüsselungsstandard angenommen. AES ersetzt die Benutzer-Hauptelement-Verschlüsselung als Regierungsstandard.

Algorithmus Ein kryptografischer Algorithmus. Hierbei handelt es sich um ein bewährtes rekursives Berechnungsverfahren zum Verschlüsseln oder Hashen von Eingabe.

Anfängliches Ticket Ein Ticket, das direkt ausgegeben wird (d. h. nicht auf einem vorhandenen Ticket-gewährenden Ticket basiert). Für einige Services, wie z. B. Anwendungen zum Ändern von Passwörtern, kann es erforderlich sein, dass Tickets als *anfängliche* Tickets gekennzeichnet werden, um sicherzustellen, dass der Client Kenntnisse über den Geheimschlüssel unter Beweis stellen kann. Ein anfängliches Ticket ist wichtig, denn es gibt an, dass der Client sich kürzlich authentifiziert hat (ein Ticket-gewährendes Ticket ist möglicherweise schon seit längerer Zeit vorhanden).

Anwendungsserver Weitere Informationen finden Sie unter Netzwerkanwendungsserver.

Asynchrones Prüfereignis Die wenigsten Systemereignisse sind asynchron. Diese Ereignisse sind keinem Prozess zugewiesen. Daher sind keine Prozesse verfügbar, die blockiert oder zu einem späteren Zeitpunkt reaktiviert werden können. Das erstmalige Booten des Systems und Aufrufen bzw. Beenden von PROM sind Beispiele für asynchrone Ereignisse.

Authentifizierer Authentifizierer werden von Clients übergeben, wenn sie Tickets (von einem KDC) und Services (von einem Server) anfordern. Sie enthalten Informationen, die vor kurzer Zeit mit einem nur dem Client und dem Server bekannten Sitzungsschlüssel generiert wurden und daher die Sicherheit der Transaktion gewährleisten. In Verbindung mit einem Ticket kann ein Authentifizierer zur Authentifizierung eines Benutzer-Hauptelements verwendet werden. Ein Authentifizierer schließt den Hauptelementnamen des Benutzers, die IP-Adresse vom Host des Benutzers und einen Zeitstempel ein. Im Unterschied zu einem Ticket kann ein Authentifizierer nur einmal verwendet werden. Dies geschieht normalerweise, wenn Zugriff auf einen Service angefordert wird. Ein Authentifizierer wird unter Verwendung des Sitzungsschlüssels für diesen Client und diesen Server verschlüsselt.

Authentifizierung Überprüfung der Identität eines Hauptelements

Autorisierung 1. In Kerberos wird anhand der Autorisierung festgestellt, ob ein Hauptelement einen Service verwenden kann, auf welche Objekte das Hauptelement Zugriff hat sowie der für jedes Objekt gewährte Zugriffstyp.

2. Bei der rollenbasierten Zugriffssteuerung (Role-based Access Control, RBAC) entspricht eine Autorisierung einer Berechtigung, die einer Rolle oder einem Benutzer zugewiesen oder in ein Berechtigungsprofil eingebettet werden kann, um bestimmte Aktionen auszuführen, die andernfalls aufgrund der Sicherheitsrichtlinie nicht zulässig wären.

Basissicherheitsmodul (BSM) Die Oracle Solaris-Prüfservice- und Gerätezuordnung. Zusammen entsprechen diese Funktionen der Sicherheitsstufe C2.

Begrenzter Satz Die äußere Beschränkung für die Berechtigungen, die einem Prozess und dessen untergeordneten Prozessen zur Verfügung stehen.

Benutzer-Hauptelement Ein Hauptelement, das einem bestimmten Benutzer zugewiesen ist. Der primäre Name eines Benutzer-Hauptelements ist ein Benutzername und die optionale Instanz ist ein Name, der zur beabsichtigten Verwendung der entsprechenden Berechtigungsnachweise dient (z. B. `jdoe` oder `jdoe/admin`). Dies wird auch als Benutzerinstanz bezeichnet. Weitere Informationen finden Sie unter Service-Hauptelement.

Berechtigung Eine einzelne Berechtigung für einen Prozess in einem Oracle Solaris-System. Mit Berechtigungen können Prozesse genauer gesteuert werden als mit `root`. Berechtigungen werden im Kernel definiert und durchgesetzt. Eine vollständige Beschreibung von Berechtigungen finden Sie auf der Manpage `privileges(5)`.

Berechtigungseskalation Das Erhalten von Zugriff auf Ressourcen, für die Sie gemäß Ihrer Sicherheitsattribute über keine Berechtigungen (einschließlich Überschreibungen) verfügen. Das Ergebnis besteht darin, das ein Prozess unberechtigte Aktionen ausführen kann.

Berechtigungsmodell Ein strengeres Sicherheitsmodell auf einem Computersystem als das Superuser-Modell. In einem Berechtigungsmodell benötigen Prozesse Berechtigungen, um ausgeführt zu werden. Die Verwaltung des Systems kann in verschiedene Teile getrennt werden, die auf den Prozessberechtigungen der Administratoren basieren. Berechtigungen können dem Anmeldeprozess eines Administrators zugewiesen werden. Berechtigungen können auch nur bestimmten Befehlen zugewiesen werden.

Berechtigungsnachweis Ein Informationspaket, das ein Ticket und einen übereinstimmenden Sitzungsschlüssel enthält. Es wird zur Authentifizierung der Identität eines Hauptelements verwendet. Weitere Informationen finden Sie unter Ticket und Sitzungsschlüssel.

Berechtigungsnachweis-Cache Ein Speicherplatz (normalerweise eine Datei) für die vom KDC erhaltenen Berechtigungsnachweise

Berechtigungsprofil Wird auch als Berechtigung oder Profil bezeichnet. Eine Sammlung von Überschreibungen in RBAC, die einer Rolle oder einem Benutzer zugewiesen werden können. Ein Berechtigungsprofil kann aus Autorisierungen, Berechtigungen, Befehlen mit Sicherheitsattributen und anderen Berechtigungsprofilen bestehen.

Berechtigungssatz Eine Sammlung von Berechtigungen. Jeder Prozess hat vier Berechtigungssätze, die festlegen, ob ein Prozess eine bestimmte Berechtigung verwenden kann. Weitere Informationen finden Sie unter Begrenzter Satz, Effektiver Satz, Zugelassener Satz und Vererbbarer Satz.

Der Grundlegender Satz von Berechtigungen ist eine Sammlung von Berechtigungen, die dem Prozess eines Benutzers bei der Anmeldung zugewiesen werden.

Bereich 1. Das logische Netzwerk, in dem eine einzige Kerberos-Datenbank und ein Satz von Key Distribution Centers (KDCs) verwendet werden.

2. Dritter Teil eines Hauptelementnamens. In dem Hauptelementnamen `jdoe/admin@ENG.EXAMPLE.COM` lautet der Bereich wie folgt: `ENG.EXAMPLE.COM`. Weitere Informationen finden Sie unter Hauptelementname.

Beziehung Eine Konfigurationsvariable oder Beziehung, die in der Datei `kdc.conf` oder der Datei `krb5.conf` definiert ist.

Blowfish Ein symmetrischer Blockzifferalgorithmus, der einen Schlüssel mit variabler Länge zwischen 32 und 448 Bit akzeptiert. Der Autor, Bruce Schneier, ist der Meinung, dass Blowfish für Anwendungen optimiert ist, bei denen der Schlüssel nicht häufig geändert wird.

Client Im engeren Sinn ist dies ein Prozess, der einen Netzwerkdienst im Namen eines Benutzers verwendet, beispielsweise eine Anwendung, die `rlogin` nutzt. In einigen Fällen kann ein Server selbst ein Client eines anderen Servers oder Service sein.

Im weiteren Sinn ist darunter ein Host zu verstehen, der a) einen Kerberos-Berechtigungsnachweis erhält und b) einen von einem Server bereitgestellten Service nutzt.

Inoffiziell wird damit auch ein Hauptelement bezeichnet, das einen Service verwendet.

Client-Hauptelement (RPCSEC_GSS API) Ein Client (ein Benutzer oder eine Anwendung), der RPCSEC_GSS-gesicherte Netzwerkdienste verwendet. Die Namen der Client-Hauptelemente werden in Form von `rpc_gss_principal_t`-Strukturen gespeichert.

DES Data Encryption Standard. Eine 1975 entwickelte und 1981 als ANSI X.92.56 von ANSI standardisierte symmetrische Verschlüsselungsmethode. DES verwendet einen 56-Bit-Schlüssel.

Diffie-Hellman-Protokoll Wird auch als Public-Key-Kryptografie bezeichnet. Ein von Diffie und Hellman 1976 entwickeltes asymmetrisches Kryptografieprotokoll zum Schlüsselaustausch. Mithilfe dieses Protokolls können zwei Benutzer einen Geheimschlüssel über einen nicht datensicheren Übertragungskanal austauschen. Diffie-Hellman wird von Kerberos verwendet.

Digest Weitere Informationen finden Sie unter Meldungs-Digest.

DSA Digital Signature Algorithm. Ein Public-Key-Algorithmus mit einer variablen Schlüsselgröße zwischen 512 und 4096 Bit. Der Standard der US-Regierung, DSS, verwendet bis zu 1024 Bit. DSA verlässt sich zur Eingabe auf SHA1.

Effektiver Satz Der Satz von Privilegien, die derzeit für einen Prozess verwendet werden.

Einzelnes System-Image Der Begriff "einzelnes System-Image" wird bei Oracle Solaris-Prüfungen zur Beschreibung einer Gruppe geprüfter Systeme verwendet, die den gleichen Naming Service nutzen. Diese Systeme senden Prüfdatensätze an einen zentralen Prüfserver, wobei die Datensätze so verglichen werden können, als kämen sie von einem System.

Erneuerbares Ticket Da Tickets mit einer sehr langen Lebensdauer ein Sicherheitsrisiko darstellen, können sie als *erneuerbar* definiert werden. Ein erneuerbares Ticket hat zwei Ablaufzeiten: a) die Zeit, zu der die aktuelle Instanz des Tickets abläuft, und b) die maximale Lebensdauer für jedes Ticket, die eine Woche beträgt. Wenn ein Client ein Ticket weiterhin verwenden möchte, erneuert er es vor Ende der ersten Ablaufzeit. Beispiel: Ein Ticket kann für eine Stunde gültig sein, während alle Tickets eine maximale Lebensdauer von zehn Stunden aufweisen. Wenn der Client das Ticket für mehr als eine Stunde behalten möchte, muss er es erneuern. Erreicht ein Ticket die maximale Lebensdauer für Tickets, läuft es automatisch ab und kann nicht erneuert werden.

FQDN Vollständig qualifizierter Domainname (Fully Qualified Domain Name). Beispielsweise `central.example.com` (statt einfach `denver`).

Geheimer Schlüssel Weitere Informationen finden Sie unter Privater Schlüssel.

Geräterichtlinie Geräteschutz auf Kernel-Ebene. Die Geräterichtlinie wird durch zwei Berechtigungssätze auf einem Gerät implementiert. Ein Berechtigungssatz steuert den Lesezugriff auf das Gerät. Der zweite Berechtigungssatz steuert den Schreibzugriff auf das Gerät. Weitere Informationen finden Sie unter Richtlinie.

Gerätezuordnung Geräteschutz auf Benutzerebene. Durch die Gerätezuordnung wird die Verwendung eines Geräts auf jeweils einen Benutzer beschränkt. Die Gerätedaten werden vor der erneuten Verwendung des Geräts gelöscht. Mit Autorisierungen kann beschränkt werden, wer ein Gerät zuordnen darf.

Grundlegender Satz Der Berechtigungssatz, der dem Benutzerprozess bei der Anmeldung zugewiesen wird. Auf einem unveränderten System entspricht der ursprünglich vererbbare Satz jedes Benutzers dem grundlegenden Satz bei der Anmeldung.

GSS-API Generic Security Service Application Programming Interface. Eine Netzwerkebene, die verschiedene modulare Sicherheitsservices, wie den Kerberos-Service, unterstützt. Die GSS-API bietet Sicherheitsauthentifizierungs-, Integritäts- und Vertraulichkeitsservices. Weitere Informationen finden Sie unter Authentifizierung, Integrität und Vertraulichkeit.

Hardwareprovider Im Oracle Solaris Cryptographic Framework entspricht dies einem Gerätetreiber und dessen Hardwarebeschleuniger. Hardwarebeschleuniger übernehmen aufwändige kryptografische Vorgänge für das Computersystem und entlasten so die CPU-Ressourcen, sodass diese für andere Zwecke zur Verfügung stehen. Weitere Informationen finden Sie unter Provider.

Hauptelement 1. Eine eindeutig benannte Client/Benutzer- oder Server/Service-Instanz, die an einer Kommunikation über das Netzwerk beteiligt ist. Kerberos-Transaktionen umfassen Interaktionen zwischen Hauptelementen (Service-Hauptelemente und Benutzer-Hauptelemente) oder zwischen Hauptelementen und KDCs. In anderen Worten stellt ein Hauptelement eine eindeutige Einheit dar, der Kerberos Tickets zuweisen kann. Weitere Informationen finden Sie unter Hauptelementname, Service-Hauptelement und Benutzer-Hauptelement.

2. (RPCSEC_GSS API) Weitere Informationen finden Sie unter Client-Hauptelement und Server-Hauptelement.

Hauptelementname 1. Der Name eines Hauptelements im Format *primary/instance@REALM*. Weitere Informationen finden Sie unter Instanz, Primärer Name und Bereich.

2. (RPCSEC_GSS API) Weitere Informationen finden Sie unter Client-Hauptelement und Server-Hauptelement.

Host System, das über ein Netzwerk verfügbar ist

Host-Hauptelement Eine bestimmte Instanz eines Service-Hauptelements, in der das Hauptelement (gekennzeichnet durch den primären Namen `host`) zur Bereitstellung einer Reihe von Netzwerkdiensten wie `ftp`, `rcp` oder `rlogin` eingerichtet ist. Ein Beispiel eines Host-Hauptelements ist `host/central.example.com@EXAMPLE.COM`. Weitere Informationen finden Sie unter Server-Hauptelement.

Instanz Der zweite Teil eines Hauptelementnamens, die den primären Namen des Hauptelements näher bestimmt. Bei einem Service-Hauptelement ist die Instanz erforderlich. Die Instanz gehört zum vollständig qualifizierten Domainnamen, wie z. B. `host/central.example.com`. Für Benutzer-Hauptelemente ist eine Instanz optional. Beachten Sie jedoch, dass `jdoe` und `jdoe/admin` eindeutige Hauptelemente sind. Weitere Informationen finden Sie unter Primärer Name, Hauptelementname, Service-Hauptelement und Benutzer-Hauptelement.

Integrität Ein Sicherheitsservice, der zusätzlich zur Benutzerauthentifizierung die Gültigkeit der übertragenen Daten durch kryptografische Prüfsummen gewährleistet. Weitere Informationen finden Sie unter Authentifizierung und Vertraulichkeit.

KDC Key Distribution Center. Ein Rechner mit drei Kerberos V5-Komponenten:

- Hauptelement und Schlüsseldatenbank
- Authentifizierungsservice
- Ticket-gewährender Service

Jeder Bereich hat ein Master-KDC und sollte über ein oder mehrere Slave-KDCs verfügen.

Kerberos Ein Authentifizierungsservice, das Protokoll, das von dem Service verwendet wird, oder der Code zur Implementierung des Service.

	Die Oracle Solaris Kerberos-Implementierung, die sich eng an der Kerberos V5-Implementierung orientiert. Kerberos und Kerberos V5 sind zwar technisch verschieden, werden jedoch in der Kerberos-Dokumentation oft als Synonyme verwendet. Kerberos (auch Cerberus geschrieben) ist der dreiköpfige Höllenhund, der in der griechischen Mythologie den Eingang zur Unterwelt bewacht.
Kerberos-Richtlinie	Ein Satz von Regeln, die die Passwortverwendung im Kerberos-Service steuert. Richtlinien können die Zugriffe eines Hauptelements oder Ticketparameter wie die Lebensdauer regeln.
kvno	Schlüsselversionsnummer (Key Version Number). Eine Sequenznummer, die in der Reihenfolge des Generierens für Schlüssel vergeben wird. Die höchste kvno ist der neueste und aktuelle Schlüssel.
MAC	1. Siehe Message Authentication Code (MAC). 2. Wird auch als "Labeling" bezeichnet. In der Sicherheitsterminologie der US-Regierung steht MAC für Mandatory Access Control. Bezeichnungen wie "Top Secret" und "Confidential" sind Beispiele für MAC. MAC unterscheidet sich von DAC (Discretionary Access Control). UNIX-Berechtigungen sind ein Beispiel für DAC. 3. Eindeutige Systemadresse für Hardware in einem LAN. Bei einem Ethernet-System entspricht MAC der Ethernet-Adresse.
Master-KDC	Das Haupt-KDC in jedem Bereich, das den Kerberos-Administrationsserver `kadmind` und den Authentifizierungs- und Ticket-gewährenden Dämon `krb5kdc` einschließt. Jeder Bereich muss mindestens ein Master-KDC aufweisen und kann über zahlreiche duplizierte oder Slave-KDCs verfügen, die Clients Authentifizierungsservices bieten.
MD5	Eine iterative kryptografische Hash-Funktion, die zur Nachrichtenauthentifizierung, einschließlich digitaler Signaturen, verwendet wird. Diese Funktion wurde 1991 von Rivest entwickelt.
Mechanismus	1. Ein Softwarepaket, das kryptografische Techniken angibt, um die Authentizität oder Vertraulichkeit von Daten sicherzustellen. Beispiele: Kerberos V5, öffentlicher Diffie-Hellman-Schlüssel. 2. Im Oracle Solaris Cryptographic Framework ist dies eine Implementierung eines Algorithmus für einen bestimmten Zweck. Ein DES-Mechanismus, der auf Authentifizierung angewendet wird, wie z. B. CKM_DES_MAC, ist beispielsweise ein separater Mechanismus aus einem DES-Mechanismus, der auf Verschlüsselung angewendet wird (CKM_DES_CBC_PAD).
Meldungs-Digest	Ein Meldungs-Digest entspricht dem Hash-Wert, der aus einer Meldung errechnet wurde. Der Hash-Wert identifiziert die Meldung fast eindeutig. Ein Digest eignet sich zum Überprüfen der Integrität einer Datei.
Message Authentication Code (MAC)	MAC bietet Zusicherung der Datenintegrität und authentifiziert den Datenursprung. MAC bietet keinen Schutz gegenüber Lauschangriffen.

Minimierung Minimale Betriebssysteminstallation, die zum Ausführen des Servers notwendig ist. Software, die nicht direkt für den Serverbetrieb erforderlich ist, wird entweder nicht installiert oder nach der Installation gelöscht.

Nachdatiertes Ticket Ein nachdatiertes Ticket ist ein Ticket, das erst eine bestimmte Zeit nach seiner Erstellung gültig wird. Ein solches Ticket eignet sich beispielsweise für Batch-Jobs, die spät nachts ausgeführt werden sollen, da das Ticket im Falle eines Diebstahls nicht verwendet werden kann, bis der Batch-Job ausgeführt werden muss. Wenn ein nachdatiertes Ticket ausgestellt wird, wird es als *ungültig* ausgestellt und bleibt dies auch solange, bis a) seine Startzeit abgelaufen ist und b) der Client die Validierung durch das KDC anfordert. Ein nachdatiertes Ticket ist normalerweise bis zur Ablaufzeit des Ticket-gewährenden Tickets gültig. Wenn das Ticket jedoch als *erneuerbar* gekennzeichnet wird, wird seine Lebensdauer normalerweise so festgelegt, dass sie der vollen Lebensdauer des Ticket-gewährenden Tickets entspricht. Weitere Informationen finden Sie unter Ungültiges Ticket und Erneuerbares Ticket.

Name Service-Bereich Der Bereich, in dem eine Rolle gültig ist, d. h. ein einzelner Host oder alle Hosts, die einen bestimmten Naming Service wie NIS, NIS+ oder LDAP verwenden. Bereiche werden auf Solaris Management Console-Werkzeugleisten angewendet.

Netzwerkanwendungsserver Ein Server, der eine Netzwerkanwendung wie `ftp` bereitstellt. Ein Bereich kann mehrere Netzwerkanwendungsserver enthalten.

Nicht zuweisbare Prüfereignisse Ein Prüfereignis, dessen Initiator nicht bestimmt werden kann, wie z. B. das Ereignis AUE_BOOT.

NTP Network Time Protocol. Software der University of Delaware, die eine genaue Zeit- oder Netzwerkuhrsynchronisierung (oder beides) in einer Netzwerkumgebung ermöglicht. Sie können NTP zur Aufrechterhaltung einer Uhrdifferenz in einer Kerberos-Umgebung verwenden. Weitere Informationen finden Sie unter "Uhrdifferenz".

PAM Pluggable Authentication Module. Ein Framework, das die Verwendung von mehreren Authentifizierungsmechanismen erlaubt, ohne die Services neu kompilieren zu müssen, die diese verwenden. PAM ermöglicht eine Kerberos-Sitzungsinitialisierung bei der Anmeldung.

Passwortrichtlinie Die Verschlüsselungsalgorithmen, die zum Generieren von Passwörtern verwendet werden können. Der Begriff kann sich auch auf allgemeinere Aspekte von Passwörtern beziehen, beispielsweise wie oft die Passwörter geändert werden müssen, wie viele falsche Eingaben zulässig sind und andere Sicherheitsfragen. Sicherheitsrichtlinien erfordern Passwörter. Passwortrichtlinien können festlegen, dass Passwörter mit dem MD5-Algorithmus verschlüsselt werden müssen und weitere Anforderungen an Passwörter enthalten.

Passwortsatz Ein Satz, mit dem überprüft wird, ob ein privater Schlüssel vom Benutzer des Passwortsatzes (Kennsatzes) erstellt wurde. Ein guter Passwortsatz ist 10 bis 30 Zeichen lang, besteht aus Buchstaben und Zahlen und enthält keinen einfachen Text und keine leicht zu erratenden Namen. Sie werden nach dem Passwortsatz gefragt, um den privaten Schlüssel zu authentifizieren und Nachrichten zu verschlüsseln und zu entschlüsseln.

Primärer Name Der erste Teil eines Hauptelementnamens. Weitere Informationen finden Sie unter Instanz, Hauptelementname und Bereich.

Privater Schlüssel Ein Schlüssel, den jedes Benutzer-Hauptelement erhält, und der nur dem Benutzer des Hauptelements und dem KDC bekannt ist. Bei Benutzer-Hauptelementen basiert der Schlüssel auf dem Passwort des Benutzers. Weitere Informationen finden Sie unter Schlüssel.

Privilegierte Anwendung Eine Anwendung, die Systemeinstellungen außer Kraft setzen kann. Die Anwendung überprüft Sicherheitsattribute wie spezifische UIDs, GIDs, Autorisierungen oder Berechtigungen.

Profil-Shell In RBAC ist dies eine Shell, mit der eine Rolle (oder ein Benutzer) jede privilegierte Anwendung, die den Berechtigungsprofilen der Rolle zugewiesen ist, auf der Befehlszeile ausführen kann. Die Profil-Shells sind `pfsh`, `pfcsh` und `pfksh`. Sie entsprechen der Bourne-Shell (`sh`), C-Shell (`csh`) bzw. Korn-Shell (`ksh`).

Provider Im Oracle Solaris Cryptographic Framework ist dies ein kryptografischer Service, der für Verbraucher bereitgestellt wird. PKCS #11-Bibliotheken, kryptografische Kernel-Module und Hardwarebeschleuniger sind Beispiele für Provider. Provider werden in das kryptografische Framework integriert und daher auch als *Plugins* bezeichnet. Beispiele für Verbraucher finden Sie unter Verbraucher.

Proxy-fähiges Ticket Ein Ticket, das im Auftrag eines Clients von einem Service verwendet werden kann, um einen Vorgang für den Client auszuführen. Der Service agiert dann als Proxy des Clients. Mit dem Ticket kann der Service die Identität des Clients annehmen. Der Service kann ein Proxy-fähiges Ticket verwenden, um ein Service-Ticket bei einem anderen Service zu erhalten, kann jedoch kein Ticket-gewährendes Ticket erhalten. Der Unterschied zwischen einem Proxy-fähigen Ticket und einem weiterleitbaren Ticket besteht darin, dass ein Proxy-fähiges Ticket nur für einen einzigen Vorgang gültig ist. Weitere Informationen finden Sie unter Weiterleitbares Ticket.

Prüfdateien Binäre Prüfprotokolle. Prüfdateien werden separat in einer Prüfpartition gespeichert.

Prüfpartition Eine Festplattenpartition, die zum Speichern von Prüfdateien konfiguriert ist.

Prüfpfad Die gesammelten Prüfdateien aller Hosts

Prüfrichtlinie Die globalen und benutzerspezifischen Einstellungen, die bestimmen, welche Prüfereignisse aufgezeichnet werden. Die globalen Einstellungen für den Prüfservice legen in der Regel fest, welche optionalen Informationen in den Prüfpfad aufgenommen werden. Zwei Einstellungen, `cnt` und `ahlt`, betreffen den Betrieb des Systems, wenn sich die Prüfwarteschlange füllt. Beispielsweise kann die Prüfrichtlinie erfordern, dass jeder Prüfdatensatz eine Sequenznummer enthält.

QOP Sicherheitsqualität (Quality of Protection). Ein Parameter zur Auswahl kryptografischer Algorithmen, die in Verbindung mit dem Integritätsservice oder Vertraulichkeitsservice verwendet werden

RBAC Rollenbasierte Zugriffssteuerung (Role-Based Access Control). Eine Alternative zum Superuser-Modell (alles oder nichts). Mit RBAC können Superuser-Fähigkeiten unterteilt und bestimmten Benutzerkonten, auch Rollen genannt, zugewiesen werden. Die Rollen können einzelnen Benutzern entsprechend ihrer Zuständigkeit zugewiesen werden.

RBAC-Richtlinie Die Sicherheitsrichtlinie, die einem Befehl zugewiesen ist. Derzeit sind `suser` und `solaris` gültige Richtlinien. Die Richtlinie `solaris` erkennt Berechtigungen, Autorisierungen und `setuid`-Sicherheitsattribute. Die Richtlinie `suser` erkennt nur `setuid`-Sicherheitsattribute. Trusted Solaris- und Trusted Extensions-Systeme, die mit einem Oracle Solaris-System interagieren können, bieten die Richtlinie `tsol`, die Berechtigungen, `setuid`-Sicherheitsattribute und Bezeichnungen für Prozesse erkennt.

Richtlinie Allgemein ist dies ein Plan oder eine Vorgehensweise, die Entscheidungen und Aktionen beeinflusst oder bestimmt. Bei Computersystemen bezieht sich dieser Begriff in der Regel auf die Sicherheitsrichtlinie. Die für Ihren Standort geltende Sicherheitsrichtlinie stellt eine Reihe von Regeln dar, die die Sensitivität der verarbeiteten Informationen sowie die zum Schutz der Informationen vor unberechtigtem Zugriff angewendeten Maßnamen bestimmen. Beispielsweise kann die Sicherheitsrichtlinie erfordern, dass Systeme geprüft werden, Geräte durch Berechtigungen geschützt werden und Passwörter alle sechs Wochen geändert werden.

Informationen zur Implementierung einer Richtlinie in spezifischen Bereichen des Oracle Solaris-Betriebssystem finden Sie unter Prüfrichtlinie, Richtlinie im kryptografischen Framework, Geräterichtlinie, Kerberos-Richtlinie, Passwortrichtlinie und RBAC-Richtlinie.

Richtlinie für öffentliche Schlüsseltechnologien Im Key Management Framework (KMF) besteht eine Richtlinie darin, die Zertifikatverwendung zu verwalten. Die KMF-Richtliniendatenbank kann die Verwendung der von der KMF-Bibliothek verwalteten Schlüssel und Zertifikate einschränken.

Richtlinie im kryptografischen Framework In Oracle Solaris Cryptographic Framework besteht eine Richtlinie darin, vorhandene kryptografische Mechanismen zu deaktivieren. Diese Mechanismen können dann nicht verwendet werden. Eine Richtlinie im kryptografischen Framework kann die Verwendung eines bestimmten Mechanismus wie `CKM_DES_CBC` von einem Provider wie DES verhindern.

Rolle Eine spezielle Identität zum Ausführen privilegierter Anwendungen, die nur von den Benutzern angenommen werden kann, denen sie zugewiesen ist.

RSA Eine Methode zum Beziehen digitaler Signaturen und Public-Key-Kryptosystemen. Diese Methode wurde zuerst 1978 von seinen Entwicklern Rivest, Shamir und Adleman beschrieben.

Schlüssel

1. Im Allgemeinen einer von zwei Hauptschlüsseltypen:
   - Ein *symmetrischer Schlüssel* ist ein Verschlüsselungsschlüssel, der mit einem Entschlüsselungsschlüssel identisch ist. Symmetrische Schlüssel werden zum Verschlüsseln von Dateien verwendet.
   - Ein *asymmetrischer Schlüssel* oder *öffentlicher Schlüssel* wird in öffentlichen Schlüsselalgorithmen wie Diffie-Hellman oder RSA verwendet. Öffentliche Schlüssel schließen einen privaten Schlüssel ein, der nur einem Benutzer bekannt ist, einen öffentlichen Schlüssel, der vom Server oder der allgemeinen Ressource verwendet wird und ein Paar aus privatem und öffentlichem Schlüssel, in dem beide kombiniert werden. Ein privater Schlüssel wird auch als *geheimer* Schlüssel bezeichnet. Der öffentliche Schlüssel wird auch als *gemeinsam genutzter* oder *nicht geheimer* Schlüssel bezeichnet.
   - 2. Ein Eintrag (Hauptelementname) in der Schlüsseltabellendatei. Weitere Informationen finden Sie unter Schlüsseltabellendatei.

   3. Ein Verschlüsselungsschlüssel in Kerberos, wobei es drei Typen gibt:
   - Ein *privater Schlüssel* ist ein Schlüssel, der von einem Hauptelement und dem KDC gemeinsam genutzt wird und außerhalb der Grenzen des Systems verteilt wird. Weitere Informationen finden Sie unter Privater Schlüssel.
   - Ein *Serviceschlüssel* dient dem gleichen Zweck wie der private Schlüssel, wird jedoch von Servern und Services verwendet. Weitere Informationen finden Sie unter Serviceschlüssel.
   - Ein *Sitzungsschlüssel* ist ein temporärer Verschlüsselungsschlüssel, der zwischen zwei Hauptelementen verwendet wird und dessen Lebensdauer auf eine einzige Anmeldesitzung begrenzt ist. Weitere Informationen finden Sie unter Sitzungsschlüssel.

Schlüsseltabellendatei

Eine Schlüsseltabellendatei enthält mindestens einen Schlüssel (Hauptelemente). Ein Host oder Service verwendet eine Schlüsseltabellendatei auf die gleiche Art, auf die auch ein Benutzer ein Passwort verwendet.

SEAM

Sun Enterprise Authentication Mechanism. Der Produktname der ersten Versionen eines Systems zur Authentifizierung von Benutzern über ein Netzwerk, das auf der vom Massachusetts Institute of Technology entwickelten Kerberos V5-Technologie beruhte. Das Produkt wird nun Kerberos-Service genannt. SEAM bezieht sich jetzt auf die Teile des Kerberos-Service, die nicht in die verschiedenen Solaris-Versionen integriert wurden.

Secure Shell

Ein spezielles Protokoll für eine sichere Remote-Anmeldung und andere sichere Netzwerkdienste über ein unsicheres Netzwerk.

Seed

Ein numerischer Startpunkt zum Generieren von Zufallszahlen. Wenn der Startpunkt aus einer zufälligen Quelle stammt, wird er als *Random Seed* (Zufallsstartpunkt) bezeichnet.

Server

Ein Hauptelement, das eine Ressource für Netzwerkclients bereitstellt. Beispiel: Bei `ssh` auf dem System `central.example.com` ist dieses System der Server, der den `ssh`-Service bereitstellt. Weitere Informationen finden Sie unter Service-Hauptelement.

Server-Hauptelement (RPCSEC_GSS API) Ein Hauptelement, das einen Service bereitstellt. Das Server-Hauptelement wird als ASCII-Zeichenfolge in der Form *service*@*host* gespeichert. Weitere Informationen finden Sie unter Client-Hauptelement.

Service 1. Eine Ressource, die den Netzwerkclients zur Verfügung gestellt wird, oft von mehreren Servern. Bei `rlogin` auf dem Rechner `central.example.com` ist dieser Rechner der Server zur Bereitstellung des `rlogin`-Service.

2. Ein Sicherheitsservice (entweder Integrität oder Vertraulichkeit), der mehr Schutz als die Authentifizierung bietet. Weitere Informationen finden Sie unter Integrität und Vertraulichkeit.

Service-Hauptelement Ein Hauptelement, das eine Kerberos-Authentifizierung für einen oder mehrere Services bietet. Für Sicherheits-Hauptelemente ist der primäre Name der Name des Service wie `ftp` und die Instanz der vollständig qualifizierte Hostname des Systems, das den Service bereitstellt. Weitere Informationen finden Sie unter Host-Hauptelement und Benutzer-Hauptelement.

Serviceschlüssel Ein Verschlüsselungsschlüssel, der vom Service-Hauptelement und dem KDC gemeinsam genutzt wird und außerhalb der Systemgrenzen verteilt wird. Weitere Informationen finden Sie unter Schlüssel.

SHA1 Secure Hashing Algorithm. Dieser Algorithmus arbeitet mit jeder Eingabelänge kleiner als 2^{64}, um einen Meldungs-Digest zu erzeugen. Der SHA-1-Algorithmus ist die Eingabe für DSA.

Sicherheitsattribute In RBAC bezieht sich dieser Begriff auf Überschreibungen der Sicherheitsrichtlinie, durch die ein administrativer Befehl von einem anderen Benutzer als dem Superuser erfolgreich ausgeführt werden kann. Im Superuser-Modell sind die Programme `setuid` und `setgid` Sicherheitsattribute. Wenn diese Attribute auf einen Befehl angewendet werden, kann der Befehl unabhängig von dem Benutzer erfolgreich ausgeführt werden. In einem Berechtigungsmodell sind Sicherheitsattribute Berechtigungen. Wenn ein Befehl eine Berechtigung erhält, kann er erfolgreich ausgeführt werden. Das Berechtigungsmodell ist mit dem Superuser-Modell kompatibel, da das Berechtigungsmodell ebenfalls die Programme `setuid` und `setgid` als Sicherheitsattribute erkennt.

Sicherheitsmechanismus Weitere Informationen finden Sie unter Mechanismus.

Sicherheitsrichtlinie Weitere Informationen finden Sie unter Richtlinie.

Sicherheitsservice Weitere Informationen finden Sie unter Service.

Sicherheitsvariante Weitere Informationen finden Sie unter Variante.

Sitzungsschlüssel Ein Schlüssel, der vom Authentifizierungsservice oder dem Ticket-gewährenden Service generiert wird. Ein Sitzungsschlüssel wird generiert, um sichere Transaktionen zwischen einem Client und einem Service zu gewährleisten. Die Lebensdauer eines Sitzungsschlüssels ist auf eine einzige Anmeldesitzung beschränkt. Weitere Informationen finden Sie unter Schlüssel.

Slave-KDC Eine Kopie eines Master-KDC, die die meisten Funktionen des Masters durchführen kann. Jeder Bereich hat normalerweise mehrere Slave-KDCs (und nur ein Master-KDC). Weitere Informationen finden Sie unter KDC und Master-KDC.

Softwareprovider Im Oracle Solaris Cryptographic Framework ist dies ein Kernel-Softwaremodul oder eine PKCS #11-Bibliothek, die kryptografische Services bietet. Weitere Informationen finden Sie unter Provider.

Stash-Datei Eine Stash-Datei enthält eine verschlüsselte Kopie des Master-Schlüssels für das KDC. Dieser Master-Schlüssel wird verwendet, wenn ein Server zur automatischen Authentifizierung des KDC vor dem Starten der Prozesse `kadmind` und `krb5kdc` neu gestartet wird. Da die Stash-Datei den Master-Schlüssel enthält, sollten sie und die zugehörigen Backups vor unberechtigten Zugriffen geschützt werden. Andernfalls kann der Schlüssel von unberechtigten Benutzern verwendet werden, um auf die KDC-Datenbank zuzugreifen oder sie zu ändern.

Superuser-Modell Das typische UNIX-Sicherheitsmodell auf einem Computersystem. Beim Superuser-Modell hat ein Administrator entweder die gesamte Kontrolle über ein System oder gar keine. In der Regel meldet sich ein Benutzer als Superuser (`root`) an, um die administrativen Aufgaben für ein System durchzuführen.

Synchrones Prüfereignis Die meisten Prüfereignisse. Ereignisse, die einem Prozess im System zugewiesen sind. Ein nicht zuweisbares Ereignis, das mit einem Prozess verbunden ist, wird als synchrones Ereignis bezeichnet. Beispiel: fehlgeschlagene Anmeldung.

TGS Ticket-gewährender Service. Der Teil des KDC, der für die Ausgabe von Tickets zuständig ist.

TGT Ticket-gewährendes Ticket. Ein Ticket, das vom KDC ausgegeben wurde und einem Client die Anforderung von Tickets für andere Services ermöglicht.

Ticket Ein Informationspaket, das zur sicheren Übergabe der Identität eines Benutzers an einen Server oder Service verwendet wird. Ein Ticket ist nur für einen einzigen Client und einen bestimmten Service auf einem spezifischen Server gültig. Ein Ticket enthält den Hauptelementnamen des Service, den Hauptelementnamen des Benutzers, die IP-Adresse vom Host des Benutzers, einen Zeitstempel und einen Wert, der die Lebensdauer des Tickets definiert. Ein Ticket wird mit einem nach dem Zufallsprinzip erstellten Sitzungsschlüssel erstellt, der von Client und Service verwendet wird. Nach der Erstellung eines Tickets kann es solange wiederverwendet werden, bis es abläuft. Ein Ticket dient nur zur Authentifizierung eines Clients, wenn es über einen aktuellen Authentifizierer verfügt. Weitere Informationen finden Sie unter Authentifizierer, Berechtigungsnachweis, Service und Sitzungsschlüssel.

Ticketdatei Weitere Informationen finden Sie unter Berechtigungsnachweis-Cache.

Uhrdifferenz Die maximale Zeitspanne für die Abweichung der internen Systemuhren auf allen Hosts, die an einem Kerberos-Authentifizierungssystem beteiligt sind. Wenn die Uhrdifferenz zu einem der Hosts überschritten wird, werden Anforderungen abgewiesen. Die Uhrdifferenz kann in der Datei `krb5.conf` angegeben werden.

Ungültiges Ticket Ein nachdatiertes Ticket, das noch nicht verwendet werden kann. Ein ungültiges Ticket wird solange von einem Anwendungsserver abgewiesen, bis es validiert wird. Dazu muss ein ungültiges Ticket nach Ablauf seiner Startzeit vom Client in einer TGS-Anforderung an das KDC gesendet werden, wobei das Flag `VALIDATE` festgelegt sein muss. Weitere Informationen finden Sie unter Nachdatiertes Ticket.

Variante Herkömmlich hatten *Sicherheitsvariante* und *Authentifizierungsvariante* dieselbe Bedeutung, nämlich eine Variante, die den Typ der Authentifizierung (AUTH_UNIX, AUTH_DES, AUTH_KERB) angab. RPCSEC_GSS ist außerdem eine Sicherheitsvariante, da sie Integritäts- und Vertraulichkeitsservices zusätzlich zur Authentifizierung bietet.

Verbraucher In Oracle Solaris Cryptographic Framework ist ein Verbraucher ein Benutzer von kryptografischen Services, die von Providern bereitgestellt werden. Benutzer können Anwendungen, Endbenutzer oder Kernel-Vorgänge sein. Kerberos, IKE und IPsec sind Beispiele für Verbraucher. Beispiele für Provider finden Sie unter Provider.

Vererbbarer Satz Der Berechtigungssatz, den ein Prozess über einen Aufruf von `exec` erben kann.

Verschlüsselung mit öffentlichem Schlüssel Ein Verschlüsselungsalgorithmus, bei dem jeder Benutzer über zwei Schlüssel verfügt, einen öffentlichen und einen privaten Schlüssel. Bei einer Verschlüsselung mit einem öffentlichen Schlüssel, verschlüsselt der Absender die Nachricht mit dem öffentlichen Schlüssel des Empfängers und der Empfänger entschlüsselt die Nachricht mit einem privaten Schlüssel. Der Kerberos-Service basiert auf privaten Schlüsseln. Weitere Informationen finden Sie unter Verschlüsselung mit privatem Schlüssel.

Verschlüsselung mit privatem Schlüssel Bei einer Verschlüsselung mit einem privaten Schlüssel verwenden Sender und Empfänger den gleichen Schlüssel zur Verschlüsselung. Weitere Informationen finden Sie unter Verschlüsselung mit öffentlichem Schlüssel.

Verschlüsselungsalgorithmus Weitere Informationen finden Sie unter Algorithmus.

Vertraulichkeit Weitere Informationen finden Sie unter Vertraulichkeit.

Vertraulichkeit Ein Sicherheitsservice, der Daten vor der Übertragung verschlüsselt. Dieser Service schließt auch Datenintegrität und Benutzerauthentifizierung ein. Weitere Informationen finden Sie unter Authentifizierung, Integrität und Service.

Virtuelles privates Netzwerk (VPN) Ein Netzwerk, das durch Verschlüsselung und Tunneling eine sichere Kommunikation zwischen Benutzern in einem öffentlichen Netzwerk ermöglicht.

Weiterleitbares Ticket Ein Ticket, mit dem der Client ein Ticket auf einem Remote-Host anfordern kann, ohne dass der vollständige Authentifizierungsprozess auf dem Host durchgeführt wird. Beispiel: Wenn der Benutzer `david` ein weiterleitbares Ticket abruft, während er sich am Rechner von `jennifer` befindet, kann er sich bei seinem eigenen Rechner anmelden, ohne dafür ein neues Ticket zu benötigen (und sich somit erneut zu authentifizieren). Weitere Informationen finden Sie unter Proxy-fähiges Ticket.

Zugelassener Satz Berechtigungssatz, der von einem Prozess verwendet werden kann

Zugriffssteuerungsliste (Access Control List, ACL)

Mit einer Zugriffssteuerungsliste (Access Control List, ACL) kann die Dateisicherheit genauer bestimmt werden als mit dem traditionellen UNIX-Dateischutz. Beispielsweise können Sie mit einer ACL einer Gruppe Lesezugriff und einem Mitglied der Gruppe Schreibzugriff auf eine Datei gewähren.

Index

Zahlen und Symbole

$$ (doppeltes Dollarzeichen), Nummer des übergeordneten Shell-Prozesses, 267
[] (eckige Klammern), `bsmrecord` (Ausgabe), 710
@ (At-Zeichen), `device_allocate` (Datei), 103
^ (Caret) in Prüfklassenpräfixen, 705
? (Fragezeichen), tune-Dateien bei ASET, 177
= (Gleichheitszeichen), Dateiberechtigungssymbol, 137
- (Minussymbol), Dateitypsymbol, 132
- (Minuszeichen)
  Dateiberechtigungssymbol, 137
  Prüfklassenpräfix, 704
  `sulog` (Datei), 78
+ (Pluszeichen)
  ACL-Eintrag, 150
  Dateiberechtigungssymbol, 137
  Prüfklassenpräfix, 704
  `sulog` (Datei), 78
. (Punkt)
  Autorisierungsnamen-Trennzeichen, 252
  Pfadvariableneintrag, 51
  verborgene Dateien anzeigen, 143
(Rautezeichen)
  `device_allocate` (Datei), 103
  `device_maps` (Datei), 102
; (Semikolon)
  `device_allocate` (Datei), 102
  Trennzeichen für Sicherheitsattribute, 260
* (Sternchen)
  `device_allocate` (Datei), 102, 103
  in RBAC-Autorisierungen überprüfen, 245
* (Sternchen) *(Fortsetzung)*
  Platzhalterzeichen
    in ASET, 175, 177
    in RBAC-Autorisierungen, 252, 256
\ (umgekehrter Schrägstrich)
  `device_allocate` (Datei), 103
  `device_maps` (Datei), 102
> (Ausgabe umleiten), verhindern, 52
>> (Ausgabe anfügen), verhindern, 52
`~/.gkadmin` (Datei), Beschreibung, 587
`~/.k5login` (Datei), Beschreibung, 587
`~/.rhosts` (Datei), Beschreibung, 399
`~/.shosts` (Datei), Beschreibung, 400
`~/.ssh/authorized_keys` (Datei)
  Beschreibung, 399
  Überschreibung, 401
`~/.ssh/config` (Datei)
  Beschreibung, 400
  Überschreibung, 400
`~/.ssh/environment` (Datei), Beschreibung, 400
`~/.ssh/id_dsa` (Datei), Überschreibung, 401
`~/.ssh/id_rsa` (Datei), Überschreibung, 401
`~/.ssh/identity` (Datei), Überschreibung, 401
`~/.ssh/known_hosts` (Datei)
  Beschreibung, 399
  Überschreibung, 401
`~/.ssh/rc` (Datei), Beschreibung, 400
`3des` (Verschlüsselungsalgorithmus), `ssh_config` (Datei), 393
`3des-cbc` (Verschlüsselungsalgorithmus), `ssh_config` (Datei), 393

A

-A (Option), auditreduce (Befehl), 668
-a (Option)
  bsmrecord (Befehl), 665
  digest (Befehl), 304
  encrypt (Befehl), 307
  getfacl (Befehl), 153
  kerberisierte Befehle, 579
  mac (Befehl), 305
  smrole (Befehl), 223–224
Abrufen
  Berechtigungsnachweis für einen Server, 600–601
  Berechtigungsnachweis für einen TGS, 599
  Tickets mit kinit, 570–571
  weiterleitbare Tickets, 570
  Zugriff auf einen bestimmten Service, 601–602
Absoluter Mode, besondere Berechtigungen
  festlegen, 138
Absoluter Modus
  Beschreibung, 136
  besondere Dateiberechtigungen ändern, 148–149
  Dateiberechtigungen ändern, 136, 147–148
ACL
  ACL-Einträge kopieren, 152
  Befehle, 141
  Benutzerverfahren, 149–154
  Beschränkungen beim Kopieren von Einträgen, 139
  Beschreibung, 55–56, 138–141
  Einträge ändern, 152–153
  Einträge anzeigen, 141, 153–154
  Einträge einstellen, 150–151
  Einträge löschen, 141, 153
  Einträge prüfen, 149–150
  Format der Einträge, 138–141
  für eine Datei einstellen, 150
  gültige Dateieinträge, 140
  kadm5.acl (Datei), 539, 541, 545
  Standardeinträge für Verzeichnisse, 140–141
  Übersicht der Schritte, 149–154
  Verzeichniseinträge, 140–141
acl (Prüf-Token), Format, 712
add_drv (Befehl), Beschreibung, 98
admin_server (Abschnitt)
  krb5.conf (Datei), 439, 446
administrative (Prüfklasse), 704
administrative (veraltet) (Prüfklasse), 704
AES (Kernel-Provider), 310
aes128-cbc (Verschlüsselungsalgorithmus),
  ssh_config (Datei), 393
aes128-ctr (Verschlüsselungsalgorithmus),
  ssh_config (Datei), 393
Agentendämon, Secure Shell, 380–381
ahlt (Prüfrichtlinie)
  Beschreibung, 629
  einrichten, 654–655
Aktivieren
  Abbruch über Tastatur, 81–82
  Gerätezuordnung, 88–89
  kryptografische Mechanismen, 315
  Mechanismen und Funktionen auf
    Hardwareprovider, 320
  nur kerberisierte Anwendungen, 506
  Prüfservice, 656–657
  Prüfservice (Übersicht der Schritte), 648–649
  Prüfung, 656–657
  Verwendung von Kernel-Softwareprovidern, 317
Aktualisieren
  kryptografische Services, 321–322
  Prüfservice, 659–660
Algorithmen
  Dateiverschlüsselung, 307–309
  Definition im kryptografischen Framework, 291
  im kryptografischen Framework auflisten, 310–312
  Passwortverschlüsselung, 43
Algorithmus
  Passwort
    Konfiguration, 73–74
all, in Benutzerprüffeldern, 699
all (Prüfklasse)
  Beschreibung, 703
  Vorsicht bei Verwendung, 705
All (RBAC), Berechtigungsprofil, 251
Allgemeine Schlüssel
  berechnen, 339
  DH-Authentifizierung, 336–340
allhard (Zeichenfolge), audit_warn (Skript), 701
allocate (Befehl)
  Autorisierungen, 101

allocate (Befehl) *(Fortsetzung)*
Autorisierungen erforderlich, 263
Bandlaufwerk, 94
Benutzerautorisierung, 89
Beschreibung, 100
verwenden, 93–94
Zuweisungsfehlerstatus, 101
AllowGroups (Schlüsselwort), sshd_config (Datei), 393
AllowTcpForwarding (Schlüsselwort)
ändern, 375
sshd_config (Datei), 393
AllowUsers (Schlüsselwort), sshd_config (Datei), 393
allsoft (Zeichenfolge), audit_warn (Skript), 700
ALTSHELL in Secure Shell, 397
always-audit classes
audit_user (Datenbank), 699
Prozessvorauswahlmaske, 707
Analyse, praudit (Befehl), 693
Andere ACL-Einträge, Beschreibung, 140
Ändern
ACL-Einträge, 152–153
audit_class (Datei), 646
audit_control (Datei), 639–641
audit_event (Datei), 647–648
Benutzer (RBAC), 241–243
Benutzereigenschaft über Befehlszeile, 243
Berechtigungsprofil über Befehlszeile, 240
Berechtigungsprofilinhalt, 238–241
besondere Dateiberechtigungen, 148–149
Dateiberechtigungen
absoluter Modus, 147–148
besondere, 148–149
symbolischer Modus, 146
Dateieigentümerschaft, 144–145
Eigenschaften einer Rolle, 236–238
geheime Schlüssel bei NFS, 337
Geräterichtlinie, 85–86
Gruppeneigentümerschaft einer Datei, 145–146
Hauptelemente (Kerberos), 542–543
Password mit passwd, 574
Passwort einer Rolle, 234–236
Passwort eines Hauptelements (Kerberos), 542–543
Passwort mit kpasswd, 574
Ändern *(Fortsetzung)*
Passwortalgorithmen (Übersicht der Schritte), 72–73
Passwortalgorithmus für eine Domain, 74
Passwortsatz für Secure Shell, 378–379
Richtlinien (Kerberos), 553–554
Rollen (RBAC), 236–238
Rollenzuweisung eines Benutzers, 220
root-Benutzer in Rolle, 226–229
Standard-Passwortalgorithmus, 72–73
zuordenbare Geräte, 91–92
Anfängliches Ticket, Definition, 593
Anfügepfeil (>>), Anfügen verhindern, 52
Anmeldedateien, fehlgeschlagene
Anmeldeversuche, 68–70
Anmelden
Anmeldestatus eines Benutzers anzeigen, 65–66
Anmeldungen prüfen, 686–687
AUTH_DH, 337–338
Fehlschläge überwachen, 67–68
grundlegender Berechtigungssatz von Benutzern, 207
mit Secure Shell, 379–380
Protokoll fehlgeschlagener Anmeldeversuche, 68–70
root-Anmeldung
auf Konsole beschränken, 78–80
überwachen, 50
Sicherheit
fehlgeschlagene Versuche aufzeichnen, 67–68
root-Anmeldung überwachen, 50
Systemzugriffssteuerung, 41
Zugriffsbeschränkungen, 41
Zugriffssteuerung auf Geräten, 46
Übersicht der Schritte, 64
vorübergehend deaktivieren, 67
Annehmen einer Rolle
in Solaris Management Console, 232–233
in Terminalfenster, 230–232
Primary Administrator, 231
root, 231
Vorgehensweise, 215–229, 229
Anpassen, Manifeste, 114–117
Anpassen eines Berichts (BART), 124–125

Anwendungsserver, konfigurieren, 458–460
Anzeigen
ACL-Einträge, 141, 149–150, 153–154
Anmeldestatus eines Benutzers, 65–66
ASET-Aufgabenstatus, 161, 165
Attribute eines Hauptelements, 536–538
ausgewählte Prüfdatensätze, 667–669
Benutzer ohne Passwort, 66
Berechtigungen auf einem Prozess, 267
Berechtigungen in einer Shell, 267, 276
binäre Prüfdateien, 671–673
Dateiberechtigungen, 143–144
Dateien und verbundene Informationen, 132
Dateiinformationen, 143–144
Digest einer Datei, 304
direkt zugewiesene Berechtigungen, 276
Format der Prüfdatensätze, 665–667
Geräterichtlinie, 84–85
Informationen zur Gerätezuordnung, 90
Inhalt von Berechtigungsprofilen, 252
kryptografische Mechanismen
verfügbar, 312, 316
vorhandene, 311, 312, 316
Liste der Hauptelemente, 534–536
Liste der Richtlinien, 547–549
MAC einer Datei, 306
Provider im kryptografischen Framework, 310–312
Prüfdatensätze, 671–673
Prüfdatensätze in XML-Format, 673
Prüfdatensatzformate, 665–667
Prüfrichtlinien, 654
Richtlinienattribute, 549–551
Rollen, die Sie annehmen können, 230, 262
`root`-Zugriffsversuche, 78–80
Schlüssellistenpuffer mit Befehl `list`, 565
Schlüssellistenpuffer mit dem Befehl `list`, 566
Teilliste von Hauptelementen (Kerberos), 535
Tickets, 571–572
verfügbare kryptografische Mechanismen, 312, 316
Versuche mit dem Befehl `su`, 78–80
vorhandene kryptografische Mechanismen, 312, 316
XML-Prüfdatensätze, 672, 694
zuordenbare Geräte, 90
`application` (Prüfklasse), 704
`arbitrary` (Prüf-Token)
Druckformatfeld, 713
Elementgrößenfeld, 713
Format, 713–714
`ARCFOUR` (Kernel-Provider), 310
`arcfour` (Verschlüsselungsalgorithmus), `ssh_config` (Datei), 393
Archivieren, Prüfdateien, 674–675
Archivierungsbandlaufwerk-Bereinigungsskript, 104
`arg` (Prüf-Token), Format, 714
`arge` (Prüfrichtlinie)
Beschreibung, 630
`arge` (Prüfrichtlinie), einrichten, 682
`arge` (Prüfrichtlinie)
und `exec_env` (Token), 716
`argv` (Prüfrichtlinie)
Beschreibung, 630
`argv` (Prüfrichtlinie), einrichten, 682
`argv` (Prüfrichtlinie)
und `exec_args` (Token), 715–716
ASET
Aliase-Datei
Beispiele, 178
Beschreibung, 167
`UID_ALIASES` (Variable), 170
Arbeitsverzeichnis, 174
`aset` (Befehl)
interaktive Version, 178–179
`-p` (Option), 180
starten, 160
ASET-Ausführung planen, 170, 174
ASET regelmäßig ausführen, 180
`aset.restore` (Befehl), 171
`ASETDIR` (Variable), 174
`asetenv` (Datei), 168, 169
`ASETSECLEVEL` Variable, 174
Ausführungsprotokoll, 164
Beispiele für tune-Dateien, 176
Berichte erfassen, 181–182
Beschreibung, 53, 159–178
`CKLISTPATH_level` (Variable), 176
Fehlerbehebung, 182
Fehlermeldungen, 182

ASET *(Fortsetzung)*
interaktiv ausführen, 178–179
konfigurieren, 168–171, 171
Master-Dateien, 162, 167, 168
NFS-Services, 172
`PERIODIC_SCHEDULE` (Variable), 170, 174
regelmäßig ausführen, 180
regelmäßige Ausführung anhalten, 180–181
`TASKS` (Variable), 169, 175
tune-Dateien, 167, 171
Übersicht der Schritte, 178–182
`uid_aliases` (Datei), 167
`UID_ALIASES` (Variable), 168, 170, 175
Umgebungsdatei, 168
Umgebungsvariablen, 173
ursprünglichen Systemstatus wiederherstellen, 171
`YPCHECK` (Variable), 171, 175
`at` (Befehl), Autorisierungen erforderlich, 263
At-Zeichen (@), `device_allocate` (Datei), 103
`atq` (Befehl), Autorisierungen erforderlich, 263
Attribute, Schlüsselwort in BART, 127
`attribute` (Prüf-Token), 714
Audiogeräte, Sicherheit, 105
`audit` (Befehl)
Beschreibung, 691
Prüfdateien erneut lesen (Option `-s`), 690
Prüfservice aktualisieren, 659–660
Syntax der Datei `audit_control` (Option `-v`) überprüfen, 640
Verzeichniszeiger zurücksetzen (Option `-n`), 690
Vorauswahlmaske für vorhandene Prozesse (Option `-s`), 659
`audit administration` (Prüfklasse), 704
`audit_class` (Datei)
Beschreibung, 696
Fehlerbehebung, 646
Klasse hinzufügen, 646
Audit Control (Berechtigungsprofil), 702
`audit_control` (Datei)
Ausnahmen für `flags` in Datenbank `audit_user`, 699–700
Beispiele, 698
Beschreibung, 697
Einträge, 697
`audit_control` (Datei) *(Fortsetzung)*
Einträge und Zonen, 702–703
`flags`(Zeile)
Prozessvorauswahlmaske, 707
Kernel-Maske für nicht zuweisbare Ereignisse ändern, 659
Klassen überprüfen, 677
konfigurieren, 639–641
`minfree` (Warnung), 700
nach Bearbeitung durch Prüfdämon erneut lesen, 659
`plugin` (Zeile), 642
Präfixe in Zeile `flags`, 705
Syntax überprüfen, 640
Syntaxfehler, 701
systemweite Prüfung, 615
`audit_event` (Datei)
Beschreibung, 614
Ereignisse sicher entfernen, 685
Klassenmitgliedschaft ändern, 647–648
`audit.notice` (Eintrag), `syslog.conf` (Datei), 642
Audit Review (Berechtigungsprofil), 702
`audit_startup` (Skript)
Beschreibung, 699
konfigurieren, 653–656
`audit_user` (Datei), Klassen überprüfen, 677
`audit_user` (Datenbank)
Ausnahme zu systemweiten Prüfklassen, 616
Benutzerausnahmen angeben, 644–645
Benutzerprüffelder, 699–700
Präfixe für Klassen, 705
Prozessvorauswahlmaske, 707
`audit_warn` (Skript)
`auditd` Dämonausführung, 690
Bedingungen für Aufruf, 700
Beschreibung, 700
konfigurieren, 653
Zeichenfolgen, 701
`auditconfig` (Befehl)
Beschreibung, 695
Präfixe für Klassen, 705
Prüfklassen als Argumente, 616, 703
Prüfrichtlinie einrichten, 655, 682

auditd (Dämon)
  audit_warn (Skript)
    Ausführung, 690
    Beschreibung, 700
  Datei audit_control erneut lesen, 659
  Funktionen, 690
  geladene Plugins, 690
  geordnete Prüfdateien öffnen, 697
  Informationen vom Kernel erneut lesen, 659
  Prüfpfaderstellung, 690, 707
auditlog (Datei), Prüfdatensätze im Textformat, 642
auditreduce (Befehl), 691
  Beispiele, 667–669
  Beschreibung, 691
  -c (Option), 671
  Filterungsoptionen, 669
  -O (Option), 667–669
  ohne Optionen, 692
  Optionen, 692
  Optionen in Großbuchstaben verwenden, 668
  Optionen in Kleinbuchstaben verwenden, 669
  Prüfdateien bereinigen, 673–674
  Prüfdatensätze auswählen, 669–671
  Prüfdatensätze zusammenführen, 667–669
  trailer-Token, 728
  Zeitstempel verwenden, 709
Aufheben der Zuordnung
  erzwingen, 91
  Geräte, 97
  Mikrofon, 97
Auflisten
  Benutzer ohne Passwort, 66
  Geräterichtlinie, 84–85
  Hardwareprovider, 318–319
  Inhalt des Schlüsselspeichers, 327
  kryptografische Framework-Provider, 318–319
  Provider im kryptografischen Framework, 310–312
  Rollen, die Sie annehmen können, 230, 262
  verfügbare Provider im kryptografischen Framework, 310–312
Aufwandsteuerung, und Prüfung, 633
Aufzeichnen, fehlgeschlagene
  Anmeldeversuche, 67–68
Ausführbare Stacks
  Meldungen ausgeben, 142
  Protokollierung von Meldungen deaktivieren, 157
  schützen, 141, 156–157
Ausführen von ASET (Übersicht der Schritte), 178–182
Ausführungsprotokoll (ASET), 164
Aushängen, zugeordnete Geräte, 97
Austauschen von Master- und Slave-KDCs, 484–489
Auswählen
  Ereignisse aus Prüfpfad, 669–671
  Passwort, 573–574
  Prüfdatensätze, 669–671
  Prüfklassen, 639–641
auth_attr (Datenbank)
  Beschreibung, 256–257
  Zusammenfassung, 253
AUTH_DES (Authentifizierung), *Siehe* AUTH_DH (Authentifizierung)
AUTH_DH (Authentifizierung), NFS, 335
Authentifizierer
  Kerberos, 592, 600
Authentifizierung
  auf NFS eingehängte Dateien, 346
  AUTH_DH-Client-Server-Sitzung, 337–340
  bereichsübergreifend konfigurieren, 456–458
  Beschreibung, 58–60
  DH-Authentifizierung, 336–340
  Kerberos, 407
  mit der Option -X deaktivieren, 580
  mit NFS verwenden, 335
  Naming Services, 335
  Netzwerksicherheit, 58–60
  Secure RPC, 335
  Secure Shell
    Methoden, 366–368
    Prozess, 390–391
  Terminologie, 591–592
  Typen, 58–60
  Übersicht zu Kerberos, 598
Authentifizierung mithilfe von öffentlichen Schlüsseln, Secure Shell, 366

Authentifizierungsmethoden
GSS-API-Berechtigungsnachweise in Secure Shell, 367
Hostbasiert in Secure Shell, 367, 371–373
Interaktiv mit Tastatur in Secure Shell, 367
öffentliche Schlüssel in Secure Shell, 367
Passwort in Secure Shell, 367
Secure Shell, 366–368
`authlog` (Datei), fehlgeschlagene Anmeldeversuche aufzeichnen, 68–70
`authorized_keys` (Datei), Beschreibung, 399
`AuthorizedKeysFile` (Schlüsselwort), `sshd_config` (Datei), 393
`auths` (Befehl), Beschreibung, 261
`AUTHS_GRANTED` (Schlüsselwort), `policy.conf` (Datei), 260
`auto_transition` (Option), SASL, 363
Automated Security Enhancement Tool, *Siehe* ASET
Automatische Anmeldung
aktivieren, 579
deaktivieren, 580
Automatisches Aktivieren der Prüfung, 699
Automatisieren der Erstellung von Hauptelementen, 533–534
Autorisierungen
Kerberos, 407
Typen, 58–60
Autorisierungen (RBAC)
auf Platzhalter überprüfen, 245
Befehle, die Autorisierungen erfordern, 262–263
Beschreibung, 193, 252–253
Datenbank, 253–261
Definition, 196–197
delegieren, 253
für Gerätezuordnung nicht erforderlich, 92
Gerätezuordnung, 89, 100–101
Granularität, 253
in privilegierter Anwendung prüfen, 198
Namenskonvention, 252
`solaris.device.allocate`, 89, 100
`solaris.device.revoke`, 101
`auxprop_login` (Option), SASL, 363

B

`-b` (Option), `auditreduce` (Befehl), 670
Backup
Kerberos-Datenbank, 489–490
Slave-KDCs, 429
Bandlaufwerke
Bereinigungsskripten, 104
Daten bereinigen, 104
zuordnen, 94
`Banner` (Schlüsselwort), `sshd_config` Datei, 393
BART
ausführliche Ausgabe, 129
Komponenten, 108–110
programmatische Ausgabe, 129
Sicherheitsüberlegungen, 112
Übersicht, 107–110
Übersicht der Schritte, 111
`bart` (Befehl), 107
`bart compare`-Befehl, 109
`bart create` (Befehl), 108–109, 112
Basic Audit Reporting Tool, *Siehe* BART
Basic Security Module (BSM)
Siehe Gerätezuordnung
Siehe Prüfung
Basic Solaris User (RBAC), Inhalt des Berechtigungsprofils, 250
`Batchmode` (Schlüsselwort), `ssh_config` (Datei), 393
Beenden, Signal beim Herunterfahren der Prüfung, 701
Befehle
Siehe auch einzelne Befehle
ACL-Befehle, 141
auf Berechtigungen prüfen, 198
Befehle der Gerätezuordnung, 99
Befehle für Secure RPC, 337
Befehle im kryptografischen Framework, 293
Befehle zum Schützen von Dateien, 131
die Berechtigungen zuweisen, 208
Geräterichtlinienbefehle, 98–99
Kerberos, 589–590
kryptografische Befehle auf Benutzerebene, 293–294
privilegierte Befehle des Benutzers festlegen, 277–278

Befehle *(Fortsetzung)*
Prüfung, 689–695
RBAC-Verwaltungsbefehle, 261–262
Secure Shell-Befehle, 401–403
zum Verwalten von Berechtigungen, 281
Befehlsausführung, Secure Shell, 391–392
Befehlszeilenäquivalente des SEAM-Tools, 529–530
Begrenzen
Prüfdateigröße, 686
Verwendung von Berechtigungen durch Benutzer oder Rolle, 272–274
Begrenzter Berechtigungssatz, 206
Benutzer
alle Befehle prüfen, 680–682
Anmeldestatus anzeigen, 65–66
Anmeldung deaktivieren, 67
Berechtigungen zuweisen zu, 271–272
Dateien verschlüsseln, 307–309
Digest von Dateien berechnen, 304–305
direkt zugewiesene Berechtigungen festlegen, 275–276
eigene privilegierte Befehle festlegen, 277–278
Eigenschaften ändern (RBAC), 241–243
Eigenschaften über Befehlszeile, 243
Fehlerbehebung beim Ausführen privilegierter Befehle, 277–278
Geräte zuordnen, 93–94
grundlegende Berechtigungen beschränken, 273
grundlegender Berechtigungssatz, 207
lokalen Benutzer erstellen, 226
lokalen Benutzer hinzufügen, 226
MAC von Dateien berechnen, 305–306
ohne Passwort, 66
Prüfungsvorauswahlmaske ändern, 644–645
RBAC-Standardwerte zuweisen, 260–261
symmetrischen Schlüssel erstellen, 301–304
ursprüngliche vererbbare Berechtigungen, 207
zugeordnete Geräte aushängen, 97
zugeordnete Geräte einhängen, 94–96
Zuordnung von Geräten aufheben, 97
Zuordnungsautorisierung zuweisen, 89
Benutzer-ACL-Einträge
Beschreibung, 140
einstellen, 150–151
Benutzer-ACL-Einträge *(Fortsetzung)*
Standardeinträge für Verzeichnisse, 140–141
Benutzer-Hauptelement, Beschreibung, 413
Benutzer-ID
in NFS-Services, 463–464
Prüf-ID, 609–611, 707
Benutzer-IDs (UIDs), spezielle Konten, 45
Benutzerdatenbank (RBAC), *Siehe* `user_attr`-Datenbank
Benutzerklassen von Dateien, 132
Benutzerkonten
Siehe auch Benutzer
Anmeldestatus anzeigen, 65–66
ASET-Prüfungen, 162
Benutzerprüffelder, `audit_user` (Datenbank), 699–700
Benutzerskripten, für Dämon `ssh-agent` in CDE konfigurieren, 381–382
Benutzerverfahren
ACLs verwenden, 149–154
`chkey` (Befehl), 345
Dateien entschlüsseln, 307–309
Dateien schützen, 143–149
Dateien verschlüsseln, 298
Digest einer Datei berechnen, 304–305
Geräte zuordnen, 93
MAC einer Datei berechnen, 305–306
mit dem Befehl `pktool`, 325–326
Passwortsatz für Schlüsselspeicher generieren, 330–331
privaten Schlüssel des NIS-Benutzers verschlüsseln, 345
Rolle annehmen, 215–229
Secure Shell verwenden, 375–376
selbstsigniertes Zertifikat erstellen, 326–327
symmetrischen Schlüssel generieren
mit Befehl `dd`, 298–300
mit Befehl `pktool`, 301–304
Zertifikate importieren, 327–329
zugewiesene Rolle verwenden, 215–229
Benutzervorgänge, Zertifikate exportieren, 329–330
Benutzervorgehensweisen
Rolle annehmen, 229
zugewiesene Rolle verwenden, 229

Berechnen
DH-Schlüssel, 344
Digest einer Datei, 304–305
Geheimschlüssel, 298–300, 301–304
MAC einer Datei, 305–306
Berechtigungen
Siehe Berechtigungsprofile
ACLs, 55–56
Anforderungen an die Fehlerbehebung für, 268–270
auf einem Prozess auflisten, 267–268
aus begrenztem Satz entfernen, 273
aus dem grundlegenden Satz entfernen, 273
Auswirkungen auf SEAM-Tool, 559
Befehle, 281
Befehle mit Berechtigung ausführen, 209
Behandlung bei ASET, 160
Behandlung durch ASET, 161
Benutzerklassen, 132
Berechtigungen erkennende Programme, 208
Beschreibung, 193, 203
besondere Dateiberechtigungen, 134–135, 135, 138
Dateiberechtigungen
absoluter Modus, 136, 147–148
ändern, 136–138, 146
Beschreibung, 133
besondere Berechtigungen, 135, 138
symbolischer Modus, 136, 137, 146
Dateiberechtigungen ändern
absoluter Modus, 136, 147–148
`chmod` (Befehl), 132
symbolischer Modus, 136, 137, 146
Dateien, 282–283
Dateien mit `setuid`-Berechtigungen suchen, 155
direkt zugewiesene festlegen, 275–276
einem Benutzer zuweisen, 208
Eskalation, 284
fehlende finden, 269–270
Fehlersuche, 211, 268
Geräte, 210–211
im Shell-Skript verwenden, 274
in Sätzen implementiert, 206
Kategorien, 203
Kernel-Prozesse schützen, 202
Berechtigungen *(Fortsetzung)*
`PRIV_PROC_LOCK_MEMORY`, 189, 205–206
Prozesse mit zugewiesenen Berechtigungen, 207
Prüfung, 283–284
`setgid`-Berechtigungen
absoluter Modus, 138, 149
Beschreibung, 135
symbolischer Modus, 137
`setuid`-Berechtigungen
absoluter Modus, 138, 149
Beschreibung, 134–135
Sicherheitsrisiken, 134
symbolischer Modus, 137
Standardwerte, 135–136
Sticky Bit, 135
tune-Dateien (ASET), 167, 171
Übersicht der Schritte, 265
UFS-ACLs, 138–141
`umask`-Wert, 135–136
Unterschiede zum Superuser-Modell, 204
verglichen mit Superuser-Modell, 201–211
verwalten, 266
verwenden, 275
Verwendung durch Benutzer oder Rolle begrenzen, 272–274
Verzeichnisberechtigungen, 133
von einem Benutzer entfernen, 209
von Prozessen geerbt, 207
zu Befehl hinzufügen, 270–271
zu Benutzer oder Rolle zuweisen, 271–272
zu einem Befehl zuweisen, 208
zu einem Skript zuweisen, 210
Berechtigungen ausführen, symbolischer Modus, 137
Berechtigungsnachweis
Beschreibung, 338, 592
Cache, 598
für einen Server erhalten, 600–601
für einen TGS erhalten, 599
oder Tickets, 409
Berechtigungsnachweise, zuordnen, 430
Berechtigungsprofil, über Befehlszeile ändern, 240
Berechtigungsprofile
All, 248, 251
ändern, 238–241

Berechtigungsprofile *(Fortsetzung)*
für Prüfservice, 702
Basic Solaris User, 248, 250
Berechtigungseskalation verhindern, 191
Berechtigungseskalation vermeiden, 223
Beschreibung, 193, 198–199
Beschreibung der wichtigsten Berechtigungsprofile, 247
Datenbanken
Siehe `prof_attr`- und `exec_attr`-Datenbank
erstellen
in Befehlszeile, 239
in Solaris Management Console, 240
Fehlerbehebung, 241
Inhalt ändern, 238–241
Inhalt anzeigen, 252
Inhalt typischer, 247
Methoden zur Erstellung, 238–241
Operator, 247, 249
Printer Management, 248, 250
Reihenfolge, 251–252
Rollen erstellen, 218–221
System Administrator, 247, 249
vertrauenswürdigen Benutzern zuweisen, 191, 223
Berechtigungsprüfung, in Anwendungen, 197
Berechtigungssatz, auflisten, 207
Berechtigungssätze
begrenzt, 206
Berechtigungen entfernen, 209
Berechtigungen hinzufügen, 209
effektiv, 206
grundlegend, 207
vererbbar, 206
zugelassen, 206
Berechtigungstabelle, einzelnen Eintrag hinzufügen, 464–465
Berechtigungstool, Beschreibung, 238–241
Bereich (RBAC), Beschreibung, 200
Bereiche (Kerberos)
Anzahl, 426–427
bereichsübergreifende Authentifizierung, 456–458
direkt, 457–458
Hauptelementnamen, 413
Hierarchie, 427
Bereiche (Kerberos) *(Fortsetzung)*
hierarchisch, 456–457
hierarchisch oder nicht hierarchisch, 413–414
Hostnamen zuordnen, 427–428
Inhalt, 414
Konfigurationsentscheidungen, 426–427
Namen, 426
Server, 414
Tickets für einen bestimmten anfordern, 580
Bereichsübergreifende Authentifizierung, konfigurieren, 456–458
Bereinigen, binäre Prüfdateien, 673–674
Bereinigungsskripten
Audiogeräte, 105
Bandlaufwerke, 104
Beschreibung, 104–105
CD-ROM-Laufwerke, 105
Diskettenlaufwerke, 105
neue Skripten erstellen, 105
Objektwiederverwendung, 104–105
Optionen, 105
Berichte
ASET, 166, 167, 173
BART, 107
vergleichen (ASET), 167
Verzeichnis (ASET), 166
Berichterstellungs-Tool, *Siehe* `bart compare`
Beschränken
Benutzerberechtigungen, 273
Superuser (Übersicht der Schritte), 77
Superuser-Zugriff über Remote-Systeme, 78–80
Beschränken des Zugriffs auf KDC-Server, 506–507
Besondere Berechtigungen
`setgid`-Berechtigungen, 135
`setuid`-Berechtigungen, 134–135
Sticky Bit, 135
Bibliotheken, Provider auf Benutzerebene, 310
`BindAddress` (Schlüsselwort), `ssh_config` (Datei), 393
binding (Steuer-Flag), PAM, 355
Blowfish (Verschlüsselungsalgorithmus)
für Passwörter verwenden, 74
`Blowfish` (Verschlüsselungsalgorithmus), Kernel-Provider, 310

Blowfish (Verschlüsselungsalgorithmus)
policy.conf (Datei), 74
ssh_config (Datei), 393
blowfish-cbc (Verschlüsselungsalgorithmus),
ssh_config (Datei), 393
Bourne-Shell, privilegierte Version, 200
bsmconv (Skript)
Beschreibung, 701
Datei device_maps erstellen, 101–102
Prüfservice aktivieren, 656–657
bsmrecord (Befehl)
[] (eckige Klammern) in Ausgabe, 710
alle Formate auflisten, 665
Beispiel, 666
Beschreibung, 691
Formate der Klasse auflisten, 666–667
Formate eines Programms auflisten, 666
optionale Token ([]), 710
Prüfdatensatzformate anzeigen, 665–667
bsmunconv (Skript), Prüfservice deaktivieren, 658–659

C

-C (Option), auditreduce (Befehl), 668
C-Shell, privilegierte Version, 200
-c (Option)
auditreduce (Befehl), 670, 671
bsmrecord (Befehl), 666–667
c2audit (Modul), Laden überprüfen, 676
c2audit:audit_load (Eintrag), system (Datei), 696
Cache, Berechtigungsnachweis, 598
canon_user_plugin (Option), SASL, 363
Caret (^) in Prüfklassenpräfixen, 705
CD-ROM-Laufwerke
Sicherheit, 105
zuordnen, 96
cdrw (Befehl), Autorisierungen erforderlich, 263
ChallengeResponseAuthentication (Schlüsselwort),
Siehe KbdInteractiveAuthentication
(Schlüsselwort)
changepw (Hauptelement), 561
CheckHostIP (Schlüsselwort), ssh_config (Datei), 393
chgrp (Befehl)
Beschreibung, 132
chgrp (Befehl) *(Fortsetzung)*
Syntax, 145
chkey (Befehl), 337, 345
chmod (Befehl)
Beschreibung, 132
besondere Berechtigungen ändern, 149
besondere Dateiberechtigungen, 148–149
Syntax, 148
chown (Befehl), Beschreibung, 132
ChrootDirectory (Schlüsselwort), ssh_config
(Datei), 393
Cipher (Schlüsselwort), ssh_config (Datei), 393
Ciphers (Schlüsselwort), Secure Shell, 393
cklist.rpt (Datei), 162, 166
CKLISTPATH_level (Variable bei ASET), 176
Clear (Schutzebene), 581
ClearAllForwardings (Schlüsselwort), Secure
Shell-Port-Weiterleitung, 393
ClientAliveCountMax (Schlüsselwort), ssh_config
(Datei), 393
ClientAliveInterval (Schlüsselwort), ssh_config
(Datei), 393
Clientnamen, in Kerberos planen, 428
Clients
AUTH_DH-Client-Server-Sitzung, 337–340
Definition in Kerberos, 591
für Secure Shell konfigurieren, 390, 392
Kerberos konfigurieren, 468–482
clntconfig-Hauptelement
erstellen, 442, 450
cmd (Prüf-Token), 622, 715
cnt (Prüfrichtlinie), Beschreibung, 630
Compression (Schlüsselwort), Secure Shell, 393
CompressionLevel (Schlüsselwort), ssh_config
(Datei), 393
Computer Emergency Response Team/Coordination
Center (CERT/CC), 62
Computersicherheit, *Siehe* Systemsicherheit
ConnectionAttempts (Schlüsselwort), ssh_config
(Datei), 393
CONSOLE in Secure Shell, 397
crammd5.so.1 (Plugin), SASL, 362
cred (Datenbank)
Benutzerberechtigungsnachweis hinzufügen, 343

cred (Datenbank) *(Fortsetzung)*
DH-Authentifizierung, 336–340
cred (Tabelle)
DH-Authentifizierung, 337
durch Server gespeicherte Informationen, 339
cred Datenbank, Clientberechtigungsnachweis hinzufügen, 342
crontab (Dateien)
ASET regelmäßig ausführen, 160
Autorisierungen erforderlich, 263
regelmäßige Ausführung von ASET anhalten, 180–181
crypt (Befehl), Dateisicherheit, 55
CRYPT_ALGORITHMS_ALLOW (Schlüsselwort), policy.conf (Datei), 44
CRYPT_ALGORITHMS_DEPRECATE (Schlüsselwort), policy.conf (Datei), 44
crypt_bsdbf (Passwortalgorithmus), 43
crypt_bsdmd5 (Passwortalgorithmus), 43
crypt.conf (Datei)
mit neuem Passwortmodul ändern, 76–77
Passwortmodule anderer Anbieter, 76–77
CRYPT_DEFAULT (Schlüsselwort), policy.conf (Datei), 44
CRYPT_DEFAULT (Systemvariable), 73
crypt_sha256 (Passwortalgorithmus), 43
crypt_sunmd5 (Passwortalgorithmus), 43
crypt_unix (Passwortalgorithmus), 43, 73–77
Crypto Management (RBAC)
Berechtigungsprofil verwenden, 314, 316
Rolle erstellen, 225
cryptoadm (Befehl)
Beschreibung, 292
Hardwaremechanismen deaktivieren, 319–321
Kernel-Softwareprovider wiederherstellen, 317
kryptografische Mechanismen, 314
kryptografische Mechanismen verwenden, 316
-m (Option), 315, 316
-p (Option), 315, 316
PKCS #11-Bibliothek installieren, 314
Provider auflisten, 310
cryptoadm install (Befehl), PKCS #11-Bibliothek installieren, 314
Cryptoki, *Siehe* PKCS #11-Bibliothek
csh (Befehl), privilegierte Version, 200
.cshrc (Datei), Pfadvariableneintrag, 51
Custom Operator (RBAC), Rolle erstellen, 223–224

D

-D (Option)
auditreduce (Befehl), 669
ppriv (Befehl), 268
d_passwd (Datei)
Beschreibung, 46
Einwahl-Anmeldungen vorübergehend deaktivieren, 72
erstellen, 71
-d (Option)
auditreduce (Befehl), 671
getfacl (Befehl), 154
praudit (Befehl), 693
setfacl (Befehl), 153
Dämonen
auditd, 690
kcfd, 293
keyserv, 341
mit Berechtigungen ausführen, 204
nscd (Name Service-Cache-Dämon), 218, 261
rpc.nispasswd, 75
ssh-agent, 380–381
sshd, 389–392
Tabelle von Kerberos, 590
vold, 89
Data Encryption Standard, *Siehe* DES-Verschlüsselung
Datei-vnode-Prüf-Token, 714
Dateiberechtigungsmodi, absoluter Modus, 136
Dateiberechtigungsmodus, symbolischer Modus, 137
Dateien
ACL ändern, 152–153
ACL einstellen, 150–151
ACL-Einträge
anzeigen, 141, 153–154
einstellen, 150–151
gültige Einträge, 140
hinzufügen oder ändern, 152–153
löschen, 141, 153
prüfen, 149–150

Dateien *(Fortsetzung)*
ACL-Einträge anzeigen, 153–154
ACL-Einträge kopieren, 152
ACL feststellen, 149–150
ACL löschen, 153
ASET-Prüfungen, 162
BART-Manifeste, 125–126
Berechtigungen
absoluter Modus, 136, 147–148
ändern, 132, 136–138, 146
Beschreibung, 133
`setgid`, 135
`setuid`, 134–135
Standardwerte, 135–136
Sticky Bit, 135
symbolischer Modus, 136, 137, 146
`umask`-Wert, 135–136
Berechtigungen mit Bezug auf, 203
besondere Dateiberechtigungen ändern, 148–149
besondere Dateien, 134–135
Dateien mit `setuid`-Berechtigungen suchen, 155
Dateiinformationen, 143–144
Dateitypen, 132
Digest, 304–305
Digest berechnen, 304–305
Digests berechnen, 304–305
Eigentümerschaft
`setgid`-Berechtigung, 135
`setuid`-Berechtigung, 134–135
Eigentümerschaft ändern, 132, 144–145
entschlüsseln, 307–308
Gruppeneigentümerschaft ändern, 145–146
Hashing, 298
Informationen anzeigen, 132
Integrität mit `digest` überprüfen, 304–305
`kdc.conf`, 595
Kerberos, 587–589
MAC berechnen, 305–306
Manifeste (BART), 125–126
mit ACLs schützen, 149–154
mit Berechtigungsinformationen, 282–283
mit DH-Authentifizierung einhängen, 346
mit DH-Authentifizierung gemeinsam nutzen, 346
mit Secure Shell kopieren, 384–385
Dateien *(Fortsetzung)*
mit UNIX-Berechtigungen schützen, 143–149
öffentliche Objekte, 614
PKCS #12, 330
Prüfungsänderungen, 683
Sicherheit
ACL, 55–56
Benutzerklassen, 132
Berechtigungen ändern, 136–138, 146
besondere Dateiberechtigungen, 138
Dateiberechtigungen, 133
Dateiinformationen anzeigen, 132, 143–144
Dateitypen, 132
Eigentümerschaft ändern, 144–145
`umask`-Standardwerte, 135–136
UNIX-Berechtigungen, 131–138
Verschlüsselung, 55, 298
Verzeichnisberechtigungen, 133
Zugriffsbeschränkung, 52
Zugriffsbeschränkungen, 52
Symbole für Dateitypen, 132
`syslog.conf` (Datei), 696
verborgene Dateien anzeigen, 143
verschlüsseln, 298, 307–309
zum Verwalten von Secure Shell, 399
Dateisysteme
Dateien gemeinsam nutzen, 56
NFS, 335
Sicherheit
Authentifizierung und NFS, 335
TMPFS-Dateisystem, 135
TMPFS, 135
Dateiübertragungen, Prüfung, 687–688
Datenbanken
`audit_user`, 699–700
`auth_attr`, 256–257
Backup und Weitergabe von KDC, 489–490
`cred` für Secure RPC, 337, 342
`exec_attr`, 259–260
geheime Schlüssel bei NFS, 337
KDC erstellen, 439
KDC-Weitergabe, 431
mit Berechtigungsinformationen, 282–283
`prof_attr`, 258–259

Datenbanken *(Fortsetzung)*
publickey für Secure RPC, 337
RBAC, 253–261
user_attr, 255–256
Datenweiterleitung, Secure Shell, 391–392
dd (Befehl), Geheimschlüssel generieren, 298–300
Deaktivieren
Abbruch-Sequenz, 81–82
Abbruch über Tastatur, 81–82
Anmeldungen, vorübergehend, 67
ausführbare Dateien mit Sicherheitsrisiken, 141–142
ausführbare Stacks, 156–157
ausführbare Stacks für Programme, 156–157
Benutzeranmeldungen, 67
Einwahl-Anmeldungen, 72
Einwahl-Anmeldungen, vorübergehend, 72
Gerätezuordnung, 658
Hardwaremechanismen, 319–321
Herunterfahren über Tastatur, 81–82
kryptografische Mechanismen, 314
Protokollierung ausführbarer Stack-Meldungen, 157
Prüfrichtlinie, 653–656
Prüfservice, 658–659
root-Zugriff über Remote-Systeme, 78–80
Sequenz zum Herunterfahren des Systems, 81–82
Service auf einem Host (Kerberos), 565–567
deallocate (Befehl)
Autorisierungen, 101
Autorisierungen erforderlich, 263
Bereinigungsskripten, 105
Beschreibung, 100
verwenden, 97
Zuweisungsfehlerstatus, 101
decrypt (Befehl)
Beschreibung, 294
Syntax, 307–308
default/login (Datei), Beschreibung, 399
default_realm (Abschnitt)
krb5.conf (Datei), 439, 446
defaultpriv (Schlüsselwort), user_attr (Datenbank), 283
Deinstallieren, kryptografische Provider, 316
Delegieren, RBAC-Autorisierungen, 253
delete_entry (Befehl), ktutil (Befehl), 566
DenyGroups (Schlüsselwort), sshd_config (Datei), 393
DenyUsers (Schlüsselwort), sshd_config (Datei), 393
DES (Verschlüsselung), Kernel-Provider, 310
DES-Verschlüsselung, Secure NFS, 336
/dev/arp (Gerät), IP MIB-II-Informationen abrufen, 86–87
/dev/urandom (Gerät), 298–300
devfsadm (Befehl), Beschreibung, 98
device_allocate (Datei)
Beispiel, 91, 102
Beschreibung, 102–104
Format, 103
device_maps (Datei)
Beispieleinträge, 101
Beschreibung, 101
Format, 101
Device Security (RBAC), Rolle erstellen, 219
dfstab (Datei)
Dateien gemeinsam nutzen, 56
Sicherheitsmodi, 467
DH-Authentifizierung
Beschreibung, 336–340
Dateien einhängen, 346
Dateien gemeinsam nutzen, 346
für NIS+-Client, 342
für NIS-Client, 344
in NIS+ konfigurieren, 342–343
in NIS konfigurieren, 344
DHCP Management (RBAC), Rolle erstellen, 220
Dialogschlüssel
in Secure RPC generieren, 338
mit Secure RPC entschlüsseln, 339
dialups (Datei), erstellen, 71
Diffie-Hellman-Authentifizierung, *Siehe* DH-Authentifizierung
digest (Befehl)
Beispiel, 304
Beschreibung, 293
Syntax, 304
digestmd5.so.1 (Plugin), SASL, 362
Digests
Dateien, 304

Digests *(Fortsetzung)*
für Datei berechnen, 304–305
von Dateien, 304–305
`dir` (Zeile), `audit_control` (Datei), 697
Direkte Bereiche, 457–458
Diskettenlaufwerke
Bereinigungsskripten, 105
zuordnen, 95–96
`dminfo` (Befehl), 101
DNS, Kerberos, 428
`domain_realm` (Abschnitt)
`krb5.conf` (Datei), 439, 446
`krb5.conf`(Datei), 427–428
Doppeltes Dollarzeichen ($$), Nummer des übergeordneten Shell-Prozesses, 267
Drucken, Prüfprotokoll, 672
Druckformatfeld, `arbitrary` (Token), 713
`DSAAuthentication` (Schlüsselwort), *Siehe* `PubkeyAuthentication` (Schlüsselwort)
DTD für Befehl `praudit`, 694
`.dtprofile` (Skript), in Secure Shell verwenden, 381–382
Duplizieren, Hauptelemente (Kerberos), 541
`DynamicForward` (Schlüsselwort), `ssh_config` (Datei), 393

E

`-e` (Option)
`auditreduce` (Befehl), 671
`ppriv` (Befehl), 268
`ebusy` (Zeichenfolge), `audit_warn` (Skript), 701
Eckige Klammern (`[]`), `bsmrecord` (Ausgabe), 710
`eeprom` (Befehl), 41, 80–82
`eeprom.rpt` (Datei), 163, 166
Effektiver Berechtigungssatz, 206
Effizienz, Prüfung, 635
Eigentümerschaft für Dateien
ändern, 144–145
Gruppeneigentümerschaft ändern, 145–146
UFS-ACLs, 138–141
Eigentümerschaft von Dateien
ACLs, 55–56
ändern, 132
Eingeschränkte Shell (`rsh`), 51
Einhängen
Dateien mit DH-Authentifizierung, 346
Prüfverzeichnisse, 708
zugeordnete Geräte, 94–96
zugeordnetes CD-ROM-Laufwerk, 96
zugeordnetes Diskettenlaufwerk, 95–96
Einrichten
`arge` (Richtlinie), 682
`argv` (Richtlinie), 682
Prüfrichtlinie, 653–656
Standardwerte für Hauptelemente (Kerberos), 543–544
Einwahl-Passwörter
deaktivieren, 47
erstellen, 70–72
`/etc/d_passwd` (Datei), 47
Sicherheit, 46–47
vorübergehend deaktivieren, 72
`eject` (Befehl), Gerätebereinigung, 105
Elementgrößenfeld, `arbitrary` (Token), 713
`elfsign` (Befehl)
Beschreibung, 293, 294
`encrypt` (Befehl)
Beschreibung, 294
Fehlerbehebung, 309
Fehlermeldungen, 309
Syntax, 299
Ende, Signal beim Herunterfahren der Prüfung, 701
Entfernen
ACL-Einträge, 153
Berechtigungen aus begrenztem Satz, 273
Berechtigungen aus dem grundlegenden Satz, 273
Geräterichtlinie, 86
Hauptelemente mit dem Befehl `ktremove`, 564
kryptografische Provider, 316
Prüfereignisse von Datei `audit_event`, 685
Richtlinie von Gerät, 86
Service-Hauptelement aus Schlüsseltabellendatei, 564
Softwareprovider
dauerhaft, 318
vorübergehend, 317

Entschlüsseln
Dateien, 307–308
Dialogschlüssel für Secure RPC, 339
geheime Schlüssel, 337–338
geheime Schlüssel bei NFS, 337
env.rpt (Datei), 163, 166
Ereignis, Beschreibung, 614
Ereignismodifikatorfeld-Flags (Token header), 718
Erfolg
Prüfklassen deaktivieren, 705
Prüfklassenpräfix, 704
Erhalten
Berechtigungen, 207, 208, 271–272
Berechtigungen auf einem Prozess, 267–268
Berechtigungsnachweis für einen Server, 600–601
Berechtigungsnachweis für einen TGS, 599
privilegierte Befehle, 236–238
Zugriff auf einen bestimmten Service, 601–602
Erneuerbares Ticket, Definition, 594
Ersetzen, Superuser durch Rollen, 215–217
Erstellen
angepasste Rolle, 223–224
Berechtigungsnachweistabelle, 463–464
Berechtigungsprofile, 238–241
Berechtigungsprofile mit Solaris Management Console, 240
d_passwd (Datei), 71
Datei-Digests, 304–305
Einwahl-Passwörter, 70–72
/etc/d_passwd (Datei), 71
Geheimschlüssel
für Verschlüsselung, 298–300, 301–304
lokaler Benutzer, 226
neue Bereinigungsskripten, 105
neue Richtlinie (Kerberos), 538, 551–552
neues Hauptelement (Kerberos), 538–540
Operator (Rolle), 219
Partitionen für binäre Prüfdateien, 649–653
Passwörter für vorübergehende Benutzer, 71
Prüfpfad
auditd (Dämon), 707
Funktion des Dämons auditd, 690
Rollen
für bestimmte Profile, 218–221
Erstellen, Rollen *(Fortsetzung)*
mit beschränktem Bereich, 220
über Befehlszeile, 221–224
root-Benutzer als Rolle, 226–229
Schlüsseltabellendatei, 440, 448
Secure Shell-Schlüssel, 376–378
sicherheitsbezogene Rollen, 219–220
Stash-Datei, 455, 499
System Administrator (Rolle), 219
Tickets mit kinit, 570–571
Erzwungene Bereinigung, st_clean (Skript), 105
EscapeChar (Schlüsselwort), ssh_config (Datei), 393
/etc/d_passwd (Datei)
erstellen, 71
Einwahl-Anmeldungen vorübergehend deaktivieren, 72
/etc/passwd (Datei), 46
/etc/default/kbd (Datei), 81–82
/etc/default/login (Datei)
Beschreibung, 399
root-Zugriff über Remote-Systeme beschränken, 78–80
Secure Shell, 397
Standardeinstellungen für die Anmeldung, 69
/etc/default/su (Datei)
Versuche mit dem Befehl su anzeigen, 78–80
Verwendung des Befehls su überwachen, 78
Zugriffsversuche überwachen, 78–80
/etc/dfs/dfstab (Datei)
Dateien gemeinsam nutzen, 56
Sicherheitsmodi, 467
/etc/dialups (Datei), erstellen, 71
/etc/group (Datei), ASET-Prüfungen, 162
/etc/hosts.equiv (Datei), Beschreibung, 400
/etc/krb5/kadm5.acl (Datei), Beschreibung, 588
/etc/krb5/kadm5.keytab (Datei), Beschreibung, 588
/etc/krb5/kdc.conf (Datei), Beschreibung, 588
/etc/krb5/kpropd.acl (Datei), Beschreibung, 588
/etc/krb5/krb5.conf (Datei), Beschreibung, 588
/etc/krb5/krb5.keytab (Datei), Beschreibung, 588
/etc/krb5/warn.conf (Datei), Beschreibung, 588
/etc/logindevperm (Datei), 46

/etc/nologin (Datei)
  Benutzeranmeldungen vorübergehend deaktivieren, 67
  Beschreibung, 399
/etc/nsswitch.conf (Datei), 41
/etc/pam.conf (Datei), Kerberos, 588
/etc/passwd (Datei), ASET-Prüfungen, 162
/etc/publickey (Datei), DH-Authentifizierung, 337
/etc/security/audit_event (Datei), Prüfereignisse und, 614
/etc/security/audit_startup (Datei), 699
/etc/security/audit_warn (Skript), 700
/etc/security/bsmconv (Skript), 101–102
  Beschreibung, 701
/etc/security/crypt.conf (Datei)
  mit neuem Passwortmodul ändern, 76–77
  Passwortmodule anderer Anbieter, 76–77
/etc/security/device_allocate (Datei), 102
/etc/security/device_maps (Datei), 101
/etc/security/policy.conf (Datei), Algorithmuskonfiguration, 73–74
/etc/ssh_host_dsa_key.pub (Datei), Beschreibung, 399
/etc/ssh_host_key.pub (Datei), Beschreibung, 399
/etc/ssh_host_rsa_key.pub (Datei), Beschreibung, 399
/etc/ssh/shosts.equiv (Datei), Beschreibung, 400
/etc/ssh/ssh_config (Datei)
  (Beschreibung), 400
  Hostspezifische Parameter, 396
  Schlüsselwörter, 393–397
  Secure Shell konfigurieren, 392
  Überschreibung, 400
/etc/ssh/ssh_host_dsa_key (Datei), Beschreibung, 399
/etc/ssh/ssh_host_key (Datei)
  Beschreibung, 399
  Überschreibung, 400
/etc/ssh/ssh_host_rsa_key (Datei), Beschreibung, 399
/etc/ssh/ssh_known_hosts (Datei)
  Beschreibung, 399
  Distribution steuern, 398
  sichere Distribution, 398
/etc/ssh/ssh_known_hosts (Datei) *(Fortsetzung)*
  Überschreibung, 401
/etc/ssh/sshd_config (Datei)
  Beschreibung, 399
  Schlüsselwörter, 393–397
/etc/ssh/sshrc (Datei), Beschreibung, 400
/etc/syslog.conf (Datei)
  fehlgeschlagene Anmeldungen, 68–70
  PAM, 353
  Prüfung, 642, 696
/etc/syslog.conf Datei, ausführbare Stack-Meldungen, 142
/etc/system (Datei), 696
exec (Prüfklasse), 704
exec_args (Prüf-Token)
  argv (Richtlinie), 715–716
  Format, 715–716
exec_attr (Datenbank)
  Beschreibung, 259–260
  Zusammenfassung, 253
exec_env (Prüf-Token), Format, 716
exit (Prüf-Token), Format, 716
export (Unterbefehl), pktool (Befehl), 329–330
EXTERNAL (Plugin für Sicherheitsmechanismus), SASL, 362

F

-f (Option)
  kerberisierte Befehle, 579, 581–582
  setfacl (Befehl), 152
  st_clean (Skript), 105
-F (Option)
  deallocate (Befehl), 101
  kerberisierte Befehle, 580, 581–582
FallBackToRsh (Schlüsselwort), ssh_config (Datei), 394
fd_clean (Skript), Beschreibung, 105
Fehler
  interne Fehler, 701
  Prüfklassen deaktivieren, 705
  Prüfklassenpräfix, 704
  Prüfverzeichnisse voll, 690, 701
  Zuweisungsfehlerstatus, 101

Fehlerbehebung
  Anmeldung als Superuser, 229
  ASET-Fehler, 182
  Benutzer der ausgeführten privilegierten Befehle, 277–278
  Berechtigungsanforderungen, 268–270
  Berechtigungsprofile, 241
  Dateien mit `setuid`-Berechtigungen suchen, 155
  Einbruchsversuche auf Computern, 67–68
  `encrypt` (Befehl), 309
  fehlende Berechtigung, 268–270
  Gerät einhängen, 96
  Gerät zuordnen, 94
  Kerberos, 523
  `list_devices` (Befehl), 90
  `praudit` (Befehl), 673
  Programme an der Verwendung ausführbarer Stacks hindern, 156–157
  Prüfklassen
    angepasst, 646, 678
  Prüfung, 675–688
  Remote-Zugriff für Superuser, 79
  Rollenfähigkeiten, 220
  `root` als Rolle, 229
  Terminal zur Eingabe des Befehls `su`, 78
Fehlermeldungen
  `encrypt` (Befehl), 309
  Kerberos, 509–522
  mit `kpasswd`, 575
Fehlersuche, Berechtigungen, 268
Fehlersuche der Sequenznummer, 725
Fehlgeschlagene Anmeldeversuche
  `loginlog` (Datei), 67–68
  `syslog.conf` (Datei), 68–70
Fensterbereiche, Tabelle des SEAM-Tools, 555–558
Fensterverifikator, 339
Festlegen
  Berechtigungen auf einem Prozess, 267–268
  Übersicht der Schritte für Berechtigungen, 275
Festplatte, Speicherplatzanforderungen für Prüfung, 634–635
Feststellen
  ACL für Datei, 149–150
  Dateien mit `setuid`-Berechtigungen, 155
Feststellen *(Fortsetzung)*
  Modul `c2audit` geladen, 676
  Prüf-ID eines Benutzers, 684
  Prüfung wird ausgeführt, 676–678
  Richtigkeit der `audit_control`-Flags, 677
  Richtigkeit der `audit_user`-Flags, 677
`FILE` (Berechtigungen), 203
`file` (Prüf-Token), Format, 716–717
`file_attr_acc` (Prüfklasse), 703
`file_attr_mod` (Prüfklasse), 703
`file_close` (Prüfklasse), 704
`file_creation` (Prüfklasse), 703
`file_deletion` (Prüfklasse), 703
`file_read` (Prüfklasse), 703
`file_write` (Prüfklasse), 703
`find` (Befehl), Dateien mit `setuid`-Berechtigungen suchen, 155
`firewall.rpt` (Datei), 164, 166
Firewall-Systeme
  Paketübertragungen, 61
  Paketzerstörung, 61
  sichere Hostverbindungen, 385
  Sicherheit, 60–61
  Verbindung von externem Host herstellen, 386–387
  Verbindungen zu externem Host mit Secure Shell herstellen
    Konfigurationsdatei, 385–387
    über Befehlszeile, 386–387
  vertrauenswürdige Hosts, 61
Firewallsysteme, ASET-Konfiguration, 163
`flags` (Zeile)
  `audit_control` (Datei), 697
  Prozessvorauswahlmaske, 707
Format der Prüfdatensätze, `bsmrecord` (Befehl), 666
`ForwardAgent` (Schlüsselwort), von Secure Shell weitergeleitete Authentifizierung, 394
`ForwardX11` (Schlüsselwort), Secure Shell-Port-Weiterleitung, 394
FQDN (Fully Qualified Domain Name), in Kerberos, 428
Fragezeichen (?), in tune-Dateien bei ASET, 177
`ftp` (Befehl)
  Dateiübertragungen protokollieren, 687–688
  Kerberos, 579–581, 589

ftp (Befehl) *(Fortsetzung)*
Schutzebene festlegen in, 581
ftpd (Dämon), Kerberos, 590

G

GatewayPorts (Schlüsselwort), Secure Shell, 394
Gateways, *Siehe* Firewallsysteme
Geheime Schlüssel, für Secure RPC generieren, 337
Geheimschlüssel
erstellen, 298–300, 301–304
generieren
mit Befehl dd, 298–300
mit Befehl pktool, 301–304
Gemeinsame Nutzung von Dateien, mit DH-Authentifizierung, 346
Gemeinsames Nutzen von Dateien, Netzwerksicherheit, 56
gencert (Unterbefehl), pktool (Befehl), 326–327
Generic Security Service API, *Siehe* GSS-API
Generieren
geheime Schlüssel bei NFS, 337
Passwortsätzepktool (Befehl), 330–331
Schlüssel für Secure Shell, 376–378
Secure Shell-Schlüssel, 376–378
symmetrischer Schlüssel
mit Befehl dd, 298–300
mit Befehl pktool, 301–304
Zertifikate mit dem Befehl pktool, 326–327
Zufallszahl
mit Befehl dd, 298–300
mit Befehl pktool, 301–304
Geräte
Anmeldezugriffssteuerung, 46
Aufheben der Zuordnung erzwingen, 91
auflisten, 84–85
Autorisierung für Verwendung nicht erforderlich, 92
Benutzer für Zuordnung autorisieren, 89
Berechtigungsmodell, 210–211
/dev/urandom (Gerät), 298–300
durch Gerätezuordnung schützen, 47
Gerätenamen auflisten, 90
Geräterichtlinie ändern, 85–86
Geräte *(Fortsetzung)*
Geräterichtlinie anzeigen, 84–85
Geräterichtlinie hinzufügen, 85–86
Gerätezuordnung
Siehe Gerätezuordnung
im Kernel schützen, 47
IP MIB-II-Informationen abrufen, 86–87
Richtlinie entfernen, 86
Richtlinienänderungen prüfen, 86
Richtlinienbefehle, 98–99
Sicherheit, 47–49
Superuser-Modell, 210–211
verwalten, 84
Verwendung aller verhindern, 92
Verwendung einiger verhindern, 92
Verwendung zuordnen, 93
Zonen, 48
zugeordnete Geräte aushängen, 97
zugeordnete Geräte einhängen, 94–96
Zuordenbarkeit ändern, 91–92
Zuordnung aktivieren, 88–89
Zuordnung eines Geräts aufheben, 97
Zuordnung erzwingen, 90–91
Zuordnung prüfen, 92–93
Zuordnung verwalten, 87–88
Zuordnungsinformationen anzeigen, 90
Geräterichtlinie
add_drv (Befehl), 98
ändern, 85–86
Änderungen prüfen, 86
anzeigen, 84–85
Befehle, 98
Geräte verwalten, 84
Kernel-Schutz, 98–105
konfigurieren, 84–87
Übersicht, 47–49
Übersicht der Schritte, 84
update_drv (Befehl), 85–86, 98
von Gerät entfernen, 86
Geräteverwaltung, *Siehe* Geräterichtlinie
Gerätezuordnung
aktivieren, 88–89
allocate (Befehl), 100
Aufheben der Gerätezuordnung erzwingen, 91

Gerätezuordnung *(Fortsetzung)*
Autorisierung erfordern, 91–92
Autorisierung nicht erforderlich, 92
Autorisierungen für Befehle, 100–101
Befehl `allocate` verwenden, 93–94
Befehle, 99
Beispiele, 94
Benutzer für Zuordnung autorisieren, 89
Benutzerverfahren, 93
Bereinigungsskripten
Audiogeräte, 105
Bandlaufwerke, 104
Beschreibung, 104–105
CD-ROM-Laufwerke, 105
Diskettenlaufwerke, 105
neue Skripten erstellen, 105
Optionen, 105
deaktivieren, 658
`deallocate` (Befehl), 100
Bereinigungsskripten, 105
verwenden, 97
`device_allocate` (Datei), 102–104
`device_maps` (Datei), 101–102
Fehlerbehebung, 94, 96
Fehlerbehebung von Berechtigungen, 90
für Gerät aktivieren, 88–89
Geräte einhängen, 94–96
Geräte hinzufügen, 87–88
Geräte verwalten, 87–88
Geräte zuordnen, 93–94
Gerätezuordnung aufheben, 97
Gerätezuordnung erzwingen, 90–91
Informationen anzeigen, 90
Komponenten des Mechanismus, 99
Konfigurationsdatei, 101
Prüfung, 92–93
Übersicht der Schritte, 87–88
verhindern, 92
verwenden, 93
zugeordnete Geräte aushängen, 97
zuordenbare Geräte, 104
zuordenbare Geräte ändern, 91–92
Zuweisungsfehlerstatus, 101
Geringste Berechtigung, Prinzip, 203
`getdevpolicy` (Befehl), Beschreibung, 98
`getfacl` (Befehl)
`-a` (Option), 153
ACL-Einträge überprüfen, 151
Beispiele, 153–154
Beschreibung, 141
`-d` (Option), 154
`getfacl` (Beispiel), ACL-Einträge anzeigen, 153–154
Gewähren von Zugriff auf Ihr Konto, 576–578
`gkadmin` (Befehl)
Siehe auch SEAM-Tool
Beschreibung, 589
`.gkadmin` (Datei)
Beschreibung, 587
SEAM-Tool, 530
Gleichheitszeichen (=),
Dateiberechtigungssymbol, 137
`GlobalKnownHostsFile` (Schlüsselwort)
Siehe `GlobalKnownHostsFile` (Schlüsselwort)
`ssh_config` (Datei), 394
Größe der Prüfdateien
Speicherplatzanforderungen verringern, 635
verringern, 667–669, 691
`group` (Prüf-Token), durch Token `groups` ersetzt, 717
`group` (Prüfrichtlinie)
Beschreibung, 630
und Token `groups`, 630, 717
`groups` (Prüf-Token), 717
Grundlegender Berechtigungssatz, 207
Gruppen, Dateieigentümerschaft ändern, 145–146
Gruppen-ACL-Einträge
Beschreibung, 140
einstellen, 150–151
Standardeinträge für Verzeichnisse, 140–141
GSS-API
Authentifizierung bei Secure Shell, 366
Berechtigungsnachweise in Secure RPC, 342–343
Berechtigungsnachweise in Secure Shell, 391
Kerberos, 408, 423
`gssapi.so.1` (Plugin), SASL, 362
`GSSAPIAuthentication` (Schlüsselwort), Secure Shell, 394
`GSSAPIDelegateCredentials` (Schlüsselwort), `ssh_config` (Datei), 394

GSSAPIKeyExchange (Schlüsselwort), Secure Shell, 394
GSSAPIStoreDelegatedCredentials (Schlüsselwort), sshd_config (Datei), 394
gsscred (Befehl), Beschreibung, 589
gsscred (Tabelle), verwenden, 604–605
gssd (Dämon), Kerberos, 590

H

-h (Option), bsmrecord (Befehl), 666
hard (Zeichenfolge), audit_warn (Skript), 701
Hardware
  angeschlossene Hardwarebeschleuniger auflisten, 318–319
  Passwort für Zugriff anfordern, 80–81
  schützen, 40–41, 80–82
Hardwareprovider
  auflisten, 318–319
  kryptografische Mechanismen deaktivieren, 319–321
  laden, 318
  Mechanismen und Funktionen aktivieren, 320
Hash
  Algorithmen
    Kerberos, 433–434
Hashing, Dateien, 298
Hauptbenutzer, Vergleich von Benutzer-IDs, 463–464
Hauptelement
  Admin-Hauptelemente hinzufügen, 440, 448
  ändern, 542–543
  Attribute anzeigen, 536–538
  aus Schlüsseltabellendatei entfernen, 564
  Benutzer-Hauptelement, 413
  clntconfig erstellen, 442
  duplizieren, 541
  erstellen, 538–540
  erstellen clntconfig, 450
  Erstellung automatisieren, 533–534
  Hauptelementname, 413
  host erstellen, 442, 450
  Kerberos, 413
  Liste anzeigen, 534–536
  löschen, 543
  SEAM-Tool-Fensterbereiche, 555–558
Hauptelement *(Fortsetzung)*
  Service-Hauptelement, 413
  Service-Hauptelement aus Schlüsseltabelle entfernen, 564
  Service-Hauptelement zu Schlüsseltabelle hinzufügen, 560
  Service-Hauptelement zum Schlüsseltabelle hinzufügen, 562–563
  Standardwerte einrichten, 543–544
  Teilliste von Hauptelementen anzeigen, 535
  Übersicht der Schritte für die Verwaltung, 532–533
  verwalten, 527–567
Hauptelemente, ändern, 553–554
header (Prüf-Token)
  Ereignismodifikatorfeld-Flags, 718
  Format, 717–718
  Reihenfolge in Prüfdatensatz, 717–718
Hierarchische Bereiche
  Kerberos, 413–414, 427
  konfigurieren, 456–457
Hilfe
  SEAM-Tool, 530
  URL für Onlinehilfe, 434
Hinzufügen
  ACL-Einträge, 150–151
  Admin-Hauptelemente (Kerberos), 440, 448
  angepasste Rolle, 223–224
  angepasste Rollen (RBAC), 223–224
  Attribute zu einem Berechtigungsprofil, 238–241
  Berechtigungen
    direkt zu Benutzer oder Rolle, 271–272
    zu Befehl, 270–271
  Berechtigungsprofile mit Solaris Management Console, 240
  Bibliotheks-Plugin, 314
  cryptomgt (Rolle), 225
  DH-Authentifizierung für eingehängte Dateisysteme, 341
  Einwahl-Passwörter, 70–72
  Hardwareprovider-Mechanismen und -Funktionen, 320
  lokaler Benutzer, 226
  neues Berechtigungsprofil, 238–241
  Operator (Rolle), 219

Hinzufügen *(Fortsetzung)*
PAM-Module, 352
Passwortverschlüsselungsmodul, 76–77
Plugins
kryptografisches Framework, 313–314
Prüfklassen, 646
Prüfrichtlinie, 655
Prüfung der Zonen, 624–629
Prüfverzeichnisse, 649–653
RBAC-Eigenschaften zu Legacy-Anwendungen, 243–245
Rollen
Benutzer, 220
für bestimmte Profile, 218–221
mit beschränktem Bereich, 220
über Befehlszeile, 221–224
Rollen prüfen, 225–226
Schlüssel für DH-Authentifizierung, 342–343
Service-Hauptelement zu Schlüsseltabellendatei (Kerberos), 562–563
Sicherheit bei Geräten, 85–86
Sicherheit für Geräte, 88–93
Sicherheit zu Systemhardware, 80–81
Sicherheitsattribute zu Legacy-Anwendungen, 243–245
sicherheitsbezogene Rolle, 225
sicherheitsbezogene Rollen, 219–220
Softwareprovider, 313–314
Softwareprovider auf Benutzerebene, 314
System Administrator (Rolle), 219
zuordenbares Gerät, 88–89
`hmac-md5` (Algorithmus), `ssh_config` (Datei), 395
`hmac-sha1` (Verschlüsselungsalgorithmus), `ssh_config` (Datei), 395
Hohe ASET-Sicherheitsebene, 161
`Host` (Schlüsselwort)
`ssh_config` (Datei), 394, 396
`host`-Hauptelement
erstellen, 442, 450
`HostbasedAuthentication` (Schlüsselwort), Secure Shell, 394
`HostbasedUsesNameFromPacketOnly` (Schlüsselwort), `sshd_config` (Datei), 394
Hostbasierte Authentifizierung
Beschreibung, 366
in Secure Shell konfigurieren, 371–373
`HostKey` (Schlüsselwort), `sshd_config` (Datei), 394
`HostKeyAlgorithms` (Schlüsselwort), `ssh_config` (Datei), 394
`HostKeyAlias` (Schlüsselwort), `ssh_config` (Datei), 394
`HostName` (Schlüsselwort), `ssh_config` (Datei), 394
Hostnamen
Voraussetzung für Prüfung, 657
zu Bereichen zuordnen, 427–428
Hosts
Kerberos-Service deaktivieren, 565–567
hosts, Secure Shell hosts, 366
Hosts
vertrauenswürdige Hosts, 61
Voraussetzung für Prüfung, 657
`hosts.equiv` (Datei), Beschreibung, 400

I

`-I` (Option)
`bart create` (Befehl), 112
`st_clean` (Skript), 105
`-i` (Option)
`bart create` (Befehl), 112, 118
`encrypt` (Befehl), 307
`st_clean` (Skript), 105
Identitätsdateien (Secure Shell), Naming-Konventionen, 399
`IdentityFile` (Schlüsselwort), `ssh_config` (Datei), 394
IDs
Prüfsitzung, 707
Prüfung
Mechanismus, 707
Übersicht, 609–611
UNIX zu Kerberos-Hauptelementen zuordnen, 604–605
`IgnoreRhosts` (Schlüsselwort), `sshd_config` (Datei), 394
`IgnoreUserKnownHosts` (Schlüsselwort), `sshd_config` (Datei), 394

`import` (Unterbefehl), `pktool` (Befehl), 327–329
`in.ftpd` (Dämon), Kerberos, 590
`in.rlogind` (Dämon), Kerberos, 590
`in.rshd` (Dämon), Kerberos, 590
`in.telnetd` (Dämon), Kerberos, 590
include (Steuer-Flag), PAM, 355
Inhalt der Hilfe, SEAM-Tool, 530
`install` (Unterbefehl), `cryptoadm` (Befehl), 314
Installation, Secure by Default, 53
Installieren
  Passwortverschlüsselungsmodul, 76–77
  Provider im kryptografischen Framework, 295
Instanz, Hauptelementnamen, 413
Integrität
  Kerberos, 407
  Sicherheitsservice, 415
Interaktives Ausführen von ASET, 178–179
INTERNAL (Plugin), SASL, 362
Internet-Firewall-Einrichtung, 60–61
Internetbezogene Token
  `ip` (Token), 719
  `ip_addr` (Token), 718
  `iport` (Token), 720
  `socket` (Token), 725–726
`ioctl` (Prüfklasse), 704
`ioctl()` (Systemaufrufe), 704
  `AUDIO_SETINFO()`, 105
`ip` (Prüf-Token), Format, 719
`ip_addr` (Prüf-Token), Format, 718
IP-Adressen, Secure Shell überprüfen, 393
IP MIB-II, Informationen abrufen`/dev/arp`, 86–87
`ipc` (Prüf-Token), 719–720
  Format, 719–720
`ipc` (Prüfklasse), 704
`IPC` Berechtigungen, 203
`ipc_perm` (Prüf-Token), Format, 720
ipc-Typfeldwerte (Token `ipc`), 719–720
`iport` (Prüf-Token), Format, 720

J

JASS-Toolkit, Verweis auf, 53

K

`-k` (Option)
  `encrypt` (Befehl), 307
  kerberisierte Befehle, 580
  `mac` (Befehl), 305
`-K` (Option)
  kerberisierte Befehle, 580
  `usermod` (Befehl), 271
`.k5.`*REALM* (Datei), Beschreibung, 588
`.k5login` (Datei)
  Beschreibung, 576–578, 587
  lieber als Passwort bekanntgeben, 577
`kadm5.acl` (Datei)
  Beschreibung, 588
  Format von Einträgen, 545
  Master-KDC-Eintrag, 440, 447, 487
  neue Hauptelemente, 539, 541
`kadm5.keytab` (Datei)
  Beschreibung, 560, 588
`kadmin` (Befehl)
  Beschreibung, 589
  Hauptelemente aus Schlüsseltabelle entfernen, 564
  `host`-Hauptelement erstellen, 442, 450
  `ktadd` (Befehl), 562–563
  `ktremove` (Befehl), 564
  SEAM-Tool, 528
`kadmin.local` (Befehl)
  Admin-Hauptelemente hinzufügen, 440, 448
  Beschreibung, 590
  Erstellung von Hauptelementen
    automatisieren, 533
  Schlüsseltabellendatei erstellen, 440, 448
`kadmin.log` (Datei), Beschreibung, 588
`kadmind` (Dämon)
  Kerberos, 590
  Master-KDC, 591
`kadmind` (Hauptelement), 561
`kbd` (Datei), 81–82
`KbdInteractiveAuthentication` (Schlüsselwort),
  Secure Shell, 394
`kcfd` (Dämon), 293
`kcfd`-Dämon, 321–322
`kclient` (Befehl), Beschreibung, 590
`kdb5_ldap_util` (Befehl), Beschreibung, 590

kdb5_util (Befehl)
  Beschreibung, 590
  KDC-Datenbank erstellen, 439
  Stash-Datei erstellen, 455, 499
KDC
  Administrationsdateien vom Slave auf den Master kopieren, 453, 498
  Backup und Weitergabe, 489–490
  Dämon starten, 455, 499
  Datenbank erstellen, 439
  Datenbankweitergabe, 431
  host-Hauptelement erstellen, 442, 450
  Master
    Definition, 591
  Master konfigurieren
    manuell, 438–443
    mit LDAP, 443–451
  Master und Slave austauschen, 484–489
  planen, 429
  Ports, 429
  Slave, 429
    Definition, 591
  Slave konfigurieren
    manuell, 451–455
  Slave oder Master, 414, 437
  Uhren synchronisieren
    Master-KDC, 443, 451
    Slave-KDC, 455, 499
  Zugriff auf Server beschränken, 506–507
kdc.conf (Datei)
  Beschreibung, 588
  Ticket-Lebensdauer, 595
kdc.log (Datei), Beschreibung, 588
kdestroy (Befehl)
  Beispiel, 572–573
  Kerberos, 589
KeepAlive (Schlüsselwort), Secure Shell, 394
Kerberos
  Befehle, 578–585, 589–590
  Beispiele für die Verwendung kerberisierter Befehle, 583–585
  Bereiche
    Siehe Bereiche (Kerberos)
  Dämonen, 590
Kerberos *(Fortsetzung)*
  Dateien, 587–589
  dfstab (Dateioption), 467
  Fehlerbehebung, 523
  Fehlermeldungen, 509–522
  KDC-Server konfigurieren, 437–456
  Kerberos V5-Protokoll, 408
  Komponenten, 416–417
  Konfigurationsentscheidungen, 425–434
  nur kerberisierte Anwendungen aktivieren, 506
  Onlinehilfe, 434
  Optionen zu kerberisierten Befehlen, 579
  Passwortverwaltung, 573–578
  planen, 425–434
  Referenz, 587–605
  Remote-Anwendungen, 412
  Tabelle der Netzwerkbefehlsoptionen, 581
  Terminologie, 591–598
  Übersicht
    Authentifizierungssystem, 408–414, 598
    kerberisierte Befehle, 579–581
  Verschlüsselungstypen
    Übersicht, 433–434
    verwenden, 602–604
  verwalten, 527–567
  Verwaltungstool
    Siehe SEAM-Tool
  verwenden, 569–585
  Zugriff auf Ihr Konto gewähren, 576–578
  Zugriff auf Server erhalten, 598–602
Kerberos-Authentifizierung
  dfstab (Dateioption), 467
  Secure RPC, 336
Kerberos-Befehle, 578–585
  Beispiele, 583–585
  nur kerberisierte aktivieren, 506
kern.notice (Eintrag), syslog.conf (Datei), 142
Kernel-Modul-Provider, auflisten, 310
Key Distribution Center, *Siehe* KDC
Key Management Framework (KMF), *Siehe* KMF
KEYBOARD_ABORT (Systemvariable), 81–82
keylogin (Befehl)
  DH-Authentifizierungseinrichtung überprüfen, 342

keylogin (Befehl) *(Fortsetzung)*
für Secure RPC verwenden, 337
KeyRegenerationInterval (Schlüsselwort), sshd_config (Datei), 394
keyserv (Dämon), 341
keyserver, Beschreibung, 337
keytab (Option), SASL, 363
kgcmgr (Befehl), Beschreibung, 590
kinit (Befehl)
Beispiel, 570–571
-F (Option), 570
Kerberos, 589
Ticket-Lebensdauer, 595
Klassen, *Siehe* Prüfklassen
klist (Befehl)
Beispiel, 571–572
-f (Option), 571–572
Kerberos, 589
KMF
Bibliothek, 324
Dienstprogramme, 324
erstellen
Passwort für Schlüsselspeicher, 330–331
Passwortsätze für Schlüsselspeicher, 325
selbstsigniertes Zertifikat, 326–327
Schlüsselspeicher, 324, 325
verwalten
PKI-Richtlinie, 325
Public-Key-Technologien (PKI), 323
Schlüsselspeicher, 325
Zertifikate exportieren, 329–330
Zertifikate in Schlüsselspeicher importieren, 327–329
kmfcfg (Befehl), 324
known_hosts (Datei)
Beschreibung, 399
Distribution steuern, 398
Kombinieren von Prüfdateien
auditreduce (Befehl), 667–669
von verschiedenen Zonen, 702
Komponenten
BART, 108–110
Gerätezuordnungsmechanismus, 99
RBAC, 193–196
Komponenten *(Fortsetzung)*
Secure Shell-Benutzersitzung, 391
Konfigurationsdateien
ASET, 160
audit_class (Datei), 696
audit_control (Datei), 639–641, 690, 697
audit_event (Datei), 698
audit_startup (Skript), 699
audit_user (Datenbank), 699–700
device_maps (Datei), 101
mit Berechtigungsinformationen, 282–283
nsswitch.conf (Datei), 41
für Passwortalgorithmen, 43
policy.conf (Datei), 43, 73–74, 262
Secure Shell, 390
syslog.conf (Datei), 68–70, 283, 696
system (Datei), 696
Konfigurationsentscheidungen
Kerberos
Anzahl der Bereiche, 426–427
Bereiche, 426–427
Bereichshierarchie, 427
Bereichsnamen, 426
Client- und Service-Hauptelementnamen, 428
Clients, 431–432
Datenbankweitergabe, 431
Hostnamen zu Bereichen zuordnen, 427–428
KDC-Server, 433
Ports, 429
Slave-KDCs, 429
Uhrsynchronisierung, 431
Verschlüsselungstypen, 433–434
Passwortalgorithmus, 43
Prüfung
Dateispeicherung, 626
Richtlinie, 629–633
Zonen, 624–625
zu prüfende Personen und Objekte, 627–629
Konfigurieren
ahlt (Prüfrichtlinie), 654–655
angepasste Rollen, 223–224
ASET, 168–171, 171
audit_class (Datei), 646
audit_control (Datei), 639–641

Konfigurieren *(Fortsetzung)*
audit_event (Datei), 647–648
audit_startup (Skript), 653–656
audit_user (Datenbank), 644–645
audit_warn (Skript), 653
auditconfig (Befehl), 695
Berechtigungsprofil über Befehlszeile, 240
Berechtigungsprofile, 238–241
DH-Schlüssel für NIS+-Benutzer, 343–344
DH-Schlüssel für NIS-Benutzer, 344–345
DH-Schlüssel in NIS, 344
DH-Schlüssel in NIS+, 342–343
Einwahl-Anmeldungen, 71
Geräte (Übersicht der Schritte), 83
Geräterichtlinie, 84
Gerätezuordnung, 87–88
Hardwaresicherheit, 80–82
Hostbasierte Authentifizierung für Secure Shell, 371–373
identische Prüfung für nicht globale Zonen, 661–663
Kerberos
Admin-Hauptelemente hinzufügen, 440, 448
bereichsübergreifende Authentifizierung, 456–458
Clients, 468–482
Master-KDC-Server, 438–443
Master-KDC-Server mit LDAP, 443–451
NFS-Server, 462–463
Slave-KDC-Server, 451–455
Übersicht, 435–508
Übersicht der Schritte, 435–436
Name Service, 228
Passwort für Hardwarezugriff, 80–81
perzone (Prüfrichtlinie), 655
Port-Weiterleitung in Secure Shell, 374–375
Prüfdateien, 639–648
Prüfdateien (Übersicht der Schritte), 638
Prüfpfadüberlauf verhindern, 674–675
Prüfprotokolle in Textform, 641–644
Prüfrichtlinie, 653–656
Prüfservice (Übersicht der Schritte), 648–649
Prüfung in Zonen, 620–621, 702–703
RBAC, 215–229
Konfigurieren *(Fortsetzung)*
RBAC (Übersicht der Schritte), 214–215
Rollen, 218–221, 236–238
über Befehlszeile, 221–224
Root-Benutzer als Rolle, 226–229
Secure Shell, 370
Clients, 392
Server, 392
Secure Shell (Übersicht der Schritte), 370
ssh-agent (Dämon), 381–382
vorübergehend für Prüfrichtlinie, 655
zonenweise Prüfung, 663–664
Konfigurieren von Netzwerkanwendungsservern, 458–460
Konsole, Versuche mit dem Befehl su anzeigen, 78–80
Kontextbezogene Hilfe, SEAM-Tool, 530
Konvertieren
Prüfdatensätze in lesbares Format, 672, 693
Kopieren
ACL-Einträge, 152
Dateien mit Secure Shell, 384–385
Korn-Shell, privilegierte Version, 200
kpasswd (Befehl)
Beispiel, 576
Fehlermeldung, 575
Kerberos, 589
passwd (Befehl), 574
kprop (Befehl), Beschreibung, 589
kpropd (Dämon), Kerberos, 590
kpropd.acl (Datei), Beschreibung, 588
kproplog (Befehl), Beschreibung, 590
krb5.conf (Datei)
bearbeiten, 438, 446
Beschreibung, 588
domain_realm (Abschnitt), 427–428
Portdefinition, 429
krb5.keytab (Datei), Beschreibung, 588
krb5cc_*UID* (Datei), Beschreibung, 588
krb5kdc (Dämon)
Kerberos, 590
Master-KDC, 591
starten, 455, 499
Kryptografische Services, *Siehe* kryptografisches Framework

Kryptografisches Framework
aktualisieren, 321–322
Befehle auf Benutzerebene, 293–294
Beschreibung, 290
cryptoadm (Befehl), 292, 293
Definition von Begriffen, 291
elfsign (Befehl), 293, 294
Fehlermeldungen, 309
Hardware-Plugins, 290
Interaktion, 292–293
mit Rolle verwalten, 225
neu starten, 321–322
PKCS #11-Bibliothek, 290
Provider, 290, 291
Provider auflisten, 310–312
Provider installieren, 295
Provider registrieren, 294
Provider signieren, 294
Provider verbinden, 294–295
Übersicht der Schritte, 297–298
Verbraucher, 290
Zonen, 295, 321–322
ksh (Befehl), privilegierte Version, 200
ktadd (Befehl)
Service-Hauptelement hinzufügen, 560, 562–563
Syntax, 562
ktkt_warnd (Dämon), Kerberos, 590
ktremove (Befehl), 564
ktutil (Befehl)
delete_entry (Befehl), 566
Kerberos, 589
list (Befehl), 565, 566
Liste der Hauptelemente anzeigen, 564, 565
read_kt (Befehl), 565, 566
Schlüsseltabellendatei verwalten, 561
Kurzes praudit-Ausgabeformat, 694

L

-L (Option), ssh (Befehl), 382–384
-l (Option)
digest (Befehl), 304
encrypt (Befehl), 299
mac (Befehl), 305
-l (Option) *(Fortsetzung)*
praudit (Befehl), 693
LDAP, für Master-KDC-Konfiguration, 443–451
LDAP Naming Service, Passwortalgorithmus angeben, 75–76
LDAP-Naming Service, Passwörter, 42
Lebensdauer von Tickets, Kerberos, 595–596
Lesbares Format für Prüfdatensatz, Prüfdatensätze konvertieren, 693
Lesbares Format für Prüfdatensätze, Prüfdatensätze konvertieren, 672
Leseberechtigungen, symbolischer Modus, 137
limitpriv (Schlüsselwort), user_attr (Datenbank), 283
list (Befehl), 565, 566
list (Unterbefehl), pktool (Befehl), 327
list_devices (Befehl)
Autorisierungen, 101
Autorisierungen erforderlich, 263
Beschreibung, 100
ListenAddress (Schlüsselwort), sshd_config (Datei), 394
Listenberechtigungen, SEAM-Tool, 559
LocalForward (Schlüsselwort), ssh_config (Datei), 395
log_level (Option), SASL, 364
logadm (Befehl), Prüfdateien in Textform archivieren, 674
login (Datei)
root-Zugriff beschränken, 78–80
Standardeinstellungen für die Anmeldung, 69
.login (Datei), Pfadvariableneintrag, 51
login_logout (Prüfklasse), 704
login-Umgebungsvariablen, Secure Shell, 397
LoginGraceTime (Schlüsselwort), sshd_config (Datei), 395
loginlog (Datei), fehlgeschlagene Anmeldeversuche, 67–68
logins (Befehl)
Anmeldestatus eines Benutzers anzeigen, 65–66
Benutzer ohne Passwort anzeigen, 66
Syntax, 65
LogLevel (Schlüsselwort), Secure Shell, 395

LookupClientHostnames (Schlüsselwort), sshd_config (Datei), 395
Löschen
ACL-Einträge, 141, 153
archivierte Prüfdateien, 674
Berechtigungsprofile, 239
Hauptelement (Kerberos), 543
not_terminated-Prüfdateien, 673–674
Prüfdateien, 667
Richtlinien (Kerberos), 554–555
Service des Hosts, 566
Tickets mit kdestroy, 572–573

M

-M (Option), auditreduce (Befehl), 668
-m (Option)
cryptoadm (Befehl), 315, 316
kerberisierte Befehle, 580
mac (Befehl)
Beschreibung, 293
Syntax, 305
MAC (Message Authentication Code), für Datei berechnen, 305–306
MACS (Schlüsselwort), Secure Shell, 395
Mail, mit Secure Shell verwenden, 383–384
makedbm (Befehl), Beschreibung, 261
Management
Siehe auch verwalten
Dateiberechtigungen, 142–143
Geräte, 87–88
Gerätezuordnung (Übersicht der Schritte), 87–88
Passwörter mit Kerberos, 573–578
Prüfdateien, 667–669, 674–675
Prüfdatensätze (Übersicht der Schritte), 665
Prüfpfadüberlauf, 674–675
Prüfung, 637
Prüfung in Zonen, 620–621, 702–703
Schlüsselspeicher mit KMF, 325
Manifest testen, 109
Manifeste
Siehe auch bart create
anpassen, 114–117
Dateiformat, 125–126
Manifeste *(Fortsetzung)*
Steuerung, 107
Testen, 109
Manuell konfigurieren
Kerberos
Master-KDC-Server, 438–443
Master-KDC-Server mit LDAP, 443–451
Manuelles Konfigurieren
Kerberos
Slave-KDC-Server, 451–455
Maske (Prüfung)
Beschreibung der Prozessvorauswahl, 707
systemweite Prozessvorauswahl, 697
Masken-ACL-Einträge
Beschreibung, 140
einstellen, 150–151
Standardeinträge für Verzeichnisse, 140–141
Master-Dateien (ASET), 162, 167, 168
Master KDC, Definition, 591
Master-KDC
gegen Slave-KDC austauschen, 484–489
manuell konfigurieren, 438–443
mit LDAP konfigurieren, 443–451
Slave-KDCs, 414, 437
max_life (Wert), Beschreibung, 595
max_renewable_life (Wert), Beschreibung, 596
MaxAuthTries (Schlüsselwort), sshd_config (Datei), 395
MaxAuthTriesLog (Schlüsselwort), sshd_config (Datei), 395
MaxStartups (Schlüsselwort), sshd_config (Datei), 395
MD5 (Verschlüsselungsalgorithmus), Kernel-Provider, 310
MD5-Verschlüsselungsalgorithmus, policy.conf (Datei), 73–74
mech_dh (Mechanismus), Secure RPC, 342–343
mech_dh Mechanismus,
GSS-API-Berechtigungsnachweise, 391
mech_krb-Mechanismus,
GSS-API-Berechtigungsnachweise, 391
mech_list (Option), SASL, 363
Mechanismen
alle auf Hardwareprovider deaktivieren, 319–321

Mechanismen *(Fortsetzung)*
einige auf Hardwareprovider aktivieren, 320
Mechanismus, Definition im kryptografischen Framework, 291
Media Backup (Berechtigungsprofil)
vertrauenswürdigen Benutzern zuweisen, 191, 223
Media Restore (Berechtigungsprofil), vertrauenswürdigen Benutzern zuweisen, 223
`messages` (Datei), ausführbare Stack-Meldungen, 142
Metaslot
Definition im kryptografischen Framework, 291
verwalten, 293
Mikrofon
zuordnen, 94
Zuordnung aufheben, 97
`minfree` (Zeile)
`audit_control` (Datei), 697
`audit_warn` (Bedingung), 700
Minuszeichen (-)
Dateiberechtigungssymbol, 137
Eintrag in Datei `sulog`, 78
Prüfklassenpräfix, 704
Symbol für Dateityp, 132
Mittlere ASET-Sicherheitsebene, 161
Module, Passwortverschlüsselung, 43
Modus, Definition im kryptografischen Framework, 291
`mount` (Befehl), mit Sicherheitsattributen, 89
`mt` (Befehl), Bandgerätbereinigung, 104

N

`-n` (Option)
`audit` (Befehl), 690
`bart create` (Befehl), 112
n2cp-Treiber
Hardware-Plugin zu kryptografischem Framework, 290
Mechanismen auflisten, 318–319
Nachdatiertes Ticket
Beschreibung, 409
Definition, 593
`naflags` (Zeile), `audit_control` (Datei), 697
Namen
Gerätenamen
`device_maps` (Datei), 102, 103
Prüfdateien, 708
Prüfklassen, 703
Namenskonventionen
Geräte, 90
Prüfdateien, 708
Prüfverzeichnisse, 640, 698
RBAC-Autorisierungen, 252
Naming-Konventionen, Secure Shell-Identitätsdateien, 399
Naming Services
Siehe einzelne Naming Services
Bereich und RBAC, 200
ncp-Treiber
Hardware-Plugin zu kryptografischem Framework, 290
Mechanismen auflisten, 318–319
`NET` Berechtigungen, 203
`netservices limited` (Installationsoption), 53
`network` (Prüfklasse), 704
Network Security (RBAC), Rolle erstellen, 220
Network Time Protocol, *Siehe* NTP
Netzwerk, Berechtigungen mit Bezug auf, 203
Netzwerksicherheit
Authentifizierung, 58–60
Autorisierungen, 58–60
Firewall-Systeme
Paketzerstörung, 61
vertrauenswürdige Hosts, 61
Firewallsysteme
Notwendigkeit, 60
Probleme melden, 62
Übersicht, 57
Zugriff steuern, 57–61
Neu starten
`ssh` Service, 375
`sshd` (Dämon), 375
Neue Funktionen
BART, 107–129
Befehle
`bart create`, 108–109
`cryptoadm`, 310

Neue Funktionen, Befehle *(Fortsetzung)*
`getdevpolicy`, 84–85
`kclient`, 419
`kpropd`, 419
`ppriv`, 267–268
`praudit -x`, 672
`ssh-keyscan`, 401
`ssh-keysign`, 402
Berechtigungen, 201–211
Erweiterungen der Prüffunktionen, 621–622
Kerberos-Erweiterungen, 418–421
kryptografisches Framework, 289–295
Metaslot, 289
Oracle Solaris Cryptographic Framework, 289–295
PAM-Erweiterungen, 349–350
Prozessrechtsverwaltung, 201–211
SASL, 361
Secure Shell-Verbesserungen, 368–369
Verbesserungen der Systemsicherheit, 39–40
Neustarten
kryptografische Services, 321–322
Prüfdämon, 659
never-audit classes, `audit_user` (Datenbank), 699
`newkey` (Befehl)
Schlüssel für NIS-Benutzer erstellen, 344–345
Schlüssel generieren, 337
NFS-Dateisysteme
ASET, 172
Authentifizierung, 335
Client-Server-Sicherheit bereitstellen, 337–340
sicherer Zugriff mit `AUTH_DH`, 346
NFS-Server, für Kerberos konfigurieren, 462–463
Nicht hierarchische Bereiche, Kerberos, 413–414
Nicht zuweisbare Klassen, 697
Niedrige ASET-Sicherheitsebene, 160
NIS+-Name Service, ASET-Prüfungen, 171
NIS+-Naming Service
authentifizierten Benutzer hinzufügen, 343–344
Authentifizierung, 335
`cred` (Datenbank), 343
`cred` (Tabelle), 337
NIS+ Naming Service, Passwortalgorithmus
angeben, 75
NIS+-Naming Service
Passwörter, 42
NIS-Naming Service
Authentifizierung, 335
NIS Naming Service, Passwortalgorithmus
angeben, 74
NIS-Naming Service
Passwörter, 42
`nisaddcred` (Befehl)
Clientberechtigungsnachweis hinzufügen, 342
Schlüssel generieren, 337
`no_class` (Prüfklasse), 703
`nobody` (Benutzer), 56–57
`noexec_user_stack` (Variable), 141, 157
`noexec_user_stack_log` (Variable), 142, 157
`NoHostAuthenticationForLocalHost` (Schlüsselwort), `ssh_config` (Datei), 395
`nologin` (Datei), Beschreibung, 399
`non_attrib` (Prüfklasse), 703
`nscd` (Name Service-Cache-Dämon)
mit Befehl `svcadm` starten, 218
verwenden, 261
NSS, Schlüsselspeicher verwalten, 325
`nsswitch.conf` (Datei),
Anmeldezugriffsbeschränkungen, 41
NTP
Kerberos planen, 431
Master-KDC, 443, 451
Slave-KDC, 455, 499
`null` (Prüfklasse), 703
`NumberOfPasswordPrompts` (Schlüsselwort), `ssh_config` (Datei), 395

O

`-O` (Option), `auditreduce` (Befehl), 667–669
`-o` (Option), `encrypt` (Befehl), 307
Objektwiederverwendung, Anforderungen
Bereinigungsskripten
Bandlaufwerke, 104
neue Skripten erstellen, 105
Geräte, 104–105
Öffentliche Objekte, Prüfung, 614

Öffentliche Schlüssel
DH-Authentifizierung, 336–340
Paar aus öffentlichem und privatem Schlüssel, 376–378
Passwortsatz ändern, 378–379
Secure Shell-Identitätsdateien, 399
Öffentliche Verzeichnisse
Prüfung, 614
Sticky Bit, 135
Onlinehilfe
SEAM-Tool, 530
URL, 434
opaque (Prüf-Token), Format, 721
OpenSSH, *Siehe* Secure Shell
OpenSSL, Schlüsselspeicher verwalten, 325
Operator (RBAC)
empfohlene Rolle, 191
Inhalt des Berechtigungsprofils, 249
Rolle erstellen, 219
optional (Steuer-Flag), PAM, 355
Optionen zu kerberisierten Befehlen, 579
Oracle Solaris Cryptographic Framework, *Siehe* kryptografisches Framework
other (Prüfklasse), 704
ovsec_adm.*xxxxx* (Datei), Beschreibung, 588

P

p_minfree (Attribut), audit_warn (Bedingung), 700
-p (Option)
aset (Befehl), 180
bart create, 118
bsmrecord (Befehl), 666
cryptoadm (Befehl), 315, 316
logins (Befehl), 66
Pakete, Secure Shell, 398
Paketübertragungen
Firewall-Sicherheit, 60
Paketzerstörung, 61
PAM
/etc/syslog.conf (Datei), 353
Framework, 348
Kerberos, 417, 422
PAM *(Fortsetzung)*
Konfigurationsdatei
Einführung, 353
Erläuterung zu Stacking, 354
Kerberos, 588
Stacking-Beispiel, 358
Stacking-Diagramme, 356
Steuer-Flags, 355
Syntax, 354
Modul hinzufügen, 352
planen, 351
Übersicht, 347
Übersicht der Schritte, 350
pam.conf (Datei), *Siehe* PAM-Konfigurationsdatei
pam_roles (Befehl), Beschreibung, 261
PAMAuthenticationViaKBDInt (Schlüsselwort), sshd_config (Datei), 395
Partitionieren der Festplatte, für binäre Prüfdateien, 649–653
PASSREQ in Secure Shell, 397
passwd (Befehl)
Naming Services, 42
Passwort einer Rolle ändern, 234–236
und kpasswd (Befehl), 574
passwd (Datei)
ASET-Prüfungen, 162
/etc/d_passwd (Datei), 46
PasswordAuthentication (Schlüsselwort), Secure Shell, 395
Passwort, Benutzer ohne Passwort anzeigen, 66
Passwortalgorithmen anderer Anbieter, hinzufügen, 76–77
Passwortauthentifizierung, Secure Shell, 366
Passwörter
Algorithmus angeben, 73–74
in Naming Services, 74
lokal, 72–73
ändern passwd -r (Befehl), 42
Anmeldesicherheit, 41, 42
Authentifizierung in Secure Shell, 366
Benutzer ohne Passwort suchen, 66
Blowfish-Algorithmus verwenden, 74
Einwahl-Passwörter
/etc/d_passwd (Datei), 46

Passwörter, Einwahl-Passwörter *(Fortsetzung)*
vorübergehend deaktivieren, 72
Einwahl vorübergehend deaktivieren, 72
für Einwahl erstellen, 70–72
für Hardwarezugriff anfordern, 80–81
Hardwarezugriff, 80–81
in Secure Shell entfernen, 380–381
in Secure Shell in CDE entfernen, 381–382
LDAP, 42
neuen Passwortalgorithmus angeben, 75–76
lokal, 42
Management, 573–578
MD5-Verschlüsselungsalgorithmus verwenden, 73–74
mit dem Befehl `kpasswd` ändern, 574
mit dem Befehl `passwd` ändern, 574
neuen Algorithmus verwenden, 74
NIS, 42
neuen Passwortalgorithmus angeben, 74
NIS+, 42
neuen Passwortalgorithmus angeben, 75
Passwort eines Hauptelements ändern, 542–543
PROM-Sicherheitsmodus, 41, 80–82
Richtlinien, 574
Rollenpasswort ändern, 234–236
schützen
PKCS #12-Datei, 330
Schlüsselspeicher, 330
Systemanmeldungen, 42
Übersicht der Schritte, 64
UNIX und Kerberos, 573–578
Verschlüsselung geheimer Schlüssel für Secure RPC, 337–338
Verschlüsselungsalgorithmen, 43
Verschlüsselungsmodul eines anderen Anbieters installieren, 76–77
Vorschläge zur Auswahl, 573–574
Zugriff gewähren ohne bekannt zu geben, 576–578
Passwortsätze
Beispiel, 379
`encrypt` (Befehl), 307
für MAC verwenden, 306
für Secure Shell ändern, 378–379
in KMF generieren, 330–331
Passwortsätze *(Fortsetzung)*
in Secure Shell verwenden, 378, 380–381
`mac` (Befehl), 305
sicher speichern, 307
`path` (Prüf-Token), Format, 721
`path` (Prüfrichtlinie), Beschreibung, 630
`PATH` (Umgebungsvariable)
einstellen, 51
Sicherheit, 51
`path_attr` (Prüf-Token), 622, 722
`PATH` in Secure Shell, 397
`PERIODIC_SCHEDULE` (Variable bei ASET), 170, 174
`PermitEmptyPasswords` (Schlüsselwort), `sshd_config` (Datei), 395
`PermitRootLogin` (Schlüsselwort), `sshd_config` (Datei), 395
`PermitUserEnvironment` (Schlüsselwort), `sshd_config` (Datei), 395
`perzone` (Prüfrichtlinie)
Beschreibung, 631
einrichten, 655
verwenden, 625, 663–664, 702–703
Verwendung, 620–621
`pfcsh` (Befehl), Beschreibung, 200
`pfexec` (Befehl), Beschreibung, 262
`pfksh` (Befehl), Beschreibung, 200
`pfsh` (Befehl), Beschreibung, 200
Physische Sicherheit, Beschreibung, 40–41
`PidFile` (Schlüsselwort), Secure Shell, 395
PKCS #11-Bibliothek
in Oracle Solaris Cryptographic Framework, 290
Providerbibliothek hinzufügen, 314
PKCS #11-Softtoken, Schlüsselspeicher verwalten, 325
PKCS #12-Dateien, schützen, 330
`pkcs11_kernel.so` (Provider auf Benutzerebene), 310
`pkcs11_softtoken.so` (Provider auf Benutzerebene), 310
`pkgadd` (Befehl)
Provider von Drittanbietern installieren, 313
Software anderer Anbieter installieren, 76
PKI
von KMF verwaltet, 323
von KMF verwaltete Richtlinie, 325

pktool (Befehl)
export (Unterbefehl), 329–330
Geheimschlüssel generieren, 301–304
gencert (Unterbefehl), 326–327
import (Unterbefehl), 327–329
list (Unterbefehl), 327
PKI-Objekte verwalten, 324
selbstsigniertes Zertifikat erstellen, 326–327
setpin (Unterbefehl), 330–331
plain.so.1 (Plugin), SASL, 362
Planen
Kerberos
Anzahl der Bereiche, 426–427
Bereiche, 426–427
Bereichshierarchie, 427
Bereichsnamen, 426
Client- und Service-Hauptelementnamen, 428
Datenbankweitergabe, 431
Konfigurationsentscheidungen, 425–434
Ports, 429
Slave-KDCs, 429
Uhrsynchronisierung, 431
PAM, 351
Prüfung, 624–629
Prüfung in Zonen, 624–625
RBAC, 215–217
Übersicht der Schritte zur Prüfung, 623
Platzhalterzeichen
für Hosts in Secure Shell, 386
in ASET-Dateien, 175
in RBAC-Autorisierungen, 252
in tune-Dateien bei ASET, 177
Plugfähiges Authentifizierungsmodul, *Siehe* PAM
plugin (Zeile)
audit_control (Datei), 697
p_* (Attribute), 642
qsize (Attribut), 642
plugin_list (Option), SASL, 363
Plugins
in Prüfservice, 642
kryptografisches Framework, 290
SASL, 362
vom Dämon auditd geladen, 690
Pluszeichen (+)
ACL-Eintrag, 150
Dateiberechtigungssymbol, 137
Eintrag in Datei sulog, 78
Prüfklassenpräfix, 704
policy.conf (Datei)
Basic Solaris User (Berechtigungsprofil), 250
Beschreibung, 260–261, 262
Passwortalgorithmen angeben, 73–74
Passwortalgorithmus angeben
in Naming Services, 74
Passwortverschlüsselungsmodul hinzufügen, 76–77
Schlüsselwörter
für Berechtigungen, 261, 282
für Berechtigungsprofile, 260
für Passwortalgorithmen, 44
für RBAC-Autorisierungen, 260
Verschlüsselungsalgorithmus angeben, 73–74
Port (Schlüsselwort), Secure Shell, 395
Port-Weiterleitung
in Secure Shell konfigurieren, 374–375
Secure Shell, 383–384, 384
Ports, Kerberos-KDC, 429
postsigterm (Zeichenfolge), audit_warn (Skript), 701
ppriv (Befehl), Fehlersuche, 268
ppriv (Befehle), Berechtigungen auflisten, 267
Präfixe für Prüfklassen, 704
praudit (Befehl)
Ausgabeformate, 693
DTD für Option -x, 694
in Skript verwenden, 694–695
ohne Optionen, 694
Optionen, 693
Pipe-Verkettung der auditreduce-Ausgabe, 672
Prüfdatensätze anzeigen, 671–673
Prüfdatensätze in lesbares Format
konvertieren, 672, 693
XML-Format, 673
PreferredAuthentications (Schlüsselwort),
ssh_config (Datei), 395
Primärer Name, Hauptelementnamen, 413
Primäres Prüfverzeichnis, 697
Primary Administrator (RBAC)
Berechtigungsprofilinhalte, 248

Primary Administrator (RBAC) *(Fortsetzung)*
empfohlene Rolle, 191
Rolle annehmen, 231
`principal` (Datei), Beschreibung, 588
`principal.kadm5` (Datei), Beschreibung, 588
`principal.kadm5.lock` (Datei), Beschreibung, 588
`principal.ok` (Datei), Beschreibung, 588
`principal.ulog` (Datei), Beschreibung, 588
Printer Management (RBAC), Inhalt des Berechtigungsprofils, 250
`PrintLastLog` (Schlüsselwort), `ssh_config` (Datei), 395
`PrintMotd` (Schlüsselwort), `sshd_config` (Datei), 395
Prinzip der geringsten Berechtigung, 203
`priv.debug` (Eintrag), `syslog.conf` (Datei), 283
`PRIV_DEFAULT` (Schlüsselwort)
`policy.conf` (Datei), 261, 282
`PRIV_LIMIT` (Schlüsselwort)
`policy.conf` (Datei), 261, 282
`PRIV_PROC_LOCK_MEMORY` Berechtigung, 189, 205–206
Private (Schutzebene), 581
Private Schlüssel
Siehe auch Geheime Schlüssel
Definition in Kerberos, 592
Secure Shell-Identitätsdateien, 399
`privilege` (Prüf-Token), 622, 722
`privileges` (Datei), Beschreibung, 204
Privilegierte Anwendung
Autorisierungsprüfung, 198
Berechtigungsprüfung, 197
Beschreibung, 193
ID-Prüfung, 197
Privilegierte Ports, Alternative zu Secure RPC, 59
`privs` (Schlüsselwort), `user_attr` (Datenbank), 283
`PROC` (Berechtigungen), 203
`process` (Prüf-Token), Format, 722–724
`process` (Prüfklasse), 704
`process modify` (Prüfklasse), 704
`process start` (Prüfklasse), 704
`prof_attr` (Datenbank)
Beschreibung, 258–259
Zusammenfassung, 253
Profil-Shells, Beschreibung, 200
Profile, *Siehe* Berechtigungsprofile
`.profile` (Datei), Pfadvariableneintrag, 51
`profiles` (Befehl), Beschreibung, 262
`PROFS_GRANTED` (Schlüsselwort), `policy.conf` (Datei), 260
Programme
auf RBAC-Autorisierungen überprüfen, 244
Berechtigungen erkennend, 206, 208
`project.max-locked-memory` (Ressourcensteuerungen), 189, 205–206
PROM-Sicherheitsmodus, 80–82
`Protocol` (Schlüsselwort), Secure Shell, 395
Protokolldateien
Ausführungsprotokoll (ASET), 164
BART
ausführliche Ausgabe, 128–129
programmatische Ausgabe, 128–129
Befehl `su` überwachen, 78
für Prüfservice konfigurieren, 641–644
Prüfdatensätze, 618, 672
Prüfdatensätze untersuchen, 691
`syslog` (Prüfdatensätze), 696
`/var/adm/messages`, 678
`/var/log/syslog`, 678
Protokollieren, `ftp` (Dateiübertragungen), 687–688
Provider
Bibliothek hinzufügen, 314
Definition als Plugins, 290, 291
Definition im kryptografischen Framework, 292
Hardwaremechanismen deaktivieren, 319–321
Hardwareprovider auflisten, 318–319
im kryptografischen Framework auflisten, 310–312
installieren, 295
mit dem kryptografischen Framework verbinden, 294
registrieren, 294
signieren, 294
Softwareprovider auf Benutzerebene hinzufügen, 314
Softwareprovider hinzufügen, 313–314
Verwendung von Kernel-Modul-Softwareprovidern verhindern, 316–318
Verwendung von Kernel-Softwareprovidern wiederherstellen, 317
Proxy-Ticket, Definition, 594

ProxyCommand (Schlüsselwort), ssh_config (Datei), 395
Proxyfähiges Ticket, Definition, 594
Prozessberechtigungen, 203
Prozessberechtigungsverwaltung, *Siehe* Berechtigungen
Prozessprüfungsmerkmale
  Prozessvorauswahlmaske, 707
  Prüf-ID, 707
  Prüfsitzungs-ID, 707
  Terminal-ID, 707
Prozessvorauswahlmaske, Beschreibung, 707
Prüf-ID
  Mechanismus, 707
  Übersicht, 609–611
Prüf-Plugins, Zusammenfassung, 706
Prüf-Token
  Siehe auch einzelne Prüf-Token-Namen
  Beschreibung, 613, 617
  durch Prüfrichtlinie hinzugefügt, 706
  Format, 711
  Liste, 711
  neu in aktueller Version, 622
  Prüfdatensatzformat, 709
Prüfdämon, *Siehe* auditd (Dämon)
Prüfdateien
  auditreduce (Befehl), 691
  drucken, 672
  Festplatte partitionieren, 649–653
  freier Speicherplatz (mindestens) für Dateisysteme, 697
  Größe beschränken, 686
  kombinieren, 667–669, 691
  konfigurieren, 639–648
  Management, 674–675
  Meldungen in eine Datei kopieren, 671
  Namen, 708, 709
  Reihenfolge für Öffnen, 697
  Speicherplatz für Prüfdatensätze, 690
  Speicherplatzanforderungen verringern, 634–635, 635
  verringern, 667–669, 691
  Zeitstempel, 709
  zu neuer Datei wechseln, 690
Prüfdateien kombinieren, auditreduce (Befehl), 691
Prüfdatensätze
  anzeigen, 671–673
  Beispiel für Formatierung, 666
  Beschreibung, 613
  Format, 709
  Formate anzeigen
    Verfahren, 665–667
    Zusammenfassung, 691
  Formate einer Prüfklasse anzeigen, 666–667
  Formate eines Programms anzeigen, 666
  in lesbares Format konvertieren, 672, 693
  in XML-Format anzeigen, 673
  Prüfdateien verringern, 667–669
  Prüfverzeichnisse voll, 690, 701
  Sequenz der Token, 709
  syslog.conf (Datei), 612
  Übersicht, 616
  /var/adm/auditlog (Datei), 642
  von Ereignissen generiert, 611
  zusammenführen, 667–669
Prüfereignisse
  audit_event (Datei), 614
  aus Prüfpfad auswählen, 669–671
  aus Prüfpfad in Zonen auswählen, 702
  Beschreibung, 614
  Klassenmitgliedschaft ändern, 647–648
  von binären Dateien anzeigen, 671–673
  zu Klassen zuordnen, 616
  Zusammenfassung, 613
Prüfklassen
  Ausnahmen in Datenbank audit_user, 699–700
  Ausnahmen zu systemweiten Einstellungen, 616
  Beschreibung, 613, 614
  Definitionen, 703
  Einträge in Datei audit_control, 697
  Ereignisse zuordnen, 616
  hinzufügen, 646
  Präfixe, 704
  Prozessvorauswahlmaske, 707
  Standardwerte ändern, 646
  Syntax, 704, 705
  systemweit, 697
  systemweit einstellen, 703
  Übersicht, 615–616

Prüfklassen *(Fortsetzung)*
Vorauswahl, 613, 639–641
Prüfklassen-Vorauswahl, Auswirkung auf öffentliche Objekte, 614
Prüfkonfigurationsdatei, *Siehe* `audit_control` (Datei)
Prüfmeldungen, in eine Datei kopieren, 671
Prüfmeldungen in eine Datei kopieren, 671
Prüfpfad
alle Dateien zusammenführen, 692
Analyse mit Befehl `praudit`, 693
Analyseaufwand, 634
Auswirkung der Prüfrichtlinie, 629
Beschreibung, 613
enthaltene Ereignisse, 616
Ereignisse anzeigen, 671–673
Ereignisse auswählen, 669–671
Ereignisse von verschiedenen Zonen anzeigen, 702
erstellen
Funktion des Dämons `auditd`, 690
in Echtzeit überwachen, 635
keine öffentlichen Objekte, 614
nicht abgeschlossene Dateien bereinigen, 673–674
Überlauf verhindern, 674–675
Übersicht, 611
Prüfprotokolle
Siehe auch Prüfdateien
in Text, 697
Modi, 618
Prüfprotokolle in Textform konfigurieren, 641–644
Text- und binäres Format vergleichen, 618
Prüfrichtlinie
`ahlt` einrichten, 654–655
`arge` einrichten, 682
`argv` einrichten, 682
Auswirkungen, 629–633
Beschreibung, 613
dynamisch aktualisieren, 660
einrichten, 653–656
hinzugefügte Token, 706
in globaler Zone einstellen, 702–703
ohne Auswirkung auf Token, 706
`perzone` einrichten, 655
Prüf-Token, 706
`public`, 631
Prüfrichtlinie *(Fortsetzung)*
Standardwerte, 629–633
Prüfrichtlinien, in globaler Zone einstellen, 620–621
Prüfsitzungs-ID, 707
Prüfung
aktivieren, 656–657
alle Befehle von Benutzern, 680–682
Änderungen an bestimmten Dateien suchen, 683
Änderungen der Geräterichtlinie, 86
Änderungen in aktueller Version, 621–622
Anmeldungen, 686–687
Berechtigungen, 283–284
Berechtigungsprofile, 702
deaktivieren, 658–659
Definition der Vorauswahl, 613
Fehlerbehebung, 675–688
Fehlerbehebung`praudit` (Befehl), 673
Gerätezuordnung, 92–93
identisch für alle Zonen konfigurieren, 661–663
in globaler Zone konfigurieren, 624, 654–655
in Zonen planen, 624–625
Informationen aktualisieren, 659–660
planen, 624–629
Rollen, 225–226
`sftp` (Dateiübertragungen), 687–688
Voraussetzung für `hosts`-Datenbank, 657
Zonen, 702–703
Zonen und, 620–621
zonenweise konfigurieren, 663–664
Prüfungsmerkmale
Prozessvorauswahlmaske, 691
Prüf-ID, 707
Sitzungs-ID, 707
Terminal-ID, 707
verarbeiten, 707
Vorauswahlmaske für Benutzerprozesse, 707
Prüfungsschwellenwert, 697
Prüfungsvoraussetzung, `hosts`-Datenbank ordnungsgemäß konfiguriert, 657
Prüfungsvorauswahlmaske
für einzelne Benutzer ändern, 644–645
für vorhandene Benutzer ändern, 683–685
Prüfverzeichnis
Beispielstruktur, 692

Prüfverzeichnis *(Fortsetzung)*
Beschreibung, 613
erstellen, 651
partitionieren, 649–653
Pseudo-TTY, in Secure Shell verwenden, 391–392
`PubkeyAuthentication` (Schlüsselwort), Secure Shell, 395
`public` (Prüfrichtlinie)
Beschreibung, 631
schreibgeschützte Ereignisse, 631
Public-Key-Kryptografie
allgemeine Schlüssel berechnen, 339
`AUTH_DH`-Client-Server-Sitzung, 337–340
Datenbank der öffentlichen Schlüssel für Secure RPC, 337
geheime Schlüssel bei NFS, 337
öffentliche und geheime Schlüssel bei NFS ändern, 337
Schlüssel generieren
Dialogschlüssel für Secure NFS, 338
Diffie-Hellman verwenden, 337
Public-Key-Technologien, *Siehe* PKI
`publickey` (Map), DH-Authentifizierung, 336–340
Punkt (`.`)
Autorisierungsnamen-Trennzeichen, 252
Pfadvariableneintrag, 51
verborgene Dateien anzeigen, 143
`pwcheck_method` (Option), SASL, 363

Q

`qsize` (Attribut), `plugin` (Eintrag), 642

R

`-R` (Option)
`bart create`, 112, 118
`ssh` (Befehl), 382–384
`-r` (Option)
`bart create`, 118
`passwd` (Befehl), 42
`praudit` (Befehl), 694
Rautezeichen (#)
`device_allocate` (Datei), 103
`device_maps` (Datei), 102
RBAC
angepasste Rollen hinzufügen, 223–224
Autorisierungen, 196–197
Autorisierungen mit Skripten oder Programmen überprüfen, 244
Autorisierungsdatenbank, 256–257
Basiskonzepte, 193–196
Befehle zum Verwalten, 261–262
Benutzer ändern, 241–243
Benutzereigenschaften ändern über Befehlszeile, 243
Berechtigungsprofildatenbank, 258–259
Berechtigungsprofile, 198–199
Berechtigungsprofile bearbeiten, 238–241
Datenbank, 253–261
Datenbankbeziehungen, 254–255
Elemente, 193–196
konfigurieren, 215–229
Naming Services, 255
neues Berechtigungsprofil hinzufügen, 240
planen, 215–217
privilegierte Anwendungen verwenden, 232–233
Profil-Shells, 200
Prüfprofile, 702
Rollen ändern, 236–238
Rollen hinzufügen, 218–221
Rollen prüfen, 225–226
Rollen über Befehlszeile hinzufügen, 221–224
Rollenpasswörter ändern, 234–236
Skripten sichern, 244
verglichen mit Superuser-Modell, 190–193
Verwaltungsbefehle, 261–262
RC4, *Siehe* ARCFOUR-Kernel-Provider
`rcp` (Befehl)
Kerberos, 579–581, 589
`rdist` (Befehl), Kerberos, 589
`read_kt` (Befehl), 565, 566
`reauth_timeout` (Option), SASL, 363
Rechnersicherheit, *Siehe* Systemsicherheit
Rechteprofile, System Administrator-Profil verwenden, 80

Regeldatei (BART), 110
Regeldatei-Spezifikationssprache, *Siehe* Zitatzeichensyntax
Regeldateiattribute, *Siehe* Schlüsselwörter
Regeldateiformat (BART), 126–128
Registrieren von Providern, kryptografisches Framework, 294
`rem_drv` (Befehl), Beschreibung, 98
Remote-Anmeldungen
  Authentifizierung, 58–60
  Autorisierung, 58–60
  für Superuser verhindern, 78–80
  Sicherheit, 340
`RemoteForward` (Schlüsselwort), `ssh_config` (Datei), 395
required (Steuer-Flag), PAM, 356
requisite (Steuer-Flag), PAM, 356
Ressourcensteuerungen
  Berechtigungen, 189, 205–206
  `project.max-locked-memory`, 189, 205–206
  `zone.max-locked-memory`, 189, 205–206
`RETRIES` in Secure Shell, 397
`return` (Prüf-Token), Format, 724
`rewoffl` (Option)
  `mt` (Befehl)
    Bandgerätbereinigung, 104
`.rhosts` (Datei), Beschreibung, 399
`RhostsAuthentication` (Schlüsselwort), Secure Shell, 396
`RhostsRSAAuthentication` (Schlüsselwort), Secure Shell, 396
Richtlinie
  Definition im kryptografischen Framework, 292
  Definition in Oracle Solaris, 35–36
Richtlinien
  Attribute anzeigen, 549–551
  erstellen (Kerberos), 538
  Geräte, 84–85
  Liste anzeigen, 547–549
  löschen, 554–555
  neue erstellen (Kerberos), 551–552
  Passwortalgorithmus, 72–73
  Passwörter, 574
  Prüfung, 629–633
Richtlinien *(Fortsetzung)*
  SEAM-Tool-Fensterbereiche, 555–558
  Übersicht, 35–36
  Übersicht der Schritte für die Verwaltung, 546–547
  verwalten, 527–567
`rlogin` (Befehl)
  Kerberos, 579–581, 589
`rlogind` (Dämon), Kerberos, 590
`roleadd` (Befehl)
  Beschreibung, 262
  verwenden, 221
`roledel` (Befehl), Beschreibung, 262
`rolemod` (Befehl)
  Beschreibung, 262
  Eigenschaften einer Rolle ändern, 237
`roles` (Befehl), Beschreibung, 262
Rolle
  erstellen
    Device Security (Rolle), 219
    Network Security (Rolle), 220
  mit Befehl `usermod` zuweisen, 224–225
  zugewiesene Rolle verwenden, 232–233
Rolle annehmen, System Administrator, 231–232
Rollen
  ändern, 236–238
  angepasste Rollen hinzufügen, 223–224
  annehmen, 230–232, 232–233
  Berechtigungen zuweisen, 271–272
  Beschreibung, 199–200
  direkt zugewiesene Berechtigungen festlegen, 276
  Eigenschaften ändern, 236–238
  empfohlene Rollen, 190
  erstellen
    Crypto Management (Rolle), 225
    Custom Operator (Rolle), 223–224
    DHCP Management (Rolle), 220
    für bestimmte Profile, 218–221
    Operator (Rolle), 219
    Rolle mit beschränktem Bereich, 220
    `root`-Rolle, 226–229
    sicherheitsbezogene Rollen, 219–220
    System Administrator (Rolle), 219
    über Befehlszeile, 221–224
  Fehlerbehebung, 220

Rollen *(Fortsetzung)*
für bestimmte Profile hinzufügen, 218–221
für den Zugriff auf Hardware verwenden, 80–81
in einem Terminalfenster annehmen, 200
in RBAC verwenden, 190
in Solaris Management Console annehmen, 232–233
in Terminalfenster annehmen, 230–232
lokale Rollen auflisten, 230, 262
nach Anmeldung annehmen, 199
Passwort ändern, 234–236
privilegierte Befehle einer Rolle festlegen, 278–280
prüfen, 225–226
Rolle "Primary Administrator" annehmen, 231
Rolle "System Administrator" annehmen, 231–232
`root`-Benutzer in Rolle umwandeln, 226–229
`root`-Rolle annehmen, 231
über Befehlszeile hinzufügen, 221–224
zugewiesene Rolle verwenden, 230–232
Zusammenfassung, 193
Zuweisung eines Benutzers ändern, 220
`Rollen` (Befehl), verwenden, 230
Rollenbasierte Zugriffssteuerung, *Siehe* RBAC
`root` (Benutzer), in RBAC ersetzen, 199
`root` (Hauptelement), zu Schlüsseltabelle eines Hosts hinzufügen, 560
`root` (Konto), Beschreibung, 45
Root (Rolle)
empfohlene Rolle, 191
verfügbare Rolle, 191
`root`-Benutzer
Anmeldungen überwachen, 50
in `root`-Rolle ändern, 226–229
Remote-Zugriff beschränken, 78–80
`root`-Rolle ändern, 228
Versuche mit dem Befehl `su`, 50
Versuche mit dem Befehl `su` überwachen, 78
Zugriff beschränken, 56–57
Zugriffsversuche auf Konsole anzeigen, 78–80
`root`-Rolle (RBAC)
Fehlerbehebung, 229
Rolle annehmen, 231
zurück in `root`-Benutzer umwandeln, 228
RPCSEC_GSS API, Kerberos, 423
`RSA` (Kernel-Provider), 310
`RSAAuthentication` (Schlüsselwort), Secure Shell, 396
`rsh` (Befehl)
Kerberos, 579–581, 589
`rsh` (Befehl, eingeschränkte Shell), 51
`rshd` (Dämon), Kerberos, 590
`rstchown` Systemvariable, 145

S

`-S` (Option), `st_clean` (Skript), 105
`-s` (Option)
`audit` (Befehl), 690
`praudit` (Befehl), 694
Safe (Schutzebene), 581
SASL
Optionen, 363–364
Plugins, 362
Übersicht, 361
Umgebungsvariable, 362
`saslauthd_path` (Option), SASL, 363
Schlüssel
Definition in Kerberos, 592
DH-Schlüssel für NIS-Benutzer erstellen, 344–345
für MAC verwenden, 306
für Secure Shell erstellen, 376–378
für Secure Shell generieren, 376–378
Serviceschlüssel, 560–567
Sitzungsschlüssel
Kerberos-Authentifizierung, 598
symmetrischen Schlüssel generieren
mit Befehl `dd`, 298–300
mit Befehl `pktool`, 301–304
Schlüsselserver, starten, 341
Schlüsselspeicher
Inhalt auflisten, 327
mit Passwort in KMF schützen, 330–331
von KMF unterstützt, 324, 325
von KMF verwaltet, 324
Zertifikate exportieren, 329–330
Zertifikate importieren, 327–329
Schlüsseltabellendatei
erstellen, 440, 448

Schlüsseltabellendatei *(Fortsetzung)*
Hauptelemente mit dem Befehl `ktremove` entfernen, 564
Host-Hauptelement von Master-KDC hinzufügen, 442, 450
Inhalt anzeigen `ktutil` (Befehl), 564
Inhalt mit dem Befehl `ktutil` anzeigen, 565
mit Befehl `ktutil` verwalten, 561
mit Befehl `read_kt` in Schlüsseltabellenpuffer einlesen, 565, 566
Schlüssellistenpuffer mit Befehl `list` anzeigen, 565, 566
Service eines Hosts mit dem Befehl `delete_entry` deaktivieren, 566
Service-Hauptelement entfernen, 564
Service-Hauptelement hinzufügen, 560, 562–563
verwalten, 560–567
Schlüsselwörter
Siehe auch spezifisches Schlüsselwort
Attribut in BART, 127
Befehlszeilenüberschreibungen in Secure Shell, 402
Secure Shell, 393–397
Schreibberechtigungen, symbolischer Modus, 137
Schutzebene
clear, 581
festlegen in `ftp`, 581
private, 581
safe, 581
Schützen
Anmeldungen (Übersicht der Schritte), 64
BIOS, Zeiger, 80–81
Dateien mit kryptografischem Framework, 298
durch Passwörter mit kryptografischem Framework, 325–326
Inhalt des Schlüsselspeichers, 330
Passwörter (Übersicht der Schritte), 64
PROM, 80–81
System vor gefährlichen Programmen, 155–157
Schützen von Dateien
Benutzerverfahren, 143–149
mit ACLs, 149–154
mit ACLs (Übersicht der Schritte), 149
mit UFS-ACLs, 138–141
mit UNIX-Berechtigungen, 131–138, 143–149
Schützen von Dateien *(Fortsetzung)*
mit UNIX-Berechtigungen (Übersicht der Schritte), 143
Übersicht der Schritte, 142
`scp` (Befehl)
Beschreibung, 402
Dateien kopieren, 384–385
SCSI-Geräte, `st_clean` (Skript), 104
SEAM-Tool
Anmeldefenster, 531
Attribute eines Hauptelements anzeigen, 536–538
Auswirkungen von Berechtigungen, 559
Befehlszeilenäquivalente, 529–530
Berechtigungen, 559
Beschreibungen der Fensterbereiche, 555–558
Dateien geändert, 530
eingeschränkte Administratorberechtigungen, 558–560
Filtermuster (Feld), 535
`gkadmin` (Befehl), 527
`.gkadmin` (Datei), 530
Hauptelement ändern, 542–543
Hauptelement duplizieren, 541
Hauptelement löschen, 543
Hilfe, 530
Hilfeinhalt, 530
`kadmin` (Befehl), 527
kontextbezogene Hilfe, 530
Liste der Hauptelemente anzeigen, 534–536
Liste der Richtlinien anzeigen, 547–549
Listenberechtigungen, 559
neue Richtlinie erstellen, 538, 551–552
neues Hauptelement erstellen, 538–540
oder Befehl `kadmin`, 528
Onlinehilfe, 530
Richtlinie ändern, 553–554
Richtlinien löschen, 554–555
Richtlinienattribute anzeigen, 549–551
Standardwerte, 532
Standardwerte für Hauptelemente einrichten, 543–544
starten, 531–532
Tabelle der Fensterbereiche, 555–558
Teilliste von Hauptelementen anzeigen, 535

SEAM-Tool *(Fortsetzung)*
Übersicht, 528–532
X Window-System, 529–530
Secure by Default (Installationsoption), 53
Secure NFS, 336
Secure RPC
Alternative, 59
Beschreibung, 335
Implementierung, 337–340
Kerberos, 336
keyserver, 337
Übersicht, 58–60
Secure Shell
(Dateien), 399
Änderungen in der aktuellen Version, 368–369
Authentifizierung
Anforderungen, 366–368
Authentifizierung mithilfe von öffentlichen Schlüsseln, 366
Authentifizierungsmethoden, 366–368
Authentifizierungsschritte, 390–391
Basis von OpenSSH, 368–369
Befehlsausführung, 391–392
bei Remote-Host anmelden, 379–380
Benutzerverfahren, 375–376
Beschreibung, 365
Clients konfigurieren, 392
Dateien kopieren, 384–385
Datenweiterleitung, 391–392
Identitätsdateien benennen, 399
lokale Port-Weiterleitung, 383–384, 384
Mail weiterleiten, 383–384
ohne Kennwort verwenden, 380–381
Pakete, 398
Passwortsatz ändern, 378–379
Port-Weiterleitung konfigurieren, 374–375
Port-Weiterleitung verwenden, 382–384
Protokollversionen, 366
Remote-Port-Weiterleitung, 384
Schlüssel erstellen, 376–378
Schlüssel generieren, 376–378
Schlüsselwörter, 393–397
`scp` (Befehl), 384–385
Server konfigurieren, 392
Secure Shell *(Fortsetzung)*
TCP, 374
typische Sitzung, 389–392
über Firewall verbinden, 385
Übersicht der Schritte für Administratoren, 370
Variablen für die Anmeldeumgebung, 397
Verbindung zu Host außerhalb der Firewall herstellen
über Befehlszeile, 386–387
Verbindungen zu externem Host herstellen
Konfigurationsdatei, 385–387
verwalten, 389–392
weniger Aufforderungen zur Anmeldung, 380–381
zum System hinzufügen, 398
Sekundäres Prüfverzeichnis, 697
Semikolon (;)
`device_allocate` (Datei), 102
Trennzeichen für Sicherheitsattribute, 260
`sendmail` (Befehl), Autorisierungen erforderlich, 263
`seq` (Prüfrichtlinie)
Beschreibung, 631
Token `sequence`, 725
und Token `sequence`, 631
`sequence` (Prüf-Token)
Format, 725
Prüfrichtlinie `seq`, 725
Server
`AUTH_DH`-Client-Server-Sitzung, 337–340
Berechtigungsnachweis abrufen, 600–601
Bereiche, 414
Definition in Kerberos, 591
für Secure Shell konfigurieren, 392
Zugriff mit Kerberos erhalten, 598–602
Service
auf einem Host deaktivieren, 565–567
Definition in Kerberos, 591
Zugriff auf bestimmten Service abrufen, 601–602
Service-Hauptelement
aus Schlüsseltabellendatei entfernen, 564
Beschreibung, 413
zu Schlüsseltabellendatei hinzufügen, 560, 562–563
Service-Hauptelementname, Namen planen, 428
Service Management Facility
kryptografisches Framework aktualisieren, 313

Service Management Facility *(Fortsetzung)*
kryptografisches Framework neu starten, 321–322
Schlüsselserver aktivieren, 341
Secure Shell neu starten, 375
Service Management Facility (SMF), *Siehe* SMF
Serviceschlüssel
Definition in Kerberos, 592
Schlüsseltabellendateien, 560–567
`setfacl` (Befehl)
Beispiele, 152–153
Beschreibung, 141
`-d` (Option), 153
`-f` (Option), 152
Syntax, 150–151
`setgid`-Berechtigungen
absoluter Modus, 138, 149
Beschreibung, 135
Sicherheitsrisiken, 135
symbolischer Modus, 137
`setpin` (Unterbefehl), `pktool` (Befehl), 330–331
`setuid`-Berechtigungen
absoluter Modus, 138, 149
Beschreibung, 134–135
Dateien mit eingestellten Berechtigungen suchen, 155
Sicherheitsrisiken, 52, 134
symbolischer Modus, 137
`sftp` (Befehl)
Beschreibung, 402
Dateien kopieren, 385
Dateiübertragungen prüfen, 687–688
`sh` (Befehl), privilegierte Version, 200
`SHA1` (Kernel-Provider), 310
Shell, privilegierte Versionen, 200
Shell-Befehle
`/etc/d_passwd`-Dateieinträge, 47
Nummer des übergeordneten Shell-Prozesses weitergeben, 267
Shell-Prozess, Berechtigungen auflisten, 267–268
Shell-Skripten, privilegierte schreiben, 274
`.shosts` (Datei), Beschreibung, 400
`shosts.equiv` (Datei), Beschreibung, 400
Sichere Verbindung
anmelden, 379–380
Sichere Verbindung *(Fortsetzung)*
Firewall, 385
Sicherheit
BART, 107–129
Dateien verschlüsseln, 307–309
DH-Authentifizierung, 337–340
Digest von Dateien berechnen, 304–305
Geräte, 47–49
Geräte schützen, 104–105
Hardware schützen, 80–82
Installationsoptionen, 53
Kerberos-Authentifizierung, 467
Key Management Framework, 323–331
kryptografisches Framework, 289–295
MAC von Dateien berechnen, 305–306
`netservices limited` (Installationsoption), 53
NFS-Client-Server, 337–340
Passwortverschlüsselung, 43
PROM schützen, 80–82
Prüfung, 612
Remote-Anmeldung verhindern, 78–80
Richtlinienübersicht, 35–36
Schutz vor Denial of Service, 54
Schutz vor Trojanern, 51
Secure by Default, 53
Secure Shell, 365–387
Systeme, 39
Systemhardware, 80–82
unsicheres Netzwerk, 385
Verweis auf JASS-Toolkit, 53
Sicherheitsattribute
Berechtigungen in Befehlen, 197
Beschreibung, 193
für Einhängen zugeordneter Geräte, 89
Network Security (Berechtigungsprofil), 195
prüfen, 197
spezielle ID in Befehlen, 197
Überlegungen bei direkter Zuweisung, 201
Sicherheitsmechanismus, mit der Option `-m` angeben, 580
Sicherheitsmodi, Umgebung mit mehreren einrichten, 466–468
Sicherheitsrichtlinie, Standard (RBAC), 254
Sicherheitsservice, Kerberos, 415

Sichern
Netzwerk bei Installation, 53
Skripten, 244
Signal beim Herunterfahren der Prüfung, 701
Signieren von Providern, kryptografisches Framework, 294
Single Sign-On-System, 578–585
Kerberos, 407
Sitzungs-ID, Prüfung, 707
Sitzungsschlüssel
Definition in Kerberos, 592
Kerberos-Authentifizierung, 598
Skripten
`audit_startup` (Skript), 699
`audit_warn` (Skript), 700
auf RBAC-Autorisierungen überprüfen, 244
Ausgabe `praudit` verarbeiten, 694–695
Beispiel für Überwachung der Prüfdateien, 635
Bereinigungsskripten
Siehe auch Bereinigungsskripten
`bsmconv` (Effekt), 696
`bsmconv` (Skript), 701
`bsmconv` für Gerätezuordnung, 88
`bsmconv` zum Aktivieren der Prüfung, 656–657
Geräte bereinigen, 104–105
mit Berechtigungen ausführen, 210
sichern, 244
Verwendung von Berechtigungen, 274
`slave_datatrans` (Datei)
Beschreibung, 588
KDC-Weitergabe, 489–490
`slave_datatrans_`*slave* (Datei), Beschreibung, 589
Slave-KDCs
Definition, 591
gegen Master-KDC austauschen, 484–489
konfigurieren, 451–455
Master, 437
Master-KDC, 414
planen, 429
Slot, Definition im kryptografischen Framework, 292
Smartcard-Dokumentation, Verweis auf, 34
`smattrpop` (Befehl), Beschreibung, 262
`smexec` (Befehl), Beschreibung, 262
SMF
Siehe auch Service Management Facility
`kcfd` (Service), 293
Konfiguration "Secure by Default" verwalten, 53
Service des kryptografischen Framework, 293
`ssh`-Service, 375
`smmultiuser` (Befehl), Beschreibung, 262
`smprofile` (Befehl)
Berechtigungsprofil ändern, 239
Beschreibung, 262
`smrole` (Befehl)
Beschreibung, 262
Eigenschaften einer Rolle ändern, 235, 237
verwenden, 223–224
`smuser` (Befehl)
Beschreibung, 262
RBAC-Eigenschaften eines Benutzers ändern, 242
`socket` (Prüf-Token), 725–726
soft (Zeichenfolge), `audit_warn` (Skript), 700
`solaris` (Sicherheitsrichtlinie), 259
`solaris.device.revoke` (Autorisierung), 101
Solaris-Prüfung (Übersicht der Schritte), 637
Speichern
Passwortsatz, 307
Prüfdateien, 626, 649–653
Speicherplatzanforderungen, 634–635
Speicherungsaufwand, und Prüfung, 634–635
`sr_clean` (Skript), Beschreibung, 105
`ssh` (Befehl)
Beschreibung, 401
Port-Weiterleitungsoptionen, 382–384
Proxy-Befehl verwenden, 386–387
Schlüsselworteinstellungen überschreiben, 402
verwenden, 379–380
`ssh-add` (Befehl)
Beispiel, 380–381, 381
Beschreibung, 401
private Schlüssel speichern, 380–381
`ssh-agent` (Befehl)
Beschreibung, 401
für CDE konfigurieren, 381–382
in Befehlszeile, 380–381
in Skripten, 381–382

.ssh/config (Datei)
  Beschreibung, 400
  Überschreibung, 400
ssh_config (Datei)
  Hostspezifische Parameter, 396
  Schlüsselwörter, 393–397
    Siehe spezifisches Schlüsselwort
  Secure Shell konfigurieren, 392
  Überschreibung, 400
.ssh/environment (Datei), Beschreibung, 400
ssh_host_dsa_key (Datei), Beschreibung, 399
ssh_host_dsa_key.pub (Datei), Beschreibung, 399
ssh_host_key (Datei)
  Beschreibung, 399
  Überschreibung, 400
ssh_host_key.pub (Datei), Beschreibung, 399
ssh_host_rsa_key (Datei), Beschreibung, 399
ssh_host_rsa_key.pub (Datei), Beschreibung, 399
.ssh/id_dsa (Datei), 401
.ssh/id_rsa (Datei), 401
.ssh/identity (Datei), 401
ssh-keygen (Befehl)
  Beschreibung, 401
  verwenden, 376–378
ssh-keyscan (Befehl), Beschreibung, 401
ssh-keysign (Befehl), Beschreibung, 402
.ssh/known_hosts (Datei)
  Beschreibung, 399
  Überschreibung, 401
ssh_known_hosts (Datei), 399
.ssh/rc (Datei), Beschreibung, 400
sshd (Befehl), Beschreibung, 401
sshd_config (Datei)
  Beschreibung, 399
  Schlüsselwörter, 393–397
    Siehe spezifisches Schlüsselwort
  Überschreibungen für Einträge in
    /etc/default/login, 397
sshd.pid (Datei), Beschreibung, 399
sshrc (Datei), Beschreibung, 400
st_clean (Skript)
  Bandlaufwerke, 104
  Beschreibung, 104
Standard, Berechtigungseinstellungen in policy.conf
  (Datei), 282
Standardmäßige Bereinigung, st_clean (Skript), 105
Standardwerte
  ACL-Einträge für Verzeichnisse, 140–141
  audit_startup (Skript), 699
  praudit (Ausgabeformat), 694
  systemweit in Datei policy.conf, 43
  systemweite Prüfung, 703
  umask-Wert, 135–136
Starten
  ASET regelmäßig ausführen, 180
  ASET von Shell, 160
  Gerätezuordnung, 88–89
  interaktiv, von ASET, 178–179
  KDC-Dämon, 455, 499
  Prüfdämon, 660
  Prüfung, 656–657
  Schlüsselserver mit Secure RPC, 341
Stash-Datei
  Definition, 591
  erstellen, 455, 499
Sternchen (*)
  device_allocate (Datei), 102, 103
  in RBAC-Autorisierungen überprüfen, 245
  Platzhalterzeichen
    in ASET, 175, 177
    in RBAC-Autorisierungen, 252, 256
Steuern
  Systemverwendung, 50–55
  Systemzugriff, 63–64
  Zugriff auf Systemhardware, 80
Steuerungs-Manifeste (BART), 107
Sticky Bit-Berechtigungen
  absoluter Modus, 138, 149
  Beschreibung, 135
  symbolischer Modus, 137
StrictHostKeyChecking (Schlüsselwort), ssh_config
  (Datei), 396
StrictModes (Schlüsselwort), sshd_config
  (Datei), 396
su (Befehl)
  in Rollenannahme, 230–232, 232–233
  Verwendung überwachen, 78

su (Befehl) *(Fortsetzung)*
Zugriffsversuche auf Konsole anzeigen, 78–80
su-Datei, Versuche mit dem Befehl su überwachen, 78
subject (Prüf-Token), Format, 726–727
Subsystem (Schlüsselwort), sshd_config (Datei), 396
sufficient (Steuer-Flag), PAM, 356
sulog (Datei), 78
Inhalt überwachen, 78
Sun Crypto Accelerator 1000-Board, Mechanismen auflisten, 319–321
Sun Crypto Accelerator 6000-Board
Hardware-Plugin zu kryptografischem Framework, 290
Mechanismen auflisten, 318–319
SUPATH in Secure Shell, 397
Superuser
Fehlerbehebung bei Umwandlung in root-Rolle, 229
Fehlerbehebung für Remote-Zugriff, 79
in RBAC entfernen, 199
Unterschiede zum Berechtigungsmodell, 204
verglichen mit Berechtigungsmodell, 201–211
verglichen mit RBAC-Modell, 190–193
Zugriffsversuche überwachen, 78–80
suser (Sicherheitsrichtlinie), 259
svcadm (Befehl)
Dämon syslog neu starten, 642
kryptografisches Framework aktualisieren, 313–314
kryptografisches Framework verwalten, 292, 293
Name Service neu starten, 218
Neu starten
Secure Shell, 375
neu starten
syslog (Dämon), 69
NFS-Server neu starten, 651
Schlüsselserver-Dämon aktivieren, 341
svcadm-Befehl, kryptografisches Framework aktivieren, 321–322
svcs (Befehl), Schlüsselserver-Service auflisten, 341
svcs-Befehl), kryptografische Services auflisten, 321–322
Symbolische Links, Dateiberechtigungen, 133
Symbolischer Modus
Beschreibung, 136
Symbolischer Modus *(Fortsetzung)*
Dateiberechtigungen ändern, 137, 146
Synchronisieren von Uhren
Master-KDC, 443, 451
Slave-KDC, 455, 499
Übersicht, 482–483
SYS Berechtigungen, 203
sysconf.rpt (Datei), 163, 166
syslog (Format), Prüfdatensätze, 696
syslog.conf (Datei)
audit.notice (Ebene), 642
ausführbare Stack-Meldungen, 142
fehlgeschlagene Anmeldeversuche aufzeichnen, 68–70
kern.notice (Ebene), 142
priv.debug (Eintrag), 283
Prüfdatensätze, 612
Prüfung, 696
SYSLOG_FAILED_LOGINS
in Secure Shell, 397
Systemvariablen, 69
SyslogFacility (Schlüsselwort), sshd_config (Datei), 396
system (Datei), bsmconv (Effekt), 696
System Administrator (RBAC)
Berechtigungsprofil, 249
empfohlene Rolle, 191
Rolle annehmen, 231–232
Rolle erstellen, 219
system state (Prüfklasse), 704
System V IPC
Berechtigungen, 203
ipc (Prüf-Token), 719–720
ipc (Prüfklasse), 704
ipc_perm (Prüf-Token), 720
system-wide administration (Prüfklasse), 704
Systemadministrator (RBAC), Hardware, 80
Systemaufrufe
arg (Prüf-Token), 714
close, 704
exec_args (Prüf-Token), 715–716
exec_env (Prüf-Token), 716
ioctl(), 704
ioctl für Audiogerätbereinigung, 105

Systemaufrufe *(Fortsetzung)*
`return` (Prüf-Token), 724
Systeme, vor gefährlichen Programmen schützen, 155–157
Systemeigenschaften, Berechtigungen mit Bezug auf, 203
Systemhardware, Zugriff steuern, 80–82
Systemsicherheit
Anmeldezugriffsbeschränkungen, 41
anzeigen
Anmeldestatus eines Benutzers, 65–66
Benutzer ohne Passwort, 66
Befehl `su` überwachen, 78
Berechtigungen, 201–211
eingeschränkte Shell, 51, 52
Einwahl-Passwörter
vorübergehend deaktivieren, 72
Einwahlanmeldungen und -passwörter, 46–47
fehlgeschlagene Anmeldeversuche aufzeichnen, 67–68
Firewallsysteme, 60–61
Hardwareschutz, 40–41, 80–82
Passwörter, 42
Passwortverschlüsselung, 43
Rechnerzugriff, 40–41
rollenbasierte Zugriffssteuerung (RBAC), 50, 190–193
`root`-Zugriff über Remote-Systeme, 78–80
`root`-Zugriffsbeschränkungen, 56–57, 78–80
Spezielle Konten, 45
Übersicht, 39, 40
Übersicht der Schritte, 155
UFS-ACLs, 138–141
Verwendung des Befehls `su` überwachen, 50
vor gefährlichen Programmen schützen, 155–157
Zugriff, 39
Systemvariable, `noexec_user_stack`, 157
Systemvariablen
Siehe auch Variablen
`CRYPT_DEFAULT`, 73
`KEYBOARD_ABORT`, 81–82
`noexec_user_stack_log`, 157
`rstchown`, 145
`SYSLOG_FAILED_LOGINS`, 69

T

Tabellen, `gsscred`, 604–605
`tail` (Befehl), Bespiel für Verwendung, 635
`TASKS` (Variable bei ASET), 175
`TASKS` Variable (ASET), 169
`taskstat` (Befehl bei ASET), 161, 165
TCP
Adressen, 720
Secure Shell, 374, 391–392
`telnet` (Befehl)
Kerberos, 579–581, 589
`telnetd` (Dämon), Kerberos, 590
Terminal-ID, Prüfung, 707
Terminologie
authentifizierungsspezifisch, 591–592
Kerberos, 591–598
Kerberos-spezifisch, 591
`text` (Prüf-Token), Format, 728
TGS, Berechtigungsnachweis erhalten für, 599
TGT, Kerberos, 409–411
Ticket-gewährender Service, *Siehe* TGS
Ticket-gewährendes Ticket, *Siehe* TGT
Ticketdatei, *Siehe* Berechtigungsnachweis-Cache
Tickets
abrufen, 569–570
anfänglich, 593
anzeigen, 571–572
Datei
Siehe Berechtigungsnachweis-Cache
Definition, 408
Definition in Kerberos, 592
erneuerbar, 594
erstellen, 569–570
`-F` (Option) oder `-f` (Option), 580
für einen bestimmten Bereich anfordern, 580
`-k` (Option), 580
`klist` (Befehl), 571–572
Lebensdauer, 595–596
löschen, 572–573
maximale erneuerbare Lebensdauer, 596
mit `kinit` erstellen, 570–571
nachdatierbar, 593
nachdatiert, 409
oder Berechtigungsnachweise, 409

Tickets *(Fortsetzung)*
Proxy, 594
proxyfähig, 594
Typen, 593–598
ungültig, 593
Warnung vor Ablauf, 476
weiterleitbar, 409, 570, 581–582, 593
`TIMEOUT` in Secure Shell, 397
`/tmp/krb5cc_`*UID* (Datei), Beschreibung, 588
`/tmp/ovsec_adm.`*xxxxx* (Datei), Beschreibung, 588
tmpfile (Zeichenfolge), `audit_warn` (Skript), 701
TMPFS-Dateisystem, Sicherheit, 135
Token, Definition im kryptografischen Framework, 292
`trail` (Prüfrichtlinie)
Beschreibung, 631
und Token `trailer`, 631
`trailer` (Prüf-Token)
Format, 728–729
`praudit` (Anzeige), 729
Reihenfolge in Prüfdatensatz, 728–729
Transparenz, Definition in Kerberos, 408
Trojaner, 51
`truss` (Befehl), zur Fehlersuche bei Berechtigungen, 269
tune-Dateien (ASET)
ändern, 171
Beispiele, 176, 177
Beschreibung, 167
Regeln, 177
`tune.rpt` (Datei), 162, 166
Typen von Tickets, 593–598
`TZ` in Secure Shell, 397

U

`-U` (Option)
`allocate` (Befehl), 101
`list_devices` (Befehl), 100
`uauth` (Prüf-Token), 622, 729
Übersicht der Schritte
Anmeldungen und Passwörter schützen, 64
ASET, 178–182
ASET ausführen, 178–182
Übersicht der Schritte *(Fortsetzung)*
BART verwenden (Übersicht der Schritte), 111
Berechtigungen verwalten und verwenden, 265
Dateien mit ACLs schützen, 149
Dateien mit kryptografischen Mechanismen schützen, 298
Dateien mit UNIX-Berechtigungen schützen, 143
Dateien schützen, 142
Fehlerbehebung bei der Solaris-Prüfung, 675–688
Geräte, 83
Geräte konfigurieren, 83
Geräte zuordnen, 93
Geräterichtlinie, 84
Geräterichtlinie konfigurieren, 84
Geräterichtlinie verwalten, 84
Gerätezuordnung, 87–88
Gerätezuordnung verwalten, 87–88
Gerätezuordnung verwenden, 93
Hauptelemente verwalten (Kerberos), 532–533
Kerberos-Konfiguration, 435–436
Kerberos-NFS-Server konfigurieren, 461
Kerberos-Wartung, 436
kryptografisches Framework, 297–298
kryptografisches Framework verwalten, 309–310
kryptografisches Framework verwenden, 297–298
PAM, 350
Prüfdateien konfigurieren, 638
Prüfdatensätze verwalten, 665
Prüfservice aktivieren, 648–649
Prüfservice konfigurieren, 648–649
Prüfung, 637
Prüfung planen, 623
RBAC konfigurieren, 214–215
RBAC verwalten, 233–234
RBAC verwenden, 213–214
Richtlinien verwalten (Kerberos), 546–547
Rollen verwenden, 229
Secure RPC verwalten, 340–341
Secure Shell, 370
Secure Shell konfigurieren, 370
Secure Shell verwenden, 375–376
Standardalgorithmus für Passwortverschlüsselung ändern, 72–73
Superuser überwachen und beschränken, 77

Übersicht der Schritte *(Fortsetzung)*
Systeme sichern, 63–64
Systemhardware schützen, 80
Systemzugriff, 63–64
Verwenden von Key Management Framework (Übersicht der Schritte), 325–326
vor Programmen mit Sicherheitsrisiko schützen, 155
Zugriff auf Systemhardware steuern, 80
Überwachen
fehlgeschlagene Anmeldungen, 67–68
Prüfpfad in Echtzeit, 635
Superuser (Übersicht der Schritte), 77
Superuser-Zugriffsversuche, 78–80
Systemverwendung, 54, 55
Versuche mit dem Befehl `su`, 50, 78
Verwendung privilegierter Befehle, 225–226
UDP
Adressen, 720
für Remote-Prüfprotokolle verwenden, 618
Port-Weiterleitung, 374
Secure Shell, 374
Uhrdifferenz
Kerberos, 482–483
Kerberos planen, 431
Uhren synchronisieren
Kerberos-Master-KDC, 443, 451
Kerberos-Slave-KDC, 455
Kerberos-Slave-Server, 499
Uhrsynchronisierung, Kerberos planen, 431
`uid_aliases` (Datei bei ASET), 167, 170
`UID_ALIASES` (Variable bei ASET), 168, 170, 175
`umask`-Wert
Dateierstellung, 135–136
typische Einstellungen, 136
Umgebungsvariable, `ASETSECLEVEL` (ASET), 174
Umgebungsvariablen
Siehe auch Variablen
`ASETDIR` (ASET), 174
`CKLISTPATH_level` (ASET), 170, 176
in Prüfdatensätzen, 711
in Prüfdatensätzen vorhanden, 630
mit Befehl `ssh-agent` verwenden, 401
`PATH`, 51
Umgebungsvariablen *(Fortsetzung)*
`PERIODIC_SCHEDULE` (ASET), 170, 174
Proxy-Server und Ports überschreiben, 386
Prüf-Token, 716
Secure Shell, 397
`TASKS` (ASET), 169, 175
Übersicht (ASET), 173
`UID_ALIASES` (ASET), 168, 170, 175
`YPCHECK` (ASET), 171, 175
Umleitungspfeil (>), Umleitung verhindern, 52
`umount` (Befehl), mit Sicherheitsattributen, 89
Ungültiges Ticket, Definition, 593
UNIX-Dateiberechtigungen, *Siehe* Dateien, Berechtigungen
Unterer Grenzwert
`audit_warn` (Bedingung), 700
Beschreibung der Zeile `minfree`, 697
Unverarbeitetes `praudit`-Ausgabeformat, 694
`update_drv` (Befehl)
Beschreibung, 98
verwenden, 85–86
`upriv` (Prüf-Token), 729
URL für Onlinehilfe, Graphical Kerberos Tool, 434
`use_authid` (Option), SASL, 364
`UseLogin` (Schlüsselwort), `sshd_config` (Datei), 396
`UseOpenSSLEngine` (Schlüsselwort), Secure Shell, 396
`UsePrivilegedPort` (Schlüsselwort), Secure Shell, 396
`User` (Schlüsselwort), `ssh_config` (Datei), 396
User Accounts (Tool), Beschreibung, 241–243
`user administration` (Prüfklasse), 704
`user_attr` (Datenbank)
Beschreibung, 253, 255–256
`defaultpriv` (Schlüsselwort), 283
`limitpriv` (Schlüsselwort), 283
`privs` (Schlüsselwort), 283
RBAC-Beziehungen, 254–255
`useradd` (Befehl)
Beschreibung, 262
lokalen Benutzer hinzufügen, 226
`userdel` (Befehl), Beschreibung, 262
`UserKnownHostsFile` (Schlüsselwort), `ssh_config` (Datei), 396
`UserKnownHostsFile2` (Schlüsselwort), *Siehe* `UserKnownHostsFile` (Schlüsselwort)

usermod (Befehl)
  Beschreibung, 262
  RBAC-Eigenschaften eines Benutzers ändern, 242
  zum Zuweisen einer Rolle verwenden, 224–225
UseRsh (Schlüsselwort), ssh_config (Datei), 396
/usr/aset (Verzeichnis), 160
/usr/aset/asetenv (Datei), 168, 169
/usr/aset/masters/tune (Dateien)
  ändern, 171
  Beschreibung, 167
  Regeln, 177
/usr/aset/masters/uid_aliases (Datei), 167
/usr/aset/reports (Verzeichnis), Struktur, 166
/usr/aset/reports/latest (Verzeichnis), 166
/usr/aset/reports Verzeichnisstruktur, 165
/usr/bin/ftp (Befehl), Kerberos, 589
/usr/bin/kdestroy (Befehl), Kerberos, 589
/usr/bin/kinit (Befehl), Kerberos, 589
/usr/bin/klist (Befehl), Kerberos, 589
/usr/bin/kpasswd (Befehl), Kerberos, 589
/usr/bin/ktutil (Befehl), Kerberos, 589
/usr/bin/rcp (Befehl), Kerberos, 589
/usr/bin/rdist (Befehl), Kerberos, 589
/usr/bin/rlogin (Befehl), Kerberos, 589
/usr/bin/rsh (Befehl), Kerberos, 589
/usr/bin/telnet (Befehl), Kerberos, 589
/usr/lib/kprop (Befehl), Beschreibung, 589
/usr/lib/krb5/kadmind (Dämon), Kerberos, 590
/usr/lib/krb5/kpropd (Dämon), Kerberos, 590
/usr/lib/krb5/krb5kdc (Dämon), Kerberos, 590
/usr/lib/krb5/ktkt_warnd (Dämon), Kerberos, 590
/usr/lib/libsasl.so (Bibliothek), Übersicht, 361
/usr/sbin/gkadmin (Befehl), Beschreibung, 589
/usr/sbin/gsscred (Befehl), Beschreibung, 589
/usr/sbin/in.ftpd (Dämon), Kerberos, 590
/usr/sbin/in.rlogind (Dämon), Kerberos, 590
/usr/sbin/in.rshd (Dämon), Kerberos, 590
/usr/sbin/in.telnetd (Dämon), Kerberos, 590
/usr/sbin/kadmin (Befehl), Beschreibung, 589
/usr/sbin/kadmin.local (Befehl), Beschreibung, 590
/usr/sbin/kclient (Befehl), Beschreibung, 590
/usr/sbin/kdb5_ldap_util (Befehl),
  Beschreibung, 590
/usr/sbin/kdb5_util (Befehl), Beschreibung, 590
/usr/sbin/kgcmgr (Befehl), Beschreibung, 590
/usr/sbin/kproplog (Befehl), Beschreibung, 590
/usr/share/lib/xml (Verzeichnis), 694
usrgrp.rpt (Datei)
  Beispiel, 166
  Beschreibung, 163, 166
uucico (Befehl), Anmeldeprogramm, 71

V

v1-Protokoll, Secure Shell, 366
-v (Option)
  audit (Befehl), 640
  digest (Befehl), 304
  mac (Befehl), 305
  ppriv (Befehl), 267
v2-Protokoll, Secure Shell, 366
/var/adm/auditlog (Datei), Prüfdatensätze im
  Textformat, 642
/var/adm/loginlog (Datei), fehlgeschlagene
  Anmeldeversuche aufzeichnen, 67–68
/var/adm/messages (Datei)
  ausführbare Stack-Meldungen, 142
  Fehlerbehebung bei Prüfung, 678
/var/adm/sulog (Datei), Inhalt überwachen, 78
/var/krb5/.k5.*REALM* (Datei), Beschreibung, 588
/var/krb5/kadmin.log (Datei), Beschreibung, 588
/var/krb5/kdc.log (Datei), Beschreibung, 588
/var/krb5/principal (Datei), Beschreibung, 588
/var/krb5/principal.kadm5 (Datei),
  Beschreibung, 588
/var/krb5/principal.kadm5.lock (Datei),
  Beschreibung, 588
/var/krb5/principal.ok (Datei), Beschreibung, 588
/var/krb5/principal.ulog (Datei),
  Beschreibung, 588
/var/krb5/slave_datatrans (Datei),
  Beschreibung, 588
/var/krb5/slave_datatrans_*slave* (Datei),
  Beschreibung, 589
/var/log/authlog (Datei), fehlgeschlagene
  Anmeldungen, 68–70
/var/log/syslog (Datei), Fehlerbehebung bei
  Prüfung, 678

/var/run/sshd.pid (Datei), Beschreibung, 399
Variablen
  ASET-Umgebungsvariablen
    ASETDIR, 174
    ASETSECLEVEL, 174
    CKLISTPATH_level, 168, 170, 176
    PERIODIC_SCHEDULE, 170, 174
    TASKS, 169, 175
    Übersicht, 173
    UID_ALIASES, 168, 170, 175
    YPCHECK, 171, 175
  die einem Befehl zugewiesenen prüfen, 715
  für Proxy-Server und Ports, 386
  in Secure Shell einstellen, 397
  KEYBOARD_ABORT, 81–82
  login und Secure Shell, 397
  noexec_user_stack, 141
  noexec_user_stack_log, 142
  rstchown, 145
  zu Prüfdatensatz hinzufügen, 630, 716
Verarbeitungszeit, Aufwand, von Prüfservice, 633
Verbraucher, Definition im kryptografischen Framework, 291
Vererbbarer Berechtigungssatz, 206
Verhindern
  Einwahl-Anmeldungen, vorübergehend, 72
  Prüfpfadüberlauf, 674–675
  Verwendung von Hardwaremechanismen, 319–321
  Verwendung von Kernel-Modul-Softwareprovidern, 316–318
  Zugriff auf Systemhardware, 80
Verhindern von Speicherüberlauf, Prüfpfad, 674–675
Verhindern von Überlauf, Prüfpfad, 674–675
Verifikatoren
  an NFS-Client zurückgegeben, 340
  Beschreibung, 339
  Fenster, 339
VerifyReverseMapping (Schlüsselwort), ssh_config (Datei), 396
Vermeiden, Sicherheitsrisiken durch ausführbare Dateien, 141–142
Verringern
  Prüfdateien, 667–669, 691
  Speicherplatzanforderungen für Prüfdateien, 635
Verschlüsseln
  Dateien, 55, 298, 307–309
  encrypt-Befehl, 307–309
  Kommunikation zwischen Hosts, 380
  mit Befehlen auf Benutzerebene, 293–294
  Netzwerkverkehr zwischen Hosts, 365–368
  Passwortalgorithmus angeben
    lokal, 72–73
  Passwörter, 72–73
  privaten Schlüssel des NIS-Benutzers, 345
  Secure NFS, 336
Verschlüsselung
  Algorithmen
    Kerberos, 433–434
  Algorithmen in Datei ssh_config angeben, 393
  DES-Algorithmus, 336
  Liste der Passwortalgorithmen, 43
  mit der Option -x, 580
  Modi
    Kerberos, 433–434
  Passwortalgorithmus, 43
  Passwortmodule anderer Anbieter installieren, 76–77
  symmetrischen Schlüssel generieren
    mit Befehl dd, 298–300
    mit Befehl pktool, 301–304
  Typen
    Kerberos, 433–434, 602–604
  Vertraulichkeitsservice, 407
Verschlüsselungen, Passwortalgorithmen für Datei policy.conf angeben, 43
Vertrauenswürdige Hosts, 61
Vertraulichkeit
  Kerberos, 407
  Sicherheitsservice, 415
  Verfügbarkeit, 581
Verwalten
  ACLs, 149–154
  Befehle im kryptografischen Framework, 293
  Berechtigungen, 266
  Berechtigungsprofile, 238–241
  Dateiberechtigungen, 142–143, 143–149
  Eigenschaften einer Rolle, 236–238
  Einwahl-Anmeldungen, 71

Verwalten *(Fortsetzung)*
Geräterichtlinie, 84
Gerätezuordnung, 87–88
Kerberos
Hauptelemente, 532–546
Richtlinien, 546–555
Schlüsseltabellen, 560–567
kryptografisches Framework und Zonen, 295
Metaslot, 293
NFS-Client-Server-Dateisicherheit, 337–340
ohne Berechtigungen, 204
Passwortalgorithmus, 72–73
Prüfung
`auditreduce` (Befehl), 667–669
Aufwandsteuerung, 633
Beschreibung, 610
Effizienz, 635
Prozessvorauswahlmaske, 691
Prüfdateien, 671–673
Prüfdatensätze, 616
Prüfereignisse, 614
Prüfklassen, 615–616, 703
Prüfpfadüberlauf verhindern, 674–675
Speicherplatzanforderungen verringern, 634–635
Übersicht der Schritte, 637
in Zonen, 620–621, 702–703
Prüfung in Zonen, 624–625
RBAC (Übersicht der Schritte), 233–234
RBAC-Eigenschaften, 238–241
Remote-Anmeldungen mit Secure Shell, 376–378
Rollen, 218–221
Rollen zum Ersetzen von Superuser, 215–217
Rollenpasswort, 234–236
Secure RPC (Übersicht der Schritte), 340–341
Secure Shell
Clients, 392
Server, 392
Übersicht, 389–392
Übersicht der Schritte, 370
Übersicht der Schritte des kryptografischen Frameworks, 310
Übersicht der Schritte für Berechtigungen, 266
Verwaltung von Benutzerrechten, *Siehe* Berechtigungen
Verwenden
ACLs, 150–151
`allocate` (Befehl), 93–94
ASET, 178–182
BART, 111
Berechtigungen, 275
`cryptoadm` (Befehl), 310
Dateiberechtigungen, 142–143
`dd` (Befehl), 298–300
`deallocate` (Befehl), 97
`digest`-Befehl, 304–305
`encrypt`-Befehl, 307–309
Gerätezuordnung, 93
`mac`-Befehl, 305–306
`mount` (Befehl), 95
neuen Passwortalgorithmus, 74
`pktool` (Befehl), 301–304
`ppriv` (Befehl), 267
RBAC (Übersicht der Schritte), 213–214
Rollen, 230
Rollen (Übersicht der Schritte), 229
Secure Shell (Übersicht der Schritte), 375–376
`smrole` (Befehl), 272
`ssh-add` (Befehl), 380–381
`ssh-agent` (Dämon), 380–381
`truss` (Befehl), 269
Übersicht der Schritte des kryptografischen Frameworks, 297–298
Übersicht der Schritte für Berechtigungen, 275
`umount` (Befehl), 97
`usermod` (Befehl), 271
Verwenden von Key Management Framework (Übersicht der Schritte), 325–326
Verzeichnisse
Siehe auch Dateien
ACL-Einträge, 140–141
Arbeitsverzeichnis (ASET), 174, 178–179
`audit_control` (Dateidefinitionen), 697
`auditd` (Dämonzeiger), 690
Berechtigungen
Beschreibung, 133
Standardwerte, 135–136

Verzeichnisse *(Fortsetzung)*
Berichte (ASET), 166
Checklisten-Aufgabeneinstellung (ASET), 170, 176
Dateien und verbundene Informationen anzeigen, 132, 143–144
Master-Dateien (ASET), 167
öffentliche Verzeichnisse, 135
Prüfverzeichnisse einhängen, 708
Prüfverzeichnisse voll, 690, 701
Viren
Denial-of-Service-Angriffe, 54
Trojaner, 51
`vnode` (Prüf-Token), Format, 714
`vold` (Dämon), durch Gerätezuordnung deaktiviert, 89
Vorauswahl, Prüfklassen, 639–641
Vorauswahl bei Prüfung, 613
Vorauswahlmaske (Prüfung)
Beschreibung, 707
Speicheraufwand verringern, 691
systemweit, 697

W

`warn.conf` (Datei), Beschreibung, 588
Warnung vor dem Ablauf eines Tickets, 476
Weitergabe
KDC-Datenbank, 431
Kerberos-Datenbank, 489–490
Weiterleitbare Tickets
Beispiel, 570
Beschreibung, 409
Definition, 593
mit der Option `-F`, 580, 581–582
mit der Option `-f`, 579, 581–582
Wiederherstellen, kryptografische Provider, 317
Wiederholte Transaktionen, 339

X

`-X` (Option), kerberisierte Befehle, 580
X Window-System, SEAM-Tool, 529–530
X11-Weiterleitung
in Datei `ssh_config` konfigurieren, 394
in Secure Shell, 391–392
`X11DisplayOffset` (Schlüsselwort), `sshd_config` (Datei), 396
`X11Forwarding` (Schlüsselwort), `sshd_config` (Datei), 396
`X11UseLocalHost` (Schlüsselwort), `sshd_config` (Datei), 396
`-x` (Option)
kerberisierte Befehle, 580
`praudit` (Befehl), 694
`xauth` (Befehl), X11-Weiterleitung, 396
`XAuthLocation` (Schlüsselwort), Secure Shell-Port-Weiterleitung, 396
XML-Format, Prüfdatensätze, 673
XML-Option, `praudit` (Befehl), 694
Xylogics-Bandlaufwerk-Bereinigungsskript, 104

Y

`YPCHECK` (Variable bei ASET), 171, 175

Z

Zeitstempel
ASET-Berichte, 166
Prüfdateien, 709
Zertifikate
für die Verwendung durch ein anderes System exportieren, 329–330
in Schlüsselspeicher importieren, 327–329
mit dem Befehl `pktool gencert` generieren, 326–327
Zitatzeichensyntax in BART, 128
`zone.max-locked-memory` (Ressourcensteuerungen), 189, 205–206
Zonen
Geräte, 48
kryptografische Services und, 321–322
kryptografisches Framework, 295
`perzone` (Prüfrichtlinie), 620–621, 625, 702–703
Prüfung, 702–703

Zonen *(Fortsetzung)*
Prüfung in globaler Zone konfigurieren, 654–655
Prüfung planen, 624–625
Prüfung und, 620–621
`zonename` (Prüfrichtlinie), 625, 702–703
`zonename` (Prüf-Token), 622, 729
`zonename` (Prüfrichtlinie)
Beschreibung, 631
verwenden, 625, 702–703
Zufallszahlen
`dd` (Befehl), 298–300
`pktool` (Befehl), 301–304
Zugelassener Berechtigungssatz, 206
Zugriff
Anmeldungsauthentifizierung mit Secure Shell, 380–381
auf einen bestimmten Service abrufen, 601–602
auf Ihr Konto gewähren, 576–578
auf KDC-Server beschränken, 506–507
Authentifizierung mit Secure RPC, 335
beschränken
Geräte, 47–49, 84
Systemhardware, 80–82
Dateien gemeinsam nutzen, 56
für Server erhalten
Kerberos, 598–602
`root`-Zugriff
Anmeldung verhindern (RBAC), 226–229
beschränken, 56–57, 78–80
Versuche auf Konsole anzeigen, 78–80
Versuche mit dem Befehl `su` überwachen, 50, 78
Sicherheit
ACLs, 55–56
Anmeldezugriffsbeschränkungen, 41
Anmeldungen steuern, 41
Anmeldungsauthentifizierung, 380–381
Dateizugriffsbeschränkungen, 52
fehlgeschlagene Anmeldeversuche aufzeichnen, 67–68
Firewall-Einrichtung, 60–61
Geräte, 84
im Netzwerk steuern, 57–61
NFS-Client-Server, 337–340
`PATH`-Variableneinstellung, 51
Zugriff, Sicherheit *(Fortsetzung)*
periphere Geräte, 47
physische Sicherheit, 40–41
Probleme melden, 62
Remote-Systeme, 365
`root`-Anmeldung verfolgen, 50
`setuid`-Programme, 52
Systemhardware, 80–82
Systemverwendung steuern, 50–55
Systemverwendung überwachen, 54, 55
UFS-ACLs, 138–141
Steuerungslisten
Siehe ACL
Zugriffssteuerungsliste
Siehe ACL
Zugriffssteuerungslisten (ACLs), *Siehe* ACL
Zugriffsteuerungsliste, *Siehe* ACL
Zuordnen
Hostnamen zu Bereichen (Kerberos), 427–428
UIDs zu Kerberos-Hauptelementen, 604–605
Zuordnen von Geräten
Benutzer, 93–94
erzwingen, 90–91
Fehlerbehebung, 94
Übersicht der Schritte, 93
Zuordnen von GSS-Berechtigungsnachweisen, 430
Zuordnungen, Ereignisse zu Klassen (Prüfung), 616
Zusammenführen, binäre Prüfdatensätze, 667–669
Zuweisen
Berechtigungen zu Befehlen in Berechtigungsprofil, 270–271
Berechtigungen zu Befehlen in Skript, 274
Berechtigungen zu Benutzer oder Rolle, 271–272
Rolle einem Benutzer, 218, 220
Rolle einem Benutzer lokal zuweisen, 224–225
Zuweisungsfehlerstatus, 101