



Sun Java™ System

Sun Java Enterprise System 5 Aufrüstungshandbuch für UNIX

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
USA

Part No: 819-6553-10
März 2007

Copyright © 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, USA. Alle Rechte vorbehalten.

Sun Microsystems, Inc., ist Inhaber der Urheberrechte für die Technologie, die in den in diesem Dokument beschriebenen Produkten verwendet wird. Diese Urheberrechte können insbesondere und ohne Einschränkungen ein oder mehrere der unter <http://www.sun.com/patents> aufgelisteten US-Patente und weitere Patente oder angemeldete Patente in den USA und anderen Ländern einschließen.

DIESES PRODUKT ENTHÄLT VERTRAULICHE INFORMATIONEN UND GESCHÄFTSGEHEIMNISSE VON SUN MICROSYSTEMS, INC., VERWENDUNG, OFFENLEGUNG ODER REPRODUKTION IST OHNE VORHERIGE SCHRIFTLICHE GENEHMIGUNG DURCH SUN MICROSYSTEMS, INC., NICHT GESTATTET.

Rechte der US-Regierung – Kommerzielle Software. Regierungsbenutzer unterliegen dem standardmäßigen Lizenzvertrag von Sun Microsystems, Inc., sowie den anwendbaren Bestimmungen der FAR und ihrer Zusätze.

Diese Ausgabe kann von Drittanbietern entwickelte Bestandteile enthalten.

Teile dieses Produkts können von Berkeley BSD Systems abgeleitet sein, lizenziert durch die University of California. UNIX ist ein eingetragenes Warenzeichen in den USA und anderen Ländern und exklusiv durch X/Open Company, Ltd. lizenziert.

Sun, Sun Microsystems, das Sun-Logo, Java, Solaris, JDK, Java Naming and Directory Interface, JavaMail, JavaHelp, J2SE, iPlanet, das Duke-Logo, das Java-Kaffeetassenlogo, das Solaris-Logo, das SunTone Certified-Logo und das Sun ONE-Logo sind Marken oder eingetragene Marken von Sun Microsystems, Inc., in den USA und anderen Ländern.

Alle SPARC-Marken werden unter Lizenz verwendet und sind Marken oder eingetragene Marken von SPARC International, Inc. in den USA und anderen Ländern. Produkte, die SPARC-Marken aufweisen, basieren auf der von Sun Microsystems, Inc., entwickelten Architektur.

Legato und das Legato-Logo sind eingetragene Marken und Legato NetWorker ist eine Marke bzw. eine eingetragene Marke von Legato Systems, Inc. Das Netscape Communications Corp-Logo ist eine Marke bzw. eine eingetragene Marke der Netscape Communications Corporation.

Die grafische Benutzeroberfläche von OPEN LOOK und Sun(TM) wurde von Sun Microsystems, Inc., entwickelt, für die entsprechenden Benutzer und Lizenznehmer. Sun erkennt die Pionierleistung von Xerox bei der Ausarbeitung und Entwicklung des Konzepts von visuellen oder grafischen Benutzeroberflächen für die Computerindustrie an. Sun ist Inhaber einer einfachen Lizenz von Xerox für die Xerox Graphical User Interface (grafische Benutzeroberfläche von Xerox). Mit dieser Lizenz werden auch die Sun-Lizenznehmer abgedeckt, die grafische OPEN LOOK-Benutzeroberflächen implementieren und sich ansonsten an die schriftlichen Sun-Lizenzvereinbarungen halten.

Produkte, die in diesem Diensthandbuch beschrieben sind, und die in diesem Handbuch enthaltenen Informationen unterliegen den Gesetzen der US-Exportkontrolle und können den Export- oder Importgesetzen anderer Länder unterliegen. Die Verwendung im Zusammenhang mit Nuklear-, Raketen-, chemischen und biologischen Waffen, im nuklear-maritimen Bereich oder durch in diesem Bereich tätige Endbenutzer, direkt oder indirekt, ist strengstens untersagt. Der Export oder Rückexport in Länder, die einem US-Embargo unterliegen oder an Personen und Körperschaften, die auf der US-Exportausschlussliste stehen, einschließlich (jedoch nicht beschränkt auf) der Liste nicht zulässiger Personen und speziell ausgewiesener Staatsangehöriger, ist strengstens untersagt.

DIE DOKUMENTATION WIRD IN DER VERFÜGBAREN FORM ZUR VERFÜGUNG GESTELLT UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN BEDINGUNGEN, ANGABEN UND GARANTIEEN, INKLUSIVE ALLER STILLSCHWEIGENDEN GARANTIEEN BEZÜGLICH HANDELSÜBLICHKEIT, EIGNUNG ZU EINEM BESTIMMTEN ZWECK ODER MÄNGELGEWÄHR, SIND VON DER HAFTUNG AUSGESCHLOSSEN, AUSSER EIN SOLCHER AUSSCHLUSS WIRD ALS RECHTSWIDRIG BEFUNDEN.

Inhalt

Liste der Tabellen	17
Vorwort	21
An wen richtet sich dieses Handbuch?	22
Konventionen in diesem Handbuch	22
Verwaltungsschnittstellen	22
Typografische Konventionen	23
Symbole	23
Shell-Eingabeaufforderungen	24
Verwandte Dokumentation	25
Handbücher im Java ES-Dokumentationssatz	25
Suche nach Sun-Produktdokumentation	26
Online-Zugriff auf Sun-Ressourcen	27
Kontakt zum technischen Support von Sun	27
Website-Referenzen von Drittanbietern	28
Kommentare sind willkommen	28
 Kapitel1 Planung hinsichtlich der Aktualisierungen	29
Java ES 5-Komponenten	30
Release 5: Produktkomponenten	30
Release 5: Gemeinsam genutzte Komponenten	31
Java ES-Aktualisierungstechnologien	33
Aktualisierung von Produktkomponenten	33
Ansätze zur Aktualisierung von Produktkomponenten	34
Ansatz zur Aktualisierung für alle Produktkomponenten	36
Aktualisierungen gemeinsam genutzter Komponenten	38
Der Aktualisierungsvorgang	39
Überlegungen zum Aktualisierungsplan	40
-Aktualisierungsabhängigkeiten	41
Unterstützte Aktualisierungswege und Strategien	42

Alle aktualisieren oder eine Auswahl aktualisieren	45
Aktualisierungen mehrerer Instanzen	46
Aspekte zum Betriebssystem	47
Erforderliche Betriebssystem-Patches	47
Duale Aktualisierungen: Java ES und Betriebssystem-Software	48
Aktualisierungen des Betriebssystems	49
Solaris 10-Umgebungen mit mehreren Zonen	49
Java ES-Komponentenabhängigkeiten	49
Abhängigkeiten zu gemeinsam genutzten Komponenten	49
Abhängigkeiten zu Produktkomponenten	55
Richtlinien für die Aktualisierungsreihenfolge	60
Sonderfälle	64
Selektive Aktualisierung: Anwendungsserver nicht aktualisiert	64
Aktualisierung von Portal Server Interim Feature Release (IFR) 7.0 auf Java ES 5	65
Aktualisierung von Java ES 5 und Solaris 10-Zonen	65
Zonenunterstützung im Java ES-Installationsprogramm	66
Aktualisierung von Produktkomponenten	66
Alle gemeinsam genutzten Komponenten synchronisieren	67
Empfohlene Vorgehensweisen zur Aktualisierung	68
Sonderfälle oder Ausnahmen	69
Sonderfälle zu den Produktkomponenten	69
Sonderfälle zu den gemeinsam genutzten Komponenten	70
 Kapitel2 Aktualisieren der gemeinsam genutzten Java ES-Komponenten	 71
Überblick über die Aktualisierung der gemeinsam genutzten Komponenten	72
Allgemeine zu berücksichtigende Aspekte	72
Gemeinsam genutzte Komponenten synchronisieren	73
Alle gemeinsam genutzten Komponenten synchronisieren	74
Zu berücksichtigende Aspekte hinsichtlich Solaris 10-Zonen	75
Ansätze zur Aktualisierung gemeinsam genutzter Komponenten	76
Aktualisierungsverfahren für gemeinsam genutzte Komponenten	77
Besondere Aktualisierungsverfahren	77
Aktualisierungsverfahren für Java SE	78
Überprüfen der symbolischen Java SE-Verknüpfung	79
Überprüfen der aktuellen Java SE-Version	79
Aktualisierungsverfahren für Common Agent Container	80
 Kapitel3 Sun Cluster-Software	 83
Überblick über Aktualisierungen der Sun Cluster-Software	84
Über Sun Cluster-Software Release 5	84
Wegweiser für die Aktualisierung von Sun Cluster	85
Sun Cluster-Daten	86

Vorgehensweise zur Aktualisierung von Sun Cluster	87
Kompatibilität	87
Sun Cluster-Abhängigkeiten	87
Aktualisieren der Sun Cluster-Software auf Java ES Release 5	88
Einführung	88
Aktualisierung von Sun Cluster	89
Aufgaben vor der Aktualisierung	89
Aktualisieren der Sun Cluster-Software	93
Überprüfen der Aktualisierung	94
Aufgaben nach der Aktualisierung	95
Aufheben der Aktualisierung	95
 Kapitel4 Sun Cluster Geographic Edition	97
Überblick über Aktualisierungen von Sun Cluster Geographic Edition	98
Über Java ES Release 5	98
Java ES Wegweiser für die Aktualisierung auf Release 5	98
Sun Cluster Geographic Edition-Daten	99
Vorgehensweise zur Aktualisierung von Sun Cluster Geographic Edition	99
Kompatibilität	100
Abhängigkeiten	100
Aktualisieren von Sun Cluster Geographic Edition von Version 3.1 8/05	100
Einführung	101
Aktualisierung der Sun Cluster Geographic Edition Version 3.1 8/05	101
Aufgaben vor der Aktualisierung	102
Aktualisierung von Version 3.1 8/05 von Sun Cluster Geographic Edition	104
Überprüfen der Aktualisierung	107
Aufgaben nach der Aktualisierung	107
Aufheben der Aktualisierung	108
 Kapitel5 Directory Server	109
Überblick über Aktualisierungen von Directory Server	111
Über Java ES Release 5	111
Java ES Wegweiser für die Aktualisierung auf Release 5	111
Directory Server-Daten	113
Vorgehensweise zur Aktualisierung von Directory Server	114
Kompatibilität	114
-Abhängigkeiten	114
Aktualisieren von Directory Server von Java ES Release 4	116
Einführung	116
Aktualisierung der Release 4-Version von Directory Server	117
Aufgaben vor der Aktualisierung	117
Aktualisieren von Release 4 von Directory Server	118

Überprüfen der Aktualisierung	124
Aufgaben nach der Aktualisierung	124
Aufheben der Aktualisierung	124
Aktualisierung mehrerer Instanzen	124
Rolling Upgrades von Directory Server-Replikaten	125
Aktualisieren von Directory Server als Datendienst	125
Aktualisieren von Directory Server von Java ES Release 3	125
Aktualisieren von Directory Server von Java ES Release 2	126
Kapitel6 Directory Proxy Server	127
Überblick über Aktualisierungen von Directory Proxy Server	129
Über Java ES Release 5	129
Wegweiser für die Aktualisierung auf Java ES Release 5	129
Directory Proxy Server-Daten	131
Directory Proxy Server Vorgehensweise zur Aktualisierung	131
Kompatibilität	132
-Abhängigkeiten	133
Aktualisieren von Directory Proxy Server von Java ES Release 4	134
Einführung	134
Aktualisierung der Release 4-Version von Directory Proxy Server	135
Aufgaben vor der Aktualisierung	135
Aktualisieren von Release 4 von Directory Proxy Server	136
Überprüfen der Aktualisierung	139
Aufgaben nach der Aktualisierung	139
Aufheben der Aktualisierung	140
Aktualisierung mehrerer Instanzen	140
Aktualisieren von Directory Proxy Server von Java ES Release 3	141
Aktualisieren der Directory Proxy Server Release 2-Version Java ES	142
Kapitel7 Webserver	143
Überblick über Aktualisierungen von Webserver	144
Über Java ES Release 5 Webserver	144
Wegweiser für die Aktualisierung von Webserver	145
Webserver-Daten	145
Vorgehensweise zur Aktualisierung von Webserver	146
Kompatibilität	146
Webserver-Abhängigkeiten	147
Aktualisieren von Webserver von Java ES Release 4	148
Einführung	148
Aktualisierung der Release 4-Version von Webserver	149
Aufgaben vor der Aktualisierung	149
Aktualisieren von Release 4 von Webserver	150

Überprüfen der Aktualisierung	163
Aufgaben nach der Aktualisierung	164
Aufheben der Aktualisierung	167
Aktualisieren von Webserver von Java ES Release 3	169
Aktualisieren von Webserver von Java ES Release 2	170
 Kapitel8 Java DB	171
Überblick über Aktualisierungen von Java DB	172
Über Java ES Release 5	172
Java ES Wegweiser für die Aktualisierung auf Release 5	172
Java DB-Daten	173
Vorgehensweise zur Aktualisierung von Java DB	173
Kompatibilität	173
-Abhängigkeiten	173
Aktualisieren von Java DB von Java ES Release 4	174
Einführung	174
Aktualisierung der Release 4-Version von Java DB	175
Aufgaben vor der Aktualisierung	175
Aktualisieren von Release 4 von Java DB	176
Überprüfen der Aktualisierung	177
Aufgaben nach der Aktualisierung	178
Aufheben der Aktualisierung	178
Aktualisierung mehrerer Instanzen	178
 Kapitel9 High Availability Session Store	179
Überblick über Aktualisierungen von HADB	181
Über Java ES Release 5 HADB	181
Wegweiser für die Aktualisierung von HADB	181
HADB-Daten	182
Vorgehensweise zur Aktualisierung von HADB	182
Kompatibilität	182
HADB-Abhängigkeiten	183
Aktualisieren von HADB von Java ES Release 4	184
Einführung	184
Aktualisierung der Release 4-Version von HADB	185
Aufgaben vor der Aktualisierung	185
Aktualisieren von Release 4 von HADB	186
Überprüfen der Aktualisierung	189
Aufgaben nach der Aktualisierung	190
Aufheben der Aktualisierung	191
Aktualisieren von HADB von Java ES Release 3	192

Kapitel10 Message Queue	193
Überblick über Aktualisierungen von Message Queue	194
Über Java ES Release 5 Message Queue	194
Wegweiser für die Aktualisierung von Message Queue	195
Message Queue-Daten	196
Vorgehensweise zur Aktualisierung von Message Queue	197
Kompatibilität	197
Message Queue-Abhängigkeiten	197
Aktualisieren von Message Queue von Java ES Release 4	199
Einführung	199
Aktualisierung der Release 4-Version von Message Queue	200
Aufgaben vor der Aktualisierung	200
Aktualisieren von Release 4 von Message Queue	202
Überprüfen der Message Queue-Aktualisierung	203
Aufgaben nach der Aktualisierung	203
Aufheben der Aktualisierung	204
Aktualisierung mehrerer Instanzen	205
Aktualisieren von Message Queue von Java ES Release 3	206
Aktualisieren der Message Queue Release 2-Version aus Java ES-Release 2	207
Einführung	207
Release 2-Kompatibilitätsprobleme	208
Protokollkompatibilität	208
Broker-Kompatibilität	208
Kompatibilität der verwalteten Objekte	209
Kompatibilität des Administrationstools	210
Clientkompatibilität	210
Aktualisierung der Release 2-Version von Message Queue	210
Aufgaben vor der Aktualisierung	211
Aktualisieren der Release 2-Version von Message Queue (Solaris)	212
Aktualisieren der Release 2-Version von Message Queue (Linux)	214
Installation des Kompatibilitätspakets (Linux)	216
Überprüfen der Message Queue-Aktualisierung	216
Aufgaben nach der Aktualisierung	216
Aufheben der Aktualisierung	217
Aktualisierung mehrerer Instanzen	217
 Kapitel11 Anwendungsserver	 219
Überblick über Aktualisierungen von Anwendungsserver	221
Über Java ES Release 5 Anwendungsserver	221
Anwendungsserver Wegweiser für die Aktualisierung von	221
Anwendungsserver-Daten	224
Anwendungsserver Vorgehensweise zur Aktualisierung von	225
Kompatibilität	225

Anwendungsserver-Abhängigkeiten	225
Aktualisieren von Anwendungsserver von Java ES Release 4	227
Einführung	227
Aktualisierung der Release 4-Version von Anwendungsserver	228
Aufgaben vor der Aktualisierung	228
Aktualisieren von Release 4 von Anwendungsserver	230
Überprüfen der Aktualisierung	232
Aufgaben nach der Aktualisierung	232
Aufheben der Aktualisierung	232
Aktualisieren von Anwendungsserver von Java ES Release 3	233
Aktualisieren von Anwendungsserver von Java ES Release 2	234
Einführung	234
Aktualisierung der Release 2-Version von Anwendungsserver	235
Aufgaben vor der Aktualisierung	235
Aktualisieren der Release 2-Version von Anwendungsserver (Solaris)	238
Aktualisieren der Release 2-Version von Anwendungsserver (Linux)	243
Überprüfen der Aktualisierung	243
Aufgaben nach der Aktualisierung	244
Aufheben der Aktualisierung	244
Aktualisierung der im Lieferumfang von Solaris enthaltenen Anwendungsserver-Version in einer Solaris 10-Multi-Zone-Umgebung	245
Kapitel12 Service Registry	249
Überblick über Aktualisierungen von Service Registry	251
Über Java ES Release 5	251
Java ES Wegweiser für die Aktualisierung auf Release 5	251
Service Registry-Daten	252
Vorgehensweise zur Aktualisierung von Service Registry	252
Kompatibilität	252
Abhängigkeiten	253
Aktualisieren von Service Registry von Java ES Release 4	254
Einführung	254
Aktualisierung der Release 4-Version von Service Registry	255
Aufgaben vor der Aktualisierung	255
Aktualisieren von Release 4 von Service Registry	257
Überprüfen der Aktualisierung	260
Aufgaben nach der Aktualisierung	261
Aufheben der Aktualisierung	261
Aktualisierung mehrerer Instanzen	262
Kapitel13 Web Proxy Server	263
Überblick über Aktualisierungen von Web Proxy Server	264

Über Java ES Release 5 Web Proxy Server	264
Wegweiser für die Aktualisierung von Web Proxy Server	264
Web Proxy Server-Daten	265
Vorgehensweise zur Aktualisierung von Web Proxy Server	265
Kompatibilität	266
Web Proxy Server-Abhängigkeiten	266
Aktualisieren von Web Proxy Server von Java ES Release 4	267
Einführung	267
Aktualisierung der Release 4-Version von Web Proxy Server	268
Aufgaben vor der Aktualisierung	268
Aktualisieren der Release 4-Version von Web Proxy Server (Solaris)	269
Aktualisieren der Release 4-Version von Web Proxy Server (Linux)	271
Überprüfen der Aktualisierung	272
Aufgaben nach der Aktualisierung	273
Aufheben der Aktualisierung (Solaris)	273
Aktualisierung von Web Proxy Server von Version 3.6	274
Einführung	274
Web Proxy Server-Aktualisierung von Version 3.6	275
Aufgaben vor der Aktualisierung	275
Aktualisieren von Version 3.6 von Web Proxy Server	276
Überprüfen der Aktualisierung	278
Aufgaben nach der Aktualisierung	278
Aufheben der Version 3.6-Aktualisierung	279
Kapitel14 Access Manager	281
Überblick über Aktualisierungen von Access Manager	282
Über Java ES Release 5 Access Manager	282
Access Manager Wegweiser für die Aktualisierung von	283
Access Manager-Daten	285
Access Manager Vorgehensweise zur Aktualisierung	286
Kompatibilität	286
Access Manager-Abhängigkeiten	287
Aktualisierungsszenarios für den Webcontainer	288
Aktualisieren von Access Manager von Java ES Release 4	290
Einführung	290
Vollständige Aktualisierung von Access Manager Release 4	291
Aufgaben vor der Aktualisierung	291
Aktualisieren von Release 4 von Access Manager	295
Überprüfen der Access Manager-Aktualisierung	307
Aufgaben nach der Aktualisierung	307
Aufheben der Aktualisierung	308
Aktualisierung mehrerer Instanzen	309
Ausschließliche Aktualisierung der Release 4-Version von Access Manager SDK	311

Aufgaben vor der Aktualisierung	312
Aktualisieren der Release 4-Version von Access Manager SDK	313
Überprüfen der Access Manager SDK-Aktualisierung	313
Aufheben der Aktualisierung	314
Aktualisieren von Access Manager von Java ES Release 3	315
Aktualisierung der Release 3-Version von Access Manager	315
Aktualisierung mehrerer Instanzen	315
Aktualisieren der Access Manager Release 2-Version Java ES	320
Aufgaben vor der Aktualisierung	320
Access Manager-Abhängigkeiten aktualisieren	321
Directory-Schema aktualisieren	321
Indizieren Sie das Directory neu	322
Aktualisierung der Release 2-Version von Access Manager	323
Aktualisieren der Release 2-Version von Access Manager: Webserver-Webcontainer	323
Aktualisieren der Release 2-Version von Access Manager: Anwendungsserver-Webcontainer .	323
Überprüfen der Access Manager-Aktualisierung	334
Aufgaben nach der Aktualisierung	335
Aufheben der Aktualisierung	335
Aktualisierung mehrerer Instanzen	335
Kapitel15 Portal Server	337
Überblick über Aktualisierungen von Portal Server	339
Über Java ES Release 5 Portal Server	339
Wegweiser für die Aktualisierung von Portal Server	339
Portal Server-Daten	340
Portal Server Vorgehensweise zur Aktualisierung	341
Kompatibilität	342
Portal Server-Abhängigkeiten	342
Selektive Aktualisierung	344
Aktualisierungsszenarios für den Webcontainer	344
Aktualisieren von Portal Server von Java ES Release 4	346
Einführung	346
Aktualisierung der Release 4-Version von Portal Server	348
Aufgaben vor der Aktualisierung von Release 4	349
Aktualisieren der Release 4-Version von Portal Server (Solaris)	355
Aktualisieren der Release 4-Version von Portal Server (Linux)	360
Überprüfen der Aktualisierung	363
Aufgaben nach der Aktualisierung von Release 4	364
Aufheben der Aktualisierung (Solaris)	371
Aufheben der Aktualisierung (Linux)	373
Aktualisierung mehrerer Instanzen	373
Aktualisieren von Portal Server von Java ES Release 3	378

Aufgabe vor der Aktualisierung von Release 3: Aktualisieren der Portal Server-Abhängigkeiten .	
378	
Aktualisieren von Release 3 Portal Server	379
Aufgaben nach der Aktualisierung von Release 3	379
Abonnieren einer Diskussion	379
Aktualisierung mehrerer Instanzen	380
Aktualisieren von Portal Server von Java ES Release 2	381
Aufgaben vor der Aktualisierung von Release 2	381
Aktualisieren von Release 2 Portal Server	382
Aktualisieren der Release 2-Version von Portal Server: Webserver-Webcontainer	382
Aktualisieren der Release 2-Version von Portal Server: Anwendungsserver-Webcontainer	383
Aufgaben nach der Aktualisierung von Release 2	387
Single Sign-On-Konfiguration	387
Aktivieren des URLScraper-Kanals	391
Löschen des Gateway-Diensteintrags	391
Aktualisierung mehrerer Instanzen	391
Aktualisieren von Portal Server von der Interim Feature Release 7.0	392
Portal Server Einführung in die IFR-Aktualisierung	392
Portal Server Aktualisierung von IFR 7.0	393
Aufgaben vor der Aktualisierung der IFR 7	393
Aktualisieren der Portal Server-IFR 7.0 (Solaris)	394
Aktualisieren der Portal Server-IFR 7 (Linux)	396
IFR 7-Aktualisierungsverfahren (Linux)	397
Überprüfen der Aktualisierung	400
Aufgaben nach der Aktualisierung der IFR 7	400
Aufheben der Aktualisierung (Solaris)	408
Aufheben der Aktualisierung (Linux)	410
Aktualisierung mehrerer Instanzen	410
Kapitel16 Portal Server Secure Remote Access	413
Überblick über Aktualisierungen von Portal Server Secure Remote Access	415
Über Java ES Release 5 Portal Server Secure Remote Access	415
Wegweiser für die Aktualisierung von Portal Server Secure Remote Access	416
Portal Server Secure Remote Access-Daten	416
Vorgehensweise zur Aktualisierung von Portal Server Secure Remote Access	417
Kompatibilität	417
Portal Server Secure Remote Access-Abhängigkeiten	418
Selektive Aktualisierung	419
Aktualisieren von Portal Server Secure Remote Access von Java ES Release 4	420
Einführung	420
Aktualisierung der Release 4-Version von Portal Server Secure Remote Access	422
Aufgaben vor der Aktualisierung von Release 4	422
Aktualisieren der Release 4-Version von Portal Server Secure Remote Access (Solaris)	426

Aktualisieren der Release 4-Version von Portal Server Secure Remote Access (Linux)	429
Überprüfen der Aktualisierung	431
Aufgaben nach der Aktualisierung von Release 4	431
Aufheben der Aktualisierung (Solaris)	433
Aufheben der Aktualisierung (Linux)	435
Aktualisierung mehrerer Instanzen	435
Aktualisieren von Portal Server Secure Remote Access von Java ES Release 3	441
Aktualisierung der Portal Server Secure Remote Access-Abhängigkeiten	441
Aktualisieren von Release 3 Portal Server Secure Remote Access	442
Aktualisierung mehrerer Instanzen	442
Aktualisieren von Portal Server Secure Remote Access von Java ES Release 2	443
Aufgaben vor der Aktualisierung von Release 2	443
Aktualisierung der Portal Server Secure Remote Access-Abhängigkeiten	443
Löschen des Gateway-Diensteintrags	444
Aktualisieren von Release 2 Portal Server Secure Remote Access	444
Aufgaben nach der Aktualisierung von Release 2	445
Festlegen der Portal Server-Domäne für Proxylet-Dienst	445
Aktualisierung mehrerer Instanzen	445
Aktualisieren von Portal Server Secure Remote Access von Interim Feature Release 7.0	446
Einführung	446
Aktualisieren von Portal Server Secure Remote Access IFR 7.0	447
Aufgaben vor der Aktualisierung	447
Aktualisieren von Portal Server Secure Remote Access IFR 7.0 (Solaris)	447
Aktualisieren von Portal Server Secure Remote Access IFR 7.0 (Linux)	449
IFR 7-Aktualisierungsverfahren (Linux)	449
Überprüfen der Aktualisierung	451
Aufgaben nach der Aktualisierung	452
Aufheben der Aktualisierung (Solaris)	452
Aufheben der Aktualisierung (Linux)	452
Aktualisierung mehrerer Instanzen	453
Anhang A Java Enterprise System-Versionsinhalte	455
Java ES 2003Q4 (Release 1)	456
Release 1: Im Installationsprogramm auswählbare Komponenten	456
Release 1: Gemeinsam genutzte Komponenten	457
Java ES 2004Q2 (Release 2)	458
Release 2: Im Installationsprogramm auswählbare Komponenten	458
Release 2: Gemeinsam genutzte Komponenten	459
Java ES 2005Q1 (Release 3)	461
Release 3: Im Installationsprogramm auswählbare Komponenten	461
Release 3: Gemeinsam genutzte Komponenten	464
Java ES 2005Q4 (Release 4)	466
Release 4: Im Installationsprogramm auswählbare Komponenten	466

Release 4: Gemeinsam genutzte Komponenten	469
Java ES 5 (Release 5)	471
Release 2: Im Installationsprogramm auswählbare Komponenten	471
Release 5: Gemeinsam genutzte Komponenten	474
Index	477

Liste der Tabellen

Tabelle 1	Typografische Konventionen	23
Tabelle 2	Symbolkonventionen	23
Tabelle 3	Shell-Eingabeaufforderungen	24
Tabelle 4	Java Enterprise System Dokumentation	25
Tabelle 1-1	Java ES 5 Produktkomponenten	30
Tabelle 1-2	Java ES 5 gemeinsam genutzte Komponenten	31
Tabelle 1-3	Ansätze zur Aktualisierung von Java ES-Produktkomponenten	36
Tabelle 1-4	Phasen des Aktualisierungsvorgangs	39
Tabelle 1-5	Wege zur Aktualisierung auf Java ES 5 (Release 5)	43
Tabelle 1-6	Selektive Auswahl im Vergleich zur Aktualisierung aller Komponenten	46
Tabelle 1-7	Abhängigkeiten von Java ES 5 (Release 5)-Produktkomponenten zu gemeinsam genutzten Komponenten	51
Tabelle 1-8	Abhängigkeiten der Java ES-Produktkomponenten	56
Tabelle 1-9	Patches, die erforderlich sind, wenn Anwendungsserver nicht auf Release 5 aktualisiert wird	64
Tabelle 2-1	Symbolische Verknüpfung auf Java SE nach Plattform	78
Tabelle 2-2	Ausgaben der Versionsüberprüfung von Java SE	79
Tabelle 2-3	Verzeichnispfade für Common Agent Container	80
Tabelle 3-1	Wege für die Aktualisierung auf Java ES 5 (Release 5): Sun Cluster 3.1 8/05-Software 85	
Tabelle 3-2	Verwendung von Sun Cluster-Daten	86
Tabelle 3-3	Sun Cluster Ausgaben der Versionsüberprüfung	91
Tabelle 4-1	Sun Cluster Geographic Edition Verzeichnispfade	97
Tabelle 4-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Sun Cluster Geographic Edition 3.1 2006Q4	99
Tabelle 4-3	Sun Cluster Geographic Edition-Verwendung der Daten	99

Tabelle 4-4	Sun Cluster Geographic Edition-Ausgaben der Versionsüberprüfung	102
Tabelle 5-1	Directory Server Verzeichnispfade	109
Tabelle 5-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Directory Server 6.0	111
Tabelle 5-3	Directory Server Verwendung der Daten	113
Tabelle 5-4	Directory Server Ausgaben der Versionsüberprüfung	117
Tabelle 6-1	Directory Proxy Server Verzeichnispfade	128
Tabelle 6-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Directory Proxy Server 6.0	130
Tabelle 6-3	Verwendung von Directory Proxy Server-Daten	131
Tabelle 6-4	Directory Proxy ServerAusgaben der Versionsüberprüfung	135
Tabelle 7-1	Webserver Verzeichnispfade	144
Tabelle 7-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Webserver 7.0	145
Tabelle 7-3	Verwendung der Webserver-Daten	146
Tabelle 7-4	Webserver-Standardnamen	147
Tabelle 7-5	Webserver-Ausgaben der Versionsüberprüfung	149
Tabelle 7-6	WSInstall.properties Values	155
Tabelle 7-7	wadm Allgemeine Befehlsoptionen	158
Tabelle 7-8	wadm migrate-server Befehlsoptionen und Operanden	159
Tabelle 7-9	wadm create-instance Befehlsoptionen und Operanden	162
Tabelle 7-10	wadm deploy-cofig Befehlsoptionen und Operanden	162
Tabelle 7-11	wadm set-virtual-server-prop Befehlsoptionen und Operanden	164
Tabelle 7-12	wadm set-search-collection-prop Befehlsoptionen und Operanden	166
Tabelle 8-1	Java DB Verzeichnispfade	171
Tabelle 8-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Java DB 10.1.3	172
Tabelle 8-3	Java DB-Datenverwendungen	173
Tabelle 8-4	Java DB-Ausgaben der Versionsüberprüfung	175
Tabelle 9-1	HADB Verzeichnispfade	179
Tabelle 9-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): HADB 4.4.3	181
Tabelle 9-3	HADB Verwendung der Daten	182
Tabelle 9-4	HADB Ausgaben der Versionsüberprüfung	185
Tabelle 9-5	Paketversionen für die Aktualisierung von HADB unter Solaris	187
Tabelle 10-1	Message Queue Verzeichnispfade	193
Tabelle 10-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Message Queue 3.7 UR1	195
Tabelle 10-3	Message Queue Verwendung der Daten (Solaris OS)	196
Tabelle 10-4	Message Queue-Ausgaben der Versionsüberprüfung	201

Tabelle 10-5	Message Queue-Ausgaben der Versionsüberprüfung	211
Tabelle 11-1	Anwendungsserver Verzeichnispfade	220
Tabelle 11-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Anwendungsserver Enterprise Edition 8.2	222
Tabelle 11-3	Aktualisierungswege für Anwendungsserver Versionen im Lieferumfang des Solaris-Betriebssystems	223
Tabelle 11-4	Anwendungsserver Verwendung der Daten	224
Tabelle 11-5	Anwendungsserver Ausgaben der Versionsüberprüfung	229
Tabelle 12-1	Service Registry Verzeichnispfade	249
Tabelle 12-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Service Registry 3.1	251
Tabelle 12-3	Service Registry-Verwendung der Daten	252
Tabelle 12-4	Service Registry Ausgaben der Versionsüberprüfung	256
Tabelle 13-1	Web Proxy Server Verzeichnispfade	263
Tabelle 13-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Web Proxy Server 4.0.4 ...	264
Tabelle 13-3	Verwendung der Web Proxy Server-Daten	265
Tabelle 13-4	Web Proxy Server Ausgaben der Versionsüberprüfung	268
Tabelle 13-5	Patches für die Aktualisierung von Web Proxy Server unter Solaris	270
Tabelle 13-6	Patches für die Aktualisierung von Web Proxy Server unter Linux	271
Tabelle 13-7	Web Proxy Server-Ausgaben der Versionsüberprüfung	275
Tabelle 14-1	Access Manager Verzeichnispfade	282
Tabelle 14-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Access Manager 7.1	283
Tabelle 14-3	Access Manager Verwendung der Daten	285
Tabelle 14-4	Szenarien für die Access Manager-Aktualisierung für Webcontainer	288
Tabelle 14-5	Access Manager Ausgaben der Versionsüberprüfung	292
Tabelle 14-6	Patches für die Aktualisierung der Access Manager Mobile Access-Software	296
Tabelle 14-7	Patch-Parameter für Mobile Access	297
Tabelle 14-8	Access Manager Konfigurationsparameter: ampre71upgrade	297
Tabelle 14-9	Administrative Server-Modi mit Unterstützung von amconfig	301
Tabelle 14-10	Access Manager Konfigurationsparameter: amconfig	302
Tabelle 14-11	amconfig-Parameter: Release 5Webserver	304
Tabelle 14-12	Access Manager Konfigurationsparameter: amupgrade	305
Tabelle 14-13	Patches für die Aktualisierung von Access Manager Mobile Access-Software	325
Tabelle 14-14	Patch-Parameter für Mobile Access	325
Tabelle 14-15	Access Manager Konfigurationsparameter: ampre71upgrade	326
Tabelle 14-16	Access Manager Konfigurationsparameter: amconfig	330

Tabelle 14-17	Access Manager Konfigurationsparameter: amupgrade	333
Tabelle 15-1	Portal Server Verzeichnispfade	338
Tabelle 15-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Portal Server 7.1	340
Tabelle 15-3	Portal Server Verwendung der Daten	340
Tabelle 15-4	Szenarien für die Portal Server-Aktualisierung für Webcontainer	345
Tabelle 15-5	Portal Server Ausgaben der Versionsüberprüfung	349
Tabelle 15-6	Vom Skript psupgrade für die Webcontainer-Aktualisierungsszenarien benötigte Informationen	351
Tabelle 15-7	Speicherort der JVM-Einstellungen	354
Tabelle 15-8	Patches für die Aktualisierung der Portal Server-IFR auf Release 5	392
Tabelle 16-1	Portal Server Secure Remote Access Verzeichnispfade	414
Tabelle 16-2	Wege für die Aktualisierung auf Java ES 5 (Release 5): Portal Server Secure Remote Access 7.1	416
Tabelle 16-3	Portal Server Secure Remote Access Verwendung der Daten	417
Tabelle 16-4	Portal Server Secure Remote AccessAusgaben der Versionsüberprüfung	423
Tabelle 16-5	Patches für die Aktualisierung von Portal Server Secure Remote Access IFR auf Release 5	446

Vorwort

Das *Java Enterprise System Aufrüstungshandbuch für UNIX* enthält die Informationen, die für die Aktualisierung der Sun Java™ Enterprise System (Java ES)-Software in einer Umgebung mit dem Sun Solaris™-Betriebssystem (Solaris OS) bzw. dem Red Hat Enterprise Linux-(RHEL-)Betriebssystem erforderlich sind. Es enthält keine Informationen zur Aktualisierung in einer HP-UX-Umgebung.

Das Handbuch beschreibt die Aktualisierung von Java ES 2004Q2 (Release 2), Java ES 2005Q1 (Release 3) und Java ES 2005Q4 (Release 4) auf Java ES 5 (Release 5).

Dieses Vorwort enthält die folgenden Abschnitte:

- „An wen richtet sich dieses Handbuch?“ auf Seite 22
- „Konventionen in diesem Handbuch“ auf Seite 22
- „Verwandte Dokumentation“ auf Seite 25
- „Online-Zugriff auf Sun-Ressourcen“ auf Seite 27
- „Kontakt zum technischen Support von Sun“ auf Seite 27
- „Website-Referenzen von Drittanbietern“ auf Seite 28
- „Kommentare sind willkommen“ auf Seite 28

An wen richtet sich dieses Handbuch?

Dieses Handbuch ist für Systemadministratoren oder Softwaretechniker bestimmt, die die Aktualisierung der Java ES-Software durchführen möchten.

Das Handbuch setzt Kenntnisse in Bezug auf folgende Punkte voraus:

- Unternehmensweite Installation von Softwareprodukten
- Derzeit in Ihrer Umgebung bereitgestellte Java ES-Komponenten
- Systemverwaltung und Netzwerkverwaltung auf der jeweiligen unterstützten Java ES-Plattform
- Clustering-Modell (sofern Sie Cluster-Software installieren)

Konventionen in diesem Handbuch

In den in diesem Abschnitt enthaltenen Tabellen werden die Konventionen erläutert, die in diesem Handbuch verwendet werden.

Verwaltungsschnittstellen

Für die Mehrzahl der in diesem *Aktualisierungshandbuch* dokumentierten Verfahren können zwei Verwaltungsschnittstellen verwendet werden: eine grafische Benutzeroberfläche (Graphical User Interface, GUI) und eine Befehlszeilenschnittstelle.

In diesem *Aktualisierungshandbuch* werden Aktualisierungsverfahren für Java ES-Komponenten vorwiegend unter Verwendung der Befehlszeilenschnittstelle beschrieben. Die Befehlszeilenschnittstelle kann beim Automatisieren (Scripting) der Aktualisierung von Java ES-Bereitstellungen verwendet werden, sodass die Verfahren bei Bedarf schnell und einfach wiederholt werden können.

Verfahren, in denen das Java ES-Installationsprogramm verwendet wird, werden jedoch nicht unter Verwendung der interaktiven textbasierten Schnittstelle, sondern unter Verwendung der GUI beschrieben. Die Java ES-Installationssitzungen können in einer Statusdatei gespeichert werden, mit der die Verfahren bei Bedarf wiederholt werden können.

Typografische Konventionen

In der nachfolgenden Tabelle werden die in diesem Handbuch verwendeten typografischen Änderungen erläutert.

Tabelle 1 Typografische Konventionen

Schriftart	Bedeutung	Beispiele
AaBbCc123 (nichtproportional)	API und Sprachelemente, HTML-Tags, Website-URLs, Befehlsnamen, Dateinamen, Verzeichnispfadnamen, Bildschirmcomputerausgaben, Beispielcode.	Bearbeiten Sie Ihre <code>.login</code> -Datei. Verwenden Sie <code>ls -a</code> zum Auflisten aller Dateien. % Sie haben eine E-Mail erhalten.
AaBbCc123 (nichtproportional, fett)	Eingabe durch den Benutzer (im Gegensatz zur Computerausgabe auf dem Bildschirm).	% su Passwort:
<i>AaBbCc123</i> (kursiv)	Buchtitel, neue Begriffe, Wörter, die betont werden sollen. Ein Platzhalter in einem Befehl oder Pfadnamen, der mit einem wirklichen Namen oder einem Wert ersetzt werden soll.	Lesen Sie Kapitel 6 im <i>Benutzerhandbuch</i> . Diese Optionen werden <i>class</i> -Optionen genannt. Speichern Sie die Datei <i>nicht</i> . Die Datei befindet sich im Verzeichnis <i>installationsverzeichnis/bin</i> .

Symbole

In der folgenden Tabelle werden die in diesem Handbuch verwendeten Symbolkonventionen beschrieben.

Tabelle 2 Symbolkonventionen

Symbol	Beschreibung	Beispiel	Bedeutung
[]	Enthält mögliche Befehlsoptionen.	ls [-l]	Die Option -l ist nicht erforderlich.

Tabelle 2 Symbolkonventionen (*Fortsetzung*)

Symbol	Beschreibung	Beispiel	Bedeutung
{ }	Enthält verschiedene Möglichkeiten für eine erforderliche Befehlsoption.	-d {y n}	Für die Option -d muss entweder das Argument y oder das Argument n verwendet werden.
-	Gibt eine Kombination aus mehreren Tasten an.	STRG-A	Halten Sie die Taste STRG gedrückt, während Sie die Taste A drücken.
+	Gibt die aufeinander folgende Betätigung mehrerer Tasten an.	STRG+A+N	Drücken Sie die Taste STRG, lassen Sie sie los und drücken Sie anschließend die nachfolgenden Tasten.
>	Zeigt die Auswahl eines Menüelements in einer grafischen Benutzeroberfläche an.	Datei > Neu > Vorlagen	Wählen Sie im Menü „Datei“ die Option „Neu“ aus. Wählen Sie im Untermenü „Neu“ die Option „Vorlagen“ aus.

Shell-Eingabeaufforderungen

In der nachfolgenden Tabelle werden die in diesem Handbuch verwendeten Shell-Eingabeaufforderungen erläutert.

Tabelle 3 Shell-Eingabeaufforderungen

Shell	Eingabeaufforderung
C-Shell unter UNIX oder Linux	<i>computername%</i>
C-Shell-Superuser unter UNIX oder Linux	<i>computername#</i>
Bourne-Shell und Korn-Shell unter UNIX oder Linux	\$
Bourne-Shell- und Korn-Shell-Superuser unter UNIX oder Linux	#
Windows-Befehlszeile	C:\

Verwandte Dokumentation

Auf der Website <http://docs.sun.com>SM können Sie online auf die technische Dokumentation von Sun zugreifen. Sie können das Archiv durchsuchen oder nach einem bestimmten Handbuchtitel oder Thema suchen.

Handbücher im Java ES-Dokumentationssatz

Die Java ES-Handbücher sind als Online-Dateien im PDF-Format (Portable Document Format) und HTML-Format (Hypertext Markup Language) verfügbar. Beide Formate können von unterstützenden Technologien für Benutzer mit Behinderungen gelesen werden. Unter folgender Adresse können Sie auf die SunTM-Dokumentations-Website zugreifen:

<http://docs.sun.com>

Die Java ES-Dokumentation enthält Informationen über das System in seiner Gesamtheit sowie über seine Komponenten. Zugriff auf diese Dokumentation:

<http://docs.sun.com/coll/1695.1>

In der nachfolgenden Tabelle sind die Handbücher auf Systemebene aufgeführt, die Bestandteil des Java ES-Dokumentationssatzes sind. In der linken Spalte werden der Name sowie der Speicherort der Teilenummer der einzelnen Dokumente angegeben. In der rechten Spalte wird der allgemeine Inhalt des Dokuments beschrieben.

Tabelle 4 Java Enterprise System Dokumentation

Dokument	Inhalt
<i>Java Enterprise System 5 Versionshinweis für UNIX</i> http://docs.sun.com/doc/820-0448	Enthält die neuesten Informationen über das Java ES, einschließlich bekannter Probleme. Zudem verfügen die Komponenten über ihre eigenen Versionshinweise.
<i>Java Enterprise System 5 – Technische Übersicht</i> http://docs.sun.com/doc/820-0887	Bietet eine Einführung in die technischen und konzeptionellen Grundlagen von Java ES. Beschreibt die Komponenten, die Architektur sowie Prozesse und Funktionen.

Tabelle 4 Java Enterprise System Dokumentation (*Fortsetzung*)

Dokument	Inhalt
<i>Java Enterprise System – Handbuch zur Bereitstellungsplanung</i> http://docs.sun.com/doc/819-3454	Bietet eine Einführung in die Planung und die Konzeptentwicklung von Bereitstellungslösungen für Unternehmen, die auf Java ES basieren. Beschreibt die Grundlagen und Prinzipien der Bereitstellungsplanung und des Bereitstellungskonzepts sowie den Lebenszyklus einer Lösung und bietet hochklassige Beispiele und Strategien, die Sie bei der Planung der unternehmensweiten Bereitstellung von Lösungen mit Java ES anwenden können.
<i>Java Enterprise System 5 – Handbuch zur Installationsplanung</i> http://docs.sun.com/doc/820-0080	Unterstützt Sie bei der Entwicklung von Implementierungsspezifikationen für Hardware-, Betriebssystem- und Netzwerkaspekte Ihrer Java ES-Bereitstellung. Beschreibt beispielsweise Komponentenabhängigkeiten, die bei Ihrer Installations- und Konfigurationsplanung berücksichtigt werden müssen.
<i>Java Enterprise System 5-Installationshandbuch für UNIX</i> http://docs.sun.com/doc/820-0098	Führt Sie durch die Installation von Java ES unter dem Solaris- oder dem Linux-Betriebssystem. Beschreibt, wie Sie die Komponenten nach der Installation konfigurieren und überprüfen, ob die Komponenten ordnungsgemäß funktionieren.
<i>Java Enterprise System 5 Installation Reference for UNIX</i> http://docs.sun.com/doc/820-0584	Enthält zusätzliche Informationen zu Konfigurationsparametern, bieten Arbeitsblätter für die Konfigurationsplanung und listet Referenzangaben, wie beispielsweise Standardverzeichnisse und Anschlussnummern auf.
<i>Java Enterprise System 5-Aufrüstungshandbuch für UNIX</i> http://docs.sun.com/doc/820-0894	Enthält Anleitungen zur Aktualisierung von Java ES unter dem Solaris- oder Linux-Betriebssystem.
<i>Sun Java Enterprise System 5 Monitoring Guide</i> http://docs.sun.com/doc/820-1587	Enthält Anleitungen zur Einrichtung von Monitoring Framework für jede Produktkomponente sowie zur Verwendung der Monitoring Console für die Anzeige von Echtzeitdaten und das Festlegen von Schwellenwert-Alarmen.
<i>Java Enterprise System Glossary</i> http://docs.sun.com/doc/819-4626	Definiert die Begriffe, die in der Java ES-Dokumentation verwendet werden.

Suche nach Sun-Produktdokumentation

Zusätzlich zur Suche nach Sun-Produktdokumentation auf der Website `docs.sun.com` können Sie eine Suchmaschine verwenden. Verwenden Sie hierfür im Suchfeld folgende Syntax:

suchbegriff site:docs.sun.com

Um beispielsweise nach „Broker“ zu suchen, geben Sie Folgendes ein:

Broker site:docs.sun.com

Um andere Websites in die Suche mit einzubeziehen (z. B. java.sun.com, www.sun.com, developers.sun.com), geben Sie im Suchfeld `sun.com` anstelle von `docs.sun.com` ein.

Online-Zugriff auf Sun-Ressourcen

Produktdownloads, professionelle Dienste, Patches und Support sowie zusätzliche Informationen für Entwickler erhalten Sie hier:

- Download Center
<http://www.sun.com/software/download/>
- Client-Lösungen
<http://www.sun.com/service/sunjavasystem/sjsservicessuite.html>
- Sun Enterprise Services, Solaris-Patches und Support
<http://sunsolve.sun.com/>
- Informationen für Entwickler
<http://developers.sun.com>

Unter folgender Adresse erhalten Sie Informationen über Java Enterprise System und seine Komponenten:

<http://www.sun.com/software/javaenterprisesystem/index.html>

Kontakt zum technischen Support von Sun

Wenn Sie technische Fragen zu diesem Produkt haben, die nicht in der Produktdokumentation beantwortet werden, besuchen Sie die Website <http://www.sun.com/service/contacting>.

Website-Referenzen von Drittanbietern

Sun ist nicht haftbar für die Verfügbarkeit der Websites Dritter, die in diesem Dokument erwähnt werden. Sun unterstützt keine Inhalte, Werbung, Produkte oder sonstige Materialien, die auf oder über solche Websites oder Ressourcen verfügbar sind, und übernimmt keine Verantwortung oder Haftung dafür. Sun ist nicht verantwortlich oder haftbar für tatsächliche oder vermeintliche Schäden oder Verluste, die durch oder in Verbindung mit der Verwendung von über solche Websites oder Ressourcen verfügbaren Inhalten, Waren oder Dienstleistungen bzw. dem Vertrauen darauf entstanden sind.

Kommentare sind willkommen

Sun möchte seine Dokumentation laufend verbessern. Ihre Kommentare und Vorschläge sind daher immer willkommen.

Zum Mitteilen Ihrer Kommentare rufen Sie <http://docs.sun.com> auf und klicken Sie auf „Send Comments“. Geben Sie im Online-Formular den Dokumenttitel und die Teilenummer an. Die Teilenummer ist eine 7-stellige oder 9-stellige Zahl, die Sie auf der Titelseite des Handbuchs oder am Anfang des Dokuments finden.

Planung hinsichtlich der Aktualisierungen

Dieses Kapitel enthält Informationen zur Planung der Aktualisierung von Sun Java™ Enterprise System (Java ES) Software auf Java ES Release 5 in einem Sun Solaris™ Betriebssystem oder einer Betriebssystemumgebung von Red Hat Enterprise Linux (vereinfacht als Linux bezeichnet).

Es besteht aus folgenden Abschnitten:

- „Java ES 5-Komponenten“ auf Seite 30
- „Java ES-Aktualisierungstechnologien“ auf Seite 33
- „Der Aktualisierungsvorgang“ auf Seite 39
- „Überlegungen zum Aktualisierungsplan“ auf Seite 40
- „Java ES-Komponentenabhängigkeiten“ auf Seite 49
- „Richtlinien für die Aktualisierungsreihenfolge“ auf Seite 60
- „Sonderfälle“ auf Seite 64
- „Aktualisierung von Java ES 5 und Solaris 10-Zonen“ auf Seite 65

Java ES 5-Komponenten

Als Einführung zur Planung der Aktualisierung der Java ES-Software werden in diesem Abschnitt die Komponenten in Java ES Release 5 überprüft. Abhängig von Ihrem Aktualisierungsszenario müssen Sie möglicherweise eine oder mehrere dieser Komponenten auf die Version von Release 5 aktualisieren.

Java ES-Komponenten werden in zwei Gruppen unterteilt, wie im *Java Enterprise System 5 – Technische Übersicht* (<http://docs.sun.com/doc/819-3588>) beschrieben.

- **Produktkomponenten.** Java ES *Produktkomponenten* bestehen aus:
 - Systemdienstkomponenten, die die wichtigsten Java ES-Infrastrukturdienste bieten
 - Dienstqualitätskomponenten zur Erweiterung der Systemdienste

Produktkomponenten können im Installationsprogramm Java ES ausgewählt werden.
- **Gemeinsam genutzte Komponenten.** Java ES *Gemeinsam genutzte Komponenten* sind lokal vorhandene gemeinsam genutzte Bibliotheken, von denen die Java ES-Produktkomponenten abhängen. Gemeinsam genutzte Komponenten werden automatisch vom Java ES-Installationsprogramm installiert. Welche gemeinsam genutzten Komponenten installiert werden, hängt davon ab, welche Produktkomponenten installiert sind.

Release 5: Produktkomponenten

Die Produktkomponenten in Release 5 sind in der folgenden Tabelle alphabetisch aufgeführt zusammen mit den Abkürzungen, die in den folgenden Tabellen dafür verwendet werden. Für die Dienstqualitätskomponenten wird auch die Diensttyperweiterung angegeben, die von der jeweiligen Komponente bereitgestellt wird.

Tabelle 1-1 Java ES 5 Produktkomponenten

Produktkomponente	Abkürzung	Version	Typ
Access Manager	AM	7.1	Systemdienstkomponente
Anwendungsserver	AS	8.2	Systemdienstkomponente
Directory Proxy Server	DPS	6.0	Dienstqualität: Zugriffskomponente
Directory Server	DS	6.0	Systemdienstkomponente

Tabelle 1-1 Java ES 5 Produktkomponenten (*Fortsetzung*)

Produktkomponente	Abkürzung	Version	Typ
High Availability Session Store	HADB	4.4.3	Dienstqualität: Verfügbarkeitskomponente
Java DB	JavaDB	10.2	Systemdienstkomponente
Message Queue	MQ	3.7 UR1	Systemdienstkomponente
Monitoring Console	MC	1.0	Dienstqualität: Verwaltungskomponente
Portal Server	PS	7.1	Systemdienstkomponente
Portal Server Secure Remote Access	PSRA	7.1	Dienstqualität: Zugriffskomponente
Service Registry	SR	3.1	Systemdienstkomponente
Sun Cluster	SC	3.1 8/05	Dienstqualität: Verfügbarkeitskomponente
Sun Cluster Geographic Edition	SCG	2006Q4	Dienstqualität: Verfügbarkeitskomponente
Web Proxy Server	WPS	4.0.4	Dienstqualität: Zugriffskomponente
Webserver	WS	7.0	Systemdienstkomponente

Release 5: Gemeinsam genutzte Komponenten

Die gemeinsam genutzten Komponenten in Release 5 sind in der folgenden Tabelle alphabetisch aufgeführt zusammen mit den Abkürzungen, die in den folgenden Tabellen dafür verwendet werden.

Tabelle 1-2 Java ES 5 gemeinsam genutzte Komponenten

Gemeinsam genutzte Komponente	Version	Abkürzung
Apache Commons Logging	1.0.3	ACL
Auf Jakarta ANT Java/XML basierendes Tool	1.6.5	ANT
Berkeley Datenbank	4.2.52	BDB
Common Agent Container	1.1 und 2.0	CAC
FastInfoSet	1.0.2	FIS
International Components for Unicode	3.2	ICU
Instant Messenger SDK	6.2.8	IM-SDK
Java 2 Platform, Standard Edition	5.0 Update 7	Java SE

Tabelle 1-2 Java ES 5 gemeinsam genutzte Komponenten *(Fortsetzung)*

Gemeinsam genutzte Komponente	Version	Abkürzung
JavaBeans™ Activation Framework	1.0.3	JAF
Java Studio Web Application Framework	2.1.5	JATO
JavaHelp™ Runtime	2.0	JHELP
JavaMail™ Runtime	1.3.2	JMAIL
Java Architecture for XML Binding Runtime	2.0.3	JAXB
Java API for XML Processing	1.3.1	JAXP
Java API for XML Registries Runtime	1.0.8	JAXR
Java API for XML-based Remote Procedure Call Runtime	1.1.3_01	JAX-RPC
Java API for Web Services Runtime	2.0	JAXWS
Java Calendar API	1.2	JCAPI
Java Dynamic Management™ Kit Runtime	5.1.2	JDMK
Java Security Services (Network Security Services für Java)	4.2.4 und 3.1.11	JSS und JSS3
JavaServer Pages™ Standard Tag Library	1.0.6	JSTL
KT Search Engine	1.3.4	KTSE
LDAP C SDK	6.0	LDAP C SDK
LDAP Java SDK	4.19	LDAP J SDK
Mobile Access Core	6.2	MA Core
Netscape Portable Runtime	4.6.4	NSPR
Network Security Services	3.11.4	NSS
SOAP Runtime with Attachments API for Java	1.3	SAAJ
Simple Authentication and Security Layer	2.19	SASL
Sun Explorer Data Collector (nur Solaris)	4.3.1	SEDC
Sun Java Monitoring Framework	2.0	MFWK
Sun Java Web Console	3.0.2	SJWC
Web Services Common Library	2.0	WSCL
XML Web Services Security	2.0	XWSS

Java ES-Aktualisierungstechnologien

Keiner der einzelnen Systemdienste aktualisiert alle Java ES-Komponenten. Aktualisierungen der Produktkomponenten und gemeinsam genutzten Komponenten haben unterschiedliche Merkmale und Aktualisierungstechnologien, wie im folgenden Abschnitt beschrieben.

Aktualisierung von Produktkomponenten

Die Aktualisierung von Java ES-Produktkomponenten auf Release 5 wird Komponente für Komponente und Computer für Computer anhand der in diesem *Aufrüstungshandbuch* beschriebenen komponentenspezifischen Aktualisierungsverfahren durchgeführt.

Die Aktualisierung einer Produktkomponente kann Hauptaktualisierungen umfassen, die möglicherweise nicht mit der früheren Version der Komponente kompatibel sind, oder Aktualisierungen mit Fehlerkorrekturen, die mit der Vorgängerversion vollständig kompatibel sind. Aufgrund der Abhängigkeiten zwischen den Java ES-Komponenten, zieht eine Aktualisierung möglicherweise die Aktualisierung weiterer Komponenten nach sich.

Die Aktualisierung der Java ES-Produktkomponenten umfasst zwei grundlegende Vorgänge, die die ursprüngliche Installation und Konfiguration der Java ES-Produktkomponenten widerspiegeln:

- **Installation von Software-Aktualisierungen** Eine aktualisierte Software erweitert oder korrigiert eine bestehende Software oder ersetzt eine bestehende Software. Eine Software kann installiert werden, indem Patches auf bestehende Software-Pakete angewandt, bestehende Pakete selektiv ausgetauscht, neue Pakete installiert werden oder eine Komponenten-Software vollständig neu installiert wird.
- **Neukonfiguration.** Bei der Neukonfiguration werden sämtliche Änderungen der Konfigurationsdaten, Benutzerdaten bzw. der dynamischen Anwendungsdaten durchgeführt, die für die Unterstützung der aktualisierten Software erforderlich sind. Die Datenänderung kann aus dem Hinzufügen zusätzlicher Daten bestehen, aus einer Änderung des Datenformats (in Eigenschaftsdateien oder Datenbankschema) oder aus einer Änderung des Speicherorts der Daten. Zur Neukonfiguration muss manchmal ein bestimmtes Verfahren durchgeführt werden und manchmal erfolgt sie automatisch. In einigen Fällen ist es zur Neukonfiguration erforderlich, die Komponentensoftware in einen Webcontainer zu verschieben.

Außerdem umfassen Aktualisierungen von Java ES-Produktkomponenten normalerweise Aufgaben, die vor der Aktualisierung durchgeführt werden müssen, und in einigen Fällen Verfahren nach der Aktualisierung, um diese betriebsbereit zu machen.

Ansätze zur Aktualisierung von Produktkomponenten

Zu den komponentenspezifischen Aktualisierungsverfahren zur Installation aktualisierter Software und zur Durchführung einer Neukonfiguration der Komponenten zählen die folgenden Aktualisierungsansätze:

- [Verwendung der Aktualisierungsfunktionen im Java ES Installationsprogramm.](#)
- [Neuinstallation der Produktkomponente](#)
- [Starten eines komponentenspezifischen Dienstprogramms zur Aktualisierung](#)
- [Anwendung von Patches auf vorhandene Komponentenpakete](#)

Verwendung der Aktualisierungsfunktionen im Java ES Installationsprogramm.

Das Installationsprogramm in Release 5 enthält eine Aktualisierungsfunktion zur Aktualisierung von Produktkomponenten in einigen besonderen Fällen: Anwendungsserver, Message Queue, HADB und Java DB. Erkennt das Java ES-Installationsprogramm die vorher installierten Release-Versionen dieser Produktkomponenten, so kennzeichnet es diese Komponenten als „aktualisierbar.“

Vor Aktualisierung dieser Komponenten überprüft das Installationsprogramm, ob aktuelle und frühere Versionen gemeinsam genutzter Komponenten vorhanden sind. Erkennt das Installationsprogramm, dass eine für die ausgewählte Komponente erforderliche gemeinsam genutzte Komponente einen früheren Versionsstand hat oder fehlt, so aktualisiert das Installationsprogramm alle gemeinsam genutzten installierten Komponenten und installiert alle fehlenden für die ausgewählte Komponente erforderlichen gemeinsam genutzten Komponenten. In einigen Fällen (vor allem Anwendungsserver) aktualisiert das Installationsprogramm die Produktkomponenten, von denen die zu aktualisierende Komponente abhängt.

Das Installationsprogramm entfernt Pakete mit früheren Versionen, installiert die Pakete mit Produktkomponenten für Release 5 und konfiguriert gegebenenfalls die Produktkomponente neu, die aktualisiert wird. (Wenn Anwendungsserver im Lieferumfang des Betriebssystems Solaris 9 enthalten ist, entfernt das Installationsprogramm jedoch keine Pakete; siehe [„Aktualisierung der Release 2-Version von Anwendungsserver“ auf Seite 235](#)).

Wenn Sie die Funktion der Betriebssystemzone von Solaris 10 verwenden, sind einige besondere Aspekte zu beachten. Siehe auch „[Zonenunterstützung im Java ES-Installationsprogramm](#)“ auf Seite 66.

Neuinstallation der Produktkomponente

Einige Produktkomponenten werden aktualisiert durch Neuinstallation der Komponenten über das Java ES-Installationsprogramm. Dazu entfernen Sie zunächst die Pakete der früheren Version und installieren dann Release 5 im gleichen Pfad. Sie können aber auch Release 5 in einem parallelen Pfad installieren und die frühere Version beibehalten.

In beiden Fällen werden die Produktkomponenten neu konfiguriert, indem man die Konfigurationsdaten der früheren Version in die neue Installation migriert, eine Neukonfiguration durchführt oder eine Kombination aus beiden Verfahren anwendet. Für einige Produktkomponenten gibt es ein Dienstprogramm zur Neukonfiguration oder Migration von Konfigurationsdaten dieser Komponente.

Starten eines komponentenspezifischen Dienstprogramms zur Aktualisierung

Einige Produktkomponenten bieten ein Dienstprogramm zur Aktualisierung oder ein Skript, das die Aktualisierung der Komponente auf Release 5 automatisiert. Das Dienstprogramm führt sowohl die Aktualisierung der Softwarepakete als auch zur Aktualisierung benötigte Neukonfigurationen durch. Für Komponenten, die in einen Webcontainer ausgelagert wurden, überträgt das Dienstprogramm in der Regel die aktualisierte Komponenten-Software in den Webcontainer.

Anwendung von Patches auf vorhandene Komponentenpakete

Einige Produktkomponenten werden durch manuelle Anwendung von Patches auf bestehende Softwarepakete aktualisiert. Während Plattformen unter Solaris und Linux ähnliche Technologien zur Verwaltung installierter Software-Pakete und zur Nachverfolgung von Änderungen an diesen Paketen durch eine Paket-Registry einsetzen, wirken sich die unterschiedlichen Technologien der Plattformen zur Anwendung von Patches auf die Aktualisierungsverfahren aus.

- **Solaris-Plattform.** Pakete werden über die Solaris-Befehle `pkgadd` und `pkgrm` installiert und entfernt. Die installierten Paketinhalte können mithilfe von Patches geändert werden. Diese werden mit den Befehlen `patchadd` und `patchrm` angewendet bzw. entfernt. Die Patches für Solaris-Pakete sind über die SunSolve-Website unter folgender Adresse erhältlich:
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

Solaris-Patches werden auf ein oder mehrere Pakete angewendet. Der Befehl `patchadd` erstellt eine Sicherungskopie des Pakets, auf das das Patch angewendet wird, um das Entfernen des Patches mit dem Befehl `patchrm` zu ermöglichen. Patches werden durch eine Patch-ID identifiziert, die aus einer Patch-Nummer gefolgt von einer Revisionsnummer besteht. Die Revisionsnummer erhöht sich entsprechend der im Laufe der Zeit vorgenommenen Änderungen.

- **Linux-Plattform.** Red Hat Enterprise Linux-Pakete (RPMs) können durch den Befehl `rpm` installiert oder aktualisiert werden. Die installierten Paketinhalte können durch Anwendung von Patches nicht geändert werden. RPM-Pakete werden stattdessen mit der Befehlsoption `rpm -U` aktualisiert. Dabei wird das aktuelle Paket durch eine neuere Version des Pakets ersetzt.

Um das Beziehen der RPMs zu erleichtern, sind zahlreiche RPM-Paketaktualisierungen nicht nur in der Java ES-Verteilung von Release 5 enthalten, sondern auch über die SunSolve-Website unter folgender Adresse erhältlich:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

RPM-Pakete, die über SunSolve erhältlich sind, sind zu Patches zusammengefasst, denen wie Solaris-Patches eine Patch-ID und eine Revisionsnummer zugewiesen ist. Diese Linux-Patches können ein oder mehrere RPM-Pakete enthalten, die jeweils durch einen eindeutigen RPM-Namen, eine RPM-Nummer sowie eine Revisionsnummer gekennzeichnet sind. Die Revisionsnummer erhöht sich entsprechend der im Laufe der Zeit vorgenommen Änderungen des RPM-Pakets.

Ansatz zur Aktualisierung für alle Produktkomponenten

Der Ansatz zur Aktualisierung aller Produktkomponenten auf Release 5 ist in der folgenden Tabelle beschrieben:

Tabelle 1-3 Ansätze zur Aktualisierung von Java ES-Produktkomponenten

Produktkomponente	Installation von aktualisierter Software	Neukonfiguration
Access Manager	Ersetzen von Paketen: Verwenden Sie das Skript zur Entfernung von Paketen und installieren Sie das System neu.	Verwenden Sie die Skripte <code>amconfig</code> und <code>amupgrade</code> zur Neukonfiguration und erneuten Bereitstellung im Webcontainer

Tabelle 1-3 Ansätze zur Aktualisierung von Java ES-Produktkomponenten (*Fortsetzung*)

Produktkomponente	Installation von aktualisierter Software	Neukonfiguration
Anwendungsserver	Ersetzen von Paketen: Verwenden Sie die Aktualisierungsfunktion des Java ES-Installationsprogramms	keine, außer im Fall einer Aktualisierung von Release 2, bei der Sie die Skripte <code>postinstall</code> und <code>asupgrade</code> verwenden
Directory Proxy Server	Führen Sie eine Neuinstallation durch, ohne die früheren Pakete zu ersetzen.	Manuelle Neukonfiguration
Directory Server	Führen Sie eine Neuinstallation durch, ohne die früheren Pakete zu ersetzen.	Verwenden Sie den Befehl <code>dsmig</code> , um Verzeichnisdaten zu migrieren.
High Availability Session Store	Ersetzen von Paketen: Verwenden Sie die Funktion des Java ES-Installationsprogramms oder parallele Neuinstallation	Keine
Java DB	Ersetzen von Paketen: Verwenden Sie die Aktualisierungsfunktion des Java ES-Installationsprogramms	Keine
Message Queue	Ersetzen von Paketen: Verwenden Sie die Aktualisierungsfunktion des Java ES-Installationsprogramms oder das Skript <code>mqupgrade</code> (aus Release 2)	Keine, außer im Fall einer Aktualisierung von Release 2 auf Linux, wofür Sie das Skript <code>mqmigrate</code> verwenden
Portal Server	Ersetzen von Paketen: Verwenden Sie das Skript <code>psupgrade</code>	Verwenden Sie das Skript <code>psupgrade</code> zur Neukonfiguration und erneuten Bereitstellung im Webcontainer
Portal Server Secure Remote Access	Ersetzen von Paketen: Verwenden Sie das Skript <code>psupgrade</code>	<code>psupgrade</code> zur Neukonfiguration
Service Registry	Führen Sie eine Neuinstallation durch, ohne die früheren Pakete zu ersetzen.	Führen Sie eine manuelle Neukonfiguration durch und verwenden Sie das Skript <code>ant upgrade</code> zur erneuten Bereitstellung in der Anwendungsserver Domäne

Tabelle 1-3 Ansätze zur Aktualisierung von Java ES-Produktkomponenten *(Fortsetzung)*

Produktkomponente	Installation von aktualisierter Software	Neukonfiguration
Sun Cluster	Ersetzen von Paketen: Verwenden Sie das Skript <code>scinstall</code> , um Binärdateien zu ersetzen.	Verwenden Sie das Skript <code>scinstall</code> , um die Konfiguration zu migrieren.
Sun Cluster Geo	Ersetzen von Paketen: Verwenden Sie das Skript <code>uninstall</code> und führen Sie eine Neuinstallation durch	Keine
Web Proxy Server	Patch-Binärdateien	Keine
Webserver	Führen Sie eine Neuinstallation durch, ohne die früheren Pakete zu ersetzen.	Verwenden Sie den Befehl <code>wadm migrate-server</code> , um die Konfiguration der Server-Instanz zu migrieren

Aktualisierungen gemeinsam genutzter Komponenten

Die Aktualisierung von gemeinsam genutzten Java ES-Komponenten ist häufig ein notwendiger Bestandteil der Aktualisierung der Produktkomponenten, die von den gemeinsam genutzten Komponenten abhängen.

Zur Aktualisierung gemeinsam genutzter Komponenten ist weder eine Neukonfiguration der Komponenten erforderlich noch die Durchführung bestimmter Verfahren vor und nach der Aktualisierung. Aktualisierungen gemeinsam genutzter Komponenten können außerdem nicht rückgängig gemacht werden.

Die große Anzahl (ca. 30) an gemeinsam genutzten Java ES-Komponenten sowie die komplexe Interaktion zwischen gemeinsam genutzten Komponenten und Produktkomponenten machen es erforderlich, dass alle gemeinsam genutzten Komponenten innerhalb eines Betriebssystems auf dieselbe Java ES Release-Version synchronisiert werden. Eine Betriebssystem-Instanz bedeutet, dass das Linux-Betriebssystem Solaris 9, Solaris 10 oder Red Hat Enterprise auf einem einzelnen Computer läuft, oder dass das Betriebssystem Solaris 10 auf einer der virtuellen Betriebssystemumgebungen (Zonen) eines Computers läuft.

Da eine Synchronisierung erforderlich ist, sollten Sie gemeinsam genutzte Java ES-Komponenten nicht einzeln aktualisieren, sondern gleichzeitig auf Release 5 aktualisieren.

Gemeinsam genutzte Komponenten können mithilfe des Java ES-Installationsprogramms auf Release 5 synchronisiert werden. Das Installationsprogramm synchronisiert gemeinsam genutzte Komponenten bei der Aktualisierung von Produktkomponenten (siehe [„Verwendung der Aktualisierungsfunktionen im Java ES Installationsprogramm.“ auf Seite 34](#)) oder bei Neuinstallation von Produktkomponenten. Das Installationsprogramm enthält auch eine Synchronisierungsfunktion, die alle vorhandenen gemeinsam genutzten Komponenten aktualisiert und fehlende gemeinsam genutzte Komponenten installiert. Eine vollständige Beschreibung dieser Funktion erhalten Sie unter [„Alle gemeinsam genutzten Komponenten synchronisieren“ auf Seite 74](#).

Der Aktualisierungsvorgang

Der Java ES-Aktualisierungsprozess umfasst eine Reihe von Phasen, die normalerweise zunächst in einer Testumgebung durchgeführt werden, bevor sie in einer Produktionsumgebung ablaufen. In einer Testumgebung können Sie jede Phase zunächst testen und Skripte schreiben, die dann von IT-Mitarbeitern zur Aktualisierung komplexer Java ES-Bereitstellungen verwendet werden können.

Wenn Sie einen Aktualisierungsvorgang in einer Testumgebung getestet haben und sicher sind, dass die Aktualisierung richtig funktioniert, können Sie den Vorgang in der Produktionsumgebung reproduzieren.

Der Vorgang umfasst die Phasen, die in der folgenden Tabelle aufgeführt und in diesem *Aufriistungshandbuch* dokumentiert sind. Die Phasen lassen sich auf einzelne Komponentenaktualisierungen wie auch auf ihre Java ES-Bereitstellung insgesamt anwenden.

Tabelle 1-4 Phasen des Aktualisierungsvorgangs

Aktualisierungsphase	Beschreibung
Plan	Sie entwickeln einen Aktualisierungsplan. Darin spezifizieren Sie die zu aktualisierenden Java ES-Komponenten und die Reihenfolge, in der diese auf den verschiedenen Computern oder Betriebssystem-Instanzen Ihrer Bereitstellung aktualisiert werden sollen.
Vorbereitung der Aktualisierung	Sie sichern Ihre Konfigurations- und Anwendungsdaten, wenden Betriebssystem-Patches an, aktualisieren alle erforderlichen Abhängigkeiten und führen andere Aufgaben zur Vorbereitung der Aktualisierung aller einzelnen Komponenten aus.

Tabelle 1-4 Phasen des Aktualisierungsvorgangs (*Fortsetzung*)

Aktualisierungsphase	Beschreibung
Aktualisieren	Sie beziehen alle für die Aktualisierung erforderlichen Pakete, Patches und Tools. Sie installieren Software-Aktualisierungen und führen vorschriftsmäßig eine Neukonfiguration zu jeder Komponente durch, einschließlich einer Migration der Daten in das aktualisierte System.
Überprüfung	Sie stellen sicher, dass die Aktualisierung erfolgreich war, indem Sie vorgeschriebene Überprüfungen durchführen, einschließlich Start der aktualisierten Software-Komponenten und Testen verschiedener Verwendungsszenarios.
Verfahren nach der Aktualisierung	Sie führen alle weiteren Konfigurationen, Anpassungen oder Aufgaben aus, die erforderlich sein könnten, um die aktualisierte Komponente betriebsbereit zu machen, wie zum Beispiel die Einbindung neuer Funktionen.
Aufheben der Aktualisierung/Wiederherstellung	Heben Sie die Aktualisierung auf und überprüfen Sie, ob die Aufhebung erfolgreich war. Es ist wichtig, die Aufhebung der Aktualisierung zu überprüfen, wenn Sie aus irgendwelchen Gründen die alte Version der Produktionsumgebung wiederherstellen müssen.

Überlegungen zum Aktualisierungsplan

In einem Aktualisierungsplan spezifizieren Sie die auf Release 5 zu aktualisierenden Java ES-Komponenten und die Reihenfolge, in der diese auf den verschiedenen Computern oder Betriebssystem-Instanzen Ihrer Bereitstellung aktualisiert werden sollen.

Ihr Aktualisierungsplan hängt von den Zielen und Prioritäten Ihrer Aktualisierung ab sowie vom Umfang und der Komplexität Ihrer Bereitstellungsarchitektur.

Ihre Java ES-Bereitstellungsarchitektur kann beispielsweise aus einer einzelnen Java ES-Komponente bestehen, die auf einem einzelnen Computer ausgeführt wird. Das Ziel der Aktualisierung könnte dabei die Behebung von Fehlern der früheren Softwareversion sein. Ihre Java ES-Bereitstellungsarchitektur kann jedoch auch aus einer Reihe voneinander abhängigen Java ES-Komponenten bestehen, die auf zahlreichen verschiedenen Computern bereitgestellt sind. Das Ziel der Aktualisierung könnte dabei die Bereitstellung neuer Funktionen sein, wobei nur die Mindestanzahl an Komponenten aktualisiert werden soll und die Ausfallzeit so gering wie möglich gehalten werden soll.

Grundsätzlich gilt, je höher die Anzahl der Java ES-Komponenten und je höher die Anzahl der Computer in Ihrer Bereitstellungsarchitektur ist, desto komplexer gestaltet sich der Aktualisierungsplan.

Ihr Aktualisierungsplan hängt von zahlreichen Faktoren ab, die über den Umfang und die Komplexität Ihrer Bereitstellungsarchitektur hinausgehen. Dazu zählen folgende Faktoren:

- -Aktualisierungsabhängigkeiten
- Alle aktualisieren oder eine Auswahl aktualisierens
- Unterstützte Aktualisierungswege und Strategien
- Aktualisierungen mehrerer Instanzen
- Aspekte zum Betriebssystem

-Aktualisierungsabhängigkeiten

Einer der wichtigsten Faktoren bei der Planung der Aktualisierung einer Java ES-Produktkomponente ist die Kenntnis der Abhängigkeiten dieser Komponente von anderen Java ES-Komponenten und davon, ob andere Komponenten, von denen die zu aktualisierende Komponente abhängig ist, ebenfalls aktualisiert werden müssen, um die Aktualisierung der Komponente zu unterstützen.

Es gibt zwei Arten von Aktualisierungsabhängigkeiten:

- **Zwingende Aktualisierungsabhängigkeit.** Die Aktualisierung einer Produktkomponente erfordert die Aktualisierung einer Komponente, von der diese abhängig ist. Diese Anforderung ergibt sich beispielsweise aufgrund einer neuen Funktion, neuer Schnittstellen oder Fehlerkorrekturen, die für die abhängige Komponente benötigt werden. Bei einer zwingenden Aktualisierungsabhängigkeit können Sie die Komponente erst dann erfolgreich aktualisieren und verwenden, wenn die Komponente, von der die Komponente abhängig ist, aktualisiert wurde.
- **Keine zwingende Aktualisierungsabhängigkeit.** Die Aktualisierung einer Produktkomponente erfordert keine Aktualisierung einer Komponente, von der diese abhängig ist. Bei einer nicht zwingenden Aktualisierungsabhängigkeit können Sie die Komponente erfolgreich aktualisieren und verwenden, auch wenn die Komponente, von der die Komponente abhängig ist, nicht aktualisiert wurde.

Bei der Aktualisierung einer Java ES-Produktkomponente müssen alle Komponenten, von denen die Komponente *zwingend* abhängig ist, aktualisiert werden. Abgesehen von einigen Ausnahmen, die in diesem Handbuch genannt sind, müssen Komponenten, von denen die Komponente nicht zwingend abhängig

ist, nicht aktualisiert werden. Wenn mehrere voneinander abhängige Komponenten aktualisiert werden sollen, müssen Sie eine Komponente aktualisieren, sobald eine der zu aktualisierenden Java ES-Komponenten zwingend von dieser speziellen Komponente abhängig ist.

Aufgrund von eingeführten Inkompatibilitäten müssen Sie in einigen besonderen Fällen bei der Aktualisierung einer Komponente auch die Komponente aktualisieren, die diese unterstützt. Diese besonderen Fälle werden in diesem Handbuch genannt.

Unterstützte Aktualisierungswege und Strategien

Ihr Aktualisierungsplan hängt vom Java ES Release ab, den Sie auf Release 5 aktualisieren wollen.

Es können zwar alle früheren Release-Versionen der Java ES-Software auf Java ES 5 (Release 5) aktualisiert werden, jedoch nur die Aktualisierung von Java ES 2005Q4 (Release 4) und Java ES 2005Q1 (Release 3) und Java ES 2004Q2 (Release 2) wird unterstützt. Während dieses *Aufrüstungshandbuch* Strategien zur Aktualisierung von Java ES 2003Q4 (Release 1) und Release-Versionen älter als Java ES bietet, erhalten Sie darin keine Anweisungen zur Durchführung dieser Aktualisierungen.

In der folgenden Tabelle werden die verschiedenen Aktualisierungswege für Release 5, deren Merkmale sowie die Aktualisierungsstrategien zur Durchführung der Aktualisierung beschrieben.

Aufgrund der Unterschiede der in dieser Tabelle beschriebenen Aktualisierungswege und weil der Vorgang zur Aktualisierung von Produktkomponenten oft davon abhängt, auf welche Release-Version aktualisiert wird, sind die Kapitel dieses *Aufrüstungshandbuchs*, in denen beschrieben wird, wie jede einzelne Produktkomponente aktualisiert wird, in Abschnitte unterteilt, wovon jeder einen anderen Aktualisierungsweg beschreibt.

Tabelle 1-5 Wege zur Aktualisierung auf Java ES 5 (Release 5)

Produkt version	Java ES Release	Systemmerkmale	Vorgehensweise zur Aktualisierung
2005Q4	Release 4	Java ES 5 (Release 5) unterstützt eine Mischung aus Produktkomponenten von Release 4 und Release 5 auf einem einzelnen Computer. Es ist jedoch erforderlich, dass gemeinsam genutzte Komponenten auf dieselbe Release-Version synchronisiert werden. Die Interoperabilität zwischen Release 4- und Release 5-Produktkomponenten wurde getestet. Bekannte Inkompatibilitäten sind im <i>Java Enterprise System 5 Versionshinweis für UNIX</i> (http://docs.sun.com/doc/819-3426) dokumentiert.	Die Koexistenz von Release 4- und Release 5-Komponenten bietet die Möglichkeit, auf einem Computer oder innerhalb einer Bereitstellungsarchitektur mit mehreren Computern lediglich eine Auswahl an Release 4-Produktkomponenten auf Release 5 zu aktualisieren. Wenn eine Release 5-Produktkomponente von einer gemeinsam genutzten Release 5-Komponente unterstützt werden muss, so müssen alle gemeinsam genutzten Komponenten auf dem Computer auf Release 5 synchronisiert werden.
2005Q1	Release 3	Ähnlich dem oben genannten Weg zur Aktualisierung auf Release 4. Java ES 5 (Release 5) unterstützt eine Mischung aus Produktkomponenten von Release 3 (auch Release 4) und Release 5 auf einem einzelnen Computer. Es ist jedoch erforderlich, dass gemeinsam genutzte Komponenten auf dieselbe Release-Version synchronisiert werden. Die Interoperabilität zwischen Release 3- und Release 5-Produktkomponenten wurde getestet. Bekannte Inkompatibilitäten sind im <i>Java Enterprise System 5 Versionshinweis für UNIX</i> (http://docs.sun.com/doc/819-3426) dokumentiert.	Ähnlich dem oben genannten Weg zur Aktualisierung auf Release 4. Die Koexistenz von Release 3- und Release 5-Komponenten bietet die Möglichkeit, auf einem Computer oder innerhalb einer Bereitstellungsarchitektur mit mehreren Computern lediglich eine Auswahl an Release 3-Komponenten auf Release 5 zu aktualisieren. Wenn eine Release 5-Produktkomponente von einer gemeinsam genutzten Release 5-Komponente unterstützt werden muss, so müssen alle gemeinsam genutzten Komponenten auf dem Computer auf Release 5 synchronisiert werden.

Tabelle 1-5 Wege zur Aktualisierung auf Java ES 5 (Release 5) (*Fortsetzung*)

Produkt version	Java ES Release	Systemmerkmale	Vorgehensweise zur Aktualisierung
2004Q2	Release 2	Anders als die oben genannten Wege zur Aktualisierung auf Release 4 und Release 3. Java ES 5 (Release 5) unterstützt <i>keine</i> Mischung aus Release 2- und Release 5-Komponenten auf einem Computer, weder Produktkomponenten noch gemeinsam genutzte Komponenten. Zwischen diesen Release-Versionen bestehen bekannte Inkompatibilitäten. Die Interoperabilität der Release 2- und Release 4-Komponenten ist nicht zertifiziert (wurde nicht getestet.)	Bei der Aktualisierung von Komponenten von Release 2 auf Release 5 auf einem Computer müssen alle Release 2-Komponenten auf Release 5 aktualisiert werden. Es ist jedoch in einigen Fällen möglich, Release 2- mit Release 5-Komponenten zu mischen, die sich auf <i>verschiedenen</i> Computern innerhalb einer Bereitstellungsarchitektur befinden.
2003Q4 und frühere Versionen	Release 1 und Versionen vor Java ES	Ähnlich dem oben genannten Weg zur Aktualisierung auf Release 2. Java ES 5 (Release 5) unterstützt keine Mischung aus Release 2- und Release 5-Komponenten auf einem Computer, weder Produktkomponenten noch gemeinsam genutzte Komponenten. Zwischen diesen Release-Versionen bestehen bekannte Inkompatibilitäten. Die Interoperabilität der Release 1- oder früheren Release-Versionen und Release 5-Komponenten ist nicht zertifiziert (wurde nicht getestet).	Java ES ist nicht zertifiziert für die direkte Aktualisierung von Release 1 oder früheren Release-Versionen auf Release 5. In einigen Fällen können Sie jedoch eine Aktualisierung von Release 1 durchführen, indem Sie zunächst auf Java ES Release 3 aktualisieren, wie im Release 3 <i>Java Enterprise System Upgrade and Migration Guide</i>, http://docs.sun.com/doc/819-0062 beschrieben; danach aktualisieren Sie von Release 3 auf Release 5. Auf diese Möglichkeit wird im Wegweiser zur Aktualisierung der jeweiligen Komponente in diesem <i>Aufrüstungshandbuch</i> hingewiesen. In anderen Fällen kann die Aktualisierung von Release 1 auf Release 5 wie eine Aktualisierung von Release 2 oder Release 3 auf Release 5 durchgeführt werden. Auf diese Möglichkeit wird im Wegweiser für die Aktualisierung der jeweiligen Komponente in diesem <i>Aufrüstungshandbuch</i> hingewiesen.

HINWEIS Wenn für Produktkomponenten eine vorläufige Ausgabe (Interim Feature Release, IFR) zwischen offiziellen Java ES Release-Versionen vorgesehen ist, wird eine Aktualisierung der IFR normalerweise in der gleichen Weise durchgeführt wie bei der vorigen Java ES Release-Version. Wenn es zum Beispiel zwischen Release 3 und Release 4 eine IFR gibt, so würde die Komponente genauso aktualisiert werden wie bei einer Aktualisierung von Release 3 auf Release 5. Ansonsten (zum Beispiel bei Portal Server und Portal Server Secure Remote Access) ist die IFR-spezifische Vorgehensweise zur Aktualisierung in diesem *Aufrüstungshandbuch* dokumentiert.

Alle aktualisieren oder eine Auswahl aktualisieren

Der Unterschied zwischen zwingenden und nicht zwingenden Abhängigkeiten bietet die Möglichkeit innerhalb Ihres Aktualisierungsplans, lediglich eine Auswahl der Java ES-Produktkomponenten innerhalb eines bereitgestellten Systems zu aktualisieren. Eine selektive Aktualisierung trifft für die Aktualisierung von Release 3 und Release 4 auf Release 5 auf einem einzelnen Computer zu. Eine selektive Aktualisierung von Release 2 auf Release 5 auf einem Computer wird nicht unterstützt.

Sie haben grundsätzlich die Wahl zwischen einer selektiven Aktualisierung oder der Aktualisierung aller Java ES-Produktkomponenten auf einem Computer:

- **Selektive Aktualisierung.** Bei diesem Ansatz beginnen Sie mit der Java ES-Produktkomponente, die Sie auf Release 5 aktualisieren wollen. Sie bestimmen die zwingenden Abhängigkeiten für diese Komponente; diese Komponenten müssen ebenfalls aktualisiert werden. Wiederholen Sie diesen Vorgang nacheinander für jede zwingende Abhängigkeit, bis keine weiteren Komponenten mehr aktualisiert werden müssen. Sie erhalten sämtliche Java ES-Produktkomponenten, die aktualisiert werden müssen.
- **Aktualisierung aller Komponenten.** Bei diesem Ansatz aktualisieren Sie alle bereitgestellten Java ES-Produktkomponenten auf Release 5. In einigen Fällen ist es aufgrund der Komplexität einer Bereitstellung aus geschäftlichen Gründen nicht machbar, ein gesamtes System auf einmal zu aktualisieren.

In der folgenden Tabelle werden die beiden Ansätze des Aktualisierungsverfahrens verglichen.

Tabelle 1-6 Selektive Auswahl im Vergleich zur Aktualisierung aller Komponenten

Aktualisierungsansatz	Vorteile	Nachteile
Selektive Aktualisierung	Reduziert die Anzahl der zu aktualisierenden Komponenten.	Daraus resultierend ist die Version sämtlicher Komponenten im Bereitstellungssystem inkonsistent.
Aktualisierung aller Komponenten	Die Version sämtlicher Komponenten im Bereitstellungssystem bleibt konsistent.	Erhöht die Anzahl der zu aktualisierenden Komponenten.

Eine selektive Aktualisierung wurde auch in Java ES Release 4 unterstützt. Daher ist es möglich, sowohl Release 3-Produktkomponenten als auch Release 4-Produktkomponenten auf einem Computer zu haben, wobei beide selektiv auf Release 5 aktualisiert werden können.

Aktualisierungen mehrerer Instanzen

Die Reihenfolge der Aktualisierungsverfahren innerhalb eines Aktualisierungsplans kann davon abhängen, ob Redundanz in einer Bereitstellungsarchitektur eingesetzt wird und wie diese erreicht wird. Hochverfügbarkeit, Skalierbarkeit, Wartungseignung oder eine Kombination dieser Dienstqualitäten kann durch mehrere Instanzen einer Java ES-Komponente erreicht werden. Drei Technologien nutzen redundante Komponenten in einer Java ES-Bereitstellungsarchitektur: Lastenausgleich (Directory Proxy Server, Webserver, Web Proxy Server, Anwendungsserver, Access Manager und Portal Server), Hochverfügbarkeitstechniken (Sun Cluster und High Availability Session Store) und Directory Server-Replikation.

In den meisten Fällen mit Redundanz müssen Aktualisierungen ohne erhebliche Ausfallzeiten durchgeführt werden. Bei diesen parallelen Aktualisierungen werden die redundanten Instanzen einer Komponente aktualisiert, ohne den von der Komponente bereitgestellten Dienst zu beeinträchtigen.

Redundante Instanzen werden normalerweise auf mehreren Computern bereitgestellt. Zur Aktualisierungsplanung müssen Sie möglicherweise die Aktualisierung der replizierten Komponenten von der Aktualisierung anderer Komponenten isolieren, um die Ausfallzeit so gering wie möglich zu halten. Sie

führen dazu auf jedem Computer alle vor der Aktualisierung notwendigen Aufgaben für die replizierten Komponenten aus, bevor Sie dann das sogenannte Rolling Upgrade, die Aktualisierung aller Komponenten nacheinander, durchführen.

Für alle Replikationstechnologien sind Konfigurations- oder Neukonfigurationsvorgänge notwendig, die sich auf die allgemeine Reihenfolge der Aktualisierung der Java ES-Komponenten auswirken können. Komponenten, die beispielsweise in einer Sun Cluster-Umgebung ausgeführt werden, erfordern möglicherweise die Aktualisierung von Sun Cluster vor der Aktualisierung der in der Sun Cluster-Umgebung ausgeführten Komponenten.

In den Kapiteln dieses *Aufrüstungshandbuchs*, in denen die Aktualisierung der einzelnen Produktkomponenten beschrieben ist, wird auch beschrieben, wie mehrere Instanzen für deren jeweilige Komponente aktualisiert werden.

Aspekte zum Betriebssystem

Ihr Java ES-Aktualisierungsplan kann durch eine Reihe von Aspekten bezüglich des Betriebssystems beeinflusst werden, wie im Folgenden beschrieben.

Erforderliche Betriebssystem-Patches

Die erfolgreiche Aktualisierung einer Java ES-Produktkomponente erfordert möglicherweise zunächst, Patches für das Betriebssystem anzuwenden oder das Betriebssystem auf die für die Java ES 5-Produktkomponente benötigte Version zu aktualisieren. Es ist jedoch besser, vor der Aktualisierung spezifischer Produktkomponenten das Betriebssystem als Ganzes auf die von Java ES 5 benötigte Version zu aktualisieren, anstatt die jeweils benötigten speziellen Patches oder Fehlerkorrekturen anzuwenden.

- **Solaris-Plattform.** Betriebssystem-Patches sind über die SunSolve-Website in Form eines Patch-Clusters erhältlich. In dem Patch-Cluster sind die Betriebssystem-Patches zusammengefasst, die als Gruppe angewendet werden können. Die zur Unterstützung von Java ES Release 5 für Solaris 9 und 10 erforderlichen Patch-Clusters erhalten Sie unter <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
- **Linux-Plattform.** Release-Versionen zur Aktualisierung erhalten Sie unter <https://www.redhat.com/apps/download/>. Es ist jedoch nicht erforderlich, das Linux-Betriebssystem zu aktualisieren, bevor Sie Java ES-Aktualisierungen durchführen.

Duale Aktualisierungen: Java ES und Betriebssystem-Software

Zwei Situationen können dazu führen, dass das Betriebssystem und die Java ES-Software nicht mehr zusammenpassen und Sie sowohl Java ES als auch das Betriebssystem aktualisieren müssen.

- Sie aktualisieren das Betriebssystem auf eine Version, die nicht von der installierten Java ES-Software unterstützt wird.

Java ES 2004Q2 (Release 2) wird zum Beispiel auf dem Betriebssystem Solaris 8 und 9 und unter Red Hat Enterprise Linux (RHEL) 2.1 unterstützt. Wenn Sie Ihr Betriebssystem auf das von Java ES Release 2 nicht unterstützte Betriebssystem Solaris 10 oder RHEL 3.0 aktualisieren möchten, müssen Sie Java ES Release 2 auf eine Java ES Release-Version aktualisieren, die die aktualisierte Plattform unterstützt, vorzugsweise auf Java ES 5 (Release 5).

Da es für die Aktualisierung einiger Java ES-Komponenten erforderlich ist, dass andere Java ES-Komponenten ausgeführt werden, sollten Sie nicht einfach nur Ihre Betriebssystem-Plattform auf Solaris 10 oder RHEL 3.0 aktualisieren (die Java ES Release 2 nicht unterstützen) und dann auf Java ES-Komponenten von Release 2 auf Release 5 aktualisieren.

- Sie aktualisieren Java ES damit auf eine Version, die nicht von der vorhandenen Betriebssystem-Software unterstützt wird.

Beispielsweise werden Java ES 2005Q1 (Release 3) und Java ES 2005Q4 (Release 4) auf Solaris 8 und RHEL 2.1 unterstützt. Wollen Sie jedoch Java ES auf Release 5 aktualisieren, die nicht auf Solaris 8 oder RHEL 2.1 unterstützt wird, so müssen Sie Ihr Betriebssystem auf Versionen aktualisieren, die von Java ES 5 (Release 5) unterstützt werden, vorzugsweise auf Solaris 10 oder RHEL 4.0.

In beiden Situationen müssen Sie sowohl die Java ES-Software als auch die Betriebssystem-Software aktualisieren. Zur Durchführung solcher dualer Aktualisierungen muss die folgende Reihenfolge eingehalten werden:

1. Sichern aller Java ES-Konfigurationsdateien und Anpassungen.
2. Deinstallieren der aktuell vorhandenen Java ES Release-Version.
3. Aktualisieren Ihrer Betriebssystem-Software.
4. Neuinstallieren von Java ES 5.
5. Konfigurieren von Java ES 5 anhand der in [Schritt 1](#) gespeicherten Konfigurationsdaten.

Aktualisierungen des Betriebssystems

In einigen Fällen überschreibt eine Aktualisierung des Solaris-Betriebssystems die vorhandenen gemeinsam genutzten Java ES-Komponenten durch frühere Versionen. In diesen Fällen können die korrekten Java ES-Versionen durch Aktualisierung der im Lieferumfang des Solaris-Betriebssystems enthaltenen Message Queue auf Version 5 wiederhergestellt werden. Die Aktualisierung von Message Queue erzwingt auch die Aktualisierung aller lokal vorhandener gemeinsam genutzter Komponenten.

Solaris 10-Umgebungen mit mehreren Zonen

Zur Installation und Aktualisierung von Java ES-Komponenten in einer Umgebung mit mehreren Zonen sind einige Aspekte zu beachten: Eine Beschreibung der Vorteile und Einschränkungen zur Bereitstellung von Java ES in Solaris 10-Zonen sowie die empfohlenen Vorgehensweisen zur Aktualisierung von Java ES-Komponenten in einer Umgebung mit mehreren Zonen erhalten Sie unter [„Aktualisierung von Java ES 5 und Solaris 10-Zonen“ auf Seite 65](#).

Java ES-Komponentenabhängigkeiten

Eine der wichtigsten Überlegungen beim Erstellen eines Aktualisierungsplans sind die Abhängigkeiten, die zwischen den verschiedenen Java ES-Komponenten in Ihrem bereitgestellten System bestehen. Die Reihenfolge, in der Sie Komponenten aktualisieren, hängt von der Art der Abhängigkeiten zwischen diesen Komponenten ab.

In diesem Abschnitt erhalten Sie Informationen zu den Abhängigkeiten zwischen Java ES-Komponenten, die sich auf Ihren Aktualisierungsplan auswirken.

- [Abhängigkeiten zu gemeinsam genutzten Komponenten](#)
- [Abhängigkeiten zu Produktkomponenten](#)

Abhängigkeiten zu gemeinsam genutzten Komponenten

[Tabelle 1-7 auf Seite 51](#) zeigt die Abhängigkeiten von Java ES 5 (Release 5)-Produktkomponenten zu gemeinsam genutzten Java ES -Komponenten. Die Abkürzungen der Produktkomponenten in den Spaltenbezeichnungen in [Tabelle 1-7](#) wurden aus [Tabelle 1-1 auf Seite 30](#) entnommen. Die Abkürzungen der gemeinsam genutzten Komponenten finden Sie in [Tabelle 1-2 auf Seite 31](#).

Innerhalb des Rasters von [Tabelle 1-7](#) sind zwingende Abhängigkeiten für Release 3 und Release 4 bis 5 mit „H“ und keine zwingenden Abhängigkeiten mit „S“ gekennzeichnet. Bei Aktualisierungen von Release 2 bis Release 5 handelt es sich bei allen gemeinsam genutzten Komponentenabhängigkeiten um zwingende Abhängigkeiten; alle gemeinsamen Komponenten müssen von Release 2 bis Release 5 aktualisiert werden.

Tabelle 1-7 Abhängigkeiten von Java ES 5 (Release 5)-Produktkomponenten zu gemeinsam genutzten Komponenten

Gemeinsam genutzte Komponente	AM	AS	DPS	DS	DS Console	HADB	JavaDB	MQ	PS	PSRA	SC	SCG	SR	WPS	WS
ANT		E							H	H			H		
ACL	E												H		
BDB	E														
CAC	H	E	H	H	H						S ¹	S ¹			
FIS															
ICU		E	H	H					E					E	E
IM-SDK									E						
Java SE	E	E	H	H	H	E	H	E	E	E	E	E	H	E	E
JAF	E	E							E	E			H		
JATO	E	E							E		E	E			
JavaHelp™	E	E						E							E
JavaMail™	E	E							E	E			H		E
JAXB	E	E													E
JAXP	E	E							E	E			H		E
JAXR	E	E											H		E
JAX-RPC	E	E											H		E
JAXWS															E
JCAPI															
JDMK	H	E	H	H	H						E	E			E
JSS	E								E	E				E	E
JSTL															
KTSE									E					E	E
LDAP C SDK	H			H										E	E
LDAP J SDK	E														
MA Core	E								H	H					
MFWK	H			H											

Tabelle 1-7 Abhängigkeiten von Java ES 5 (Release 5)-Produktkomponenten zu gemeinsam genutzten Komponenten *(Fortsetzung)*

Gemeinsam genutzte Komponente	AM	AS	DPS	DS	DS Console	HADB	JavaDB	MQ	PS	PSRA	SC	SCG	SR	WPS	WS
NSPR	E	E	H	H				H	E	E	E	E		E	H
NSS	E	E		H				H	E	E	E	E		E	H
SAAJ	E	E							E	E			H		
SASL				H										E	E
SEDC											E	E			
SJWC	E	E			H						E	E			
WSCL	E	E											H		E
XWSS													H		

1. Diese Abhängigkeit besteht besonders zu Common Agent Container (CAC) Version 1.1.

Die in [Tabelle 1-7](#) gezeigten Abhängigkeiten für Produktkomponenten verdeutlichen sowohl direkte als auch indirekte Abhängigkeiten zu gemeinsam genutzten Komponenten. Das heißt, eine Produktkomponente kann von einer bestimmten gemeinsam genutzten Komponente abhängen (direkte Abhängigkeit), die wiederum von einer oder mehreren gemeinsam genutzten Komponenten abhängt (indirekte Abhängigkeit). Die folgende Abbildung verdeutlicht die gegenseitigen Abhängigkeiten der gemeinsam genutzten Komponenten.

Abbildung 1-1 Abhängigkeiten von gemeinsam genutzten Komponenten

In [Tabelle 1-7](#) ist angegeben, welche gemeinsam genutzten Komponenten aktualisiert werden müssen, wenn Sie auf eine oder mehrere Produktkomponenten auf einem Computer aktualisieren.

Da jedoch gemeinsam genutzte Komponenten synchronisiert werden müssen (siehe „[Aktualisierungen gemeinsam genutzter Komponenten](#)“ auf Seite 38), können Sie gemeinsam genutzte Java ES-Komponenten nicht einzeln aktualisieren, sondern müssen alle gemeinsam genutzten Komponenten auf einem Computer oder in einer Betriebssystem-Instanz gleichzeitig auf Release 5 aktualisieren.

Wenn keine zwingenden Aktualisierungsabhängigkeiten bestehen, müssen Sie gemeinsam genutzte Komponenten nicht aktualisieren. Es wird jedoch empfohlen, die zugrundeliegenden gemeinsam genutzten Java ES-Komponenten auf die jeweils aktuellste Version zu aktualisieren. Wenn Produktkomponenten mit dem Java ES-Installationsprogramm installiert oder aktualisiert werden, werden alle gemeinsam genutzten Komponenten auf dem Host-Computer automatisch auf Release 5 synchronisiert.

Verfahren zur manuellen Aktualisierung gemeinsam genutzter Komponenten finden Sie in [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“](#)..

Abhängigkeiten zu Produktkomponenten

Abhängigkeiten zu Produktkomponenten werden in zwei allgemeine Kategorien unterteilt: Runtime-Abhängigkeiten und Konfigurationsabhängigkeiten.

- **Runtime-Abhängigkeiten.** Die Ausführung eines Softwaresystems basiert auf der Interaktion zwischen den bereitgestellten Komponenten. Die Infrastrukturabhängigkeiten zwischen Java ES-Produktkomponenten werden im *Java Enterprise System 5 – Technische Übersicht* erläutert. Wenn für eine Release 5-Produktkomponente eine zwingende Abhängigkeit zu einer anderen Produktkomponente besteht, kann die abhängige Komponente nur dann erfolgreich aktualisiert und wie vorgesehen verwendet werden, wenn die Komponente, von der sie abhängig ist, ebenfalls aktualisiert wird.
- **Konfigurationsabhängigkeiten.** In einigen Fällen muss eine Java ES-Komponente installiert, konfiguriert und für die Konfiguration einer anderen Komponente ausgeführt werden. Beispielsweise muss ein Directory Server-Benutzer-/Gruppenverzeichnis für einen zu registrierenden Access Manager-Dienst ausgeführt sein. Das Aktualisierungsverfahren einer Komponente umfasst häufig die Neukonfiguration der aktualisierten Komponente oder die Migration der Konfigurationsdaten. Konfigurationsabhängigkeiten können sich auf die Reihenfolge der Aktualisierungsvorgänge auswirken.

Für Runtime-Abhängigkeiten kann es drei Arten von Abhängigkeiten zwischen Produktkomponenten geben:

- **Obligatorisch.** Die Komponente kann ohne die sie unterstützende Komponente nicht arbeiten.
- **Optional.** Die Komponente kann ohne die sie unterstützende Komponente arbeiten, eine Unterfunktion benötigt jedoch die unterstützende Komponente.
- **Co-Abhängigkeit.** Beide Komponenten können ohne Unterstützung der jeweils anderen arbeiten, beide Komponenten zusammen können jedoch in bestimmten Fällen eine erweiterte Funktion oder Leistung bieten.

In der folgenden Tabelle werden die Abhängigkeiten und Abhängigkeitsbeziehungen zwischen den in Tabelle [Tabelle 1-1 auf Seite 30](#) aufgeführten Java ES-Produktkomponenten beschrieben. Diese Informationen können dazu dienen, die zwingenden Abhängigkeiten festzustellen, die sich auf Ihren Aktualisierungsplan auswirken.

In der ersten Spalte sind die Release 5-Produktkomponenten aufgelistet. Die zweite Spalte zeigt andere Java ES-Komponenten, von der eine andere Release 5-Komponente abhängig ist. Die dritte Spalte enthält die Java ES

Release-Versionen, die eine Release 5-Abhängigkeit unterstützen. Die vierte Spalte kennzeichnet die Abhängigkeitsbeziehung und die letzte Spalte gibt spezielle Merkmale der Abhängigkeit an, wie etwa, ob die unterstützende Komponente lokal vorhanden sein muss (im Gegensatz zu dezentral) oder ob andere Drittanbieter-Produkte diese Abhängigkeit unterstützen können.

Wenn zu einer Produktkomponente, die Sie auf Release 5 aktualisieren, eine Abhängigkeit zu Release 5 einer unterstützenden Komponente besteht (im Gegensatz zu einer früheren Release-Version), dann stellt die unterstützende Komponente eine zwingende Aktualisierungsabhängigkeit dar. Die unterstützende Komponente muss ebenfalls auf Release 5 aktualisiert werden.

Tabelle 1-8 Abhängigkeiten der Java ES-Produktkomponenten

Release 5 Produktkomponente	Abhängigkeit ¹	Java ES Release	Art der Abhängigkeit	Merkmale
Access Manager	Directory Server	2-5	Obligatorisch: Speichert Konfigurationsdaten und ermöglicht die Suche nach Benutzerdaten	
	J2EE-Webcontainer:		Obligatorisch: Stellt Webcontainer-Runtime-Dienste bereit	Nur lokal
	- Anwendungsserver	4-5		Ebenfalls unterstützt;
	- Webserver	4-5		- Weblogic ² - WebSphere ³
Access Manager SDK	Access Manager	3-5	Obligatorisch: Stellt Access Manager Dienste zur Verfügung	
Access Manager	Access Manager	4-5	Obligatorisch: Stellt Access Manager Dienste zur Verfügung	
Dezentrale Authentifizierung	J2EE-Webcontainer:		Obligatorisch: Stellt Webcontainer-Runtime-Dienste bereit	Nur lokal
	- Anwendungsserver	4-5		Ebenfalls unterstützt;
	- Webserver	4-5		- Weblogic ² - WebSphere ³
Access Manager Sitzungs-Failover	Access Manager	5	Obligatorisch: Stellt Access Manager Dienste zur Verfügung	
	Message Queue	4-5	Obligatorisch: Stellt zuverlässiges asynchrones Messaging zur Verfügung	

Tabelle 1-8 Abhängigkeiten der Java ES-Produktkomponenten (*Fortsetzung*)

Release 5 Produktkomponente	Abhängigkeit ¹	Java ES Release	Art der Abhängigkeit	Merkmale
Anwendungsserver	Message Queue	3-5	Obligatorisch: Stellt zuverlässiges asynchrones Messaging zur Verfügung	Nur lokal
	High Availability Session Store (HADB)	5	Obligatorisch: Speichert den Sitzungsstatus für die Unterstützung von Failover zwischen den Instanzen	Nur lokal
	Java DB	5	Obligatorisch: Stellt eine Standard-Entwicklerdatenbank und andere persistente Speichermöglichkeiten zur Verfügung.	Nur lokal
	Webserver	3-5	Optional: Stellt Lastenausgleich zwischen Instanzen zur Verfügung	Nur lokal
Directory Proxy Server	Directory Server	1-5	Co-Abhängigkeit: Schafft höhere Sicherheit und Leistung für Verzeichnisanfragen. Überträgt Daten an den Directory Proxy Server	
Directory Server	Directory Proxy Server	1-5	Co-Abhängigkeit: Schafft höhere Sicherheit und Leistung für Verzeichnisanfragen. Verteilt die Last und nimmt Daten vom Directory Server in den Cache-Speicher auf	
High Availability Session Store (HADB)	Keine			
Java DB	Keine			
Message Queue	Directory Server	2-5	Optional: Speichert verwaltete Objekte und Benutzerdaten	
	J2EE-Webcontainer:		Optional: Unterstützt die HTTP-Übertragung zwischen Client und Message Queue-Broker	
	- Anwendungsserver	2-5		
	- Webserver	2-5		
	Java DB	5	Optional: Speichert persistente Meldungen.	Nur lokal
	Sun Cluster	2-5	Optional: Unterstützt hohe Verfügbarkeit	

Tabelle 1-8 Abhängigkeiten der Java ES-Produktkomponenten (*Fortsetzung*)

Release 5 Produktkomponente	Abhängigkeit ¹	Java ES Release	Art der Abhängigkeit	Merkmale
Portal Server	Directory Server	4-5	Obligatorisch: Speichert und ermöglicht die Suche nach Benutzerprofilen	
	J2EE-Webcontainer:		Obligatorisch: Stellt Webcontainer-Runtime-Dienste bereit	Nur lokal
	- Anwendungsserver	4-5		Ebenfalls unterstützt;
	- Webserver	4-5		- Weblogic ² - WebSphere ³
	Access Manageroder Access Manager SDK	4-5	Obligatorisch: Stellt Authentifizierungs- und Autorisierungsdiensten, Single-Sign-On, bereit	Nur lokal (Wenn Access Manager dezentral vorhanden ist, muss Access Manager SDK lokal vorhanden sein)
	Portal Server Secure Remote Access	5	Optional: Stellt sicheren dezentralen Zugriff über die Gateway-, Rewriter Proxy- und Netlet Proxy-Komponenten zur Verfügung	
	Service Registry Client	5	Obligatorisch: Stellt Bibliotheken zur Verfügung, die zur Kompilierung benötigt werden	
Portal Server Secure Remote Access Gateway	Java DB	5	Optional: Unterstützt verschiedene Portlet-Anwendungen	
	Portal Server	5	Obligatorisch: Unterstützt Gateway-Funktionen	
	Access Manageroder Access Manager SDK	4-5	Obligatorisch: Stellt Authentifizierungs- und Autorisierungsdiensten, Single-Sign-On, bereit	Nur lokal (Wenn Access Manager dezentral vorhanden ist, muss Access Manager SDK lokal vorhanden sein)
	Directory Server	4-5	Obligatorisch: Speichert und ermöglicht die Suche nach Benutzerdaten	

Tabelle 1-8 Abhängigkeiten der Java ES-Produktkomponenten (*Fortsetzung*)

Release 5 Produktkomponente	Abhängigkeit¹	Java ES Release	Art der Abhängigkeit	Merkmale
Rewriter Proxy	Portal Server	5	Obligatorisch: Unterstützt Rewriter Proxy-Funktionen	
Netlet Proxy	Portal Server	5	Obligatorisch: Unterstützt Netlet Proxy-Funktionen	
Service Registry Bereitstellung	Anwendungsserver	5	Obligatorisch: Stellt Container-Runtime-Dienste bereit	Nur lokal
	Java DB	5	Obligatorisch: Stellt eine Standarddatenbank zum Speichern von Diensten und zugehörigen Metadaten zur Verfügung	Nur lokal
	Service Registry Client	5	Obligatorisch: Stellt erforderliche Client-Bibliotheken zur Verfügung	Nur lokal
Client	Keine			
Sun Cluster	Keine			
Sun Cluster-Agenten	Sun Cluster	4-5	Obligatorisch: Stellt den Zugriff auf Sun Cluster-Dienste zur Verfügung	Nur lokal
Sun Cluster Geographic Edition	Sun Cluster	4-5	Obligatorisch: Unterstützt Sun Cluster Geographic Edition-Funktionen	Nur lokal
Web Proxy Server	Directory Server	2-5	Optional: Stellt LDAP-basierte Authentifizierung zur Verfügung	
	Webserver	2-5	Co-Abhängigkeit: Schafft höhere Sicherheit und Leistung für HTTP-Anfragen. Überträgt Daten an den Web Proxy Server	Ebenfalls unterstützt; - Weblogic ² - WebSphere ³
Webserver	Directory Server	1-5	Optional: Stellt LDAP-basierte Authentifizierung zur Verfügung	
	Web Proxy Server	1-5	Co-Abhängigkeit: Schafft höhere Sicherheit und Leistung für HTTP-Anfragen. Verteilt die Last und nimmt Daten vom Webserver in den Cache-Speicher auf	

1. Die Abhängigkeiten für jede Produktkomponente sind in der Reihenfolge aufgeführt, in der sie normalerweise aktualisiert werden.
2. BEA WebLogic Server
3. IBM WebSphere Application Server

Richtlinien für die Aktualisierungsreihenfolge

Die Wahl zwischen selektiver Aktualisierung und Aktualisierung aller Komponenten, die Auswirkungen zwingender Aktualisierungsabhängigkeiten sowie alle anderen Faktoren, die in den vorausgegangenen Abschnitten behandelt wurden, können bestimmen, welche Java ES-Komponenten Sie aktualisieren wollen und in welcher Reihenfolge Sie diese aktualisieren müssen. Es gelten dennoch allgemeine Richtlinien für die Aktualisierungsreihenfolge; diese sind jedoch nicht in jedem Fall anzuwenden.

Die folgende Liste gibt die Reihenfolge an, in der die Java ES-Komponenten auf einem Computer oder in einem bereitgestellten System erfolgreich aktualisiert werden können. Bei der Planung Ihrer Aktualisierung können Sie die Komponenten, die nicht zu Ihrer Bereitstellungsarchitektur gehören, ausschließen. Optional können Sie bei der Durchführung einer selektiven Aktualisierung jene Komponenten ausschließen, für die nicht zwingende Aktualisierungsabhängigkeiten bestehen.

Die Kapitel dieses *Aufrüstungshandbuchs* sind in der Reihenfolge strukturiert, in der die Komponenten in der folgenden Liste aufgeführt sind.

HINWEIS Stellen Sie vor der Aktualisierung von Java ES-Komponenten sicher, dass Sie Ihr Betriebssystem aktualisieren, falls dies erforderlich ist (siehe auch [„Erforderliche Betriebssystem-Patches“ auf Seite 47](#)).

Lesen Sie auch die [„Sonderfälle“ auf Seite 64](#), um zu sehen, ob einige davon auf Ihr Aktualisierungsszenario zutreffen.

1. **Gemeinsam genutzte Komponenten** (siehe [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#))

Gemeinsam genutzte Komponenten sollten vor der Aktualisierung der Komponenten aktualisiert werden, die von diesen Komponenten abhängig sind. In den meisten Fällen werden gemeinsam genutzte Komponenten mithilfe des Java ES-Installationsprogramms aktualisiert. Bei Web Proxy Server und Portal Server müssen Sie gemeinsam genutzte Komponenten jedoch explizit aktualisieren.

2. Sun Cluster-Software (siehe [Kapitel 3, „Sun Cluster-Software“](#) auf Seite 83)

Wenn Komponenten in einer Sun Cluster-Umgebung ausgeführt werden und die Sun Cluster-Software aktualisiert werden muss, sollte die Software vor den Komponenten aktualisiert werden, die die Sun Cluster-Dienste verwenden. Wenn Sun Cluster-Agenten aktualisiert werden, sollten diese als Teil der Sun Cluster-Aktualisierung aktualisiert werden.

3. Sun Cluster Geographic Edition-Software (siehe [Kapitel 4, „Sun Cluster Geographic Edition“](#) auf Seite 97)

Sun Cluster Geographic Edition sollte nach der Sun Cluster-Software aktualisiert werden, von der diese abhängt. Sie sollte vor Aktualisierung der Komponenten aktualisiert werden, die die Sun Cluster-Dienste verwenden.

4. Directory Server (Siehe [Kapitel 5, „Directory Server“](#) auf Seite 109)

Viele Komponenten speichern Benutzer- oder Konfigurationsdaten in Directory Server. Aktualisierungen von Directory Server sollten daher grundsätzlich vor der Aktualisierung der Komponenten durchgeführt werden, für die eine Runtime- oder Konfigurationsabhängigkeit zu Directory Server besteht.

5. Directory Proxy Server (siehe [Kapitel 6, „Directory Proxy Server“](#) auf Seite 127)

Für Directory Proxy Server besteht eine nicht zwingende Aktualisierungsabhängigkeit zu Directory Server und kann daher jederzeit aktualisiert werden. Einige Komponenten könnten jedoch über den Directory Proxy Server auf den Directory Server zugreifen. Wenn daher der Directory Proxy Server aktualisiert werden soll, sollte er direkt nach dem Directory Server aktualisiert werden.

6. Webserver (Siehe [Kapitel 7, „Webserver“](#) auf Seite 143)

Eine Reihe von Java ES-Komponenten erfordern Unterstützung durch einen Webcontainer. Der Webcontainer sollte vor den Komponenten aktualisiert werden, die die Webcontainer-Dienste erfordern. Webcontainer-Dienste werden üblicherweise von Webserver oder Anwendungsserver bereitgestellt; wenn jedoch in Ihrer Bereitstellungsarchitektur beide Komponenten vorhanden sind, aktualisieren Sie zuerst Webserver, bevor Sie Anwendungsserver aktualisieren.

7. Java DB (Siehe [Kapitel 8, „Java DB“ auf Seite 171](#))

Java DB muss vor Anwendungsserver aktualisiert werden, weshalb Java DB als Standarddatenbank vorhanden sein muss. Java DB wird jedoch automatisch mithilfe des Java ES-Installationsprogramms installiert, wenn dieses den Anwendungsserver aktualisiert.

8. High Availability Session Store (siehe [Kapitel 9, „High Availability Session Store“ auf Seite 179](#))

High Availability Session Store (HADB) sollte vor Anwendungsserver aktualisiert werden, der High Availability Session Store für Hochverfügbarkeitszwecke benötigt. HADB wird jedoch automatisch mithilfe des Java ES-Installationsprogramms installiert, wenn dieses den Anwendungsserver aktualisiert.

9. Message Queue (Siehe [Kapitel 10, „Message Queue“ auf Seite 193](#))

Message Queue muss vor Anwendungsserver aktualisiert werden, wozu Message Queue mit der Java Enterprise Edition (Java EE) kompatibel sein muss. Message Queue wird jedoch automatisch mithilfe des Java ES-Installationsprogramms installiert, wenn dieses den Anwendungsserver aktualisiert.

10. Anwendungsserver (Siehe [Kapitel 11, „Anwendungsserver“ auf Seite 219](#))

Anwendungsserver ist abhängig von Message Queue und High Availability Session Store und sollte deshalb gegebenenfalls nach diesen Komponenten aktualisiert werden. Anwendungsserver kann auch aufgrund von dessen Plug-in zum Lastenausgleich von Webserver abhängig sein. Wenn Sie diese Funktion nutzen, sollten Sie Anwendungsserver nach Webserver aktualisieren.

11. Service Registry (Siehe [Kapitel 12, „Service Registry“ auf Seite 249](#))

Service Registry kann jederzeit nach Anwendungsserver aktualisiert werden, da Service Registry aufgrund der Runtime-Container-Dienste von Anwendungsserver abhängig ist.

12. Web Proxy Server (Siehe [Kapitel 13, „Web Proxy Server“ auf Seite 263](#))

Web Proxy Server kann zu jedem Zeitpunkt aktualisiert werden. Grundsätzlich wird die Aktualisierung jedoch nach der Aktualisierung der Webserver- oder Anwendungsserver-Komponente durchgeführt, für den Web Proxy Server einen Proxy-Dienst bereitstellt. Web Proxy Server ist eine neue Java ES Release 5-Komponente, deren frühere Version, die keine Java ES Release-Komponente war, aktualisiert werden kann.

13. Access Manager (siehe [Kapitel 14, „Access Manager“](#) auf Seite 281)

Access Manager spielt eine zentrale Rolle bei der Authentifizierung und Autorisierung, einschließlich Single-Sign-On. Diese Komponente sollte vor den Komponenten aktualisiert werden, die von Access Manager hinsichtlich dieser Dienste abhängen.

14. Portal Server (Siehe [Kapitel 15, „Portal Server“](#) auf Seite 337)

Portal Server hängt von vielen der oben genannten Komponenten ab (Directory Server, ein Webcontainer und Access Manager) und sollte gegebenenfalls nach diesen Komponenten aktualisiert werden.

15. Portal Server Secure Remote Access (Siehe [Kapitel 16, „Portal Server Secure Remote Access“](#) auf Seite 413)

Portal Server Secure Remote Access muss zusammen mit Portal Server aktualisiert werden.

Sonderfälle

Bei Planung einer Aktualisierung von Java ES-Komponenten auf Release 5 sollten einige Sonderfälle beachtet werden. Diese sind im folgenden Abschnitt beschrieben.

Selektive Aktualisierung: Anwendungsserver nicht aktualisiert

Wenn Sie eine selektive Aktualisierung einer Java ES-Komponente auf Java ES 5 auf einem Computer durchführen, auf dem Anwendungsserver Release 3 oder Release 4 ausgeführt ist (8.1), und dabei Anwendungsserver nicht auf Release 5 aktualisieren, so müssen Sie einige Situationen beachten, um die reibungslose Funktion von Anwendungsserver sicher zu stellen:

- **Fehler bei der JSP-Kompilierung.** Vor Durchführung einer selektiven Aktualisierung sollten Sie zunächst den in der folgenden Tabelle aufgeführten Anwendungsserver-Patch anwenden.

Tabelle 1-9 Patches¹, die erforderlich sind, wenn Anwendungsserver nicht auf Release 5 aktualisiert wird

Beschreibung	Patch-ID: Solaris 9 & 10	Patch-ID: Linux
Fehlerkorrektur für Release 3 und Release 4 Anwendungsserver	119166-17 (SPARC) 119166-17 (x86)	119168-17

1. Patch-Versionsnummern gehören zu den Mindestanforderungen. Wenn neuere Versionen verfügbar sind, verwenden Sie anstelle der in dieser Tabelle genannten Versionen die neueren Versionen.

Wenn Sie den Patch nicht anwenden, treten in Anwendungsserver Fehler in der JSP-Kompilierung auf. (Die Patches in [Tabelle 1-9](#) können zur Behebung des Problems auch nachträglich angewandt werden.)

- **Verlagerung von Binärdateien mit freigegebenen ANT-Komponenten auf Linux.** Release 5 ANT ist nun in einem anderen Pfad gespeichert als in früheren Versionen. Die Anwendungsserver-Umgebungsvariable, die in Datei *AppServer8-base/config/asenv.conf* angegeben ist und auf ANT verweist, muss geändert werden von:

`AS_ANT_LIB="/opt/sun/lib"`

in:

`AS_ANT_LIB="/opt/sun/share/lib"`

und Anwendungsserver muss danach neu gestartet werden.

Aktualisierung von Portal Server Interim Feature Release (IFR) 7.0 auf Java ES 5

Wenn Sie Portal Server in einer Webserver-Umgebung von Interim Feature Release (IFR) 7.0 2005Q4 auf Release 5 aktualisieren, informieren Sie sich unter „Aktualisieren von Portal Server von der Interim Feature Release 7.0“ auf Seite 392 über die Ausnahmen zu den Richtlinien unter „Richtlinien für die Aktualisierungsreihenfolge“ auf Seite 60.

Aktualisierung von Java ES 5 und Solaris 10-Zonen

In diesem Abschnitt werden Aspekte zur Aktualisierung von Java ES-Software in Solaris 10-Zonen behandelt und Vorgehensweise in einer solchen Umgebung empfohlen. In diesem Abschnitt erhalten Sie ergänzende Informationen zu Java ES 5 und Solaris 10-Zonen unter *Java Enterprise System 5 – Handbuch zur Installationsplanung*, <http://docs.sun.com/doc/820-0080>.

Er umfasst folgende Themen:

- [Zonenunterstützung im Java ES-Installationsprogramm](#)
- [Empfohlene Vorgehensweisen zur Aktualisierung](#)
- [Sonderfälle oder Ausnahmen](#)

Zonenunterstützung im Java ES-Installationsprogramm

Das Java ES 5-Installationsprogramm bietet qualifizierte Unterstützung der Zonen zur Aktualisierung (und Installation) von Java ES-Produktkomponenten und zur Synchronisierung von gemeinsam genutzten Komponenten. Im Installationsprogramm wurden bestimmte Richtlinien implementiert, um problematische Aktualisierungsszenarios zu verhindern.

Aktualisierung von Produktkomponenten

Wie unter „[Verwendung der Aktualisierungsfunktionen im Java ES Installationsprogramm.](#)“ auf Seite 34 beschrieben, kann das Java ES-Installationsprogramm dazu verwendet werden, eine begrenzte Anzahl an Produktkomponenten und deren gemeinsam genutzte Komponenten zu aktualisieren. Die Möglichkeit zur Aktualisierung besteht für globale Zonen und alle nicht globalen Zonen.

Es gibt jedoch drei Ausnahmen zu diesem Verhalten, das sich auf die Zonen bezieht:

- In Sparse-Root-Zonen können einige Komponenten nicht installiert oder aktualisiert werden, da sie sich in schreibgeschützten Verzeichnissen befinden. In diesen Fällen wird die Aktualisierung von Produktkomponenten so lange verschoben, bis die betreffenden gemeinsam genutzten Komponenten in der globalen Zone installiert oder aktualisiert wurden. Im Installationsprogramm wird folgende Meldung angezeigt: „Die folgenden gemeinsam genutzten Komponenten, die für die von Ihnen ausgewählten Komponenten erforderlich sind, können in einer Sparse-Root-Zone nicht installiert oder aktualisiert werden. Installieren oder aktualisieren Sie diese gemeinsam genutzten Komponenten in der globalen Zone, bevor Sie fortfahren. Verwenden Sie dazu die Option „Alle gemeinsam genutzten Komponenten“.“
- Sowohl Anwendungsserver als auch Message Queue sind im Lieferumfang des Solaris -Betriebssystems enthalten. Keine der beiden Versionen kann direkt in einer Sparse-Root-Zone aktualisiert werden. Weitere Informationen zu diesen im Lieferumfang enthaltenen Komponenten erhalten Sie unter „[Sonderfälle zu den Produktkomponenten](#)“ auf Seite 69.
- Wenn nicht globale Zonen vorhanden sind und anstelle einer Aktualisierung aller bereits installierter gemeinsam genutzter Komponenten bzw. einer Installation fehlender und von einer ausgewählten Komponente benötigten Komponenten, synchronisiert das Installationsprogramm *alle* Java ES gemeinsam genutzten Komponenten auf Release 5 ungeachtet dessen, ob sie

von einer bestimmten Produktkomponente benötigt werden oder nicht. Dadurch können alle gemeinsam genutzten Release 5-Komponenten auf nicht globale Zonen übernommen werden, wodurch sichergestellt wird, dass keine unterschiedlichen Versionen der gemeinsam genutzten Komponenten in nicht globalen Zonen vorhanden sind.

HINWEIS Es gibt einige besondere Fälle oder Ausnahmen, die eine Installation oder Aktualisierung von Produktkomponenten in nicht globalen Zonen beeinträchtigen könnten. Diese sind beschrieben unter [„Sonderfälle oder Ausnahmen“ auf Seite 69](#).

Alle gemeinsam genutzten Komponenten synchronisieren

In Release 5 steht eine Option zur Synchronisierung gemeinsam genutzter Komponenten zur Verfügung, um Situationen gerecht zu werden, in denen alle gemeinsam genutzten Komponenten auf Release 5 synchronisiert werden müssen. Wenn die Option „Alle gemeinsam genutzten Komponenten“ ausgewählt wird, aktualisiert das Installationsprogramm alle aktuell installierten gemeinsam genutzten Komponenten und installiert alle fehlenden gemeinsam genutzten Komponenten, ungeachtet dessen, ob sie von einer speziellen Produktkomponente benötigt werden oder nicht. Diese Option trifft auf globale Zonen und Whole-Root-Zonen zu (nicht aber auf Sparse-Root-Zonen).

Die Option „Alle gemeinsam genutzten Komponenten“, die genauer unter [„Alle gemeinsam genutzten Komponenten synchronisieren“ auf Seite 74](#) beschrieben ist, wird für die folgenden beiden zonenbasierten Aktualisierungsszenarios benötigt.

- **Produktkomponenten manuell aktualisieren.** Die Option Alle gemeinsam genutzten Komponenten ist erforderlich zur Installation und Aktualisierung von gemeinsam genutzten Produktkomponenten, die zur Installation von Produktkomponenten benötigt werden, die *nicht* mithilfe des Java ES-Installationsprogramms aktualisiert werden können.
- **Aktualisierungen in einer Sparse-Root-Zone.** Einige gemeinsam genutzte Komponenten können nicht in Standard-Sparse-Root-Zonen installiert oder aktualisiert werden. Wenn Sie demnach das Java ES-Installationsprogramm zur Aktualisierung von Produktkomponenten in Sparse-Root-Zonen verwenden, müssen Sie möglicherweise zunächst die gemeinsam genutzten Komponenten in der globalen Zone aktualisieren, und zwar abhängig davon, welche gemeinsam genutzten Komponenten davon betroffen sind. Sie verwenden dazu die Option Alle gemeinsam genutzten Komponenten in der globalen Zone, um die in diesem Fall benötigten gemeinsam genutzten Komponenten zu installieren oder zu aktualisieren.

Eine Zusammenfassung zum Verhalten des Java ES-Installationsprogramms in den Zonen im Hinblick auf gemeinsam genutzte Komponenten erhalten Sie in der Beschreibung zu Java ES 5 und Solaris 10-Zonen unter *Java Enterprise System 5 – Handbuch zur Installationsplanung*, <http://docs.sun.com/doc/820-0880>.

Empfohlene Vorgehensweisen zur Aktualisierung

Wenn Sie einen Aktualisierungsplan aufstellen, sollten Sie vorher die in mehreren Zonen vorhandenen Bereitstellungen der Java ES-Software ausfindig machen und die Strategien zur Installation und Verwaltung der Zonen beachten, die unter *Java Enterprise System 5 – Handbuch zur Installationsplanung*, <http://docs.sun.com/doc/820-0880> beschrieben sind. In einigen Fällen müssen Sie möglicherweise die in einer oder mehreren Zonen vorhandenen Komponenten deinstallieren und in anderen Zonen neu installieren, um die folgenden empfohlenen Vorgehensweisen durchführen zu können:

- Unterschiedliche Strategien nicht vermischen. Im Besonderen:
 - Gestalten Sie Ihre Strategie zur Bereitstellung und Verwaltung von Java ES-Zonen so einfach wie möglich. Vermischen Sie keine Whole-Root- und Sparse-Root-Bereitstellungen von Java ES-Komponenten auf demselben Computer. (Verfahren und Vorgehensweisen zur Unterstützung von Bereitstellungen der Sparse-Root-Zonen können Bereitstellungen von Whole-Root-Zonen beeinträchtigen.)
 - Installieren Sie eine Java ES-Produktkomponente nicht gleichzeitig in der globalen Zone und in nicht globalen Zonen, auch wenn es sich um unterschiedliche Versionen handelt. (Vorgehensweisen zur Aktualisierung einer Bereitstellung in einer globalen Zone können Bereitstellungen in nicht globalen Zonen zerstören.)
 - Wenn Java ES-Komponenten mit Release 4 (oder einer früheren Version) in einer Whole-Root-Zone installiert wurden, dürfen Sie in der globalen Zone vorhandene Java ES-Komponenten nicht auf Release 5 aktualisieren. Eine Aktualisierung in der globalen Zone könnte eine Vermischung von Release 4- und Release 5-Dateien in der Whole-Root-Zone verursachen.
- Vorgehensweisen zur Aktualisierung:

- Wenn Sie alle installierten Release 4-Produktkomponenten auf Release 5 aktualisieren wollen, synchronisieren Sie alle gemeinsam genutzten Java ES-Komponenten in der globalen Zone und aktualisieren Sie dann die gewünschten Produktkomponenten in den Zonen, in denen diese installiert wurden. (Gemeinsam genutzte Release 5-Komponenten sind rückwärts kompatibel.)
- Wenn Sie Release 4- oder Release 5-Produktkomponenten in einer Umgebung ohne Zonen installiert haben und nicht globale Zonen zur Umgebung hinzufügen wollen, um Produktkomponenten in diesen neuen nicht globalen Zonen zu installieren, so müssen Sie möglicherweise die Komponenten in der globalen Zone deinstallieren und diese in den nicht globalen Zonen erneut installieren.

Sonderfälle oder Ausnahmen

Es gibt eine Reihe von Sonderfällen, die sich teilweise daraus ergeben, dass einige gemeinsam genutzte Java ES-Komponenten und einige Java ES-Produktkomponenten im Lieferumfang von Solaris 10 vorhanden sind. Daher sind diese Java ES-Komponenten automatisch in der globalen Zone vorhanden und damit auch in jeder nicht globalen Zone, die durch diese globale Zone angelegt wird.

Sonderfälle zu den Produktkomponenten

- **Message Queue.** Message Queue ist im Lieferumfang von Solaris 10 vorhanden und wird daher automatisch übernommen, wenn nicht globale Zonen angelegt werden (außer Sie haben Message Queue vorher aus der globalen Zone entfernt). Message Queue kann nicht in Sparse-Root-Zonen installiert oder aktualisiert werden. Wenn Message Queue jedoch mithilfe des Java ES-Installationsprogramms in einer globalen Zone installiert oder aktualisiert wird, so wird sie im Gegensatz zu anderen Produktkomponenten standardmäßig auf nicht globale Zonen übernommen.
- **Anwendungsserver.** Anwendungsserver ist im Lieferumfang von Solaris 10 vorhanden und wird daher automatisch übernommen, wenn nicht globale Zonen angelegt werden (außer Sie haben Anwendungsserver vorher aus der globalen Zone entfernt). Wenn die im Lieferumfang enthaltene Komponente Anwendungsserver, die unter /usr installiert wurde, auf diese Weise übernommen wurde, so kann sie nicht mithilfe des Java ES-Installationsprogramms in einer Sparse-Root-Zone aktualisiert werden (/usr ist standardmäßig schreibgeschützt). Zur Behebung dieses Problems müssen die im Lieferumfang vorhandenen Anwendungsserver-Pakete

manuell aus der globalen Zone entfernt werden, bevor Release 5-Anwendungsserver in einer Sparse-Root-Zone installiert werden kann. Siehe auch „[Nur Solaris: Entfernen Sie manuell die im Betriebssystem enthaltenen Anwendungsserver-Pakete.](#)“ auf Seite 236.

- **Sun Cluster.** Die Sun Cluster-Software wird in nicht globalen Zonen nicht unterstützt.

Sonderfälle zu den gemeinsam genutzten Komponenten

- **Sun Java Web Console (SJWC).** SJWC-Pakete, die im Lieferumfang von Solaris 10 (Update 1 und Update 2) enthalten sind, können nicht mithilfe des Java ES-Installationsprogramms entfernt werden. Bei diesen älteren SJWC-Paketen ist Attribut `SUNW_PKG_ALLZONES` auf `True` gesetzt, was bedeutet, dass das Paket in allen Zonen identisch sein muss und nur vom globalen Administrator verwaltet werden kann. Diese Pakete müssen daher manuell aus der globalen Zone entfernt und durch die richtigen Pakete ersetzt werden.

Wenn das Java ES-Installationsprogramm eine ausgewählte Produktkomponente in einer nicht globalen Zone installieren will und dabei feststellt, dass SJWC aktualisiert werden muss, so bricht das Installationsprogramm den Vorgang ab. Dies trifft zu, wenn eine Installation auf Solaris 10, Update 1 und 2 vorgenommen wird.

Um dieses Problem zu umgehen, wurde ein Skript entwickelt, das die alten SJWC-Paket aus der globalen Zone entfernt und durch Release 5-SJWC ersetzt, das den richtigen Attributwert zur Übernahme der Zonen enthält. Einzelheiten finden Sie im Handbuch *Java Enterprise System 5-Installationshandbuch für UNIX*.

- **Common Agent Container (CAC).** Version 1.1 wird nur installiert, wenn Sun Cluster, Sun Cluster Geographic Edition oder Sun Cluster-Agenten installiert sind. Sie wird nicht installiert, wenn die Option Alle gemeinsam genutzten Komponenten ausgewählt wurde. In diesem Fall wird nur Version 2.0 installiert.
- **Sun Explorer Data Collector.** Diese gemeinsam genutzte Komponente wird nur installiert, wenn Sun Cluster, Sun Cluster Geographic Edition oder Sun Cluster-Agenten installiert sind. Sie wird nicht installiert, wenn die Option Alle gemeinsam genutzten Komponenten ausgewählt wurde.

Aktualisieren der gemeinsam genutzten Java ES-Komponenten

Dieses Kapitel enthält Informationen zur Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Java ES 5 (Release 5)

Jede Java ES-Produktkomponente hängt von einer oder mehreren gemeinsam genutzten Bibliotheken ab, die als Java ES *gemeinsam genutzte* -Komponenten bezeichnet werden. Gemeinsam genutzte Komponenten werden entsprechend der zu installierenden Produktkomponenten bei der Installation der Produktkomponente automatisch vom Java ES-Installationsprogramm installiert. Die Komponenten müssen während der Bereitstellung der Java ES-Produktkomponenten nicht ausdrücklich ausgewählt, installiert oder konfiguriert werden.

Die gemeinsam genutzten Komponenten der Produktkomponenten, die mit dem Java ES-Installationsprogramm aktualisiert werden können, werden ebenfalls automatisch aktualisiert.

Bei einer manuellen Aktualisierung von Produktkomponenten, wie in den verschiedenen Kapiteln dieses *Aktualisierungshandbuchs* beschrieben, müssen die gemeinsam genutzten Komponenten jedoch ausdrücklich entsprechend der Verfahren aktualisiert werden, die in diesem Kapitel beschrieben sind.

Das Kapitel enthält die folgenden Abschnitte:

- „Überblick über die Aktualisierung der gemeinsam genutzten Komponenten“ auf Seite 72
- „Aktualisierungsverfahren für gemeinsam genutzte Komponenten“ auf Seite 77
- „Besondere Aktualisierungsverfahren“ auf Seite 77

Überblick über die Aktualisierung der gemeinsam genutzten Komponenten

Die Aktualisierung der gemeinsam genutzten Komponenten auf Java ES 5 (Release 5) sollte als Bestandteil eines umfassenden Aktualisierungsplans, wie in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#), beschrieben, durchgeführt werden. Um eine erfolgreiche Aktualisierung zu gewährleisten, lesen Sie die Informationen in Kapitel 1 sorgfältig durch und bereiten Sie einen Aktualisierungsplan vor, der Ihren Anforderungen entspricht.

In diesem Abschnitt werden die folgenden Themen behandelt:

- [Allgemeine zu berücksichtigende Aspekte](#)
- [Gemeinsam genutzte Komponenten synchronisieren](#)
- [Alle gemeinsam genutzten Komponenten synchronisieren](#)
- [Zu berücksichtigende Aspekte hinsichtlich Solaris 10-Zonen](#)

Allgemeine zu berücksichtigende Aspekte

Beachten Sie bei der Aktualisierung der gemeinsam genutzten Komponenten folgende Aspekte:

- **Betriebssystem.** Führen Sie gegebenenfalls Aktualisierungen des Betriebssystems durch, wie unter [„Aspekte zum Betriebssystem“ auf Seite 47](#) beschrieben. Aktualisieren Sie alle Betriebssysteme, mit Ausnahme von Solaris 10 OS, bevor Sie die gemeinsam genutzten Komponenten aktualisieren.
- **Richtlinien zur Aktualisierungsreihenfolge.** Beachten Sie die Richtlinien zur Aktualisierungsreihenfolge unter [„Richtlinien für die Aktualisierungsreihenfolge“ auf Seite 60](#). Üblicherweise werden gemeinsam genutzte Komponenten zuerst aktualisiert. Sie sollten jedoch die gesamte Abfolge der Aktualisierung auf Java ES Release 5 verstehen, bevor Sie mit der Aktualisierung beginnen.

Gemeinsam genutzte Komponenten synchronisieren

Da das Testen und die Unterstützung der großen Anzahl (ca. 30) an gemeinsam genutzten Java ES-Komponenten sehr aufwendig ist und aufgrund der komplexen Interaktion zwischen gemeinsam genutzten Java ES-Produktkomponenten ist es erforderlich, alle gemeinsam genutzten Komponenten innerhalb einer Betriebssysteminstanz auf dieselbe Java ES-Version zu synchronisieren. Eine Betriebssysteminstanz steht für einen einzelnen Computer, auf dem das Solaris 9- oder Linux-Betriebssystem ausgeführt wird oder im Fall des Solaris 10-Betriebssystems für eine der virtuellen Betriebssystemumgebungen (Zonen), die auf einem einzelnen Computer ausgeführt wird.

Das heißt, alle in einer Betriebssysteminstanz installierten gemeinsam genutzten Java ES-Komponenten müssen dieselbe Version aufweisen. Aufgrund dieser Synchronisierungsanforderung gelten für die Installation und Aktualisierung der gemeinsam genutzten Java ES-Komponenten bestimmte Einschränkungen:

- Unterschiedliche Versionen der gemeinsam genutzten Java ES-Komponenten können nur auf verschiedenen Betriebssysteminstanzen vorhanden sein. Sie können beispielsweise gemeinsam genutzte Java ES Release 4-Komponenten in einer Betriebssysteminstanz und gemeinsam genutzte Java ES Release 5-Komponenten in einer anderen Betriebssysteminstanz installieren. Sie können diese Komponenten jedoch nicht zusammen auf derselben Betriebssysteminstanz installieren.
- Wenn einer der gemeinsam genutzten Komponenten in einer Betriebssysteminstanz aktualisiert wird oder eine neue gemeinsam genutzte Komponente einer höheren Version hinzugefügt wird, müssen alle gemeinsam genutzten Komponenten in dieser Betriebssysteminstanz ebenfalls zum gleichen Zeitpunkt aktualisiert werden. (Da gemeinsam genutzte Komponenten rückwärts kompatibel sein müssen, können Release 4-Produktkomponenten zusammen mit gemeinsam genutzten Release 5-Komponenten eingesetzt werden.)

Beispielsweise kann eine Release 5-Produktkomponente in einer Betriebssysteminstanz installiert sein, in der eine oder mehrere Release 4-Produktkomponenten vorhanden sind. Da für die Release 5-Produktkomponente eine Reihe von gemeinsam genutzten Release 5-Komponenten erforderlich ist, müssen aufgrund der Synchronisierungsanforderung alle gemeinsam genutzten Release 4-Komponenten in dieser Betriebssysteminstanz dann auf Release 5

aktualisiert werden, wenn die Release 5-Produktkomponente installiert wird. (Diese trifft auch zu, wenn für die zu installierende Release 5-Produktkomponente andere gemeinsam genutzte Komponenten als für die bereits installierte Produktkomponente erforderlich sind.)

Ebenso müssen bei einer Aktualisierung einer Release 4-Produktkomponente auf Release 5, bei der gemeinsam genutzte Komponenten aktualisiert werden müssen, von denen die Produktkomponente abhängt, alle in dieser Betriebssysteminstanz installierten gemeinsam genutzten Komponenten auf Release 5 aktualisiert werden. Dies gilt unabhängig davon, ob für die jeweilige zu installierende Release 4-Produktkomponente eine Abhängigkeit zu allen gemeinsam genutzten Komponenten besteht oder nicht.

Alle gemeinsam genutzten Komponenten synchronisieren

Das Java ES-Installationsprogramm verfügt über eine Funktion für die Synchronisierung aller gemeinsam genutzten Komponenten. Diese Funktion kann verwendet werden, wenn alle gemeinsam genutzten Komponenten auf die jeweilige Release 5-Version synchronisiert werden müssen.

Wenn auf der Seite für die Komponentenauswahl des Java ES-Installationsprogramms die Option „Alle gemeinsam genutzten Komponenten“ ausgewählt wird, aktualisiert das Installationsprogramm alle vorhandenen gemeinsam genutzten Komponenten und installiert alle fehlenden gemeinsam genutzten Komponenten, ungeachtet dessen, ob sie von einer speziellen Produktkomponente benötigt werden oder nicht.

Die Funktion zum Synchronisieren aller gemeinsam genutzten Komponenten unterstützt die Aktualisierung von Produktkomponenten, die *nicht* explizit vom Java ES-Installationsprogramm aktualisiert werden (d. h. alle Java ES-Produktkomponenten, mit Ausnahme von Anwendungsserver, Message Queue, HADB und Java DB). Die Funktion zum Synchronisieren aller gemeinsam genutzten Komponenten wird beispielsweise für die Aktualisierung von Web Proxy Server und Portal Server auf Release 5 verwendet.

In diesem Fall muss die Synchronisierung *aller* gemeinsam genutzten Komponenten durchgeführt werden, da dem Installationsprogramm zu diesem Zeitpunkt nicht bekannt ist, welche gemeinsam genutzten Komponenten auf einem Computer synchronisiert werden müssen. Aus diesem Grund installiert bzw. aktualisiert diese Funktion *alle* gemeinsam genutzten Komponenten auf die Release 5-Version.

Die Funktion zum Synchronisieren von allen gemeinsam genutzten Komponenten unterstützt eine Reihe von Szenarios hinsichtlich Zonen, wie im folgenden Abschnitt [„Zu berücksichtigende Aspekte hinsichtlich Solaris 10-Zonen,“](#) beschrieben.

Zu berücksichtigende Aspekte hinsichtlich Solaris 10-Zonen

Für die Bereitstellung von Java ES in einer Solaris 10-Umgebung mit mehreren Zonen gelten bestimmte Einschränkungen, die sich aus den zu berücksichtigenden Aspekten bezüglich gemeinsam genutzter Komponenten ergeben.

Zunächst muss beachtet werden, dass eine hohe Anzahl an gemeinsam genutzten Komponenten aufgrund der schreibgeschützten Dateisysteme in Sparse-Root-Zonen nicht in diesen Zonen installiert werden kann. Diese Einschränkung gilt für die gemeinsam genutzten Komponenten, deren Basisverzeichnis /usr lautet (ein von der globalen Zone standardmäßig gemeinsam verwendetes Verzeichnis).

Da man eine hohe Anzahl an gemeinsam genutzten Java ES-Komponenten nicht in Sparse-Root-Zonen installieren kann, müssen für eine erfolgreiche Installation bzw. Aktualisierung der von diesen gemeinsam genutzten Komponenten abhängigen Produktkomponenten in Sparse-Root-Zonen zunächst die gemeinsam genutzten Komponenten in der globalen Zone installiert bzw. aktualisiert werden, von der aus sie in nicht globalen Zonen übernommen werden.

Aufgrund der Synchronisierungsanforderungen bezüglich gemeinsam genutzten Komponenten (siehe [„Gemeinsam genutzte Komponenten synchronisieren“ auf Seite 73](#)) und da die Installation bzw. Aktualisierung gemeinsam genutzter Komponenten in der globalen Zone allen in der Sparse-Root-Zone zu installierenden bzw. zu aktualisierenden Produktkomponenten Rechnung tragen muss, müssen alle gemeinsam genutzten Komponenten in der globalen Zone auf die jeweilige Release 5-Version synchronisiert werden. Das heißt, alle vorhandenen gemeinsam genutzten Komponenten sowie alle fehlenden gemeinsam genutzten Komponenten müssen unabhängig davon, ob diese von einer bestimmten Produktkomponente in einer Sparse-Root-Zone benötigt werden, aktualisiert bzw. installiert werden.

Um alle gemeinsam genutzten Komponenten in der globalen Zone zu synchronisieren, wählen Sie im Java ES-Installationsprogramm auf der Seite für die Komponentenauswahl die Option „Alle gemeinsam genutzten Komponenten“ aus.

Wenn gemeinsam genutzte Komponenten in der globalen Zone installiert und von dort aus übernommen werden (z. B. durch die Installation einer Java ES-Produktkomponente in der globalen Zone), muss besonders darauf geachtet werden, dass die gemeinsam genutzten Komponenten in *allen* Zonen immer synchronisiert sind. Andernfalls können gemeinsame Komponenten einer früheren Version in einer nicht globalen Zone nicht zusammen mit gemeinsam genutzten Release 5-Komponenten eingesetzt werden, die aus der globalen Zone übernommen wurden.

Ansätze zur Aktualisierung gemeinsam genutzter Komponenten

Für die Aktualisierung gemeinsam genutzter Komponenten, die für die Aktualisierung einer bestimmten Java ES-Produktkomponente erforderlich sind, kommen zwei Ansätze in Betracht. Zum einen können Sie die erforderlichen gemeinsam genutzten Komponenten ermitteln und manuell installieren bzw. auf die jeweilige Release 5-Version aktualisieren. Der zweite Ansatz besteht in der Verwendung der Funktion des Java ES-Installationsprogramms für die Synchronisierung aller gemeinsam genutzten Komponenten.

Aufgrund der Synchronisierungsanforderung bezüglich gemeinsam genutzter Komponenten (siehe [„Gemeinsam genutzte Komponenten synchronisieren“ auf Seite 73](#)) ist jedoch nur die Verwendung der Funktion des Java ES-Installationsprogramms für die Synchronisierung aller gemeinsam genutzter Komponenten zweckmäßig.

Der Grund hierfür liegt darin, dass sich das Ermitteln der zu installierenden bzw. zu aktualisierenden gemeinsam genutzten Komponenten in den meisten Fällen als problematisch erweist und die manuelle Aktualisierung schwierig ist. Manche der gemeinsam genutzten Komponenten können mithilfe von Patches auf Release 5 aktualisiert werden, in einigen Fällen müssen jedoch die vorherigen Pakete durch die Release 5-Pakete ersetzt werden. Je nach Aktualisierungsweg müssen manche Pakete der vorherigen Version unter Umständen manuell entfernt werden.

In früheren Versionen erschwerte die Problematik der manuellen Aktualisierung gemeinsam genutzter Komponenten die Aktualisierung von Produktkomponenten erheblich. Die Funktion zum Synchronisieren aller gemeinsam genutzten Komponenten stellt daher eine beachtliche Verbesserung im Vergleich mit der manuellen Aktualisierung gemeinsam genutzter Komponenten dar, die in Java ES Release 3 und Release 4 erforderlich war.

Aktualisierungsverfahren für gemeinsam genutzte Komponenten

In dem Verfahren zum Aktualisieren gemeinsam genutzter Komponenten wird die Funktion des Java ES-Installationsprogramms für die Synchronisierung aller gemeinsam genutzten Komponenten verwendet (Option „Alle gemeinsam genutzten Komponenten“).

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Beenden Sie die unter „[Besondere Aktualisierungsverfahren](#)“ auf Seite 77 angegebenen Dienste und Prozesse.

3. Starten Sie das Java ES-Installationsprogramm.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

wobei *os_arch* der Plattform entspricht, wie z. B. *Solaris_sparc*. (Verwenden Sie die Option `installer -nodisplay` für die Befehlszeilenschnittstelle.)

Nach der Willkommenseite sowie der Lizenzvereinbarung wird eine Seite für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten erkannt werden, die direkt vom Java ES-Installationsprogramm aktualisiert werden können, wird der Status als „aktualisierbar“ angezeigt.)

4. Wählen Sie auf der Seite für die Komponentenauswahl „Alle gemeinsam genutzten Komponenten“ aus.

5. Bestätigen Sie Ihre Auswahl.

Alle gemeinsam genutzten Komponenten werden auf die jeweilige Release 5-Version synchronisiert.

6. Beenden Sie das Java ES-Installationsprogramm.

Anschließend durchzuführende Verfahren finden Sie unter „[Besondere Aktualisierungsverfahren](#)“ auf Seite 77.

Besondere Aktualisierungsverfahren

In diesem Abschnitt werden besondere Verfahren beschrieben, die für die Aktualisierung folgender gemeinsam genutzter Komponenten durchgeführt werden müssen:

- „Aktualisierungsverfahren für Java SE“ auf Seite 78
- „Aktualisierungsverfahren für Common Agent Container“ auf Seite 80

Aktualisierungsverfahren für Java SE

Java ES Release 5 ist für Java Platform, Standard Edition (Java SE) Version 5.0 Update 9 zertifiziert, das im Folgenden Java SE 5.0 Update 9 genannt wird. (Java SE 5.0 wird manchmal als Entwicklerversion 1.5.0 bezeichnet.)

Bei der Aktualisierung von Java SE auf Version 5.0 Update 9 verhält sich das Java ES-Installationsprogramm wie folgt:

- Bei der Aktualisierung wird ein bereits installiertes Major-Release von Java SE *nicht* entfernt (z. B. Java SE Version 1.4.2 oder Java SE Version 1.6.x), da andere Anwendungen möglicherweise von dieser Version abhängen. Bei der Aktualisierung wird jedoch eine symbolische Verknüpfung auf die Release 5-Version gesetzt, wie in folgender Tabelle gezeigt.

Tabelle 2-1 Symbolische Verknüpfung auf Java SE nach Plattform

Plattform	Symbolische Verknüpfung	Standort
Solaris OS	/usr/jdk/entsys-j2se	/usr/jdk/instances/jdk1.5.0
Linux	/usr/jdk/entsys-j2se	/usr/java/jdk1.5.0_09

- Bei der Aktualisierung wird ein bereits installiertes Major-Release von Java SE *entfernt* (z. B. Java SE Version 5.0 Update 5) und durch Java SE 5.0 Update 9 ersetzt.

Sie sollten alle Zeiger auf Major-Releases von Java SE (z. B. Java SE 1.4.2) für die Dienste beibehalten, die die vorherige Version benötigen. Informationen darüber, wie Sie symbolische Verknüpfungen zu früheren Versionen von Java SE beibehalten, finden Sie in der entsprechenden Dokumentation zur jeweiligen Produktkomponente.

Wenn Sie eine Aktualisierung von Java SE durchführen, beenden Sie zuerst alle Dienste, von denen die derzeit installierte Java SE-Version abhängt. Dadurch werden mögliche Probleme im Zusammenhang mit diesen Diensten vermieden. Wenn Sie die von Java SE abhängigen Dienste nicht beenden, müssen Sie das System nach der Aktualisierung von Java SE auf Release 5 neu starten.

HINWEIS Das Java ES-Installationsprogramm installiert Java SE 5.0 Update 9 bzw. aktualisiert Java SE unabhängig davon, ob andere gemeinsam genutzte Komponenten installiert oder aktualisiert werden. Um Java SE 5.0 Update 9 zu installieren, müssen Sie die Option „Alle gemeinsam genutzten Komponenten“ nicht ausdrücklich auswählen.

Überprüfen der symbolischen Java SE-Verknüpfung

Java Enterprise System behält eine symbolische Verknüpfung auf die unterstützte Version der Java SE-Plattform bei, um sicherzustellen, dass Java ES-Dienste die zu verwendende Java SE-Laufzeit finden.

Überprüfen Sie die symbolische Verknüpfung (z. B. unter Solaris) wie folgt:

```
ls -l /usr/jdk/entsys-j2se
lrwxrwxrwx 1 root  other  7 Jul 7 23:18 /usr/jdk/entsys-j2se ->
    /usr/jdk/instances/jdk1.5.0
```

wobei /usr/jdk/instances/jdk1.5.0 der Standard-Speicherort ist.

Überprüfen der aktuellen Java SE-Version

Um zu ermitteln, welche Java SE-Version von Ihrer Java ES-Installation verwendet wird, führen Sie folgenden Befehl aus. Mit diesem Befehl wird die von der symbolischen Java SE-Verknüpfung referenzierte Java SE-Version überprüft:

```
/usr/jdk/entsys-j2se/bin/java -version
```

Die Ausgaben werden in der folgenden Tabelle aufgelistet:

Tabelle 2-2 Ausgaben der Versionsüberprüfung von Java SE

Java ES Release	Java SE-Versionsnummer	Java SE-Versionszeichenfolge
Release 2	1.4.2 Update 5	1.4.2_05
Release 3	5.0 Update 1	1.5.0_01
Release 4	5.0 Update 4	1.5.0_04
Release 5	5.0 Update 9	1.5.0_09

Aktualisierungsverfahren für Common Agent Container

Wenn Sie die gemeinsam genutzte Common Agent Container-Komponente in Vorbereitung auf eine Aktualisierung der Sun Cluster-Software aktualisieren (d. h. Patches auf Version 1.1 anwenden), führen Sie das Verfahren für die Aktualisierung der abhängigen Software unter „Upgrading Sun Cluster Software“ im *Sun Cluster Software Installation Guide for Solaris OS* (<http://docs.sun.com/doc/819-0420/6n2rlnncr?a=view>) durch.

Aktualisierungen des oben genannten Handbuchs finden Sie unter „Upgrading to Sun Cluster 3.1 8/05 Software“ im *Sun Cluster 3.1 8/05 With Java Enterprise System 5 Special Instructions* (<http://docs.sun.com/doc/819-4351>).

Wenn Sie die gemeinsam genutzte Common Agent Container-Komponente in Vorbereitung auf die Aktualisierung anderer Java ES-Komponenten aktualisieren (d. h. auf Version 2.0 aktualisieren), führen Sie folgendes Verfahren durch und beachten Sie dabei folgende Variablen für Pfadnamen:

Tabelle 2-3 Verzeichnispfade für Common Agent Container

Variable des Pfadnamens	Solaris OS	Linux OS
<i>rel4CACbase-dir</i>	/opt/SUNWcacao	/opt/sun/cacao
<i>rel5CAC-admin-dir</i>	/usr/lib/cacao	/opt/sun/cacao

1. Wenn für die aktuelle Installation benutzerdefinierte Konfigurationseinstellungen verwendet werden, ermitteln Sie die Konfigurationseinstellungen mit folgenden Befehlen:

```
rel4CAC-base-dir/bin/cacoadm list-params
```

Die Ausgabe sieht etwa so aus:

```
java-flags=-Xms4M -Xmx64M
jmxmp-connector-port=10162
snmp-adaptor-port=10161
snmp-adaptor-trap-port=10162
commandstream-adaptor-port=10163
retries=4
```

Das obige Beispiel zeigt die Standardwerte. Notieren Sie alle Einstellungen, die keine Standardeinstellungen sind. Diese Einstellungen werden in [Schritt 4 auf Seite 81](#) wieder verwendet.

2. Halten Sie die Common Agent Container-Prozesse mit folgenden Befehlen an:

```
rel4CAC-base-dir/bin/cacoadm stop
echo $?
```

Wenn der Exit-Code nicht 0 ist, erzwingen Sie das Beenden:

```
rel4CAC-base-dir/bin/cacoadm stop -f
```

3. Aktualisieren Sie Common Agent Container unter Verwendung der Funktion des Java ES-Installationsprogramms zum Synchronisieren aller gemeinsam genutzten Komponenten (Option „Alle gemeinsam genutzten Komponenten“).

Siehe auch „[Aktualisierungsverfahren für gemeinsam genutzte Komponenten](#)“ auf Seite 77.

4. Wenden Sie alle in [Schritt 1 auf Seite 80](#) ermittelten benutzerdefinierten Konfigurationseinstellungen an.

```
rel5CAC-admin-dir/bin/cacoadm set-param java-flags=Wert
rel5CAC-admin-dir/bin/cacoadm set-param jmxmp-connector-port=Wert
rel5CAC-admin-dir/bin/cacoadm set-param snmp-adaptor-port=Wert
rel5CAC-admin-dir/bin/cacoadm set-param
    snmp-adaptor-trap-port=Wert
rel5CAC-admin-dir/bin/cacoadm set-param
    commandstream-adaptor-port=Wert
rel5CAC-admin-dir/bin/cacoadm set-param retries=Wert
```

5. Wenn Sie Java SE auf Java SE Version 5 aktualisieren, führen Sie das Dienstprogramm „rebuild-dependencies“ aus:

```
rel5CAC-admin-dir/bin/cacoadm rebuild-dependencies
```

Die Ausgabe dieses Befehls lautet wie folgt:

```
Property updated: [java-home].
Property updated: [jdk-home].
Property updated: [nss-lib-home].
Property updated: [nss-tools-home].
```

6. Starten Sie die Common Agent Container-Dienste neu:

```
rel5CAC-admin-dir/bin/cacoadm stop
rel5CAC-admin-dir/bin/cacoadm start
```

7. Überprüfen Sie die Aktualisierung von Common Agent Container:

```
rel5CAC-admin-dir/bin/cacoadm status
rel5CAC-admin-dir/bin/cacoadm verify-configuration
```


Sun Cluster-Software

In diesem Kapitel wird die Aktualisierung der Sun Cluster-Software auf Java ES 5 (Release 5) beschrieben: Sun Cluster 3.1 8/05-Software.

Das Kapitel enthält einen Überblick über die Aktualisierungsaspekte der Sun Cluster-Software auf Release 5.

Die Sun Cluster-Software wird nur auf Solaris-Plattformen unterstützt.

Die in diesem Kapitel beschriebene Aktualisierung der Sun Cluster-Software beschreibt sowohl die Aktualisierung der Sun Cluster-Framework-Software als auch der Sun Cluster-Datendienst-Software oder -Agenten.

- „Überblick über Aktualisierungen der Sun Cluster-Software“ auf Seite 84
- „Aktualisieren der Sun Cluster-Software auf Java ES Release 5“ auf Seite 88

Überblick über Aktualisierungen der Sun Cluster-Software

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung der Sun Cluster-Software auf Java ES 5 (Release 5) beschrieben:

- [Über Sun Cluster-Software Release 5](#)
- [Wegweiser für die Aktualisierung von Sun Cluster](#)
- [Sun Cluster-Daten](#)
- [Vorgehensweise zur Aktualisierung von Sun Cluster](#)

Über Sun Cluster-Software Release 5

Release 5 der Sun Cluster-Software stellt eine kleinere Aktualisierung im Gegensatz zu Release 4 der Sun Cluster-Software dar (siehe *Sun Cluster Release Notes*, <http://docs.sun.com/doc/819-1405/6n3p13hac?a=view>). Release 5 der Sun Cluster-Software ist im Grunde mit Release 4 identisch, bis auf den Unterschied, dass Release 5 das Solaris 8-Betriebssystem nicht unterstützt.

Änderungen am Dokumentationssatz von Sun Cluster 3.1 8/05 finden Sie unter *Sun Cluster 3.1 8/05 With Java Enterprise System 5 Special Instructions*, <http://docs.sun.com/doc/819-4351>. Ansonsten gelten die Verfahren im Dokumentationssatz von Sun Cluster 3.1 8/05 für Release 5 der Sun Cluster-Software.

- HINWEIS

Wenn Sie die Sun Cluster 3.1 8/05-Software unter Solaris 8 benötigen, müssen Sie die Sun Cluster 3.1 8/05-Software aus der Java ES Release 4-Verteilung beziehen, die Sie unter folgender Adresse finden:

<http://www.sun.com/software/javaenterprisesystem/previous/index.xml>.

Die Installation der Sun Cluster 3.1 8/05-Software unter Solaris 8 wird vom Java ES 5-Installationsprogramm nicht mehr unterstützt.

Führen Sie die folgenden Schritte aus, um die Sun Cluster 3.1 8/05-Software unter Solaris 8 zu installieren:

 1. Installieren Sie die Sun Cluster 3.1 8/05-Software aus der Java ES Release 4-Verteilung.
 2. Installieren Sie alle erforderlichen Patches für die Sun Cluster 3.1 8/05-Software.

Wegweiser für die Aktualisierung von Sun Cluster

In [Tabelle 3-1](#) werden die unterstützten Sun Cluster-Aktualisierungswege auf Java ES 5 (Release 5) dargestellt. Die Tabelle enthält nur Informationen für das Solaris-Betriebssystem.

Die Sun Cluster-Versionen stimmen nicht eins zu eins mit den Java ES Releases überein. In der Vergangenheit wurden vorläufige Releases (Interim Feature Releases, IFRs) der Sun Cluster-Software zwischen vollständigen Java ES Releases in Java ES integriert. Aus diesem Grund beinhaltet die Aktualisierung von Java ES von Sun Cluster Release 2, Release 3 und Release 4 auf Sun Cluster Release 5 (siehe [Tabelle 3-1](#)) die Aktualisierung der Sun Cluster 3.1 4/04-, Sun Cluster 3.1 9/04- und Sun Cluster 3.1 8/05-Software auf Release 5.

Tabelle 3-1 Wege für die Aktualisierung auf Java ES 5 (Release 5): Sun Cluster 3.1 8/05-Software

Java ES Release	Sun Cluster Softwareversion	Allgemeiner Ansatz	Neukonfiguration erforderlich
Release 4	Sun Cluster 3.1 8/05 (2005Q4)	Direkte Aktualisierung ¹ : Durch Anwendung des Sun Cluster-Dienstprogramms scinstall.	Keine.

Tabelle 3-1 Wege für die Aktualisierung auf Java ES 5 (Release 5): Sun Cluster 3.1 8/05-Software

Java ES Release	Sun Cluster Softwareversion	Allgemeiner Ansatz	Neukonfiguration erforderlich
Release 3	Sun Cluster 3.1 9/04 oder Sun Cluster 3.1 8/05 (IFR)	Direkte Aktualisierung: Durch Anwendung des Sun Cluster-Dienstprogramms scinstall.	Cluster-Konfiguration wird automatisch in die aktualisierte Version migriert. Bei der Aktualisierung des IFR auf Release 5 ist keine Neukonfiguration erforderlich.
Release 2	Sun Cluster 3.1 4/04 oder Sun Cluster 3.1 9/04 (IFR)	Direkte Aktualisierung: Durch Anwendung des Sun Cluster-Dienstprogramms scinstall.	Cluster-Konfiguration wird automatisch in die aktualisierte Version migriert
Release 1	Sun Cluster 3.1	Direkte Aktualisierung nicht zertifiziert. Kann jedoch mit dem Dienstprogramm scinstall durchgeführt werden.	Cluster-Konfiguration wird automatisch in die aktualisierte Version migriert
Versionen vor Java ES	Sun Cluster 3.0	Direkte Aktualisierung nicht zertifiziert. Kann jedoch mit dem Dienstprogramm scinstall durchgeführt werden.	Cluster-Konfiguration wird automatisch in die aktualisierte Version migriert

1. Eine Aktualisierung von Release 4 auf Release 5 ist nur erforderlich, wenn die von der Sun Cluster-Software gemeinsam genutzten Komponenten auf Release 5 aktualisiert wurden.

Sun Cluster-Daten

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Sun Cluster-Software betroffen sein können.

Tabelle 3-2 Verwendung von Sun Cluster-Daten

Datentyp	Standort	Verwendung
Cluster-Konfigurationsdateien	Cluster-Konfigurations-Repository, das auf allen Cluster-Knoten repliziert und synchronisiert wird (VORSICHT: Bearbeiten Sie CCR-Dateien in keinem Fall manuell; dies kann einen Funktionsausfall eines Knotens oder des gesamten Clusters verursachen)	Speichert Konfigurationsinformationen für sämtliche Sun Cluster-Vorgänge: Cluster-Knotenkonfiguration, Failover-Mechanismen, Ressourcenverwaltung usw.

Vorgehensweise zur Aktualisierung von Sun Cluster

Die Vorgehensweise zur Aktualisierung von Sun Cluster hängt im Grunde von den verschiedenen Aspekten ab, die in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) besprochen wurden: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

Dieser Abschnitt konzentriert diese grundsätzliche Erläuterung auf Sun Cluster, indem Probleme dargestellt werden, die möglicherweise Ihren Aktualisierungsplan für Sun Cluster beeinflussen.

Kompatibilität

Die Java ES Release 5-Version der Sun Cluster-Software enthält eine neue grafische Verwaltungsschnittstelle, ist jedoch rückwärts kompatibel zu Vorgängerversionen der Sun Cluster-Agenten.

Sun Cluster-Abhängigkeiten

Sun Cluster-Abhängigkeiten zu anderen Java ES-Komponenten beeinflussen möglicherweise das Verfahren für die Aktualisierung und Neukonfiguration der Sun Cluster-Software. Änderungen der Sun Cluster-Schnittstellen oder -Funktionen könnten beispielsweise aktualisierte Versionen der Komponenten erforderlich machen, von denen die Sun Cluster-Software abhängig ist. Welche dieser Komponenten aktualisiert werden müssen, hängt von dem jeweiligen Aktualisierungsweg ab.

Für Sun Cluster bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Die Sun Cluster-Software ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)).
- **Datendienste.** Die Sun Cluster-Software erfordert bestimmte Datendienste (oder Agenten), um Java ES-Produktkomponenten hochverfügbar zu machen. Für jede Produktkomponente, die in einer Sun Cluster-Umgebung ausgeführt wird, muss ein entsprechender Datendienst für die Verwaltung der jeweiligen Cluster-Ressourcen vorhanden sein. Die Aktualisierung der Agentenpakete ist üblicherweise Bestandteil des Sun Cluster-Aktualisierungsvorgangs.

Aktualisieren der Sun Cluster-Software auf Java ES Release 5

Dieser Abschnitt enthält Informationen zur Aktualisierung der Sun Cluster-Software von Java ES 2005Q4 (Release 4), Java ES 2005Q1 (Release 3) und Java ES 2004Q2 (Release 2) auf Java ES 5 (Release 5). Die Aktualisierungsvorgänge sind für die drei Sun Cluster-Versionen in diesen Java ES Releases identisch: Sun Cluster 3.1 4/04-, Sun Cluster 3.1 9/04- und Sun Cluster 3.1 8/05-Software.

Wenn Sie die Sun Cluster 3.1 8/05-Software (Release 3 oder Release 4) bereits installiert haben, müssen Sie nur auf Release 5 aktualisieren, wenn die von der Sun Cluster-Software gemeinsam genutzten Komponenten auf Release 5 aktualisiert wurden.

In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung von Sun Cluster](#)

Einführung

Berücksichtigen Sie bei der Aktualisierung der Sun Cluster-Software auf Java ES Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch die Ausführung des Skripts `scinstall`, das die Sun Cluster-Software aktualisiert und nach Abschluss der Software-Lokalisierung die vorherige Sun Cluster-Konfiguration anwendet. Es müssen alle Knoten in einer Cluster-Umgebung auf dieselbe Version aktualisiert werden, entweder durch Beenden des Clusters und die Aktualisierung sämtlicher Knoten oder durch ein Rolling Upgrade, bei dem die Knoten nacheinander aktualisiert werden, ohne den Cluster zu beenden.
- **Aktualisierungsabhängigkeiten.** Während die Sun Cluster-Software von einer Reihe gemeinsam genutzter Java ES-Komponenten abhängt (siehe [Tabelle 1-7 auf Seite 51](#)), handelt es sich dabei nicht um zwingende Abhängigkeiten: Die Sun Cluster-Software von Java ES Release 5 ist mit den Release 4-Versionen dieser Komponenten kompatibel.

- **Rückwärtskompatibilität.** Release 5 der Sun Cluster-Framework-Software ist rückwärts kompatibel mit früheren Cluster Agents. Release 5 der Sun Cluster-Agent-Software ist rückwärts kompatibel mit Java ES Release 4-Komponenten. Alle Knoten in einem Cluster müssen jedoch die gleiche Version der Framework- und Agent-Software ausführen.
- **Aufheben der Aktualisierung.** Das Zurücksetzen der Release 5-Aktualisierung der Sun Cluster-Software auf frühere Versionen wird nicht unterstützt.
- **Plattformspezifische Aspekte.** Der Ansatz zur Aktualisierung der Sun Cluster-Software ist auf allen Solaris-Plattformen und Hardware-Architekturen identisch; die Sun Cluster-Software wird jedoch nicht auf Linux-Plattformen unterstützt.

Aktualisierung von Sun Cluster

Dieser Abschnitt bietet einen Überblick über das Aktualisierungsverfahren der Sun Cluster-Software von Java ES Release 4 auf Java ES Release 5:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren der Sun Cluster-Software](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

Der Abschnitt behandelt die nicht parallel ausgeführte Aktualisierung von Sun Cluster. Der Unterschied dieses Verfahrens zu einem Rolling Upgrade besteht darin, dass der Cluster bei der Aktualisierung nicht beendet wird. Das im Folgenden beschriebene allgemeine Verfahren zur Aktualisierung eines Cluster-Knotens ist jedoch für beide Fälle identisch. Die jeweiligen Verfahren finden Sie im Kapitel zur Aktualisierung im *Sun Cluster Installation Guide*, <http://docs.sun.com/doc/819-0420/6n2rlnncr?a=view>. Änderungen für Sun Cluster Release 5 finden Sie unter *Sun Cluster 3.1 8/05 With Java Enterprise System 5 Special Instructions*, <http://docs.sun.com/doc/819-4351>.

Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung der Sun Cluster-Software beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)

- Cluster-Knoten für die Aktualisierung vorbereiten
- Betriebssystem aktualisieren
- Sun Cluster-Aktualisierungsabhängigkeiten
- Erforderliche Konfigurationsinformationen und Passwörter abrufen

Aktuelle Versionsinformationen überprüfen

Sie können die aktuelle Version der Sun Cluster-Software durch Eingabe des folgenden Befehls überprüfen:

```
scinstall -pv
```

Der Befehl gibt die Sun Cluster-Version und die Version der installierten Softwarepakete zurück. Wenn mit diesem Befehl die 3.1 8/05-Version zurückgegeben wird (3.1u4), überprüfen Sie die Patch-Versionsnummer, um zu ermitteln, ob Sie über Release 4 oder Release 5 der Software verfügen (siehe folgende Tabelle).

Tabelle 3-3 Sun Cluster Ausgaben der Versionsüberprüfung

Java ES Release	Sun Cluster-Versionsnummer	Patch-Versionsnummern
Release 1 (Sun Cluster 3.1)	3.1	
Release 2 (Sun Cluster 3.1 4/04)	3.1u2	
Release 2 oder 3 (Sun Cluster 3.1 9/04)	3.1u3	
Release 3 oder 4 (Sun Cluster 3.1 8/05)	3.1u4	Solaris 9 SPARC: 117949-15 Solaris 8 SPARC: 117950-15 Solaris 9 x86: 117909-15
Release 5 (Sun Cluster 3.1 8/05)	3.1u4	Solaris 10 SPARC: 120500-08 ¹ Solaris 9 SPARC: 117949-23 Solaris 8 SPARC: 117950-23 Solaris 10 x86: 120501-08 Solaris 9 x86: 117909-23

1. Diese Patch-Versionsnummern sind für die Aktualisierung auf Java ES Release 5 für die verschiedenen Plattformen mindestens erforderlich. Wenn neuere Versionen verfügbar sind, verwenden Sie anstelle der in dieser Tabelle genannten Versionen die neueren Versionen.

Cluster-Knoten für die Aktualisierung vorbereiten

Vor der Aktualisierung der Sun Cluster-Software muss der Cluster-Knoten aus der Cluster-Umgebung entfernt werden:

- **Nicht parallel ausgeführte Aktualisierungen.** Für das Entfernen des Knotens aus der Cluster-Umgebung muss die Umgebung beendet werden: Offline schalten und Deaktivieren der Ressourcengruppen, Beenden der in der Umgebung ausgeführten Anwendungen, Sichern der gemeinsam genutzten Daten, Sichern der Systemfestplatte und Neustarten des Knotens im Nicht-Cluster-Modus.
- **Parallel ausgeführte Aktualisierungen.** Das Entfernen des Knotens aus der Cluster-Umgebung erfordert das Verschieben der Ressourcen- und Gerätegruppen aus dem Knoten, das Sichern der gemeinsam genutzten Daten und der Systemfestplatte und das Neustarten des Knotens im Nicht-Cluster-Modus.

Detaillierte Informationen zu diesen und anderen Vorgängen, die in bestimmten Situationen gegebenenfalls ausgeführt werden müssen, finden Sie im Kapitel zur Aktualisierung im *Sun Cluster Installation Guide*,
<http://docs.sun.com/doc/819-0420/6n2rlnncr?a=view>.

Betriebssystem aktualisieren

Möglicherweise möchten Sie die durch die Aktualisierung notwendige Ausfallzeit nutzen, um Ihr Betriebssystem und die Version des verwendeten Volume-Managers zu aktualisieren.

Detaillierte Informationen zu den jeweiligen Verfahren finden Sie im Kapitel zur Aktualisierung im *Sun Cluster Installation Guide*,
<http://docs.sun.com/doc/819-0420/6n2rlnncr?a=view>.

Sun Cluster-Aktualisierungsabhängigkeiten

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Release 5 zu aktualisieren. Die Aktualisierung der gemeinsam genutzten Release 4-Komponenten, von denen die Sun Cluster-Software abhängt, ist optional und kann wie in [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“](#), beschrieben durchgeführt werden. (Die Aktualisierung der gemeinsam genutzten Release 2-Komponenten auf Release 5 ist jedoch zwingend.)

HINWEIS Wenn gemeinsam genutzte Java ES-Komponenten auf Release 5 synchronisiert wurden, muss die Sun Cluster-Software auf Release 5 aktualisiert werden. Dies ist erforderlich, da Sun Cluster Release 4 nicht mit den gemeinsam genutzten Komponenten der Sun Java Web Console Release 5 kompatibel ist.

Wenn die Sun Java Web Console auf Release 5 (Version 3.0) aktualisiert wurde, sollten Sie die neuesten Sun Cluster-Patches ausführen oder Sun Cluster wie in diesem Kapitel beschrieben aktualisieren.

Erforderliche Konfigurationsinformationen und Passwörter abrufen

Es werden keine bestimmten Informationen zur aktuell installierten Version benötigt. Sie müssen jedoch als Superuser angemeldet sein, um die Aktualisierung durchführen zu können.

Aktualisieren der Sun Cluster-Software

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren der Sun Cluster-Software haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

Zu berücksichtigende Aspekte bei der Aktualisierung

Bei der Aktualisierung der Sun Cluster-Software auf Java ES Release 5 müssen folgende Aspekte berücksichtigt werden:

- Wenn Sie die Sun Cluster-Framework-Software aktualisieren, wird empfohlen, die Datendienste zu aktualisieren, die für die Verwaltung der hochverfügbaren Java ES-Komponenten und anderer in Ihrer Cluster-Umgebung ausgeführten Anwendungen erforderlich sind.
- Die Aktualisierung der Sun Cluster-Software bietet auch eine Gelegenheit, die Java ES-Komponenten oder andere in Ihrer Cluster-Umgebung ausgeführte Anwendungen zu aktualisieren.

Aktualisierungsverfahren

Das folgende Verfahren ist für die Aktualisierung der Sun Cluster-Software auf den einzelnen Cluster-Knoten anzuwenden. Die folgenden Schritte sind sehr allgemein gehalten. Detaillierte Informationen zur Ausführung dieser Schritte finden Sie im Kapitel zur Aktualisierung im *Sun Cluster Installation Guide*, <http://docs.sun.com/doc/819-0420/6n2rlnnr?a=view>. Änderungen für Sun Cluster Release 5 finden Sie unter *Sun Cluster 3.1 8/05 With Java Enterprise System 5 Special Instructions*, <http://docs.sun.com/doc/819-4351>.

1. Starten Sie im Nicht-Cluster-Modus.
2. Melden Sie sich als Root oder Superuser an.

```
su -
```

3. Wechseln Sie in folgendes Verzeichnis der Java ES Release 5-Verteilung:

```
cd /os_arch/Product/sun_cluster/os-ver/Tools
```

wobei *os_arch* der Plattform entspricht, wie z. B. *Solaris_sparc*, und *os-ver* ist *Solaris 9* oder *Solaris 10*.

4. Führen Sie das Dienstprogramm `scinstall` aus.

```
./scinstall
```

Es wird ein Hauptmenü für die Durchführung der Cluster-Installation, der Konfiguration und der Aktualisierungsaufgaben angezeigt.

5. Aktualisieren Sie die Sun Cluster-Framework-Software und die gewünschten Datendienste.

Die aktualisierten Datendienste müssen konfiguriert werden, indem die entsprechenden Ressourcen in die aktualisierten Ressourcentypen migriert werden (siehe „[Aufgaben nach der Aktualisierung](#)“ auf Seite 95).

6. Wenden Sie alle erforderlichen Patches auf die Sun Cluster-Framework-Software und -Datendienste an.

Informationen zum Zugriff und zum Anwenden der entsprechenden Patches finden Sie in *Sun Cluster 3.0-3.1 Release Notes Supplement*, <http://docs.sun.com/app/docs/doc/816-3381/6m9lratq9?a=view#gcpom>.

7. Starten Sie den Knoten im Cluster neu.

Überprüfen der Aktualisierung

Um zu überprüfen, ob die Aktualisierung der Sun Cluster-Software erfolgreich war, gehen Sie wie folgt vor:

1. Geben Sie folgenden Befehl ein:

```
scinstall -pv
```

Der Befehl gibt die Sun Cluster-Version und die Version der installierten Softwarepakete zurück. Wenn mit diesem Befehl die 3.1 8/05-Version zurückgegeben wird (3.1u4), überprüfen Sie die Patch-Versionsnummer, um zu ermitteln, ob Sie über Release 4 oder Release 5 der Software verfügen (siehe [Tabelle 3-3 auf Seite 91](#)).

2. Überprüfen Sie die Protokolldatei der Datendienstaktualisierung.

Ein Verweis auf die Protokolldatei finden Sie am Ende der Ausgabemeldungen der Aktualisierung.

Aufgaben nach der Aktualisierung

Nach der Aktualisierung der Sun Cluster-Software müssen Sie eine Reihe zusätzlicher Aufgaben durchführen. Diese sind davon abhängig, ob Sie eine parallel oder eine nicht parallel durchgeführte Aktualisierung vorgenommen haben. Zu den Aufgaben, die für eine vollständige Wiederherstellung Ihrer Cluster-Umgebung erforderlich sind, gehören unter anderem:

- Überprüfung des Status der Cluster-Konfiguration
- Migration der Ressourcen in die neuen Versionen der Ressourcentypen
- Aktualisierung weiterer im Cluster installierter Java ES-Komponenten oder -Anwendungen

Detaillierte Informationen zu den Aufgaben, die nach der Installation durchgeführt werden müssen, finden Sie im Kapitel zur Aktualisierung im *Sun Cluster Installation Guide*, <http://docs.sun.com/doc/819-0420/6n2rlnncr?a=view>.

Aufheben der Aktualisierung

Das Aufheben der Aktualisierung der Sun Cluster-Software wird nicht unterstützt. Die während der Aktualisierung vorgenommenen Änderungen sind nicht einfach rückgängig zu machen.

Sun Cluster Geographic Edition

In diesem Kapitel wird die Aktualisierung von Sun Cluster Geographic Edition auf Java ES 5 (Release 5) beschrieben: Sun Cluster Geographic Edition 3.1 2006Q4.

Das Kapitel enthält einen Überblick über die Aspekte der verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird dabei nur die Aktualisierung unter dem Solaris-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Sun Cluster Geographic Edition“ auf Seite 98
- „Aktualisieren von Sun Cluster Geographic Edition von Version 3.1 8/05“ auf Seite 100

HINWEIS Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf einen Verzeichnispfad, der im Folgenden als *SunClusterGeo-base* angegeben wird. Bei der Installation von Sun Cluster Geographic Edition wurde dieser Pfad mindestens teilweise als Installationsverzeichnis angegeben. Wenn nicht, wurde vom Geographic Edition-Installationsprogramm ein Standardwert zugewiesen.

Die Standardwerte für diesen Verzeichnispfad sind in der folgenden Tabelle aufgelistet.

Tabelle 4-1 Sun Cluster Geographic Edition Verzeichnispfade

Variable des Pfadnamens	Solaris OS	Linux OS
<i>SunClusterGeo-base</i>	/opt/SUNWscgeo	Nicht anwendbar

Überblick über Aktualisierungen von Sun Cluster Geographic Edition

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Sun Cluster Geographic Edition auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5](#)
- [Java ES Wegweiser für die Aktualisierung auf Release 5](#)
- [Sun Cluster Geographic Edition-Daten](#)
- [Vorgehensweise zur Aktualisierung von Sun Cluster Geographic Edition](#)

Über Java ES Release 5

Sun Cluster Geographic Edition von Java ES Release 5 ist das erste Release, das als Java ES-Komponente bereitgestellt wird. Sun Cluster Geographic Edition 3.1 wurde zunächst als Standalone-Produkt veröffentlicht.

Sun Cluster Geographic Edition Release 5 stellt im Gegensatz zu Sun Cluster Geographic Edition 3.1 8/05 ein kleineres Release dar. Es handelt sich um das erste Release, das die Solaris x86-Plattform unterstützt. Sun Cluster Geographic Edition Release 5 beinhaltet auch einige ausgewählte Fehlerkorrekturen, verschiedene Funktionen für Hardware- und Softwarekomponenten sowie Unterstützung für zusätzliche Datenreplizierungsprodukte.

Java ES Wegweiser für die Aktualisierung auf Release 5

[Tabelle 4-2](#) zeigt die unterstützten Wege für die Aktualisierung von Sun Cluster Geographic Edition auf Java ES Release 5. Die Tabelle gilt ausschließlich für das Solaris-Betriebssystem.

Tabelle 4-2 Wege für die Aktualisierung auf Java ES 5 (Release 5): Sun Cluster Geographic Edition 3.1 2006Q4

Java ES Release	Sun Cluster Geographic Edition Version	Allgemeiner Ansatz	Neukonfiguration erforderlich
Versionen vor Java ES	Sun Cluster Geographic Edition 3.1 8/05	Direkte Aktualisierung: Ersetzen Sie Sun Cluster Geographic Edition 3.1 8/05 durch eine neue Installation.	Keine

Sun Cluster Geographic Edition-Daten

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Sun Cluster Geographic Edition-Software betroffen sein können.

Tabelle 4-3 Sun Cluster Geographic Edition-Verwendung der Daten

Datentyp	Standort	Verwendung
Sun Cluster Geographic Edition-Konfigurationsdaten	Cluster-Konfigurations-Repository, das auf allen Cluster-Knoten repliziert und synchronisiert wird (VORSICHT: Bearbeiten Sie CCR-Dateien in keinem Fall manuell; dies kann einen Funktionsausfall eines Knotens oder des gesamten Clusters verursachen)	Speichert Konfigurationsinformationen für sämtliche Sun Cluster Geographic Edition-Vorgänge.

Vorgehensweise zur Aktualisierung von Sun Cluster Geographic Edition

Ihre Vorgehensweise bei der Aktualisierung von Sun Cluster Geographic Edition hängt grundsätzlich von den zahlreichen in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) erläuterten Aspekten ab: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

Dieser Abschnitt konzentriert diese grundsätzliche Erläuterung auf Sun Cluster Geographic Edition, indem Probleme dargestellt werden, die möglicherweise Ihren Aktualisierungsplan für Sun Cluster Geographic Edition beeinflussen.

Kompatibilität

Auf beiden Clustern in einer Partnerschaft muss die gleiche Version von Sun Cluster Geographic Edition ausgeführt werden. Somit kann Sun Cluster Geographic Edition Release 5 in einer Partnerschaft nicht mit Sun Cluster Geographic Edition 3.1 8/05 zusammen verwendet werden (es besteht keine Rückwärtskompatibilität). Sun Cluster Geographic Edition Release 5 beinhaltet zusätzliche Konfigurationsdaten, die von Sun Cluster Geographic Edition 3.1 8/05 nicht gelesen werden können.

Abhängigkeiten

Sun Cluster Geographic Edition-Abhängigkeiten zu anderen Java ES-Komponenten beeinflussen möglicherweise das Verfahren für die Aktualisierung und Neukonfiguration der Sun Cluster Geographic Edition-Software. Änderungen der Sun Cluster Geographic Edition-Schnittstellen oder -Funktionen könnten beispielsweise eine aktualisierte Version der Komponenten erforderlich machen, von denen Sun Cluster Geographic Edition abhängig ist. Welche dieser Komponenten aktualisiert werden müssen, hängt von dem jeweiligen Aktualisierungsweg ab.

Für Sun Cluster Geographic Edition bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Sun Cluster Geographic Edition ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)).
- **Sun Cluster.** Für Sun Cluster Geographic Edition besteht eine zwingende Abhängigkeit zu Sun Cluster, das Grundfunktionen zur Verfügung stellt.

Aktualisieren von Sun Cluster Geographic Edition von Version 3.1 8/05

Dieser Abschnitt enthält Informationen zur Aktualisierung von Sun Cluster Geographic Edition von Version 3.1 8/05 auf Java ES 5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Sun Cluster Geographic Edition Version 3.1 8/05](#)

Einführung

Berücksichtigen Sie bei der Aktualisierung von Sun Cluster Geographic Edition 3.1 8/05 auf Release 5 die folgenden Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch die Deinstallation von Version 3.1 8/05 sowie erneute Installation von Sun Cluster Geographic Edition Release 5. Konfigurationsdaten werden beibehalten.
- **Aktualisierungsabhängigkeiten.** Sun Cluster Geographic Edition ist von einer Reihe gemeinsam genutzter Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)), die alle automatisch vom Java ES -Installationsprogramm auf Release 5 aktualisiert werden, wenn Sie eine Aktualisierung von Sun Cluster Geographic Edition durchführen. Insbesondere für Sun Cluster Geographic Edition besteht eine zwingende Aktualisierungsabhängigkeit zu Common Agent Container, Version 1.1. Für Sun Cluster Geographic Edition besteht ebenfalls eine zwingende Aktualisierungsabhängigkeit zu Sun Cluster: Sun Cluster Release 4 (3.1 8/05) muss auf Release 5 aktualisiert werden, um Sun Cluster Geographic Edition Release 5 zu unterstützen.
- **Rückwärtskompatibilität.** Sun Cluster Geographic Edition Release 5 ist nicht mit Sun Cluster Geographic Edition 3.1 8/05 kompatibel. Alle Cluster in einer Partnerschaft müssen auf Release 5 aktualisiert werden.
- **Aufheben der Aktualisierung.** Das Zurücksetzen der Release 5-Aktualisierung der Sun Cluster Geographic Edition-Software auf Version 3.1 8/05 wird nicht unterstützt.
- **Plattformspezifische Aspekte.** Der Ansatz zur Aktualisierung der Sun Cluster Geographic Edition-Software ist auf allen Solaris-Plattformen und Hardware-Architekturen identisch; die Sun Cluster Geographic Edition-Software wird jedoch nicht auf Linux-Plattformen unterstützt.

Aktualisierung der Sun Cluster Geographic Edition Version 3.1 8/05

In diesem Abschnitt wird die Aktualisierung von Sun Cluster Geographic Edition von Version 3.1 8/05 auf Java ES Release 5 beschrieben. Die folgenden Themen werden in diesem Abschnitt behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisierung von Version 3.1 8/05 von Sun Cluster Geographic Edition](#)

- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung der Sun Cluster Geographic Edition-Software beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Cluster für die Aktualisierung vorbereiten](#)
- [Sun Cluster Geographic Edition-Aktualisierungsabhängigkeiten](#)
- [Sun Cluster Geographic Edition-Daten sichern](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

Aktuelle Versionsinformationen überprüfen

Sie können die aktuelle Version von Sun Cluster Geographic Edition mithilfe des folgenden Befehls überprüfen:

```
/usr/cluster/bin/geoadm --version
```

Die Versionszeichenfolge wird nach dem Copyright angezeigt und ist in der folgenden Tabelle aufgeführt:

Tabelle 4-4 Sun Cluster Geographic Edition-Ausgaben der Versionsüberprüfung

Java ES Release	Sun Cluster Geographic Edition-Versionsnummer
Version 3.1 8/05	1.0
Release 5	1.1

Cluster für die Aktualisierung vorbereiten

Führen Sie die folgenden Schritte für alle Cluster aus, bei denen mit dem Cluster, das Sie aktualisieren, eine Partnerschaft besteht. Bei dem Vorgang wird die Sun Cluster Geographic Edition-Schicht aus der Produktion entfernt.

1. Stellen Sie sicher, dass das Cluster ordnungsgemäß ausgeführt wird.

Um den aktuellen Status des Clusters anzuzeigen, führen Sie auf einem beliebigen Knoten den folgenden Befehl aus.

```
scstat
```

2. Melden Sie sich als Root oder Superuser an.

```
su -
```

3. Entfernen Sie alle Anwendungsressourcengruppen aus den Schutzgruppen.

Bei hochverfügbaren Anwendungen kommt es während der Sun Cluster Geographic Edition-Aktualisierung zu keinen Ausfallzeiten.

```
geopg remove-resource-group resourcegroup protectiongroupname
```

4. Führen Sie Schritt [Schritt 1](#) bis [Schritt 3](#) auf allen Clustern aus, bei denen eine Partnerschaft mit diesem Cluster besteht.

5. Halten Sie alle Schutzgruppen an, die auf dem Cluster aktiv sind.

```
geopg stop protectiongroupname -e local | global
```

6. Entfernen Sie das ICRM-Plug-In aus allen Heartbeats auf beiden Partner-Clustern.

```
geohp remove-plugin icrmplugin heartbeatname
```

Sun Cluster Geographic Edition-Aktualisierungsabhängigkeiten

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Für Sun Cluster Geographic Edition bestehen jedoch zwingende Aktualisierungsabhängigkeiten zu bestimmten gemeinsam genutzten Komponenten und Sun Cluster.

Wenn Sie die Sun Cluster Geographic Edition-Abhängigkeiten aktualisieren, sollten Sie dies in der unten angegebenen Reihenfolge vornehmen, bevor Sie Sun Cluster Geographic Edition aktualisieren. Überspringen Sie dabei die bereits aktualisierten Abhängigkeiten. Die Aktualisierung gemeinsam genutzter Komponenten erfolgt in der Regel automatisch durch das Java ES-Installationsprogramm.

1. **Gemeinsam genutzte Komponenten.** Anleitungen für die Synchronisierung von gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie unter [„Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#). Alle gemeinsam genutzten Komponenten, die von Sun Cluster Geographic Edition benötigt werden, werden jedoch automatisch vom Java ES-Installationsprogramm aktualisiert, wenn Sie eine Aktualisierung von Sun Cluster Geographic Edition auf Release 5 durchführen.

HINWEIS Wenn gemeinsam genutzte Java ES-Komponenten auf Release 5 aktualisiert werden, muss die Sun Cluster Geographic Edition-Software auch auf Release 5 aktualisiert werden, da Sun Cluster Geographic Edition 3.1 8/05 nicht mit der Sun Java Web Console Release 5 kompatibel ist.

2. **Sun Cluster.** Anleitungen für die Aktualisierung von Sun Cluster auf Release 4 finden Sie in [Kapitel 3, „Sun Cluster-Software“ auf Seite 83](#).

Sun Cluster Geographic Edition-Daten sichern

Sun Cluster Geographic Edition speichert alle Daten im Cluster-Konfigurations-Repository, wodurch die Sicherung der aktuellen Daten nicht erforderlich ist.

Erforderliche Konfigurationsinformationen und Passwörter abrufen

Es werden keine bestimmten Informationen zur aktuell installierten Version benötigt. Sie müssen jedoch als Superuser angemeldet sein, um die Aktualisierung durchführen zu können.

Aktualisierung von Version 3.1 8/05 von Sun Cluster Geographic Edition

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Sun Cluster Geographic Edition haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

Zu berücksichtigende Aspekte bei der Aktualisierung

Die Aktualisierung der Sun Cluster Geographic Edition-Software auf Java ES Release 5 ist in der Regel möglich, ohne dabei die derzeit ausgeführten Anwendungen zu unterbrechen. Sie können die Sun Cluster Geographic Edition-Software ohne Unterbrechungen auf ein derzeit ausgeführtes Cluster

aktualisieren. Das Cluster bleibt weiterhin in Produktion, wobei alle Dienste ausgeführt werden. So können Sie ebenfalls Sun Cluster Geographic Edition-Patches ohne Ausfallzeiten anwenden. Konfigurationsdaten werden während des Aktualisierungsvorgangs beibehalten.

Die Sun Cluster Geographic Edition-Software muss auf allen Knoten der Cluster aktualisiert werden, bei denen eine Partnerschaft mit dem aktualisierten Cluster besteht.

Wenn Sie das Solaris-Betriebssystem während des Aktualisierungsvorgangs der Sun Cluster Geographic Edition-Software aktualisieren möchten, müssen Sie die Sun Cluster Geographic Edition-Pakete entfernen, bevor Sie das Solaris-Betriebssystem aktualisieren.

Aktualisierungsverfahren

Das im Folgenden beschriebene Verfahren ist für Sun Cluster Geographic Edition-Instanzen anzuwenden, die lokal auf dem Computer ausgeführt werden, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Beenden Sie Sun Cluster Geographic Edition 3.1 8/05.

```
/usr/cluster/bin/geoadm stop
```

Weitere Informationen dazu, wie zugrundeliegende Anwendungen weiterhin ausgeführt werden, während Sun Cluster Geographic Edition beendet wird, finden Sie im Sun Cluster Geographic Edition *Administration Guide*, <http://docs.sun.com/doc/817-7501>.

3. Deinstallieren Sie Sun Cluster Geographic Edition 3.1 8/05.

```
SunClusterGeo-base/install/uninstall/uninstaller
```

Weitere Informationen zur Verwendung des Sun Cluster Geographic Edition-Installationsprogramms im Deinstallationsmodus finden Sie im Sun Cluster Geographic Edition *Installation Guide*, <http://docs.sun.com/doc/817-7500>.

4. Starten Sie Sun Cluster, sofern es nicht ausgeführt wird.

Sun Cluster muss für die Installation von Sun Cluster Geographic Edition ausgeführt werden. Sie können dies überprüfen, indem Sie den Befehl `scstat` verwenden.

5. Führen Sie eine Neuinstallation von Sun Cluster Geographic Edition Release 5 aus, indem Sie das Java ES-Installationsprogramm verwenden.

- a. Starten Sie das Java ES-Installationsprogramm auf dem Computer, der als Host für Access Manager Release 4 dient.

```
cd Java ES Release 5 distribution/os_arch  
./installer
```

wobei *os_arch* der Plattform entspricht, wie z. B. *Solaris_sparc*.
(Verwenden Sie die Option `installer -nodisplay` für die Befehlszeilenschnittstelle.)

Nach der Willkommenseite sowie der Lizenzvereinbarung wird eine Seite für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten erkannt werden, die direkt vom Java ES-Installationsprogramm aktualisiert werden können, wird der Status als „aktualisierbar“ angezeigt.)

- b. Wählen Sie auf der Seite für die Komponentenauswahl Sun Cluster Geographic Edition.
 - c. Wählen Sie „Jetzt konfigurieren“ oder „Später konfigurieren“.
 - Es spielt keine Rolle, ob Sie die Konfiguration zu diesem Zeitpunkt oder später durchführen, da eine erneute Konfiguration nicht erforderlich ist.
 - d. Falls erforderlich, wählen Sie die Option zur Installation von lokalisierten Paketen.
 - e. Beenden Sie das Java ES-Installationsprogramm, nachdem die Installation abgeschlossen wurde.

HINWEIS Wenn Sie die Sun Cluster Geographic Edition-Software unter Solaris 8 aktualisieren, müssen Sie den Befehl `pkgadd` verwenden, um die Software aus der Java ES Release 5-Verteilung zu aktualisieren. Das Java ES-Installationsprogramm unterstützt keine Installation der Sun Cluster Geographic Edition-Software unter Solaris 8.

6. Installieren Sie alle erforderlichen Sun Cluster Geographic Edition-Patches.

Weitere Informationen hierzu finden Sie im *Sun Cluster Geographic Edition Installation Guide*, <http://docs.sun.com/doc/817-7500>.

7. Führen Sie Schritt [Schritt 1 auf Seite 105](#) bis [Schritt 6](#) auf allen Clustern aus, bei denen eine Partnerschaft mit diesem Cluster besteht.

8. Starten Sie die Sun Cluster Geographic Edition-Software Release 5 neu.

```
/usr/cluster/bin/geoadm start
```

Wenn für das Cluster eine Partnerschaft vorliegt, müssen alle Knoten auf beiden Partnern aktualisiert werden, bevor die Sun Cluster Geographic Edition-Software gestartet wird.

Weitere Informationen finden Sie im zuvor aufgeführten *Installation Guide* und im *Sun Cluster Geographic Edition Administration Guide*,
<http://docs.sun.com/doc/817-7501>.

9. Fügen Sie alle Anwendungsressourcengruppen hinzu, die Sie zuvor beim Vorbereiten des Clusters für die Aktualisierung entfernt haben (siehe „[Cluster für die Aktualisierung vorbereiten](#)“ auf Seite 102).

```
geopg add-resource-group resourcegroup protectiongroupname
```

10. Starten Sie alle Schutzgruppen, die Sie hinzugefügt haben.

```
geopg start protectiongroupname -e local | global [-n]
```

Überprüfen der Aktualisierung

Um zu überprüfen, ob die Aktualisierung der Sun Cluster Geographic Edition-Software erfolgreich war, gehen Sie wie folgt vor:

1. Führen Sie folgenden Befehl aus:

```
/usr/cluster/bin/geoadm --version
```

Ausgabewerte finden Sie in [Tabelle 4-4 auf Seite 102](#).

2. Führen Sie nach der Aktualisierung beider Partner gegebenenfalls die folgenden Befehle auf einem Cluster-Knoten beider Partner aus:

```
/usr/cluster/bin/geoadm start
```

```
/usr/cluster/bin/geoadm show
```

Über den Befehl wird angezeigt, ob die Sun Cluster Geographic Edition-Software auf dem entsprechenden Knoten aktiv ist.

Aufgaben nach der Aktualisierung

Mit Ausnahme der in „[Aktualisierungsverfahren](#)“ auf Seite 105 beschriebenen Schritte müssen keine weiteren Aufgaben nach der Aktualisierung durchgeführt werden.

Aufheben der Aktualisierung

Das Aufheben der Aktualisierung der Sun Cluster Geographic Edition-Software wird nicht unterstützt.

Sie können jedoch Sun Cluster Geographic Edition Release 5 entfernen, indem Sie die Deinstallationsfunktion des Java ES-Installationsprogramms verwenden und anschließend das Installationsprogramm der Version 3.1 8/05 verwenden, um Version 3.1 8/05 erneut zu installieren. Da Sun Cluster Geographic Edition Release 5 Daten schreibt, die Version 3.1 8/05 nicht lesen kann, muss ein Zurücksetzen vor dem Start von Release 5 erfolgen, also vor dem Start der aktualisierten Sun Cluster Geographic Edition-Software (siehe „[Aktualisierungsverfahren](#)“ auf Seite 105).

Directory Server

In diesem Kapitel wird die Aktualisierung von Directory Server auf Java ES 5 (Release 5) beschrieben: Sun Java System Directory Server 6.0.

Das Kapitel enthält einen Überblick über die Aspekte der verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Directory Server“ auf Seite 111
- „Aktualisieren von Directory Server von Java ES Release 4“ auf Seite 116
- „Aktualisieren von Directory Server von Java ES Release 3“ auf Seite 125
- „Aktualisieren von Directory Server von Java ES Release 2“ auf Seite 126

HINWEIS Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf Verzeichnispfade, die im Folgenden als *serverRoot* (Directory Server 5.x) und *DirServer-base* (Directory Server 6.0) angegeben werden. Bei der Installation von Directory Server wurden diese Pfade mindestens teilweise als Installationsverzeichnisse angegeben. Wenn nicht, wurde vom Java ES-Installationsprogramm ein Standardwert zugewiesen.

Die Standardwerte für diese Verzeichnispfade sind in der folgenden Tabelle aufgelistet.

Tabelle 5-1 Directory Server Verzeichnispfade

Variable des Pfadnamens	Solaris OS	Linux OS
<i>serverRoot</i> (Directory Server 5.x)	/var/opt/mps/serverroot	/var/opt/sun/directory-server

Tabelle 5-1 Directory Server Verzeichnispfade *(Fortsetzung)*

Variable des Pfadnamens	Solaris OS	Linux OS
<i>DirServer-base</i> (Directory Server 6.0)	/opt/SUNWdsee	/opt/sun

Überblick über Aktualisierungen von Directory Server

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Directory Server auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5](#)
- [Java ES Wegweiser für die Aktualisierung auf Release 5](#)
- [Directory Server-Daten](#)
- [Vorgehensweise zur Aktualisierung von Directory Server](#)

Über Java ES Release 5

Java ES Release 5 Directory Server stellt ein größeres Release mit einer Reihe neuer Funktionen und Verbesserungen dar. Weitere Informationen erhalten Sie in den *Directory Server Enterprise Edition 6 Release Notes* unter <http://docs.sun.com/doc/820-0284>.

Java ES Wegweiser für die Aktualisierung auf Release 5

[Tabelle 5-2](#) zeigt die unterstützten Wege für die Aktualisierung von Directory Server auf Java ES Release 5. Die Tabelle gilt sowohl für das Solaris- als auch für das Linux-Betriebssystem.

Tabelle 5-2 Wege für die Aktualisierung auf Java ES 5 (Release 5): Directory Server 6.0

Java ES Release	Directory Server Version	Allgemeiner Ansatz	Neukonfiguration erforderlich
Release 4	Sun Java System Directory Server 5.2 2005Q4	Direkte Aktualisierung: Neuinstallation und Migration sämtlicher Daten.	Konfigurationsdaten wurden von der vorherigen Version zum neu installierten Directory Server migriert
	Sun Java System Administration Server 5.2 2005Q4	Administration Server-Funktionalität wurde durch Directory Service Control Center und Directory Server EE-Befehlszeilenprogramme ersetzt.	

Tabelle 5-2 Wege für die Aktualisierung auf Java ES 5 (Release 5): Directory Server 6.0

Java ES Release	Directory Server Version	Allgemeiner Ansatz	Neukonfiguration erforderlich
Release 3	Sun Java System Directory Server 5 2005Q1	Direkte Aktualisierung: Neuinstallation und Migration sämtlicher Daten.	Konfigurationsdaten wurden von der vorherigen Version zum neu installierten Directory Server migriert
	Sun Java System Administration Server 5 2005Q1	Administration Server-Funktionalität wurde durch Directory Service Control Center und Directory Server EE-Befehlszeilenprogramme ersetzt.	
Release 2	Sun Java System Directory Server 5.2 2004Q2	Direkte Aktualisierung: Neuinstallation und Migration sämtlicher Daten.	Konfigurationsdaten wurden von der vorherigen Version zum neu installierten Directory Server migriert
	Sun Java System Administration Server 5.2 2004Q2	Administration Server-Funktionalität wurde durch Directory Service Control Center und Directory Server EE-Befehlszeilenprogramme ersetzt.	
Release 1	Sun ONE Directory Server 5.2	Direkte Aktualisierung nicht zertifiziert. Sie können jedoch denselben Ansatz wie für die Aktualisierung von Release 2 anwenden.	Konfigurationsdaten wurden von der vorherigen Version zum neu installierten Directory Server migriert
	Sun ONE Administration Server 5.2		
Versionen vor Java ES	Sun ONE Directory Server 5.2	Direkte Aktualisierung nicht zertifiziert. Sie können jedoch denselben Ansatz wie für die Aktualisierung von Release 2 anwenden.	Konfigurationsdaten wurden von der vorherigen Version zum neu installierten Directory Server migriert
	Sun ONE Administration Server 5.2		
	Sun ONE Directory Server 5.1 Sun ONE Administration Server 5.1	Keine direkte Aktualisierung: Aktualisieren Sie zuerst auf Release 3. Informationen dazu finden Sie im <i>Java Enterprise System 2005Q1 Upgrade and Migration Guide</i> unter http://docs.sun.com/doc/819-0062 . Führen Sie anschließend eine Aktualisierung von Release 3 auf Release 5 durch.	Informationen hierzu erhalten Sie im <i>Java Enterprise System 2005Q1 Upgrade and Migration Guide</i> unter http://docs.sun.com/doc/819-0062 .

Directory Server-Daten

Directory Server 5.x-Versionen verwendeten Directory Server für das Speichern der Konfigurationsdaten. Die Daten wurden in einer bestimmten Baumstruktur innerhalb des Verzeichnisses gespeichert. Die Directory Server-Instanz, die als Host für die Konfiguration dient, wurde als Konfigurationsverzeichnis bezeichnet. Das Konfigurationsverzeichnis konnte sich auf demselben Computer befinden wie andere Directory Server-Instanzen. In den meisten Bereitstellungsarchitekturen befand sich das Konfigurationsverzeichnis jedoch auf einem anderen Computer als die übrigen Komponenten, die das Verzeichnis zum Speichern der Konfigurationsdaten nutzen.

Directory Server 6.0 speichert keine Konfigurationsdaten mehr in einem Konfigurationsverzeichnis. Die Konfiguration wird mithilfe des Directory Service Control Center (oder der Directory Server EE-Befehlszeilenprogramme) ausgeführt. Der Zugriff auf die Konfiguration sollte über diese Schnittstelle erfolgen. Die Konfigurationsdaten werden vom Directory Service Control Center in seiner eigenen lokalen Directory Server-Instanz gespeichert.

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Directory Server-Software auf Release 5 betroffen sind.

Tabelle 5-3 Directory Server Verwendung der Daten

Datentyp	Standort	Verwendung
Directory Server-Konfigurationsdaten	Directory Server 5.1 und 5.2: Konfigurationsverzeichnis Directory Server 6.0: Zugriff über den Directory Service Control Center und die Directory Server EE-Befehlszeilenprogramme.	Konfiguration der Directory Server-Instanzen
Directory Server-Schema		Struktur und Semantik von Daten innerhalb des Verzeichnisses definieren
Sicherheitsdaten	Directory Server 5.1 und 5.2: Konfiguration von SSL über die Directory Server Console. Directory Server 6.0: Konfiguration von SSL über den Directory Service Control Center und die Directory Server EE-Befehlszeilenprogramme.	Serverzertifikate.
Benutzerdaten	Directory Server	Anwendungen mit benutzerspezifischen Konfigurationsdaten und Benutzerprofilen unterstützen

Vorgehensweise zur Aktualisierung von Directory Server

Die Vorgehensweise zur Aktualisierung von Directory Server hängt im Grunde von den verschiedenen Aspekten ab, die in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) besprochen wurden: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

In diesem Abschnitt wird im Detail auf Directory Server eingegangen, indem Themen besprochen werden, die Ihre Aktualisierungspläne von Directory Server beeinflussen können.

Kompatibilität

Java ES Release 5 Directory Server führt keine neuen öffentlichen Schnittstellen ein und ist rückwärts kompatibel mit Release 4 Directory Server und früheren Versionen.

Release 5 führt jedoch Änderungen an privaten Administrationsschnittstellen ein. Die Release 5-Schnittstellen sind nicht mit früheren Versionen von Directory Server kompatibel. Insbesondere wurde für die Konfiguration früherer Directory Server-Instanzen verwendete Administration Server durch das Directory Service Control Center and Directory Server EE-Befehlszeilenprogramme ersetzt und das Verzeichnissuffix `o=NetscapeRoot` zum Speichern von Directory Server-Konfigurationsinformationen wurde gelöscht. Detaillierte Informationen erhalten Sie im *Directory Server Enterprise Edition 6 Migration Guide* unter <http://docs.sun.com/doc/819-0994>.

-Abhängigkeiten

Abhängigkeiten zu anderen Java ES-Komponenten können grundsätzlich das Verfahren für die Aktualisierung und Neukonfiguration der Directory Server-Software beeinflussen.

Für Directory Server bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Directory Server ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)). Die Aktualisierung von Directory Server hängt möglicherweise von den aktualisierten Versionen dieser gemeinsam genutzte Komponenten ab.

- **Directory Proxy Server.** Für Directory Server besteht eine Abhängigkeit zu Web Proxy Server für die Bereitstellung von verbesserten Sicherheitsfunktionen und Leistungen für LDAP-Anfragen.

Aktualisieren von Directory Server von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von Directory Server von Java ES 2005 Q4 (Release 4) auf Java ES 2005 Q5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 4-Version von Directory Server](#)
- [Aktualisierung mehrerer Instanzen](#)

Einführung

Berücksichtigen Sie bei der Aktualisierung von Java ES von Directory Server Release 4 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch eine Neuinstallation von Directory Server Release 5 und anschließende Verwendung von Migrationstools, um die vorherigen Directory Server-Instanzen in neuen, eindeutigen Directory Server Release 5-Instanzen erneut zu erstellen.
- **Aktualisierungsabhängigkeiten.** Directory Server ist von einer Reihe von gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)), die alle automatisch vom Java ES-Installationsprogramm auf Release 5 aktualisiert werden, wenn Sie eine Aktualisierung von Directory Server durchführen.
- **Rückwärtskompatibilität.** Directory Server Release 5 ist nicht rückwärts kompatibel zur Release 4-Version, wie unter „[Kompatibilität](#)“ auf [Seite 114](#) beschrieben. Mithilfe der Migrationstools ist es jedoch möglich, das Suffix o=NescapeRoot zu migrieren, wenn Sie eine Reihe an Directory Server-Instanzen beibehalten, die sich auf das Directory Server 5.x-Administrationsframework stützen.
- **Zurücksetzen der Aktualisierung.** Das Zurücksetzen der Aktualisierung auf Release 5 erfolgt durch das Zurückkehren zur vorherigen Version, die bei der Aktualisierung auf Release 5 unverändert beibehalten wurde.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Directory Server ist für das Solaris- und Linux-Betriebssystem identisch.

Aktualisierung der Release 4-Version von Directory Server

In diesem Abschnitt wird die Aktualisierung von Directory Server von Java ES Release 4 auf Java ES Release 5 unter Solaris und Linux beschrieben. Plattformspezifische Vorgänge sind durch die Angabe des jeweiligen Betriebssystems, auf das sich der Vorgang bezieht, gekennzeichnet. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren von Release 4 von Directory Server](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung der Directory Server-Software beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Directory Server-Aktualisierungsabhängigkeiten](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)
- [Directory Server-Image erstellen \(optional\)](#)

Aktuelle Versionsinformationen überprüfen

Sie können die aktuelle Version von Directory Server überprüfen, indem Sie den Directory Server-Daemon mithilfe der Option `-v` neu starten:

```
cd serverRoot/bin/slapd/server
./ns-slapd -v
```

Tabelle 5-4 Directory Server Ausgaben der Versionsüberprüfung

Java ES Release	Directory Server-Versionsnummer
Release 2	Sun Java(TM) System Directory Server/5.2_Patch_2
Release 3	Sun Java(TM) System Directory Server/5.2_Patch_3
Release 4	Sun Java(TM) System Directory Server/5.2_Patch_4

Tabelle 5-4 Directory Server Ausgaben der Versionsüberprüfung

Java ES Release	Directory Server-Versionsnummer
Release 5	Sun Java(TM) System Directory Server/6.0

Wenn unter Solaris 10 die Ausführung des Befehls `ns-slapd` fehlschlägt, setzen Sie den Bibliothekspfad bei Ausführung des Befehls auf null.

`LD_LIBRARY_PATH= ./ns-slapd -v`

Directory Server-Aktualisierungsabhängigkeiten

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Alle gemeinsam genutzte Komponenten, die von Directory Server benötigt werden, werden jedoch automatisch aktualisiert, wenn Sie eine Aktualisierung von Directory Server auf Release 5 durchführen.

Erforderliche Konfigurationsinformationen und Passwörter abrufen

Sie sollten über die Benutzer-ID und das Passwort des Administrators der aktuell installierten Version von Directory Server verfügen. Andere Konfigurationsinformationen werden durch den Aktualisierungsvorgang erhalten.

Directory Server-Image erstellen (optional)

Wenn Directory Server Release 5 auf einem anderen Computer installiert wird als sich die Release 4-Version befindet, sollte auf dem Computer, auf dem Directory Server installiert wird, ein Image der Release 4-Version erstellt werden. Das Image wird für die automatische Datenmigration (mithilfe des Befehls `dsmig`) auf die neuen Directory Server Release 5-Instanzen benötigt.

Das Release 4-Image beinhaltet sämtliche Schema-, Konfigurations-, Sicherheits- und Datenbankdateien in einem identischen Layout im Vergleich zur ursprünglichen Directory Server 5.x *serverRoot*-Dateistruktur. Das Image wird benötigt, um die Datenmigration zu den neuen Release 5 Directory Server-Instanzen durchzuführen.

Aktualisieren von Release 4 von Directory Server

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Directory Server haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

Zu berücksichtigende Aspekte bei der Aktualisierung

Bei der Aktualisierung der Directory Server-Software auf Java ES Release 5 müssen folgende Aspekte berücksichtigt werden:

- Sämtliche Java ES-Komponenten, die eine Directory Server-Instanz verwenden (wie z. B. Access Manager, Portal Server oder Sun Java Communications Suite-Komponenten) sollten beendet und gegebenenfalls neukonfiguriert werden, um auf die entsprechende neue Release 5-Instanz zugreifen zu können.
- Im Falle von Bereitstellungsarchitekturen, in denen mehrere Directory Server-Instanzen auf einem einzelnen Computer ausgeführt werden (und demselben installierten Directory Server-Image entsprechen) müssen Sie das Directory Server-Image nur ein Mal aktualisieren. Sie müssen jedoch die Migration der Daten für jede Instanz einzeln durchführen.
- In vielen Directory Server Release 4-Bereitstellungsarchitekturen ist das Konfigurationsverzeichnis eine separate Directory Server-Instanz. Diese Instanzen müssen nicht aktualisiert werden, da das Konfigurationsverzeichnis in Release 5 gelöscht wurde. Andererseits beinhaltet die Aktualisierung gegebenenfalls die Bereitstellung der Directory Server Release 5-Verwaltungskonsole (das Directory Service Control Center) auf einem separaten Computer, von dem aus Sie Directory Server-Instanzen remote verwalten.
- Directory Server ist mit einem Befehlszeilentool ausgestattet, mit dem die Migration von Schema-, Konfigurations-, Sicherheits- und Benutzerdaten automatisiert werden kann. Das Migrationstool ermöglicht eine schrittweise Migration dieser unterschiedlichen Daten. Die meisten Aktualisierungsszenarios profitieren zumindest bei einigen Daten von der automatischen Migration.

Aktualisierungsverfahren

Das im Folgenden beschriebene Verfahren ist für Directory Server-Instanzen anzuwenden, die lokal auf dem Computer ausgeführt werden, auf dem die Aktualisierung durchgeführt wird, oder für sämtliche Instanzen, die auf dem Zielcomputer ausgeführt werden, wenn Instanzen zu einem anderen Computer migriert werden.

1. Melden Sie sich als Root oder Superuser an.

su -

2. Beenden Sie die Directory Server (5.2) Release 4-Instanzen.

`serverRoot/slapd-instanceName/stop-slapd`

Überprüfen Sie im Fehlerprotokoll (`serverRoot/slapd-hostName/logs/errors`), ob die Instanzen ordnungsgemäß beendet wurden.

```
[23/Jan/2006:15:56:47 +0100] - All database threads now stopped
```

```
[23/Jan/2006:15:56:50 +0100] - slapd stopped.
```

3. Stellen Sie sicher, dass der Hostcomputer für Directory Server Release 5 über ausreichenden Speicherplatz verfügt.

Die grundlegende Rechnung lautet:

$2 * (\text{space for existing server}) + (\text{space for LDIF files})$

Es gibt leider kein Tool, mit dem die Größe einer aus einer exportierten Datenbank erstellten LDIF-Datei vorhergesehen werden kann. Die Größe richtet sich nach der Anzahl an Dateneinträgen, ihrer internen Darstellung, der Anzahl von Indexen etc.

4. Zur remoten Installation von Release 5 erstellen Sie ein Release 4-Image und übertragen es an den Remote-Computer.

Siehe auch „[Directory Server-Image erstellen \(optional\)](#)“ auf Seite 118.

5. Stellen Sie sicher, dass alle Java ES-Komponenten, von denen Directory Server zwingend abhängig ist (siehe „[Directory Server-Aktualisierungsabhängigkeiten](#)“ auf Seite 118) aktualisiert wurden.
6. Führen Sie eine Neuinstallation von Directory Server Release 5 aus.

Führen Sie die folgenden Schritte aus:

- a. Starten Sie das Java ES-Installationsprogramm.

```
cd java ES Release 5 distribution/os_arch

./installer
```

wobei *os_arch* der Plattform entspricht, wie z. B. *Solaris_sparc*. (Verwenden Sie die Option *installer -nodisplay* für die Befehlszeilenschnittstelle.)

Nach der Willkommenseite sowie der Lizenzvereinbarung wird eine Seite für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten erkannt werden, die direkt vom Java ES-Installationsprogramm aktualisiert werden können, wird der Status als „aktualisierbar“ angezeigt.)

- b.** Wählen Sie die Directory Server-Subkomponente der Directory Server Enterprise Edition.

Sie müssen ebenfalls die gewünschten administrativen Subkomponenten installieren (Directory Service Control Panel oder Befehlszeilenprogramme).

- c.** Geben Sie einen Installationspfad an, der sich vom Installationspfad des vorhandenen Release 4 Directory Server unterscheidet.
- d.** Wählen Sie „Jetzt konfigurieren“ oder „Später konfigurieren“.

Es ist unerheblich, ob Sie die Konfiguration zu diesem Zeitpunkt oder später durchführen, da eigentlich keine Konfiguration für Directory Server erforderlich ist. Wenn Sie jedoch die Konfiguration zu diesem Zeitpunkt durchführen möchten, sollten Sie *keine* neue Instanz erstellen.

- e.** Bestätigen Sie Ihre Auswahl für die Installation.

Die Directory Server-Pakete werden aktualisiert. Anschließend wird eine Aktualisierungszusammenfassung angezeigt.

- f.** Beenden Sie das Java ES-Installationsprogramm.

7. Erstellen Sie eine Directory Server-Instanz.

DirServer-base/ds6/bin/dsadm create *instancePath*

wobei *instancePath* der vollständige Pfad zur Directory Server-Instanz ist.

Informationen zum Erstellen von Directory Server-Instanzen finden Sie im *Directory Server Enterprise Edition 6 Administration Guide* unter <http://docs.sun.com/doc/819-0995..>

Wenn Sie keine neue Instanz erstellen, wird bei der Migration von Daten mit dem Befehl dsmig command (**Schritt 8**) automatisch eine neue Instanz erstellt.

Wenn unter Solaris 10 die Ausführung des Befehls dsadm fehlschlägt, setzen Sie den Bibliothekspfad bei Ausführung des Befehls auf null.

LD_LIBRARY_PATH= ./dsadm create *instancePath*

8. Migrieren Sie Release 4-Daten in die Directory Server Release 5-Instanz.

Verwenden Sie die Befehle *DirServer-base*/ds6/bin/dsmig.

Mithilfe der dsmig-Befehle werden die Release 4-Daten an das Release 5-Format angepasst und an den entsprechenden Speicherorten gespeichert. Eine typische auf einem einzelnen Computer mit einer Directory Server-Instanz durchgeführte Migration könnte beispielsweise wie folgt aussehen:

```
dsmig migrate-schema -v old_instancePath new_instancePath

dsmig migrate-config -v old_instancePath new_instancePath

dsmig migrate-security -v old_instancePath new_instancePath

dsmig migrate-data -v old_instancePath new_instancePath
```


HINWEIS
S

- Wenn unter Solaris 10 die Ausführung des Befehls `dsmig migrate-config` fehlschlägt, setzen Sie den Bibliothekspfad bei Ausführung des Befehls auf null.

```
LD_LIBRARY_PATH= ./dsmig migrate-config ...
```

- Wenn die von Ihnen migrierte Directory Server-Instanz Konfigurationsdaten für andere Java ES-Komponenten speichert, wie beispielsweise für die Sun Java Communications Suite Messaging Server-Komponente, müssen Sie möglicherweise einen bestimmten Teil des Directory Information Tree mit dem Namen `o=netscaperoot.` migrieren. Dieses Root-Suffix wird nicht standardmäßig migriert. Um `o=netscaperoot.` zu migrieren, verwenden Sie die Option `-N` der Befehle `dsmig migrate-config` und `dsmig migrate-data`. Beispiel:

```
dsmig migrate-config -v old_instancePath  
new_instancePath -N
```

- Wenn Sie aus einer Instanz innerhalb einer 32-Bit-Architektur in eine Instanz innerhalb einer 64-Bit-Architektur migrieren, können Sie den Befehl `dsmig migrate-data` (Tool für die automatische Migration) nicht verwenden. In diesem Fall müssen Sie die Daten manuell migrieren, wie im unten referenzierten *Migrationshandbuch* beschrieben. Sie können jedoch weiterhin Schema-, Konfigurations- und Sicherheitsdaten automatisch migrieren.
- In einigen Fällen werden beim Starten von Directory Server nach der Migration von Verzeichnisdaten von der neuen Fehlerüberprüfung von Release 5 in Directory Server-Gruppeneinträgen zirkuläre Definitionen entdeckt. Zwar sind diese zirkulären Definitionen funktionell betrachtet harmlos, sie können jedoch aufgrund der Tatsache, dass Sie in der Fehlerdatei protokolliert sind, zu einer Vielzahl an Fehlern führen.

Weitere Informationen zum Migrationsprozess, zu den `dsmig`-Befehlen und zur manuellen Migration erhalten Sie im *Directory Server Enterprise Edition 6 Migration Guide* unter <http://docs.sun.com/doc/819-0994>.

Überprüfen der Aktualisierung

Um zu überprüfen, ob die Aktualisierung von Directory Server erfolgreich war, gehen Sie wie folgt vor:

1. Starten Sie die Directory Server-Instanz wie folgt:

DirServer-base/ds6/bin/dsadm -V

Ausgabewerte finden Sie in [Tabelle 5-4 auf Seite 117](#).

2. Prüfen Sie die Startmeldungen im Directory Server-Fehlerprotokoll:

instancePath/logs/errors

HINWEIS Beim Starten werden nun von Directory Server Release 5 zirkuläre Definitionen entdeckt. Diese zirkulären Definitionen sind zwar funktionell betrachtet harmlos, können jedoch zu einer Vielzahl an Fehlern führen, wenn Sie eine Aktualisierung von einer früheren Version durchführen, die solche zirkulären Definitionen enthält.

Aufgaben nach der Aktualisierung

Abgesehen davon, dass sämtliche Java ES-Komponenten, die von Directory Server abhängig sind, neu konfiguriert werden müssen, sodass sie auf die neuen Directory Server-Instanzen verweisen, müssen neben den in [„Aktualisierungsverfahren“ auf Seite 119](#) beschriebenen Schritten keine weiteren Aufgaben nach der Aktualisierung durchgeführt werden.

Aufheben der Aktualisierung

Das Zurücksetzen der Release 5-Aktualisierung erfolgt durch das Zurückkehren zur vorherigen Version, die bei der Aktualisierung auf Release 5 unverändert beibehalten wurde.

Aktualisierung mehrerer Instanzen

In den unter [„Aktualisierung der Release 4-Version von Directory Server“ auf Seite 117](#) beschriebenen Verfahren werden die Bereitstellungsarchitekturen, in denen Directory Server für Hochverfügbarkeit und Skalierbarkeit repliziert wird, nicht ausdrücklich behandelt. Diese Architekturen können eine Replikation von Directory Server oder die Bereitstellung von Directory Server als Datendienst in einer Sun Cluster-Umgebung beinhalten.

In diesem Abschnitt wird die Aktualisierung von Directory Server für diese Fälle beschrieben.

Rolling Upgrades von Directory Server-Replikaten

Mehrere Directory Server-Instanzen auf verschiedenen Computersystemen, wie sie beispielsweise in Bereitstellungsarchitekturen mit Multimaster-Replikation verwendet werden, können nacheinander jeweils einzeln aktualisiert werden. Nach der ersten Synchronisierung sämtlicher Directory Server-Master aktualisieren Sie jede Instanz auf dem entsprechenden Hostcomputer, während die anderen Instanzen weiterhin ausgeführt werden. Dieses so genannte Rolling Upgrade ermöglicht, dass der Verzeichnisdienst während der Aktualisierung der einzelnen Directory Server-Instanzen, die den Dienst bereitstellen, online bleiben kann.

Aktualisieren von Directory Server als Datendienst

Die Informationen bezüglich der Aktualisierung und der Aufhebung der Aktualisierung von Directory Server als Datendienst in einer Sun Cluster-Umgebung befinden sich derzeit in der Entwicklungsphase.

Aktualisieren von Directory Server von Java ES Release 3

Das Verfahren zur Aktualisierung von Java ES 2003Q1 (Release 3) Directory Server auf Release 5 ist mit dem Verfahren zur Aktualisierung von Directory Server Release 4 auf Release 5 identisch.

Um die Release 3-Version von Directory Server auf Release 5 zu aktualisieren, folgen Sie den Anweisungen unter „[Aktualisieren von Directory Server von Java ES Release 4](#)“ auf Seite 116. Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 3.

Aktualisieren von Directory Server von Java ES Release 2

Das Verfahren für die Aktualisierung von Java ES 2004Q2 (Release 2) Directory Server auf Release 5 ist mit der Aktualisierung von Directory Server Release 4 auf Release 5 identisch. Eine Ausnahme besteht jedoch bei den Aufgaben, die vor der Aktualisierung durchgeführt werden müssen. Hier sollte eine Aktualisierung aller gemeinsam genutzte Komponenten auf Release 5 durchgeführt werden (siehe [Tabelle 1-7 auf Seite 51](#)).

Anleitungen für die Aktualisierung von gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie in [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#).

Um die Release 2-Version von Directory Server auf Release 5 zu aktualisieren, folgen Sie den Anweisungen unter [„Aktualisieren von Directory Server von Java ES Release 4“ auf Seite 116](#). Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 2.

Directory Proxy Server

In diesem Kapitel wird die Aktualisierung von Directory Proxy Server auf Java ES 5 (Release 5) beschrieben: Sun Java System Directory Proxy Server 6.0.

Das Kapitel enthält einen Überblick über die Aspekte der verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Directory Proxy Server,, auf Seite 129
- „Aktualisieren von Directory Proxy Server von Java ES Release 4,, auf Seite 134
- „Aktualisieren von Directory Proxy Server von Java ES Release 3,, auf Seite 141
- „Aktualisieren der Directory Proxy Server Release 2-Version Java ES,, auf Seite 142

HINWEIS Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf Verzeichnispfade, die im Folgenden als *serverRoot* (Directory Proxy Server 5.x) und *DirServer-base* (Directory Proxy Server 6.0) angegeben werden. Bei der Installation von Directory Proxy Server wurden diese Pfade mindestens teilweise als Installationsverzeichnisse angegeben. Wenn nicht, wurde vom Java ES-Installationsprogramm ein Standardwert zugewiesen.

Die Standardwerte für diese Verzeichnispfade sind in der folgenden Tabelle aufgelistet.

Tabelle 6-1 Directory Proxy Server Verzeichnispfade

Variable des Pfadnamens	Solaris OS	Linux OS
<i>serverRoot</i> (Directory Proxy Server 5.x)	/var/opt/mps/serverroot	/var/opt/sun/directory-server
<i>DirServer-base</i> (Directory Proxy Server 6.0)	/opt/SUNWdsee	/opt/sun

Überblick über Aktualisierungen von Directory Proxy Server

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Directory Proxy Server auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5](#)
- [Wegweiser für die Aktualisierung auf Java ES Release 5](#)
- [Directory Proxy Server-Daten](#)
- [Directory Proxy Server Vorgehensweise zur Aktualisierung](#)

Über Java ES Release 5

Java ES Release 5 Directory Proxy Server stellt eine Major-Release dar und ist in Bezug auf Release 4 Directory Proxy Server und all seine vorherigen Releases ein neues Produkt.

Bei Release 5 Directory Proxy Server handelt es sich weiterhin um einen LDAP-Proxy, das Programm verfügt jedoch über neue, erweiterbare Routing-Möglichkeiten. Release 5 ermöglicht ebenfalls die Verwendung von Virtual Directory, womit mehrere Datenansichten in einer einzigen Ansicht dargestellt werden können. Diese Datenansichten können sowohl LDAP- als auch SQL-zugängliche Datenspeicher darstellen.

Weitere Informationen erhalten Sie in den *Directory Server Enterprise Edition 6 Release Notes*.

Wegweiser für die Aktualisierung auf Java ES Release 5

[Tabelle 6-2](#) zeigt die unterstützten Wege für die Aktualisierung von Directory Proxy Server auf Java ES Release 5. Die Tabelle gilt sowohl für das Solaris- als auch für das Linux-Betriebssystem.

Tabelle 6-2 Wege für die Aktualisierung auf Java ES 5 (Release 5): Directory Proxy Server 6.0

Java ES Release	Directory Proxy Server Version	Allgemeiner Ansatz	Neukonfiguration erforderlich
Release 4	Sun Java System Directory Proxy Server 5.2 2005Q4	Direkte Aktualisierung: Ersetzen Sie Release 4 durch eine Neuinstallation und Konfiguration von Release 5.	Wenn die neue Konfiguration rückwärts kompatibel sein soll, muss die vorherige Konfiguration mit neuen Konfigurationseinstellungen verknüpft werden.
Release 3	Sun Java System Directory Proxy Server 5.2 2005Q1	Direkte Aktualisierung: Ersetzen Sie Release 3 mit einer Neuinstallation und Konfiguration von Release 5.	Wenn die neue Konfiguration rückwärts kompatibel sein soll, muss die vorherige Konfiguration mit neuen Konfigurationseinstellungen verknüpft werden.
Release 2	Sun Java System Directory Proxy Server 5.2 2004Q2	Direkte Aktualisierung: Ersetzen Sie Release 2 mit einer Neuinstallation und Konfiguration von Release 5.	Wenn die neue Konfiguration rückwärts kompatibel sein soll, muss die vorherige Konfiguration mit neuen Konfigurationseinstellungen verknüpft werden.
Release 1	Sun ONE Directory Proxy Server5.2	Direkte Aktualisierung nicht zertifiziert. Sie können jedoch denselben Ansatz wie für die Aktualisierung von Release 2 anwenden.	Wenn die neue Konfiguration rückwärts kompatibel sein soll, muss die vorherige Konfiguration mit neuen Konfigurationseinstellungen verknüpft werden.
Versionen vor Java ES	Sun ONE Directory Proxy Server5.2	Direkte Aktualisierung nicht zertifiziert. Sie können jedoch denselben Ansatz wie für die Aktualisierung von Release 2 anwenden.	Wenn die neue Konfiguration rückwärts kompatibel sein soll, muss die vorherige Konfiguration mit neuen Konfigurationseinstellungen verknüpft werden.
	Sun ONE Directory Access Router 5.0 oder 5.0 SP1	Keine direkte Aktualisierung: Aktualisieren Sie zuerst auf Release 3. Informationen dazu finden Sie im <i>Java Enterprise System 2005Q1 Upgrade and Migration Guide</i> , http://docs.sun.com/doc/819-0062 . Führen Sie anschließend eine Aktualisierung von Release 3 auf Release 5 durch.	Informationen hierzu erhalten Sie im <i>Java Enterprise System 2005Q1 Upgrade and Migration Guide</i> , http://docs.sun.com/doc/819-0062 .

Directory Proxy Server-Daten

Directory Proxy Server verwendet nicht mehr Directory Server für das Speichern von Konfigurationsdaten. Die Konfiguration wird mithilfe des neuen Directory Service Control Center oder der Directory Server EE-Befehlszeilenprogramme durchgeführt.

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Directory Proxy Server-Software betroffen sein können.

Tabelle 6-3 Verwendung von Directory Proxy Server-Daten

Datentyp	Standort	Verwendung
Directory Proxy Server-Konfigurationsdaten	Directory Proxy Server 5.2: Konfigurationsverzeichnis Directory Proxy Server 6.0: Zugriff über den Directory Service Control Center und die Directory Server EE-Befehlszeilenprogramme.	Konfiguration von Directory Proxy Server
Sicherheitsdaten	Directory Proxy Server 5.2: Konfiguration von SSL über die Directory Proxy Server Console. Directory Proxy Server 6.0: Konfiguration von SSL über den Directory Service Control Center und die Directory Server EE-Befehlszeilenprogramme.	Serverzertifikate

Directory Proxy Server Vorgehensweise zur Aktualisierung

Ihre Vorgehensweise bei der Aktualisierung von Directory Proxy Server hängt grundsätzlich von den zahlreichen in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) erläuterten Aspekten ab: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

Dieser Abschnitt konzentriert diese grundsätzliche Erläuterung auf Directory Proxy Server, indem Probleme dargestellt werden, die möglicherweise Ihren Aktualisierungsplan für Directory Proxy Server beeinflussen.

Kompatibilität

Release 5 Directory Proxy Server enthält Änderungen an der Schnittstelle, durch die ältere Versionen von Directory Proxy Server nicht kompatibel sind. Release 5 Directory Proxy Server basiert auf einer vollständig neuen Java-basierten Implementierung und die Konfiguration unterscheidet sich grundlegend von Release 4 Directory Proxy Server sowie älteren Releases.

Release 5 Directory Proxy Server kann jedoch so konfiguriert werden, dass das Programm rückwärts kompatibel ist und sich wie Release 4 Directory Proxy Server und ältere Releases verhält. Diese Konfiguration erfordert eine manuelle Verknüpfung vorheriger Konfigurationsattribute mit Konfigurationseigenschaften von Release 5. Detaillierte Informationen erhalten Sie im *Directory Server Enterprise Edition 6 Migration Guide*, <http://docs.sun.com/doc/819-0994>.

Release 5 Directory Proxy Server verfügt jedoch über unterschiedliche Standardverhaltensweisen im Vergleich zu vorherigen Versionen: LDAP-Steuerungen werden nicht durch den Proxy gelassen. Um das Verhalten vorheriger Versionen wiederherzustellen, können Sie die Sperrung dieser Steuerungen wie in „[Aufgaben nach der Aktualisierung](#)“, auf Seite 139 beschrieben aufheben.

-Abhängigkeiten

Abhängigkeiten zu anderen Java ES-Komponenten beeinflussen möglicherweise das Verfahren für die Aktualisierung und Neukonfiguration der Directory Proxy Server-Software.

Für Directory Proxy Server bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Directory Proxy Server ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)). Die Aktualisierung von Directory Proxy Server hängt möglicherweise von den aktualisierten Versionen dieser gemeinsam genutzten Komponenten ab.
- **Directory Server.** Directory Proxy Server verfügt über eine parallele Abhängigkeit zu Directory Server zur Bereitstellung erhöhter Sicherheit und verbesserter Leistung für LDAP-Anfragen. Directory Proxy Server bietet direkten Zugriff auf Directory Server, ist jedoch über diese funktionale Verbindung hinaus nicht abhängig von Directory Server.

Aktualisieren von Directory Proxy Server von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von Directory Proxy Server von Java ES 2005Q4 (Release 4) auf Java ES 5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 4-Version von Directory Proxy Server](#)
- [Aktualisierung mehrerer Instanzen](#)

Einführung

Berücksichtigen Sie bei der Aktualisierung von Java ES von Directory Proxy Server Release 4 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch eine Neuinstallation von Release 5 Directory Proxy Server und anschließender Konfiguration neuer Directory Proxy Server-Instanzen mithilfe des Directory Service Control Center oder Directory Server EE-Befehlszeilenprogrammen.
- **Aktualisierungsabhängigkeiten.** Directory Proxy Server ist von einer Reihe von gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)), die alle automatisch vom Java ES-Installationsprogramm auf Release 5 aktualisiert werden, wenn Sie eine Aktualisierung von Directory Proxy Server durchführen.
- **Rückwärtskompatibilität.** Release 5 Directory Proxy Server kann so konfiguriert werden, dass eine Rückwärtskompatibilität mit Release 4 gewährleistet wird. Weitere Informationen dazu finden Sie in „[Kompatibilität](#)„ auf [Seite 132](#).
- **Zurücksetzen der Aktualisierung.** Das Zurücksetzen der Release 5-Aktualisierung erfolgt durch das Zurückkehren zur vorherigen Version, die bei der Aktualisierung auf Release 5 nicht verändert wurde.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Directory Proxy Server ist für das Solaris- und Linux-Betriebssystem identisch.

Aktualisierung der Release 4-Version von Directory Proxy Server

In diesem Abschnitt wird die Aktualisierung von Directory Proxy Server von Java ES Release 4 auf Java ES Release 5 unter Solaris und Linux beschrieben. Plattformspezifische Vorgänge sind durch die Angabe des jeweiligen Betriebssystems, auf das sich der Vorgang bezieht, gekennzeichnet. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren von Release 4 von Directory Proxy Server](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung der Directory Proxy Server-Software beginnen, führen Sie die folgenden beschriebenen Aufgaben durch.

- [Aktuelle Versionsinformationen überprüfen](#)
- [Directory Proxy Server-Abhängigkeiten aktualisieren](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

Aktuelle Versionsinformationen überprüfen

Sie können die aktuelle Version von Directory Proxy Server mithilfe der folgenden Befehle überprüfen:

```
cd serverRoot/bin/dps/server/bin
./ldapfwd -v
```

Die Ausgabe wird in der folgenden Tabelle aufgelistet:

Tabelle 6-4 Directory Proxy Server Ausgaben der Versionsüberprüfung

Java ES Release	Directory Proxy Server-Versionsnummer
Release 2	Sun ONE Directory Proxy Server Version 5.2_Patch_2
Release 3	Sun ONE Directory Proxy Server Version 5.2_Patch_3
Release 4	Sun ONE Directory Proxy Server Version 5.2_Patch_4

Tabelle 6-4 Directory Proxy ServerAusgaben der Versionsüberprüfung

Java ES Release	Directory Proxy Server-Versionsnummer
Release 5 ¹	Sun ONE Directory Proxy Server Version 6.0

1. Der Befehl `ldapfwd` kann nicht für die Ausgabe einer Versionsnummer für Release 5 verwendet werden. Siehe auch [„Überprüfen der Aktualisierung“, auf Seite 139](#).

Directory Proxy Server-Abhängigkeiten aktualisieren

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkkumgebung) auf Java ES Release 5 zu aktualisieren. Für Directory Proxy Server bestehen nur für wenige gemeinsam genutzte Komponenten zwingende Aktualisierungsabhängigkeiten.

Wenn Sie die Directory Proxy Server-Abhängigkeiten aktualisieren, sollten Sie dies in der unten angegebenen Reihenfolge vornehmen, bevor Sie Directory Proxy Server aktualisieren. Überspringen Sie dabei die bereits aktualisierten Abhängigkeiten. Die Aktualisierung gemeinsam genutzter Komponenten erfolgt in der Regel automatisch durch das Java ES-Installationsprogramm.

- 1. Gemeinsam genutzte Komponenten.** Anleitungen für die Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie unter [„Aktualisieren der gemeinsam genutzten Java ES-Komponenten“, auf Seite 71](#). Alle gemeinsam genutzten Komponenten, die von Directory Proxy Server benötigt werden, werden jedoch automatisch vom Java ES-Installationsprogramm aktualisiert, wenn Sie eine Aktualisierung von Directory Proxy Server auf Release 5 durchführen.
- 2. Directory Server (keine zwingende Abhängigkeit)** Anleitungen für die Aktualisierung von Directory Server auf Release 5 finden Sie in [Kapitel 5, „Directory Server“ auf Seite 109](#). Release 5 Directory Proxy Server wird jedoch von Release 4 Directory Server unterstützt.

Erforderliche Konfigurationsinformationen und Passwörter abrufen

Konfigurationsinformationen werden durch den Aktualisierungsvorgang erhalten und können für das Verknüpfen von Konfigurationsattributen der Release 5 mit Konfigurationseigenschaften der Release 5 verwendet werden. Siehe auch [„Kompatibilität“, auf Seite 132](#).

Aktualisieren von Release 4 von Directory Proxy Server

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Directory Proxy Server haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

Zu berücksichtigende Aspekte bei der Aktualisierung

Bei der Aktualisierung der Directory Proxy Server-Software auf Java ES Release 5 müssen folgende Aspekte berücksichtigt werden:

- Sämtliche Java ES-Komponenten, die eine Directory Proxy Server-Instanz verwenden (wie z. B. Access Manager, Communications Express, Messaging Server oder Portal Server), sollten beendet und neukonfiguriert werden, um auf die entsprechende neue Release 5-Instanz zugreifen zu können.
- In einer Bereitstellungsarchitektur, in der mehrere Instanzen von Directory Proxy Server auf einem einzelnen Computer ausgeführt werden (wobei alle Instanzen demselben Directory Proxy Server-Image entsprechen), müssen bei der Aktualisierung des Images von Directory Proxy Server neue Directory Proxy Server-Instanzen erstellt werden.
- In Release 4-Bereitstellungsarchitekturen, die Directory Proxy Server enthalten, wurde ein Administration Server für die Konfiguration und Verwaltung von Directory Proxy Server-Instanzen verwendet. In Release 5 beinhaltet die Aktualisierung von Directory Proxy Server möglicherweise den Einsatz des Directory Service Control Center für die Konfiguration und Verwaltung von Directory Proxy Server-Instanzen.

Aktualisierungsverfahren

Das im Folgenden beschriebene Verfahren ist für Directory Proxy Server-Instanzen anzuwenden, die lokal auf dem Computer ausgeführt werden, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

su -

2. Beenden Sie alle Java ES-Komponenten, die von den zu aktualisierenden Directory Proxy Server-Instanzen abhängig sind. Dieser Schritt hängt möglicherweise davon ab, wie Directory Proxy Server innerhalb Ihrer Bereitstellungsarchitektur repliziert wird.

Weitere Informationen zum Beenden von Java ES-Komponenten finden Sie im Administrationshandbuch zur jeweiligen Komponente.

3. Installieren Sie Release 5 Directory Proxy Server neu.

Führen Sie die folgenden Schritte aus:

- a. Starten Sie das Java ES-Installationsprogramm.

```
cd Java ES Release 5-Bereitstellung/os_arch  
./installer
```

wobei *os_arch* der Plattform entspricht, wie z. B. *Solaris_sparc*.
(Verwenden Sie die Option `installer -nodisplay` für die
Befehlszeilenschnittstelle.)

Nach der Willkommensseite sowie der Lizenzvereinbarung wird eine Seite
für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten
erkannt werden, die direkt vom Java ES-Installationsprogramm
aktualisiert werden können, wird der Status als „aktualisierbar“
angezeigt.)

- b. Wählen Sie die Directory Proxy Server-Subkomponente der Directory
Server Enterprise Edition.

Sie müssen ebenfalls die gewünschten administrativen Subkomponenten
installieren (Directory Service Control Panel oder
Befehlszeilenprogramme).

- c. Geben Sie einen Installationspfad an, der sich vom Installationspfad des
vorhandenen Release 4 Directory Proxy Server unterscheidet.

- d. Wählen Sie „Jetzt konfigurieren“ oder „Später konfigurieren“.

Es ist unerheblich, ob Sie die Konfiguration zu diesem Zeitpunkt oder
später durchführen, da eigentlich keine Konfiguration für Directory Proxy
Server erforderlich ist. Wenn Sie jedoch die Konfiguration zu diesem
Zeitpunkt durchführen möchten, werden Sie gefragt, ob Sie eine neue
Instanz erstellen möchten. (Sobald die Komponente installiert wurde,
können Sie eine beliebige Anzahl Directory Proxy Server-Instanzen
erstellen.)

- e. Falls erforderlich, wählen Sie die Option zur Installation von lokalisierten
Paketen.

- f. Bestätigen Sie Ihre Auswahl für die Installation.

Directory Proxy Server-Pakete werden installiert und eine
Installationszusammenfassung wird angezeigt.

- g. Beenden Sie das Java ES-Installationsprogramm.

Wenn Sie keine neue Instanz erstellt haben, fahren Sie fort mit [Schritt 4](#),
anderenfalls fahren Sie fort mit [Schritt 5](#).

4. Erstellen Sie eine Directory Proxy Server-Instanz.

DirServer-base/dps6/bin/dpadm create instancePath

wobei *instancePath* der vollständige Pfad zur Directory Proxy Server-Instanz ist.

Informationen zum Erstellen von Directory Proxy Server-Instanzen finden Sie im *Directory Server Enterprise Edition 6 Administration Guide*, <http://docs.sun.com/doc/819-0995>.

5. Falls erforderlich verknüpfen Sie Release 4-Konfigurationsattribute mit den Release 5 Directory Proxy Server-Eigenschaften.

Details zur Vorgehensweise bei der Verknüpfung finden Sie im *Directory Server Enterprise Edition 6 Migration Guide*, <http://docs.sun.com/doc/819-0994>.

Überprüfen der Aktualisierung

Um zu überprüfen, ob die Aktualisierung von Directory Proxy Server erfolgreich war, gehen Sie wie folgt vor:

1. Starten Sie die Directory Proxy Server-Instanz.

DirServer-base/dps6/bin/dpadm start instancePath

2. Suchen Sie die Directory Proxy Server-Version.

DirServer-base/dps6/bin/dpadm --version

Die Ausgabewerte werden in [Tabelle 6-4 auf Seite 135](#) dargestellt.

Aufgaben nach der Aktualisierung

Alle Java ES-Komponenten, die von Directory Proxy Server abhängig sind, müssen neu konfiguriert werden, sodass Sie auf die neuen Directory Proxy Server-Instanzen verweisen.

Des Weiteren muss gewährleistet werden, dass LDAP-Steuerungen durch den Proxy gelassen werden, um das Standardverhalten vorheriger Versionen wiederherzustellen. Sie aktivieren diese Steuerungen, indem Sie die Eigenschaft `allowed-ldap-controls` wie folgt einstellen:

```
cd DirServer-base/dps6/bin
./dpconf set-server-prop
allowed-ldap-controls:auth-request
allowed-ldap-controls:chaining-loop-detection
allowed-ldap-controls:manage-dsa
```

```
allowed-ldap-controls:persistent-search  
allowed-ldap-controls:proxy-auth-v1  
allowed-ldap-controls:proxy-auth-v2  
allowed-ldap-controls:real-attributes-only  
allowed-ldap-controls:server-side-sorting
```

Aufheben der Aktualisierung

Das Zurücksetzen der Release 5-Aktualisierung erfolgt durch das Zurückkehren zur vorherigen Version, die bei der Aktualisierung auf Release 5 unverändert beibehalten wurde.

Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen wird Directory Proxy Server auf mehreren Computersystemen bereitgestellt, um die Skalierbarkeit zu gewährleisten und die Verfügbarkeit zu verbessern. Möglicherweise führen Sie beispielsweise Directory Proxy Server-Komponenten auf mehreren Computern zusammen mit einem Lastenausgleichsprogramm aus, um die Last zu verteilen.

Für Directory Proxy Server-Instanzen mit Lastenausgleich können Sie kein sogenanntes Rolling Upgrade durchführen. Das Lastenausgleichsprogramm muss beendet und neu konfiguriert werden, um auf die Release 5-Instanzen zugreifen zu können. Unter „[Aktualisierung der Release 4-Version von Directory Proxy Server](#)“, [auf Seite 135](#) wird beschrieben, wie Sie die Aktualisierung der einzelnen Instanzen durchführen.

Aktualisieren von Directory Proxy Server von Java ES Release 3

Die Vorgehensweise für die Aktualisierung von Java ES 2005Q1 (Release 3) Directory Proxy Server auf Release 5 ist mit der Aktualisierung von Release 4 Directory Proxy Server auf Release 5 identisch.

Um die Release 3-Version von Directory Proxy Server auf Release 4 zu aktualisieren, folgen Sie den Anweisungen unter „[Aktualisieren von Directory Proxy Server von Java ES Release 4](#)“, auf Seite 134. Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 3.

Aktualisieren der Directory Proxy Server Release 2-Version Java ES

Das Verfahren für die Aktualisierung von Java ES 2004Q2 (Release 2) Directory Proxy Server auf Release 5 ist mit der Aktualisierung von Directory Proxy Server Release 4 auf Release 5 identisch. Eine Ausnahme besteht jedoch bei den Aufgaben, die vor der Aktualisierung durchgeführt werden müssen. Hier sollte eine Synchronisierung aller gemeinsam genutzter Komponenten auf Release 5 (siehe [Tabelle 1-7 auf Seite 51](#)) und sämtlicher lokal vorhandener Produktkomponenten, von denen Directory Proxy Server abhängt, durchgeführt werden.

Anleitungen für die Synchronisierung von gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie in [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#).

Um die Release 2-Version von Directory Proxy Server auf Release 5 zu aktualisieren, folgen Sie den Anweisungen unter [„Aktualisieren von Directory Proxy Server von Java ES Release 4,“ auf Seite 134](#). Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 2.

Webserver

In diesem Kapitel wird die Aktualisierung von Webserver auf Java ES 5 (Release 5) beschrieben: Sun Java System Webserver 7.0.

Das Kapitel enthält einen Überblick über die Aspekte der verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Webserver“ auf Seite 144
- „Aktualisieren von Webserver von Java ES Release 4“ auf Seite 148
- „Aktualisieren von Webserver von Java ES Release 3“ auf Seite 169
- „Aktualisieren von Webserver von Java ES Release 2“ auf Seite 170

HINWEIS Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf Verzeichnispfade, die im Folgenden als *WebServer6-base* (Webserver 6.x) und *WebServer7-base* and *WebServer7Config-base* (Webserver 7.0) angegeben werden. Wenn Webserver erstmalig installiert wurde, wurden diese Pfade mindestens teilweise als Installationsverzeichnis angegeben. Wenn nicht, wurde vom Java ES-Installationsprogramm ein Standardwert zugewiesen.

Die Standardwerte für diese Verzeichnispfade sind in der folgenden Tabelle aufgelistet.

Tabelle 7-1 Webserver Verzeichnispfade

Variable des Pfadnamens	Solaris OS	Linux OS
<i>WebServer6-base</i>	/opt/SUNWwbsvr	/opt/sun/webserver
<i>WebServer7-base</i>	/opt/SUNWwbsvr7	/opt/sun/webserver7
<i>WebServer7Config-base</i>	/var/opt/SUNWwbsvr7	/var/opt/sun/webserver7

Überblick über Aktualisierungen von Webserver

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Webserver auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5 Webserver](#)
- [Wegweiser für die Aktualisierung von Webserver](#)
- [Webserver-Daten](#)
- [Vorgehensweise zur Aktualisierung von Webserver](#)

Über Java ES Release 5 Webserver

Java ES Release 5 Webserver stellt im Gegensatz zu Release 4 ein größeres Release mit einer Reihe neuer Funktionen und Schnittstellenverbesserungen dar.

Webserver Release 5 verfügt über eine neue Administrationsinfrastruktur mit neuen Administrationstools. Die Administrationsinfrastruktur umfasst eine Administrationsserver-Instanz, die als Host für Konfigurationsinformationen einer beliebigen Anzahl an Webserver-Instanzen dient. Über eine neue Befehlszeilenschnittstelle (wadm) und eine neue grafische Benutzeroberfläche werden Webserver-Instanzen entweder lokal auf dem Computer oder auf Remote-Computern erstellt, konfiguriert und verwaltet. Für die neuen Administrationstools sind ein Benutzername und ein Passwort des Administrators erforderlich.

Weitere Informationen zur neuen Administrationsinfrastruktur finden Sie im *Webserver 7.0 Administrator's Guide*, <http://docs.sun.com/doc/819-2629>.

Diese Änderungen an der Administrationsschnittstelle von Webserver haben deutliche Auswirkungen auf eine Aktualisierung.

Wegweiser für die Aktualisierung von Webserver

Tabelle 7-2 zeigt die unterstützten Wege für die Aktualisierung von Webserver auf Java ES Release 5. Die Tabelle gilt sowohl für das Solaris- als auch für das Linux-Betriebssystem.

Tabelle 7-2 Wege für die Aktualisierung auf Java ES 5 (Release 5): Webserver 7.0

Java ES Release	Webserver Version	Allgemeiner Ansatz	Neukonfiguration erforderlich
Release 4	Sun Java System Webserver 6.1 SP5 2005Q4	Direkte Aktualisierung: Neuinstallation gefolgt von einer Datenmigration	Migration der Instanzkonfiguration auf eine neue Instanz.
Release 3	Sun Java System Webserver 6 2005Q1 Update 1 SP 4	Direkte Aktualisierung: Neuinstallation gefolgt von einer Datenmigration	Migration der Instanzkonfiguration auf eine neue Instanz.
Release 2	Sun Java System Webserver 6 2004Q2 Update 1 SP 2 Plattform und Enterprise Edition	Direkte Aktualisierung: Neuinstallation gefolgt von einer Datenmigration	Migration der Instanzkonfiguration auf eine neue Instanz.
Release 1	Sun ONE Webserver 6.1 (2003Q4)	Direkte Aktualisierung nicht zertifiziert. Kann jedoch durch eine Neuinstallation gefolgt von einer Datenmigration erfolgen.	Migration der Instanzkonfiguration auf eine neue Instanz.
Versionen vor Java ES		Keine direkte Aktualisierung.	

Webserver-Daten

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Webserver-Software betroffen sein können.

Tabelle 7-3 Verwendung der Webserver-Daten

Datentyp	Standort	Verwendung
Konfigurationsdaten	Webserver 6.x (Java ES Release 2, 3 und 4): <i>WebServer6-base/https-instanceName/config/</i> Webserver 7.0 (Java ES Release 5) <i>Instanzkonfiguration</i> <i>WebServer7Config-base/https-configName/config¹/</i> Zentraler Konfigurationsspeicherplatz Zugriff über die Webserver Console und über die Befehlszeilenschnittstelle wadm.	Konfiguration der Webserver-Instanzen

1. Beachten Sie, dass sich der Pfad *WebServer7Config-base* wesentlich vom Pfad *WebServer6-base* unterscheidet.

Vorgehensweise zur Aktualisierung von Webserver

Ihre Vorgehensweise bei der Aktualisierung von Webserver hängt grundsätzlich von den zahlreichen in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) erläuterten Aspekten ab: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

Dieser Abschnitt konzentriert diese grundsätzliche Erläuterung auf Webserver, indem Probleme dargestellt werden, die möglicherweise Ihren Aktualisierungsplan für Webserver beeinflussen.

Kompatibilität

Java ES Release 5 Webserver führt keine Änderungen für öffentliche Schnittstellen ein und ist somit rückwärts kompatibel mit früheren Versionen. Die neuen Administrationsschnittstellen sind jedoch nicht rückwärts kompatibel mit früheren Administrationsschnittstellen. Dies hat einen Einfluss auf die Aktualisierung und die erneute Bereitstellung von Webanwendungen (beispielsweise Java ES-Komponenten).

Insbesondere Webserver Release 5 verwendet verschiedene Standardwerte für Instanzverzeichnisse und virtuelle Servernamen, wie in der folgenden Tabelle dargestellt.

Tabelle 7-4 Webserver-Standardnamen

Element	Java ES Release 2, 3 und 4 Webserver 6.x-Standard	Java ES Release 5 Webserver 7.0-Standard
Konfigurationsname		<i>hostName.domainName</i>
Instanzverzeichnispfad	<i>WebServer6-base/ https-hostName.domainName</i>	<i>WebServer7Config-base https-hostName.domainName</i>
Virtueller Servername	<i>https-hostName.domainName</i>	<i>hostName.domainName</i>

Webserver-Abhängigkeiten

Für Webserver bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Webserver ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)). Die Aktualisierung von Webserver hängt möglicherweise von den aktualisierten Versionen dieser gemeinsam genutzten Komponenten ab.
- **Directory Server.** Für Webserver besteht eine optionale Abhängigkeit zu Directory Server für die Authentifizierung auf LDAP-Basis.
- **Web Proxy Server.** Für Webserver besteht eine Abhängigkeit zu Web Proxy Server für die Bereitstellung von verbesserten Sicherheitsfunktionen und Leistungen für HTTP-Anfragen.

Aktualisieren von Webserver von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von Webserver von Java ES 2005Q4 (Release 4) auf Java ES 2005Q5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 4-Version von Webserver](#)

Einführung

Berücksichtigen Sie bei der Aktualisierung von Webserver von Java ES Release 4 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch eine Neuinstallation von Webserver Release 5, eine Migration der Konfigurationsinformationen der Release 4 Webserver-Instanz auf eine Release 5-Konfiguration und ein anschließendes Erstellen einer Release 5 Webserver-Instanz, die der Release 4-Instanz entspricht.
- **Aktualisierungsabhängigkeiten.** Webserver ist von einer Reihe gemeinsam genutzter Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)), die alle automatisch vom Java ES -Installationsprogramm auf Release 5 aktualisiert werden, wenn Sie eine Aktualisierung von Webserver durchführen. Doch zwingende Aktualisierungsabhängigkeiten für Webserver bestehen nur zu gemeinsam genutzten NSS- und NSPR-Komponenten.
- **Rückwärtskompatibilität.** Die Administrationsschnittstellen von Webserver Release 5 sind nicht rückwärts kompatibel zur Release 4-Version.
- **Aufheben der Aktualisierung.** Das Zurücksetzen der Aktualisierung auf Release 5 erfolgt durch das Zurückkehren zur Release 4-Installation, die unverändert beibehalten wurde.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Webserver ist für das Solaris- und Linux-Betriebssystem identisch.

Aktualisierung der Release 4-Version von Webserver

In diesem Abschnitt wird die Aktualisierung von Webserver von Java ES Release 4 auf Java ES Release 5 unter Solaris und Linux beschrieben. Plattformspezifische Vorgänge sind durch die Angabe des jeweiligen Betriebssystems, auf das sich der Vorgang bezieht, gekennzeichnet. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren von Release 4 von Webserver](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung der Webserver-Software beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Webserver-Aktualisierungsabhängigkeiten](#)
- [Webserver-Daten sichern](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

Aktuelle Versionsinformationen überprüfen

Sie können die aktuelle Webserver-Version überprüfen, indem Sie den Webserver-Instanzenserver mit der Option `-version` ausführen.

`WebServer6-base/https-hostName.domainName/start -version`

Tabelle 7-5 Webserver-Ausgaben der Versionsüberprüfung

Java ES Release	Webserver-Versionsnummer
Release 2	6.1SP2
Release 3	6.1SP4
Release 4	6.1SP5
Release 5	7.0

Webserver-Aktualisierungsabhängigkeiten

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Alle gemeinsam genutzten Komponenten, die von Webserver benötigt werden (siehe [Tabelle 1-7 auf Seite 51](#)), werden jedoch automatisch vom Java ES-Installationsprogramm aktualisiert, wenn Sie eine Aktualisierung von Webserver auf Release 5 durchführen.

Webserver-Daten sichern

Bei der Webserver-Aktualisierung von Release 4 auf Release 5 werden keine bestehenden Konfigurationsdaten geändert. Eine Sicherung der aktuellen Daten ist daher nicht erforderlich.

Erforderliche Konfigurationsinformationen und Passwörter abrufen

Sie müssen als Superuser angemeldet sein, um die Aktualisierung durchführen zu können. Zudem muss das Benutzerkonto, über das die Migration erfolgt, über die entsprechenden Berechtigungen verfügen, um auf die bestehenden Webserver-Installationsverzeichnisse zuzugreifen.

Aktualisieren von Release 4 von Webserver

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Webserver haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

Zu berücksichtigende Aspekte bei der Aktualisierung

Bei der Aktualisierung der Webserver-Software auf Java ES Release 5 müssen folgende Aspekte berücksichtigt werden:

- **„Jetzt konfigurieren“ oder „Später konfigurieren“.** Wenn Sie eine Aktualisierung durchführen, können Sie angeben, ob Sie Webserver Release 5 über die Option „Jetzt konfigurieren“ oder „Später konfigurieren“ installieren möchten:
 - Bei Auswahl der Option „Jetzt konfigurieren“ richtet das Installationsprogramm einen Administration Server oder Administrationsknoten ein und erstellt eine Standardkonfiguration und eine entsprechende Webserver-Instanz. Diese Vorgehensweise eignet sich bei der Installation auf einem einzelnen Computer, wobei der Standardkonfigurationsname jedoch möglicherweise die Migration von bestehenden Instanzkonfigurationen während des Aktualisierungsvorgangs beeinflusst.

- Bei Auswahl der Option „Später konfigurieren“ führt das Installationsprogramm keine Konfiguration durch: Sie müssen das Skript `configureServer` manuell ausführen, nachdem Sie die Eigenschaftswerte in einer Eingabedatei bereitgestellt haben. Diese Vorgehensweise eignet sich für eine automatisierte Installation auf mehreren Computern über entsprechende Skripte für eine automatische Installation. Sie können die Konfigurationsnamen auch vollständig steuern und so Konflikte bei der Migration von bestehenden Instanzkonfigurationen während des Aktualisierungsvorgangs vermeiden.
- **Migration einer standardmäßigen Release 4-Instanzkonfiguration.** Beim Durchführen einer Aktualisierung migrieren Sie die Konfigurationsdaten für jede Release 4 Webserver-Instanz auf einen zentralen Konfigurationsspeicherplatz, der vom Webserver Administration Server verwaltet wird. Die Migration wird durchgeführt, indem Sie den Befehl `wadm migrate-server` oder die Release 5 Administration Console verwenden.

Wenn es sich bei einer migrierten Instanz um eine standardmäßige Release 4 Webserver-Instanz (6.x) handelt, verfügt sie über denselben Namen (`hostName.domainName`) wie die standardmäßige Release 5 Webserver-Konfiguration (7.0), die automatisch über die Option „Jetzt konfigurieren“ erstellt wird.

Es gibt drei Ansätze für die Durchführung der Migration einer standardmäßigen Release 4-Instanzkonfiguration auf Release 5. Bei jedem Ansatz wird ein anderer Konfigurationsname erstellt.

Der von Ihnen ausgewählte Ansatz kann einen Einfluss auf später erfolgende Aktualisierungen bereitgestellter Webanwendungen haben. So ist es beispielsweise bei einer Aktualisierung von bereitgestellten Java ES-Komponenten (wie z. B. Access Manager und Portal Server) sowie Sun Java Communications Suite-Komponenten (wie z. B. Communications Express, Instant Messaging und Delegierter Administrator) in der Regel erforderlich, dass die Person, die die Aktualisierung durchführt, den Namen der Release 5-Konfiguration kennt, auf die die Release 4-Instanzkonfiguration migriert wurde.

Im Folgenden werden die drei verschiedenen Ansätze beschrieben:

- Geben Sie einen *neuen* Konfigurationsnamen an, der sich vom Standardnamen unterscheidet, wie z. B. "JavaESapps". Über den Befehl `migrate-server` wird dann eine neue Konfiguration mit dem Namen JavaESapps erstellt.

Anschließend aktualisierte Webanwendungen müssen für die Konfiguration JavaESapps erneut bereitgestellt werden.

- Geben Sie keinen neuen Konfigurationsnamen an, sondern löschen Sie die neue standardmäßige Release 5-Instanz und -Konfiguration (*hostName.domainName*), bevor Sie den Befehl `migrate-server` ausführen. Über den Befehl `migrate-server` wird dann eine neue Konfiguration mit dem Standardnamen (*hostName.domainName*) erstellt. Die folgende Reihenfolge wird dabei eingehalten (weitere Informationen unter `wadm help`):

```
wadm delete-instance
wadm delete-config
wadm migrate-server
wadm create-instance
```

Anschließend aktualisierte Webanwendungen müssen für die Konfiguration *hostName.domainName* erneut bereitgestellt werden, die mit dem standardmäßigen Release 4-Instanznamen übereinstimmt.

- Geben Sie keinen neuen Konfigurationsnamen an und löschen Sie die neue standardmäßige Release 5-Konfiguration nicht. Über den Befehl `migrate-server` wird dann eine neue Konfiguration mit dem folgenden Namen erstellt: *hostName.domainName-1*.

Anschließend aktualisierte Webanwendungen müssen für die Konfiguration *hostName.domainName-1* erneut bereitgestellt werden.

Bei allen drei Ansätzen für die Migration der Release 4-Instanzkonfigurationen ist es wichtig, dass Sie die Person, die anschließende Aktualisierungen von bereitgestellten Webanwendungen ausführt, über den von Ihnen gewählten Ansatz informieren.

- **Migration von Konfigurationsdaten.** Bei der Migration von Release 4-Instanzkonfigurationen werden die folgenden Informationen automatisch migriert:
 - Alle Konfigurationsinformationen im Release 4 Webserver-Instanzverzeichnis: *WebServer6-base/https-instanceName/config*. Dies beinhaltet auch Konfigurationsinformationen für alle Webanwendungen, die in der Release 4-Instanz bereitgestellt werden (z. B. Java ES-Komponenten wie Access Manager und Portal Server).
 - acl-Informationen aus *WebServer6-base/httpacl*
 - auth-db-Informationen aus *WebServer6-base/userdb*
 - Planungsinformationen aus *WebServer6-base/https-admserv/config*
 - Zertifikatsinformationen aus *WebServer6-base/alias*

- Informationen zur Suchsammlung und zu Indexdateien, die Sie beim Durchführen der Migration angegeben haben.

Die automatische Migration umfasst *nicht* die folgenden Daten:

- docroot-Inhalte. Die neue Konfiguration zeigt dagegen auf das alte docroot-Verzeichnis und eine Protokollmeldung wird im Migrationsprotokoll aufgezeichnet.
- Webdav-Daten. Informationen zur Webdav-Sammlung werden migriert.
- NSAPI-Plug-Ins von Drittanbietern werden nicht migriert. Stattdessen zeigen sie auf die Release 4-Datei und eine Protokollmeldung wird im Migrationsprotokoll aufgezeichnet.
- Protokolldateien
- Änderungen an der docroot-Suchsammlung.
- Befehlszeilenskripte (startsvr, startsvr.bat, stopsvr, stopsvr.bat, restart, reconfig, reconfig.bat).

Weitere Informationen zur Datenmigration finden Sie im *Webserver 7.0 Installation and Migration Guide*, <http://docs.sun.com/doc/819-2625>.

- **Erstellen von Release 5 Webserver-Instanzen.** Nach der Migration müssen Sie eine Release 5 Webserver-Instanz erstellen, die der migrierten Release 4-Instanz entspricht. Dieser Vorgang wird nicht automatisch ausgeführt.

Aktualisierungsverfahren

Das folgende Verfahren ist für alle Webserver-Instanzen anzuwenden, die demselben installierten Webserver-Image auf dem Computer entsprechen, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

su -

2. Halten Sie alle derzeit ausgeführten Instanzen von Webserver und Administration Server an.

WebServer6-base/https-instanceName/stop
WebServer6-base/https-admserv/stop

3. Führen Sie eine Neuinstallation von Webserver Release 5 aus.

Führen Sie die folgenden Schritte aus:

- a. Starten Sie das Java ES-Installationsprogramm.

```
cd Java ES Release 5 distribution/os_arch  
./installer
```

wobei *os_arch* der Plattform entspricht, wie z. B. *Solaris_sparc*.
(Verwenden Sie die Option `installer -nodisplay` für die
Befehlszeilenschnittstelle.)

Nach der Willkommensseite sowie der Lizenzvereinbarung wird eine Seite
für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten
erkannt werden, die direkt vom Java ES-Installationsprogramm
aktualisiert werden können, wird der Status als „aktualisierbar“
angezeigt.)

- b. Wählen Sie auf der Seite für die Komponentenauswahl Webserver.
- c. Geben Sie einen Installationspfad an, der sich vom Installationspfad von
Webserver Release 4 unterscheidet.
- d. Wählen Sie „Jetzt konfigurieren“ oder „Später konfigurieren“.
- Wenn Sie die Option „Jetzt konfigurieren“ wählen, fahren Sie mit
[Schritt e](#) fort.
 - Wenn Sie die Option „Später konfigurieren“ wählen, fahren Sie mit
[Schritt f](#) fort.
- e. Wenn Sie die Option „Jetzt konfigurieren“ wählen, bietet das
Java ES-Installationsprogramm zwei Möglichkeiten an:
- Administrationsinstanz als Administration Server konfigurieren
Wählen Sie diese Option auf dem Computer, der als Host für den
Administration Server dient und neben anderen administrativen
Aufgaben auch für die Migration von Release 4-Instanzen auf Release
5 erforderlich ist.
 - Administrationsinstanz als Administrationsknoten konfigurieren
Wählen Sie diese Option auf einem Computer, der als Host für eine
Webserver-Instanz dient und nicht mit dem Administration Server
identisch ist. Die Administrationsinstanz wird als Knotenagent
konfiguriert, der mit dem Administration Server interagiert.
- i. Geben Sie die erforderlichen Konfigurationswerte an.
- Sie müssen den Host-Namen, den HTTP-Anschluss sowie den
Benutzernamen und das Passwort des Administrators angeben.
- ii. Bestätigen Sie Ihre Auswahl für die Installation.

Die Webserver-Pakete werden installiert und eine Installationszusammenfassung wird angezeigt.

Das Java ES-Installationsprogramm erstellt eine Standardkonfiguration mit dem Namen *hostName.domainName* sowie eine entsprechende Webserver-Instanz.

III. Schließen Sie das Java ES-Installationsprogramm und fahren Sie mit [Schritt 4 auf Seite 157](#) fort.

f. Wenn Sie die Option „Später konfigurieren“ wählen, erstellt das Java ES-Installationsprogramm das Skript `configureServer`, das Sie in [Schritt IV auf Seite 157](#) ausführen.

I. Bestätigen Sie Ihre Auswahl für die Installation.

Die Webserver-Pakete werden installiert und eine Installationszusammenfassung wird angezeigt.

II. Beenden Sie das Java ES-Installationsprogramm.

III. Legen Sie die Werte in der Datei `WebServer7-base/setup/WSInstall.properties` fest.

Geben Sie die Werte für alle erforderlichen (nicht optionalen) Eigenschaften in der folgenden Tabelle an.

Tabelle 7-6 WSInstall.properties Values

Eigenschaft	Beschreibung
WS_DOCROOT	(Optional) Dokumentspeicherort, der als Host für Webinhaltsdateien dienen kann.
WS_SERVER_NAME	Hostname, der für HTTP-Anfragen verwendet werden kann.
WS_SERVER_USER	UNIX-Laufzeit-Benutzer. Gültige Werte sind root, ein beliebiger UNIX-Benutzer oder webservd (Standard).
WS_HTTP_PORT	Instanzanschluss, der für das Abhören von HTTP-Anfragen verwendet werden kann.
WS_ADMIN_SSL_PORT	Admin-SSL-Anschluss.
WS_ADMIN_HOST	Administrativer Hostname für administrative Serveraufgaben.
WS_CONFIG_NAME	Konfigurationsname für diesen Host. Dieser Wert kann mit dem Wert unter WS_SERVER_NAME identisch sein.

Tabelle 7-6 WSInstall.properties Values *(Fortsetzung)*

Eigenschaft	Beschreibung
WS_ADMIN_SERVER_USER	UNIX-Laufzeit-Benutzer des Admin-Servers. Gültige Werte: 'root' oder der gleiche Benutzer wie unter WS_SERVER_USER.
WS_ADMIN_LOGIN_USER	Benutzername des Administrators für die Anmeldung am Server.
WS_ADMIN_LOGIN_PASSWORD	Passwort des Administrators für die Anmeldung am Server.
WS_ADMIN_HTTP_PORT	(Optional) Administrativer Nicht-SSL-Anschluss. Standard: 8800
WS_START_ON_BOOT	(Optional) Funktion für einen Start nach Systemstart (true/false). Bei true können die Serverinstanz und der Admin-Server automatisch nach einem Systemstart starten. Standard: false
WS_64BIT_INSTALL	(Optional) Serverlaufzeit-Modus (true/false). Bei true wird der Server im 64-Bit-Modus konfiguriert. (Nur für Solaris). Bei false wird der Server im 32-Bit-Modus konfiguriert. (Nur für Solaris) Standard: false
WS_ADMIN_IS_SERVER_MODE	(Optional) Admin-Konfigurationsmodus. (true/false). Bei true wird der Server im Admin-Servermodus konfiguriert. Bei false wird der Server im Admin-Agentenmodus konfiguriert. Standard: true
WS_REGISTER_ADMIN_AGENT	(Optional) Remote-Agentenregistration. (true/false). Dies ist nur erforderlich, wenn WS_ADMIN_IS_SERVER_MODE auf „false“ gesetzt wurde. Bei true müssen Sie den Remote-Admin-Serverhost für die Registrierung bereitstellen. Standard: true
WS_AGENT_SSL_PORT	(Optional) Administrativer Agent-SSL-Anschluss. Dies ist nur erforderlich, wenn WS_ADMIN_IS_SERVER_MODE auf false gesetzt wurde.
WS_AGENT_HOST=	(Optional) Administrativer Agent-Hostname. Dies ist nur erforderlich, wenn WS_ADMIN_IS_SERVER_MODE auf false gesetzt wurde.

IV. Führen Sie das Skript configureServer aus.

```
WebServer7-base/setup/configureServer
-inputfile WebServer7-base/setup/WSInstall.properties
-logfile WebServer7-base/setup/WSInstall.log
-verbose
```

Das Skript configureServer erstellt eine Standardkonfiguration mit dem Namen *hostName.domainName* sowie eine entsprechende Webserver-Instanz.

4. Starten Sie den Dienst Webserver Administration Server.

```
WebServer7Config-base/admin-server/bin/startserv
```

5. Migrieren Sie die Release 4 Webserver-Instanzkonfigurationen auf Release 5-Konfigurationen.

Sie können entweder die Befehlszeile (wadm) oder die grafische Benutzeroberfläche der Administrationstools verwenden (melden Sie sich bei der Webserver Admin Server-GUI an). Die folgenden Schritte beziehen sich auf die Befehlszeilenschnittstelle wadm.

Beispiel: Migration einer Instanz mit dem Namen myinstance auf eine neue Konfiguration:

```
WebServer7-base/bin/wadm migrate-server --user=admin
--host=localhost --server-root=/opt/SUNWwbsvr
--instance=https-myinstance --config=newconfigname
```

Die vollständige Befehlssyntax lautet:

```
WebServer7-base/bin/wadm migrate-server
```

```
--user=admin-user [--password-file=admin-pswd-file] [--host=admin-host]
[--echo] [--rcfile=rcfile] [--no-prompt] [--verbose]
```

```
[--search-collection-copy-path=searchCollectionPath]
[--log-dir=directory] --serverroot=path
([--all] | [--instance=https-instanceName] [--config=newconfigName])
```

Der erste Block der oben angegebenen Befehlsoptionen gilt allgemein für alle wadm-Befehle und ist in [Tabelle 7-7](#) angegeben. Der zweite Block der Befehlsoptionen gilt speziell für den Befehl „migrate-server“ und ist in [Tabelle 7-8](#) angegeben.

Das Aufrufen von `wadm` mit nur dem ersten Block der Befehlsoptionen führt zur Befehlsshell `wadm`. Beim Aufrufen von Befehlen in dieser Shell müssen Sie die allgemeinen Optionen nicht erneut angeben.

Wenn Sie die vollständigen `wadm`-Befehle außerhalb der Shell aufrufen, müssen Sie zumindest die Optionen `--user` und `--host` angeben. (Wenn Sie die Option `--password-file` auslassen, werden Sie nach einem Passwort gefragt. Wenn Sie andere Optionen auslassen, werden Standardwerte verwendet.) Bei Befehlen, die Vorgänge in diesem Kapitel veranschaulichen, wurden jedoch die Optionen `--user` und `--host` nicht eingeschlossen, um die Vorgänge einfacher darzustellen.

Standardmäßig verwendet `wadm` das SSL-Protokoll auf Anschluss 8989.

Detaillierte Informationen zu den `wadm`-Befehlen und -Optionen finden Sie im *Webserver 7.0 CLI Reference Manual*, <http://docs.sun.com/doc/819-3283>.

Tabelle 7-7 `wadm` Allgemeine Befehlsoptionen

Option	Beschreibung
user (Benutzer)	Autorisierte administrative Webserver-Benutzer-ID.
password-file	Datei mit dem Passwort, das für die Autorisierung des administrativen Benutzers für den Administration Server erforderlich ist. Die Passwortdatei muss die Zeile <code>WADM_PASSWORD=password</code> enthalten. Ist diese Option im Befehl nicht angegeben, werden Sie nach einem Passwort gefragt.
host	Name des Computers, auf dem der Administration Server ausgeführt wird. Standard: <code>localhost</code> .
echo	Wenn diese Option auf <code>true</code> gesetzt ist, wird die Befehlszeile in der Standardausgabe angezeigt, bevor der Befehl ausgeführt wird. Standard: <code>false</code>
interactive	Wenn diese Option auf <code>true</code> gesetzt ist, müssen die erforderlichen Passwortoptionen angegeben werden. Standard: <code>true</code> .
rcfile	Startdatei, die für den Ladevorgang beim Starten von <code>wadm</code> verwendet wird. Standard: <code>~/wadmrc</code> .
no-prompt	Wenn diese Option auf <code>true</code> gesetzt ist, wird der Benutzer nie zur Eingabe von Informationen aufgefordert. Der Befehl gibt einen Fehler aus, sobald bestimmte Parameter fehlen. Der Benutzer wird nicht zur Eingabe von Informationen aufgefordert und auf eine Eingabe durch den Benutzer wird somit nicht gewartet. Sie können die Option auf <code>true</code> setzen, wenn Sie die <code>wadm</code> -Befehle mit einem Shell-Skript verwenden, damit der Vorgang immer abgebrochen und nicht auf eine Eingabe durch den Benutzer gewartet wird. Standard: <code>false</code> .

Tabelle 7-7 wadm Allgemeine Befehlsoptionen (Fortsetzung)

Option	Beschreibung
verbose	Wenn diese Option auf <code>true</code> gesetzt ist, wird eine ausführliche Liste angezeigt. Standard: <code>false</code> .

Tabelle 7-8 wadm migrate-server Befehlsoptionen und Operanden

Option/Operand	Beschreibung
search-collection-copy-path	Gibt den Pfad an, auf den die Indexdateien für die Suchsammlung beim Migrieren der Suchsammlungen kopiert werden. Die folgenden Migrationsszenarios sind möglich: Wenn sich der Pfad der Suchsammlung von Webserver 6.x außerhalb der Webserver 6.x-Instanz befindet, verweist der Pfad der migrierten Suchsammlung auf den Pfad der Suchsammlung von Webserver 6.x und diese Option wird ignoriert. Wenn sich der Pfad der Suchsammlung von Webserver 6.x innerhalb der Webserver 6.x-Instanz befindet und ein gültiger Pfad für diese Option angegeben ist, werden die Indexdateien der Suchsammlung in das folgende Verzeichnis kopiert: <i>searchCollectionPath/configName/virtualServerName/collectionName</i>. Wenn der angegebene Pfad nicht gültig ist, wird eine Fehlermeldung protokolliert. Wenn sich der Pfad der Suchsammlung von Webserver 6.x innerhalb der Webserver 6.x-Instanz befindet, aber kein gültiger Pfad für diese Option angegeben ist, werden die Indexdateien der Suchsammlung nicht kopiert: Eine Meldung wird in das Migrationsprotokoll aufgenommen und der Benutzer wird dazu aufgefordert, die Indexdateien der Suchsammlung manuell über den Befehl <code>wadm add-documents</code> zu kopieren. In diesem Fall lautet der Pfad für die migrierte Suchsammlung wie folgt: <i>WebServer7Config-base/https-configName/config/collections/virtualServerName/collectionName</i>.
log-dir	Der Speicherort des Migrationsprotokolls. Standard: <i>WebServer7Config-base/admin-serv/logs</i>
serverroot	Installationsverzeichnis (Speicherort) für Webserver 6.x: identisch mit <i>WebServer6-base</i>.
all	Wenn diese Option auf <code>true</code> gesetzt ist, werden alle Webserver 6.x-Instanzkonfigurationen auf Webserver 7.0-Konfigurationen mit dem gleichen Namen wie die Instanzen migriert. Wenn eine Konfiguration mit diesem Namen bereits vorhanden ist, wird <i>instanceName-1</i> für den Konfigurationsnamen verwendet. Standard: <code>false</code>.

Tabelle 7-8 wadm migrate-server Befehlsoptionen und Operanden (Fortsetzung)

Option/Operand	Beschreibung
instance	Wenn Instanzkonfigurationen individuell migriert werden sollen (all=false), wird der Name der zu migrierenden Webserver 6.x-Instanzkonfiguration angegeben (Format: https-instanceName). Der Standardname der Webserver 6.x-Instanz lautet hostName.domainName.
config	Name der Konfiguration, auf die die angegebene Webserver 6.x-Instanzkonfiguration migriert werden soll. Standardmäßig wird der Name instanceName der Webserver 6.x-Instanzkonfiguration verwendet. Wenn jedoch eine Konfiguration mit diesem Namen bereits vorhanden ist, wird dem Namen eine Ganzzahl angehängt. Hierbei handelt es sich um ein wahrscheinliches Szenario, wenn die standardmäßige Webserver 6.x-Instanzkonfiguration migriert wird.

Berücksichtigen Sie bei der Verwendung des Befehls migrate-server die folgenden Aspekte:

- Wenn Sie mehrere Release 4-Instanzkonfigurationen migrieren möchten, können Sie den Befehl migrate-server wiederholt mit verschiedenen --instance-Werten und entsprechenden --config-Argumenten verwenden. Sie können jedoch auch die Option --all verwenden und so alle Instanzkonfigurationen gleichzeitig zu migrieren.
- Bei jedem Aufruf des Befehls „migrate-server“ wird bei der Migration eine Protokolldatei in einem Verzeichnis erstellt, das durch die Option --log-dir festgelegt wurde (oder im Standardverzeichnis WebServer7Config-base/admin-server/logs). Der Name der Protokolldatei lautet wie folgt:

MIGRATION_yyyymmddhhmmss.log

Wenn Sie die Option --all auswählen, werden in der Protokolldatei die Migrationsinformationen für alle migrierten Instanzen gespeichert.

- Bei Daten, die nicht über den Befehl migrate-server migriert werden (siehe „Zu berücksichtigende Aspekte bei der Aktualisierung“ auf Seite 150), müssen Sie die Migration manuell durchführen (siehe „Aufgaben nach der Aktualisierung“ auf Seite 164).

6. Erstellen Sie Release 5 Webserver-Instanzen.

Sie müssen eine neue Release 5-Instanz für jede Release 4-Instanzkonfiguration erstellen, die Sie in [Schritt 5](#) migriert haben. (Wenn Sie eine Migration auf die Standardkonfiguration durchgeführt haben, ist eine entsprechende Standardinstanz bereits vorhanden und Sie können mit [Schritt c](#) fortfahren.)

- a. Überprüfen Sie vor dem Erstellen einer neuen Instanz das Migrationsprotokoll und beheben Sie mögliche Probleme in der migrierten Konfiguration.
- b. Führen Sie den Befehl `create-instance` aus.

```
webServer7-base/bin/wadm create-instance
--config=configName nodehost1 [nodehost2 ...nodehostN]
```

Allgemeine Befehlsoptionen finden Sie in [Tabelle 7-7 auf Seite 158](#).

Optionen für den Befehl `create-instance` sind in der folgenden Tabelle aufgeführt.

Tabelle 7-9 wadm create-instance Befehlsoptionen und Operanden

Option/Operand	Beschreibung
config	Der Name der Release 5-Konfiguration, auf den die Instanz verweisen soll.
nodehost	Der Name des Computers, auf dem die Instanz erstellt wird. Sie können mehrere Computer in einer durch Leerzeichen getrennten Liste angeben (<i>hostName.domainName</i>) und so mehrere identische Instanzen erstellen.

Der Befehl `create-instance` erstellt ein Instanzverzeichnis unter *WebServer7Config-base/https-configName* auf den angegebenen Knoten und stellt die Konfiguration den entsprechenden Instanzverzeichnissen bereit.

- c. Wenn die Zielinstanz bereits als Standardinstanz vorhanden ist, stellen Sie einfach die entsprechende Konfiguration bereit. Sie müssen in diesem Fall keine Instanz erstellen.

WebServer7-base/bin/wadm `deploy-config`
`[--force] [--restart] [--no-reconfig]`
configName

Allgemeine Befehlsoptionen finden Sie in [Tabelle 7-7 auf Seite 158](#). Optionen für den Befehl `deploy-config` sind in der folgenden Tabelle aufgeführt.

Tabelle 7-10 wadm deploy-cofig Befehlsoptionen und Operanden

Option/Operand	Beschreibung
force	Wenn diese Option auf <code>true</code> gesetzt ist, wird das Überschreiben einer Instanzkonfiguration erzwungen, die seit der Bereitstellung der vorherigen Konfiguration manuell geändert wurde. Standard: <code>false</code>
restart	Wenn diese Option auf <code>true</code> gesetzt ist, werden aktuell ausgeführte Instanzen neu gestartet, um die Konfigurationseinstellungen der bereitgestellten Konfiguration zu übernehmen. Standard: <code>false</code>
no-reconfig	Wenn diese Option auf <code>true</code> gesetzt ist, übernehmen aktuell ausgeführte Instanzen die Konfigurationseinstellungen der bereitgestellten Konfiguration erst, wenn die Instanz neu gestartet wird. Standard: <code>false</code>

Tabelle 7-10 wadm deploy-cofig Befehlsoptionen und Operanden

Option/Operand	Beschreibung
configName	Der Name der Release 5-Konfiguration, die für eine Webserver-Instanz bereitgestellt wird, deren Instanzname mit dem Konfigurationsnamen übereinstimmt.

7. Starten Sie alle Release 5-Instanzen.

WebServer7Config-base/https-configName/bin/startserv

Das Skript *startserv* wird zusammen mit der Instanz erstellt. Wenn die Instanz problemlos gestartet wird, informiert Sie eine Meldung über den erfolgreichen Serverstart. Der Standard-URL für die Instanz wird angezeigt.

Überprüfen der Aktualisierung

Sie können die Aktualisierung von Webserver auf Release 5 überprüfen, indem Sie die folgenden Schritte ausführen:

- 1. Überprüfen Sie das neu erstellte Migrationsprotokoll auf Fehlermeldungen (ERROR).

Führen Sie gegebenenfalls die erforderlichen Änderungen durch (siehe [„Aufgaben nach der Aktualisierung“ auf Seite 164](#)).

- 2. Überprüfen Sie die Release 5 Webserver-Instanzen.

Rufen Sie über einen Webbrowser den folgenden URL auf und stellen Sie sicher, dass die Begrüßungsseite angezeigt wird:

http://hostName.domainName:port

Dabei entsprechen der voll qualifizierte Hostname und der Anschluss jeder Instanz. Sie können auch den folgenden URL in den Browser kopieren:

WebServer7Config-base/https-configName/bin/startserv

- 3. Führen Sie die Webserver-Instanz mit der Option *-version* aus:

WebServer7Config-base/https-configName/bin/startserv -version

Ausgabewerte finden Sie in [Tabelle 7-5 auf Seite 149](#).

Aufgaben nach der Aktualisierung

Die Hauptaufgaben nach der Aktualisierung beziehen sich auf die manuelle Migration bestimmter Release 4-Daten, sofern erforderlich. Dabei handelt es sich um Daten, die in der Regel einem oder mehreren virtuellen Servern zugeordnet sind, die für Release 4 konfiguriert wurden und in der Konfigurationsdatei `server.xml` angegeben sind.

Beachten Sie die für die folgenden Situationen erforderlichen Aufgaben nach der Aktualisierung:

- [Migrieren des docroot-Inhalts von Webserver 6.1](#)
- [Migrieren von Informationen zur Webdav-Sammlung](#)
- [Migrieren von Protokolldateien](#)
- [Migrieren von NSAPI-Plug-Ins von Drittanbietern](#)
- [Ändern des Dokument-Root der Suchsammlung](#)
- [Anpassen von Befehlszeilenskripten](#)

Migrieren des docroot-Inhalts von Webserver 6.1

1. Kopieren Sie den docroot-Inhalt von Webserver 6.1 an einen beliebigen Ort.
2. Aktualisieren Sie den neuen Dokument-Root-Pfad über den folgenden Befehl:

```
WebServer7-base/bin/wadm set-virtual-server-prop  
--config=configName --vs=virtualServerName  
document-root=new docroot path
```

Allgemeine Befehlsoptionen finden Sie in [Tabelle 7-7 auf Seite 158](#). Optionen für den Befehl `set-virtual-server-prop` sind in der folgenden Tabelle aufgeführt.

Tabelle 7-11 `wadm set-virtual-server-prop` Befehlsoptionen und Operanden

Option/Operand	Beschreibung
config	Der Name der Release 5-Konfiguration, für die der neue Dokument-Root-Pfad festgelegt wird.
vs	Der Name des virtuellen Servers, mit dem der migrierte Dokument-Root übereinstimmt.
document-root	Der Pfad zum neuen Dokument-Root-Verzeichnis.

3. Stellen Sie die Konfiguration für die relevanten Webserver-Instanzen erneut bereit.

```
WebServer7-base/bin/wadm deploy-config
[--force] [--restart] [--no-reconfig]
configName
```

Befehlsoptionen finden Sie in [Tabelle 7-10 auf Seite 162](#).

Migrieren von Informationen zur Webdav-Sammlung

Eine zusätzliche manuelle Migration ist nicht erforderlich. Eine Aktualisierung des docroot-Pfads ist ausreichend.

Migrieren von Protokolldateien

Kopieren Sie diese Dateien an einen beliebigen Speicherort, um sie zu sichern. (Andernfalls werden Sie beim Entfernen der Release 4-Installation auch entfernt).

Migrieren von NSAPI-Plug-Ins von Drittanbietern

1. Kopieren Sie die Bibliotheksdateien vom Release 4-Speicherort in das Verzeichnis *WebServer7-base/lib*.
2. Exportieren Sie die Konfigurationsdateien *magnus.conf* und *obj.conf* in ein temporäres Verzeichnis.

```
WebServer7-base/bin/wadm get-config-file --config=configName
magnus.conf > /tmp/magnus.conf
```

```
WebServer7-base/bin/wadm get-config-file --config=configName
obj.conf > /tmp/obj.conf
```

Allgemeine Befehlsoptionen finden Sie in [Tabelle 7-7 auf Seite 158](#).

3. Bearbeiten Sie die Dateien *magnus.conf* und „*obj.conf*“ wie in der Dokumentation zum NSAPI-Plug-In des Drittanbieters angegeben.
4. Importieren Sie die Konfigurationsdateien *magnus.conf* und *obj.conf* aus dem temporären Verzeichnis.

```
WebServer7-base/bin/wadm set-config-file --config=configName
--upload-file=/tmp/magnus.conf magnus.conf
```

```
WebServer7-base/bin/wadm set-config-file --config=configName
--upload-file=/tmp/obj.conf obj.conf
```

Allgemeine Befehlsoptionen finden Sie in [Tabelle 7-7 auf Seite 158](#).

- 5. Stellen Sie die bearbeitete Konfiguration für die relevanten Webserver-Instanzen erneut bereit.

```
WebServer7-base/bin/wadm deploy-config
[--force] [--restart] [--no-reconfig]
configName
```

Befehlsoptionen finden Sie in [Tabelle 7-10 auf Seite 162](#).

Ändern des Dokument-Root der Suchsammlung

Über den Befehl „migrate-server“ besteht die Option, die Informationen der Suchsammlung zu migrieren. Sie können jedoch den Dokument-Root der Suchsammlung wie folgt ändern:

- 1. Wenn sich der Dokument-Root für die Suchsammlung von dem in Release 4 verwendeten Dokument-Root unterscheidet, können Sie über den folgenden Befehl den Dokument-Root für die Suchsammlung festlegen:

```
WebServer7-base/bin/wadm set-search-collection-prop
--config=configName --vs=virtualServerName
--collection-name=searchCollectionName document-root=new docroot path for
the search collection
```

Allgemeine Befehlsoptionen finden Sie in [Tabelle 7-7 auf Seite 158](#). Optionen für den Befehl set-search-collection-prop sind in der folgenden Tabelle aufgeführt.

Tabelle 7-12 wadm set-search-collection-prop Befehlsoptionen und Operanden

Option/Operand	Beschreibung
config	Der Name der Release 5-Konfiguration, für die der Dokument-Root der Suchsammlung festgelegt wird.
vs	Der Name des virtuellen Servers, mit dem die Suchsammlung übereinstimmt.
collection-name	Der Name der Suchsammlung, für die ein neuer Dokument-Root-Pfad festgelegt wird.
document-root	Der Pfad auf das neue Dokument-Root-Verzeichnis für die Suchsammlung.

2. Stellen Sie die Konfiguration für die relevanten Webserver-Instanzen erneut bereit.

```
WebServer7-base/bin/wadm deploy-config
[--force] [--restart] [--no-reconfig]
configName
```

Befehlsoptionen finden Sie in [Tabelle 7-10 auf Seite 162](#).

Anpassen von Befehlszeilenskripten

Wurden Skripte wie z. B. `startsvr`, `startsvr.bat`, `stopsvr`, `stopsvr.bat`, `restart`, `reconfig` und `reconfig.bat` angepasst, müssen Sie die gleichen Änderungen an den Standardskripten von Release 5 vornehmen. Die Skripte befinden sich im folgenden Verzeichnis: `WebServer7-base/bin`.

Aufheben der Aktualisierung

Webserver Release 4 wurde bei der Neuinstallation von Release 5 und anschließenden Migrationen von Webserver-Instanzkonfigurationen unverändert beibehalten. Somit sind für das Aufheben der Aktualisierung von Webserver Release 5 die folgenden Schritte erforderlich, über die Sie zur Release 4-Version zurückkehren können.

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Halten Sie alle derzeit ausgeführten Webserver-Instanzen einzeln an.

```
WebServer7Config-base/https-configName/bin/stopserv
```

Wenn der Server ordnungsgemäß angehalten wurde, informiert Sie eine Meldung darüber, dass der Server heruntergefahren wurde.

3. Entfernen Sie die Release 5 Webserver-Installation.

Sie müssen alle Release 5-Instanzen und die migrierten Konfigurationen entfernen:

- a. Löschen Sie alle Release 5-Instanzen.

```
WebServer7-base/bin/wadm delete-instance --user ...
--config=configName hostName.domainName
```

- b. Löschen Sie alle Release 5-Konfigurationen.

```
WebServer7-base/bin/wadm delete-config --user ... configName
```

4. Starten Sie die Webserver-Instanzen neu, die bei der Aktualisierung von Webserver angehalten wurden (siehe „[Aktualisierungsverfahren](#)“ auf [Seite 153](#)).

Aktualisieren von Webserver von Java ES Release 3

Das Verfahren zur Aktualisierung von Java ES 2005Q1 (Release 3) Webserver auf Release 5 ist mit dem Verfahren zur Aktualisierung von Webserver Release 4 auf Release 5 identisch.

Um die Release 3-Version von Webserver auf Release 4 zu aktualisieren, folgen Sie den Anweisungen unter „[Aktualisieren von Webserver von Java ES Release 4](#)“ auf [Seite 148](#). Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 3.

Aktualisieren von Webserver von Java ES Release 2

Das Verfahren zur Aktualisierung von Java ES 2004Q2 (Release 2) Webserver auf Release 5 ist mit dem Verfahren zur Aktualisierung von Webserver Release 4 auf Release 5 identisch.

Um die Release 2-Version von Webserver auf Release 5 zu aktualisieren, folgen Sie den Anweisungen unter „[Aktualisieren von Webserver von Java ES Release 4](#)“ auf [Seite 148](#). Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 2.

Java DB

In diesem Kapitel wird die Aktualisierung von Java DB auf Java ES 5 (Release 5) beschrieben: Java DB 10.1.3.

Das Kapitel enthält einen Überblick über die Aspekte der verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Java DB“ auf Seite 172
- „Aktualisieren von Java DB von Java ES Release 4“ auf Seite 174

HINWEIS Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf einen Verzeichnispfad, der im Folgenden als *JavaDB-base* angegeben wird. Dieser Pfad wurde vom Java ES-Installationsprogramm bei der Installation von Java DB festgelegt.

Die Werte für diesen Verzeichnispfad sind in der folgenden Tabelle aufgelistet.

Tabelle 8-1 Java DB Verzeichnispfade

Variable des Pfadnamens	Solaris OS	Linux OS
<i>JavaDB-base</i>	/opt/SUNWjavadb	/opt/sun/javadb

Überblick über Aktualisierungen von Java DB

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Java DB auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5](#)
- [Java ES Wegweiser für die Aktualisierung auf Release 5](#)
- [Java DB-Daten](#)
- [Vorgehensweise zur Aktualisierung von Java DB](#)

Über Java ES Release 5

Java ES von Java DB Release 5 ist das erste Release, das als Java ES-Produktkomponente bereitgestellt wird. Java DB wurde zunächst als gemeinsam genutzte Komponente mit dem Namen DerbyDatabase veröffentlicht und ist in Java ES Release 4 enthalten.

Java DB Release 5 stellt im Gegensatz zu Release 4 ein kleineres Release dar. Es beinhaltet einige verbesserte Funktionen, aktualisierte Schnittstellen und ausgewählte Fehlerkorrekturen.

Java ES Wegweiser für die Aktualisierung auf Release 5

[Tabelle 8-2](#) zeigt die unterstützten Wege für die Aktualisierung von Java DB auf Java ES Release 5. Die Tabelle gilt sowohl für das Solaris- als auch für das Linux-Betriebssystem.

Tabelle 8-2 Wege für die Aktualisierung auf Java ES 5 (Release 5): Java DB 10.1.3

Java ES Release	Java DB Version	Allgemeiner Ansatz	Neukonfiguration erforderlich
Release 4	Derby Database 10.0.2	Direkte Aktualisierung: Ersetzen Sie Release 4 durch eine Neuinstallation. Dies hat keine Auswirkung auf persistente Daten.	Keine

Java DB-Daten

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Java DB-Software betroffen sein können.

Tabelle 8-3 Java DB-Datenverwendungen

Datentyp	Standort	Verwendung
Konfigurationsdaten	Die Instanzkonfiguration ist anwendungsspezifisch, wird nicht unter <i>JavaDB-base</i> gespeichert und ist nicht von der Aktualisierung betroffen.	Konfiguration der Java DB-Instanz
Persistente Daten	Datenbankverzeichnisse und deren Inhalt sind anwendungsspezifisch und werden nicht unter <i>JavaDB-base</i> gespeichert.	Datenbank und Benutzerzertifikate

Vorgehensweise zur Aktualisierung von Java DB

Die Vorgehensweise zur Aktualisierung von Java DB hängt im Grunde von den verschiedenen Aspekten ab, die in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) besprochen wurden: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

In diesem Abschnitt wird im Detail auf Java DB eingegangen, indem Themen besprochen werden, die Ihre Aktualisierungspläne von Java DB beeinflussen können.

Kompatibilität

Die Rückwärtskompatibilität von Java DB Release 5 zur Release 4-Version ist gewährleistet.

-Abhängigkeiten

Für Java DB besteht nur zur gemeinsam verwendeten J2SE-Komponente eine Abhängigkeit (siehe [Tabelle 1-7 auf Seite 51](#)).

Aktualisieren von Java DB von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von Java DB von Java ES 2005Q4 (Release 4) auf Java ES 2005Q5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 4-Version von Java DB](#)
- [Aktualisierung mehrerer Instanzen](#)

Einführung

Berücksichtigen Sie bei der Aktualisierung von Java ES von Java DB Release 4 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch eine Neuinstallation von Java DB Release 5, durch die die Release 4-Version ersetzt wird. Die Daten und die Konfiguration von Release 4 werden unverändert beibehalten.
- **Aktualisierungsabhängigkeiten.** Für Java DB besteht eine zwingende Aktualisierungsabhängigkeit zur gemeinsam verwendeten J2SE-Komponente (siehe [Tabelle 1-7 auf Seite 51](#)), die automatisch vom Java ES-Installationsprogramm auf Release 5 aktualisiert wird, wenn Sie eine Aktualisierung von Java DB durchführen.
- **Rückwärtskompatibilität.** Die Java DB Release 5-Version ist mit Release 4 vollständig kompatibel.
- **Aufheben der Aktualisierung.** Das Zurücksetzen der Release 5-Aktualisierung kann nur durch Zurückkehren zu einer gesicherten Release 4-Installation erfolgen.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Java DB ist für das Solaris- und Linux-Betriebssystem identisch.

Aktualisierung der Release 4-Version von Java DB

In diesem Abschnitt wird die Aktualisierung von Java DB von Java ES Release 4 auf Java ES Release 5 unter Solaris und Linux beschrieben. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren von Release 4 von Java DB](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung der Java DB-Software beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Java DB-Abhängigkeiten aktualisieren](#)
- [Java DB-Daten sichern](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

Aktuelle Versionsinformationen überprüfen

Sie können die aktuelle Version von Java DB mithilfe des folgenden Befehls überprüfen:

```
java -cp JavaDB-base/lib/derby.jar org.apache.derby.tools.sysinfo
```

Die Versionsinformationen (für die Datei `derby.jar`) werden in der folgenden Tabelle aufgeführt:

Tabelle 8-4 Java DB-Ausgaben der Versionsüberprüfung

Java ES Release	Java DB-Versionsnummer
Release 4	10.0.2.1
Release 5	10.1.3.1

Java DB-Abhängigkeiten aktualisieren

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Alle gemeinsam genutzten Komponenten, die von Java DB benötigt werden, werden jedoch automatisch vom Java ES-Installationsprogramm aktualisiert, wenn Sie eine Aktualisierung von Java DB auf Release 5 durchführen.

Java DB-Daten sichern

Bei der Java DB-Aktualisierung von Release 4 auf Release 5 werden keine Konfigurationsdaten oder persistenten Daten geändert. Eine Sicherung der aktuellen Daten ist daher nicht erforderlich. Aus Sicherheitsgründen sollten Sie jedoch eine Sicherungskopie Ihrer gesamten Java DB-Installation und Ihrer Daten erstellen.

Erforderliche Konfigurationsinformationen und Passwörter abrufen

Bei der Aktualisierung von Java DB sind keine Konfigurationsinformationen und kein Passwort erforderlich.

Aktualisieren von Release 4 von Java DB

In diesem Abschnitt wird das Aktualisierungsverfahren unter Solaris und Linux beschrieben.

Aktualisierungsverfahren

Das im Folgenden beschriebene Verfahren ist für alle Java DB-Instanzen anzuwenden, die lokal auf dem Computer ausgeführt werden, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

`su -`

2. Java DB Release 4 anhalten.

Wenn Sie gerade einen Netzwerkservers ausführen, verwenden Sie den folgenden Befehl:

```
java -cp JavaDB-base/lib/derby.jar:JavaDB-base/lib/derbynet.jar
org.apache.derby.drda.NetworkServerControl shutdown
```

Andernfalls beenden Sie einfach sämtliche Anwendungen, die Java DB verwenden.

3. Führen Sie eine Neuinstallation von Java DB Release 5 aus.

Führen Sie die folgenden Schritte aus:

- a. Starten Sie das Java ES-Installationsprogramm auf dem Computer, der als Host für Java DB Release 4 dient.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

wobei *os_arch* der Plattform entspricht, wie z. B. *Solaris_sparc*.
(Verwenden Sie die Option `installer -nodisplay` für die Befehlszeilenschnittstelle.)

Nach der Willkommensseite sowie der Lizenzvereinbarung wird eine Seite für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten erkannt werden, die direkt vom Java ES-Installationsprogramm aktualisiert werden können, wird der Status als „aktualisierbar“ angezeigt.)

- b. Wählen Sie auf der Seite für die Komponentenauswahl Java DB.

Die vorherige Installation wird daraufhin überschrieben.

- c. Wählen Sie die Option „Später konfigurieren“ aus.

Die Option „Jetzt konfigurieren“ wird nicht unterstützt.

- d. Falls erforderlich, wählen Sie die Option zur Installation von lokalisierten Paketen.

- e. Beenden Sie das Java ES-Installationsprogramm, nachdem die Installation abgeschlossen wurde.

4. Starten Sie Java DB Release 5.

Wenn Sie gerade einen Netzwerkservers ausführen, verwenden Sie den folgenden Befehl:

```
java -jar <JavaDB-base>/lib/derbynet.jar start
```

Andernfalls starten Sie sämtliche Anwendungen, die Java DB verwenden, einfach im integrierten Modus.

Überprüfen der Aktualisierung

Mithilfe des folgenden Befehls können Sie überprüfen, ob die Aktualisierung von Java DB erfolgreich war:

```
java -cp JavaDB-base/lib/derby.jar org.apache.derby.tools.sysinfo
```

Ausgabewerte (für die Version der Datei `derby.jar`) finden Sie in [Tabelle 8-4 auf Seite 175](#).

Aufgaben nach der Aktualisierung

Bei der Java DB-Aktualisierung von Release 4 auf Release 5 müssen Sie Daten mit dem Java DB-Festplattenformat 10.0 in das Format 10.1 konvertieren. Um diese Konvertierung durchzuführen, stellen Sie mit dem an die JDBC-URL angehängten Befehl `upgrade=true` eine Verbindung zur Datenbank her. Beispiel:

```
java -cp JavaDB-base/lib/derbytools.jar:JavaDB-base/lib/derby.jar  
org.apache.derby.tools.ij
```

```
ij version 10.1
```

```
ij> connect 'jdbc:derby:/databasePath;upgrade=true';
```

```
ij> exit;
```

Aufheben der Aktualisierung

Das Zurücksetzen der Release 5-Aktualisierung kann nur durch Zurückkehren zu einer gesicherten Release 4-Installation und den entsprechenden Daten erfolgen.

Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen wird Java DB auf mehreren Computersystemen bereitgestellt, um die Skalierbarkeit zu gewährleisten und die Verfügbarkeit zu verbessern. Möglicherweise führen Sie beispielsweise Java DB-Instanzen auf mehreren Computern zusammen mit einem Lastenausgleichsprogramm aus, um die Last zu verteilen.

Informationen zur Aktualisierung von Java DB auf den einzelnen Computern erhalten Sie unter [„Aktualisierung der Release 4-Version von Java DB“ auf Seite 175](#).

High Availability Session Store

In diesem Kapitel wird die Aktualisierung von High Availability Session Store auf Java ES 5 (Release 5) beschrieben: High Availability Session Store (HADB) 4.4.3.

Das Kapitel bietet zunächst einen allgemeinen Überblick über die Aktualisierung und beschreibt anschließend die verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von HADB“ auf Seite 181
- „Aktualisieren von HADB von Java ES Release 4“ auf Seite 184
- „Aktualisieren von HADB von Java ES Release 3“ auf Seite 192

HINWEIS Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf einen Verzeichnispfad, der im Folgenden als *HADB-base* angegeben wird. Bei der erstmaligen Installation und Konfiguration von HADB wurde möglicherweise ein Teil dieses Pfades als Installationsverzeichnis angegeben. Wenn nicht, wurde vom Installationsprogramm ein Standardwert zugewiesen.

Der Standardwert für *HADB-base* hängt nicht vom Betriebssystem ab, wie in der folgenden Tabelle dargestellt.

Tabelle 9-1 HADB Verzeichnispfade

Variable des Pfadnamens	Solaris OS	Linux OS
<i>HADB-base</i>	/opt/SUNWhadb/ <i>version_number</i>	/opt/SUNWhadb/ <i>version_number</i>
Java ES-Installationsprogramm		

Tabelle 9-1 HADB Verzeichnispfade (*Fortsetzung*)

Variable des Pfadnamens	Solaris OS	Linux OS
<i>HADB-base</i>	/opt/SUNWappserver/appserver	/opt/SUNWappserver/appserver
Standalone	/hadb/ <i>version_number</i>	/hadb/ <i>version_number</i>
Anwendungsserver 8.2		
EE-Installationsprogramm		

Überblick über Aktualisierungen von HADB

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von HADB auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5 HADB](#)
- [Wegweiser für die Aktualisierung von HADB](#)
- [HADB-Daten](#)
- [Vorgehensweise zur Aktualisierung von HADB](#)

Über Java ES Release 5 HADB

Java ES Release 5 von HADB stellt im Gegensatz zu Release 4 von HADB kleinere Verbesserungen in der Benutzerfreundlichkeit dar.

Wegweiser für die Aktualisierung von HADB

[Tabelle 9-2](#) zeigt die unterstützten Wege für die Aktualisierung von HADB auf Java ES Release 5. Die Tabelle gilt sowohl für das Solaris- als auch für das Linux-Betriebssystem.

Tabelle 9-2 Wege für die Aktualisierung auf Java ES 5 (Release 5): HADB 4.4.3

Java ES Release	HADB Version	Allgemeiner Ansatz	Neukonfiguration erforderlich
Release 4	HADB 4.4.2 (2005Q4)	Direkte Aktualisierung: Es stehen sowohl Online- als auch Offline-Aktualisierungsansätze zur Verfügung.	Keine
Release 3	HADB 4.4.1 (2005Q1)	Direkte Aktualisierung: Es stehen sowohl Online- als auch Offline-Aktualisierungsansätze zur Verfügung.	Keine
Release 2	HADB 4.4.0-14 (2004Q2)	Aktualisierung nicht unterstützt.	Keine
Release 1	Nicht verfügbar	Keine Aktualisierung:	Keine

Tabelle 9-2 Wege für die Aktualisierung auf Java ES 5 (Release 5): HADB 4.4.3

Java ES Release	HADB Version	Allgemeiner Ansatz	Neukonfiguration erforderlich
Versionen vor Java ES	Nicht verfügbar	Keine Aktualisierung.	Keine

HADB-Daten

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der HADB-Software betroffen sein können.

Tabelle 9-3 HADB Verwendung der Daten

Datentyp	Standort	Verwendung
Dynamische Anwendungsdaten	/var/opt/SUNWhadb and /etc/opt/SUNWhadb	High Availability Session Store und Konfigurationsinformationen.

Vorgehensweise zur Aktualisierung von HADB

Die Vorgehensweise zur Aktualisierung von HADB hängt im Grunde von den verschiedenen Aspekten ab, die in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) besprochen wurden: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

In diesem Abschnitt wird im Detail auf HADB eingegangen, indem Themen besprochen werden, die Ihre Aktualisierungspläne von HADB beeinflussen können.

Kompatibilität

Die Rückwärtskompatibilität von HADB Release 5 zu HADB mit Java ES Release 4 ist gewährleistet.

HADB-Abhängigkeiten

Für HADB Release 5 besteht nur zur gemeinsam verwendeten J2SE-Komponente eine Abhängigkeit Java™ 2 Platform, Standard Edition (J2SE™) Version 1.4 oder höher.

Aktualisieren von HADB von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von HADB von Java ES 2005Q4 (Release 4) auf Java ES 2005Q5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 4-Version von HADB](#)

Einführung

Berücksichtigen Sie bei der Aktualisierung von Java ES von HADB Release 4 auf Java ES Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch das Entfernen der Java ES Release 4 HADB-Pakete und das Hinzufügen der Java ES Release 5-Pakete. Zwei Aktualisierungsansätze sind möglich:
 - **Online-Aktualisierung.** Verwenden Sie die Online-Aktualisierung, um eine Unterbrechung der HADB-Dienste zu vermeiden.
 - **Offline-Aktualisierung.** Verwenden Sie die Offline-Aktualisierung, wenn Sie für das Ersetzen der HADB-Pakete durch neuere Versionen die HADB-Dienste unterbrechen können.
- **Aktualisierungsabhängigkeiten.** Für HADB bestehen keine zwingenden Abhängigkeiten. HADB erfordert J2SE Version 1.4 oder höher. Demzufolge besteht eine nicht zwingende Aktualisierungsabhängigkeit zu J2SE.
- **Rückwärtskompatibilität.** Die in Java ES Release 5 enthaltene HADB ist rückwärts kompatibel zur HADB in Java ES Release 4.
- **Aufheben der Aktualisierung.** Das Zurücksetzen der Java ES Release 5-Aktualisierung auf Java ES Release 4 erfolgt durch Wiederherstellen der Release 4-Versionspakete.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von HADB ist für das Solaris- und Linux-Betriebssystem identisch.

Aktualisierung der Release 4-Version von HADB

In diesem Abschnitt wird die Aktualisierung von HADB von Java ES Release 4 auf Java ES Release 5 unter Solaris und Linux beschrieben. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren von Release 4 von HADB](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung der HADB-Software beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [HADB-Aktualisierungsabhängigkeiten](#)
- [Verzeichnisdaten und Konfigurationsdateien sichern](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

Aktuelle Versionsinformationen überprüfen

Um die aktuelle HADB-Version zu überprüfen, verwenden Sie ein Standarddienstprogramm für die Versionsüberprüfung. Beispiel:

Unter Solaris:

```
pkgparam -v SUNWhadba
```

Unter Linux:

```
rpm -qi sun-hadb-a-4.4.3-5.i386.rpm
```

Tabelle 9-4 HADB Ausgaben der Versionsüberprüfung

Java ES Release	HADB-Versionsnummer
Release 2	VERSION=4.4.0,REV=14 SUNW_PRODVERS=4.4.0
Release 3	VERSION=4.4.1,REV=7 SUNW_PRODVERS=4.4.1

Tabelle 9-4 HADB Ausgaben der Versionsüberprüfung

Java ES Release	HADB-Versionsnummer
Release 4	VERSION=4.4.2,REV=7
	SUNW_PRODVERS=4.4.2
Release 5	VERSION=4.4.3,REV=5
	SUNW_PRODVERS=4.4.3

HADB-Aktualisierungsabhängigkeiten

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Alle gemeinsam genutzten Komponenten, die von HADB (nämlich J2SE) benötigt werden, werden jedoch automatisch vom Java ES-Installationsprogramm aktualisiert, wenn Sie eine Aktualisierung von HADB auf Release 5 durchführen.

Verzeichnisdaten und Konfigurationsdateien sichern

Bei der Aktualisierung von HADB von Java ES Release 4 auf Java ES Release 5 werden keine dynamischen HADB-Daten geändert. Sie können jedoch die Java ES Release 4-Pakete sichern, für den Fall, dass Sie die Aktualisierung rückgängig machen möchten.

Sichern Sie darüber hinaus die folgenden Dateien, wenn Sie seit der vorherigen HADB-Installation Änderungen an ihnen vorgenommen haben.

```
/etc/opt/SUNWhadb/mgt.cfg
/etc/init.d/ma-initd
```

Erforderliche Konfigurationsinformationen und Passwörter abrufen

Für die Aktualisierung von HADB benötigen Sie das Superuser-Passwort.

Aktualisieren von Release 4 von HADB

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von HADB haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

Zu berücksichtigende Aspekte bei der Aktualisierung

Bei der Aktualisierung der HADB-Software auf Java ES Release 5 müssen folgende Aspekte berücksichtigt werden:

- Sie müssen entsprechend Ihrer Produktionsumgebung festlegen, ob eine Online- oder eine Offline-Aktualisierung angebracht ist.
- Die Patches für die Aktualisierung auf Java ES Release 5 unter Solaris und Linux werden in der folgenden Tabelle aufgeführt: Die Solaris-Pakete sind entsprechend der Installationsreihenfolge aufgelistet.

Tabelle 9-5 Paketversionen für die Aktualisierung von HADB unter Solaris

Solaris-Pakete	Linux-Pakete
SUNWhadba	sun-hadb-a-4.4.3-5.i386.rpm
SUNWhadbc	sun-hadb-c-4.4.3-5.i386.rpm
SUNWhadbe	sun-hadb-e-4.4.3-5.i386.rpm
SUNWhadbi	sun-hadb-i-4.4.3-5.i386.rpm
SUNWhadbj	sun-hadb-j-4.4.3-5.i386.rpm
SUNWhadbm	sun-hadb-m-4.4.3-5.i386.rpm
SUNWhadbs	sun-hadb-s-4.4.3-5.i386.rpm
SUNWhadbv	sun-hadb-v-4.4.3-5.i386.rpm
SUNWhadbx	sun-hadb-x-4.4.3-5.i386.rpm

Online-Aktualisierung von HADB

Bei einer Online-Aktualisierung von HADB müssen Sie HADB Release 5 zunächst auf allen zu aktualisierenden Servern im Cluster installieren. Jeder Server hebt die Registrierung der früheren Installation von HADB auf und registriert anschließend die neu installierte HADB-Version.

Genaue Informationen zur Durchführung einer Online-Aktualisierung finden Sie im folgenden Abschnitt im *Sun Java System Anwendungsserver Enterprise Edition 8.2 High Availability Administration Guide* unter <http://docs.sun.com/doc/819-4740/6n4r9q07n?a=view>

Offline-Aktualisierung von HADB

Die Offline-Aktualisierung von HADB steht für die Aktualisierung von jeder Java ES Release 3- oder Release 4-Version zur Verfügung.

Um eine Offline-Aktualisierung durchzuführen, beenden Sie Ihre HADB-Dienste und ersetzen Sie die vorhandenen HADB-Pakete durch die Pakete der neuen Versionen, die in der Java ES 5 Release 5-Verteilung verfügbar sind (siehe [Tabelle 9-5 auf Seite 187](#)).

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Beenden Sie alle HADB-Dienste.

- a. Listen Sie sämtliche Datenbanken auf, die gerade ausgeführt werden.

```
HADB-base/bin/hadbm list
```

- b. Beenden Sie sämtliche aufgeführten Datenbanken.

```
HADB-base/bin/hadbm stop databaseName
```

Ignorieren Sie die Meldung, wenn sich eine Datenbank bereits im angehaltenen Status befindet.

- c. Beenden Sie den HADB-Management Agent auf jedem Host, auf dem ein Management Agent ausgeführt wird.

```
/etc/init.d/ma-initd stop
```

(Das Skript `ma-initd` befindet sich unter *HADB-base/bin*, wenn Sie HADB mithilfe des Anwendungsserver-Installationsprogramms anstelle des Java ES-Installationsprogramms installiert haben.)

3. Starten Sie das Java ES-Installationsprogramm.

```
cd Java ES Release 5 distribution/os_arch  
./installer
```

wobei *os_arch* der Plattform entspricht, wie beispielsweise *Solaris_sparc*. (Verwenden Sie die Option `installer -nodisplay` für die Befehlszeilenschnittstelle.)

Nach der Willkommenseite sowie der Lizenzvereinbarung wird eine Seite für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten erkannt werden, die direkt vom Java ES-Installationsprogramm aktualisiert werden können, wird der Status als „aktualisierbar“ angezeigt.)

4. Wählen Sie High Availability Session Store 4.4 auf der Seite für die Komponentenauswahl aus.

Wenn Sie Anwendungsserver Enterprise Edition 8.2 bereits ausgewählt haben, wird HADB automatisch ausgewählt.

5. Bestätigen Sie Ihre Auswahl für die Aktualisierung.

Die Anwendungsserver-Pakete werden aktualisiert. Anschließend wird eine Aktualisierungszusammenfassung angezeigt.

6. Beenden Sie das Java ES-Installationsprogramm.

7. Stellen Sie die unter „[Verzeichnisdaten und Konfigurationsdateien sichern](#)“ auf Seite 186 gesicherten Dateien wieder her.

8. Stellen Sie sicher, dass die symbolische Verknüpfung `/opt/SUNWhadb/4` nun auf *HADB-base* verweist.

Für die Standardvariable *HADB-base* lautet sie beispielsweise:

```
ls -l /opt/SUNWhadb/4
lrwxrwxrwx 1 root other 7 Jul 7 23:18 /opt/SUNWhadb/4 ->
4.4.3-5/
```

Überprüfen der Aktualisierung

Um die abgeschlossene Online-Aktualisierung zu überprüfen, führen Sie folgendes Verfahren durch. Nachdem Sie überprüft haben, ob die Aktualisierung erfolgreich war, können Sie die alten Installationspakete löschen.

Um zu überprüfen, ob die ausgeführten Prozesse die aktualisierten HADB-Dienste verwenden, führen Sie folgende Schritte aus:

1. Führen Sie für jeden ausgeführten HADB-Dienst einen der folgenden Befehle aus:

```
HADB-base/bin/ma -V
HADB-base/bin/hadbm -V
```

Beispiel:

```
HADB-base/bin/ma -V
Sun Java System High Availability Database 4.4 Database Management
Agent
Version: 4.4.3.5 [V4-5-3-5 2006-03-31 13:59:50 pakker@astra07]
(SunOS_5.9_sparc)
```

2. Überprüfen Sie, ob die Datenbank ausgeführt wird:

```
HADB-base/bin/hadbm status -n databaseName
```

Geben Sie beispielsweise für eine Datenbank mit dem Namen „Example DB“ die folgenden Befehle ein:

```
HADB-basebin/hadbm list
```

```
Database
```

```
ExampleDB
```

```
HADB-base/bin/hadbm status ExampleDB
```

```
Database      Status
```

```
ExampleDB     FaultTolerant
```

```
HADB-base/bin/hadbm status -n ExampleDB
```

NodeNo	HostName	Port	NodeRole	NodeState	MirrorNode
0	sungod012	15000	active	running	1
1	sungod012	15020	active	running	0

Alle HADB-Dienste für die aufgelisteten Knoten sollten den Status „running“ aufweisen.

3. Überprüfen Sie, ob sämtliche Produkte, die HADB verwenden, den neuen HADB-Pfad verwenden.

```
HADB-base/bin/hadbm get PackageName databaseName
```

Geben Sie beispielsweise für eine Datenbank mit dem Namen „Example DB“ die folgenden Befehle ein:

```
HADB-base/bin/hadbm get PackageName ExampleDB
```

```
Attribute      Wert
```

```
PackageName    V4.4.3.5
```

Der obige Befehl zeigt die aktuelle HADB-Version an. Um eine genaue Auflistung zu erhalten, führen Sie folgenden Befehl aus:

```
HADB-base/bin/hadbm get --all ExampleDB
```

Aufgaben nach der Aktualisierung

Mit Ausnahme der in [„Aktualisieren von HADB von Java ES Release 4“ auf Seite 184](#) beschriebenen Schritte müssen keine weiteren Aufgaben nach der Aktualisierung durchgeführt werden.

Aufheben der Aktualisierung

Um die Aktualisierung von HADB aufzuheben, ersetzen Sie die neueren Versionen der installierten HADB-Pakete durch die Versionen, die Sie zuvor gesichert haben, wie in „[Verzeichnisdaten und Konfigurationsdateien sichern](#)“ auf Seite 186 beschrieben.

Aktualisieren von HADB von Java ES Release 3

Das Verfahren zur Aktualisierung von Java ES 2005Q1 (Release 3) HADB auf Release 5 ist mit dem Verfahren zur Aktualisierung von HADB Release 4 auf Release 5 identisch.

Um die Release 3-Version von HADB auf Release 5 zu aktualisieren, folgen Sie den Anweisungen unter „[Aktualisieren von HADB von Java ES Release 4](#)“ auf [Seite 184](#). Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 3.

Message Queue

In diesem Kapitel wird die Aktualisierung der Message Queue-Software von früheren Java ES-Versionen auf Java ES 5 (Release 5) beschrieben: Sun Java System Message Queue 3.7 UR1.

Das Kapitel enthält einen Überblick über die Aspekte der verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Message Queue“ auf Seite 194
- „Aktualisieren von Message Queue von Java ES Release 4“ auf Seite 199
- „Aktualisieren von Message Queue von Java ES Release 3“ auf Seite 206
- „Aktualisieren der Message Queue Release 2-Version aus Java ES-Release 2“ auf Seite 207

HINWEIS Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf einen festen Verzeichnispfad, der im Folgenden als *MessageQueue-base* angegeben wird.

Der Wert für *MessageQueue-base* hängt vom Betriebssystem ab, wie in der folgenden Tabelle dargestellt.

Tabelle 10-1 Message Queue Verzeichnispfade

Variable des Pfadnamens	Solaris OS	Linux OS
<i>MessageQueue-base</i>	/usr/bin	/opt/sun/mq/bin

Überblick über Aktualisierungen von Message Queue

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Message Queue auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5 Message Queue](#)
- [Wegweiser für die Aktualisierung von Message Queue](#)
- [Message Queue-Daten](#)
- [Vorgehensweise zur Aktualisierung von Message Queue](#)

Über Java ES Release 5 Message Queue

Java ES Release 5 Message Queue stellt im Gegensatz zu Release 4 eine kleinere Aktualisierung dar. Es beinhaltet größtenteils Kodekorrekturen und keine kleineren Verbesserungen von Funktionen.

Die Message Queue-Software war früher in den Ausgaben Platform Edition und die Enterprise Edition erhältlich. Die beiden Ausgaben weisen unterschiedliche Funktionalitäten und einen unterschiedlichen Lizenzierungsumfang auf. Die Enterprise Edition war für die Bereitstellung und Ausführung von Messaging-Anwendungen in einer Produktionsumgebung eines Unternehmens konzipiert. Die Platform Edition wurde hauptsächlich für die Entwicklung, die Fehlerbehebung und das Testen der Lastverteilung von Messaging-Anwendungen und -Komponenten verwendet. Bei Message Queue Release 5 wurde die Platform Edition verworfen und Message Queue beinhaltet sämtliche Funktionen der Enterprise Edition. Bei der Aktualisierung von früheren Java ES-Release-Versionen auf Release 5 werden sämtliche installierte Funktionen der Platform Edition in die vollständigen Funktionen der Message Queue Enterprise Edition konvertiert.

Wegweiser für die Aktualisierung von Message Queue

[Tabelle 10-2](#) zeigt die unterstützten Wege für die Aktualisierung von Message Queue auf Java ES Release 5. Die Tabelle gilt sowohl für das Solaris- als auch für das Linux-Betriebssystem.

Tabelle 10-2 Wege für die Aktualisierung auf Java ES 5 (Release 5): Message Queue 3.7 UR1

Java ES Release	Message Queue Version	Allgemeiner Ansatz	Neukonfiguration erforderlich
Release 4	Sun Java System Message Queue 2005Q4 (3.6 SP3)) nur Enterprise Edition	Direkte Aktualisierung: Durch Anwendung des Java ES-Installationsprogramms.	Automatisch durchgeführte Konvertierung von Daten.
Release 3	Sun Java System Message Queue 2005Q1 (3.6) nur Enterprise Edition	Direkte Aktualisierung: Durch Anwendung des Java ES-Installationsprogramms.	Automatisch durchgeführte Konvertierung von Daten.
Release 2	Sun Java System Message Queue 2004Q2 (3.5 SP1) Platform und Enterprise Edition	Direkte Aktualisierung: Durch Anwendung des Skripts mqupgrade.	Wird auf Solaris-Plattformen automatisch durchgeführt; für Linux-Plattformen steht das Skript mqmigrate zur Verfügung.
Release 1	Sun Java System Message Queue 2003Q4 (3.0.1 SP2) Platform und Enterprise Edition	Direkte Aktualisierung nicht zertifiziert. Kann jedoch mit dem Skript mqupgrade durchgeführt werden. ¹	Wird auf Solaris-Plattformen automatisch durchgeführt; für Linux-Plattformen steht das Skript mqmigrate zur Verfügung.
Versionen vor Java ES	Sun Java System Message Queue 3.0.x und frühere Versionen Platform und Enterprise Edition	Direkte Aktualisierung nicht zertifiziert. Kann jedoch mit dem Java ES-Installationsprogramm durchgeführt werden.	

1. Vor und nach Ausführen des Skripts mqupgrade müssen Sie die folgenden Dateien möglicherweise sichern und wiederherstellen: Beispielsweise (auf Solaris OS): wiederherstellen von /etc/imq/passwd und /etc/imq/accesscontrol.properties in /var/imq/instances/instanceName/etc/

Zusätzlich zu den in [Tabelle 10-2](#) aufgelisteten Message Queue Release-Versionen von Java ES ist Message Queue im Lieferumfang mit der Solaris-Betriebssystemsoftware enthalten. Die Aktualisierung der im Lieferumfang enthaltenen Versionen von Message Queue auf Release 5 kann mithilfe des Java ES-Installationsprogramms durchgeführt werden.

Message Queue-Daten

Wie andere Java ES-Komponenten auch verwendet Message Queue verschiedene Datentypen, die bei einer Aktualisierung möglicherweise auf eine aktualisierte Version migriert werden müssen. Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Message Queue-Software betroffen sein können.

[Tabelle 10-3](#) enthält die Speicherorte der Daten auf Solaris-Betriebssystemen. Die Speicherorte auf Linux-Betriebssystemen sind identisch (in der Tabelle wurde `/imq` durch `/opt/sun/mq` ersetzt). Weitere Informationen finden Sie im *Message Queue 3.7 UR1 Administration Guide* unter <http://docs.sun.com/doc/819-4467/6n6k98brl?a=view>.

In [Tabelle 10-3](#) gibt *instanceName* die Message Queue-Broker-Instanz an, der die Daten zugeordnet sind.

Tabelle 10-3 Message Queue Verwendung der Daten (Solaris OS)

Datenkategorie	Speicherort (unter Solaris)	Verwendung
Konfigurationseigenschaften der Broker-Instanz	<code>/var/imq/instances/instanceName/props/config.properties</code>	Konfigurationen der Broker und zugehöriger Dienste
Persistenter Speicher für dynamische Anwendungsdaten	Release 2, Release 3 und Release 4: <code>/var/imq/instances/instanceName/fs350/</code> Release 5 <code>/var/imq/instances/instanceName/fs370/</code> oder ein JDBC-zugänglicher Datenspeicher	Speichert Nachrichten, Ziele, dauerhafte Abonnements, Transaktionen und andere dynamische Daten
Verwaltete Objekte (Objektspeicher)	lokales Verzeichnis Ihrer Wahl oder ein LDAP-Directory Server	Für die Konfiguration von Client/Broker-Verbindungen verwendete Objekte
Sicherheit: Benutzer-Repository	<code>/var/imq/instances/instanceName/etc/passwd</code> oder ein LDAP-Directory Server	Speichert Benutzerdaten für Authentifizierung und Autorisierung
Sicherheit: Zugriffssteuerungsdatei (Standard-Speicherort)	<code>/var/imq/instances/instanceName/etc/accesscontrol.properties</code>	Legt die Regeln für die Autorisierung des Benutzerzugriffs auf Ziele und zusammenhängende Funktionen fest
Sicherheit: Passfile-Verzeichnis (Standard-Speicherort)	<code>/var/imq/instances/instanceName/etc/</code>	Speichert verschlüsselte Passwortinformationen
Sicherheit: Speicherort der Broker-Schlüsseldatei	<code>/etc/imq/</code>	Speichert verschlüsselte Zertifikatsinformationen für sicheres Messaging

Vorgehensweise zur Aktualisierung von Message Queue

Die Vorgehensweise zur Aktualisierung von Message Queue hängt im Grunde von den verschiedenen Aspekten ab, die in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) besprochen wurden: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

In diesem Abschnitt wird im Detail auf Message Queue eingegangen, indem Themen besprochen werden, die Ihre Aktualisierungspläne von Message Queue beeinflussen können.

Kompatibilität

Message Queue Release 5 führt keine neuen Inkompatibilitäten zu Release 3 oder Release 4 ein. Es bestehen jedoch beträchtliche Kompatibilitätsprobleme in Bezug auf Release 2 und frühere Versionen. Diese werden erläutert unter [„Release 2-Kompatibilitätsprobleme“ auf Seite 208](#).

Darüber hinaus gilt im Allgemeinen: Wenn Sie Release 4-Broker und Broker früherer Message Queue-Versionen und Message Queue-Release 5-Broker zusammen in einem Cluster verwenden, muss der Broker der früheren Release als Master-Broker verwendet werden; das Cluster wird als Message Queue-Cluster der früheren Version ausgeführt.

Message Queue-Abhängigkeiten

Message Queue-Abhängigkeiten zu anderen Java ES-Komponenten beeinflussen möglicherweise das Verfahren für die Aktualisierung und Neukonfiguration der Message Queue-Software. Änderungen der Message Queue-Schnittstellen oder -Funktionen könnten beispielsweise eine aktualisierte Version der Komponenten erforderlich machen, von denen Message Queue abhängig ist. Welche dieser Komponenten aktualisiert werden müssen, hängt von dem jeweiligen Aktualisierungsweg ab.

Für Message Queue bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Message Queue ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)).

- **Directory Server.** Für Message Queue besteht eine optionale Abhängigkeit zu Directory Server: Sie können Message Queue so konfigurieren, dass verwaltete Objekte bzw. Benutzerdaten statt lokal in einem LDAP-Verzeichnis (Directory Server) gespeichert werden.
- **Web Container.** Für Message Queue besteht eine optionale Abhängigkeit zu Webserver, Anwendungsserver oder einem Drittanbieter-Webcontainer, um das HTTP Messaging zwischen Client und Broker zu unterstützen.
- **Datenbanken.** Für Message Queue besteht eine optionale Abhängigkeit von Java DB (oder Drittanbieterdatenbanken), um der Message Queue-Persistenzschicht statt eines Flatfile-Nachrichtenspeichers einen JDBC-zugänglichen Datenspeicher bereitzustellen.
- **Sun Cluster.** Für Message Queue besteht zur Hochverfügbarkeitsunterstützung eine optionale Abhängigkeit zu Sun Cluster.

Aktualisieren von Message Queue von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von Message Queue von Java ES 2005Q4 (Release 4) auf Java ES 2005Q5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 4-Version von Message Queue](#)
- [Aktualisierung mehrerer Instanzen](#)

Einführung

Berücksichtigen Sie bei der Aktualisierung von Message Queue von Java ES Release 4 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt mithilfe des Java ES-Installationsprogramms. Die Release 4-Konfigurationsdaten werden vom Installationsprogramm automatisch migriert. Darüber hinaus werden die Release 4 zugeordneten dynamischen Anwendungsdaten beim erstmaligen Ausführen von `imqbrokerd` automatisch konvertiert. Bei einem dateibasierten Speicher bedeutet das, dass der Inhalt des Verzeichnisses `fs350` in ein neues `fs370`-Verzeichnis kopiert wird. Im Falle eines JDBC-Speichers werden die bestehenden Datenbanktabellen einer einfachen Versionsaktualisierung unterzogen.
- **Aktualisierungsabhängigkeiten.** Message Queue ist von einer Reihe gemeinsam genutzter Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)), die alle automatisch vom Java ES -Installationsprogramm auf Release 5 aktualisiert werden, wenn Sie eine Aktualisierung von Message Queue durchführen.

Darüber hinaus bestehen für Message Queue Release 5 Abhängigkeiten zu Java ES-Produktkomponenten, wie in „[Message Queue-Abhängigkeiten](#)“ auf [Seite 197](#) beschrieben. Bei diesen Komponenten ist es jedoch nicht erforderlich, eine Aktualisierung von Message Queue auf Release 5 durchzuführen.

- **Rückwärtskompatibilität.** Release 5 von Message Queue ist mit Release hinsichtlich der Protokolle, Broker-Kompatibilität, verwalteten Objekte, Verwaltungstools und Client-Anwendungen vollständig kompatibel.

- **Aufheben der Aktualisierung.** Für das Zurücksetzen der Message Queue-Aktualisierung auf Release 4 steht kein Dienstprogramm zur Verfügung. Sie müssen die aktualisierten Komponenten entfernen und die frühere Version sowie Konfigurationsdaten manuell wiederherstellen.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Message Queue ist für das Solaris- und Linux-Betriebssystem identisch.

Aktualisierung der Release 4-Version von Message Queue

In diesem Abschnitt wird die vollständige Aktualisierung von Message Queue von Java ES Release 4 auf Java ES Release 5 beschrieben:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren von Release 4 von Message Queue](#)
- [Überprüfen der Message Queue-Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung der Message Queue-Software beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Message Queue-Abhängigkeiten aktualisieren](#)
- [Sichern Message Queue](#)

Aktuelle Versionsinformationen überprüfen

Um die Version und Ausgabe von Message Queue auf Ihrem System zu ermitteln, starten Sie den Message Queue-Broker mit der Option `-version`:

```
imqbrokerd -version
```

Tabelle 10-4 Message Queue-Ausgaben der Versionsüberprüfung

Java ES Release	Message Queue-Versionsnummer
Release 2	Sun Java(tm) System Message Queue 3 2004Q2 Version: 3.5
Release 3	Sun Java(tm) System Message Queue 3 2005Q1 Version: 3.6
Release 4	Sun Java(tm) System Message Queue 3 2005Q4 Version: 3.6 SP3
Release 5	Sun Java(tm) System Message Queue 3.7 Version: 3.7 UR1

Message Queue-Abhängigkeiten aktualisieren

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Für Message Queue bestehen nur zu ein paar gemeinsam genutzten Komponenten zwingende Aktualisierungsabhängigkeiten.

Wenn Sie die Message Queue-Abhängigkeiten aktualisieren, sollten Sie dies in der unten angegebenen Reihenfolge vornehmen, bevor Sie Message Queue aktualisieren. Überspringen Sie dabei die bereits aktualisierten Abhängigkeiten. Die Aktualisierung gemeinsam genutzter Komponenten erfolgt automatisch durch das Java ES-Installationsprogramm.

1. **Gemeinsam genutzte Komponenten.** Anleitungen für die Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie unter [„Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#). Alle gemeinsam genutzten Komponenten, die von Message Queue benötigt werden, werden jedoch automatisch vom Java ES-Installationsprogramm aktualisiert, wenn Sie eine Aktualisierung von Message Queue auf Release 5 durchführen.
2. **Sun Cluster (keine zwingende Abhängigkeit)** Anleitungen für die Aktualisierung von Sun Cluster auf Release 5 finden Sie in [Kapitel 3, „Sun Cluster-Software“ auf Seite 83](#).
3. **Directory Server (keine zwingende Abhängigkeit)** Anleitungen für die Aktualisierung von Directory Server auf Release 5 finden Sie in [Kapitel 5, „Directory Server“ auf Seite 109](#).
4. **Java DB (keine zwingende Abhängigkeit).** Sie müssen Java DB Release 5 neu installieren, wenn Sie Message Queue aktualisieren.

5. **Webcontainer-Software (keine zwingende Abhängigkeit).** Anweisungen zur Aktualisierung von Webserver und Anwendungsserver finden Sie in [Kapitel 7, „Webserver“ auf Seite 143](#) bzw. [Kapitel 11, „Anwendungsserver“ auf Seite 219](#).

Sichern Message Queue

Wenn Sie eine Aktualisierung durchführen, ist es stets empfehlenswert, Anwendungsdaten in einer Produktionsumgebung zu sichern. Beachten Sie den in [Tabelle 10-3 auf Seite 196](#) angegebenen persistenten Speicher für dynamische Anwendungsdaten.

Aktualisieren von Release 4 von Message Queue

So führen Sie die Aktualisierung durch

1. Halten Sie sämtliche derzeit ausgeführten Message Queue-Client-Anwendungen an.

Wenn Message Queue in einer Anwendungsserver-Umgebung verwendet wird, beenden Sie Anwendungsserver ebenfalls.

2. Halten Sie sämtliche ausgeführten Broker an. Sie werden zur Eingabe des Admin-Benutzernamens und des zugehörigen Passworts aufgefordert:

```
imqcmd shutdown bkr [-b hostName:port]
```

3. Wenn Sie dynamische Daten, das Flatfile-Benutzer-Repository Message Queue und die der jeweiligen Broker-Instanz zugeordnete Message Queue-Zugriffssteuerungsdatei nicht beibehalten möchten, entfernen Sie diese Daten mit folgendem Befehl:

```
imqbrokerd -name instanceName -remove instance
```

Andernfalls werden die dynamischen Daten und Konfigurationsinformationen beibehalten und für Release 5 Message Queue verwendet.

4. Melden Sie sich als Root-Benutzer an.

```
su -
```


5. Starten Sie das Java ES-Installationsprogramm.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

wobei *os_arch* der Plattform entspricht, wie z. B. *Solaris_sparc*. (Verwenden Sie die Option *installer -nodisplay* für die Befehlszeilenschnittstelle.)

Nach der Willkommensseite sowie der Lizenzvereinbarung wird eine Seite für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten erkannt werden, die direkt vom Java ES-Installationsprogramm aktualisiert werden können, wird der Status als „aktualisierbar“ angezeigt.)

6. Wählen Sie auf der Seite für die Komponentenauswahl Message Queue.
7. Bestätigen Sie Ihre Auswahl für die Aktualisierung.

Die Message Queue-Pakete werden aktualisiert. Anschließend wird eine Aktualisierungszusammenfassung angezeigt.

8. Beenden Sie das Java ES-Installationsprogramm.

Überprüfen der Message Queue-Aktualisierung

Überprüfen Sie nach Durchführung des Aktualisierungsverfahrens, ob die Aktualisierung erfolgreich war, indem Sie den Message Queue-Broker mit der Option *-version* starten.

```
imqbrokerd -version
```

Der Befehl gibt die Java ES-Versionsnummer sowie die Message Queue-spezifische Versionsnummer zurück.

Aufgaben nach der Aktualisierung

Wenn Sie den Webcontainer aktualisiert haben und das HTTP-Tunneling-Servlet von Message Queue verwenden, müssen Sie es möglicherweise erneut im Webcontainer bereitstellen. Am HTTP-Tunneling-Servlet von Release 4 wurden im Vergleich zu Release 5 keine Änderungen vorgenommen. Weitere Informationen zur HTTP-Unterstützung erhalten Sie im *Message Queue 3.7 UR1 Administration Guide* unter <http://docs.sun.com/doc/819-4467>.

Wenn Sie sicher sind, dass Sie die Aktualisierung nicht rückgängig machen müssen, können Sie den im Verzeichnis *fs350* enthaltenen dateibasierten Datenspeicher von Release 4 entfernen (siehe [Tabelle 10-3 auf Seite 196](#)).

Aufheben der Aktualisierung

Für das Zurücksetzen von Message Queue in den Zustand vor der Aktualisierung stehen keine Skripte zur Verfügung. Der Vorgang muss wie folgt manuell durchgeführt werden:

1. Halten Sie sämtliche derzeit ausgeführten Message Queue-Client-Anwendungen an.
2. Halten Sie sämtliche ausgeführten Broker an. Sie werden zur Eingabe des Admin-Benutzernamens und des zugehörigen Passworts aufgefordert:

`imqcmd shutdown bkr [-b hostName:port]`
3. Wenn Sie dynamische Daten, das Flatfile-Benutzer-Repository Message Queue und die der jeweiligen Broker-Instanz zugeordnete Message Queue-Zugriffssteuerungsdatei löschen möchten, entfernen Sie diese Daten mit folgendem Befehl:

```
imqbrokerd -name instanceName -remove instance
```

4. Melden Sie sich als Root oder Superuser an.

`su -`
5. Rufen Sie mit folgendem Befehl die Liste der installierten Message Queue-Pakete ab:

Unter Solaris:
`pkginfo | grep -i "message queue"`

Unter Linux:
`rpm -qa | grep mq`

6. Entfernen Sie mit folgendem Befehl die Message Queue-Pakete:

Unter Solaris:

```
pkgrm packageName
```

Dabei steht *packageName* für ein beliebiges Message Queue-Paket. Wenn Sie mehrere Pakete entfernen möchten, trennen Sie die Paketnamen durch ein Leerzeichen.

Unter Linux:

```
rpm -e --nodeps RPMName
```

Dabei steht *RPMName* für eine der Message Queue-RPM-Komponenten. Wenn Sie mehrere Komponenten entfernen möchten, trennen Sie die RPM-Namen durch ein Leerzeichen.

Da die Message Queue-Pakete möglicherweise von anderen Produkten verwendet werden, sollten Sie beim Entfernen vorsichtig vorgehen. Durch den Befehl `pkgrm` werden Sie gewarnt, ob Abhängigkeiten mit einem Paket bestehen, bevor dieses entfernt wird. Geben Sie bei der entsprechenden Aufforderung Ihre Anforderung zum Entfernen `j` (ja) ein.

7. Geben Sie zum Beenden „q“ ein.
8. Verlassen Sie die Root-Shell.
9. Installieren Sie Message Queue Release 4 erneut.
Verwenden Sie das Java ES Release 4-Installationsprogramm.
10. Stellen Sie die in „[Sichern Message Queue](#)“ auf Seite 202 gesicherten Daten von Message Queue Release 4 wieder her.

Message Queue Release 4 funktioniert ordnungsgemäß mit den vor der Aktualisierung auf Release 5 gesicherten Daten.

Aktualisierung mehrerer Instanzen

Um ein Message Queue-Cluster zu aktualisieren, in dem mehrere Broker zusammenarbeiten, um einen skalierbaren Meldungsdienst bereitzustellen, können Sie ein Rolling Upgrade durchführen, bei dem der Cluster online bleibt, während die einzelnen Message Queue-Instanzen nacheinander von Release 4 auf Release 5 aktualisiert werden. Beachten Sie bei der Aktualisierung eines Clusters die folgenden zwei Bedingungen:

- Solange ein Broker für die Aktualisierung heruntergefahren ist, sind die vom Broker gespeicherten persistenten Meldungen nicht verfügbar. Die Meldungen sind erst dann wieder verfügbar, wenn der Broker neu gestartet wurde.

- Der Master-Broker sollte als letzter aktualisiert werden.

Andernfalls handelt es sich um ein unkompliziertes Verfahren: Sie beenden, aktualisieren und starten die einzelnen Broker nacheinander neu, bis alle Broker aktualisiert sind.

Aktualisieren von Message Queue von Java ES Release 3

Das Verfahren zur Aktualisierung von Java ES 2005Q1 (Release 3) Message Queue auf Release 5 ist mit dem Verfahren zur Aktualisierung von Message Queue Release 4 auf Release 5 identisch.

Um die Release 3-Version von Message Queue auf Release 5 zu aktualisieren, folgen Sie den Anweisungen unter „[Aktualisieren von Message Queue von Java ES Release 4](#)“ auf Seite 199. Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 3.

Aktualisieren der Message Queue Release 2-Version aus Java ES-Release 2

Dieser Abschnitt enthält Informationen zur Aktualisierung von Message Queue von Java ES 2004Q2 (Release 2) auf Java ES Release 5. In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Release 2-Kompatibilitätsprobleme](#)
- [Aktualisierung der Release 2-Version von Message Queue](#)
- [Aktualisierung mehrerer Instanzen](#)

Einführung

Berücksichtigen Sie bei der Aktualisierung von Message Queue von Java ES Release 2 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch die Ausführung des Skripts `mqupgrade`, das automatisch die Softwarepakete früherer Versionen durch die neuen Pakete ersetzt und die Migration der Release 2-Konfigurationsdaten vornimmt.
- **Aktualisierungsabhängigkeiten.** Die Aktualisierung einer Java ES-Komponente auf einem Computer von Release 2 erfordert eine Aktualisierung aller übrigen Java ES-Komponenten, die sich auf diesem Computer befinden. Die Auswahl einzelner Java ES-Komponenten bei einer Aktualisierung von Release 2 auf Release 5 wird nicht unterstützt. Insbesondere alle von Message Queue verwendeten gemeinsam genutzten Java ES-Komponenten müssen aktualisiert werden.

Die Release 5-Version von Message Queue ist optional von Directory Server und Webserver abhängig (oder Anwendungsserver), wie unter „[Message Queue-Abhängigkeiten](#)“ auf Seite 197 beschrieben. Wenn sie auf demselben Computer installiert sind, ist eine Aktualisierung dieser Komponenten auf Release 5 ebenfalls erforderlich.

- **Rückwärtskompatibilität.** Message Queue Release 5 ist nicht vollständig kompatibel mit Release 2, wie unter „[Release 2-Kompatibilitätsprobleme](#),“ beschrieben.

- **Aufheben der Aktualisierung.** Das Zurücksetzen der Release 5-Aktualisierung auf Release 2 wird zurzeit nicht unterstützt (siehe „[Aufheben der Aktualisierung](#)“).
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Message Queue ist für das Solaris- und Linux-Betriebssystem identisch. Bei Linux-Betriebssystemen sind jedoch einige zusätzliche Verfahren erforderlich. In den folgenden Verfahren werden plattformspezifische Befehle, Dateispeicherorte oder Verfahren entsprechend gekennzeichnet.

Release 2-Kompatibilitätsprobleme

Message Queue Release 5 führt die folgenden allgemeinen Message Queue-Kompatibilitätsprobleme in Bezug auf Release 2 und frühere Versionen ein.

Protokollkompatibilität

Für Message Queue besteht eine zwingende Abhängigkeit zum Webcontainer, um HTTP-Protokollunterstützung für Message Queue-Clients und -Broker bereitzustellen. Aufgrund einer Protokolländerung müssen bei Verwendung von Sun Java System Webserver für die Bereitstellung eines Webcontainers für die Message Queue-Anwendung `mqhttp.war` sowohl die Webserver-Komponente als auch die Message Queue aktualisiert werden (siehe „[Aufgaben nach der Aktualisierung](#)“ auf [Seite 203](#) und [Seite 216](#)).

Broker-Kompatibilität

Der Message Queue-Broker der Release 5-Version kann mit einem Release 4-, Release 3- oder Release 2-Broker zusammenarbeiten; die seit Release 2 vorgenommenen Änderungen der Broker-Eigenschaften und des Schemas für den persistenten Speicher können sich jedoch auf die Kompatibilität auswirken.

Message Queue der Release 5-Version kann Release 4-, Release 3- und Release 2-Daten verwenden, mit Ausnahme der Daten auf Linux-Systemen; Release 2-Daten müssen zunächst in Release 5 migriert werden.

Beachten Sie bei der Aktualisierung von Message Queue auf Release 5 Folgendes:

- Message Queue `config.properties`-Dateien früherer Versionen können verwendet werden. Sie können diese Dateien in einem anderen Verzeichnis speichern und die darin enthaltenen Eigenschaftseinstellungen für die Konfiguration des Message Queue-Brokers der Release 5-Version verwenden.

- Alle persistenten Message Queue-Daten (Meldungen, Ziele, dauerhafte Abonnements) werden gegebenenfalls automatisch in Release 5 Message Queue-Daten konvertiert, wenn Sie den Broker zum ersten Mal ausführen. Vorhandene Ziele werden beispielsweise gegebenenfalls in Release 5 Message Queue-Ziele konvertiert, wobei die vorhandenen Attributswerte beibehalten und für neue Attribute Standardwerte verwendet werden.
- Wenn Sie Message Queue Release 2-Broker und Message Queue Release 5-Broker zusammen in einem Cluster verwenden, muss der Master-Broker ein Message Queue Release 2-Broker sein (in jedem Fall der ältere); das Cluster wird als Message Queue Release 2-Cluster ausgeführt.

Kompatibilität der verwalteten Objekte

Die verwalteten Message Queue-Objekte der Release 5-Version sind mit den verwalteten Objekten der Release 3- und Release 4-Version identisch. Manche der verwalteten Objekte der Release 3-Version wurden jedoch im Vergleich zu Vorgängerversionen umbenannt oder durch neue Attribute erweitert. Beachten Sie daher beim Aktualisieren von Release 2 Message Queue auf Release 5 Folgendes:

- Sie können denselben Objektspeicher und dieselben verwalteten Objekte, die Sie in Release 2 erstellt haben, verwenden. Es wird jedoch empfohlen, die verwalteten Objekte in Release 5 zu migrieren. Die Administrationskonsole (`imqadmin`) und das ObjectManager-Befehlszeilendienstprogramm (`imqobjmgr`) wandelt beim Aktualisierungsvorgang die verwalteten Release 2-Objekte in verwaltete Release 5-Objekte um.
- Die Release 5-Client-Runtime sucht nach Release 2-verwalteten Objekten, erstellt Instanzen von diesen Objekten und wandelt die Objekte um, sodass diese von Release 5-Clients verwendet werden können. Hierdurch werden jedoch *keine* verwalteten Release 2-Objekte konvertiert, die sich in dem Objektspeicher befinden, von dem aus die Suche durchgeführt wurde.
- Vorhandene Release 2-Clients (Anwendungen und/oder Komponenten), d. h. Clients, die nicht erst nach verwalteten Objekten suchen, sondern diese direkt instanziierten, sind mit Release 5 kompatibel. Wenn die Clients jedoch die *neuen* verwalteten Objektattribute verwenden sollen, müssen diese neu geschrieben werden (Informationen zu verwalteten Objektattributen finden Sie in Kapitel 16 im *Message Queue 3.7 UR1 Administration Guide* unter <http://docs.sun.com/doc/819-4467>). (Um anzuzeigen, welche Message Queue Release 2-Attribute in Release 5 umbenannt wurden, führen Sie eine Neukompilierung durch. Die alten Namen können weiterhin verwendet werden.)

- Skripte, die Java-Clients starten und verwalteten Objektattributwerte mithilfe von Befehlszeilenoptionen festlegen, sind mit Release 5 kompatibel. Wenn die Skripte jedoch die *neuen* verwalteten Objektattribute verwenden sollen, müssen diese neu geschrieben werden (Informationen zu verwalteten Objektattributen finden Sie in Kapitel 16 im *Message Queue 3.7 UR1 Administration Guide* unter <http://docs.sun.com/doc/819-4467>).

Kompatibilität des Administrationstools

Da in Release 3 neue Befehle und neue Verwaltungsfunktionen hinzugefügt wurden, funktionieren die Release 5-Administrationstools (die Administrationskonsole und das Befehlszeilen-Dienstprogramm) nur mit Release 3-, Release 4- und Release 5-Brokern. Sämtliche Release 2-Befehle und -Befehlsoptionen werden jedoch weiterhin unterstützt.

Clientkompatibilität

Release 3- und Release 4-Clients sind vollständig mit Message Queue Release 5 kompatibel. Bei der Aktualisierung von Release 2 auf Release 5 sollten Sie jedoch hinsichtlich der Java-Clients folgende Kompatibilitätsaspekte berücksichtigen:

- Ein Release 5-Broker unterstützt Release 2-Clients (jedoch ohne zusätzliche Release 5-Funktionen).
- Ein Release 5-Java-Client kann eine Verbindung zu einem Release 2-Broker herstellen (jedoch ohne zusätzliche Release 5-Funktionen).
- C-Client-Programme werden mit einer Enterprise Edition-Lizenz oder einer Testlizenz der Platform Edition von Release 2-, Release 3- oder Release 4-Brokern unterstützt.

Aktualisierung der Release 2-Version von Message Queue

In diesem Abschnitt wird die vollständige Aktualisierung von Message Queue von Java ES Release 2 auf Java ES Release 5 beschrieben:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren der Release 2-Version von Message Queue \(Solaris\)](#)
- [Aktualisieren der Release 2-Version von Message Queue \(Linux\)](#)
- [Installation des Kompatibilitätspakets \(Linux\)](#)

- [Überprüfen der Message Queue-Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung der Message Queue-Software beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Message Queue-Abhängigkeiten aktualisieren](#)
- [Sichern Message Queue](#)

Aktuelle Versionsinformationen überprüfen

Um die Version und Ausgabe von Message Queue auf Ihrem System zu ermitteln, starten Sie den Message Queue-Broker mit der Option `-version`:

```
imqbrokerd -version
```

Tabelle 10-5 Message Queue-Ausgaben der Versionsüberprüfung

Java ES Release	Message Queue-Versionsnummer
Release 2	Sun Java(tm) System Message Queue 3 2004Q2 Version: 3.5
Release 3	Sun Java(tm) System Message Queue 3 2005Q1 Version: 3.6
Release 4	Sun Java(tm) System Message Queue 3 2005Q4 Version: 3.6 SP3
Release 5	Sun Java(tm) System Message Queue 3.7 Version: 3.7 UR1

Message Queue-Abhängigkeiten aktualisieren

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Für Message Queue bestehen nur zu ein paar gemeinsam genutzten Komponenten zwingende Aktualisierungsabhängigkeiten.

Wenn Sie die Message Queue-Abhängigkeiten aktualisieren, sollten Sie dies in der unten angegebenen Reihenfolge vornehmen, bevor Sie Message Queue aktualisieren. Überspringen Sie dabei die bereits aktualisierten Abhängigkeiten.

1. **Gemeinsam genutzte Komponenten.** Anleitungen für die Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie in [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#)).
2. **Sun Cluster (keine zwingende Abhängigkeit)** Anleitungen für die Aktualisierung von Sun Cluster auf Release 5 finden Sie in [Kapitel 3, „Sun Cluster-Software“ auf Seite 83](#).
3. **Directory Server (keine zwingende Abhängigkeit)** Anleitungen für die Aktualisierung von Directory Server auf Release 5 finden Sie in [Kapitel 5, „Directory Server“ auf Seite 109](#).
4. **Java DB (keine zwingende Abhängigkeit).** Sie müssen Java DB Release 5 neu installieren, wenn Sie Message Queue aktualisieren.
5. **Webcontainer-Software (keine zwingende Abhängigkeit).** Anweisungen zur Aktualisierung von Webserver und Anwendungsserver finden Sie in [Kapitel 7, „Webserver“ auf Seite 143](#) bzw. [Kapitel 11, „Anwendungsserver“ auf Seite 219](#).

Sichern Message Queue

Wenn Sie eine Aktualisierung durchführen, ist es stets empfehlenswert, Anwendungsdaten in einer Produktionsumgebung zu sichern. Unter Solaris OS werden dynamische Daten im folgenden Verzeichnis gespeichert:
`/var/imq/instances/instanceName`.

Weitere Informationen zu anderen Betriebssystemen finden Sie im *Message Queue 3.7 UR1 Administration Guide* unter <http://docs.sun.com/doc/819-4467>.

Aktualisieren der Release 2-Version von Message Queue (Solaris)

Bei der Aktualisierung von Message Queue-Software auf Java ES Release 5 wird das Skript `mqugrade` verwendet, mit dem die Release 5-Pakete installiert werden.

So führen Sie die Aktualisierung durch

1. Halten Sie sämtliche derzeit ausgeführten Message Queue-Client-Anwendungen an.

Wenn Message Queue in einer Anwendungsserver-Umgebung verwendet wird, beenden Sie Anwendungsserver ebenfalls.

2. Halten Sie sämtliche ausgeführten Broker an. Sie werden zur Eingabe des Admin-Benutzernamens und des zugehörigen Passworts aufgefordert:
`imqcmd shutdown bkr [-b hostName:port]`
3. Wenn Sie dynamische Daten, das Flatfile-Benutzer-Repository Message Queue und die der jeweiligen Broker-Instanz zugeordnete Message Queue-Zugriffssteuerungsdatei nicht beibehalten möchten, entfernen Sie diese Daten mit folgendem Befehl:
`imqbrokerd -name instanceName -remove instance`
 Andernfalls werden die dynamischen Daten und Konfigurationsinformationen beibehalten und für Release 5 Message Queue verwendet.
4. Melden Sie sich als Root-Benutzer an.
`su -`
5. Wechseln Sie in das Tools-Verzeichnis der Java ES Release 5-Verteilung.
Unter Solaris SPARC:
`cd Solaris_sparc/Product/message_queue/Tools`
Unter Solaris x86:
`cd Solaris_x86/Product/message_queue/Tools`
6. Führen Sie das Skript `mqupgrade` aus.
 - a. Starten Sie das Skript.
`./mqupgrade`
 Mithilfe des Skripts `mqupgrade` werden installierte Message Queue-Komponenten aufgelistet.
 - b. Geben Sie `y` (ja) ein, um die Message Queue-Komponenten zu aktualisieren.
 Mithilfe des Skripts `mqupgrade` werden installierte Lokalisierungsdateien ermittelt und aufgelistet.
 Wenn die Message Queue-Komponenten nicht aktualisiert werden sollen, geben Sie `n` (nein) ein. Mithilfe des Skripts `mqupgrade` wird der Vorgang beendet, ohne dass Message Queue-Komponenten aktualisiert werden.

- c. Geben Sie y (ja) ein, um Lokalisierungsdateien zu aktualisieren.

Vom mqupgrade-Skript wird eine Ausgabe an die Protokolldatei gesendet, die sich hier befindet:

```
/var/sadm/install/logs/Message_Queue_upgrade_'date'.log
```

Aktualisieren der Release 2-Version von Message Queue (Linux)

Die Aktualisierung von Release 2 Message Queue auf Release 5 auf der Linux-Plattform ist dadurch kompliziert, dass Java ES Release 2 nur auf RHEL 2.1 unterstützt wird, Java ES Release 5 jedoch nicht auf RHEL 2.1 unterstützt wird. Daher ist eine duale Aktualisierung erforderlich: Sowohl das Betriebssystem als auch Message Queue müssen aktualisiert werden. Siehe [„Duale Aktualisierungen: Java ES und Betriebssystem-Software“ auf Seite 48](#)

Bei der Basisvorgehensweise wird zuerst das Linux-Betriebssystem aktualisiert, anschließend werden sämtliche Message Queue-Abhängigkeiten und zuletzt Message Queue aktualisiert.

Die Aktualisierung von Message Queue Release 2 auf Release 5 beinhaltet einen Schritt für die Datenmigration, der bei Solaris-Systemen erforderlich ist, und zwar die Migration von Broker-Instanzdaten in das entsprechende Release 5-Verzeichnis. Wenn Sie Ihre Release 2-Daten bei der Aktualisierung auf Release 5 beibehalten möchten, führen Sie die Migration mit dem Migrationstool mqmigrate von Message Queue durch.

Um eine Aktualisierung von Release 2 auf Release 5 durchzuführen, folgen Sie den Anweisungen unter [„Aktualisieren der Release 2-Version von Message Queue \(Solaris\)“ auf Seite 212](#). Führen Sie jedoch das Skript mqmigrate ([Schritt 6 auf Seite 215](#)) wie folgt aus, bevor Sie das Skript mqupgrade ([Schritt 7 auf Seite 215](#)) ausführen:

1. Halten Sie sämtliche derzeit ausgeführten Message Queue-Client-Anwendungen an.
2. Halten Sie sämtliche ausgeführten Broker an. Sie werden zur Eingabe des Admin-Benutzernamens und des zugehörigen Passworts aufgefordert:

```
imqcmd shutdown bkr [-b hostName:port]
```

3. Wenn Sie dynamische Daten, das Flatfile-Benutzer-Repository Message Queue und die der jeweiligen Broker-Instanz zugeordnete Message Queue-Zugriffssteuerungsdatei nicht beibehalten möchten, entfernen Sie diese Daten mit folgendem Befehl:

```
imqbrokerd -name instanceName -remove instance
```

Andernfalls werden die dynamischen Daten und Konfigurationsinformationen beibehalten und für Release 5 Message Queue verwendet.

4. Melden Sie sich als Root oder Superuser an.

```
su -
```

5. Wechseln Sie in das Tools-Verzeichnis der Java ES Release 5-Verteilung.

```
cd Linux_x86/Product/message_queue/Tools
```

6. Migrieren Sie Broker-Instanzdaten mithilfe dieses Befehls:

```
./mqmigrate
```

Das Skript `mqmigrate` verschiebt die Konfigurationsdaten der Release 2-Broker-Instanz in das entsprechende Verzeichnis der Release 4-Version.

7. Führen Sie das Skript `mqupgrade` aus.

- a. Starten Sie das Skript.

```
./mqupgrade
```

Mithilfe des Skripts `mqupgrade` werden installierte Message Queue-Komponenten aufgelistet.

- b. Geben Sie y (ja) ein, um die Message Queue-Komponenten zu aktualisieren.

Mithilfe des Skripts `mqupgrade` werden installierte Lokalisierungsdateien ermittelt und aufgelistet.

Wenn die Message Queue-Komponenten nicht aktualisiert werden sollen, geben Sie n (nein) ein. Mithilfe des Skripts `mqupgrade` wird der Vorgang beendet, ohne dass Message Queue-Komponenten aktualisiert werden.

- c. Geben Sie y (ja) ein, um Lokalisierungsdateien zu aktualisieren.

Vom `mqupgrade`-Skript wird eine Ausgabe an die Protokolldatei gesendet, die sich hier befindet:

```
/var/sadm/install/logs/Message_Queue_upgrade_'date' .log
```

Installation des Kompatibilitätspakets (Linux)

Wenn Sie über Skripte verfügen, die vom Speicherort der installierten Release 5-Dateien abhängen, oder Ihre Release 2-Client-Anwendungen solche Skripte enthalten, müssen Sie das Paket `sun-mq-compat` installieren. Das Paket enthält Symlinks von den Speicherorten der Release 2-Dateien zu den Speicherorten der Release 5-Dateien.

Das `sun-mq-compat`-Paket befindet sich im nachfolgenden Verzeichnis, in das Sie die Java ES Release 5-Verteilung entzippt haben.

```
Linux_x86/Product/message_queue/Packages
```

So installieren Sie das `sun-mq-compat`-Paket

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Rufen Sie vom Paketverzeichnis aus folgenden Befehl auf:

```
rpm -ivh --nodeps sun-mq-compat-3.7-RelNo.i386.rpm
```

Überprüfen der Message Queue-Aktualisierung

Überprüfen Sie nach Durchführung des Aktualisierungsverfahrens, ob die Aktualisierung erfolgreich war, indem Sie den Message Queue-Broker mit der Option `-version` starten.

```
imqbrokerd -version
```

Der Befehl gibt die Java ES Versionsnummer sowie die Message Queue-spezifische Versionsnummer zurück.

Aufgaben nach der Aktualisierung

Wenn Sie das HTTP-Tunneling-Servlet verwenden, um Unterstützung für den HTTP-Verbindungsdienst bereitzustellen, wurde das Servlet bei der Message Queue-Aktualisierung von Release 2 auf Release 5 aktualisiert. Das heißt, Sie müssen das Servlet nach der Aktualisierung von Message Queue auf Release 5 erneut bereitstellen. Weitere Informationen zur HTTP-Unterstützung finden Sie im *Message Queue 3.7 UR1 Administration Guide* unter <http://docs.sun.com/doc/819-4467>.

Sie müssen darüber hinaus mithilfe der Administrationskonsole (`imqadmin`) die verwalteten Release 2-Objekte in die Release 5-Versionen migrieren und/oder führen Sie mit dem ObjectManager-Befehlszeilendienstprogramm (`imqobjmgr`) eine Aktualisierung durch.

Aufheben der Aktualisierung

Die Aktualisierung von Message Queue von Release 2 auf Release 5 wird zurzeit nicht unterstützt. Das hierfür angewendete Verfahren entspräche normalerweise dem Zurücksetzen der Release 5-Aktualisierung auf Release 4 (siehe „[Aufheben der Aktualisierung](#)“ auf Seite 204). Da jedoch die Java ES-Produktregistrierung durch die Aktualisierung von Message Queue von Release 2 auf Release 5 nicht aktualisiert wird, kann Message Queue Release 2 vom Java ES-Installationsprogramm nicht neu installiert werden.

Um dieses Problem zu umgehen, wenden Sie sich an die Sun Services.

Aktualisierung mehrerer Instanzen

Um ein Message Queue-Cluster zu aktualisieren, in dem mehrere Broker zusammenarbeiten, um einen skalierbaren Meldungsdienst bereitzustellen, können Sie ein Rolling Upgrade durchführen, bei dem der Cluster online bleibt, während die einzelnen Message Queue-Instanzen nacheinander von Release 2 auf Release 5 aktualisiert werden. Beachten Sie bei der Aktualisierung eines Clusters die folgenden zwei Bedingungen:

- Solange ein Broker für die Aktualisierung heruntergefahren ist, sind die vom Broker gespeicherten persistenten Meldungen nicht verfügbar. Die Meldungen sind erst dann wieder verfügbar, wenn der Broker neu gestartet wurde.
- Der Master-Broker sollte als letzter aktualisiert werden.

Andernfalls handelt es sich um ein unkompliziertes Verfahren: Sie beenden, aktualisieren und starten die einzelnen Broker nacheinander neu, bis alle Broker aktualisiert sind.

Aktualisieren der Message Queue Release 2-Version aus Java ES-Release 2

Anwendungsserver

In diesem Kapitel wird die Aktualisierung von Anwendungsserver auf Java ES 5 (Release 5) beschrieben: Sun Java System Anwendungsserver Enterprise Edition 8.2.

Das Kapitel enthält einen Überblick über die Aspekte der verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Anwendungsserver“ auf Seite 221
- „Aktualisieren von Anwendungsserver von Java ES Release 4“ auf Seite 227
- „Aktualisieren von Anwendungsserver von Java ES Release 3“ auf Seite 233
- „Aktualisieren von Anwendungsserver von Java ES Release 2“ auf Seite 234
- „Aktualisierung der im Lieferumfang von Solaris enthaltenen Anwendungsserver-Version in einer Solaris 10-Multi-Zone-Umgebung“ auf Seite 245

HINWEIS Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf Verzeichnispfade, die im Folgenden als *AppServer8-base* und *AppServer8Config-base* (Anwendungsserver 8. x), *AppServer7-base* und *AppServer7Config-base* (Anwendungsserver 7.x) angegeben werden. Bei der Installation von Anwendungsserver wurden diese Pfade mindestens teilweise als Installationsverzeichnisse oder Domänenverzeichnisse angegeben. Wenn nicht, wurde vom Java ES-Installationsprogramm ein Standardwert zugewiesen. Die Standardwerte für diese Verzeichnispfade sind in der folgenden Tabelle aufgelistet.

Tabelle 11-1 Anwendungsserver Verzeichnispfade

Variable des Pfadnamens	Solaris OS	Linux OS
<i>AppServer8-base</i>	/opt/SUNWappserver/appserver	/opt/sun/appserver
<i>AppServer8Install-base</i>	/opt/SUNWappserver	/opt/sun/appserver
<i>AppServer8Config-base</i>	/var/opt/SUNWappserver	/var/opt/sun/appserver
<i>AppServer7-base</i>	/opt/SUNWappserver7	/opt/SUNWappserver7
<i>AppServer7Config-base</i>	/var/opt/SUNWappserver7	/var/opt/SUNWappserver7

HINWEIS Der standardmäßige Anwendungsserver-Domänenname für Release 5 Anwendungsserver (8.x) lautet `domain1`. Demnach ist `domain1` der Standardwert für die in diesem Kapitel verwendete Variable *domainName*.

Zusätzlich lautet der standardmäßige Directory Administration Service (DAS)-Objektnamen `server`. J2EE-Anwendungen werden in der Regel nicht in der DAS-Instanz, sondern in anderen Standalone-Instanzen eingesetzt.

Weitere Informationen über die in diesem Kapitel verwendeten `asadmin`-Befehle finden Sie im *Sun Java System Application Server Enterprise Edition 8.2 Reference Manual*,
<http://docs.sun.com/doc/819-4736>.

Überblick über Aktualisierungen von Anwendungsserver

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Anwendungsserver auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5 Anwendungsserver](#)
- [Anwendungsserver Wegweiser für die Aktualisierung von](#)
- [Anwendungsserver-Daten](#)
- [Anwendungsserver Vorgehensweise zur Aktualisierung von](#)

Über Java ES Release 5 Anwendungsserver

Java ES Release 5 Anwendungsserver stellt eine Minor-Release in Bezug auf Release 4 dar und enthält nur ausgewählte Fehlerkorrekturen. Die Funktionalität der Release 5-Version von Anwendungsserver ist mit der Release 4-Version identisch.

Anwendungsserver Wegweiser für die Aktualisierung von

Es stehen zwei Wege für die Aktualisierung von Anwendungsserver auf Java ES Release 5 zur Verfügung:

- [Tabelle 11-2](#) zeigt die unterstützten Wege für die Aktualisierung von Java ES Anwendungsserver auf Java ES Release 5. Die Tabelle gilt sowohl für das Solaris- als auch für das Linux-Betriebssystem.
- [Tabelle 11-3](#) stellt die unterstützten Wege für die Aktualisierung von dem im Lieferumfang von Solaris enthaltenen Anwendungsserver auf Java ES Release 5 dar. Anwendungsserver Plattform Edition ist im Lieferumfang der Solaris-Betriebssystemsoftware enthalten. Die Aktualisierung der im Lieferumfang enthaltenen Versionen von Anwendungsserver auf Release 5 Enterprise Edition kann mithilfe des Java ES-Installationsprogramms durchgeführt werden, wie aus [Tabelle 11-3](#) ersichtlich.

Tabelle 11-2 Wege für die Aktualisierung auf Java ES 5 (Release 5): Anwendungsserver Enterprise Edition 8.2

Java ES Release	Anwendungsserver Version	Allgemeiner Ansatz	Neukonfiguration erforderlich
Release 4	Sun Java System Anwendungsserver Enterprise Edition 8.1 2005Q4	Direkte Aktualisierung: Durch Anwendung des Java ES-Installationsprogramms. ¹	Keine
Release 3	Sun Java System Anwendungsserver Enterprise Edition 8.1 2005Q1	Direkte Aktualisierung: Durch Anwendung des Java ES-Installationsprogramms.	Keine
Release 2	Sun Java System Anwendungsserver 7.0 Update 3 (2004Q2) Platform und Enterprise Edition	Direkte Aktualisierung: Verwenden Sie das Java ES-Installationsprogramm für die Aktualisierung von Paketen, das Skript postInstall für die Neukonfiguration und das Dienstprogramm asupgrade für die Migration von Domänendaten. ²	Umgebungsvariablen, Domänen und andere Konfigurationsdaten Die J2EE-Komponenten und -Anwendungen müssen in die neue Anwendungsserver-Umgebung migriert und erneut bereitgestellt werden.
Release 1	Sun ONE Anwendungsserver 7.0 Update 1 (2003Q4) Platform und Enterprise Edition	Direkte Aktualisierung nicht zertifiziert. Verwenden Sie denselben Ansatz wie für die Aktualisierung von Release 2 Anwendungsserver.	Umgebungsvariablen, Domänen und andere Konfigurationsdaten Die J2EE-Komponenten und -Anwendungen müssen in die neue Anwendungsserver-Umgebung migriert und erneut bereitgestellt werden.
Versionen vor Java ES		Keine direkte Aktualisierung: Sie können jedoch zunächst auf Release 3 aktualisieren, wie im <i>Java Enterprise System 2005Q1 Aktualisierungs- und Migrationshandbuch</i> (http://docs.sun.com/doc/819-0062) beschrieben. Führen Sie anschließend eine Aktualisierung von Release 3 auf Release 5 durch.	

1. Wenn Sie Anwendungsserver von Release 4 auf Release 5 aktualisieren möchten, ohne die Konfigurations- oder Domänenendaten beizubehalten, können Sie das Deinstallationsprogramm für Java ES Release 4 verwenden, um Release 4 Anwendungsserver zu deinstallieren, und anschließend das Installationsprogramm für Java ES Release 5 verwenden, um Release 5 Anwendungsserver neu zu installieren. Wenn Release 4 Anwendungsserver jedoch mit der Option „Später konfigurieren“ installiert wurde, müssen Sie vor der Deinstallation von Release 4 Anwendungsserver erst die Datei `$HOME/.asadminprefs` erstellen (wobei es sich bei `$HOME` um das Basisverzeichnis des Benutzers handelt, der Anwendungsserver installiert und ausführt). Die Datei verfügt über die folgenden zwei Zeilen:
- ```
AS_ADMIN_PASSWORD=password
AS_ADMIN_USER=admin
```
2. Besondere Vorsicht ist bei der Aktualisierung von Release 2 Anwendungsserver auf einer Solaris-Plattform erforderlich, da sowohl der im Lieferumfang von Solaris enthaltene Anwendungsserver als auch Java ES Release 2 Anwendungsserver auf dem Computer vorhanden sind. Siehe [Tabelle 11-3](#) sowie der darauf folgende Hinweis.

**Tabelle 11-3** Aktualisierungswege für Anwendungsserver Versionen im Lieferumfang des Solaris-Betriebssystems

| Solaris OS Version | Anwendungsserver Version                                    | Allgemeiner Ansatz                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Neukonfiguration erforderlich                                                                                                                                                                                    |
|--------------------|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Solaris 10         | Sun Java System Anwendungsserver Plattform Edition 8.0.0_01 | Direkte Aktualisierung:<br>Durch Anwendung des Java ES-Installationsprogramms.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Keine.                                                                                                                                                                                                           |
| Solaris 9          | Sun Java System Anwendungsserver 7.0.0_03c                  | Direkte Aktualisierung:<br><br>Wenn Anwendungsserver <i>verwendet wurde</i> und Domänen erstellt wurden, müssen die Domänenendaten migriert werden. Verwenden Sie den für die Aktualisierung von Release 2 Anwendungsserver dargestellten Ansatz, bei dem Sie die Option „Später konfigurieren“ des Java ES-Installationsprogramms, das Skript <code>postInstall</code> und das Dienstprogramm <code>asupgrade</code> einsetzen.<br><br>Wenn Anwendungsserver <i>nicht</i> oder ohne Erstellung von Domänen verwendet wurde, verwenden Sie den Ansatz wie für die Aktualisierung von Release 2 Anwendungsserver dargestellt. Verwenden Sie dabei jedoch die Option „Jetzt konfigurieren“ des Java ES-Installationsprogramms und verwenden Sie nicht das Skript <code>postInstall</code> oder das Dienstprogramm <code>asupgrade</code> . | Umgebungsvariablen, Domänen (falls erstellt) und andere Konfigurationsdaten<br><br>Die J2EE-Komponenten und -Anwendungen müssen in die neue Anwendungsserver-Umgebung migriert und erneut bereitgestellt werden. |

**HINWEIS** Besondere Vorsicht ist bei der Aktualisierung von Release 2 Anwendungsserver auf einer Solaris-Plattform geboten, da sowohl die im Lieferumfang enthaltene Version als auch die Java ES-Version von Anwendungsserver auf dem Computer vorhanden sind. Dadurch müssen Sie erst die im Lieferumfang enthaltene Version (und alle damit verbundenen Domänen) deinstallieren, bevor Sie mit der Aktualisierung von der Release 2-Version fortfahren. Siehe auch „[Nur Solaris: Entfernen Sie manuell die im Betriebssystem enthaltenen Anwendungsserver-Pakete.](#)“ auf Seite 236.

## Anwendungsserver-Daten

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Anwendungsserver-Software betroffen sein können.

**Tabelle 11-4** Anwendungsserver Verwendung der Daten

| Datentyp                  | Standort                                                                                                                                                                                                                                                                                           | Verwendung                                                                                 |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Umgebungsvariablen        | <i>AppServer8-base/config/asenv.conf</i>                                                                                                                                                                                                                                                           | Globale Variablen                                                                          |
| Konfigurationsdaten       | Release 3, Release 4 & Release 5:<br>Datei <i>domain.xml</i> und <i>server.policy</i> in<br><i>AppServer8Config-base/domains/domainName/config</i><br><br>Release 2:<br>Datei <i>server.xml</i> und <i>server.policy</i> in<br><i>AppServer7Config-base/domains/domainName/instanceName/config</i> | Konfiguration der<br>Anwendungsserver-Instanzen                                            |
| Bereitstellungsdaten      | Release 3, Release 4 & Release 5:<br><i>AppServer8Config-base/domains/domainName/applications</i><br><br>Release 2:<br><i>AppServer7Config-base/domains/domainName/instanceName/applications</i>                                                                                                   | Konfiguration des<br>J2EE-Containers für bestimmte<br>J2EE-Komponenten und<br>-Anwendungen |
| Zugriffsprotokoll-Dateien | Release 3, Release 4 & Release 5:<br><i>AppServer8Config-base/domains/domainName/logs/access/</i><br>Enthält zwei Dateien:<br><i>server_acces_log</i> und <i>_asadmin_access_log</i><br><br>Release 2:<br><i>AppServer7Config-base/domains/domainName/instanceName/logs/access</i>                 | Zugriffsprotokollierung                                                                    |

# Anwendungsserver Vorgehensweise zur Aktualisierung von

Ihre Vorgehensweise bei der Aktualisierung von Anwendungsserver hängt grundsätzlich von den zahlreichen in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) erläuterten Aspekten ab: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

Dieser Abschnitt konzentriert diese grundsätzliche Erläuterung auf Anwendungsserver, indem Probleme dargestellt werden, die möglicherweise Ihren Aktualisierungsplan für Anwendungsserver beeinflussen.

## Kompatibilität

In der Release 5-Version von Anwendungsserver wurden seit Release 4 oder Release 3 keine Änderungen an der Schnittstelle vorgenommen. Es bestehen jedoch grundsätzliche Änderungen der Schnittstelle der Release 5-Version zu Release 2, sodass Release 5 nicht mit Release 2 kompatibel ist.

Release 5 Anwendungsserver unterstützt jedoch nicht Release 4 Service Registry. Wenn Anwendungsserver auf Release 5 aktualisiert wird, muss Service Registry ebenfalls auf Release 5 aktualisiert werden.

## Anwendungsserver-Abhängigkeiten

Anwendungsserver-Abhängigkeiten zu anderen Java ES-Komponenten beeinflussen möglicherweise das Verfahren für die Aktualisierung und Neukonfiguration der Anwendungsserver-Software. Änderungen der Anwendungsserver-Schnittstellen oder -Funktionen könnten beispielsweise aktualisierte Versionen der Komponenten erforderlich machen, von denen Anwendungsserver abhängig ist. Welche dieser Komponenten aktualisiert werden müssen, hängt von dem jeweiligen Aktualisierungsweg ab.

Für Anwendungsserver bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Anwendungsserver ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)).
- **Message Queue.** Anwendungsserver ist von Message Queue abhängig, um Unterstützung für asynchrones Messaging zu bieten, das mit J2EE Java Message Service kompatibel ist.

- **High Availability Session Store.** Anwendungsserver hängt von High Availability Session Store ab, um Sitzungsstatusinformationen zu verwalten, die für das Failover zwischen den Instanzen erforderlich sind.

---

**HINWEIS** Wenn Sie über eine ältere Installation von Anwendungsserver verfügen, die nicht HADB erfordert, muss HADB installiert werden, bevor Sie Anwendungsserver auf Release 5 aktualisieren können. Release 5 HADB muss beispielsweise installiert werden, um die Anwendungsserver-Versionen im Lieferumfang des Solaris-Betriebssystems zu aktualisieren. Das Java ES-Installationsprogramm führt in diesen Situationen automatisch die Installation von HADB durch.

---

- **Java Database.** Anwendungsserver erfordert Java Database als Standard-Entwicklerdatenbank und zur Speicherung von Beispielanwendungsdaten, die für Enterprise Java Beans-Timer benötigt werden.
- **Webcontainer (optionale Abhängigkeit).** Anwendungsserver ist von Webcontainerdiensten für das optionale Lastenausgleichs-Plug-In von Anwendungsserver abhängig. Diese Unterstützung kann entweder durch Java ES Webserver- oder Drittanbieter-Webcontainer (wie z. B. Apache, Webserver und Microsoft IIS) gewährleistet werden.



# Aktualisieren von Anwendungsserver von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von Anwendungsserver von Java ES 2005Q4 (Release 4) auf Java ES 5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 4-Version von Anwendungsserver](#)

## Einführung

Berücksichtigen Sie bei der Aktualisierung von Anwendungsserver von Java ES Release 4 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt mithilfe des Java ES-Installationsprogramms. Bei der Aktualisierung der Release 4-Version von Anwendungsserver auf Release 5 ist keine Neukonfiguration von Anwendungsserver und keine Neukonfiguration oder Migration der J2EE-Komponenten erforderlich.
- **Aktualisierungsabhängigkeiten.** Anwendungsserver ist von einer Reihe von gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)), die alle automatisch vom Java ES-Installationsprogramm auf Release 5 aktualisiert werden, wenn Sie eine Aktualisierung von Anwendungsserver durchführen. Anwendungsserver ist nur von der gemeinsam genutzten Komponente NSS zwingend abhängig.

Des Weiteren ist Release 5 Anwendungsserver wie in „[Anwendungsserver-Abhängigkeiten](#)“ auf [Seite 225](#) beschrieben von Message Queue, HADB und Java DB abhängig. Hierbei handelt es sich um zwingende Abhängigkeiten. Alle Komponenten müssen auf Release 5 aktualisiert werden.

Des Weiteren ist Anwendungsserver optional abhängig von Java ES Webserver oder Drittanbieter-Webcontainern. Hierbei handelt es sich jedoch nicht um zwingende Aktualisierungsabhängigkeiten; eine Aktualisierung der Webcontainer ist hinsichtlich der Aktualisierung von Anwendungsserver auf Release 5 optional.

- **Rückwärtskompatibilität.** Die Rückwärtskompatibilität von Anwendungsserver Release 5 zu Release 4 ist gewährleistet.

- **Aufheben der Aktualisierung.** Die Aktualisierung auf Release 5 kann nicht auf Release 4 zurückgesetzt werden.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Anwendungsserver ist für das Solaris- und Linux-Betriebssystem identisch.

## Aktualisierung der Release 4-Version von Anwendungsserver

In diesem Abschnitt wird die Aktualisierung von Anwendungsserver von Java ES Release 4 auf Java ES Release 5 unter Solaris und Linux beschrieben. Plattformspezifische Vorgänge sind durch die Angabe des jeweiligen Betriebssystems, auf das sich der Vorgang bezieht, gekennzeichnet. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren von Release 4 von Anwendungsserver](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

### Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung der Anwendungsserver-Software beginnen, führen Sie die folgenden Aufgaben durch.

- [Aktuelle Versionsinformationen überprüfen](#)
- [Anwendungsserver-Abhängigkeiten aktualisieren](#)
- [Anwendungsserver-Daten sichern](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

#### *Aktuelle Versionsinformationen überprüfen*

Sie können die aktuelle Version von Anwendungsserver durch Eingabe des folgenden Befehls überprüfen:

```
AppServer8-base/bin/asadmin version --verbose
```

**Tabelle 11-5** Anwendungsserver Ausgaben der Versionsüberprüfung

| Java ES Release | Anwendungsserver-Versionsnummer                                       |
|-----------------|-----------------------------------------------------------------------|
| Release 2       | Sun ONE Anwendungsserver 7.0.0_03c                                    |
| Release 3       | Sun Java Enterprise System Anwendungsserver Enterprise Edition 8.1    |
| Release 4       | Sun Java Enterprise System Anwendungsserver Enterprise Edition 8.1_02 |
| Release 5       | Sun Java Enterprise System Anwendungsserver Enterprise Edition 8.2    |

### *Anwendungsserver-Abhängigkeiten aktualisieren*

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Für Anwendungsserver besteht eine zwingende Aktualisierungsabhängigkeit zu gemeinsam genutzten NSS-Komponenten und zu Message Queue, HADB und Java DB-Produktkomponenten.

Wenn Sie die Anwendungsserver-Abhängigkeiten aktualisieren, sollten Sie dies in der unten angegebenen Reihenfolge vornehmen, bevor Sie Anwendungsserver aktualisieren. Überspringen Sie dabei die bereits aktualisierten Abhängigkeiten. Die Aktualisierung von gemeinsam genutzten Komponenten sowie Message Queue, HADB und Java DB wird jedoch normalerweise automatisch bei der Aktualisierung von Anwendungsserver durch das Java ES-Installationsprogramm vorgenommen.

- 1. Gemeinsam genutzte Komponenten.** Anleitungen für die Synchronisierung von gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie unter [„Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#). Alle gemeinsam genutzten Komponenten, die von Anwendungsserver benötigt werden, werden jedoch automatisch vom Java ES-Installationsprogramm aktualisiert, wenn Sie eine Aktualisierung von Anwendungsserver auf Release 5 durchführen.
- 2. Message Queue.** Anleitungen für die Aktualisierung von Message Queue auf Release 4 finden Sie in [Kapitel 10, „Message Queue“ auf Seite 193](#).
- 3. High Availability Session Store (HADB).** Anleitungen für die Aktualisierung von HADB finden Sie in [Kapitel 9, „High Availability Session Store“ auf Seite 179](#).

4. **Java DB.** Anweisungen zur Aktualisierung von Java DB finden Sie in [Kapitel 8, „Java DB“](#) auf Seite 171.
5. **Webcontainer-Software (keine zwingende Abhängigkeit).** Anweisungen zur Aktualisierung von Webserver finden Sie in [Kapitel 7, „Webserver“](#) auf Seite 143.

### *Anwendungsserver-Daten sichern*

Bei der Anwendungsserver-Aktualisierung von Release 4 auf Release 5 werden keine Konfigurationsdaten geändert. Eine Sicherung der aktuellen Daten ist daher nicht erforderlich.

### *Erforderliche Konfigurationsinformationen und Passwörter abrufen*

Sie sollten über die Benutzer-ID und das Passwort des Administrators der aktuell installierten Version von Anwendungsserver verfügen.

## Aktualisieren von Release 4 von Anwendungsserver

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Anwendungsserver haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung*

Bei der Aktualisierung der Anwendungsserver-Software auf Java ES Release 5 müssen folgende Aspekte berücksichtigt werden:

- Bevor Sie eine Anwendungsserver-Instanz aktualisieren, sollten sämtliche in dieser Instanz ausgeführten J2EE-Komponenten beendet werden. Diese Anforderung ist hinfällig, wenn Lastenausgleich für Hochverfügbarkeit oder Skalierbarkeit eingesetzt wird.
- Alle Anwendungsserver-Instanzen, die auf einem einzelnen Computer ausgeführt werden (wobei alle Instanzen demselben installierten Anwendungsserver-Image entsprechen), müssen vor der Aktualisierung des installierten Image beendet werden.
- In Bereitstellungen mit mehreren Knoten, führen Sie das Aktualisierungsverfahren auf jedem Knoten oder Computer durch, der als Host für die Anwendungsserver-Instanzen dient.

### *Aktualisierungsverfahren*

Das im Folgenden beschriebene Verfahren ist für Anwendungsserver-Instanzen anzuwenden, die lokal auf dem Computer ausgeführt werden, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

`su -`

2. Beenden Sie alle J2EE-Komponenten, die in den zu aktualisierenden Anwendungsserver-Instanzen ausgeführt werden.
3. Beenden Sie alle Anwendungsserver-Instanzen auf dem zu aktualisierenden Computer.

- a. Beenden Sie alle laufenden Knotenagenten.

```
AppServer8-base/bin/asadmin stop-node-agent --user admin_ID
nodeagentName
```

wobei *nodeagentName* der Form *hostName\_domainName* entspricht, jedoch standardmäßig nur *hostName* lautet.

- b. Halten Sie den Domain Administration Server (DAS) an.

```
AppServer8-base/bin/asadmin stop-domain --user admin_ID
domainName
```

- c. Halten Sie den PointBase-Datenbankserver an (falls verwendet).

```
AppServer8Config-base/appserver/pointbase/tools/stopserver.sh
```

4. Starten Sie das Java ES-Installationsprogramm.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

wobei *os\_arch* der Plattform entspricht, wie z. B. *Solaris\_sparc*. (Verwenden Sie die Option `installer -nodisplay` für die Befehlszeilenschnittstelle.)

Nach der Willkommenseite sowie der Lizenzvereinbarung wird eine Seite für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten erkannt werden, die direkt vom Java ES-Installationsprogramm aktualisiert werden können, wird der Status als „aktualisierbar“ angezeigt.)

5. Wählen Sie auf der Seite für die Komponentenauswahl Anwendungsserver.

Da die Aktualisierung zwingend notwendig ist, werden Message Queue, HADB und Java DB ebenfalls automatisch für eine Aktualisierung ausgewählt.

6. Wählen Sie die Option „Jetzt konfigurieren“.

7. Geben Sie die erforderlichen Konfigurationswerte an.

Es werden eine Reihe von Konfigurationsbereichen angezeigt.

8. Bestätigen Sie Ihre Auswahl für die Aktualisierung.

Anwendungsserver Pakete (und, falls erforderlich, Pakete für Message Queue, HADB und Java DB) werden aktualisiert. Anschließend wird eine Aktualisierungszusammenfassung angezeigt.

9. Beenden Sie das Java ES-Installationsprogramm.

10. Starten Sie den Domain Administration Server (DAS) neu.

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
domainName
```

11. Starten Sie die aktualisierten Anwendungsserver-Instanzen neu.

```
AppServer8-base/bin/asadmin start-node-agent --user admin_ID
nodeagentName
```

wobei *nodeagentName* der Form *hostName\_domainName* entspricht, jedoch standardmäßig nur *hostName* lautet.

## Überprüfen der Aktualisierung

Mithilfe des folgenden Befehls können Sie überprüfen, ob die Aktualisierung erfolgreich war:

```
AppServer8-base/bin/asadmin version --verbose
```

Ausgabewerte finden Sie in [Tabelle 11-5 auf Seite 229](#).

## Aufgaben nach der Aktualisierung

Wenn Sie weiterhin die integrierte Release 4 PointBase-Datenbank statt Java DB, einer neuen Release 5 Java ES-Produktkomponente, verwenden möchten, müssen Sie die aktualisierte Datei *AppServer8-base/config/asenv.conf* manuell bearbeiten.

Nach der Aktualisierung von Application Server von Release 4 lauten die PointBase-Einstellungen in *asenv.conf* wie folgt:

```
AS_POINTBASE="%POINTBASE_HOME%"
AS_POINTBASE_SAMPLESDB="%POINTBASE_SAMPLESDB%"
```

Ändern Sie diese Einstellungen in die folgenden Werte:

```
AS_POINTBASE="AppServer8-base/pointbase"
AS_POINTBASE_SAMPLESDB="AppServerConfig8-base/var/appserver/pointbase"
```

## Aufheben der Aktualisierung

Die Aktualisierung auf Release 5 kann nicht aufgehoben werden.

# Aktualisieren von Anwendungsserver von Java ES Release 3

Die Vorgehensweise für die Aktualisierung von Java ES 2005Q1 (Release 3) Anwendungsserver auf Release 5 ist mit der Aktualisierung von Release 4 Anwendungsserver auf Release 5 identisch.

Um die Release 3-Version von Anwendungsserver auf Release 4 zu aktualisieren, folgen Sie den Anweisungen unter „[Aktualisieren von Anwendungsserver von Java ES Release 4](#)“ auf Seite 227. Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 3.

# Aktualisieren von Anwendungsserver von Java ES Release 2

Dieser Abschnitt enthält Informationen zur Aktualisierung von Anwendungsserver von Java ES (Release 2) auf Java ES 5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 2-Version von Anwendungsserver](#)

## Einführung

Berücksichtigen Sie bei der Aktualisierung von Anwendungsserver von Java ES Release 2 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch die Installation der Release 5-Version von Anwendungsserver mithilfe des Java ES-Installationsprogramms unter Auswahl der Option „Später konfigurieren“. Die Neukonfiguration wird anschließend mithilfe des Dienstprogramms `asupgrade` durchgeführt. Nach der Aktualisierung von Anwendungsserver müssen Sie die Release 2 J2EE-Komponenten und -Anwendungen in Release 5 migrieren.
- **Aktualisierungsabhängigkeiten.** Die Aktualisierung einer Java ES-Komponente auf einem Computer von Release 2 erfordert eine Aktualisierung aller übrigen Java ES-Komponenten, die sich auf diesem Computer befinden. Die Auswahl einzelner Java ES-Komponenten bei einer Aktualisierung von Release 2 auf Release 5 wird nicht unterstützt.

Insbesondere alle für Anwendungsserver erforderlichen gemeinsam genutzten Java ES-Komponenten müssen aktualisiert werden. Wenn sich Message Queue auf dem gleichen Computer befindet, muss dies ebenfalls aktualisiert werden. High Availability Session Store (HADB) und Java DB müssen installiert werden. Wenn Webserver für den Lastenausgleich verwendet wird, muss dies ebenfalls aktualisiert werden.

- **Rückwärtskompatibilität.** Die Release 5-Version von Anwendungsserver ist nicht rückwärts kompatibel zur Release 2-Version. J2EE-Komponenten und -Anwendungen müssen für die Ausführung in einer Release 5 Anwendungsserver-Umgebung migriert werden.



- **Aufheben der Aktualisierung.** Das Zurücksetzen der Release 5-Aktualisierung auf Release 2 erfolgt durch das einfache Zurückkehren zur Release 2-Installation (bei der Aktualisierung wurden keine Release 2-Konfigurationsdaten entfernt).
- **Plattformspezifische Aspekte.** Der Ansatz zur Aktualisierung von Anwendungsserver auf dem Solaris-Betriebssystem kann nicht direkt auf das Linux-Betriebssystem angewendet werden: Java ES Release 2 wird nur auf Linux 2.1 unterstützt, während Java ES Release 5 auf Linux 2.1 nicht unterstützt wird. Daher ist eine duale Aktualisierung erforderlich: Sowohl das Betriebssystem als auch Anwendungsserver müssen aktualisiert werden (siehe „[Duale Aktualisierungen: Java ES und Betriebssystem-Software](#)“ auf Seite 48).
- **Speicherorte der Daten.** Release 5 verfügt über neue Speicherorte für Konfigurationsdaten, Bereitstellungsdaten und Zugriffs-Protokolldateien. Eine Auflistung finden Sie in [Tabelle 11-4 auf Seite 224](#).

## Aktualisierung der Release 2-Version von Anwendungsserver

In diesem Abschnitt wird die Aktualisierung von Anwendungsserver von Java ES Release 2 auf Java ES Release 5 unter Solaris und Linux beschrieben. Plattformspezifische Vorgänge sind durch die Angabe des jeweiligen Betriebssystems, auf das sich der Vorgang bezieht, gekennzeichnet. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren der Release 2-Version von Anwendungsserver \(Solaris\)](#)
- [Aktualisieren der Release 2-Version von Anwendungsserver \(Linux\)](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

### Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung von Anwendungsserver beginnen, führen Sie die folgenden Aufgaben durch.

- [Nur Solaris: Entfernen Sie manuell die im Betriebssystem enthaltenen Anwendungsserver-Pakete.](#)

- [Aktuelle Versionsinformationen überprüfen](#)
- [Anwendungsserver-Abhängigkeiten aktualisieren](#)
- [Anwendungsserver-Daten sichern](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

*Nur Solaris: Entfernen Sie manuell die im Betriebssystem enthaltenen Anwendungsserver-Pakete.*

Durch die Installation von Release 2 Anwendungsserver wird nicht die im Solaris-Betriebssystem enthaltene Version von Anwendungsserver entfernt. Um Anwendungsserver vollständig von Release 2 auf Release 5 zu aktualisieren, müssen Sie die folgenden Schritte durchführen.

1. Deinstallieren Sie die im Betriebssystem enthaltene Version, indem Sie die entsprechenden Anwendungsserver-Pakete im Verzeichnis `/usr/appserver` manuell entfernen:

```
pkgrm SUNWascmnse SUNWaslb SUNWasut ...
```

wobei mit folgendem Befehl auf alle Pakete zugegriffen werden kann:

```
pkginfo -i|grep -i „application server“
```

Das Ergebnis enthält Pakete wie z. B.:

```
SUNWasacee, SUNWascmnse, SUNWasu, SUNWasuee, SUNWasac, SUNWascmn,
SUNWasdb, SUNWasdem, SUNWasdemdb, SUNWasr, SUNWasut, SUNWasman,
SUNWasjdoc
```

und enthält möglicherweise auch Lokalisierungspakete:

```
SUNWLocaleasacee, SUNWLocaleascmnse, SUNWLocaleasu, SUNWLocaleasuee
```

2. Wenn die im Lieferumfang enthaltene Version verwendet wurde, müssen Sie die Domäneninformationen löschen:

```
rm /usr/appserver/domains
```

### *Aktuelle Versionsinformationen überprüfen*

Sie können die aktuelle Version von Anwendungsserver durch Eingabe des folgenden Befehls überprüfen:

```
AppServer7-base/bin/asadmin version --verbose
```

Ausgabewerte finden Sie in [Tabelle 11-5 auf Seite 229](#).

### *Anwendungsserver-Abhängigkeiten aktualisieren*

Die Aktualisierung von Anwendungsserver-Abhängigkeiten erfordert die Aktualisierung auf Release 5 aller lokalen Release 2-Komponenten, von denen Anwendungsserver abhängig ist, insbesondere Message Queue sowie gemeinsam genutzte Komponenten. Gemeinsam genutzte Komponenten werden jedoch automatisch vom Java ES-Installationsprogramm als Teil des Aktualisierungsvorgangs aktualisiert (siehe „[Aktualisierungsverfahren](#)“ auf Seite 239).

Die Aktualisierung von Anwendungsserver erfordert zusätzlich die Installation von HADB und Java DB, von denen Release 5 Anwendungsserver abhängig ist. Diese Produktkomponenten werden jedoch automatisch vom Java ES-Installationsprogramm als Teil des Aktualisierungsvorgangs ausgewählt und installiert (siehe „[Aktualisierungsverfahren](#)“ auf Seite 239).

Grundsätzlich sollte bei einer Aktualisierung der Anwendungsserver-Abhängigkeiten in der unten angegebenen Reihenfolge vorgegangen werden (unter Auslassung der bereits aktualisierten Abhängigkeiten), bevor Sie Anwendungsserver aktualisieren. Die Aktualisierung von gemeinsam genutzten Komponenten sowie die Installation von HADB und Java DB wird jedoch automatisch bei der Aktualisierung von Anwendungsserver durch das Java ES-Installationsprogramm vorgenommen.

1. **Gemeinsam genutzte Komponenten.** Anleitungen für die Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie unter „[Aktualisieren der gemeinsam genutzten Java ES-Komponenten](#)“ auf Seite 71. Alle gemeinsam genutzten Komponenten, die von Anwendungsserver benötigt werden, werden jedoch automatisch vom Java ES-Installationsprogramm aktualisiert, wenn Sie eine Aktualisierung von Anwendungsserver auf Release 5 durchführen.

---

**HINWEIS** Die Aktualisierung gemeinsam genutzter Komponenten auf Release 5 enthält die Aktualisierung von J2SE auf JDK Version 1.5, welche nicht von Release 2 Anwendungsserver unterstützt werden. Daher sollten Sie vor der Aktualisierung gemeinsam genutzter Komponenten Release 2 Application Server beenden. Gemeinsam genutzte Komponenten werden immer dann auf Release 5 aktualisiert, wenn das Java ES-Installationsprogramm für die Installation oder Aktualisierung von Java ES-Produktkomponenten verwendet wird (wie z. B. Directory Server, Message Queue, HADB und Java DB).

---

2. **Message Queue.** Siehe „[Aktualisieren der Message Queue Release 2-Version aus Java ES-Release 2](#)“ auf Seite 207. Message Queue kann nicht mithilfe des Java ES-Installationsprogramms von Release 2 aktualisiert werden.
3. **High Availability Session Store (HADB).** Bei der Aktualisierung von Anwendungsserver wird eine Neuinstallation von HADB durch das Java ES-Installationsprogramm durchgeführt.
4. **Java DB.** Bei der Aktualisierung von Anwendungsserver wird eine Neuinstallation von Java DB durch das Java ES-Installationsprogramm durchgeführt.
5. **Web Container Software (keine zwingende Abhängigkeit).** Siehe „[Aktualisieren von Webserver von Java ES Release 2](#)“ auf Seite 170.

### *Anwendungsserver-Daten sichern*

Bei der Anwendungsserver-Aktualisierung von Release 2 auf Release 5 werden keine Release 2-Konfigurationsdaten überschrieben. Als Vorsichtsmaßnahme sollten Sie jedoch das gesamte domains-Verzeichnis vor der Aktualisierung auf Release 5 sichern.

*AppServer7Config-base/domains*

### *Erforderliche Konfigurationsinformationen und Passwörter abrufen*

Sie benötigen folgende Informationen zur aktuell installierten Version.

- Benutzer-ID und Passwort des Anwendungsserver-Administrators
- Release 2 Anwendungsserver-Basisverzeichnis

## Aktualisieren der Release 2-Version von Anwendungsserver (Solaris)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Anwendungsserver haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung*

Bei der Aktualisierung der Anwendungsserver-Software auf Java ES Release 5 müssen folgende Aspekte berücksichtigt werden:

- Bevor Sie eine Anwendungsserver-Instanz aktualisieren, sollten sämtliche in dieser Instanz ausgeführten J2EE-Komponenten beendet werden. Diese Anforderung ist möglicherweise hinfällig, wenn Lastenausgleich für Hochverfügbarkeit oder Skalierbarkeit eingesetzt wird.

- Alle Anwendungsserver-Instanzen, die auf einem einzelnen Computer ausgeführt werden (wobei alle Instanzen demselben installierten Anwendungsserver-Image entsprechen), müssen vor der Aktualisierung des installierten Image beendet werden.

### *Aktualisierungsverfahren*

Das im Folgenden beschriebene Verfahren ist für alle Anwendungsserver-Instanzen anzuwenden, die lokal auf dem Computer ausgeführt werden, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

`su -`

2. Wenn gemeinsam genutzte Java ES-Komponenten auf Release 5 aktualisiert wurden (insbesondere wenn J2SE auf JDK 1.5 aktualisiert wurde), während Release 2 Anwendungsserver weiterhin ausgeführt wurde, muss die Datei `asenv.conf` so bearbeitet werden, dass sie direkt auf JDK 1.4 verweist.

`AS_JAVA=/usr/java`

Anwendungsserver kann nicht beendet werden ([Schritt 3](#), unten), wenn `asenv.conf` auf JDK 1.5 verweist.

3. Halten Sie alle Anwendungsserver- und zugehörigen Prozesse an.

`AppServer7-base/bin/asadmin stop-appserv domainName`

4. Installieren Sie Release 5 Anwendungsserver.

Führen Sie die folgenden Schritte aus:

- a. Führen Sie das Java ES-Installationsprogramm auf dem Computer aus, der als Host für Anwendungsserver für Release 2 dient.

`cd Java ES Release 5 distribution/os_arch  
./installer`

wobei `os_arch` der Plattform entspricht, wie z. B. `Solaris_sparc`. (Verwenden Sie die Option `installer -nodisplay` für die Befehlszeilenschnittstelle.)

Nach der Willkommensseite sowie der Lizenzvereinbarung wird eine Seite für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten erkannt werden, die direkt vom Java ES-Installationsprogramm aktualisiert werden können, wird der Status als „aktualisierbar“ angezeigt.) Anwendungsserver wird *nicht* als von Release 2 aktualisierbar dargestellt.

- b. Wählen Sie auf der Seite für die Komponentenauswahl Anwendungsserver.

Wählen Sie mindestens die ersten drei Unterkomponenten zur Installation aus, einschließlich der Knotenagent-Komponente.

- c. Klicken Sie auf „Weiter“.

Wenn Message Queue nicht bereits auf Release 5 aktualisiert wurde, wird eine Fehlermeldung angezeigt, in der Sie zur Aktualisierung von Message Queue aufgefordert werden. Klicken Sie in dem Fall auf „OK“ und aktualisieren Sie Message Queue. Die Vorgehensweise wird in [„Aktualisierung der Release 2-Version von Message Queue“ auf Seite 210](#) dargestellt.

- d. Geben Sie ein Installationsverzeichnis an, das sich von dem Installationsverzeichnis für die Installation von Release 2 Anwendungsserver unterscheidet.
- e. Wählen Sie die Option „Später konfigurieren“ aus.

---

|                |                                                                                                                                                                                                                                                                                                                                      |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HINWEIS</b> | Wenn Sie die Version von Anwendungsserver im Lieferumfang des Solaris 9-Betriebssystems besitzen, und diese Version bisher nicht verwendet haben (es wurden keine Domäneninformationen erstellt), können Sie die Option „Jetzt konfigurieren“ wählen und <a href="#">Schritt 5</a> sowie die darauf folgenden Schritte überspringen. |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

- f. Falls erforderlich, wählen Sie die Option zur Installation von lokalisierten Paketen.
  - g. Beenden Sie das Java ES-Installationsprogramm, nachdem die Installation abgeschlossen wurde.
5. Führen Sie die folgenden Schritte nach der Installation durch:
- a. Suchen Sie die Readme-Datei `postInstall` im Tools-Verzeichnis von Anwendungsserver der Java ES Release 5-Verteilung:  
*Java ES Release 5-Verteilung/os\_arch/Product/application\_svr/Tools*  
wobei *os\_arch* der Plattform entspricht, wie z. B. `Solaris_sparc`.

- b. Weitere Informationen finden Sie in der ReadMe-Datei. Führen Sie anschließend das postInstall-Skript durch.

```
cd Java ES Release 5-Verteilung/os_arch/Product/application_svr/Tools
./postInstall AppServer8Install-base AppServer8Config-base
```

Die Skripte konfigurieren und erstellen die Shell-Skripte *AppServer8-base/bin/\** und die Datei *config/asenv.conf* anhand der bei der Installation installierten Vorlagen. (Normalerweise erstellt das Java ES-Installationsprogramm die *bin/\**-Shell-Skripte; bei Auswahl der Option „Später konfigurieren“ müssen diese jedoch wie beschrieben erstellt werden.)

---

**HINWEIS** Wenn Sie Anwendungsserver auf Release 5 aktualisieren, werden die nicht administrativen Ports 8080 (Standard) und 8181 (erhöhte Sicherheit) dem Domain Administration Server (DAS) zugewiesen. Diese Portzuweisungen können möglicherweise Konflikte mit den für Release 2 Anwendungsserver-Instanzen zugewiesenen Ports auslösen. Ist dies der Fall, müssen die DAS-Ports geändert werden, um den Konflikt zu verhindern. Anweisungen dazu finden Sie im *Sun Java System Anwendungsserver Enterprise 8.2 Edition Administration Guide* im Abschnitt über das Ändern der HTTP-Listener-Attribute (<http://docs.sun.com/doc/819-4733>).

---

- c. Bearbeiten Sie gegebenenfalls die Umgebungseinstellungen in der Datei *AppServer8-base/config/asenv.conf*.

Sie müssen die Datei manuell bearbeiten.

---

**HINWEIS** Um Anwendungsserver für den Lastenausgleich zu konfigurieren, ziehen Sie den Abschnitt „Configuring Web Servers for HTTP Load Balancing“ im Kapitel „Anwendungsserver High Availability Features“ im *Sun Java System Anwendungsserver Enterprise 8.2 Edition High Availability Administration Guide* (<http://docs.sun.com/doc/819-4740>) zurate.

---

**6. Führen Sie das Dienstprogramm asupgrade aus.**

Das Dienstprogramm asupgrade erstellt einen Release 5-Knotenagenten und migriert die Anwendungsserver-Instanzen der Release 2-Version in diesen Knotenagenten.

Das Dienstprogramm befindet sich im Anwendungsserver-Verzeichnis, z. B.:

- Modus Aufrüstungsassistent: *AppServer8-base/bin/asupgrade*
- Modus Aufrüstungskonsole: *AppServer8-base/bin/asupgrade -c*

Der Aufrüstungsassistent oder die Aufrüstungskonsole führen Sie durch die erforderlichen Schritte.

**a. Geben Sie Ziel- und Quellverzeichnisse für die Migration der Domäneninformationen an:**

- Release 2: *AppServer7-base*
- Release 5: *AppServerConfig8-base/domains*

**b. Geben Sie den Admin-Benutzernamen und das zugehörige Passwort sowie das Master-Passwort von Release 2 Anwendungsserver ein.**

Wenn Sie zur Eingabe eines Master-Passworts aufgefordert werden, geben Sie *changeit* an. Wenn Sie einen Schlüssel verwenden, der über ein Kennwort verfügt, das nicht *changeit* entspricht, sollten Sie das Passwort in *changeit* ändern.

```
jdk-home/bin/keytool -storepasswd -new changeit -keystore keystore
-storepass oldpasswd
```

Weitere Informationen über das Dienstprogramm Anwendungsserver asupgrade finden Sie im Abschnitt über Benutzerbefehle im *Sun Java System Anwendungsserver Enterprise Edition 8.2 Reference Manual* <http://docs.sun.com/doc/819-4736> sowie im *Sun Java System Anwendungsserver Enterprise Edition 8.2 Upgrade and Migration Guide*, <http://docs.sun.com/doc/819-4737/6n6sao3ju?a=view>.

**7. Wenn Sie die Datei asenv.conf in [Schritt 2 auf Seite 239](#) umgeleitet haben, müssen Sie den Verweis wieder auf JDK 1.5 richten.**

```
AS_JAVA=/usr/jdk/entsys-j2se
```

Anwendungsserver kann nicht gestartet werden ([Schritt 8](#) und [Schritt 9](#), unten), wenn asenv.conf auf JDK 1.4 verweist.



## 8. Starten Sie den Domain Administration Server (DAS)

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
domainName
```

## 9. Starten Sie die aktualisierten Anwendungsserver-Instanzen neu.

Starten Sie hierfür den Knotenagenten, in den die aktualisierten Anwendungsserver-Instanzen migriert wurden.

```
AppServer8-base/bin/asadmin start-node-agent --user admin_ID
nodeagentName
```

wobei *nodeagentName* der Form *hostName\_domainName* entspricht, jedoch standardmäßig nur *hostName* lautet.

## Aktualisieren der Release 2-Version von Anwendungsserver (Linux)

Die Aktualisierung von Release 2 Anwendungsserver auf Release 5 auf der Linux-Plattform ist dadurch kompliziert, dass Java ES Release 2 nur auf RHEL 2.1 unterstützt wird, Java ES Release 5 jedoch nicht auf RHEL 2.1 unterstützt wird. Daher ist eine duale Aktualisierung erforderlich: Sowohl das Betriebssystem als auch Anwendungsserver müssen aktualisiert werden. Siehe „[Duale Aktualisierungen: Java ES und Betriebssystem-Software](#)“ auf Seite 48.

Bei der Basisvorgehensweise wird zuerst das Linux-Betriebssystem aktualisiert, anschließend alle Anwendungsserver-Abhängigkeiten und dann Anwendungsserver. Verwenden Sie dabei die in „[Aktualisieren der Release 2-Version von Anwendungsserver \(Solaris\)](#)“ auf Seite 238 dargestellte Vorgehensweise.

## Überprüfen der Aktualisierung

Starten Sie die Admin-Konsole und stellen Sie sicher, dass die betreffenden Server gestartet wurden. Falls einer der Server nicht ausgeführt wird, überprüfen Sie folgende Protokolldatei auf Fehler, die durch einen Anschlusskonflikt verursacht sein könnten:

```
AppServer8Config-base/nodeagents/nodeagentName/instanceName/logs/server.log
```

Wenn Fehler aufgrund von Anschlusskonflikten aufgetreten sind, verwenden Sie die Admin-Konsole und ändern Sie die Anschlussnummern so, dass keine Konflikte mehr vorhanden sind. Halten Sie anschließend den Knotenagenten an und starten Sie ihn neu.

Sie können die Aktualisierung von Anwendungsserver auf Release 5 durch die Eingabe folgenden Befehls überprüfen:

```
AppServer8-base/bin/asadmin version --verbose
```

Ausgabewerte finden Sie in [Tabelle 11-5 auf Seite 229](#).

## Aufgaben nach der Aktualisierung

Es müssen über die in „[Aktualisierungsverfahren](#)“ auf [Seite 239](#) beschriebenen Schritte zwei weitere Aufgaben nach der Aktualisierung durchgeführt werden:

- [Korrigieren Sie den Verweis auf JSS](#)
- [Migrieren Sie Release 2-J2EE-Komponenten](#)

### *Korrigieren Sie den Verweis auf JSS*

Damit Anwendungsserver auf die korrekte Version der gemeinsam genutzten JSS-Komponente verweist, müssen Sie `jss3.jar` durch `jss4.jar` in der Anwendungsserver-Datei `domain.xml` an folgendem Speicherort ersetzen:

```
AppServer8Config-base/domains/domainName/config/domain.xml
```

### *Migrieren Sie Release 2-J2EE-Komponenten*

Sie müssen die Release 2-J2EE-Komponenten und -Anwendungen migrieren, die in einer Release 5 Anwendungsserver-Umgebung ausgeführt werden sollen, und diese Komponenten und Anwendungen in den entsprechenden Anwendungsserver-Instanzen erneut bereitstellen. Weitere Informationen zur Migration von J2EE-Komponenten und -Anwendungen finden Sie in Kapitel 4 im *Anwendungsserver Enterprise Edition 8.2 Upgrade and Migration Guide* (<http://docs.sun.com/doc/819-4737>).

## Aufheben der Aktualisierung

Das Verfahren zum Aufheben der Aktualisierung von Anwendungsserver auf Release 5 erfolgt durch das einfache Zurückkehren zur Release 2-Version von Anwendungsserver. Die Version wurde bei der Aktualisierung auf Release 5 nicht entfernt.

# Aktualisierung der im Lieferumfang von Solaris enthaltenen Anwendungsserver-Version in einer Solaris 10-Multi-Zone-Umgebung

Anwendungsserver (sowie Message Queue, von dem Anwendungsserver abhängig ist) ist im Lieferumfang des Solaris 10-Betriebssystems enthalten. Wenn Anwendungsserver nicht aus der globalen Zone entfernt wurde, wird die im Lieferumfang enthaltene Version auch in gegebenenfalls vorhandenen nicht globalen Zonen verwendet. Wird die im Lieferumfang enthaltene Anwendungsserver-Version in allen Zonen verwendet, hat dies Einfluss auf die darauf folgende Aktualisierung von Anwendungsserver auf Release 5:

- Bei der Aktualisierung von Anwendungsserver in der globalen Zone wird die im Lieferumfang enthaltene Version in der globalen Zone und automatisch auch in allen nicht globalen Zonen gelöscht.
- Bei der Aktualisierung von Anwendungsserver auf Release 5 in der globalen Zone wird Anwendungsserver nicht in den nicht globalen Zonen aktualisiert, da Release 5 Anwendungsserver-Pakete nicht übernommen werden.

Das folgende Beispiel stellt einige der Feinheiten dar, die bei der Aktualisierung von Anwendungsserver in einer Solaris 10-Multi-Zone-Umgebung beachtet werden müssen. (Eine detailliertere Beschreibung von Java ES und Solaris 10-Zonen finden Sie in [„Aktualisierung von Java ES 5 und Solaris 10-Zonen“ auf Seite 65.](#))

Das Ziel dieses Beispiels ist es, die im Lieferumfang von Solaris enthaltene Anwendungsserver-Version (Version 8.0.0\_01) in einer Solaris 10-Sparse-Root-Zone auf Release 5 zu aktualisieren.

Sie können Anwendungsserver in einer Sparse-Root-Zone nicht ohne weiteres aktualisieren, da die im Lieferumfang von Solaris enthaltene Anwendungsserver-Version in einem schreibgeschützten Verzeichnis installiert wurde, das von der globalen Zone erstellt wurde. Daher muss vor der Aktualisierung von Anwendungsserver auf Release 5 in der Sparse-Root-Zone zuerst die im Lieferumfang enthaltene Version in der globalen Zone gelöscht werden.

Des Weiteren wurde Message Queue in der globalen Zone installiert. Dies bedeutet eine Abweichung von der Vorgehensweise, bei der nur gemeinsam genutzte Komponenten (keine Produktkomponenten) in der globalen Zone installiert werden müssen. Dies beruht auf der Tatsache, dass Message Queue nicht in einer Sparse-Root-Zone installiert oder aktualisiert werden kann, da die Verzeichnisse schreibgeschützt sind.

Die Vorgehensweise für die Aktualisierung der im Lieferumfang von Solaris enthaltenen Anwendungsserver-Version (Version 8.0.0\_01) in einer Solaris 10-Sparse-Root-Zone auf Release 5 lautet wie folgt:

**1. Stellen Sie den ursprünglichen Zustand Ihres Systems fest.**

In diesem Beispiel wird eine Solaris 10-Version mit einer Sparse-Root-Zone angenommen, die vom globalen Administrator konfiguriert, installiert und gebootet wurde.

Die Sparse-Root-Zone enthält alle Java ES-Komponenten, die bereits in der globalen Zone installiert wurden, nämlich die im Lieferumfang von Solaris 10 enthaltenen Versionen von Message Queue und Anwendungsserver.

Zusätzlich wird in dem Beispiel angenommen, dass der Benutzer zuvor die im Lieferumfang enthaltene Anwendungsserver-Version in der Sparse-Root-Zone verwendet hat, wodurch administrative Domäneninformationen erstellt wurden, die erhalten werden müssen.

**2. Aktualisieren Sie die im Lieferumfang enthaltene Anwendungsserver-Version in der globalen Zone.**

Bei dieser Vorgehensweise werden die im Lieferumfang enthaltenen Anwendungsserver-Pakete entfernt und durch Release 5-Pakete ersetzt. Dadurch werden auch die im Lieferumfang enthaltenen Pakete in der Sparse-Root-Zone entfernt und somit die Anwendungsserver-Pakete gelöscht, die Release 5-Pakete werden jedoch nicht in den nicht globalen Zonen übernommen.

- a.** Führen Sie das Java ES-Installationsprogramm in der globalen Zone durch.
- b.** Wählen Sie auf der Seite für die Komponentenauswahl Anwendungsserver.

Message Queue, HADB und Java DB werden automatisch ausgewählt und Anwendungsserver und Message Queue werden als aktualisierbar angezeigt.

- c.** Schließen Sie die Aktualisierung ab.

Während Release 5 Message Queue in der Sparse-Root-Zone übernommen wird, werden weder Anwendungsserver, HADB noch Java DB übernommen. Des Weiteren werden alle gemeinsam genutzten Komponenten auf Release 5 synchronisiert und in der Sparse-Root-Zone übernommen.

**3. Installieren Sie Anwendungsserver in der Sparse-Root-Zone.**

- a. Führen Sie das Java ES-Installationsprogramm in der Sparse-Root-Zone durch.
- b. Wählen Sie auf der Seite für die Komponentenauswahl Anwendungsserver.

Heben Sie die Auswahl von Message Queue auf, falls es automatisch ausgewählt wurde, und wählen Sie HADB und Java DB aus, wenn sie nicht automatisch ausgewählt wurden.

- c. Schließen Sie die Installation von Anwendungsserver ab.

Wählen Sie „Später konfigurieren“, sodass Domäneninformationen nicht durch den Installationsvorgang überschrieben werden.

Falls keine Domänen erstellt wurden, können Sie die Option „Jetzt konfigurieren“ wählen.

Aktualisierung der im Lieferumfang von Solaris enthaltenen Anwendungsserver-Version in einer Solaris 10-Multi-Zone-Umgebung

# Service Registry

In diesem Kapitel wird die Aktualisierung von Service Registry auf Java ES 5 (Release 5) beschrieben: Service Registry 3.1.

Das Kapitel enthält einen Überblick über die Aspekte der verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Service Registry“ auf Seite 251
- „Aktualisieren von Service Registry von Java ES Release 4“ auf Seite 254

---

**HINWEIS** Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf Verzeichnispfade, die im Folgenden als *ServiceRegistryR4-base* und *RegistryDomainR4-base* (Java ES Release 4 Service Registry) sowie *ServiceRegistryR5-base* und *RegistryDomainR5-base* (Java ES Release 5 Service Registry) angegeben werden. Bei der Installation von Service Registry wurden diese Pfade mindestens teilweise als Installationsverzeichnisse angegeben. Wenn nicht, wurde vom Java ES-Installationsprogramm ein Standardwert zugewiesen.

Die Standardwerte für diese Verzeichnispfade sind in der folgenden Tabelle aufgelistet.

---

**Tabelle 12-1** Service Registry Verzeichnispfade

| Variable des Pfadnamens       | Solaris OS        | Linux OS              |
|-------------------------------|-------------------|-----------------------|
| <i>ServiceRegistryR4-base</i> | /opt/SUNWsoar     | /opt/sun/SUNWsoar     |
| <i>RegistryDomainR4-base</i>  | /var/opt/SUNWsoar | /var/opt/sun/SUNWsoar |

---

**Tabelle 12-1** Service Registry Verzeichnispfade (*Fortsetzung*)

| <b>Variable des Pfadnamens</b> | <b>Solaris OS</b>          | <b>Linux OS</b>            |
|--------------------------------|----------------------------|----------------------------|
| <i>ServiceRegistryR5-base</i>  | /opt/SUNWsrcv-registry     | /opt/sun/srcv-registry     |
| <i>RegistryDomainR5-base</i>   | /var/opt/SUNWsrcv-registry | /var/opt/sun/srcv-registry |



# Überblick über Aktualisierungen von Service Registry

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Service Registry auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5](#)
- [Java ES Wegweiser für die Aktualisierung auf Release 5](#)
- [Service Registry-Daten](#)
- [Vorgehensweise zur Aktualisierung von Service Registry](#)

## Über Java ES Release 5

Java ES Release 5 Service Registry stellt im Gegensatz zu Release 4 Service Registry ein kleineres Release dar. Es beinhaltet einige verbesserte Funktionen, aktualisierte Schnittstellen und ausgewählte Fehlerkorrekturen.

## Java ES Wegweiser für die Aktualisierung auf Release 5

[Tabelle 12-2](#) zeigt die unterstützten Wege für die Aktualisierung von Service Registry auf Java ES Release 5. Die Tabelle gilt sowohl für das Solaris- als auch für das Linux-Betriebssystem.

**Tabelle 12-2** Wege für die Aktualisierung auf Java ES 5 (Release 5): Service Registry 3.1

| Java ES Release | Service Registry Version                    | Allgemeiner Ansatz                                                                                                                     | Neukonfiguration erforderlich |
|-----------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Release 4       | Sun Java System Service Registry 3.0 2005Q4 | Direkte Aktualisierung:<br>Ersetzen Sie Release 4 durch eine Neuinstallation und übertragen Sie die Registrierungsdaten auf Release 5. | Keine                         |

# Service Registry-Daten

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Service Registry-Software betroffen sein können.

**Tabelle 12-3** Service Registry-Verwendung der Daten

| Datentyp                       | Standort                                                                                                  | Verwendung                                                                                                                |
|--------------------------------|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Installationsparameter         | <i>ServiceRegistryR4-base/install/install.properties</i>                                                  | Konfiguration von Service Registry                                                                                        |
| Vertrauenswürdige Zertifikate  | <i>ServiceRegistryR4-base/install/install.properties</i>                                                  | Von Service Registry als vertrauenswürdig eingestufte Zertifikate, die nicht Teil der Anwendungsserver-Installation sind. |
| Konfigurationsdaten            | <i>RegistryDomainR4-base/domains/registry/applications/j2ee-modules/soar/WEB-INF/classes/*.properties</i> | Konfiguration der Service Registry-Instanz                                                                                |
| Registry-/Repository-Daten     | <i>RegistryDomainR4-base/3.0/data</i>                                                                     | Datenbank und Benutzerzertifikate                                                                                         |
| Webschnittstellenkonfiguration | <i>RegistryDomainR4-base/3.0/data</i>                                                                     | Konfiguration der Webschnittstelle                                                                                        |

## Vorgehensweise zur Aktualisierung von Service Registry

Die Vorgehensweise zur Aktualisierung von Service Registry hängt im Grunde von den verschiedenen Aspekten ab, die in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) besprochen wurden: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

In diesem Abschnitt wird im Detail auf Service Registry eingegangen, indem Themen besprochen werden, die Ihre Aktualisierungspläne von Service Registry beeinflussen können.

### Kompatibilität

Die Rückwärtskompatibilität von Service Registry Release 5 zu Service Registry Release 4 ist gewährleistet.

## Abhängigkeiten

Service Registry-Abhängigkeiten zu anderen Java ES-Komponenten beeinflussen möglicherweise das Verfahren für die Aktualisierung und Neukonfiguration der Service Registry-Software. Änderungen der Service Registry-Schnittstellen oder -Funktionen könnten beispielsweise eine aktualisierte Version der Komponenten erforderlich machen, von denen Service Registry abhängig ist. Welche dieser Komponenten aktualisiert werden müssen, hängt von dem jeweiligen Aktualisierungsweg ab.

Für Service Registry bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Service Registry ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)).
- **Anwendungsserver.** Für Service Registry besteht eine zwingende Abhängigkeit zu Anwendungsserver, um einen Container für die Service Registry-Anwendung bereitzustellen und in Java ES Release 5 die Verbindungen zur Registry-/Repository-Datenbank im Netzwerk zu verwalten.
- **Java DB.** Für Service Registry besteht eine zwingende Abhängigkeit zu Java DB als Standarddatenbank für die Speicherung von Diensten und den beschreibenden Metadaten.

# Aktualisieren von Service Registry von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von Service Registry von Java ES 2005Q4 (Release 4) auf Java ES 2005Q5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 4-Version von Service Registry](#)
- [Aktualisierung mehrerer Instanzen](#)

## Einführung

Berücksichtigen Sie bei der Aktualisierung von Java ES von Service Registry Release 4 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch eine Neuinstallation von Release 5 Service Registry, eine Migration der Daten und Konfiguration von Release 4 auf Release 5 und anschließend das Entfernen von Release 4, um Speicherplatz einzusparen.
- **Aktualisierungsabhängigkeiten.** Service Registry ist von einer Reihe gemeinsam genutzter Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)), die alle automatisch vom Java ES-Installationsprogramm auf Release 5 aktualisiert werden, wenn Sie eine Aktualisierung von Service Registry durchführen.

Für Service Registry besteht eine zwingende Aktualisierungsabhängigkeit zu Anwendungsserver und Java DB.

- **Rückwärtskompatibilität.** Die Service Registry Release 5-Version ist mit Release 4 vollständig kompatibel.
- **Aufheben der Aktualisierung.** Das Zurücksetzen der Release 5-Aktualisierung erfolgt durch das Zurückkehren zu Release 4, nachdem die gespeicherte Datenbank und Konfigurationsdaten wiederhergestellt wurden.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Service Registry ist für das Solaris- und Linux-Betriebssystem identisch.

# Aktualisierung der Release 4-Version von Service Registry

In diesem Abschnitt wird die Aktualisierung von Service Registry von Java ES Release 4 auf Java ES Release 5 unter Solaris und Linux beschrieben. Plattformspezifische Vorgänge sind durch die Angabe des jeweiligen Betriebssystems, auf das sich der Vorgang bezieht, gekennzeichnet. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren von Release 4 von Service Registry](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

## Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung von Service Registry beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Service Registry-Aktualisierungsabhängigkeiten](#)
- [Service Registry-Daten sichern](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

### *Aktuelle Versionsinformationen überprüfen*

Sie können die aktuelle Version von Service Registry überprüfen, indem Sie die Merkmale der Web Console-Benutzeroberfläche überwachen:

```
http://localhost:6060/soar
```

Sie können auch die Service Registry-Paketnamen überprüfen. Beispiel:

*Unter Solaris:*  

```
pkginfo -l|grep svc
```

*Unter Linux:*  

```
rpm -qa|grep svc
```

Die charakteristischen Merkmale und Paketnamen werden in der folgenden Tabelle aufgeführt:

**Tabelle 12-4** Service Registry Ausgaben der Versionsüberprüfung

| Java ES Release | Service Registry-Version<br>snummer | Charakteristische Merkmale                                                                                 |
|-----------------|-------------------------------------|------------------------------------------------------------------------------------------------------------|
| Release 4       | 3.0                                 | Web Console: Abschnitt für Tools im linken Bereich<br>Paketname enthält die Zeichenfolge: soar             |
| Release 5       | 3.1                                 | Web Console: drei Registerkarten im linken Bereich<br>Paketname enthält die Zeichenfolge:<br>srvc-registry |

*Service Registry-Aktualisierungsabhängigkeiten*

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Für Service Registry bestehen jedoch zwingende Aktualisierungsabhängigkeiten zu bestimmten gemeinsam genutzten Komponenten, Anwendungsserver und Java DB.

Wenn Sie die Service Registry-Abhängigkeiten aktualisieren, sollten Sie dies in der unten angegebenen Reihenfolge vornehmen, bevor Sie Service Registry aktualisieren. Überspringen Sie dabei die bereits aktualisierten Abhängigkeiten. Die Aktualisierung gemeinsam genutzter Komponenten erfolgt in der Regel automatisch durch das Java ES-Installationsprogramm.

- 1. Gemeinsam genutzte Komponenten.** Anleitungen für die Synchronisierung von gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie unter [„Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#). Alle gemeinsam genutzten Komponenten, die von Service Registry benötigt werden, werden jedoch automatisch vom Java ES-Installationsprogramm aktualisiert, wenn Sie eine Aktualisierung von Service Registry auf Release 5 durchführen.
- 2. Java DB.** Anleitungen für die Aktualisierung von Java DB auf Release 4 finden Sie in [Kapitel 8, „Java DB“ auf Seite 171](#).
- 3. Anwendungsserver.** Anleitungen für die Aktualisierung von Anwendungsserver auf Release 4 finden Sie in [Kapitel 11, „Anwendungsserver“ auf Seite 219](#).

### *HTTP-Anschlussnummer ändern*

Bearbeiten Sie die Datei *ServiceRegistryR4-base/install/install.properties*, um den HTTP-Anschluss von 6060 auf 6480 zu ändern (6060 ist ein reservierter Anschluss). Informationen zum Einstellen dieser Eigenschaft finden Sie im *Service Registry 3.1 Administration Guide*, <http://docs.sun.com/doc/819-4640>.

### *Service Registry-Daten sichern*

Bei der Service Registry-Aktualisierung von Release 4 auf Release 5 werden weder die Konfigurationsdaten noch die Registry-/Repository-Datenbank geändert. Eine Sicherung der aktuellen Daten ist daher nicht erforderlich.

### *Erforderliche Konfigurationsinformationen und Passwörter abrufen*

Sie müssen über Benutzer-IDs, Passwörter, Domänenname und Anschlussnummer für Ihr Service Registry Release 4 verfügen.

## Aktualisieren von Release 4 von Service Registry

In diesem Abschnitt wird das Aktualisierungsverfahren unter Solaris und Linux beschrieben.

### *Aktualisierungsverfahren (Solaris)*

Das im Folgenden beschriebene Verfahren ist für Service Registry-Instanzen anzuwenden, die lokal auf dem Computer ausgeführt werden, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Stellen Sie sicher, dass das auf Jakarta ANT Java/XML basierende Tool (ANT, gemeinsam genutzte Komponente) auf die korrekte Version von J2SE verweist.

(Der Befehl `ant` wird in den folgenden Schritten verwendet.)

```
PATH=/usr/jdk/entsys-j2se/bin:$PATH
```

```
export PATH
```

3. Halten Sie die Domäne von Service Registry Release 4 an (Anwendungsserver).

```
cd ServiceRegistryR4-base/install
/usr/sfw/bin/ant -f build-install.xml appserver.domain.stop
```

Die Domäne ist einer Service Registry-Instanz zugeordnet.

**4. Führen Sie eine Neuinstallation von Service Registry Release 5 aus.**

Führen Sie die folgenden Schritte aus:

- a.** Starten Sie das Java ES-Installationsprogramm auf dem Computer, der als Host für Service Registry Release 4 dient.

```
cd Java ES Release 5 distribution/os_arch
./installer
```

wobei *os\_arch* der Plattform entspricht, wie z. B. *Solaris\_sparc*.  
(Verwenden Sie die Option *installer -nodisplay* für die Befehlszeilenschnittstelle.)

Nach der Willkommenseite sowie der Lizenzvereinbarung wird eine Seite für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten erkannt werden, die direkt vom Java ES-Installationsprogramm aktualisiert werden können, wird der Status als „aktualisierbar“ angezeigt.)

- b.** Wählen Sie auf der Seite für die Komponentenauswahl Service Registry.  
**c.** Geben Sie einen Installationsverzeichnispfad an, der sich vom Installationsverzeichnispfad von Release 4 unterscheidet.

Standardmäßig unterscheidet sich der Installationspfad in Release 5 (*ServiceRegistryR5-base*) vom Installationspfad in Release 4 (*ServiceRegistryR4-base*).

- d.** Wählen Sie die Option „Später konfigurieren“ aus.

Die Option „Jetzt konfigurieren“ wird nicht unterstützt.

- e.** Falls erforderlich, wählen Sie die Option zur Installation von lokalisierten Paketen.  
**f.** Beenden Sie das Java ES-Installationsprogramm, nachdem die Installation abgeschlossen wurde.

**5. Aktualisieren und konfigurieren Sie die Service Registry-Instanz von Release 5.**

```
cd ServiceRegistryR5-base/install
/usr/sfw/bin/ant -f build-install.xml
-Dinstall.properties=ServiceRegistryR4-base/install/install.properties
upgrade
```



Anstatt die Release 4-Datei `install.properties` zu verwenden, können Sie auch die standardmäßige Release 5-Datei `install.properties` bearbeiten, um beliebige Eigenschaftswerte von Release 4 zu ändern. Informationen zum Einstellen dieser Eigenschaften finden Sie im *Service Registry 3.1 Administration Guide*, <http://docs.sun.com/doc/819-4640>.

Wenn Sie benutzerdefinierte Eigenschaftswerte verwenden, die nicht in der Datei `install.properties` enthalten sind, müssen Sie diese Eigenschaftswerte auf der Ant-Befehlszeile wie folgt (auf einer Zeile) angeben:

```
/usr/sfw/bin/ant -f build-install.xml
-Dregistry.install.RegistryServerKeystorePassword=password1
-Dregistry.install.AdministratorPassword=password2
-Dregistry.install.ApplicationServerKeystorePassword=password3
upgrade
```

Es wird jedoch empfohlen, dass Sie diese benutzerdefinierten Eigenschaftswerte in der Datei `install.properties` einschließen und dabei eingeschränkte Berechtigungen verwenden, um eine nicht autorisierte Verwendung der Befehlszeileneinstellungen zu verhindern. Weitere Informationen finden Sie im *Service Registry Administration Guide*.

Das Dienstprogramm für die Aktualisierung erstellt eine neue Anwendungsserver-Domäne, startet die Domäne und stellt die Service Registry-Instanz in der Domäne bereit. Jede Service Registry-Instanz ist einer eigenen Anwendungsserver-Domäne zugeordnet.

6. Wenn die Eigenschaftendateien des Servers der Service Registry Release 4 verändert wurden, können Sie die entsprechenden Änderungen wie folgt in der Release 5-Konfiguration von Service Registry durchführen:

- a. Halten Sie die Domäne von Service Registry Release 5 an (Anwendungsserver).

(Die Domäne wurde automatisch durch den Befehl `upgrade` aus [Schritt 5](#) gestartet.)

```
cd ServiceRegistryR5-base/install
/usr/sfw/bin/ant -f build-install.xml appserver.domain.stop
```

- b. Übertragen Sie die Service Registry-Instanzkonfiguration von Release 4 auf Release 5.

Fügen Sie Änderungen hinzu, die Sie an der Service Registry-Instanzkonfiguration von Release 4 vorgenommen haben:

```
RegistryDomainR4-base/domains/registry/applications/j2ee-modules/
soar/WEB-INF/classes/*.properties
```

Änderungen zur entsprechenden Release 5-Konfiguration hinzufügen:

```
RegistryDomainR5-base/domains/registry/applications/j2ee-modules/
soar/WEB-INF/classes/*.properties
```

7. Starten Sie die Domäne von Service Registry Release 5 an (Anwendungsserver).

```
cd ServiceRegistryR5-base/install
/usr/sfw/bin/ant -f build-install.xml appserver.domain.start
```

### *Aktualisierungsverfahren (Linux)*

Die Aktualisierung von Service Registry unter Linux ist mit den Verfahren unter Solaris identisch (siehe „[Aktualisierungsverfahren \(Solaris\)](#)“ auf Seite 257). Nur der Speicherort des Befehls `ant`, der in den verschiedenen Schritten des Aktualisierungsverfahrens verwendet wird, ist unter Linux und Solaris unterschiedlich:

```
/opt/sun/share/bin/ant
```

### Überprüfen der Aktualisierung

Sie können die erfolgreiche Aktualisierung von Service Registry überprüfen, indem Sie die Merkmale der Web Console-Benutzeroberfläche überwachen:

```
http://localhost:6480/soar
```

Sie können auch die Service Registry-Paketnamen überprüfen. Beispiel:

*Unter Solaris:*  
`pkginfo -l|grep soar`

*Unter Linux:*  
`rpm -qa|grep soar`

Die charakteristischen Merkmale und Paketnamen werden in [Tabelle 12-4 auf Seite 256](#) aufgeführt.

## Aufgaben nach der Aktualisierung

Die folgenden Schritte zum Entfernen von Service Registry Release 4 sollten nur ausgeführt werden, wenn Sie sich sicher sind, dass Sie die Aktualisierung nicht mehr rückgängig machen möchten und Release 4 nicht mehr benötigen.

1. Löschen Sie die Domäne von Service Registry Release 4 (Anwendungsserver):

```
cd ServiceRegistryR4-base/install
```

*Unter Solaris:*

```
/usr/sfw/bin/ant -f build-install.xml appserver.domain.delete
```

*Unter Linux:*

```
/opt/sun/bin/ant -f build-install.xml appserver.domain.delete
```

2. Löschen Sie das Verzeichnis, in dem sich die Domänenendaten für Service Registry Release 4 befinden.

```
rm -rf RegistryDomainR4-base
```

3. Löschen Sie das Verzeichnis, in dem sich die Installationsdateien für Service Registry Release 4 befinden.

```
rm -rf ServiceRegistryR4-base
```

## Aufheben der Aktualisierung

Das Zurücksetzen der Release 5-Aktualisierung erfolgt durch das Zurückkehren zur vorherigen Version, die bei der Aktualisierung auf Release 5 unverändert beibehalten wurde.

1. Halten Sie die Domäne von Service Registry Release 5 an (Anwendungsserver) und löschen Sie sie:

```
cd ServiceRegistryR4-base/install
```

*Unter Solaris:*

```
/usr/sfw/bin/ant -f build-install.xml appserver.domain.delete
```

*Unter Linux:*

```
/opt/sun/bin/ant -f build-install.xml appserver.domain.delete
```

2. Führen Sie das Java ES-Deinstallationsprogramm von Release 5 aus, um Service Registry Release 5 zu deinstallieren.

3. Starten Sie die Domäne von Service Registry Release 4.

```
cd ServiceRegistryR4-base/install
```

*Unter Solaris:*

```
/usr/sfw/bin/ant -f build-install.xml appserver.domain.start
```

*Unter Linux:*

```
/opt/sun/bin/ant -f build-install.xml appserver.domain.start
```

4. Greifen Sie auf die Web Console von Service Registry Release 4 zu.

```
http://localhost:6480/soar
```

5. Stellen Sie sicher, dass die Console die Merkmale von Release 4 anzeigt, die unter [„Service Registry Ausgaben der Versionsüberprüfung“](#) auf Seite 256 aufgeführt werden.

## Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen wird Service Registry auf mehreren Computersystemen bereitgestellt, um die Skalierbarkeit zu gewährleisten und die Verfügbarkeit zu verbessern. Möglicherweise führen Sie beispielsweise Service Registry-Instanzen auf mehreren Computern zusammen mit einem Lastenausgleichsprogramm aus, um die Last zu verteilen.

In diesen Architekturen handelt es sich überwiegend um schreibgeschützte Registrierungen, die auf hohe Anfragelasten reagieren, indem Sie auf die allgemeine Datenbank zugreifen.

Informationen zur Aktualisierung von Service Registry auf den einzelnen Computern erhalten Sie unter [„Aktualisierung der Release 4-Version von Service Registry“](#) auf Seite 255.

# Web Proxy Server

In diesem Kapitel wird die Aktualisierung von Web Proxy Server auf Java ES 5 (Release 5) beschrieben: Sun Java System Web Proxy Server 4.0.4.

Das Kapitel enthält einen Überblick über die Aspekte der verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Web Proxy Server“ auf Seite 264
- „Aktualisieren von Web Proxy Server von Java ES Release 4“ auf Seite 267
- „Aktualisierung von Web Proxy Server von Version 3.6“ auf Seite 274

---

**HINWEIS** Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf einen Verzeichnispfad, der im Folgenden als *WebProxyServer-base* angegeben wird. Bei der erstmaligen Installation und Konfiguration von Web Proxy Server wurde möglicherweise ein Teil dieses Pfades als Installationsverzeichnis angegeben. Wenn nicht, wird vom Java ES-Installationsprogramm ein Standardwert zugewiesen.

Der Standardwert für *WebProxyServer-base* hängt vom Betriebssystem ab, wie in der folgenden Tabelle dargestellt.

---

**Tabelle 13-1** Web Proxy Server Verzeichnispfade

| Variable des Pfadnamens    | Solaris OS     | Linux OS                |
|----------------------------|----------------|-------------------------|
| <i>WebProxyServer-base</i> | /opt/SUNWproxy | /opt/sun/webproxyserver |

---

# Überblick über Aktualisierungen von Web Proxy Server

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Web Proxy Server auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5 Web Proxy Server](#)
- [Wegweiser für die Aktualisierung von Web Proxy Server](#)
- [Web Proxy Server-Daten](#)
- [Vorgehensweise zur Aktualisierung von Web Proxy Server](#)

## Über Java ES Release 5 Web Proxy Server

Java ES Release 5 Web Proxy Server stellt im Gegensatz zu Release 4 ein kleineres Release mit Fehlerkorrekturen dar.

Web Proxy Server Release 5 weist im Vergleich zu Sun One Web Proxy Server 3.6 (vor der Integration in Java Enterprise System) eine verbesserte Leistung, eine höhere Skalierbarkeit der Architektur, eine verbesserte Einhaltung von Standards und eine neue Verwaltungsoberfläche auf.

## Wegweiser für die Aktualisierung von Web Proxy Server

[Tabelle 13-2](#) zeigt den Aktualisierungsweg für Web Proxy Server auf Java ES Release 5. Web Proxy Server war in vorherigen Java ES-Versionen nicht enthalten. Die Tabelle enthält nur Informationen bezüglich des Solaris-Betriebssystems, da Web Proxy Server auf dem Linux-Betriebssystem zuvor nicht unterstützt wurde.

**Tabelle 13-2** Wege für die Aktualisierung auf Java ES 5 (Release 5): Web Proxy Server 4.0.4

| Java ES Release | Web Proxy Server Version                      | Allgemeiner Ansatz                                     | Neukonfiguration erforderlich |
|-----------------|-----------------------------------------------|--------------------------------------------------------|-------------------------------|
| Release 4       | Sun Java System Web Proxy Server 4.0.1 2005Q4 | Direkte Aktualisierung:<br>Durch Anwendung von Patches | Keine                         |

**Tabelle 13-2** Wege für die Aktualisierung auf Java ES 5 (Release 5): Web Proxy Server 4.0.4

| Java ES Release                                      | Web Proxy Server Version                                                  | Allgemeiner Ansatz                                                                                                                                                                                           | Neukonfiguration erforderlich                                               |
|------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Versionen vor Java ES (nur Solaris-Betriebssystemen) | Sun ONE Web Proxy Server 3.6<br>(Im Folgenden als Version 3.6 bezeichnet) | Direkte Aktualisierung:<br>Durch Ausführung des Java ES-Installationsprogramms für die Installation im neuen Verzeichnis und anschließender Migration der Konfigurationsdaten mithilfe von Verwaltungstools. | Konfigurationsinformationen müssen in das neue Verzeichnis migriert werden. |

## Web Proxy Server-Daten

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Web Proxy Server-Software betroffen sein können.

**Tabelle 13-3** Verwendung der Web Proxy Server-Daten

| Datentyp            | Standort                                                                                                                                                  | Verwendung                                                                                                          |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Konfigurationsdaten | <i>WebProxyServer-base/proxy-serverid/config</i> -Verzeichnis<br>Enthält z. B. Dateien wie: <i>server.xml</i> , <i>magnus.conf</i> , <i>obj.conf</i> usw. | Speichert Konfigurationsinformationen für Server, Cache, Filter, Routing und andere Funktionen von Web Proxy Server |

## Vorgehensweise zur Aktualisierung von Web Proxy Server

Ihre Vorgehensweise bei der Aktualisierung von Web Proxy Server hängt grundsätzlich von den zahlreichen in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) erläuterten Aspekten ab: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

Dieser Abschnitt konzentriert diese grundsätzliche Erläuterung auf Web Proxy Server, indem Probleme dargestellt werden, die möglicherweise Ihren Aktualisierungsplan für Web Proxy Server beeinflussen.

## Kompatibilität

Web Proxy Server Release 5 führt keine neuen öffentlichen Schnittstellen ein und ist rückwärts kompatibel mit Web Proxy Server Release 4. Web Proxy Server Release 5 ist auch mit Version 3.6 kompatibel. Eine Ausnahme bilden jedoch die Plug-Ins, die mit der von Version 3.6 unterstützten NSAPI-Schnittstelle entwickelt wurden; diese müssen mit der von Release 5 unterstützten NSAPI-Schnittstelle neu kompiliert werden.

## Web Proxy Server-Abhängigkeiten

Für Web Proxy Server bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Web Proxy Server ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)).
- **Directory Server.** Für Web Proxy Server besteht eine optionale Abhängigkeit zu Directory Server für die Authentifizierung auf LDAP-Basis.
- **Webserver.** Für Web Proxy Server besteht eine Abhängigkeit zu Webserver für die Bereitstellung von verbesserten Sicherheitsfunktionen und Leistungen für HTTP-Anfragen.



# Aktualisieren von Web Proxy Server von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von Web Proxy Server von Java ES 2005Q4 (Release 4) auf Java ES 2005Q5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 4-Version von Web Proxy Server](#)

## Einführung

Berücksichtigen Sie bei der Aktualisierung von Web Proxy Server auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch die Verwendung von Patches. Eine zusätzliche Neukonfiguration ist nicht erforderlich.
- **Aktualisierungsabhängigkeiten.** Für Web Proxy Server bestehen Abhängigkeiten zu bestimmten gemeinsam genutzten Java ES-Komponenten (siehe [Tabelle 1-7 auf Seite 51](#)). Doch zwingende Aktualisierungsabhängigkeiten für Web Proxy Server bestehen nur zu gemeinsam genutzten NSS- und NSPR-Komponenten.
- **Rückwärtskompatibilität.** Die Web Proxy Server Release 5-Version ist rückwärts kompatibel mit Release 4.
- **Aufheben der Aktualisierung.** Das Zurücksetzen der Release 5-Aktualisierung von Web Proxy Server erfolgt durch das Entfernen der Aktualisierungs-Patches.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Web Proxy Server ist für das Solaris- und Linux-Betriebssystem identisch; dabei unterscheidet sich jedoch die angewandte Patch-Technologie. Daher enthält der Aktualisierungsvorgang plattformspezifische Verfahren.

# Aktualisierung der Release 4-Version von Web Proxy Server

Dieser Abschnitt bietet einen Überblick über das Aktualisierungsverfahren von Web Proxy Server auf Java ES Release 5. Die folgenden Themen werden in diesem Abschnitt behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren der Release 4-Version von Web Proxy Server \(Solaris\)](#)
- [Aktualisieren der Release 4-Version von Web Proxy Server \(Linux\)](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung \(Solaris\)](#)

## Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung von Web Proxy Server beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Web Proxy Server-Abhängigkeiten aktualisieren](#)
- [Web Proxy Server-Daten sichern](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

### Aktuelle Versionsinformationen überprüfen

Sie können die aktuelle Version von Web Proxy Server durch Eingabe des folgenden Befehls überprüfen:

```
WebProxyServer-base/proxy-admserv/start -version
```

**Tabelle 13-4** Web Proxy Server Ausgaben der Versionsüberprüfung

| Java ES Release                    | Web Proxy Server-Versionnummer |
|------------------------------------|--------------------------------|
| Version 3.6 (kein Java ES-Release) | 3.6                            |
| Release 4                          | 4.0.1                          |
| Release 5                          | 4.0.4                          |

### *Web Proxy Server-Abhängigkeiten aktualisieren*

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Bei der Aktualisierung von Web Proxy Server auf Release 5 müssen jedoch nur die gemeinsam genutzten NSS- und NSPR-Komponenten aktualisiert werden. Wenn diese gemeinsam genutzten Komponenten noch nicht aktualisiert wurden, sollten Sie alle gemeinsam genutzten Komponenten auf die Release 5-Version synchronisieren, indem Sie die Option „Gemeinsam genutzte Komponenten synchronisieren“ verwenden. Anweisungen hierzu erhalten Sie unter [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#).

### *Web Proxy Server-Daten sichern*

Bei der Web Proxy Server-Aktualisierung auf Release 5 werden keine Release 4-Konfigurationsdaten geändert. Eine Sicherung der aktuellen Daten ist daher nicht erforderlich.

### *Erforderliche Konfigurationsinformationen und Passwörter abrufen*

Es werden keine bestimmten Informationen zur aktuell installierten Version benötigt. Sie müssen jedoch als Superuser angemeldet sein, um die Aktualisierung durchführen zu können.

## **Aktualisieren der Release 4-Version von Web Proxy Server (Solaris)**

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Web Proxy Server haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung (Solaris)*

Bei der Aktualisierung der Web Proxy Server-Software auf Java ES Release 5 müssen folgende Aspekte berücksichtigt werden:

- Alle Web Proxy Server-Instanzen, die demselben installierten Web Proxy Server-Image entsprechen, werden gleichzeitig aktualisiert. Sämtliche dieser Instanzen sollten beendet werden, bevor Patches auf das installierte Image angewendet werden.
- Die Patches für die Aktualisierung von Web Proxy Server auf Release 5 unter Solaris OS werden in der folgenden Tabelle aufgeführt:

**Tabelle 13-5** Patches<sup>1</sup> für die Aktualisierung von Web Proxy Server unter Solaris

| Beschreibung                      | Patch-ID: SPARC<br>Solaris 9 & 10 | Patch-ID: X86<br>Solaris 9 & 10 |
|-----------------------------------|-----------------------------------|---------------------------------|
| Web Proxy Server Core             | 120981-06                         | 120982-06                       |
| Web Proxy<br>Server-Lokalisierung | 122963-01                         | 122964-01                       |

1. Diese Patch-Versionsnummern sind für die Aktualisierung auf Java ES Release 5 mindestens erforderlich. Wenn neuere Versionen verfügbar sind, verwenden Sie anstelle der in dieser Tabelle genannten Versionen die neueren Versionen.

*Aktualisierungsverfahren (Solaris)*

Das im Folgenden beschriebene Verfahren ist für Web Proxy Server auf dem Computer anzuwenden, auf dem die Aktualisierung durchgeführt wird.

- 1. Melden Sie sich als Root oder Superuser an.

su -

- 2. Halten Sie alle derzeit ausgeführten Instanzen von Web Proxy Server und Administration Server an.

WebProxyServer-base/proxy-instanceName/stop  
WebProxyServer-base/proxy-admserv/stop

- 3. Synchronisieren Sie alle gemeinsam genutzten Komponenten auf Release 5, sofern dies noch nicht erfolgt ist.

Anweisungen hierzu erhalten Sie unter [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“](#) auf Seite 71.

- 4. Beziehen Sie die in [Tabelle 13-5](#) angegebenen erforderlichen Patches.

Patches zum Download in das /tmp-Verzeichnis erhalten Sie unter:  
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

- 5. Wenden Sie zunächst den entsprechenden Web Proxy Server Core und bei Bedarf die Lokalisierungs-Patches aus [Tabelle 13-5](#) an.

patchadd /tmp/patch\_ID

6. Stellen Sie sicher, dass die Patch-Aktualisierungen erfolgreich durchgeführt wurden:
- ```
showrev -p | grep proxy
```
- Die Ausgabe sollte die Versionen der in [Schritt 5](#) angewendeten Patch-IDs zurückgeben.
7. Starten Sie die in [Schritt 2](#) angehaltenen Web Proxy Server-Instanzen neu.
- ```
WebProxyServer-base/proxy-instanceName/start
```

**Aktualisieren der Release 4-Version von Web Proxy Server (Linux)**

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Web Proxy Server haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

*Zu berücksichtigende Aspekte bei der Aktualisierung (Linux)*

Bei der Aktualisierung der Web Proxy Server-Software auf Java ES Release 5 unter Linux sind dieselben Aspekte wie unter Solaris zu berücksichtigen (siehe „[Zu berücksichtigende Aspekte bei der Aktualisierung](#)“ auf Seite 276). Die Aktualisierungs-Patches für Linux unterscheiden sich jedoch von den Aktualisierungs-Patches für Solaris.

Die Patches für die Aktualisierung von Web Proxy Server auf Release 5 unter Linux OS werden in der folgenden Tabelle aufgeführt:

**Tabelle 13-6** Patches<sup>1</sup> für die Aktualisierung von Web Proxy Server unter Linux

| Beschreibung                   | Patch-ID und RPM-Namen                                                                          |
|--------------------------------|-------------------------------------------------------------------------------------------------|
| Web Proxy Server Core          | 120983-06 <ul style="list-style-type: none"><li>sun-proxyserver-4.0-6.5.i386.rpm</li></ul>      |
| Web Proxy Server-Lokalisierung | 122965-01 <ul style="list-style-type: none"><li>sun-proxyserver-Locale-4.0.4.i386.rpm</li></ul> |

1. Diese Patch-Versionsnummern sind für die Aktualisierung auf Java ES Release 5 mindestens erforderlich. Wenn neuere Versionen verfügbar sind, verwenden Sie anstelle der in dieser Tabelle genannten Versionen die neueren Versionen.

**Aktualisierungsverfahren (Linux)**

Das im Folgenden beschriebene Verfahren ist für Web Proxy Server auf dem Computer anzuwenden, auf dem die Aktualisierung durchgeführt wird.

---

**VORSICHT** Eine Aktualisierung von Java ES Release 4 auf Java ES Release 5 unter Linux kann nicht rückgängig gemacht werden.

---

1. Melden Sie sich als Root oder Superuser an.

`su -`

2. Halten Sie alle derzeit ausgeführten Instanzen von Web Proxy Server und Administration Server an.

`WebProxyServer-base/proxy-instanceName/stop`

`WebProxyServer-base/proxy-admserv/stop`

3. Synchronisieren Sie alle gemeinsam genutzten Komponenten auf Release 5, sofern dies noch nicht erfolgt ist.

Siehe auch „[Web Proxy Server-Abhängigkeiten aktualisieren](#)“ auf Seite 269.

4. Die erforderlichen Patches und die RPM-Namen lassen sich anhand der entsprechenden Patch-Nummern aus [Tabelle 13-6](#) entnehmen. Verwenden Sie diese Informationen, um die Versionsnummern für den RPM zu erhalten.

Patches zum Download in das /tmp-Verzeichnis erhalten Sie unter:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

5. Wenden Sie zunächst den Core und anschließend bei Bedarf die Lokalisierungs-RPMs für Web Proxy Server aus [Tabelle 13-6](#) an.

`rpm -Fvh sun-proxyserver-version.i386.rpm`

6. Stellen Sie sicher, dass die Patch-Aktualisierungen erfolgreich durchgeführt wurden:

`rpm -qa | grep sun-proxyserver`

Die neuen Versionsnummern der RPMs sollten zurückgegeben werden.

7. Starten Sie die in [Schritt 2](#) angehaltenen Web Proxy Server-Instanzen neu.

`WebProxyServer-base/proxy-instanceName/start`

## Überprüfen der Aktualisierung

Sie können die Aktualisierung von Web Proxy Server auf Release 5 überprüfen, indem Sie die Web Proxy Server-Instanz mit der Option `-version` starten.

`WebProxyServer-base/proxy-admserv/start -version`

Ausgabewerte finden Sie in [Tabelle 13-4 auf Seite 268](#).

## Aufgaben nach der Aktualisierung

Mit Ausnahme der in „[Aktualisierungsverfahren \(Solaris\)](#)“ auf Seite 270 und „[Aktualisierungsverfahren \(Linux\)](#)“ auf Seite 271 beschriebenen Schritte müssen keine weiteren Aufgaben nach der Aktualisierung durchgeführt werden.

## Aufheben der Aktualisierung (Solaris)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Verfahren zum Aufheben der Aktualisierung Web Proxy Server haben, sowie eine Beschreibung des eigentlichen Verfahrens zum Aufheben der Aktualisierung.

### *Zu berücksichtigende Aspekte beim Aufheben der Aktualisierung (Solaris)*

Das Verfahren zum Aufheben der Aktualisierung auf Release 5 von Web Proxy Server entspricht größtenteils dem Verfahren zum Aktualisieren auf Release 5 in umgekehrter Reihenfolge.

### *Verfahren zum Aufheben der Aktualisierung (Solaris)*

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Halten Sie alle derzeit ausgeführten Instanzen von Web Proxy Server und Administration Server an.

```
WebProxyServer-base/proxy-instanceName/stop
```

```
WebProxyServer-base/proxy-admserv/stop
```

3. Entfernen Sie die Patches aus [Tabelle 13-5 auf Seite 270](#).

```
patchrm patch_ID
```

4. Starten Sie die in [Schritt 2](#) angehaltenen Web Proxy Server-Instanzen neu.

```
WebProxyServer-base/proxy-instanceName/start
```

# Aktualisierung von Web Proxy Server von Version 3.6

Dieser Abschnitt enthält Informationen zur Aktualisierung von Web Proxy Server von Version 3.6 auf Java ES 5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Web Proxy Server-Aktualisierung von Version 3.6](#)

## Einführung

Berücksichtigen Sie bei der Aktualisierung von Web Proxy Server auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt mit dem Java ES-Installationsprogramm, um die Release 5-Version von Web Proxy Server in einem anderen Verzeichnis als dem Verzeichnis für Version 3.6 zu installieren. Anschließend wird Web Proxy Server Administration Server für die Migration der Konfigurationseinstellungen (jedoch nicht des Cache-Inhalts) von Version 3.6 auf Release 5 verwendet.
- **Aktualisierungsabhängigkeiten.** Die Installation von gemeinsam genutzten Komponenten erfolgt automatisch durch das Java ES-Installationsprogramm bei der Aktualisierung von Web Proxy Server auf Release 5.
- **Rückwärtskompatibilität.** Die Rückwärtskompatibilität der Release 5-Version von Web Proxy Server zu Version 3.6 ist gewährleistet. Eine Ausnahme bilden jedoch die Plug-Ins, die mit der von Version 3.6 unterstützten NSAPI-Schnittstelle entwickelt wurden; diese müssen mit der von Release 5 unterstützten NSAPI-Schnittstelle neu kompiliert werden.
- **Aufheben der Aktualisierung.** Das Aufheben der Aktualisierung von Web Proxy Server auf Release 5 erfolgt durch das Zurückkehren zur Version 3.6, die bei der Aktualisierung unverändert beibehalten wurde.
- **Plattformspezifische Aspekte.** Der Ansatz zur Aktualisierung von Web Proxy Server ist auf allen Solaris-Plattformen identisch; Version 3.6 wird jedoch nicht auf Linux-Plattformen unterstützt.



## Web Proxy Server-Aktualisierung von Version 3.6

Dieser Abschnitt bietet einen Überblick über das Verfahren zur Aktualisierung von Web Proxy Server auf Java ES Release 5. Web Proxy Server wurde zuvor nicht unter Linux unterstützt. Daher wird eine Aktualisierung von Web Proxy Server auf Java ES Release 5 nur auf der Solaris-Plattform durchgeführt. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren von Version 3.6 von Web Proxy Server](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Version 3.6-Aktualisierung](#)

### Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung von Web Proxy Server beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Web Proxy Server-Aktualisierungsabhängigkeiten](#)
- [Web Proxy Server-Daten sichern](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

### *Aktuelle Versionsinformationen überprüfen*

Sie können die aktuelle Version von Web Proxy Server durch Eingabe des folgenden Befehls überprüfen:

```
WebProxyServer-base/proxy-serverid/start -version
```

**Tabelle 13-7** Web Proxy Server-Ausgaben der Versionsüberprüfung

| Java ES Release                    | Web Proxy Server-Versionsnummer |
|------------------------------------|---------------------------------|
| Version 3.6 (kein Java ES-Release) | 3.6                             |
| Release 4                          | 4.0.1                           |
| Release 5                          | 4.0.4                           |

### *Web Proxy Server-Aktualisierungsabhängigkeiten*

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Das Java ES-Installationsprogramm, das für die Aktualisierung von Web Proxy Server auf Release 5 verwendet wird, aktualisiert jedoch automatisch alle gemeinsam genutzten Komponenten, von denen Web Proxy Server abhängig ist (siehe [Tabelle 1-7 auf Seite 51](#)).

### *Web Proxy Server-Daten sichern*

Bei der Aktualisierung von Web Proxy Server auf Release 5 werden keine Version 3.6-Konfigurationsdaten geändert. Sämtliche nicht gespeicherte Änderungen der Version 3.6-Konfigurationsdaten, die mit der Verwaltungsschnittstelle vorgenommen wurden, müssen jedoch vor der Aktualisierung gespeichert werden.

### *Erforderliche Konfigurationsinformationen und Passwörter abrufen*

Für die Aktualisierung von Version 3.6 benötigen Sie den Installationsverzeichnispfad der installierten Version.

## **Aktualisieren von Version 3.6 von Web Proxy Server**

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Web Proxy Server haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung*

Alle Web Proxy Server-Instanzen, die demselben installierten Web Proxy Server-Image entsprechen, können aktualisiert werden. Die Migration der Konfigurationsdaten muss jedoch für jede Instanz einzeln durchgeführt werden. Diese Instanzen sollten während der Migration beendet werden. So wird sichergestellt, dass es zu keinen Anschlusskonflikten kommt, wenn die migrierte Instanz gestartet wird.

### *Aktualisierungsverfahren*

Das im Folgenden beschriebene Verfahren ist für die Web Proxy Server-Software auf dem Computer anzuwenden, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

`su -`

2. Installieren Sie Web Proxy Server Release 5.

- a.** Führen Sie das Java ES-Installationsprogramm aus der Java ES Release 5-Verteilung aus.
- b.** Wählen Sie auf der Seite für die Komponentenauswahl Web Proxy Server.
- c.** Wählen Sie die Option „Jetzt konfigurieren“.
- d.** Beenden Sie das Java ES-Installationsprogramm, nachdem die Installation abgeschlossen wurde.

3. Migrieren Sie die Konfigurationseinstellungen in die neu installierte Version.  
Dieser Vorgang muss für jede Web Proxy Server-Instanz einzeln durchgeführt werden.

- a. Starten Sie Web Proxy Server Administration Server.

*WebProxyServer-base/proxy-admserv/start*

- b. Melden Sie sich bei der grafischen Verwaltungsoberfläche an.
- c. Klicken Sie auf die Registerkarte „Server“ und klicken Sie anschließend auf „Server migrieren“.
- d. Geben den Installationsverzeichnispfad für Version 3.6 an.
- e. Wählen Sie die zu migrierende Instanz aus.
- f. Klicken Sie auf die Schaltfläche „Migrate“.

Nach erfolgreicher Migration wird in der Migrationsanzeige eine Liste zusätzlicher Konfigurationen angezeigt, die manuell durchgeführt werden müssen. Es werden die Daten angegeben, die hinzugefügt werden müssen, sowie die entsprechende Konfigurationsdatei.

Weitere Informationen zur Migration von Konfigurationseinstellungen finden Sie im *Sun Java System Web Proxy Server 4.0.4 Installation and Migration Guide*, <http://docs.sun.com/doc/819-5492>.

4. Nehmen Sie die in [Schritt f](#) angegebenen Konfigurationsänderungen vor.

Weitere Informationen finden Sie im *Sun Java System Web Proxy Server 4.0.4 Configuration File Reference*, <http://docs.sun.com/doc/819-5494>.

## Überprüfen der Aktualisierung

Sie können die Aktualisierung von Web Proxy Server auf Release 5 überprüfen, indem Sie die Web Proxy Server-Instanz mit der Option `-version` starten.

*WebProxyServer-base/proxy-serverid/start -version*

Ausgabewerte finden Sie in [Tabelle 13-7 auf Seite 275](#).

## Aufgaben nach der Aktualisierung

Mit Ausnahme der in [„Aktualisierungsverfahren“ auf Seite 276](#) beschriebenen Schritte müssen keine weiteren Aufgaben nach der Aktualisierung durchgeführt werden.

## Aufheben der Version 3.6-Aktualisierung

Die unter „[Aktualisieren von Version 3.6 von Web Proxy Server](#)“ auf Seite 276 beschriebene Aktualisierung von Web Proxy Server auf Release 5 kann nicht rückgängig gemacht werden. Sie können jedoch zur Version 3.6 zurückkehren, da diese bei der Aktualisierung auf Release 5 unverändert beibehalten wurde.



# Access Manager

In diesem Kapitel wird die Aktualisierung der Access Manager-Software von früheren Java ES-Versionen auf Java ES 5 (Release 5) beschrieben: Sun Java System Access Manager 7.1.

Das Kapitel enthält einen allgemeinen Überblick über die Aspekte und Verfahren bezüglich der verschiedenen Aktualisierungswege von Access Manager, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Access Manager“ auf Seite 282
- „Aktualisieren von Access Manager von Java ES Release 4“ auf Seite 290
- „Aktualisieren von Access Manager von Java ES Release 3“ auf Seite 315
- „Aktualisieren der Access Manager Release 2-Version Java ES“ auf Seite 320

---

**HINWEIS** Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf zwei verschiedene Verzeichnispfade, die im Folgenden als *AccessManager-base* und *AccessManagerConfig-base* angegeben werden. Wenn Access Manager erstmalig installiert wurde, wurden diese Pfade mindestens teilweise als Installationsverzeichnis angegeben. Wenn nicht, wurde vom Java ES-Installationsprogramm ein Standardwert zugewiesen.

Die Standardwerte für diese Verzeichnispfade sind in der folgenden Tabelle aufgelistet.

---

**Tabelle 14-1** Access Manager Verzeichnispfade

| Variable des Pfadnamens         | Solaris OS      | Linux OS              |
|---------------------------------|-----------------|-----------------------|
| <i>AccessManager-base</i>       | /opt/SUNWam     | /opt/sun/identity     |
| <i>AccessManagerConfig-base</i> | /etc/opt/SUNWam | /etc/opt/sun/identity |

## Überblick über Aktualisierungen von Access Manager

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Access Manager auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5 Access Manager](#)
- [Access Manager Wegweiser für die Aktualisierung von](#)
- [Access Manager-Daten](#)
- [Access Manager Vorgehensweise zur Aktualisierung](#)

---

**HINWEIS** Die Access Manager-Versionen vor Java ES Release 3 wurden als Identity Server bezeichnet. Verweise auf Identity Server beziehen sich demnach auf Vorgängerversionen der Java ES Access Manager-Komponente.

---

## Über Java ES Release 5 Access Manager

Java ES Release 5 Access Manager stellt eine Minor-Release dar. Das Programm enthält eine Reihe von Fehlerkorrekturen und Optimierungen in Bezug auf Java ES Release 4 Access Manager, welches eine Major-Release darstellte. Eine der Erweiterungen in Release 5 ist eine neue Überwachungsfunktion basierend auf dem Java ES Monitoring Framework. Weitere Informationen über Erweiterungen der Release 5 finden Sie in den *Sun Java System Access Manager 7.1 Release Notes*, <http://docs.sun.com/doc/820-0360>.

Ähnlich wie Release 4 unterstützt Release 5 Access Manager mehrere Identitäts-Repositories bzw. Benutzerdatenspeicher. Access Manager für Release 5 unterstützt daher nicht mehr nur ein LDAP-Directory, wie beispielsweise Directory Server, sondern auch andere Datenspeicherprotokolle und -formate.



Im Front-End wird die Access Manager-Konsole für die Konfiguration der neuen Access Manager-Dienste und -Identitäts-Repositories verwendet.

Um die Rückwärtskompatibilität mit anderen Java ES-Komponenten zu gewährleisten, kann Release 5 im Legacy-Modus ausgeführt werden. Dieser Modus unterstützt die Java ES-Komponenten, die von Access Manager-Diensten von Release 3 abhängig sind (weitere Informationen finden Sie unter [„Kompatibilität“ auf Seite 286](#)).

## Access Manager Wegweiser für die Aktualisierung von

[Tabelle 14-2](#) zeigt die unterstützten Wege für die Aktualisierung von Access Manager auf Java ES Release 5. Die Tabelle gilt sowohl für das Solaris- als auch für das Linux-Betriebssystem.

**Tabelle 14-2** Wege für die Aktualisierung auf Java ES 5 (Release 5): Access Manager 7.1

| Java ES Release | Access Manager Version                                      | Allgemeiner Ansatz                                                                                                                                                                         | Neukonfiguration erforderlich                                                                                                            |
|-----------------|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Release 4       | Sun Java System Access Manager 7.0 2005Q4                   | Direkte Aktualisierung:<br>Verwendung eines Skripts zum Entfernen der Release 4-Version vor der Aktualisierung. Anschließend vollständige Installation und Neukonfiguration von Release 5. | Konfigurationsdaten<br>Angepasste JSPs für Access Manager-Konsole und Authentifizierungs-Benutzer schnittstelle (UI)<br>Directory-Schema |
| Release 3       | Sun Java System Access Manager 6.3 2005Q1                   | Direkte Aktualisierung:<br>Verwendung eines Skripts zum Entfernen der Release 3-Version vor der Aktualisierung. Anschließend vollständige Installation und Neukonfiguration von Release 5. | Konfigurationsdaten<br>Angepasste JSPs für Access Manager-Konsole und Authentifizierungs-Benutzer schnittstelle (UI)<br>Directory-Schema |
| Release 2       | Sun Java System Identity Server 6.2 2004Q2 und auch 6.2 SP1 | Direkte Aktualisierung:<br>Verwendung eines Skripts zum Entfernen der Release 2-Version vor der Aktualisierung. Anschließend vollständige Installation und Neukonfiguration von Release 5. | Konfigurationsdaten<br>Angepasste JSPs für Access Manager-Konsole und Authentifizierungs-Benutzer schnittstelle (UI)<br>Directory-Schema |

**Tabelle 14-2** Wege für die Aktualisierung auf Java ES 5 (Release 5): Access Manager 7.1

| Java ES Release       | Access Manager Version                                                                                               | Allgemeiner Ansatz                                                                                                                                                                                                                                                                                                                                                  | Neukonfiguration erforderlich                                                                                                                    |
|-----------------------|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Release 1             | Sun ONE Identity Server 6.1                                                                                          | Keine direkte Aktualisierung:<br>Sie können jedoch zunächst auf Release 3 aktualisieren, wie im <i>Java Enterprise System 2005Q1 Aktualisierungs- und Migrationshandbuch</i> ( <a href="http://docs.sun.com/doc/819-0062">http://docs.sun.com/doc/819-0062</a> ) beschrieben.<br><br>Führen Sie anschließend eine Aktualisierung von Release 3 auf Release 5 durch. | Konfigurationsdaten<br><br>Angepasste JSPs für Access Manager-Konsole und Authentifizierungs-Benutzer schnittstelle (UI)<br><br>Directory-Schema |
| Versionen vor Java ES | Sun ONE Identity Server 6.0 oder 6.0 SP 1 oder<br><br>iPlanet Directory Server Access Management Edition (DSAME) 5.1 | Keine direkte Aktualisierung.                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                  |

## Access Manager-Daten

Wie andere Java ES-Komponenten verwendet auch Access Manager verschiedene Datentypen, die bei einer Aktualisierung möglicherweise auf eine aktualisierte Version migriert werden müssen. Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Access Manager-Software betroffen sein können.

**Tabelle 14-3** Access Manager Verwendung der Daten

| Datentyp                                                                | Standort                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Verwendung                                                                             |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Konfigurationsdaten                                                     | <i>AccessManagerConfig-base/config/AMConfig.properties</i><br><i>AccessManagerConfig-base/config/serverconfig.xml</i><br>JAR-Dateien für Authentifizierung und benutzerdefinierte Module<br><i>AccessManager-base/lib</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Konfiguration von Access Manager und die Integration mit einem Back-End-Datenspeicher. |
| Zugriffssteuerung und Konfigurationsdateien für Webcontainer            | Webserver 7.0 (Java ES Release 5)<br>Datei <i>server.policy</i> und <i>server.xml</i> in <i>WebServer7Config-base/https-configName/config</i><br>Webserver 6.x (Java ES Release 2, 3 und 4)<br>Datei <i>server.policy</i> und <i>server.xml</i> in <i>WebServer6-base/https-hostname/config</i><br>Anwendungsserver 8.x (Java ES Release 3, 4 und 5):<br>Datei <i>server.policy</i> und <i>domain.xml</i> in <i>AppServer8Config-base/domains/domainName/config</i><br>Anwendungsserver 7.x (Java ES Release 2):<br>Datei <i>server.policy</i> und <i>server.xml</i> in <i>AppServer7Config-base/domains/domainName/config</i><br>WebSphere und WebLogic:<br>Bei einer Konfiguration von Access Manager für diese Webcontainer werden die entsprechenden Richtlinien- und Konfigurationsdaten geändert. | Konfiguration der Access Manager-Webcontainer-Instanz.                                 |
| Benutzerdefinierte Daten (Webcontainer, benutzerdefinierte JSP-Dateien) | Administratorkonsole: (Java ES Release 2 und 3):<br><i>AccessManager-base/web-src/applications</i><br>Administratorkonsole: (Java ES Release 4 und 5):<br><i>AccessManager-base/web-src/services</i><br>Authentifizierungs-UI:<br><i>AccessManager-base/web-src/services</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Konfiguration der Access Manager-Administrationsschnittstelle.                         |

**Tabelle 14-3** Access Manager Verwendung der Daten

| Datentyp                                                       | Standort         | Verwendung                                                                                                                                                                                                    |
|----------------------------------------------------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Directory-Schema<br>Dienstekonfiguration<br>n<br>Benutzerdaten | Directory Server | Access Manager bietet Authentifizierungs- und Autorisierungsdienste für Endbenutzer. Diese Dienste basieren auf den in einem Verzeichnis gespeicherten Dienstkonfigurations-, Benutzer- und Richtliniendaten. |
| Dynamische<br>Anwendungsdaten                                  | Keine            | Anwendungsdaten, wie beispielsweise zum Sitzungsstatus, werden von Access Manager nicht dauerhaft gespeichert.                                                                                                |

# Access Manager Vorgehensweise zur Aktualisierung

Ihre Vorgehensweise bei der Aktualisierung von Access Manager hängt grundsätzlich von den zahlreichen in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) erläuterten Aspekten ab: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

Dieser Abschnitt konzentriert diese grundsätzliche Erläuterung auf Access Manager, indem Probleme dargestellt werden, die möglicherweise Ihren Aktualisierungsplan für Access Manager beeinflussen.

## Kompatibilität

Release 5 Access Manager ist rückwärts kompatibel mit Release 4 Access Manager. Bei Release 4 Access Manager handelt es sich jedoch um eine Major-Release, die (außer bei Konfiguration für den Betrieb im Legacy-Modus) nicht kompatibel mit früheren Releases ist. Ähnlich verhält es sich bei Release 5 Access Manager: Wird das Programm nicht für den Betrieb im Legacy-Mode konfiguriert, ist es nicht rückwärts kompatibel mit Release 3 Access Manager (oder Release 4 Access Manager im Legacy-Modus).

Des Weiteren ist Release 5 Access Manager unabhängig vom Modus nicht rückwärts kompatibel mit Release 2 Access Manager; eine Interaktion von Release 5 Access Manager mit Release 2 Access Manager SDK und *umgekehrt* ist nicht möglich.

Release 5 Access Manager unterstützt in der Konfiguration im neuen Realm-Modus mehrere Identitäts-Repositories und Datenspeicherprotokolle. Die Directory-Daten müssen in eine neue Struktur migriert werden, um den Betrieb im Realm-Modus zu unterstützen. Des Weiteren unterstützt der Realm-Modus keine weiteren Java ES-Komponenten, wie z. B. Portal Server, oder Sun Java Communications Suite-Komponenten, wie z. B. Communications Express und Messaging Server.

Bei einer Konfiguration für den Legacy-Modus ist Release 5 Access Manager jedoch mit wenigen Ausnahmen (siehe *Sun Java System Access Manager 7.1 Release Notes*, <http://docs.sun.com/doc/820-0360>) rückwärts kompatibel mit Release 3 Access Manager und entsprechenden Directory-Daten.

Der Legacy-Modus ist für die Unterstützung anderer Java ES-Komponenten sowie für ältere Versionen der Access Manager-Richtlinienagenten erforderlich, die nicht mit Access Manager im Realm-Modus interagieren können. Diese Inkompatibilität spielt bei einer Aktualisierung eine wichtige Rolle. Für die meisten Java ES-Bereitstellungen ergibt sich daraus, dass Access Manager auf Release 5 im Legacy-Modus aktualisiert werden sollte.

Selbst bei einer Konfiguration für den Betrieb im Legacy-Modus ist Release 5 Access Manager jedoch nicht kompatibel mit Release 3 oder früheren Sun Java Communications Suite-Komponenten. Falls Access Manager auf Release 5 aktualisiert wird, muss Release 3 oder eine frühere Version von Delegierter Administrator ebenfalls auf Release 5 aktualisiert werden, um die Verfügbarkeit von Messaging Server und Calendar Server zu gewährleisten. An sich ist eine Aktualisierung von Messaging Server und Calendar Server auf Release 5 jedoch nicht erforderlich.

Die Release 5 Access Manager-Konsole unterstützt wie die Release 4-Konsole sowohl den Realm- als auch den Legacy-Modus. Wenn Sie Access Manager jedoch für den Betrieb im Legacy-Modus konfiguriert haben, können Sie weiterhin die nur für den Legacy-Modus konzipierte Konsole der Release 2 und Release 3 verwenden.

## Access Manager-Abhängigkeiten

Access Manager-Abhängigkeiten zu anderen Java ES-Komponenten beeinflussen möglicherweise das Verfahren für die Aktualisierung und Neukonfiguration der Access Manager-Software. Änderungen der Access Manager-Schnittstellen oder -Funktionen könnten beispielsweise eine aktualisierte Version der Komponenten erforderlich machen, von denen Access Manager abhängig ist. Welche dieser Komponenten aktualisiert werden müssen, hängt von dem jeweiligen Aktualisierungsweg ab.

Für Access Manager bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Access Manager ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)). Die Aktualisierung von Access Manager hängt möglicherweise von den aktualisierten Versionen dieser gemeinsam genutzten Komponenten ab.
- **Webcontainer.** Access Manager verfügt über eine obligatorische Abhängigkeit zu Webcontainerdiensten, die entweder über Java ES Webserver, Java ES Anwendungsserver oder Drittanbieter-Webcontainer (von Weblogic und WebSphere) bereitgestellt werden können. Access Manager-Aktualisierungen erfordern möglicherweise die Migration von benutzerdefinierten JSPs für die Access Manager-Konsole oder für die Authentifizierungs-UI in die aktualisierte Access Manager-Umgebung.
- **Directory Server.** Access Manager verfügt über eine obligatorische Abhängigkeit zu Directory Server, das für die Speicherung von Konfigurations- und Benutzerdaten eingesetzt wird. Daher sind bei einer Aktualisierung von Access Manager möglicherweise Erweiterungen des Directory-Schemas erforderlich.

### Aktualisierungsszenarios für den Webcontainer

Access Manager kann in einem Webcontainer eingesetzt werden, der entweder von Webserver oder Anwendungsserver bereitgestellt wurde. Daher kann die Aktualisierung von Access Manager auf Release 5 dadurch kompliziert werden, dass möglicherweise auch der Webcontainer auf Release 5 aktualisiert werden muss, in dem er eingesetzt wird. Es sind eine Reihe von Aktualisierungsszenarios für den Webcontainer möglich, die in der folgenden Tabelle dargestellt werden.

**Tabelle 14-4** Szenarien für die Access Manager-Aktualisierung für Webcontainer

| Szenario   | Webcontainer, in dem Access Manager ursprünglich bereitgestellt wurde | Webcontainer, in dem Access Manager nach der Aktualisierung bereitgestellt wird | Anwendbare Access Manager Aktualisierungswege:<br>Aktualisierungen von |
|------------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Szenario 1 | Webserver 6.x                                                         | Webserver 6.x                                                                   | Release 2<br>Release 3<br>Release 4                                    |
| Szenario 2 | Webserver 6.x                                                         | Webserver 7.0                                                                   | Release 2<br>Release 3<br>Release 4                                    |

**Tabelle 14-4** Szenarien für die Access Manager-Aktualisierung für Webcontainer

| <b>Szenario</b> | <b>Webcontainer, in dem Access Manager ursprünglich bereitgestellt wurde</b> | <b>Webcontainer, in dem Access Manager nach der Aktualisierung bereitgestellt wird</b> | <b>Anwendbare Access Manager Aktualisierungswege:<br/>Aktualisierungen von</b> |
|-----------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Szenario 3      | Anwendungsserver 8.1                                                         | Anwendungsserver 8.1                                                                   | Release 3<br>Release 4                                                         |
| Szenario 4      | Anwendungsserver 8.1                                                         | Anwendungsserver 8.2                                                                   | Release 3<br>Release 4                                                         |
| Szenario 5      | Anwendungsserver 7x                                                          | Anwendungsserver 8.2                                                                   | Release 2                                                                      |

Gehen Sie bei der Aktualisierung von Access Manager (z. B. bei der Verwendung des Skripts `amconfig`) vorsichtig vor und geben Sie die für das in [Tabelle 14-4](#) entsprechend dargestellte Aktualisierungsszenario korrekten Werte ein, insbesondere wenn dies eine Aktualisierung einer Major-Version des Webcontainers beinhaltet.

# Aktualisieren von Access Manager von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von Access Manager von Java ES 2005Q4 (Release 4) auf Java ES 5 (Release 5). In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Vollständige Aktualisierung von Access Manager Release 4](#)
- [Aktualisierung mehrerer Instanzen](#)
- [Ausschließliche Aktualisierung der Release 4-Version von Access Manager SDK](#)

## Einführung

Berücksichtigen Sie bei der Aktualisierung von Java ES von Access Manager Release 4 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch das Entfernen vorheriger Versionen von Binärdateien und die Neuinstallation von Release 5. Für das Entfernen von Release 4 steht das Skript `ampre71upgrade` zur Verfügung; für die Installation von Release 5 wird das Java ES-Installationsprogramm verwendet. Anschließend wird die Neukonfiguration von Access Manager mithilfe des Skripts `amconfig` durchgeführt und die Migration des Directory-Schemas mithilfe des Skripts `amupgrade`.
- **Aktualisierungsabhängigkeiten.** Access Manager ist von einer Reihe von gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)), die alle automatisch vom Java ES-Installationsprogramm auf Release 5 aktualisiert werden, wenn Sie eine Aktualisierung von Access Manager durchführen. Dies beinhaltet die Unterstützung des neuen Java ES Monitoring Framework, das eine Reihe von gemeinsam genutzten Komponenten erfordert, die für Release 4 Access Manager nicht erforderlich sind.

Access Manager Release 5 ist zudem von Directory Server und Webserver (oder Anwendungsserver oder Drittanbieter-Webcontainern) abhängig, wie unter „[Access Manager-Abhängigkeiten](#)“ auf [Seite 287](#) beschrieben. Hierbei handelt es sich jedoch nicht um zwingende Aktualisierungsabhängigkeiten; eine Aktualisierung dieser Komponenten ist hinsichtlich der Aktualisierung von Access Manager auf Release 5 optional.



- **Rückwärtskompatibilität.** Release 5 Access Manager ist kompatibel mit Release 4, jedoch nicht mit früheren Releases von Access Manager (siehe „Kompatibilität“ auf Seite 286).
- **Aufheben der Aktualisierung.** Für das Aufheben der Access Manager-Aktualisierung steht kein Dienstprogramm zur Verfügung. Das Aufheben der Aktualisierung ist aufgrund der erheblichen Anzahl an Neukonfigurationen, die für das Zurücksetzen von Access Manager in seinen ursprünglichen Zustand erforderlich ist, nicht durchführbar. Die beste Vorgehensweise für das Zurückkehren zur vorherigen Version ist das Erstellen einer Parallelinstallation unter Verwendung gesicherter Konfigurationsdateien und das anschließende Testen der Parallelinstallation, bevor die Aktualisierung durchgeführt wird. Dadurch können Sie falls nötig zur Parallelinstallation zurückkehren.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Access Manager ist für das Solaris- und Linux-Betriebssystem identisch. In den folgenden Verfahren werden plattformspezifische Befehle bzw. Dateispeicherorte entsprechend gekennzeichnet.

## Vollständige Aktualisierung von Access Manager Release 4

In diesem Abschnitt wird die vollständige Aktualisierung von Access Manager von Java ES Release 4 auf Java ES Release 5 beschrieben:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren von Release 4 von Access Manager](#)
- [Überprüfen der Access Manager-Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

### Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung von Access Manager beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Access Manager-Abhängigkeiten aktualisieren](#)
- [Directory Server-Daten sichern](#)

- [Konfigurationsinformationen von Access Manager Release 4 sichern](#)
- [Benutzerdefinierte Webcontainer-Dateien sichern](#)
- [Release 4 Access Manager-Protokolldateien und -Debug-Dateien sichern](#)
- [Benutzerdefinierte Lokalisierungsdateien sichern](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

*Aktuelle Versionsinformationen überprüfen*

Sie können die aktuelle Version von Access Manager mithilfe des folgenden Befehls überprüfen:

```
AccessManager-base/bin/amadmin --version
```

**Tabelle 14-5** Access ManagerAusgaben der Versionsüberprüfung

| Java ES Release | Access Manager-Versionsnummer |
|-----------------|-------------------------------|
| Release 2       | 6.2                           |
| Release 3       | 6 2005Q1                      |
| Release 4       | 7 2005Q4                      |
| Release 5       | 7.1                           |

*Access Manager-Abhängigkeiten aktualisieren*

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren. Für Access Manager bestehen zu einer Reihe gemeinsam genutzter Komponenten zwingende Aktualisierungsabhängigkeiten (siehe [Tabelle 1-7 auf Seite 51](#)).

Bei der Aktualisierung der Abhängigkeiten der Access Manager-Produktkomponenten sollte in der unten angegebenen Reihenfolge vorgegangen werden (unter Auslassung der bereits aktualisierten Abhängigkeiten), bevor Sie Access Manager aktualisieren. Die Aktualisierung gemeinsam genutzter Komponenten erfolgt in der Regel automatisch durch das Java ES-Installationsprogramm.

1. **Gemeinsam genutzte Komponenten.** Anleitungen für die Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie unter „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71. Alle gemeinsam genutzten Komponenten, die von Access Manager benötigt werden, werden jedoch automatisch vom Java ES-Installationsprogramm aktualisiert, wenn Sie eine Aktualisierung von Access Manager auf Release 5 durchführen.
2. **Directory Server (soft upgrade dependency).** Anleitungen für die Aktualisierung von Directory Server auf Release 4 finden Sie in Kapitel 5, „Directory Server“ auf Seite 109.
3. **Webcontainer-Software (keine zwingende Abhängigkeit).** Anweisungen zur Aktualisierung von Webserver und Anwendungsserver finden Sie in Kapitel 7, „Webserver“ auf Seite 143 bzw. Kapitel 11, „Anwendungsserver“ auf Seite 219.

Wenn die Webcontainer-Software nicht bereits vor Access Manager aktualisiert wurde, wird Access Manager bei der Aktualisierung (unter Verwendung des Skripts `amconfig`) für den vorhandenen Webcontainer konfiguriert und neu bereitgestellt.

### *Directory Server-Daten sichern*

Beim Aktualisierungsvorgang von Access Manager wird das Directory Server-Schema geändert. Daher sollten Sie vor der Aktualisierung von Access Manager Ihre Directory Server-Daten über die Directory Server-Konsole oder mit einem Befehlszeilen-Dienstprogramm, wie `db2bak`, sichern. Sie können `db2ldif` für das Sichern des Schemas und des Directory Information Tree (DIT) von Access Manager verwenden.

Weitere Informationen über das Sichern von Directory Server erhalten Sie im *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide* (<http://docs.sun.com/doc/819-0995>).

### *Konfigurationsinformationen von Access Manager Release 4 sichern*

Da die Neukonfiguration der Access Manager-Software von Release 5 eine Neukonfiguration von Release 4 erforderlich macht, ist es wichtig, eine Sicherungskopie der Konfigurationsdateien an einem bekannten Speicherort anzulegen. Folgende Dateien sollten gesichert werden:

- Die Datei `AMConfig.properties`  
*AccessManagerConfig-base/config/AMConfig.properties*
- Die Datei `serverconfig.xml`  
*AccessManagerConfig-base/config/serverconfig.xml*
- Webcontainer-Konfigurationsdateien:

- Bei Webserver: Entnehmen Sie den Speicherort der Dateien `server.policy` und `server.xml` der [Tabelle 14-3 auf Seite 285](#).
- Bei Anwendungsserver: Entnehmen Sie den Speicherort der Dateien `server.policy` und `domain.xml` der [Tabelle 14-3 auf Seite 285](#).
- Bei Drittanbieter-Webcontainern: die entsprechenden Konfigurationsdateien
- JAR-Dateien für Authentifizierung und benutzerdefinierte Module.  
*AccessManager-base/lib*

### ***Benutzerdefinierte Webcontainer-Dateien sichern***

Wenn Access Manager auf benutzerdefinierte Webcontainer-Dateien verweist, sollten Sie diese Dateien sichern. Zu diesen benutzerdefinierten Dateien gehören möglicherweise folgende Dateien:

- Benutzerdefinierte Access Manager-JSP-Konsolenseiten:
  - Realm/Legacy-Konsole (im Lieferumfang von Java ES Release 4 enthalten)  
*AccessManager-base/web-src/services/*
  - Konsole nur für den Legacy-Modus (im Lieferumfang von Java ES Release 2 und 3 enthalten)  
*AccessManager-base/web-src/applications/*
- Benutzerdefinierte JSP-Authentifizierungsseiten der Benutzeroberfläche.  
*AccessManager-base/web-src/services/*
- Benutzerdefinierte XML-Dateien.  
*AccessManagerConfig-base/config/xml/*

---

|             |                                                                                                                                                             |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TIPP</b> | Notieren Sie Ihre benutzerdefinierten Dateien, sodass Sie diese mit dem gesicherten Code nach der Aktualisierung von Access Manager erneut anwenden können. |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### ***Release 4 Access Manager-Protokolldateien und -Debug-Dateien sichern***

Um eine Analyse der Systemstatusinformationen durchführen zu können, sollten Sie die Protokoll- und Debug-Dateien sichern. Diese Dateien befinden sich an folgenden Speicherorten:

- Debug-Dateien  
*/var/AccessManager-base/debug*

- Protokolldateien  
*/var/AccessManager-base/logs*

### *Benutzerdefinierte Lokalisierungsdateien sichern*

Falls Sie Änderungen an den vom Java ES-Installationsprogramm installierten lokalisierten Dateien vorgenommen haben oder eine neue Sprachlokalisierung hinzugefügt haben, die nicht vom Java ES-Installationsprogramm installiert wird, sollten Sie diese benutzerdefinierten Dateien sichern. Zu den benutzerdefinierten Dateien gehören möglicherweise folgende Dateien:

- Lokalisierung der benutzerdefinierten Access Manager-Benutzeroberfläche  
*AccessManager-base/locale/\*\_Locale.properties*
- Benutzerdefinierte JSP-Authentifizierungsseiten der Benutzeroberfläche  
*AccessManager-base/web-src/services/config/auth/default\_Locale*
- Übersetzungen der benutzerdefinierten Online-Hilfe  
*AccessManager-base/web-src/services/html/Locale*

### *Erforderliche Konfigurationsinformationen und Passwörter abrufen*

Um Access Manager aktualisieren zu können, müssen Sie bestimmte Konfigurationsinformationen angeben können, einschließlich:

- Benutzer-ID und Passwort des Access Manager-Administrators
- Benutzer-ID und Passwort für LDAP
- Directory Manager-Name und -Passwort für die von Access Manager verwendete Directory Server-Instanz

## Aktualisieren von Release 4 von Access Manager

Die Aktualisierung der Access Manager-Software auf Java ES Release 5 beinhaltet Verfahren zur Neukonfiguration von Access Manager und zur Migration der Access Manager-Daten.

### *Zusammenfassung der Aktualisierung*

Das Verfahren zur Aktualisierung von Access Manager besteht aus zwei Schritten:

1. [Aktualisieren Sie die Mobile Access-Software für Access Manager.](#)
2. [Entfernen Sie die Java ES Release 4-Version von Access Manager.](#) Verwenden Sie das Skript `ampre71upgrade`.

3. Falls die Aktualisierung auf Release 5 lokalisiert werden muss, entfernen Sie die Lokalisierungspakete von Release 4. Dieser Schritt muss manuell durchgeführt werden.
4. Installieren Sie die Java ES Release 5-Version von Access Manager. Verwenden Sie das Java ES-Installationsprogramm mit der Option „Später konfigurieren“.
5. Passen Sie die JSPs für Access Manager erneut an.
6. Heben Sie die Bereitstellung von Access Manager auf, führen Sie eine Neukonfiguration durch und stellen Sie ihn erneut in einem Webcontainer bereit. Verwenden Sie das Skript amconfig.
7. Aktualisieren Sie die Directory-Struktur und das Directory-Schema. Verwenden Sie das Skript amupgrade.

Die einzelnen Schritte werden in den folgenden Verfahren beschrieben.

*Aktualisierungsverfahren*

1. Aktualisieren Sie die Mobile Access-Software für Access Manager.

Die Mobile Access-Software für Access Manager muss durch Anwendung von Patches auf Release 4 aktualisiert werden. Die erforderlichen Patches sind in der folgenden Tabelle aufgelistet:

**Tabelle 14-6** Patches<sup>1</sup> für die Aktualisierung der Access Manager Mobile Access-Software

| Beschreibung           | Patch-ID: Solaris 9 & 10 | Patch-ID: Linux                                                                                                                                            |
|------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mobile Access-Software | 119530-05 (SPARC)        | 119532-05                                                                                                                                                  |
|                        | 119531-05 (x86)          | <ul style="list-style-type: none"><li>• sun-identity-mobileaccess-6.2-25.3.i386.rpm</li><li>• sun-identity-mobileaccess-config-6.2-25.3.i386.rpm</li></ul> |

1. Diese Patch-Versionsnummern sind für die Aktualisierung auf JavaES Release 5 mindestens erforderlich. Wenn neuere Versionen verfügbar sind, verwenden Sie anstelle der in dieser Tabelle genannten Versionen die neueren Versionen.

- a. Beziehen Sie die erforderlichen Patches anhand der in [Tabelle 14-6](#) angegebenen Patch-Nummern.

Patches zum Download in das /tmp-Verzeichnis erhalten Sie unter:  
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

- b. Führen Sie alle der Installation des Patches vorangestellten Aufgaben wie in den README-Dateien der Patches beschrieben durch.
- c. Rufen Sie die Werte für folgende vom Patch angeforderten Parameter ab:

**Tabelle 14-7** Patch-Parameter für Mobile Access

| Parameter                  | Wert                           |
|----------------------------|--------------------------------|
| Directory-Manager-DN       | Standard: cn=Directory Manager |
| Directory-Manager-Passwort |                                |

- d. Wenden Sie die in [Tabelle 14-6](#) angegebenen Patches an.

*Unter Solaris:*

```
patchadd /tmp/patch_ID
```

*Unter Linux:*

```
./update
```

Führen Sie alle Aufgaben, die nach der Installation des Patches durchgeführt werden müssen, wie in den README-Dateien der Patches beschrieben durch.

2. Entfernen Sie die Java ES Release 4-Version von Access Manager.
  - a. Melden Sie sich als Root an dem Computer an, der als Host für Access Manager für Release 4 dient, oder melden Sie sich als Superuser an.  
  
su -
  - b. Wechseln Sie in das Verzeichnis *os\_arch/Product/identity\_svr/Tools* in der Java ES Release 5-Verteilung, wobei *os\_arch* Ihrer Plattform entspricht, wie z. B. *Solaris\_sparc*.
  - c. Rufen Sie die Werte der folgenden vom *ampre71upgrade*-Skript angeforderten Parameter ab:

**Tabelle 14-8** Access Manager Konfigurationsparameter: *ampre71upgrade*

| Parameter                  | Wert                                                                                      |
|----------------------------|-------------------------------------------------------------------------------------------|
| Directory Server-Host      | Legen Sie den vollständigen Namen fest:<br><i>hostname.domain</i>                         |
| Directory Server-Anschluss | Geben Sie eine Anschlussnummer an, die keine SSL-Nummer ist <sup>1</sup><br>Standard: 389 |

**Tabelle 14-8** Access Manager Konfigurationsparameter: ampre71upgrade

| Parameter                            | Wert                                              |
|--------------------------------------|---------------------------------------------------|
| Top-Level-Administrator, DN          | Standard:<br>uid=amadmin,ou=People,default_org_DN |
| Passwort für Top-Level-Administrator |                                                   |
| Verzeichnis für Sicherungsdateien    | Standard: AccessManager-base                      |

1. Der Vorgang vor der Aktualisierung wird nicht erfolgreich abgeschlossen, wenn Sie den Wert für einen Directory Server-SSL-Anschluss angeben, wie beispielsweise den SSL-Standardwert 636.

- d. Stellen Sie sicher, dass Directory Server ausgeführt wird. Wenn nicht, starten Sie ihn.
- e. Führen Sie das Skript ampre71upgrade aus.

./ampre71upgrade

Mithilfe des Skripts werden Access Manager-Konfigurationsdateien gespeichert und Release 4-Basispakete entfernt. Lokalisierte Pakete müssen manuell wie in Schritt 3 unten dargestellt entfernt werden.

- 3. Falls die Aktualisierung auf Release 5 lokalisiert werden muss, entfernen Sie die Lokalisierungspakete von Release 4.

Das in Schritt 2 oben ausgeführte Skript ampre71upgrade entfernt nicht die Lokalisierungspakete, daher müssen sie wie folgt manuell entfernt werden.

Unter Solaris:

- a. Suchen Sie die Lokalisierungspakete.

```
pkginfo | grep SUNWaml
pkginfo | grep SUNWamclnt
pkginfo | grep SUNWamdistaauth
```

- b. Entfernen Sie alle Lokalisierungspakete, die in Schritt a oben gefunden wurden.

```
pkgrm SUNWamlGebietsschema
pkgrm SUNWamclntGebietsschema
pkgrm SUNWamdistaauthGebietsschema
```



*Unter Linux:*

- a. Suchen Sie die Lokalisierungs-RPMs.

```
rpm -qa | grep sun-identity-sdk-*
rpm -qa | grep sun-identity-clientsdk-*
rpm -qa | grep sun-identity-distauth-*
```

- b. Entfernen Sie alle Lokalisierungs-RPMs, die in [Schritt a](#) oben gefunden wurden.

```
rpm -e sun-identity-sdk-Gebietsschema-*
rpm -e sun-identity-clientsdk-Gebietsschema-*
rpm -e sun-identity-distauth-Gebietsschema-*
```

4. Installieren Sie die Java ES Release 5-Version von Access Manager.

Führen Sie die folgenden Schritte aus:

- a. Führen Sie das Java ES-Installationsprogramm auf dem Computer aus, der als Host für Access Manager für Release 4 dient.

```
cd Java ES Release 5-Bereitstellung/os_arch
./installer
```

wobei *os\_arch* der Plattform entspricht, wie z. B. *Solaris\_sparc*.  
(Verwenden Sie die Option `installer -nodisplay` für die Befehlszeilenschnittstelle.)

Nach der Willkommenseite sowie der Lizenzvereinbarung wird eine Seite für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten erkannt werden, die direkt vom Java ES-Installationsprogramm aktualisiert werden können, wird der Status als „aktualisierbar“ angezeigt.)

- b. Wählen Sie auf der Seite für die Komponentenauswahl Access Manager.
- c. Geben Sie das gleiche Installationsverzeichnis an, in dem Release 4 installiert war.
- d. Wählen Sie die Option „Später konfigurieren“ aus.
- e. Falls erforderlich, wählen Sie die Option zur Installation von lokalisierten Paketen.
- f. Beenden Sie das Java ES-Installationsprogramm, nachdem die Installation abgeschlossen wurde.

5. Passen Sie die JSPs für Access Manager erneut an.

Wenden Sie die angepassten JSPs der Release 4-Version für die Access Manager-Konsole und die Authentifizierungs-Benutzerschnittstelle (UI), die Sie unter „[Benutzerdefinierte Webcontainer-Dateien sichern](#)“ auf Seite 294 gespeichert haben, erneut an.

Kopieren Sie anschließend die benutzerdefinierten JSP-Dateien in die richtigen Verzeichnisse:

- Realm/Legacy Access Manager-Konsole  
*AccessManager-base/web-src/services/console*
- Access Manager-Konsole nur für den Legacy-Modus  
*AccessManager-base/web-src/applications/console*
- Authentifizierungs-UI:  
*AccessManager-base/web-src/services/config/auth/default* oder  
*AccessManager-base/web-src/services/config/auth/default\_Locale*  
(wobei *Locale* für einen Gebietsschema-Indikator wie *ja* steht)

Weitere Informationen finden Sie im *Sun Java System Access Manager 7.1 Developer's Guide* ( <http://docs.sun.com/doc/819-4675>).

6. Heben Sie die Bereitstellung von Access Manager auf, führen Sie eine Neukonfiguration durch und stellen Sie ihn erneut in einem Webcontainer bereit.

Konfigurieren Sie Access Manager für Ihren bestimmten Webcontainer, indem Sie das Skript `amconfig` ausführen. Das Skript `amconfig` (und die dazugehörige Vorlagen-Eingabedatei `amsamplesilent`) befindet sich im folgenden Verzeichnis:

*AccessManager-base/bin*

Informationen zum Skript `amconfig` und zur Vorlagendatei `amsamplesilent` erhalten Sie im *Sun Java System Access Manager 7.1 Administration Guide* (<http://docs.sun.com/doc/819-4670>).

Führen Sie folgende Schritte durch, um Access Manager neu zu konfigurieren und erneut im Webcontainer bereitzustellen:

- a. Wenn Sie Ihre Webcontainer-Software wie unter „[Access Manager-Abhängigkeiten aktualisieren](#)“ auf Seite 292 beschrieben aktualisieren, stellen Sie sicher, dass die Aktualisierung abgeschlossen wurde.

- b. Stellen Sie sicher, dass die Administrationsinstanz Ihres Webcontainers ausgeführt wird und sich in einem Modus befindet, der wie in der Tabelle unten dargestellt vom Skript `amconfig` unterstützt wird:

**Tabelle 14-9** Administrative Server-Modi mit Unterstützung von `amconfig`

| Webcontainer                                          | Unterstützter Modus      | Standardmäßige Anschlussnummer |
|-------------------------------------------------------|--------------------------|--------------------------------|
| Anwendungsserver (8.x):<br>Java ES Release 3, 4 und 5 | SSL (sicher)<br>ohne SSL | 4849                           |
| Webserver (7.0):<br>Java ES Release 5                 | SSL (sicher)             | 8989                           |
| Webserver (6.x):<br>Java ES Release 2, 3 und 4        | ohne SSL                 | 8888                           |

- c. Wenn der Webcontainer im SSL-Modus ausgeführt wird, stellen Sie sicher, dass die SSL-Zertifikate des Containers nicht abgelaufen und weiterhin gültig sind.
- d. Falls Access Manager in Release 5 Webserver eingesetzt wird, deaktivieren Sie alle Java ES-Komponenten, die von Access Manager abhängig sind und in der gleichen Instanz wie Access Manager ausgeführt werden.

Dazu gehören möglicherweise Komponenten wie Portal Server oder Sun Java Communications Suite-Komponenten wie Communications Express, Instant Messaging oder Delegierter Administrator.

Verwenden Sie dabei folgendes Verfahren:

- I. Melden Sie sich bei `https://host:8989` als Administrator an.
- II. Wechseln Sie zu „Virtual Server bearbeiten“.
- III. Wählen Sie die Registerkarte „Web-Anwendungen“.
- IV. Wählen Sie alle Anwendungen aus, die von Access Manager abhängig sind.
- V. Klicken Sie auf „Deaktivieren“.
- VI. Klicken Sie auf „Speichern“.
- VII. Klicken Sie auf „Ausstehende Bereitstellung | Konfiguration bereitstellen“.

Die Konfigurationsänderungen werden in die Webserver-Instanz übernommen.

- e. Vergewissern Sie sich, dass Directory Server und der entsprechende Webcontainer ausgeführt werden.
- f. Erstellen Sie eine Eingabedatei `amconfig`, die auf der Vorlagen-Eingabedatei `amsamplesilent` basiert:

```
cp amsamplesilent config-file
```

(In den darauffolgenden Schritten wird angenommen, dass `config-file` sich im gleichen Verzeichnis wie `amsamplesilent` befindet.)

- g. Legen Sie die Konfigurationsparameter in `config-file` fest.

Sämtliche Parameter müssen ordnungsgemäß festgelegt werden. Einige der Werte können aus der Datei `AMConfig.properties` migriert werden; andere Werte müssen entsprechend des Aktualisierungsverfahrens festgelegt werden, wie in der folgenden Tabelle gezeigt.

**Tabelle 14-10**Access Manager Konfigurationsparameter: `amconfig`

| Parameter                       | Wert                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aktualisierungsparameter</b> |                                                                                                                                                                                                                                                                                                                                    |
| DEPLOY_LEVEL                    | 26 als Wert für die Aufhebung der Bereitstellung festlegen oder<br>1 als Wert für die Neukonfiguration und erneute Bereitstellung festlegen                                                                                                                                                                                        |
| DIRECTORY_MODE                  | 5 als Wert festlegen                                                                                                                                                                                                                                                                                                               |
| AM_REALM <sup>1</sup>           | disabled als Wert festlegen, falls der Legacy-Modus aktiviert ist<br>enabled als Wert festlegen, falls der Realm-Modus aktiviert ist<br>Standard: aktiviert                                                                                                                                                                        |
| JAVA_HOME                       | JDK Release 5-Verzeichnis als Wert festlegen:<br><code>/usr/java/jdk1.5.0_04/</code>                                                                                                                                                                                                                                               |
| WEB_CONTAINER                   | WS als Wert für Webserver 7.x festlegen<br>WS6 als Wert für Webserver 6.x festlegen<br>AS8 als Wert für Anwendungsserver 8.x festlegen<br>WAS5 als Wert für IBM WebSphere 5.x festlegen<br>WL8 als Wert für BEA WebLogic 8.x festlegen<br>Füllen Sie zusätzlich nur den entsprechenden Abschnitt von <code>config-file</code> aus. |

**Tabelle 14-10** Access Manager Konfigurationsparameter: amconfig

| Parameter                                                                        | Wert                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WS_INSTANCE<br>(Wenn Webserver 7.x als Webcontainer verwendet wird)              | Legen Sie den Verzeichnisnamen der Instanzkonfiguration unter Beachtung der Groß-/Kleinschreibung fest: <code>https-configName1</code><br><br>Das Verzeichnis befindet sich im folgenden Pfad:<br><code>WebServer7Config-base/https-configName1</code> |
| WS61_INSTANCE<br>(Wenn Webserver 6.x als Webcontainer verwendet wird)            | Legen Sie den Verzeichnisnamen der Instanzkonfiguration unter Beachtung der Groß-/Kleinschreibung fest: <code>https-instanceName</code><br><br>Das Verzeichnis befindet sich im folgenden Pfad:<br><code>WebServer6-base/https-instanceName1</code>    |
| AS81_INSTANCE<br>(Wenn Anwendungsserver 8.x als Webcontainer verwendet wird)     | Anwendungsserver 8.x <code>instanceName</code> als Wert festlegen<br><br>Standard: Server                                                                                                                                                              |
| AS81_INSTANCE_DIR<br>(Wenn Anwendungsserver 8.x als Webcontainer verwendet wird) | Domänenverzeichnis von Anwendungsserver 8.x für die Instanz festlegen. Standardmäßig ist dies<br><br><code>AppServer8Config-base/domains/domain1</code>                                                                                                |
| AS81_DOCS_DIR<br>(Wenn Anwendungsserver 8.x als Webcontainer verwendet wird)     | docroot-Verzeichnis von Anwendungsserver 8.x für die Instanz festlegen. Standardmäßig ist dies<br><br><code>AppServer8Config-base/domains/domain1/docroot</code>                                                                                       |

**Aus AMConfig.properties migriert.**

|                          |                                                             |
|--------------------------|-------------------------------------------------------------|
| SERVER_PROTOCOL          | <code>com.ipplanet.am.server.protocol</code>                |
| SERVER_PORT              | <code>com.ipplanet.am.server.port</code>                    |
| SERVER_HOST              | <code>com.ipplanet.am.server.host</code>                    |
| DS_HOST                  | <code>com.ipplanet.am.directory.host</code>                 |
| DS_PORT                  | <code>com.ipplanet.am.directory.port</code>                 |
| ROOT_SUFFIX <sup>2</sup> | <code>com.ipplanet.am.defaultOrg</code>                     |
| CONSOLE_DEPLOY_URI       | <code>com.ipplanet.am.console.deploymentDescriptor</code>   |
| SERVER_DEPLOY_URI        | <code>com.ipplanet.am.services.deploymentDescriptor</code>  |
| PASSWORD_DEPLOY_URI      | <code>com.sun.identity.password.deploymentDescriptor</code> |
| AM_ENC_PWD <sup>2</sup>  | <code>am.encryption.pwd<sup>3</sup></code>                  |

1. Weitere Informationen zum Realm- oder Legacy-Modus finden Sie unter „Kompatibilität“ auf Seite 286.

2. Der Wert dieses Parameters sollte identisch mit dem Wert in der vorherigen Version von Access Manager sein.

3. Wenn sowohl Access Manager als auch Access Manager SDK bereitgestellt werden, muss der Wert dieser Eigenschaft bei der Access Manager-Instanz und ihren jeweiligen Access Manager SDK-Instanzen identisch sein.

Legen Sie für die übrigen Parameter die Werte fest, die in der zu aktualisierenden Release 4-Konfiguration verwendet wurde, es sei denn, Sie ändern den Webcontainer oder die Passwörter. Wenn Sie z. B. Webserver auf Release 5 aktualisiert haben, geben Sie die folgenden Werte an:

**Tabelle 14-11**amconfig-Parameter: Release 5Webserver

| Parameter      | Wert                                                                            |
|----------------|---------------------------------------------------------------------------------|
| WS_CONFIG      | Der Name der Webserver-Konfiguration: <i>configName</i>                         |
| WS_INSTANCE    | <i>https-configName</i>                                                         |
| WS_HOME        | <i>WebServer7Config-base</i>                                                    |
| WS_PROTOCOL    | http oder https                                                                 |
| WS_HOST        | Vollständiger Hostname, auf dem die Webserver-Instanz nach Verbindungen sucht   |
| WS_PORT        | Anschluss, auf dem die Webserver-Instanz nach Verbindungen sucht                |
| WS_ADMINPORT   | Anschluss, auf dem die Webserver-Administrationsinstanz nach Verbindungen sucht |
| WS_ADMIN       | Benutzer-ID des Webserver-Administrators                                        |
| WS_ADMINPASSWD | Webserver-Administratorpasswort                                                 |

- h. Führen Sie amconfig aus, um die Bereitstellung von Access Manager aufzuheben.

Legen Sie in *config-file* für DEPLOY\_LEVEL den Wert 26 fest.

```
cd /AccessManager-base/bin
./amconfig -s AccessManager-base/bin/config-file
```

- i. Prüfen Sie, ob der Common Agent Container ausgeführt wird.

```
netstat -an | grep 11163
```

Wenn er nicht ausgeführt wird, starten Sie ihn.

```
/usr/sbin/cacoadm start
```

- j. Führen Sie `amconfig` aus, um Access Manager neu zu konfigurieren und in einem Webcontainer bereitzustellen.

Legen Sie in `DEPLOY_LEVEL` für *config-file* den Wert 1 fest.

```
cd /AccessManager-base/bin
```

```
./amconfig -s AccessManager-base/bin/config-file
```

## 7. Aktualisieren Sie die Directory-Struktur und das Directory-Schema.

Die Release 5-Version von Access Manager kann parallel zur Directory-Struktur von Release 4 vorhanden sein, die Struktur muss jedoch für die Unterstützung der Release 5-Funktionen bearbeitet werden. Aktualisieren Sie die Directory-Struktur und das Directory-Schema von Access Manager auf Release 5, indem Sie das Skript `amupgrade` ausführen, das im folgenden Verzeichnis installiert ist:

- *Unter Solaris:*  
`AccessManager-base/upgrade/scripts`
  - *Unter Linux:*  
`AccessManager_base/identity/upgrade/scripts`
- a. Rufen Sie die Werte für folgende vom `amupgrade`-Skript angeforderten Parameter ab:

**Tabelle 14-12** Access Manager Konfigurationsparameter: `amupgrade`

| Parameter                                   | Wert                                                                                      |
|---------------------------------------------|-------------------------------------------------------------------------------------------|
| Vollständiger Hostname für Directory Server | Legen Sie den vollständigen Namen fest:<br><i>hostname.domäne</i>                         |
| Directory ServerPort                        | Geben Sie eine Anschlussnummer an, die keine SSL-Nummer ist <sup>1</sup><br>Standard: 389 |
| Directory-Manager-DN                        | Standard: <code>cn=Directory Manager</code>                                               |
| Directory-Manager-Passwort                  |                                                                                           |
| Top-Level-Administrator, DN                 | Standard:<br><code>uid=amadmin,ou=People,default_org_DN</code>                            |

**Tabelle 14-12**Access Manager Konfigurationsparameter: amupgrade

| Parameter                                                                                                                        | Wert                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Passwort für Top-Level-Administrator                                                                                             |                                                                                                                                                                                                                 |
| Realm-Modus aktivieren<br>(Dieser Parameterwert wird nicht<br>angefordert, wenn vom Release<br>4-Realm-Modus aktualisiert wird.) | Y/N: Yes bedeutet, der Realm-Modus wird<br>aktiviert und die Dienstdaten werden in<br>die neue Realm-Struktur migriert <sup>2</sup> . No<br>(Standard) bedeutet, die Dienstdaten<br>verbleiben im Legacy-Modus. |

1. Sie müssen einen SSL-Anschluss für Directory Server festlegen, der sich vom SSL-Standardwert 636 unterscheidet.
2. Siehe auch „[Migrieren zum Realm-Modus](#)“ auf Seite 308.

- b. Führen Sie das Skript amupgrade aus.

```
cd AccessManager-base/upgrade/scripts
./amupgrade
```

Wenn die Aktualisierung erfolgreich ausgeführt wurde, zeigt das Skript eine Meldung an, die besagt, dass die Aktualisierung abgeschlossen wurde.

- c. Überprüfen Sie die folgende Aktualisierungs-Protokolldatei auf Informationen zu den Directory-Schema-Erweiterungen.

```
Unter Solaris:
/var/sadm/install/logs/
 Sun_Java_System_Access_Manager_upgrade_dit_log.mmddhhmm
```

```
Unter Linux:
/var/log/Sun_Java_System_Access_Manager_upgrade_dit_log.mmddhhmm
```

8. Aktivieren Sie alle Komponenten, die in [Schritt d auf Seite 301](#) deaktiviert wurden.
9. Starten Sie den Webcontainer neu, in dem Access Manager bereitgestellt wurde.
10. Starten Sie Access Manager.

Starten Sie den Webcontainer neu, in dem Access Manager bereitgestellt wurde.



## Überprüfen der Access Manager-Aktualisierung

Nach Abschluss des Aktualisierungsvorgangs überprüfen Sie wie folgt, ob der Aktualisierungsvorgang erfolgreich war:

1. Prüfen Sie mit folgendem Befehl die Aktualisierung der Access Manager-Pakete:

```
AccessManager-base/bin/amadmin --version
```

Ausgabewerte finden Sie in [Tabelle 14-5 auf Seite 292](#).

2. Überprüfen Sie den Status der Aktualisierung anhand folgender Installations-Protokolldateien im Verzeichnis `/var/sadm/install/logs`:
  - `Java_Shared_Component_Install.timestamp`
  - `Java_Enterprise_System_install.Atimestamp`
  - `Java_Enterprise_System_install.Btimestamp`
  - `Java_Enterprise_System_Summary_Report_install.timestamp`
3. Überprüfen Sie den Status der Access Manager-Migration anhand des Terminalfensters auf Fehler, während Sie das Skript `amupgrade` ausführen.

Prüfen Sie auch die folgende Protokolldatei im Verzeichnis `/var/sadm/install/logs` :

```
Sun_Java_System_Access_Manager_upgrade_dit_log.timestamp
```

4. Überprüfen Sie die Access Manager-Fehlerbehebungsdateien auf Fehler.

Die Dateien befinden sich an dem in der Eigenschaft `com.ipplanet.services.debug.directory` der Datei `AMConfig.properties` angegebenen Speicherort. Die Standardwerte sind:

*Unter Solaris:*

```
/var/opt/SUNWam/debug
```

*Unter Linux:*

```
/var/opt/sun/identity/debug
```

## Aufgaben nach der Aktualisierung

Beachten Sie die für die folgenden Situationen erforderlichen Aufgaben nach der Aktualisierung:

- [Migrieren zum Realm-Modus](#)
- [Security Assertion Markup Language](#)

- **Aktualisierungs-Patches**

### *Migrieren zum Realm-Modus*

Wenn Sie während der Aktualisierung von Access Manager auf Release 5 zum Realm-Modus migriert haben (wenn Sie also amupgrade für die Aktualisierung der Directory-Struktur und des Directory-Schemas verwendet haben, und Yes für die Aktivierung des Realm-Modus angegeben haben), führen Sie die folgenden Schritte durch:

1. Öffnen Sie die Datei `AccessManagerConfig-base/config/AMConfig.properties`.
2. Prüfen Sie den Wert der folgenden Eigenschaft:  
`com.sun.identity.sm.ldap.enableProxy`
3. Wenn die Eigenschaft nicht auf `false` festgelegt ist, legen Sie sie manuell auf `false` fest.

### *Security Assertion Markup Language*

Wenn Sie den Dienst für Security Assertion Markup Language (SAML) verwenden, müssen Sie das SAML-Authentifizierungsmodul über die Access Manager-Konsole hinzufügen und aktivieren. Informationen zum Erstellen der SAML-Authentifizierungsmodul-Instanz finden Sie im *Sun Java System Access Manager 7.1 Administration Guide* (<http://docs.sun.com/doc/819-4670>).

### *Aktualisierungs-Patches*

Nach der Aktualisierung sollten Sie die aktuellen Access Manager 7.1-Patches herunterladen, die Anweisungen zum Anwenden der Patches befolgen und jegliche Aufgaben nach der Patchkonfiguration durchführen.

### **Aufheben der Aktualisierung**

Für das Zurücksetzen von Access Manager in den Zustand vor der Aktualisierung stehen keine Skripte zur Verfügung. Der Vorgang muss manuell unter Verwendung der Access Manager-Daten durchgeführt werden, die im Rahmen der Aufgaben vor der Aktualisierung aktualisiert wurden (siehe „[Release 4 Access Manager-Protokolldateien und -Debug-Dateien sichern](#)“ auf Seite 294). Das Aufheben der Aktualisierung ist sehr umständlich und daher nicht praktisch.

Eine Vorgehensweise zum Aufheben der Aktualisierung ist die Neuinstallation von Release 4 und Migration aller gesicherter Konfigurationsdateien zu den entsprechenden Speicherorten. Eine weitere Vorgehensweise ist das Erstellen eines Parallelsystems anhand der gesicherten Konfigurationsdateien vor der Aktualisierung sowie das Testen des Parallelsystems vor dem Aktualisierungsversuch.

## Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen wird Access Manager auf mehreren Computersystemen bereitgestellt, um Hochverfügbarkeit und Skalierbarkeit zu gewährleisten.

Es ist in der Regel empfehlenswert, die Access Manager-Instanzen nacheinander zu aktualisieren, ohne den Dienst zu unterbrechen. In diesem Abschnitt wird die Vorgehensweise bei einem solchen Rolling Upgrade von Release 4 Access Manager auf Release 5 dargestellt.

---

**HINWEIS** Das Aktualisieren mehrerer Instanzen von Access Manager, die auf demselben Hostsystem installiert sind, wird in der aktuellen Version nicht unterstützt. Wenn auf demselben Host mehrere Instanzen vorhanden sind, müssen Sie im Anschluss an die Aktualisierung der Hauptinstanz die zusätzlichen Instanzen neu erstellen.

---

Die in der folgenden Abbildung dargestellte Bereitstellungsarchitektur erläutert die Vorgehensweise bei einem Rolling Upgrade.

**Abbildung 14-1** Beispiel für Bereitstellungsarchitektur für mehrere Access Manager-Instanzen



In dieser Architektur wird auf mehrere Access Manager-Instanzen über ein Lastenausgleichsprogramm zugegriffen, während diese Instanzen wiederum auf ein Directory zugreifen, das für die Multimaster-Replikation (MMR) eingerichtet wurde. Während andere Directory Server-Replikationsschemata möglich sind, ist MMR repräsentativ für hochverfügbare und skalierbare Directory-Dienste. In [Abbildung 14-1](#) werden die verschiedenen Instanzen von Access Manager und Directory Server gruppiert dargestellt, um den Aktualisierungsvorgang zu erläutern. Access Manager 2 stellt beispielsweise die zweite bis n-te Instanz von Access Manager dar.

Die Vorgehensweise zur Durchführung eines Rolling Upgrade von Release 4 Access Manager auf Release 5 basiert auf der folgenden Interoperabilität: Release 5 Access Manager- und Release 4 Access Manager-Instanzen können auf dem gleichen System eingesetzt und mit dem gleichen Directory betrieben werden, wenn das Directory-Schema nicht auf Release 5 aktualisiert wird.

Daher können Sie bei Access Manager-Instanzen, die auf eine einzige Directory Server-Instanz verweisen, ein Rolling Upgrade durchführen, indem Sie die Aktualisierung des Directory-Schemas erst dann durchführen, wenn alle Access Manager-Instanzen aktualisiert wurden.

Sie können ein Rolling Upgrade von Release 4 Access Manager auf Release 5 anhand der folgenden Vorgehensweise durchführen:

1. Legen Sie eine Sicherungskopie aller Release 4-Konfigurationsinformationen auf allen Access Manager-Instanzen an.
2. Aktualisieren Sie Access Manager 1.
  - a. Deaktivieren Sie Access Manager 1 im Lastenausgleichsprogramm.  
Anfragen werden nicht mehr an Access Manager 1 weitergeleitet.
  - b. Aktualisieren Sie teilweise Access Manager 1.  
Aktualisieren Sie Access Manager wie unter [„Aktualisieren von Release 4 von Access Manager“ auf Seite 295](#) beschrieben. Informationen zur Aktualisierung der Directory-Struktur und des Directory-Schemas finden Sie unter [Schritt 7 auf Seite 305](#).
  - c. Aktivieren Sie Access Manager 1 im Lastenausgleichsprogramm.
3. Aktualisieren Sie Access Manager 2 über Access Manager n.

Um die Anweisungen zu verkürzen, bedeutet "Access Manager 2" in den folgenden Schritten Access Manager 2 bis Access Manager n.

- a. Deaktivieren Sie Access Manager 2 im Lastenausgleichsprogramm.

Anfragen werden nicht mehr an Access Manager 2 weitergeleitet.

- b. Aktualisieren Sie teilweise Access Manager 2.

Aktualisieren Sie jede Instanz von Access Manager wie unter „Aktualisieren von Release 4 von Access Manager“ auf Seite 295 beschrieben. Informationen zur Aktualisierung der Directory-Struktur und des Directory-Schemas finden Sie unter [Schritt 7 auf Seite 305](#).

- c. Aktivieren Sie Access Manager 2 im Lastenausgleichsprogramm.

Anfragen werden wieder an Access Manager 2 weitergeleitet.

4. Aktualisieren Sie die Directory-Struktur und das Directory-Schema von Directory Server 1.

Verwenden Sie das Skript amupgrade wie unter [Schritt 7 auf Seite 305](#) beschrieben. Access Manager 1 bleibt weiterhin funktionstüchtig, da das Schema für Directory Server 2 nicht aktualisiert wird.

## Ausschließliche Aktualisierung der Release 4-Version von Access Manager SDK

In manchen Bereitstellungsarchitekturen wird die Access Manager SDK-Komponente auf einem oder mehreren Computern installiert, auf denen ansonsten keine weiteren Access Manager-Komponenten installiert werden. Access Manager SDK dient als eine Remote-Schnittstelle für Access Manager und muss im selben Betriebsmodus wie Access Manager neu konfiguriert werden: Legacy oder Realm.

Access Manager SDK und der gesamte Access Manager, für den es als Remote-Schnittstelle fungiert, müssen beide auf Release 5 aktualisiert werden. Da Release 5 Access Manager jedoch rückwärts kompatibel mit Release 4 Access Manager SDK ist, sollte Access Manager generell vor der Aktualisierung von Access Manager SDK auf anderen Computern aktualisiert werden.

Als Remote-Schnittstelle für Access Manager ist eine Neukonfiguration des SDK für den Zugriff auf Directory Server nicht erforderlich. Wenn Access Manager SDK zur Unterstützung einer Webkomponente verwendet wird, die von Webcontainerdiensten abhängen, wie beispielsweise Portal Server, muss Access Manager SDK für den entsprechenden Webcontainer konfiguriert werden. Access Manager SDK kann jedoch auch Komponenten unterstützen, die keine Webkomponenten sind, sodass keine Webcontainer-Unterstützung erforderlich ist.

Das Verfahren für die Aktualisierung von Access Manager SDK besteht aus einem Teil des Verfahrens für die vollständige Access Manager-Aktualisierung, basierend auf den oben genannten Merkmalen.

In diesem Abschnitt wird die ausschließliche Aktualisierung von Access Manager SDK von Java ES Release 4 auf Java ES Release 5 beschrieben:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren der Release 4-Version von Access Manager SDK](#)
- [Überprüfen der Access Manager SDK-Aktualisierung](#)
- [Aufheben der Aktualisierung](#)

## Aufgaben vor der Aktualisierung

Die Aufgaben vor der Aktualisierung von Access Manager SDK entsprechen denen für eine vollständige Aktualisierung von Access Manager (siehe [„Aufgaben vor der Aktualisierung“ auf Seite 291](#)), mit Ausnahme der Aufgaben hinsichtlich Directory Server sowie der JSP-Anpassungen des Verwaltungstools von Access Manager. Folgende Aufgaben müssen vor der Aktualisierung von Access Manager SDK durchgeführt werden:

- [„Access Manager-Abhängigkeiten aktualisieren“ auf Seite 292](#)  
Für Access Manager SDK besteht jedoch keine Abhängigkeit zu Directory Server und eine Abhängigkeit zur Webcontainer-Software besteht nur dann, wenn Access Manager SDK in einem Webcontainer ausgeführt wird.
- [„Konfigurationsinformationen von Access Manager Release 4 sichern“ auf Seite 293](#)  
Für Access Manager SDK müssen die Webcontainer-Konfigurationsdateien zudem nur dann gesichert werden, wenn Access Manager SDK in einem Webcontainer ausgeführt wird.
- [„Release 4 Access Manager-Protokolldateien und -Debug-Dateien sichern“ auf Seite 294](#)

Für den Zugriff auf diese Dateien benötigen Sie außerdem den Benutzernamen und das Passwort des Administrators.

## Aktualisieren der Release 4-Version von Access Manager SDK

Der Aktualisierungsvorgang für Access Manager SDK entspricht dem für eine vollständige Aktualisierung von Access Manager, mit Ausnahme der Aufgaben hinsichtlich der Lokalisierung, der JSP-Anpassungen des Verwaltungstools von Access Manager und der Migration des Directory-Schemas.

1. Entfernen Sie die Java ES Release 4-Version von Access Manager SDK.

Folgen Sie den Anweisungen unter „[Entfernen Sie die Java ES Release 4-Version von Access Manager.](#)“ auf Seite 297, entfernen Sie jedoch nur Access Manager SDK.

2. Installieren Sie die Java ES Release 5-Version von Access Manager SDK.

Folgen Sie den Anweisungen unter „[Installieren Sie die Java ES Release 5-Version von Access Manager.](#)“ auf Seite 299, installieren Sie jedoch nur Access Manager SDK.

3. Konfigurieren Sie Access Manager SDK neu.

Folgen Sie den Anweisungen unter „[Heben Sie die Bereitstellung von Access Manager auf, führen Sie eine Neukonfiguration durch und stellen Sie ihn erneut in einem Webcontainer bereit.](#)“ auf Seite 300, setzen Sie jedoch die Werte für den Parameter `DEPLOY_LEVEL` wie folgt:

- Wenn Access Manager SDK für einen Webcontainer konfiguriert ist: `DEPLOY_LEVEL=4` (aktualisieren Sie SDK und konfigurieren Sie den Webcontainer)
- Wenn Access Manager SDK nicht für einen Webcontainer konfiguriert ist: `DEPLOY_LEVEL=3` (aktualisieren Sie nur SDK)

## Überprüfen der Access Manager SDK-Aktualisierung

Sie können die Access Manager SDK-Aktualisierung auf drei verschiedene Arten prüfen:

- Führen Sie Portal Server oder eine andere Komponente aus, die Access Manager SDK als Schnittstelle für Access Manager verwendet und überprüfen Sie, ob die Authentifizierung funktioniert.
- Führen Sie die Access Manager SDK-Beispiele aus, die sich im folgenden Verzeichnis befinden:

*AccessManager-base/samples/sdk*

- Überprüfen Sie den Wert der Eigenschaft `com.ipplanet.am.version` in der Datei `AMConfig.properties`:

*AccessManagerConfig-base/config/AMConfig.properties*

## Aufheben der Aktualisierung

Für das Zurücksetzen von Access Manager in den Zustand vor der Aktualisierung stehen keine Skripte zur Verfügung. Der Vorgang muss manuell unter Verwendung der Access Manager-Daten durchgeführt werden, die im Rahmen der Aufgaben vor der Aktualisierung, aktualisiert wurden (siehe „[Release 4 Access Manager-Protokolldateien und -Debug-Dateien sichern](#)“ auf Seite 294). Das Aufheben der Aktualisierung ist sehr umständlich und daher nicht praktisch.

Eine Vorgehensweise zum Aufheben der Aktualisierung ist die Neuinstallation von Release 4 und Migration aller gesicherter Konfigurationsdateien zu den entsprechenden Speicherorten. Eine weitere Vorgehensweise ist das Erstellen eines Parallelsystems anhand der gesicherten Konfigurationsdateien vor der Aktualisierung sowie das Testen des Parallelsystems vor dem Aktualisierungsversuch.



# Aktualisieren von Access Manager von Java ES Release 3

Das Verfahren für die Aktualisierung von Java ES 2003Q1 (Release 3) Access Manager oder Access Manager SDK auf Release 5 ist ähnlich des Verfahrens für die Aktualisierung von Release 4 Access Manager oder Access Manager SDK auf Release 5. Eine Ausnahme besteht jedoch in der Aktualisierung mehrerer Instanzen.

- [Aktualisierung der Release 3-Version von Access Manager](#)
- [Aktualisierung mehrerer Instanzen](#)

---

**HINWEIS** Release 5 Access Manager ist mit einigen Release 3 Sun Java Communications Suite-Komponenten nicht kompatibel. Falls Access Manager auf Release 5 aktualisiert wird, muss Release 3 oder eine frühere Version von Delegierter Administrator ebenfalls auf Release 5 aktualisiert werden, um die Verfügbarkeit von Messaging Server und Calendar Server zu gewährleisten. An sich ist eine Aktualisierung von Messaging Server und Calendar Server auf Release 5 jedoch nicht erforderlich.

---

## Aktualisierung der Release 3-Version von Access Manager

Um die Release 3-Version von Access Manager oder Access Manager SDK auf Release 4 zu aktualisieren, folgen Sie den Anweisungen unter „[Aktualisieren von Access Manager von Java ES Release 4](#)“ auf Seite 290. Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 3.

## Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen wird Access Manager auf mehreren Computersystemen bereitgestellt, um Hochverfügbarkeit und Skalierbarkeit zu gewährleisten.

Es ist in der Regel empfehlenswert, mehrere Access Manager-Instanzen nacheinander zu aktualisieren, ohne den Dienst zu unterbrechen. In diesem Abschnitt wird die Vorgehensweise bei einem solchen Rolling Upgrade von Release 3 Access Manager auf Release 5 dargestellt.

---

**HINWEIS** Das Aktualisieren mehrerer Instanzen von Access Manager, die auf demselben Hostsystem installiert sind, wird in der aktuellen Version nicht unterstützt. Wenn auf demselben Host mehrere Instanzen vorhanden sind, müssen Sie im Anschluss an die Aktualisierung der Hauptinstanz die zusätzlichen Instanzen neu erstellen.

---

Die in der folgenden Abbildung dargestellte Bereitstellungsarchitektur erläutert die Vorgehensweise bei einem Rolling Upgrade.

**Abbildung 14-2** Beispiel für Bereitstellungsarchitektur für mehrere Access Manager-Instanzen



In dieser Architektur wird auf mehrere Access Manager-Instanzen über ein Lastenausgleichsprogramm zugegriffen, während diese Instanzen wiederum auf ein Directory zugreifen, das für die Multimaster-Replikation (MMR) eingerichtet wurde. Während andere Directory Server-Replikationsschemata möglich sind, ist MMR repräsentativ für hochverfügbare und skalierbare Directory-Dienste. In

[Abbildung 14-1](#) werden die verschiedenen Instanzen von Access Manager und Directory Server gruppiert dargestellt, um den Aktualisierungsvorgang zu erläutern. Access Manager 2 stellt beispielsweise die zweite bis n-te Instanz von Access Manager dar.

Die Vorgehensweise zur Durchführung eines Rolling Upgrade von Release 3 Access Manager auf Release 5 basiert auf der folgenden Bedingung: Release 5 Access Manager kann *nicht* parallel zur Directory-Struktur von Release 3 vorhanden sein. Wenn jedoch Directory Server-Instanzen wie in [Abbildung 14-2](#) dargestellt repliziert werden, können Sie ein Rolling Upgrade unter Verwendung der folgenden Verfahrensweise durchführen:

1. Legen Sie eine Sicherungskopie aller Release 3-Konfigurationsinformationen auf allen Access Manager-Instanzen an.
2. Ändern Sie die Konfiguration von Access Manager 1.
  - a. Konfigurieren Sie Access Manager 1 mit einem Verweis auf Directory Server 2 statt auf Directory Server 1.
  - b. Starten Sie Access Manager 1 neu.

Access Manager 1 wird weiterhin Anfragen bearbeiten, während Access Manager 2 bis Access Manager n aktualisiert wird.

3. Aktualisieren Sie Access Manager 2 über Access Manager n.

Um die Anweisungen zu verkürzen, bedeutet "Access Manager 2" in den folgenden Schritten Access Manager 2 bis Access Manager n.

- a. Deaktivieren Sie Access Manager 2 im Lastenausgleichsprogramm.  
Anfragen werden nicht mehr an Access Manager 2 weitergeleitet.
- b. Aktualisieren Sie teilweise Access Manager 2.

Aktualisieren Sie jede Instanz von Access Manager wie unter [„Aktualisieren von Release 4 von Access Manager“ auf Seite 295](#) beschrieben. Informationen zur Aktualisierung der Directory-Struktur und des Directory-Schemas finden Sie unter [Schritt 7 auf Seite 305](#).

- c. Deaktivieren Sie Directory Server MMR.
- d. Aktualisieren Sie die Directory-Struktur und das Directory-Schema von Directory Server 1.

Verwenden Sie das Skript amupgrade wie unter [Schritt 7 auf Seite 305](#) beschrieben. Access Manager 1 bleibt weiterhin funktionstüchtig, da das Schema für Directory Server 2 nicht aktualisiert wird.

- e. Starten Sie Access Manager 2 neu.
- f. Aktivieren Sie Access Manager 2 im Lastenausgleichsprogramm.  
Anfragen werden wieder an Access Manager 2 weitergeleitet.

4. Aktualisieren Sie Access Manager 1.
  - a. Deaktivieren Sie Access Manager 1 im Lastenausgleichsprogramm.  
Anfragen werden nicht mehr an Access Manager 1 weitergeleitet.
  - b. Aktualisieren Sie teilweise Access Manager 1.  
Aktualisieren Sie Access Manager wie unter „[Aktualisieren von Release 4 von Access Manager](#)“ auf Seite 295 beschrieben. Informationen zur Aktualisierung der Directory-Struktur und des Directory-Schemas finden Sie unter [Schritt 7 auf Seite 305](#).
  - c. Aktivieren Sie Directory Server MMR.  
Das Schema und die Daten von Directory Server 2 sind jetzt aktualisiert.
  - d. Stellen Sie die Konfiguration von Access Manager 1 wieder her, sodass auf Directory Server 1 verwiesen wird.
  - e. Starten Sie Access Manager 1 neu.
  - f. Aktivieren Sie Access Manager 1 im Lastenausgleichsprogramm.  
Anforderungen werden wieder an Access Manager 1 weitergeleitet sowie Directory Server an alle anderen aktualisierten Access Manager-Instanzen.

# Aktualisieren der Access Manager Release 2-Version Java ES

Das Verfahren für die Aktualisierung von Java ES 2004Q2 (Release 2) Access Manager auf Release 5 ist ähnlich wie das Verfahren für die Aktualisierung von Release 4 Access Manager auf Release 5, wie in den folgenden Abschnitten dargestellt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisierung der Release 2-Version von Access Manager](#)
- [Aktualisierung mehrerer Instanzen](#)

So ist auch das Verfahren für die Aktualisierung von Java ES 2004Q2 (Release 2) Access Manager SDK auf Release 5 mit vergleichbaren Ausnahmen ähnlich dem Verfahren für die Aktualisierung von Release 4 Access Manager SDK auf Release 5 (siehe „[Ausschließliche Aktualisierung der Release 4-Version von Access Manager SDK](#)“ auf Seite 311). Die ausschließliche Aktualisierung von Access Manager SDK beinhaltet nicht die Verfahren bezüglich der Lokalisierung, der JSP-Anpassungen des Verwaltungstools von Access Manager sowie die Migration des Directory-Schemas.

Release 2 Access Manager SDK und der gesamte Release 2 Access Manager, für den es als Remote-Schnittstelle fungiert, müssen beide auf Release 5 aktualisiert werden. Eine gleichzeitige Verwendung von einzelnen Release 2- und Release 5-Komponenten wird nicht unterstützt. Daher müssen alle Instanzen von Release 2 Access Manager und Release 2 Access Manager SDK auf allen Computern auf Release 5 aktualisiert werden.

## Aufgaben vor der Aktualisierung

Bevor Sie mit der Aktualisierung von Access Manager beginnen, führen Sie die unter „[Aufgaben vor der Aktualisierung](#)“ auf Seite 291 beschriebenen Verfahren mit den folgenden Ausnahmen und Erweiterungen durch:

- [Access Manager-Abhängigkeiten aktualisieren](#)
- [Directory-Schema aktualisieren](#)
- [Indizieren Sie das Directory neu](#)

## Access Manager-Abhängigkeiten aktualisieren

Im Gegensatz zur Aktualisierung von Release 4 müssen vor der Aktualisierung von Release 2 auf Release 5 alle gemeinsam genutzten Komponenten auf Release 5 aktualisiert werden (siehe [Tabelle 1-7 auf Seite 51](#)) sowie alle lokal vorhandenen Produktkomponenten, von denen Access Manager abhängt.

Halten Sie sich bei der Aktualisierung der Access Manager-Abhängigkeiten an die folgende Reihenfolge und führen Sie alle Aktualisierungen durch, bevor Sie Access Manager aktualisieren. Bereits aktualisierte Abhängigkeiten können Sie überspringen.

1. **Gemeinsam genutzte Komponenten.** Anleitungen für die Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie unter [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#). Gemeinsam genutzte Java ES-Komponenten werden jedoch automatisch vom Installationsprogramm aktualisiert, wenn Sie eine Neukonfiguration von Release 5 Access Manager durchführen.
2. **Directory Server.** Directory Server befindet sich nur in Ausnahmefällen auf demselben Computer wie Access Manager. Anleitungen für die Aktualisierung von Directory Server auf Release 5 sind jedoch in [„Aktualisieren von Directory Server von Java ES Release 2“ auf Seite 126](#) enthalten.
3. **Webcontainer-Software.** Anweisungen zur Aktualisierung von Webserver und Anwendungsserver finden Sie in [„Aktualisieren von Webserver von Java ES Release 3“ auf Seite 169](#) bzw. in [„Aktualisieren von Anwendungsserver von Java ES Release 2“ auf Seite 234](#).

## Directory-Schema aktualisieren

Wenn Directory Server mit dem Directory Preparation Tool der Sun Java Communications Suite konfiguriert wurde (`comm_dssetup.pl`), um Communication Suite-Komponenten wie z. B. Messaging Server und Calendar Server zu unterstützen, müssen Sie zuerst das Directory-Schema mithilfe des Directory Preparation Tool 6.4 aktualisieren, *bevor* Sie Access Manager aktualisieren (weitere Informationen finden Sie im *Sun Java Communications Suite 5 Upgrade Guide*, <http://docs.sun.com/doc/819-7561>). Führen Sie diese der Aktualisierung vorangestellte Aufgabe durch, nachdem Sie die Access Manager-Abhängigkeiten aktualisiert haben.

## Indizieren Sie das Directory neu

Um Komplikationen bei der Aktualisierung von Access Manager nach der Aktualisierung des Directory-Schemas zu vermeiden (siehe [“Directory-Schema aktualisieren,”](#) oben), müssen Sie das Access Manager-Directory-Root-Suffix wie folgt manuell neu indizieren:

*Release 2-Release 4 Directory Server:*

1. `cd serverRoot/slapd-`hostname``
2. `./db2index.pl -D "cn=directory manager" -w passwordFile -n databaseName`  
wobei der standardmäßige *databaseName* `userRoot` lautet.



*Release 5 Directory Server:*

1. `cd DirServer-base/ds6/bin`
2. `./dsconf reindex -D "cn=Directory Manager" -e -w passwordFile suffix`  
wobei
  - e eine unsichere Verbindung kennzeichnet
  - D der Directory Manager ist
  - w eine Passwortdatei ist, in der nur das Passwort gespeichert ist
  - suffix* das Access Manager-Directory-Root-Suffix ist.

Je nach Anzahl der Einträge im Directory kann die Neuindizierung entsprechend lange dauern.

## Aktualisierung der Release 2-Version von Access Manager

Das Verfahren für die Aktualisierung der Release 2-Version von Access Manager auf Release 5 hängt von dem Webcontainer ab, in dem die Access Manager-Software bereitgestellt werden soll.

### Aktualisieren der Release 2-Version von Access Manager: Webserver-Webcontainer

Um die Release 2-Version von Access Manager auf Release 5 zu aktualisieren, wobei die Bereitstellung in einem Webserver-Webcontainer erfolgt, folgen Sie den Anweisungen unter „[Aktualisieren von Release 4 von Access Manager](#)“ auf [Seite 295](#). Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 2.

### Aktualisieren der Release 2-Version von Access Manager: Anwendungsserver-Webcontainer

Wenn Sie die Release 2-Version von Access Manager auf Release 5 aktualisieren möchten, wobei die Bereitstellung in einem Anwendungsserver-Webcontainer erfolgt, kann einer der beiden folgenden Fälle eintreten:

- **Die Release 4-Version von Anwendungsserver wurde neu installiert.** Folgen Sie in diesem Fall den Anweisungen unter „[Aktualisieren von Release 4 von Access Manager](#)“ auf Seite 295, um die Release 2-Version von Access Manager auf Release 5 zu aktualisieren. Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 2.
- **Release 2 Anwendungsserver wurde auf Release 5 aktualisiert.** In diesem Fall wurde die Anwendungsserver-Instanz von Release 2, in der Access Manager ursprünglich bereitgestellt wurde (*instanceName*), bei einer Aktualisierung auf Release 5 in einen vom Aktualisierungsvorgang erstellten Knotenagenten migriert. Für die Aktualisierung von Access Manager in dieser aktualisierten Anwendungsserver-Instanz sind die Schritte in den folgenden Abschnitten erforderlich:

### *Zusammenfassung der Aktualisierung*

Das Verfahren zur Aktualisierung von Access Manager besteht aus zwei Schritten:

1. [Aktualisieren Sie die Mobile Access-Software von Access Manager.](#)
2. [Entfernen Sie die Java ES Release 2-Version von Access Manager.](#) Verwenden Sie das Skript `ampre71upgrade`.
3. [Falls die Aktualisierung auf Release 5 lokalisiert werden muss, entfernen Sie die Lokalisierungspakete von Release 2.](#) Dieser Schritt muss manuell durchgeführt werden.
4. [Installieren Sie die Java ES Release 5-Version von Access Manager.](#) Verwenden Sie das Java ES-Installationsprogramm mit der Option „Später konfigurieren“.
5. [Passen Sie die JSPs für Access Manager erneut an.](#)
6. [Überprüfen Sie, ob Directory Server ausgeführt wird.](#)
7. [Starten Sie die folgenden Anwendungsserver-Instanzen:](#) Domain Administration Server (DAS), Knotenagent und Serverinstanz, in der Access Manager bereitgestellt wird.
8. [Heben Sie die Bereitstellung von Access Manager auf, führen Sie eine Neukonfiguration durch und stellen Sie ihn in der Anwendungsserver-Instanz erneut bereit.](#) Verwenden Sie das Skript `amconfig`.
9. [Stellen Sie sicher, dass die Access Manager-Informationen zu classpath-suffix und server-classpath in die Release 5 Anwendungsserver-Datei domain.xml migriert wurden.](#)
10. [Beenden Sie den Domain Administration Server \(DAS\), den Knotenagenten und die Serverinstanz.](#)

11. Starten Sie den Domain Administration Server (DAS), den Knotenagenten und die Serverinstanz neu.
12. Aktualisieren Sie die Directory-Struktur und das Directory-Schema.  
Verwenden Sie das Skript amupgrade.

Die Schritte werden in dem folgenden Verfahren beschrieben.

### Aktualisierungsverfahren

1. Aktualisieren Sie die Mobile Access-Software von Access Manager.

Die Mobile Access-Software von Access Manager muss durch Anwendung von Patches auf Release 2 aktualisiert werden. Die erforderlichen Patches sind in der folgenden Tabelle aufgelistet:

**Tabelle 14-13** Patches<sup>1</sup> für die Aktualisierung von Access Manager Mobile Access-Software

| Beschreibung           | Patch-ID: Solaris 9 & 10             | Patch-ID: Linux                                                                                                                                                            |
|------------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mobile Access-Software | 119530-05 (SPARC)<br>119531-05 (x86) | 119532-05<br><ul style="list-style-type: none"> <li>• sun-identity-mobileaccess-6.2-25.3.i386.rpm</li> <li>• sun-identity-mobileaccess-config-6.2-25.3.i386.rpm</li> </ul> |

1. Diese Patch-Versionsnummern sind für die Aktualisierung auf Java ES Release 5 mindestens erforderlich. Wenn neuere Versionen verfügbar sind, verwenden Sie anstelle der in dieser Tabelle genannten Versionen die neueren Versionen.

- a. Beziehen Sie die erforderlichen Patches anhand der in [Tabelle 14-6](#) angegebenen Patch-Nummern.  
  
Patches zum Download in das /tmp-Verzeichnis erhalten Sie unter:  
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>
- b. Führen Sie alle der Installation des Patches vorangestellten Aufgaben wie in den README-Dateien der Patches beschrieben durch.
- c. Rufen Sie die Werte für folgende vom Patch angeforderten Parameter ab:

**Tabelle 14-14** Patch-Parameter für Mobile Access

| Parameter            | Wert                           |
|----------------------|--------------------------------|
| Directory-Manager-DN | Standard: cn=Directory Manager |

**Tabelle 14-14**Patch-Parameter für Mobile Access

| Parameter                  | Wert |
|----------------------------|------|
| Directory-Manager-Passwort |      |

- d. Wenden Sie die in [Tabelle 14-6](#) angegebenen Patches an.

Unter Solaris:  
patchadd *patch\_ID*

Unter Linux:  
./update

Führen Sie alle Aufgaben, die nach der Installation des Patches durchgeführt werden müssen, wie in den README-Dateien der Patches beschrieben durch.

2. Entfernen Sie die Java ES Release 2-Version von Access Manager.
- a. Melden Sie sich als Root an dem Computer an, der als Host für Access Manager für Release 4 dient, oder melden Sie sich als Superuser an.
- su -
- b. Wechseln Sie in das Verzeichnis *os\_arch/Product/identity\_svr/Tools* in der Java ES Release 5-Verteilung, wobei *os\_arch* Ihrer Plattform entspricht, wie z. B. *Solaris\_sparc*.
- c. Rufen Sie die Werte der folgenden vom *ampre71upgrade*-Skript angeforderten Parameter ab:

**Tabelle 14-15**Access Manager Konfigurationsparameter: *ampre71upgrade*

| Parameter                            | Wert                                                                                      |
|--------------------------------------|-------------------------------------------------------------------------------------------|
| Directory Server-Host                | Legen Sie den vollständigen Namen fest:<br><i>hostname.domain</i>                         |
| Directory Server-Anschluss           | Geben Sie eine Anschlussnummer an, die keine SSL-Nummer ist <sup>1</sup><br>Standard: 389 |
| Top-Level-Administrator, DN          | Standard:<br><i>uid=amadmin,ou=People,default_org_DN</i>                                  |
| Passwort für Top-Level-Administrator |                                                                                           |
| Verzeichnis für Sicherungsdateien    | Standard: <i>AccessManager-base</i>                                                       |

1. Sie müssen einen SSL-Anschluss für Directory Server festlegen, der sich vom SSL-Standardwert 636 unterscheidet.

- d. Stellen Sie sicher, dass Directory Server ausgeführt wird. Wenn nicht, starten Sie ihn.
- e. Führen Sie das Skript `ampre71upgrade` aus.

```
./ampre71upgrade
```

Mithilfe des Skripts werden Access Manager-Konfigurationsdateien gespeichert und Release 4-Basispakete entfernt. Lokalisierte Pakete müssen manuell wie in [Schritt 3](#) unten dargestellt entfernt werden.

- 3. Falls die Aktualisierung auf Release 5 lokalisiert werden muss, entfernen Sie die Lokalisierungspakete von Release 2.

Das in [Schritt 2](#) oben ausgeführte Skript `ampre71upgrade` entfernt nicht die Lokalisierungspakete, daher müssen sie wie folgt manuell entfernt werden.

*Unter Solaris:*

- a. Suchen Sie die Lokalisierungspakete.

```
pkginfo | grep SUNWaml
pkginfo | grep SUNWamclnt
pkginfo | grep SUNWamdistaauth
```

- b. Entfernen Sie alle Lokalisierungspakete, die in [Schritt a](#) oben gefunden wurden.

```
pkgrm SUNWamlGebietsschema
pkgrm SUNWamclntGebietsschema
pkgrm SUNWamdistaauthGebietsschema
```

*Unter Linux:*

- a. Suchen Sie die Lokalisierungs-RPMs.

```
rpm -qa | grep sun-identity-sdk-*
rpm -qa | grep sun-identity-clientsdk-*
rpm -qa | grep sun-identity-distaauth-*
```

- b. Entfernen Sie alle Lokalisierungs-RPMs, die in [Schritt a](#) oben gefunden wurden.

```
rpm -e sun-identity-sdk-Gebietsschema-*
rpm -e sun-identity-clientsdk-Gebietsschema-*
rpm -e sun-identity-distaauth-Gebietsschema-*
```

- 4. Installieren Sie die Java ES Release 5-Version von Access Manager.

Führen Sie die folgenden Schritte aus:

- a. Führen Sie das Java ES-Installationsprogramm auf dem Computer aus, der als Host für Access Manager für Release 2 dient.

```
cd Java ES Release 5-Bereitstellung/os_arch
./installer
```

wobei *os\_arch* der Plattform entspricht, wie z. B. *Solaris\_sparc*.  
(Verwenden Sie die Option `installer -nodisplay` für die Befehlszeilenschnittstelle.)

Nach der Willkommensseite sowie der Lizenzvereinbarung wird eine Seite für die Komponentenauswahl angezeigt. (Wenn installierte Komponenten erkannt werden, die direkt vom Java ES-Installationsprogramm aktualisiert werden können, wird der Status als „aktualisierbar“ angezeigt.)

- b. Wählen Sie auf der Seite für die Komponentenauswahl Access Manager.
  - c. Geben Sie das gleiche Installationsverzeichnis an, in dem Release 2 installiert war.
  - d. Wählen Sie die Option „Später konfigurieren“ aus.
  - e. Falls erforderlich, wählen Sie die Option zur Installation von lokalisierten Paketen.
  - f. Beenden Sie das Java ES-Installationsprogramm, nachdem die Installation abgeschlossen wurde.
5. Passen Sie die JSPs für Access Manager erneut an.

Wenden Sie die angepassten JSPs der Release 2-Version für die Access Manager-Konsole und die Authentifizierungs-Benutzerschnittstelle (UI), die Sie unter *„Benutzerdefinierte Webcontainer-Dateien sichern“* auf Seite 294 gespeichert haben, erneut an.

Kopieren Sie anschließend die benutzerdefinierten JSP-Dateien in die richtigen Verzeichnisse:

- Access Manager-Konsole nur für den Legacy-Modus  
*AccessManager-base/web-src/applications/console*
- Authentifizierungs-UI:  
*AccessManager-base/web-src/services/config/auth/default* oder  
*AccessManager-base/web-src/services/config/auth/default\_Locale*  
(wobei *Locale* für einen Gebietsschema-Indikator wie *ja* steht)

Weitere Informationen finden Sie im *Sun Java System Access Manager 7.1 Developer's Guide* ( <http://docs.sun.com/doc/819-4675>).

6. Überprüfen Sie, ob Directory Server ausgeführt wird.
7. Starten Sie die folgenden Anwendungsserver-Instanzen:

In den folgenden Befehlen und den darauf folgenden Schritten werden folgende Konventionen verwendet:

- wobei *nodeagentName* der Form *hostName\_domainName* entspricht, jedoch standardmäßig nur *hostName* lautet.
- Der Standard für *domainName* lautet *domain1*.
- Der Standard für *instanceName* lautet *server1*.

---

**HINWEIS** Starten Sie den Knotenagent separat mithilfe der Option *startinstances=false*, bevor die Serverinstanz wie unten dargestellt gestartet wird.

---

- a. Starten Sie den Domain Administration Server (DAS).

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
domainName
```

- b. Starten Sie den Knotenagenten, in den die aktualisierte Anwendungsserver-Instanz migriert wurde.

```
AppServer8-base/bin/asadmin start-node-agent
--startinstances=false --user admin_ID nodeagentName
```

- c. Starten Sie die Serverinstanz, in der Access Manager bereitgestellt wurde (*instanceName*), wenn diese Serverinstanz nicht bereits ausgeführt wird.

```
AppServer8-base/bin/asadmin start-instance --user admin_ID
instanceName
```

8. Heben Sie die Bereitstellung von Access Manager auf, führen Sie eine Neukonfiguration durch und stellen Sie ihn in der Anwendungsserver-Instanz erneut bereit.
  - a. Wenn der Webcontainer im SSL-Modus ausgeführt wird, stellen Sie sicher, dass die SSL-Zertifikate des Containers nicht abgelaufen und weiterhin gültig sind.

- b. Erstellen Sie eine Eingabedatei `amconfig`, die auf der Vorlagen-Eingabedatei `amsamplesilent` basiert:

```
cp amsamplesilent config-file
```

(In den darauffolgenden Schritten wird angenommen, dass `config-file` sich im gleichen Verzeichnis wie `amsamplesilent` befindet.)

- c. Legen Sie die Konfigurationsparameter in `config-file` fest.

Sämtliche Parameter müssen ordnungsgemäß festgelegt werden. Einige der Werte können aus der Datei `AMConfig.properties` migriert werden; andere Werte müssen entsprechend des Aktualisierungsverfahrens festgelegt werden, wie in der folgenden Tabelle gezeigt.

**Tabelle 14-16** Access Manager Konfigurationsparameter: `amconfig`

| Parameter                                                                                                                | Wert                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aktualisierungsparameter</b>                                                                                          |                                                                                                                                                             |
| DEPLOY_LEVEL                                                                                                             | 26 als Wert für die Aufhebung der Bereitstellung festlegen oder<br>1 als Wert für die Neukonfiguration und erneute Bereitstellung festlegen                 |
| DIRECTORY_MODE                                                                                                           | 5 als Wert festlegen                                                                                                                                        |
| AM_REALM <sup>1</sup>                                                                                                    | disabled als Wert festlegen, falls der Legacy-Modus aktiviert ist<br>enabled als Wert festlegen, falls der Realm-Modus aktiviert ist<br>Standard: aktiviert |
| JAVA_HOME                                                                                                                | JDK Release 5-Verzeichnis als Wert festlegen:<br>/usr/java/jdk1.5.0_04/                                                                                     |
| WEB_CONTAINER                                                                                                            | AS8 als Wert für Anwendungsserver 8.x festlegen<br>Füllen Sie zusätzlich nur den entsprechenden Abschnitt von <code>config-file</code> aus.                 |
| AS81_INSTANCE<br>(Wenn Anwendungsserver 8.x aktualisiert von<br>Anwendungsserver 7.x als<br>Webcontainer verwendet wird) | Anwendungsserver 7.x <code>instanceName</code> festlegen. Dieser lautet standardmäßig <code>server1</code> .                                                |
| AS81_INSTANCE_DIR<br>(Wenn Anwendungsserver 8.x als Webcontainer verwendet wird)                                         | Domänenverzeichnis von Anwendungsserver 8.x für die Instanz festlegen. Standardmäßig ist dies <code>AppServer8Config-base/domains/domain1</code>            |



**Tabelle 14-16** Access Manager Konfigurationsparameter: `amconfig`

| Parameter                                                                    | Wert                                                                                                                                                |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| AS81_DOCS_DIR<br>(Wenn Anwendungsserver 8.x als Webcontainer verwendet wird) | docroot-Verzeichnis von Anwendungsserver 8.x für die Instanz festlegen. Standardmäßig ist dies <i>AppServer8Config-base/domains/domain1/docroot</i> |
| <b>Aus <code>AMConfig.properties</code> migriert.</b>                        |                                                                                                                                                     |
| SERVER_PROTOCOL                                                              | <code>com.ipplanet.am.server.protocol</code>                                                                                                        |
| SERVER_PORT                                                                  | <code>com.ipplanet.am.server.port</code>                                                                                                            |
| SERVER_HOST                                                                  | <code>com.ipplanet.am.server.host</code>                                                                                                            |
| DS_HOST                                                                      | <code>com.ipplanet.am.directory.host</code>                                                                                                         |
| DS_PORT                                                                      | <code>com.ipplanet.am.directory.port</code>                                                                                                         |
| ROOT_SUFFIX <sup>2</sup>                                                     | <code>com.ipplanet.am.defaultOrg</code>                                                                                                             |
| CONSOLE_DEPLOY_URI                                                           | <code>com.ipplanet.am.console.deploymentDescriptor</code>                                                                                           |
| SERVER_DEPLOY_URI                                                            | <code>com.ipplanet.am.services.deploymentDescriptor</code>                                                                                          |
| PASSWORD_DEPLOY_URI                                                          | <code>com.sun.identity.password.deploymentDescriptor</code>                                                                                         |
| AM_ENC_PWD <sup>2</sup>                                                      | <code>am.encryption.pwd<sup>3</sup></code>                                                                                                          |

1. Weitere Informationen zum Realm- oder Legacy-Modus finden Sie unter „Kompatibilität“ auf [Seite 286](#).

2. Der Wert dieses Parameters sollte identisch mit dem Wert in der vorherigen Version von Access Manager sein.

3. Wenn sowohl Access Manager als auch Access Manager SDK bereitgestellt werden, muss der Wert dieser Eigenschaft bei der Access Manager-Instanz und ihren jeweiligen Access Manager SDK-Instanzen identisch sein.

Legen Sie für die übrigen Parameter die Werte fest, die in der zu aktualisierenden Release 2-Konfiguration verwendet wurde, es sei denn, Sie ändern den Webcontainer oder die Passwörter.

- d. Führen Sie `amconfig` aus, um die Bereitstellung von Access Manager aufzuheben.

Legen Sie in *config-file* für `DEPLOY_LEVEL` den Wert 26 fest.

```
cd /AccessManager-base/bin
./amconfig -s AccessManager-base/bin/config-file
```

- e. Prüfen Sie, ob der Common Agent Container ausgeführt wird.

```
netstat -an | grep 11163
```

Wenn er nicht ausgeführt wird, starten Sie ihn.

```
/usr/sbin/cacoadm start
```

- f. Führen Sie `amconfig` aus, um Access Manager neu zu konfigurieren und in einem Webcontainer bereitzustellen.

Legen Sie in `DEPLOY_LEVEL` für *config-file* den Wert 1 fest.

```
cd /AccessManager-base/bin
```

```
./amconfig -s AccessManager-base/bin/config-file
```

- 9. Stellen Sie sicher, dass die Access Manager-Informationen zu `classpath-suffix` und `server-classpath` in die Release 5 Anwendungsserver-Datei `domain.xml` migriert wurden.

- a. Geben Sie die Access Manager-Informationen zu `classpath-suffix` und `server-classpath` in die Datei `server.xml` der Anwendungsserver-Instanz von Release 2 ein, in der Access Manager ursprünglich bereitgestellt wurde:

```
AppServer7Config-base/domains/domainName/instanceName/config/server.xml
```

- b. Prüfen Sie, ob die Einträge `classpath-suffix` und `server-classpath` der Datei `domain.xml` der aktualisierten Anwendungsserver-Instanz hinzugefügt wurden, in der Access Manager bereitgestellt wird:

```
AppServer8Config-base/nodeagents/nodeagentName/instanceName/
config/domain.xml
```

Die classpath-Informationen sollten dem Abschnitt *instanceName-config* der `domain.xml`-Datei von Anwendungsserver Release 5 hinzugefügt werden. Dieser Abschnitt beginnt mit folgender Zeile:

```
<config dynamic-reconfiguration-enabled="true"
name="instanceName-config">
```

- 10. Aktualisieren Sie die Directory-Struktur und das Directory-Schema.

Die Release 5-Version von Access Manager kann parallel zur Directory-Struktur von Release 4 vorhanden sein, die Struktur muss jedoch für die Unterstützung der Release 5-Funktionen bearbeitet werden. Aktualisieren Sie die Directory-Struktur und das Directory-Schema von Access Manager auf Release 5, indem Sie das Skript `amupgrade` ausführen, das im folgenden Verzeichnis installiert ist:

- o *Unter Solaris:*  
*AccessManager-base/upgrade/scripts*
- o *Unter Linux:*  
*AccessManager\_base/identity/upgrade/scripts*
- a. Rufen Sie die Werte für folgende vom amupgrade-Skript angeforderten Parameter ab:

**Tabelle 14-17** Access Manager Konfigurationsparameter: amupgrade

| Parameter                                                                                                                        | Wert                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Directory Server-Host                                                                                                            | Legen Sie den vollständigen Namen fest:<br><i>hostname.domäne</i>                                                                                                                                 |
| Directory Server-Anschluss                                                                                                       | Geben Sie eine Anschlussnummer an,<br>die keine SSL-Nummer ist <sup>1</sup><br>Standard: 389                                                                                                      |
| Directory-Manager-DN                                                                                                             | Standard: cn=Directory Manager                                                                                                                                                                    |
| Directory-Manager-Passwort                                                                                                       |                                                                                                                                                                                                   |
| Top-Level-Administrator, DN                                                                                                      | Standard:<br>uid=amadmin,ou=People, <i>default_org_DN</i>                                                                                                                                         |
| Passwort für Top-Level-Administrator                                                                                             |                                                                                                                                                                                                   |
| Realm-Modus aktivieren<br>(Dieser Parameterwert wird nicht<br>angefordert, wenn vom Release<br>4-Realm-Modus aktualisiert wird.) | Y/N: Yes bedeutet, der Realm-Modus wird<br>aktiviert und die Dienstdaten werden in<br>die neue Realm-Struktur migriert. No<br>(Standard) bedeutet, die Dienstdaten<br>verbleiben im Legacy-Modus. |

1. Der Aktualisierungsvorgang wird nicht erfolgreich abgeschlossen, wenn Sie den Wert für einen Directory Server-SSL-Anschluss angeben, wie beispielsweise den SSL-Standardwert 636.

- b. Führen Sie das Skript amupgrade aus.

```
cd AccessManager-base/upgrade/scripts
./amupgrade
```

Wenn die Aktualisierung erfolgreich ausgeführt wurde, zeigt das Skript eine Meldung an, die besagt, dass die Aktualisierung abgeschlossen wurde.

- c. Überprüfen Sie die folgende Aktualisierungs-Protokolldatei auf Informationen zu den Directory-Schema-Erweiterungen.

*Unter Solaris:*

```
/var/sadm/install/logs/
Sun_Java_System_Access_Manager_upgrade_dit_log.mmdhmm
```

*Unter Linux:*

```
/var/log/Sun_Java_System_Access_Manager_upgrade_dit_log.mmdhmm
```

11. Beenden Sie den Domain Administration Server (DAS), den Knotenagenten und die Serverinstanz.

Dies sind die Instanzen, die in [Schritt 7 auf Seite 329](#) gestartet wurden.

```
AppServer8-base/bin/asadmin stop-domain --user admin_ID
domainName
```

```
AppServer8-base/bin/asadmin stop-node-agent --user admin_ID
nodeagentName
```

12. Starten Sie den Domain Administration Server (DAS), den Knotenagenten und die Serverinstanz neu.

---

**HINWEIS** Starten Sie den Knotenagent separat mithilfe der Option `startinstances=false`, bevor die Serverinstanz wie unten dargestellt gestartet wird.

---

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
domainName
```

```
AppServer8-base/bin/asadmin start-node-agent --port DASportNumber
--startinstances=false --user admin_ID --password password
nodeagentName
```

```
AppServer8-base/bin/asadmin start-instance --port DASportNumber
--user admin_ID --password password instanceName
```

Der Standardwert für *DASportNumber* lautet 4848.

## Überprüfen der Access Manager-Aktualisierung

Nach Abschluss des Aktualisierungsvorgangs überprüfen Sie wie unter [„Überprüfen der Access Manager-Aktualisierung“ auf Seite 307](#) beschrieben, ob der Aktualisierungsvorgang erfolgreich war.

## Aufgaben nach der Aktualisierung

Wenn Sie den Dienst für Security Assertion Markup Language (SAML) verwenden, müssen Sie das SAML-Authentifizierungsmodul über die Access Manager-Konsole hinzufügen und aktivieren. Informationen zum Erstellen der SAML-Authentifizierungsmodul-Instanz finden Sie im *Sun Java System Access Manager 7.1 Administration Guide* (<http://docs.sun.com/doc/819-4670>).

## Aufheben der Aktualisierung

Für das Zurücksetzen von Access Manager in den Zustand vor der Aktualisierung stehen keine Skripte zur Verfügung. Der Vorgang muss manuell unter Verwendung der Access Manager-Daten durchgeführt werden, die im Rahmen der Aufgaben vor der Aktualisierung, aktualisiert wurden (siehe „[Release 4 Access Manager-Protokolldateien und -Debug-Dateien sichern](#)“ auf Seite 294). Das Aufheben der Aktualisierung gestaltet sich jedoch als zu aufwendig.

## Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen wird Access Manager auf mehreren Computersystemen bereitgestellt, um Hochverfügbarkeit und Skalierbarkeit zu gewährleisten.

Es ist in der Regel empfehlenswert, die Access Manager-Instanzen nacheinander zu aktualisieren, ohne den Dienst zu unterbrechen. Die Vorgehensweise zur Durchführung eines Rolling Upgrade von Release 2 Access Manager auf Release 5 basiert auf der folgenden Bedingung: Release 5 Access Manager kann *nicht* parallel zur Directory-Struktur von Release 2 vorhanden sein. Wenn jedoch Directory Server-Instanzen wie in [Abbildung 14-2](#) dargestellt repliziert werden, können Sie ein Rolling Upgrade wie in „[Aktualisierung mehrerer Instanzen](#)“ auf Seite 315 dargestellt durchführen.



# Portal Server

In diesem Kapitel wird die Aktualisierung von Portal Server auf Java ES 5 (Release 5) beschrieben: Sun Java System Portal Server 7.1.

Das Kapitel enthält einen Überblick über die Aspekte der verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Portal Server“ auf Seite 339
- „Aktualisieren von Portal Server von Java ES Release 4“ auf Seite 346
- „Aktualisieren von Portal Server von Java ES Release 3“ auf Seite 378
- „Aktualisieren von Portal Server von Java ES Release 2“ auf Seite 381
- „Aktualisieren von Portal Server von der Interim Feature Release 7.0“ auf Seite 392

---

**HINWEIS** Die Dateispeicherorte in diesem Kapitel sind mit Bezug auf die mit *PortalServer6-base* und *PortalServer6Config-base* (Portal Server 6.x) und *PortalServer7-base* und *PortalServer7Config-base* (Portal Server 7.x) bezeichneten Verzeichnispfade angegeben. Wenn Portal Server erstmalig installiert wurde, wurden diese Pfade mindestens teilweise als Installationsverzeichnis angegeben. Wenn nicht, wurde vom Java ES-Installationsprogramm ein Standardwert zugewiesen.

Die Standardwerte für diese Verzeichnispfade sind in der folgenden Tabelle aufgelistet.

---

**Tabelle 15-1** Portal Server Verzeichnispfade

| <b>Variable des Pfadnamens</b>  | <b>Solaris OS</b>   | <b>Linux OS</b>     |
|---------------------------------|---------------------|---------------------|
| <i>PortalServer6-base</i>       | /opt/SUNWps         | /opt/sun/portal     |
| <i>PortalServer6Config-base</i> | /etc/opt/SUNWps     | /etc/opt/sun/portal |
| <i>PortalServer7-base</i>       | /opt/SUNWportal     | /opt/sun/portal     |
| <i>PortalServer7Config-base</i> | /etc/opt/SUNWportal | /etc/opt/sun/portal |
| <i>PortalServer7Data-base</i>   | /var/opt/SUNWportal | /var/opt/sun/portal |



# Überblick über Aktualisierungen von Portal Server

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Portal Server auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5 Portal Server](#)
- [Wegweiser für die Aktualisierung von Portal Server](#)
- [Portal Server-Daten](#)
- [Portal Server Vorgehensweise zur Aktualisierung](#)

## Über Java ES Release 5 Portal Server

Java ES Release 5 Portal Server stellt eine Major-Release im Hinblick auf Release 4 dar und weist zahlreiche neue Optimierungen und Funktionen auf. Viele der Änderungen wurden in einem vorläufigen Release (Interim Feature Release, IFR) vorgenommen, das nach Release 4 eingeführt wurde. Release 5 enthält in Bezug auf das IFR nur kleine Funktionsänderungen. Informationen zu den IFR-Optimierungen und neuen Funktionen sind in den *Sun Java System Portal Server 7.1 Release Notes* unter <http://docs.sun.com/doc/820-0901/6n4l3f365?a=view> zu finden. Insbesondere wurde die Release 4-Befehlszeilenschnittstelle für die Verwaltung durch den Befehl `psadmin` ersetzt.

## Wegweiser für die Aktualisierung von Portal Server

[Tabelle 15-2](#) zeigt die unterstützten Wege für die Aktualisierung von Portal Server auf Java ES Release 5. Die Tabelle gilt sowohl für das Solaris- als auch für das Linux-Betriebssystem.

**Tabelle 15-2** Wege für die Aktualisierung auf Java ES 5 (Release 5): Portal Server 7.1

| Java ES Release               | Portal Server Version                        | Allgemeiner Ansatz                                                                                                                                      | Neukonfiguration erforderlich                        |
|-------------------------------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| Interim Feature Release (IFR) | Sun Java System Portal Server IFR 7.0 2005Q4 | Direkte Aktualisierung:<br>Durch Anwendung von Patches und anschließender Verwendung eines Aktualisierungsskripts.                                      | Anpassungen müssen manuell erneut angewendet werden. |
| Release 4                     | Sun Java System Portal Server 6.3.1 2005Q4   | Direkte Aktualisierung:<br>Durch Anwendung eines Aktualisierungsskripts.                                                                                | Anpassungen müssen manuell erneut angewendet werden. |
| Release 3                     | Sun Java System Portal Server 6.3.1 2005Q1   | Direkte Aktualisierung:<br>Durch Anwendung eines Aktualisierungsskripts.                                                                                | Anpassungen müssen manuell erneut angewendet werden. |
| Release 2                     | Sun Java System Portal Server 6.3 2004Q2     | Direkte Aktualisierung:<br>Durch Anwendung eines Aktualisierungsskripts.                                                                                | Anpassungen müssen manuell erneut angewendet werden. |
| Release 1                     | Sun ONE Portal Server 6.2 (2003Q4)           | Keine direkte Aktualisierung:<br>Kann jedoch durch Aktualisierung auf Release 3 und anschließender Aktualisierung von Release 3 auf Release 5 erfolgen. | Konfigurationsdaten                                  |
| Versionen vor Java ES         |                                              | Keine direkte Aktualisierung.                                                                                                                           |                                                      |

## Portal Server-Daten

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Portal Server-Software betroffen sein können.

**Tabelle 15-3** Portal Server Verwendung der Daten

| Datentyp            | Standort                         | Verwendung                       |
|---------------------|----------------------------------|----------------------------------|
| Konfigurationsdaten | <i>PortalServer6Config-base/</i> | Konfiguration von Portal Server. |

**Tabelle 15-3** Portal Server Verwendung der Daten (*Fortsetzung*)

| Datentyp                                                     | Standort                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Verwendung                                                                                                                                      |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Zugriffssteuerung und Konfigurationsdateien für Webcontainer | <p>Webserver 7.0 (Java ES Release 5)<br/>Datei <code>server.policy</code> und <code>server.xml</code> in<br/><i>WebServer7Config-base/https-configName/config</i></p> <p>Webserver 6.x (Java ES Release 2, 3 und 4)<br/>Datei <code>server.policy</code> und <code>server.xml</code> in<br/><i>WebServer6-base/https-hostname/config</i></p> <p>Anwendungsserver 8.x (Java ES Release 3, 4 und 5):<br/>Datei <code>server.policy</code> und <code>domain.xml</code> in<br/><i>AppServer8Config-base/domains/domainName/config</i></p> <p>Anwendungsserver 7.x (Java ES Release 2):<br/>Datei <code>server.policy</code> und <code>server.xml</code> in<br/><i>AppServer7Config-base/domains/domainName/config</i></p> | Konfiguration der Portal Server-Webcontainer-Instanz.                                                                                           |
| Benutzerdefinierte Daten                                     | <i>PortalServer6Config-base/desktop</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | JAR-Dateien für benutzerdefinierte Module, Benutzerdefinierter Beispiel-Desktop von Portal Server                                               |
| Directory-Schema<br>Dienstekonfiguration<br>Benutzerdaten    | Directory Server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Portal Server hängt von Dienstkonfigurationen ab (z. B. Portal-Desktop) und von Benutzerprofildaten, die in einem Verzeichnis gespeichert sind. |
| Dynamische Anwendungsdaten                                   | Keine                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Anwendungsdaten, wie beispielsweise zum Sitzungsstatus, werden von Portal Server nicht dauerhaft gespeichert.                                   |

## Portal Server Vorgehensweise zur Aktualisierung

Ihre Vorgehensweise bei der Aktualisierung von Portal Server hängt grundsätzlich von den zahlreichen in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) erläuterten Aspekten ab: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

Dieser Abschnitt konzentriert diese grundsätzliche Erläuterung auf Portal Server, indem Probleme dargestellt werden, die möglicherweise Ihren Aktualisierungsplan für Portal Server beeinflussen.

## Kompatibilität

Release 5 Portal Server enthält Änderungen an der öffentlichen Schnittstelle im Befehl `psadmin`, mit dem Portal Server- und Portal Server Secure Remote Access-Komponenten verwaltet werden. Weitere Informationen finden Sie in *Sun Java System Portal Server 7.1 Command-Line Reference* (<http://docs.sun.com/doc/819-5030>).

Daher ist Release 5 Portal Server nicht mit früheren Versionen bzw. mit früheren Versionen von Portal Server Secure Remote Access-Komponenten (einschließlich SRA-Gateway, Rewriter-Proxy und Netlet-Proxy) rückwärtskompatibel, außer in einer Übergangsphase, in der Bereitstellungen mehrerer Instanzen ein Rolling Upgrade durchlaufen. Alle Portal Server-Instanzen müssen zusammen mit den Instanzen der Portal Server Secure Remote Access-Komponenten auf Java ES Release 5 synchronisiert werden.

Einzelne Portal Server-Komponenten einschließlich der Mobile Access-Komponente sind ebenso wenig rückwärtskompatibel mit früheren Versionen; sie müssen alle auf Java ES Release 5 synchronisiert werden.

Des Weiteren liegt eine Inkompatibilität zwischen den in Portal Server Release 5 und früheren Portal Server-Versionen verwendeten Directory Server-Datenstrukturen vor. Diese Inkompatibilität wirkt sich auf das Rolling Upgrade mehrerer Portal Server-Instanzen aus, die dieselben Directory Server-Daten verwenden.

## Portal Server-Abhängigkeiten

Portal Server-Abhängigkeiten zu anderen Java ES-Komponenten beeinflussen möglicherweise das Verfahren für die Aktualisierung und Neukonfiguration der Portal Server-Software. Änderungen der Portal Server-Schnittstellen oder -Funktionen könnten beispielsweise eine aktualisierte Version der Komponenten erforderlich machen, von denen Portal Server abhängig ist. Welche dieser Komponenten aktualisiert werden müssen, hängt von dem jeweiligen Aktualisierungsweg ab.

Für Portal Server bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Portal Server ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)).

- **Webcontainer.** Portal Server verfügt über eine obligatorische Abhängigkeit zu Webcontainerdiensten, die entweder durch Java ES Webserver, Java ES Anwendungsserver oder durch Drittanbieter-Webcontainer von Weblogic und WebSphere bereitgestellt werden können.

---

**HINWEIS** Die Aktualisierung von Portal Server auf Release 5 wird in Bereitstellungen in Drittanbieter-Webcontainern nicht unterstützt. Für Bereitstellungen in Webcontainern von Weblogic und WebSphere muss Release 5 Portal Server neu installiert werden.

---

- **Access Manager (oder Access Manager SDK).** Portal Server verfügt über eine obligatorische Abhängigkeit zu Access Manager, um Authentifizierungs- und Autorisierungsdienste für Endbenutzer, einschließlich Single-Sign-On, bereitzustellen. Wenn Access Manager auf einem Remote-Computer ausgeführt wird, muss Access Manager SDK lokal zur Verfügung stehen.
- **Directory Server.** Portal Server verfügt über eine obligatorische Abhängigkeit zu Directory Server, der Benutzerdaten speichert, auf die über Access Manager zugegriffen wird. Daher sind bei einer Aktualisierung von Portal Server möglicherweise Erweiterungen des Directory-Schemas erforderlich.
- **Portal Server Secure Remote Access.** Portal Server verfügt über eine optionale Abhängigkeit zu Portal Server Secure Remote Access, der sicheren dezentralen Zugriff über die Gateway-, Rewriter Proxy- und Netlet Proxy-Komponenten zur Verfügung stellt.
- **Java DB.** Portal Server verfügt über eine optionale Abhängigkeit zu Java DB, der verschiedene Portlet-Anwendungen unterstützt.
- **Service Registry.** Portal Server verfügt über eine obligatorische Abhängigkeit zu Service Registry, der Bibliotheken zur Verfügung stellt, die zur Kompilierung benötigt werden.
- **Communications Express.** Portal Server verfügt über eine optionale Abhängigkeit zu Communications Express, eine Sun Java Communications Suite-Komponente, die der Bereitstellung von Messaging- und Kalenderkanälen für Endbenutzer dient. Communications Express ist keine Java ES-Produktkomponente mehr.

## Selektive Aktualisierung

Zwar unterstützt Java ES Release 5 im Allgemeinen die selektive Aktualisierung aller Komponenten auf einem Computer; da Portal Server jedoch von so vielen anderen Java ES-Komponenten abhängt, gestaltet es sich sehr schwierig, beliebige Komponentenkombinationen über verschiedene Java ES-Release-Versionen hinweg zu zertifizieren.

Aus diesem Grund unterstützt Portal Server eine eingeschränkte Reihe von Aktualisierungsszenarios im Hinblick auf Access Manager und Webcontainer.

- **Bei Aktualisierung Portal Server von Java ES Release 4.** Sie können Directory Server, Access Manager und Webcontainer (Webserver oder Anwendungsserver) vor Portal Server oder *nur* Portal Server auf Release 5 aktualisieren (wobei die anderen Komponenten auf Release 4-Ebene verbleiben); Sie können jedoch keine Abhängigkeiten in Release 4 belassen und andere auf Release 5 aktualisieren.
- **Bei Aktualisierung Portal Server von Java ES Release 3.** Sie müssen Directory Server, Access Manager und Webcontainer (Webserver oder Anwendungsserver) vor Portal Server auf Release 4 oder Release 5 aktualisieren; Sie können jedoch weder Abhängigkeiten in Release 3 belassen noch einige Abhängigkeiten auf Release 4 und andere auf Release 5 aktualisieren.
- **Bei Aktualisierung Portal Server von Java ES Release 2.** Sie müssen Directory Server, Access Manager und Webcontainer (Webserver oder Anwendungsserver) vor Portal Server auf Release 4 oder Release 5 aktualisieren; Sie können jedoch weder Abhängigkeiten in Release 2 belassen noch einige Abhängigkeiten auf Release 4 und andere auf Release 5 aktualisieren.

## Aktualisierungsszenarios für den Webcontainer

Portal Server kann in einem Webcontainer eingesetzt werden, der entweder von Webserver oder Anwendungsserver bereitgestellt wurde. Daher kann die Aktualisierung von Portal Server auf Release 5 dadurch kompliziert werden, dass möglicherweise auch der Webcontainer auf Release 5 aktualisiert werden muss, in dem Portal Server eingesetzt wird. Es sind eine Reihe von Aktualisierungsszenarios für den Webcontainer möglich, die in der folgenden Tabelle dargestellt werden.

**Tabelle 15-4** Szenarien für die Portal Server-Aktualisierung für Webcontainer

| <b>Szenario</b> | <b>Webcontainer, in dem Portal Server ursprünglich bereitgestellt wurde</b> | <b>Webcontainer, in dem Portal Server nach der Aktualisierung bereitgestellt wird</b> | <b>Anwendbare Portal Server - Aktualisierungsweg:<br/>Aktualisierungen von</b> |
|-----------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Szenario 1      | Webserver 6.x                                                               | Webserver 6.x                                                                         | Release 2<br>Release 3<br>Release 4<br>IFR 7.0                                 |
| Szenario 2      | Webserver 6.x                                                               | Webserver 7.0                                                                         | Release 2<br>Release 3<br>Release 4<br>IFR 7.0                                 |
| Szenario 3      | Anwendungsserver 8.1                                                        | Anwendungsserver 8.1                                                                  | Release 3<br>Release 4<br>IFR 7.0                                              |
| Szenario 4      | Anwendungsserver 8.1                                                        | Anwendungsserver 8.2                                                                  | Release 3<br>Release 4<br>IFR 7.0                                              |
| Szenario 5      | Anwendungsserver 7.x                                                        | Anwendungsserver 8.2                                                                  | Release 2                                                                      |

Gehen Sie bei der Aktualisierung von Portal Server (z. B. bei der Verwendung des Skripts psupgrade) vorsichtig vor und geben Sie die für das in [Tabelle 15-4](#) entsprechend dargestellte Aktualisierungsszenario korrekten Werte ein, insbesondere wenn dies eine Aktualisierung einer Major-Version des Webcontainers beinhaltet.

# Aktualisieren von Portal Server von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von Portal Server von Java ES 2005Q4 (Release 4) auf Java ES 5 (Release 5).

---

**HINWEIS** Dieser Abschnitt behandelt nicht den Spezialfall, bei dem Portal Server in einem Anwendungsserver-Webcontainer bereitgestellt wird und vor der Release 5-Aktualisierung von Release 2 auf Release 3 oder 4 aktualisiert wurde. Der zuvor genannte Aktualisierungsweg wird für diesen Fall derzeit nicht unterstützt.

---

In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 4-Version von Portal Server](#)
- [Aktualisierung mehrerer Instanzen](#)

## Einführung

Berücksichtigen Sie bei der Aktualisierung von Java ES von Portal Server Release 4 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch die Verwendung eines Aktualisierungsskripts, `psupgrade`. Das Skript installiert neue Pakete, migriert Konfigurationsdaten, wenn erforderlich, aktualisiert Lokalisierungsdateien und stellt dem Webcontainer Portal Server-Webanwendungen erneut bereit.
- **Aktualisierungsabhängigkeiten.** Portal Server ist von einer Reihe von gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)). Portal Server Release 5 ist zwar mit der Release 4-Version dieser gemeinsamen Komponenten kompatibel, jedoch ist eine Aktualisierung dennoch erforderlich, da das für die Aktualisierung von Portal Server verwendete Skript `psupgrade` die Release 5-Version der gemeinsam genutzten ANT-Komponente benötigt.



Portal Server Release 5 verfügt auch über Abhängigkeiten von einem Webcontainer, Access Manager sowie Directory Server, wie unter „[Portal Server-Abhängigkeiten](#)“ auf [Seite 342](#) beschrieben. Es werden zwei Ansätze zur Aktualisierung dieser Abhängigkeiten unterstützt (siehe „[Selektive Aktualisierung](#)“ auf [Seite 344](#)):

- Alle von den Komponenten von Release 4 erfüllten Abhängigkeiten (es werden *keine* auf Release 5 aktualisiert)
- Alle von den Komponenten von Release 5 erfüllten Abhängigkeiten (es werden *alle* auf Release 5 aktualisiert)
- **Rückwärtskompatibilität.** Release 5 Portal Server ist nicht mit Release 4 rückwärtskompatibel.
- **Aufheben der Aktualisierung.** Das Aufheben der Aktualisierung von Portal Server auf Release 5 erfolgt durch Wiederherstellen der Pakete von Release 4. Hierbei werden die Verzeichnisdaten von Release 4 wiederhergestellt und die Portal Server-Webanwendungen dem Webcontainer erneut bereitgestellt.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Portal Server ist für das Solaris- und Linux-Betriebssystem identisch, jedoch wird Portal Server Release 5 unter Solaris in einem neuen Pfad und unter Linux im selben Release 4-Pfad installiert.

## Aktualisierung der Release 4-Version von Portal Server

In diesem Abschnitt wird die Aktualisierung von Portal Server von Java ES Release 4 auf Java ES Release 5 unter Solaris und Linux beschrieben. Plattformspezifische Vorgänge sind durch die Angabe des jeweiligen Betriebssystems, auf das sich der Vorgang bezieht, gekennzeichnet. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung von Release 4](#)
- [Aktualisieren der Release 4-Version von Portal Server \(Solaris\)](#)
- [Aktualisieren der Release 4-Version von Portal Server \(Linux\)](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung von Release 4](#)
- [Aufheben der Aktualisierung \(Solaris\)](#)
- [Aufheben der Aktualisierung \(Linux\)](#)

## Aufgaben vor der Aktualisierung von Release 4

Bevor Sie mit der Aktualisierung von Portal Server beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Portal Server-Aktualisierungsabhängigkeiten](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)
- [Konfigurationsinformationen von Portal Server Release 4 sichern](#)
- [Aufzeichnen der Java Virtual Machine \(JVM\)-Einstellungen](#)
- [Entfernen der Konfiguration für das Lastenausgleichsprogramm](#)
- [Konfiguration entfernen von Directory Proxy Server](#)

### *Aktuelle Versionsinformationen überprüfen*

Sie können die aktuelle Version von Portal Server mithilfe des folgenden Befehls überprüfen:

*PortalServer6-base/bin/version*

**Tabelle 15-5** Portal Server Ausgaben der Versionsüberprüfung

| Java ES Release | Portal Server-Versionsnummer |
|-----------------|------------------------------|
| Release 2       | 6.3                          |
| Release 3       | 6.3.1                        |
| Release 4       | 6.3.1 <sup>1</sup>           |
| IFR             | 7.0                          |
| Release 5       | 7.1                          |

1. Release 3 und Release 4 unterscheiden sich lediglich durch einen Patch. Sie können die Release 4-Patches mit dem Solaris-Befehl `showrev -p | grep patch_ID` und dem Linux-Befehl `rpm -qa sun-portal-core` suchen und die Versionen mit den im Java ES Release 4 *Aktualisierungshandbuch* aufgeführten vergleichen.

### *Portal Server-Aktualisierungsabhängigkeiten*

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkkumgebung) auf Java ES Release 5 zu aktualisieren.

Portal Server Release 5 ist zwar mit der Release 4-Version dieser gemeinsamen Java ES-Komponenten kompatibel, jedoch ist eine Aktualisierung dennoch erforderlich, da das für die Aktualisierung von Portal Server verwendete Skript `psupgrade` die Release 5-Version der gemeinsam genutzten ANT-Komponente benötigt.

Wenn Sie Abhängigkeiten der Portal Server-Produktkomponenten auf Release 5 aktualisieren möchten, müssen *alle* aktualisiert werden (siehe „[Selektive Aktualisierung](#)“ auf Seite 344). Die Abhängigkeiten sollten vor der Aktualisierung von Portal Server in der nachstehend genannten Reihenfolge aktualisiert werden (bereits aktualisierte können hierbei übersprungen werden).

1. **Gemeinsam genutzte Komponenten.** Anleitungen für die Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie unter „[Aktualisieren der gemeinsam genutzten Java ES-Komponenten](#)“ auf Seite 71.
2. **Directory Server.** Anleitungen für die Aktualisierung von Directory Server auf Release 4 finden Sie in [Kapitel 5, „Directory Server“](#) auf Seite 109.
3. **Webcontainer-Software.** Anweisungen zur Aktualisierung von Webserver und Anwendungsserver finden Sie in [Kapitel 7, „Webserver“](#) auf Seite 143 bzw. [Kapitel 11, „Anwendungsserver“](#) auf Seite 219.

---

**HINWEIS** Die Aktualisierung von Drittanbieter-Webcontainern, wie beispielsweise Webcontainer von WebLogic und WebSphere, kann dazu führen, dass Portal Server nicht ordnungsgemäß funktioniert, da Anpassungen hinsichtlich dieser Container für die Unterstützung von Portal Server bei der Container-Aktualisierung überschrieben werden.

In diesem Fall müssen Sie Portal Server erneut installieren und für die aktualisierte Container-Umgebung erneut konfigurieren.

---

4. **Access Manager (Access Manager SDK).** Anweisungen zur Aktualisierung von Access Manager auf Release 5 finden Sie in [Kapitel 14, „Access Manager“](#) auf Seite 281.
5. **Portal Server Secure Remote Access.** Anleitungen für die Aktualisierung von Portal Server Secure Remote Access auf Release 5 finden Sie in [Kapitel 16, „Portal Server Secure Remote Access“](#) auf Seite 413.
6. **Java DB.** Anleitungen für die Aktualisierung von Java DB auf Release 5 finden Sie in [Kapitel 8, „Java DB“](#) auf Seite 171.

7. **Service Registry.** Anleitungen für die Aktualisierung von Service Registry auf Release 5 finden Sie in [Kapitel 12, „Service Registry“](#) auf Seite 249.
8. **Communications Express.** Anleitungen für die Aktualisierung von Communications Express auf Release 5 finden Sie im *Sun Java Communications Suite Upgrade Guide*, <http://docs.sun.com/doc/819-7561>.

### *Erforderliche Konfigurationsinformationen und Passwörter abrufen*

Je nach Aktualisierungsszenario der Webcontainer (siehe [Tabelle 15-4 auf Seite 345](#)) müssen Sie für das Skript `psupgrade` Informationen zu Passwörtern und andere Webcontainer-Konfigurationsdaten eingeben. Die Informationen, die für die verschiedenen Aktualisierungsszenarien für Webcontainer benötigt werden, sind in [Tabelle 15-6](#) aufgeführt. Denken Sie daran, sich vor der Aktualisierung von Portal Server die relevanten Informationen zu beschaffen.

**Tabelle 15-6** Vom Skript `psupgrade` für die Webcontainer-Aktualisierungsszenarien benötigte Informationen

| Information                                                  | Aktualisierungsszenario <sup>3</sup> | Webserver 7.x<br>Beispielswerte:<br>Szenario 2                       | Anwendungsserver 8.x<br>Beispielswerte:<br>Szenario 5 <sup>2</sup> |
|--------------------------------------------------------------|--------------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------|
| Aktualisierung von Portal Server auf Webserver 7.0 (ja/nein) | 2                                    | Ja                                                                   | N/V                                                                |
| Webcontainer-Installationsverzeichnis                        | 2 und 5                              | <i>WebServer7-base</i>                                               | <i>AppServer8Install-base</i>                                      |
| Webcontainer-Objektname des virtuellen Servers               | 2                                    | <i>configName<sup>4</sup></i>                                        | N/V                                                                |
| Webcontainer-Objektname                                      | 5                                    | N/V                                                                  | Server1                                                            |
| Webcontainer-Objektverzeichnis                               | 2                                    | <i>WebServer7Config-base/<br/>https-configName<sup>3</sup>/</i>      | N/V                                                                |
| Portal-Instanz-Bereitstellungsverzeichnis                    | 5                                    | N/V                                                                  | <i>AppServer8Config-base/<br/>Domänen/domainName</i>               |
| Webcontainer-Instanzanschluss                                | 2 und 5                              | 80                                                                   | 80                                                                 |
| Webcontainer-Instanzprotokoll                                | 2 und 5                              | http                                                                 | http                                                               |
| Webcontainer-Konfigurationsname                              | 2                                    | <i>configName<sup>3</sup></i>                                        | N/V                                                                |
| Webcontainer-Domänenname                                     | 5                                    | N/V                                                                  | domain1                                                            |
| Webcontainer-Dokument-Root-Verzeichnis                       | 2 und 5                              | <i>WebServer7Config-base/<br/>https-configName<sup>3</sup>/docs/</i> | <i>AppServer8Config-base/<br/>Domänen/domainName/<br/>docroot</i>  |
| Webcontainer-Admin-Hostname                                  | 2 und 5                              | Lokaler Host                                                         | Lokaler Host                                                       |
| Webcontainer-Admin-Anschluss                                 | 2 und 5                              | 8989                                                                 | 4848                                                               |

**Tabelle 15-6** Vom Skript `psupgrade` für die Webcontainer-Aktualisierungsszenarien benötigte Informationen  
(Fortsetzung)

| Information                                       | Aktualisierungsszenario <sup>3</sup> | Webserver 7.x<br>Beispielswerte:<br>Szenario 2 | Anwendungsserver 8.x<br>Beispielswerte:<br>Szenario 5 <sup>2</sup> |
|---------------------------------------------------|--------------------------------------|------------------------------------------------|--------------------------------------------------------------------|
| Webcontainer-Admin-Protocol                       | 2 und 5                              | https                                          | https                                                              |
| Webcontainer-Admin-Benutzer-ID                    | 2 und 5                              | admin                                          | admin                                                              |
| Webcontainer-Admin-Passwort                       | 2 bis 5                              |                                                |                                                                    |
| Webcontainer-Master-Password                      | 3 bis 5                              | N/V                                            |                                                                    |
| Directory Manager (cn=Directory manager)-Passwort | 1 bis 5                              |                                                |                                                                    |
| SRA-Protokoll-Benutzerpasswort <sup>1</sup>       | 1 bis 5                              |                                                |                                                                    |
| Access Manager-Admin-Passwort                     | 1 bis 5                              |                                                |                                                                    |
| Idapuser-Passwort für Directory Server            | 1 bis 5                              |                                                |                                                                    |
| Portal-Instanz-ID <sup>2</sup>                    | 1 bis 5                              |                                                |                                                                    |

- 1. Diese Informationen werden zum Konfigurieren der Portal Server Secure Remote Access-Komponenten bei Installation mit Portal Server benötigt.
- 2. Für diesen Parameter muss ein einmaliger Wert angegeben werden, der nicht Null sein darf. Der Wert muss alphanumerisch sein und kann einen Bindestrich (-) enthalten.
- 3. Webcontainer-Aktualisierungsszenario #5 gilt für die Aktualisierung von Portal Server von Release 2.
- 4. Der Standardwert von `configName` lautet `hostName.domainName`.

*Konfigurationsinformationen von Portal Server Release 4 sichern*

Bei der Aktualisierung von Portal Server auf Release 5 ist keine Neukonfiguration der Portal Server-Software erforderlich. Als Vorsichtsmaßnahme sichert jedoch das Skript `psupgrade` die folgenden Verzeichnisse mit Konfigurationsinformationen:

*PortalServer6Config-base/*

|                |                                                                                                                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HINWEIS</b> | Es ist ratsam, die Directory Server-Instanz zu sichern, in der Portal Server Benutzerprofile und andere Daten speichert. Ohne diese Daten kann die Aktualisierung von Portal Server Release 5 nicht aufgehoben werden. |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

*Aufzeichnen der Java Virtual Machine (JVM)-Einstellungen*

Zeichnen Sie vor dem Aktualisieren von Portal Server die folgenden JVM-Webcontainer-Einstellungen auf, sofern sie von den Standardeinstellungen abweichen:

```
<jvm-options>-XX:MaxPermSize=256m</jvm-options>
<jvm-options>-XX:+CMSPermGenSweepingEnabled</jvm-options>
<jvm-options>-XX:+CMSClassUnloadingEnabled</jvm-options>
```

Der Speicherort der JVM-Einstellungen hängt vom Webcontainer ab, wie in der nachfolgenden Tabelle angezeigt.

**Tabelle 15-7** Speicherort der JVM-Einstellungen

| Webcontainer                                               | Konfigurationsdatei                                                          |
|------------------------------------------------------------|------------------------------------------------------------------------------|
| Release 2, 3, 4<br>Webserver (6.x)                         | <i>WebServer6-base/https-instanceName/config/server.xml</i>                  |
| Release 5<br>Webserver (7.0)                               | <i>WebServer7Config-base/https-configName/config/server.xml</i>              |
| Release 3, 4, 5<br>Anwendungsserver (8.x)                  | <i>AppServer8Config-base/domains/domainName/config/domain.xml</i>            |
| Anwendungsserver Instanz<br>vom Knotenagenten<br>verwaltet | <i>AppServer8Config-base/nodeagents/nodeagentName/config/<br/>domain.xml</i> |

Sie müssen später überprüfen, ob diese JVM-Einstellungen im Laufe der Portal Server-Aktualisierung nicht geändert wurden.

*Entfernen der Konfiguration für das Lastenausgleichsprogramm*

In Fällen, in denen über ein Lastenausgleichsprogramm auf die Portal Server-Instanzen zugegriffen wird, kann der Wert der Eigenschaft `LOAD_BALANCER_URL`, der für die Konfiguration dieses Zugriffs verwendet wird, mit der Portal Server-Aktualisierung interferieren. Daher muss diese Einstellung vor Durchführung der Aktualisierung geändert werden. So ändern Sie die Einstellung der Eigenschaft `LOAD_BALANCER_URL`

1. Notieren Sie sich, welche der folgenden Konfigurationsdateien lokal vorhanden sind (von denen einige Portal Server Secure Remote Access-Komponenten unterstützen und möglicherweise lokal installiert sind):

*PortalServer6Config-base/PSConfig.properties*  
*PortalServer6Config-base/GWConfig.properties* (wenn Gateway lokal vorhanden ist)  
*PortalServer6Config-base/RWPCConfig.properties* (wenn Rewriter-Proxy lokal ist)  
*PortalServer6Config-base/NLPConfig.properties* (wenn Netlet Proxy lokal vorhanden ist)

2. Notieren Sie den aktuellen Wert der Eigenschaft `LOAD_BALANCER_URL` in diesen Konfigurationsdateien.



3. Ändern Sie den Wert der Eigenschaft `LOAD_BALANCER_URL` so, dass er auf die relevante Portal Server-Instanz verweist:

`LOAD_BALANCER_URL=portalHostName:port/portal`

### *Konfiguration entfernen von Directory Proxy Server*

In Fällen, in denen Portal Server-Instanzen über eine Directory Proxy Server-Instanz auf Directory Server zugreifen, müssen die Einstellungen des Directory Proxy Server-Hosts und der Anschlussnummer vor Durchführung der Aktualisierung geändert werden. Nach erfolgter Aktualisierung müssen ihre ursprünglichen Werte wiederhergestellt werden.

So ändern Sie die entsprechenden Einstellungen

1. Zeichnen Sie den aktuellen Wert der Eigenschaften `DS_HOST` und `DS_PORT` in der folgenden Access Manager-Konfigurationsdatei auf:

`AccessManagerConfig-base/config/AMConfig.properties`

2. Ändern Sie den Wert der Eigenschaft `DS_HOST` und `DS_PORT` so, dass er auf die relevante Directory Server-Instanz verweist.

## Aktualisieren der Release 4-Version von Portal Server (Solaris)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Portal Server haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung (Solaris)*

Bei der Aktualisierung der Portal Server-Software auf Release 5 müssen folgende Aspekte berücksichtigt werden:

- Alle Portal Server-Instanzen, die demselben installierten Portal Server-Image entsprechen, werden gleichzeitig aktualisiert.
- Die Portal Server-Software besteht aus Unterkomponenten, die eine Reihe unterschiedlicher Rollen ausführen, jedoch alle zusammen aktualisiert werden:
  - **Portal-base.** Enthält Verwaltungs-Mbeans und begleitende Verwaltungssoftware, Logging Framework und Software im Zusammenhang mit der Überwachung, die alle in einem Paket zusammengefasst sind.
  - **Portal Server Webanwendungen.** Besteht aus einer Reihe von Webanwendungen, die in einem Webcontainer bereitgestellt werden. Zumindest einige dieser Webanwendungen benötigen Unterstützung von Access Manager und wiederum Directory Server.

- **Secure Remote Access Core** Software, die Portal Server Secure Remote Access unterstützt: Einige in JAR-Dateien eingebettete Servlets und Applets sowie einige Unterstützungsdateien können in einem Webcontainer nicht bereitgestellt werden.
- Das Skript `psupgrade` erkennt automatisch, welche Portal Server-Unterkomponenten und welche Webcontainer-Abhängigkeiten auf dem Host-Computer installiert sind. Beispiel: Das Skript weist das System an, die Version von Anwendungsserver oder Webserver zu erkennen, der Sie Portal Server-Webanwendungen bereitstellen, und passt die erforderlichen Informationen unter Verwendung der Informationen an, die es erkennen kann.

### *Aktualisierungsverfahren (Solaris)*

Das im Folgenden beschriebene Verfahren ist für Portal Server auf dem Computer anzuwenden, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

`su -`

2. Synchronisieren Sie alle gemeinsam genutzten Komponenten auf Release 5, sofern dies noch nicht erfolgt ist.

Anweisungen hierzu erhalten Sie unter [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“](#) auf Seite 71.

Dieser Schritt ist eine erforderliche Voraussetzung für die Ausführung des Skripts `psupgrade` in [Schritt 8 auf Seite 357](#).

3. Stoppen Sie etwaige Instanzen von Portal Server Secure Remote Access Gateway, Rewriter-Proxy oder Netlet-Proxy, die möglicherweise lokal ausgeführt werden.

```
PortalServer6-base/bin gateway stop
PortalServer6-base/bin netletd stop
PortalServer6-base/bin rwproxyd stop
```

Überprüfen Sie, ob die Prozesse angehalten wurden. Beispiel:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

4. Vergewissern Sie sich, dass Access Manager ausgeführt wird, wenn es in einem anderen Webcontainer bereitgestellt wird als dem, in dem Portal Server bereitgestellt wird.

5. Starten Sie Portal Server, sofern es nicht bereits ausgeführt wird, indem Sie den Webcontainer starten, in dem es bereitgestellt wird.

Webserver 6.x:

*WebServer-base/https-instanceName/start*

Webserver 7.0:

Admin Server--

*WebServer7Config-base/admin-server/bin/startserv*

Instance Server--

*WebServer7Config-base/https-configName/bin/startserv*

Anwendungsserver 8.x:

*AppServer8-base/bin/asadmin start-domain --user admin\_ID  
--password password domainName*

6. Setzen Sie die zwei Umgebungsvariablen (ANT\_HOME und JAVA\_HOME), die vom Skript psupgrade benötigt werden. Beispiel:

`export ANT_HOME=/usr/sfw`

`export JAVA_HOME=/usr/jdk/entsys-j2se`

7. Stellen Sie sicher, dass auf Ihrem Computer ausreichend Swap-Speicher zur Verfügung steht.

Der Swap-Speicher sollte grundsätzlich die doppelte Größe des physikalischen RAM aufweisen.

8. Führen Sie das Skript psupgrade über die Java ES Release 5-Verteilung aus.

`cd os_arch/Products/portal_svr/Tools/upgrade/bin`

`./psupgrade`

wobei *os\_arch* der Plattform entspricht, wie z. B. Solaris\_sparc.

- 
- HINWEIS** Sollten Sie `psupgrade` versehentlich vom falschen `os_arch`-Verzeichnis aus gestartet haben, müssen Sie das Verfahren folgendermaßen rückgängig machen:
- a. Wechseln Sie in das richtige `os_arch`-Verzeichnis.
  - b. Machen Sie die Änderungen an den Portal Server-Daten rückgängig.  
  
`./psupgrade rollback`  
  
Geben Sie die erforderlichen Parameter und Passwörter an.
  - c. Führen Sie `psupgrade` erneut aus.
- 

Das Skript `psupgrade` erkennt installierte Portal Server-Komponenten und Lokalisierungspakete, ruft das Java ES-Installationsprogramm auf, um neue Pakete zu installieren und weist das System an, Speicherort, Anschlussnummer und andere Informationen zum Webcontainer zu erkennen, in dem Sie Portal Server-Webanwendungen bereitstellen. Je nach Webcontainer-Aktualisierungsszenario (siehe [Tabelle 15-4 auf Seite 345](#)) fordert das Skript Sie auf, zusätzliche Informationen einzugeben, die für die Bereitstellung von Portal Server für den entsprechenden Webcontainer erforderlich sind.

[Tabelle 15-6 auf Seite 351](#) enthält die Informationen, die für die verschiedenen Webcontainer-Aktualisierungsszenarien in [Tabelle 15-4](#) erforderlich sind.

- 
- HINWEIS** Achten Sie darauf, die richtigen Werte für die `psupgrade`-Parameter einzugeben, denn Sie können nicht zurückgehen und sie ändern. Des Weiteren ist es sehr schwierig, vom Skript `psupgrade` vorgenommene Änderungen rückgängig zu machen. Zum Rückgängig machen von Änderungen an Portal Server-Daten müssen Sie
- `./psupgrade rollback`
- ausführen, bevor Sie `psupgrade` erneut ausführen.
-

9. Stellen Sie gegebenenfalls die JVM-Einstellungen des Webcontainers wieder her.

Um sicherzustellen, dass die JVM-Einstellungen Portal Server Release 5 unterstützen, führen Sie die folgenden Schritte durch:

- a. Stellen Sie sicher, dass die JVM-Einstellungen des Webcontainers für Portal Server, die Sie vor der Aktualisierung aufgezeichnet haben, nicht im Laufe der Aktualisierung geändert wurden.

Siehe auch „[Aufzeichnen der Java Virtual Machine \(JVM\)-Einstellungen](#)“ auf Seite 352.

- b. Wenn die Änderungen geändert wurden, stellen Sie die Werte wieder her, die Sie vor der Aktualisierung aufgezeichnet haben.

Vergewissern Sie sich, dass die folgenden JVM-Einstellungen enthalten sind, selbst wenn sie zuvor nicht eingerichtet wurden:

```
<jvm-options>-XX:MaxPermSize=256m</jvm-options>
<jvm-options>-XX:+CMSPermGenSweepingEnabled</jvm-options>
<jvm-options>-XX:+CMSClassUnloadingEnabled</jvm-options>
```

10. Halten Sie den Webcontainer an und starten Sie ihn erneut.

Ein Neustart des Webcontainers ist zwar nicht in jedem Fall erforderlich, dadurch wird jedoch sichergestellt, dass der Status von Portal Server beim Start eindeutig ist.

- a. Halten Sie den Webcontainer wie folgt an:

Webserver 6.x:

```
WebServer-base/https-instanceName/stop
```

Webserver 7.0:

Admin Server--

```
WebServer7Config-base/admin-server/bin/stopserv
```

Instance Server--

```
WebServer7Config-base/https-configName/bin/stopserv
```

Anwendungsserver 8.x:

```
AppServer8-base/bin/asadmin stop-domain --user admin_ID
--password password domainName
```

- b. Starten Sie den Webcontainer mit den Befehlen in [Schritt 5 auf Seite 357](#) neu.

## Aktualisieren der Release 4-Version von Portal Server (Linux)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Portal Server haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung (Linux)*

Bei der Aktualisierung der Portal Server-Software auf Release 5 unter Linux sind dieselben Aspekte wie unter Solaris zu berücksichtigen (siehe „[Zu berücksichtigende Aspekte bei der Aktualisierung \(Solaris\)](#)“ auf Seite 355), jedoch wird Portal Server Release 5 unter Linux im selben Pfad wie Release 4 installiert. Daher entfernt das Skript `psupgrade` bei der Installation der RPMs für Release 5 die vorherigen RPMs.

### *Aktualisierungsverfahren (Linux)*

Das im Folgenden beschriebene Verfahren ist für Portal Server auf dem Computer anzuwenden, auf dem die Aktualisierung durchgeführt wird.

---

**VORSICHT** Eine Aktualisierung von Java ES Release 4 auf Release 5 unter Linux kann nicht rückgängig gemacht werden. Stellen Sie sicher, dass Sie Ihr System sicher, *bevor* Sie das folgende Verfahren durchführen.

---

1. Melden Sie sich als Root oder Superuser an.

`su -`

2. Synchronisieren Sie alle gemeinsam genutzten Komponenten auf Release 5, sofern dies noch nicht erfolgt ist.

Anweisungen hierzu erhalten Sie unter [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“](#) auf Seite 71.

Dieser Schritt ist eine erforderliche Voraussetzung für die Ausführung des Skripts `psupgrade` in [Schritt 8 auf Seite 362](#).

3. Stoppen Sie etwaige Instanzen von Portal Server Secure Remote Access Gateway, Rewriter-Proxy oder Netlet-Proxy, die möglicherweise lokal ausgeführt werden.

```
PortalServer6-base/bin gateway stop
PortalServer6-base/bin netletd stop
PortalServer6-base/bin rwproxycd stop
```

Überprüfen Sie, ob die Prozesse angehalten wurden. Beispiel:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

4. Vergewissern Sie sich, dass Access Manager ausgeführt wird, wenn es in einem anderen Webcontainer bereitgestellt wird als dem, in dem Portal Server bereitgestellt wird.
5. Starten Sie Portal Server, sofern es nicht bereits ausgeführt wird, indem Sie den Webcontainer starten, in dem es bereitgestellt wird.

Webserver 6.x:

```
WebServer-base/https-instanceName/start
```

Webserver 7.0:

Admin Server--

```
WebServer7Config-base/admin-server/bin/startserv
```

Instance Server--

```
WebServer7Config-base/https-configName/bin/startserv
```

Anwendungsserver 8.x:

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
--password password domainName
```

6. Setzen Sie die zwei Umgebungsvariablen (ANT\_HOME und JAVA\_HOME), die vom Skript psupgrade benötigt werden. Beispiel:

```
export ANT_HOME=/opt/sun
export JAVA_HOME=/usr/jdk/entsys-j2se
```

7. Stellen Sie sicher, dass auf Ihrem Computer ausreichend Swap-Speicher zur Verfügung steht.

Der Swap-Speicher sollte grundsätzlich die doppelte Größe des physikalischen RAM aufweisen.

8. Führen Sie das Skript `psupgrade` über die Java ES Release 5-Verteilung aus.

```
cd os_arch/Products/portal_svr/Tools/upgrade/bin
./psupgrade
```

wobei `os_arch` der Plattform entspricht, wie z. B. `Linux_x86`.

Das Skript `psupgrade` erkennt installierte Portal Server-Komponenten und Lokalisierungspakete, ruft das Java ES-Installationsprogramm auf, um neue Pakete zu installieren und weist das System an, Speicherort, Anschlussnummer und andere Informationen zum Webcontainer zu erkennen, in dem Sie Portal Server-Webanwendungen bereitstellen. Je nach Webcontainer-Aktualisierungsszenario (siehe [Tabelle 15-4 auf Seite 345](#)) fordert das Skript Sie auf, zusätzliche Informationen einzugeben, die für die Bereitstellung von Portal Server für den entsprechenden Webcontainer erforderlich sind.

[Tabelle 15-6 auf Seite 351](#) enthält die Informationen, die für die verschiedenen Webcontainer-Aktualisierungsszenarien in [Tabelle 15-4](#) erforderlich sind.

---

**HINWEIS** Achten Sie darauf, die richtigen Werte für die `psupgrade`-Parameter einzugeben, denn Sie können nicht zurückgehen und sie ändern. Des Weiteren ist es sehr schwierig, vom Skript `psupgrade` vorgenommene Änderungen rückgängig zu machen. Erinnerung: Sichern Sie Ihr System, *bevor* Sie das Skript `psupgrade` ausführen.

---

9. Ändern Sie die Konfigurationsdatei  
`PortalServer7Config-base/platform.conf.default`.

Kopieren Sie die Zeile mit `gateway.logging.password` aus der folgenden, von `psupgrade` gesicherten Datei:

```
PortalServer6Config-base.bak/platform.conf.default
```

und platzieren Sie die Zeile in `PortalServer7Config-base/platform.conf.default`.

10. Stellen Sie gegebenenfalls die JVM-Einstellungen des Webcontainers wieder her.

Um sicherzustellen, dass die JVM-Einstellungen Portal Server Release 5 unterstützen, führen Sie die folgenden Schritte durch:



- a. Stellen Sie sicher, dass die JVM-Einstellungen des Webcontainers für Portal Server, die Sie vor der Aktualisierung aufgezeichnet haben, nicht im Laufe der Aktualisierung geändert wurden.

Siehe auch „[Aufzeichnen der Java Virtual Machine \(JVM\)-Einstellungen](#)“ auf Seite 352.

- b. Wenn die Änderungen geändert wurden, stellen Sie die Werte wieder her, die Sie vor der Aktualisierung aufgezeichnet haben.

Vergewissern Sie sich, dass die folgenden JVM-Einstellungen enthalten sind, selbst wenn sie zuvor nicht eingerichtet wurden:

```
<jvm-options>-XX:MaxPermSize=256m</jvm-options>
<jvm-options>-XX:+CMSPermGenSweepingEnabled</jvm-options>
<jvm-options>-XX:+CMSClassUnloadingEnabled</jvm-options>
```

11. Halten Sie den Webcontainer an und starten Sie ihn erneut.

Ein Neustart des Webcontainers ist zwar nicht in jedem Fall erforderlich, dadurch wird jedoch sichergestellt, dass der Status von Portal Server beim Start eindeutig ist.

- a. Halten Sie den Webcontainer wie folgt an:

Webserver 6.x:

*WebServer-base/https-instanceName/stop*

Webserver 7.0:

Admin Server--

*WebServer7Config-base/admin-server/bin/stopserv*

Instance Server--

*WebServer7Config-base/https-configName/bin/stopserv*

Anwendungsserver 8.x:

*AppServer8-base/bin/asadmin stop-domain --user admin\_ID  
--password password domainName*

- b. Starten Sie den Webcontainer mit den Befehlen in [Schritt 5 auf Seite 361](#) neu.

## Überprüfen der Aktualisierung

Sie können die Installation der Pakete von Release 5 mithilfe des folgenden Befehls überprüfen:

```
PortalServer7-base/bin/psadmin --version --adminuser admin_ID
-f adminpasswordfile.
```

Ausgabewerte finden Sie in [Tabelle 15-5 auf Seite 349](#).

Zur Überprüfung der gesamten Aktualisierung vergewissern Sie sich, dass der Portal-Desktop angezeigt wird und das Administrationsprogramm `psadmin` wie dokumentiert funktioniert.

Sie können außerdem die folgenden Aktualisierungs-Protokolldateien überprüfen:

```
/var/sadm/install/logs/Sun_Java_System_Portal_Server_upgrade.log*
PortalServer7Data-base/logs/admin/
PortalServer7Data-base/logs/config/
```

## Aufgaben nach der Aktualisierung von Release 4

Beachten Sie die für die folgenden Situationen erforderlichen Aufgaben nach der Aktualisierung:

- [Migrieren von benutzerdefinierten web-src-Daten](#)
- [Erneutes Bereitstellen von benutzerdefinierten Portlet-Anwendungen](#)
- [Migrieren von benutzerdefinierten Portlet-Anwendungen](#)
- [Richtiger Zugriff auf den Suchserver](#)
- [Konfiguration wiederherstellen von Directory Proxy Server](#)
- [Migrieren von benutzerdefinierten web-src-Daten](#) [Manuelles Registrieren von Portal Server Secure Remote Access-Komponenten](#)
- [Aktivieren des URLScrapper-Kanals](#)
- [Vornehmen von Änderungen in der Abmeldeseite](#)

### *Migrieren von benutzerdefinierten web-src-Daten*

Wenn Sie benutzerdefinierte Dateien wie z. B. Bilder, Javascript-Dateien oder andere Dateien für das Konstruieren von `portal.war` dem folgenden Verzeichnis hinzugefügt haben:

```
PortalServer6-base/web-src
```

müssen Sie diese zusätzlichen Dateien in das entsprechende Verzeichnis in Portal Server Release 5 kopieren:

```
PortalServer7-base/web-src
```

### *Erneutes Bereitstellen von benutzerdefinierten Portlet-Anwendungen*

Wenn Sie benutzerdefinierte Portlet-Anwendungen erstellt und bereitgestellt haben, müssen diese Portlets Portal Server Release 5 nach der Aktualisierung manuell erneut bereitgestellt werden. Zwar sind Anzeige-Profileinträge vorhanden und der Kanalname wird angezeigt, der Inhalt ist jedoch erst zu sehen, nachdem Sie die benutzerdefinierten Portlets erneut bereitgestellt haben.

Stellen Sie die Portlets mit dem folgenden Befehl erneut bereit:

```
PortalServer7-base/bin/psadmin deploy-portlet
```

Sie können die erneute Bereitstellung überprüfen, indem Sie die entsprechenden .war- und XML-Dateien im folgenden Verzeichnis suchen:

```
PortalServer7Data-base/portals/Upgraded/war
```

### *Migrieren von benutzerdefinierten Portlet-Anwendungen*

Portlet-Anwendungen, die auf dem von Sun Java Web Console (SJWC) gelieferten Benutzerschnittstellen-Framework basieren, müssen manuell in Release 5 migriert und erneut bereitgestellt werden.

Diese Anforderung betrifft insbesondere vier Webanwendungen, die mit Portal Server als Beispiel-Portlet-Anwendungen verteilt werden, welche dazu gedacht sind, angepasst und in einem Portal installiert zu werden: *filesharing*, *surveys*, *wiki*, *rssportlet*. Bei der Aktualisierung werden fehlerkorrigierte Versionen dieser Beispiel-Portlet-Anwendungen im Bereich der Portlet-Anwendungen auf dem Datenträger platziert. Wenn Sie diese Portlet-Anwendungen für Ihren Gebrauch angepasst haben, müssen Sie sie manuell in Release 5 migrieren und erneut bereitstellen; sie werden nicht vom Portal Server-Aktualisierungsprozess erfasst.

Standardmäßig werden einige dieser Portlet-Anwendungen (*filesharing* und *surveys*) bereitgestellt und dem Benutzer zugänglich gemacht, wenn eine Community erstellt wird.

Sie können SJWC-basierende Portlet-Anwendungen folgendermaßen aktualisieren, anpassen und erneut bereitstellen. Die Portlet-Anwendung *filesharing* dient hierbei als Beispiel:

1. Extrahieren Sie die SJWC-JAR-Dateien von Release 5.
  - a. `mkdir /tmp/lh`
  - b. `cd /tmp/lh`

- c. `/usr/jdk/entsys-j2se/bin/jar xvf  
PortalServer7-base/portlet/communityportlets.war  
WEB-INF/lib/commons-beanutils.jar  
WEB-INF/lib/commons-collections-3.1.jar  
WEB-INF/lib/commons-digester.jar  
WEB-INF/lib/commons-logging.jar  
WEB-INF/lib/dataprovider.jar WEB-INF/lib/jsf-api.jar  
WEB-INF/lib/jsf-impl.jar WEB-INF/lib/webui.jar`
  - d. Benennen Sie eine dieser Dateien um.  
  
`mv WEB-INF/lib/commons-collections-3.1.jar  
WEB-INF/lib/commons-collections.jar`
2. Suchen Sie die Portlet-Anwendung filesharing.  
  
`cd PortalServer7Config-base/portals/portal1/portletapps/filesharing`
3. Geben Sie die aktualisierten SJWC-Bibliotheken ein.  
  
`jar uvf src/filesharing.war.tokenized -C /tmp/lh WEB-INF`
4. Passen Sie die Portlet-Anwendung filesharing an.  
  
`ant customize`
5. Stellen Sie die Portlet-Anwendung filesharing erneut bereit.
  - a. `PortalServer7-base/bin/psadmin undeploy-portlet -u amadmin  
-f passwordfile -p portal_id -i instance_id -g filesharing`
  - b. `ant deploy`
  - c. Gehen Sie zum folgenden Verzeichnis (je nach Webcontainer):  
  
*Anwendungsserver 8.x:*  
  
`AppServer8Config-base/domains/domain1/applications/j2ee-modules/  
communityportlets/WEB-INF`  
  
*Webserver 6.x:*  
  
`WebServer6-base/https-instanceName/webapps/https-instanceName/  
communityportlets/WEB-INF`  
  
*Webserver 7.x:*  
  
`WebServer7Config-base/https-configName/web-app/https-configName/  
communityportlets/WEB-INF`

- d. Öffnen Sie die Datei `sun-web.xml` und fügen Sie unmittelbar vor der letzten Zeile (d. h. vor dem End-Tag `sun-web-app`) die folgende Zeile hinzu:
 

```
<class-loader delegate="false"/>
```
- e. Wiederholen Sie [Schritt c](#) und [Schritt d](#) für die Datei `sun-web.xml` unter `filesharing/WEB-INF`.
6. Wiederholen Sie [Schritt 2](#) bis [Schritt 5](#) für `surveys` und alle weiteren auf dem SJWC-Framework basierenden benutzerdefinierten Portlet-Anwendungen.
7. Starten Sie den Webcontainer neu.

### *Richtiger Zugriff auf den Suchserver*

Bei der Aktualisierung von Portal Server Release 4 auf Release 5 wird der Suchserver von Portal Server getrennt, wodurch sich der URL-Zugriff auf diesen Server ändert.

- In Release 4 lautet die URL `http://hostName:port/portal/search`
- In Release 5 lautet die URL `http://hostName:port/UpgradedSearch/search`

Daher müssen Sie die Anzeigepprofile zu allen Portalkanälen (z. B. Search, DiscussionLite, Discussions und den Instant Messaging-Kanal) aktualisieren, die die Schnittstellen `SearchProvider` oder `DiscussionProvider` implementieren. Sie müssen insbesondere die Eigenschaft `searchServer` dieser Kanäle im Hinblick darauf ändern, auf welcher organisatorischen oder Rollenebene sie im Anzeigepprofil auftreten, um den Suchserver ordnungsgemäß zu referenzieren. Ändern Sie den Wert `searchServer` folgendermaßen:

```
value=„http://hostName:port/UpgradedSearch/search“
```

Für den Instant Messaging-Kanal muss außerdem die Instant Messaging-Serverkonfigurationseigenschaft `im_arch.portal.search` mit der neuen URL des Suchservers aktualisiert werden.

### *Konfiguration wiederherstellen von Directory Proxy Server*

Wenn Portal Server-Instanzen über eine Directory Proxy Server-Instanz auf Directory Server zugegriffen haben, müssen die ursprünglichen Werte der Directory Proxy Server-Host- und Anschlussnummereinstellungen vor dem Aktualisieren wiederhergestellt werden. Siehe [„Konfiguration entfernen von Directory Proxy Server“ auf Seite 355](#); hier wurden die Werte dieser Eigenschaften als Vorbereitung auf die Aktualisierung geändert.

## *Manuelles Registrieren von Portal Server Secure Remote Access-Komponenten*

Wenn ein Null Pointer-Ausnahmefehler auftritt, der an der Standardausgabe am Ende des Aktualisierungsverfahrens gemeldet wird, bedeutet dies, dass die Registrierung der Portal Server Secure Remote Access-Komponenten, sofern vorhanden, fehlgeschlagen ist.

In dieser Situation können Sie die Portal Server Secure Remote Access-Komponenten durch Ausführen des folgenden Befehls manuell registrieren (aktivieren):

```
PortalServer7-base/bin/psadmin provision-sra -u amadminUser -f passwordFile
-p Portal_ID --gateway-profile profileName --enable
```

## *Aktivieren des URLScrapper-Kanals*

Beim Aktualisieren von Release 4 auf Release 5 müssen Sie den URLScrapper-Kanal aktivieren. Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei der Portal Server-Konsole an.

Klicken Sie auf die Registerkarte "Portal" und anschließend auf das aktualisierte Portal.

2. Wählen Sie aus dem Dropdown-Menü "Select DN" (DN auswählen) die Option "TopLevel (Global)" (Obere Ebene (Global)) und klicken Sie auf die Verknüpfung "Download Display Profile" (Anzeigeprofil herunterladen).

Speichern Sie die heruntergeladene Datei an einem temporären Speicherort.

3. Suchen Sie `com.sun.portal.providers.urlscrapper.URLScrapperProvider`.
4. Suchen Sie den XML-Teil, der folgendermaßen beginnt:

```
<Provider advanced="false"
class="com.sun.portal.providers.urlscrapper.URLScrapperProvider"
und folgendermaßen endet:
</Provider>
```

5. Ersetzen Sie den XML-Teil in [Schritt 4](#) mit der folgenden Angabe:

```
<Provider advanced="false"
class="com.sun.portal.providers.urlscrapper.URLScrapperProvider"
container="false" lock="false" merge="fuse"
name="URLScrapperProvider" version="2">

<Properties advanced="false" lock="false" merge="fuse"
name="_properties" propagate="true">
```

```

<String advanced="false" lock="false" merge="replace" name="title"
propagate="true" value="UrlScrapper Channel"/>

<String advanced="false" lock="false" merge="replace"
name="description" propagate="true" value="This is a test for
urlscrapper"/>

<Boolean advanced="true" lock="false" merge="replace"
name="isEditable" propagate="true" value="false"/>

<Boolean advanced="true" lock="false" merge="replace"
name="isTopLevel" propagate="true" value="false"/>

<String advanced="true" lock="false" merge="replace" name="editType"
propagate="true" value="edit_subset"/>

<Boolean advanced="true" lock="false" merge="replace"
name="enableUBT" propagate="true" value="false"/>

<String advanced="false" lock="false" merge="replace"
name="urlScrapperRulesetID" propagate="true"
value="default_ruleset"/>

<String advanced="false" lock="false" merge="replace" name="width"
propagate="true" value="thick"/>

<String advanced="true" lock="false" merge="replace"
name="refreshTime" propagate="true" value="0"/>

<String advanced="true" lock="false" merge="replace" name="helpURL"
propagate="true" value="en/desktop/urlscrpr.htm"/>

<String advanced="false" lock="false" merge="replace" name="url"
propagate="true" value=""/>

<String advanced="false" lock="false" merge="replace"
name="fontFace1" propagate="true" value="Sans-serif"/>

<String advanced="false" lock="false" merge="replace"
name="productName" propagate="true" value="Sun Java™ System Portal
Server 7"/>

<Boolean advanced="false" lock="false" merge="replace"
name="cookiesToForwardAll" propagate="true" value="true"/>

<String advanced="false" lock="false" merge="replace"
name="inputEncoding" propagate="true" value="UTF-8"/>

```

```

<Collection advanced="false" lock="false" merge="fuse"
name="cookiesToForwardList" propagate="true"/>

<Integer advanced="false" lock="false" merge="replace"
name="timeout" propagate="true" value="100"/>

<String advanced="true" lock="false" merge="replace" name="formData"
propagate="true" value=""/>

<Boolean advanced="true" lock="false" merge="replace"
name="isHttpAuth" propagate="true" value="false"/>

<String advanced="true" lock="false" merge="replace" name="loginUrl"
propagate="true" value=""/>

<String advanced="true" lock="false" merge="replace"
name="loginFormData" propagate="true" value=""/>

<String advanced="true" lock="false" merge="replace" name="uid"
propagate="true" value=""/>

<String advanced="true" lock="false" merge="replace" name="password"
propagate="true" value=""/>

<ConditionalProperties advanced="false" condition="client"
lock="false" merge="fuse" propagate="true" value="HTML">

<ConditionalProperties advanced="false" condition="locale"
lock="false" merge="fuse" propagate="true" value="en">

<String advanced="true" lock="false" merge="replace" name="helpURL"
propagate="true" value="en/desktop/urlscrpr.htm"/>

<String advanced="false" lock="false" merge="replace" name="url"
propagate="true" value=""/>

</ConditionalProperties>

<String advanced="true" lock="false" merge="replace" name="helpURL"
propagate="true" value="en/desktop/urlscrpr.htm"/>

<String advanced="false" lock="false" merge="replace" name="url"
propagate="true" value=""/>

</ConditionalProperties>

<ConditionalProperties advanced="false" condition="locale"
lock="false" merge="fuse" propagate="true" value="en">

```



```

<String advanced="false" lock="false" merge="replace" name="title"
propagate="true" value="UrlScraper Channel"/>

<String advanced="false" lock="false" merge="replace"
name="description" propagate="true" value="This is a test for
urlscraper"/>

</ConditionalProperties>

</Properties>

</Provider>

```

6. Speichern Sie die geänderte Datei und laden Sie sie hoch.

### *Vornehmen von Änderungen in der Abmeldeseite*

Die Abmeldeseite in Portal Server Release 5 hat sich gegenüber der vorherigen Access Manager-Abmeldeseite geändert. Beachten Sie, dass diese Änderung keinen Fehler in der Software darstellt.

### **Aufheben der Aktualisierung (Solaris)**

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Verfahren zum Aufheben der Aktualisierung Portal Server haben, sowie eine Beschreibung des eigentlichen Verfahrens zum Aufheben der Aktualisierung.

#### *Zu berücksichtigende Aspekte beim Aufheben der Aktualisierung (Solaris)*

Beim Aufheben der Aktualisierung auf Release 5 wird die Installation von Release 4 in *PortalServer6-base* wiederhergestellt und die Webanwendungen von Release 4 werden erneut bereitgestellt.

#### *Verfahren zum Aufheben der Aktualisierung (Solaris)*

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Stellen Sie den Zustand von Directory Server vor der Aktualisierung wieder her.

Verwenden Sie die Directory

Server-Sicherungs-/Wiederherstellungs-Befehlszeile und die GUI-Programme.

Lesen Sie hierzu das Kapitel "Directory Server Backup and Restore" im *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*,

<http://docs.sun.com/doc/819-0995>.

3. Beenden Sie Portal Server, indem Sie seinen Webcontainer beenden.

Webserver 6.x:

*WebServer-base/https-instanceName/stop*

Webserver 7.0:

Admin Server--

*WebServer7Config-base/admin-server/bin/stopserv*

Instance Server--

*WebServer7Config-base/https-configName/bin/stopserv*

Anwendungsserver 8.x:

*AppServer8-base/bin/asadmin stop-domain --user admin\_ID  
--password password domainName*

4. Entfernen Sie die Portal Server Release 5-Pakete.
  - a. Starten Sie das Java ES-Deinstallationsprogramm.  
*/var/sadm/prod/SUNWentsys5/uninstall*
  - b. Wählen Sie alle installierten Portal Server-Komponenten aus.
  - c. Bestätigen Sie Ihre Auswahl für die Deinstallation.
  - d. Beenden Sie das Java ES-Deinstallationsprogramm.
5. Starten Sie Portal Server neu, indem Sie seinen Webcontainer neu starten.

Webserver 6.x:

*WebServer-base/https-instanceName/start*

Webserver 7.0:

Admin Server--

*WebServer7Config-base/admin-server/bin/startserv*

Instance Server--

*WebServer7Config-base/https-configName/bin/startserv*

Anwendungsserver 8.x:

*AppServer8-base/bin/asadmin start-domain --user admin\_ID  
--password password domainName*

6. Stellen Sie die Webanwendungen von Portal Server Release 4 erneut bereit. Verwenden Sie hierzu den folgenden Befehl aus der Java ES Release 5-Verteilung:

```
cd os_arch/Products/portal_svr/Tools/upgrade/bin
./psupgrade rollback
```

wobei *os\_arch* der Plattform entspricht, wie z. B. *Solaris\_sparc*.

Mit dem Befehl `psupgrade rollback` wird die Bereitstellung der Webanwendungen von Portal Server Release 5 aufgehoben und die Webanwendungen von Portal Server Release 4 werden erneut bereitgestellt.

Mit dem Befehl wird der Inhalt aus *PortalServer6-base/web-src* in */var/PortalServer6-base/https-hostName/deploy-dir/web-apps* erneut bereitgestellt. Anpassungen der Portal Server-Webanwendung sollten daher zuerst in */web-src* vorgenommen und anschließend in */web-apps* bereitgestellt werden. Änderungen, die Sie unter */web-apps* vornehmen, sollten in */web-src* repliziert werden, *bevor* Sie den `psupgrade rollback`-Befehl ausführen. Andernfalls werden diese Änderungen überschrieben.

7. Halten Sie den Webcontainer an und starten Sie ihn erneut.

Ein Neustart des Webcontainers ist zwar nicht in jedem Fall erforderlich, dadurch wird jedoch sichergestellt, dass der Status von Portal Server beim Start eindeutig ist.

## Aufheben der Aktualisierung (Linux)

Da für die Aktualisierung auf Release 5 die binären Release 4-Dateien entfernt werden müssen, ist das Aufheben der Aktualisierung unter Linux sehr aufwändig.

Eine Möglichkeit zum Aufheben der Aktualisierung besteht darin, *vor* der Aktualisierung ein paralleles System zu erstellen und dieses System vor der Aktualisierung zu testen. Wenn Sie die Aktualisierung aufheben müssen, können Sie zu diesem parallelen System zurückkehren.

## Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen wird Portal Server auf mehreren Computersystemen bereitgestellt, um die Skalierbarkeit zu gewährleisten und die Verfügbarkeit zu verbessern. Möglicherweise führen Sie beispielsweise Portal Server-Instanzen auf mehreren Computern zusammen mit einem Lastenausgleichsprogramm aus, um die Last zu verteilen.

Für Portal Server-Instanzen mit Lastenausgleich können Sie ein sogenanntes Rolling Upgrade durchführen, bei dem Sie alle Portal Server-Instanzen nacheinander aktualisieren, ohne den Dienst zu unterbrechen, wie nachstehend beschrieben. Für dieses Verfahren gelten folgende Einschränkungen: Portal Server Release 4 funktioniert nicht mit Verzeichnisdaten aus Portal Server Release 5.

Die in [Abbildung 15-1 auf Seite 375](#) dargestellte Bereitstellungsarchitektur dient zur Demonstration eines Rolling Upgrade der Portal Server Release 4-Instanzen auf Release 5.

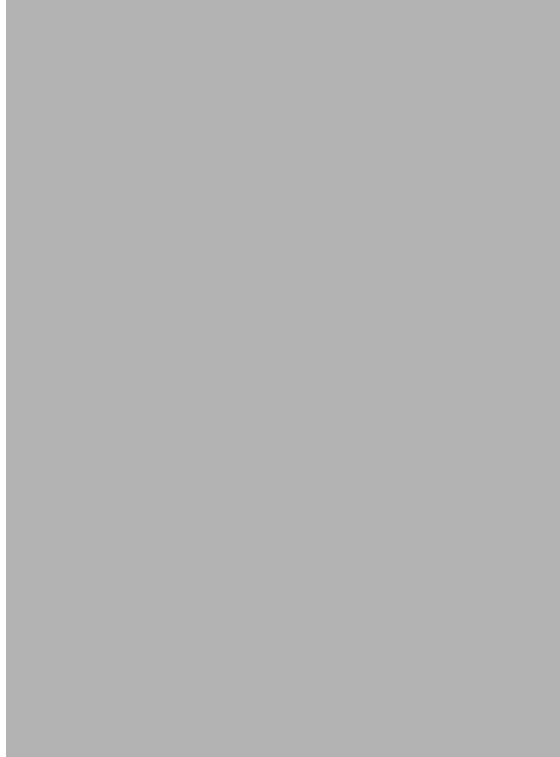
---

**HINWEIS** Informationen zu Architekturen, die Portal Server Secure Remote Access-Komponenten enthalten, finden Sie unter „[Aktualisierung mehrerer Instanzen](#)“ auf Seite 435.

---

In der in [Abbildung 15-1](#) dargestellten Architektur erfolgt der Zugriff auf mehrere Portal Server-Instanzen über einen Lastenausgleich, um Verfügbarkeit und Skalierbarkeit zu gewährleisten. Die Portal Server-Instanzen greifen wiederum über einen Lastenausgleich auf die Access Manager-Instanzen zu. Die Access Manager- und Access Manager-SDK-Instanzen greifen auf ein Verzeichnis zu, das für die Multimaster-Replikation (MMR) eingerichtet wurde. Während andere Directory Server-Replikationsschemata möglich sind, ist MMR repräsentativ für hochverfügbare und skalierbare Directory-Dienste.

In [Abbildung 15-1](#) werden die verschiedenen Instanzen von Portal Server, Access Manager und Directory Server gruppiert dargestellt, um die Erklärung des Aktualisierungsvorgangs zu erleichtern. Portal Server 2 stellt beispielsweise die zweite bis n-te Instanz von Portal Server dar.

**Abbildung 15-1** Beispiel für Bereitstellungsarchitektur für mehrere Portal Server-Instanzen

Das Rolling Upgrade von Portal Server Release 4 auf Release 5 wird folgendermaßen durchgeführt:

1. Wenn Sie von Access Manager Release 4 auf Release 5 aktualisieren, führen Sie ein Rolling Upgrade durch, wie unter „[Aktualisierung mehrerer Instanzen](#)“ auf Seite 309 beschrieben. Wenn Sie Portal Server Release 4 auf Release 5 aktualisieren, brauchen Sie Access Manager Release 4 nicht auf Release 5 zu aktualisieren.
2. Konfigurieren Sie Portal Server 2 mit einem Verweis auf Directory Server 2 statt auf Directory Server 1.

Um die Anweisungen zu verkürzen, bedeutet „Portal Server 2“ in den folgenden Schritten Portal Server 2 bis Portal Server n.

3. Aktualisieren Sie Portal Server 1.

- a. Deaktivieren Sie Portal Server 1 im Lastenausgleichsprogramm B.  
Anfragen werden nicht mehr an Portal Server 1 weitergeleitet.
- b. Deaktivieren Sie Directory Server MMR.  
Directory Server 2Anfragen werden nicht mehr an Directory Server 1.  
weitergeleitet.
- c. Aktualisieren Sie Access Manager SDK 1B auf Release 5.  
Führen Sie hierzu das unter „[Ausschließliche Aktualisierung der Release 4-Version von Access Manager SDK](#)“ auf Seite 311 beschriebene Verfahren durch.

- d. Aktualisieren Sie Portal Server 1 auf Release 5.  
Führen Sie die Aktualisierung der Portal Server-Instanz wie unter „[Aktualisierung der Release 4-Version von Portal Server](#)“ auf Seite 348 beschrieben durch und achten Sie dabei auf Folgendes:
  - Die folgende Aufgabe muss vor der Aktualisierung durchgeführt werden: „[Entfernen der Konfiguration für das Lastenausgleichsprogramm](#)“ auf Seite 354.
  - Vergewissern Sie sich vor der Durchführung der Aktualisierung, dass der Wert `am.encrypted.pwd` in der Datei `AccessManagerConfig-base/config/AMConfig.properties` im lokalen Access Manager-SDK sowie dessen zugeordneter Access Manager-Remote-Instanz identisch ist.
  - Achten Sie darauf, einen einmaligen Wert, der nicht Null lautet, für den von `psupgrade` benötigten Parameter `Portal Instance ID` für jede zu aktualisierende Portal Server-Instanz anzugeben.

Die Portal Server-Daten für Directory Server 1 werden auf Release 5 aktualisiert.

- e. Aktivieren Sie Portal Server 1 im Lastenausgleichsprogramm B.  
Anfragen werden wieder an Portal Server 2 weitergeleitet.
4. Aktualisieren Sie Portal Server 1.
    - a. Deaktivieren Sie Portal Server 1 im Lastenausgleichsprogramm B.  
Anfragen werden nicht mehr an Portal Server 2 weitergeleitet.
    - b. Stellen Sie die Konfiguration von Portal Server 1 wieder her, sodass auf Directory Server 1 verwiesen wird.

- c. Aktualisieren Sie Access Manager SDK 1B auf Release 5.

Verwenden Sie dasselbe Verfahren wie unter [Schritt c auf Seite 376](#).

- d. Aktualisieren Sie Portal Server 2 auf Release 5.

Verwenden Sie dasselbe Verfahren wie unter [Schritt d auf Seite 376](#).

- e. Aktivieren Sie Portal Server 1 im Lastenausgleichsprogramm B.

Anfragen werden wieder an Portal Server 2 weitergeleitet.

- 5. Aktivieren Sie Directory Server MMR.

Die Portal Server-Daten für Directory Server 2 werden nun mit Directory Server 1 synchronisiert.

# Aktualisieren von Portal Server von Java ES Release 3

Die Vorgehensweise für die Aktualisierung von Java ES 2005Q1 (Release 3) Portal Server auf Release 5 ist abgesehen von den folgenden Ausnahmen mit der Aktualisierung von Release 4 Portal Server auf Release 5 identisch.

- [Aufgabe vor der Aktualisierung von Release 3: Aktualisieren der Portal Server-Abhängigkeiten](#)
- [Aktualisieren von Release 3 Portal Server](#)
- [Aufgaben nach der Aktualisierung von Release 3](#)
- [Aktualisierung mehrerer Instanzen](#)

## Aufgabe vor der Aktualisierung von Release 3: Aktualisieren der Portal Server-Abhängigkeiten

Bei der Aktualisierung von Portal Server von Release 3 müssen Sie jedoch *sowohl* Access Manager als auch die Webcontainer (Webserver oder Anwendungsserver) auf Release 4 oder Release 5 aktualisieren, bevor Sie Portal Server aktualisieren. Sie können weder Abhängigkeiten in Release 4 belassen noch lediglich bestimmte Abhängigkeiten auf Release 5 aktualisieren. Weitere Informationen finden Sie unter „[Selektive Aktualisierung](#)“ auf Seite 344.

Die folgenden Abhängigkeiten müssen in der unten gezeigten Reihenfolge aktualisiert werden.

1. **Gemeinsam genutzte Komponenten.** Anleitungen für die Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie in [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“](#) auf Seite 71.
2. **Directory Server.** Anleitungen für die Aktualisierung von Directory Server auf Release 4 finden Sie in [Kapitel 5, „Directory Server“](#) auf Seite 109.
3. **Webcontainer-Software.** Anweisungen zur Aktualisierung von Webserver und Anwendungsserver finden Sie in [Kapitel 7, „Webserver“](#) auf Seite 143 bzw. [Kapitel 11, „Anwendungsserver“](#) auf Seite 219.



---

**HINWEIS** Die Aktualisierung von Drittanbieter-Webcontainern, wie beispielsweise Webcontainer von WebLogic und WebSphere, kann dazu führen, dass Portal Server nicht ordnungsgemäß funktioniert, da Anpassungen hinsichtlich dieser Container für die Unterstützung von Portal Server bei der Container-Aktualisierung überschrieben werden.

In diesem Fall müssen Sie Portal Server erneut installieren und für die aktualisierte Container-Umgebung erneut konfigurieren.

---

4. **Access Manager (Access Manager SDK).** Anweisungen zur Aktualisierung von Access Manager auf Release 5 finden Sie in [Kapitel 14, „Access Manager“ auf Seite 281](#).

## Aktualisieren von Release 3 Portal Server

Um die Release 3-Version von Portal Server auf Release 4 zu aktualisieren, folgen Sie den Anweisungen unter [„Aktualisieren von Portal Server von Java ES Release 4“ auf Seite 346](#). Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 3.

## Aufgaben nach der Aktualisierung von Release 3

Bei der Aktualisierung von Portal Server von Release 3 auf Release 5 müssen Sie zusätzlich zu den unter [„Aufgaben nach der Aktualisierung von Release 4“ auf Seite 364](#) beschriebenen Verfahren nach der Aktualisierung die Verfahren für die folgenden Situationen durchführen:

- [Abonnieren einer Diskussion](#)

### Abonnieren einer Diskussion

Das Abonnieren einer Diskussion in einer Community erfolgt erst dann erfolgreich, wenn Sie die Eigenschaften der obersten Ebene des globalen Anzeigeprofils bearbeitet haben, um die folgende String-Eigenschaft hinzuzufügen:

`helpURL=en/desktop/usedesk.htm`

Gehen Sie folgendermaßen vor:

1. Erstellen Sie eine Anzeigeprofil-XML-Snippet-Datei, `helpUrl.xml`:

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE DisplayProfile SYSTEM "jar://resources/psdp.dtd">
<Eigenschaften>
 <String name="helpURL" value="en/desktop/usedesk.htm" />
</Properties>
```

2. Führen Sie die Eigenschaften des globalen Anzeigeprofiles mit dem folgenden Befehl aus:

```
./psadmin modify-dp -u amadminUser -f /tmp/passwordFile -p portal_ID
-m -g helpUrl.xml
```

Die `-m`-Option ist erforderlich, damit nicht das gesamte globale Anzeigeprofil überschrieben wird.

## Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen wird Portal Server auf mehreren Computersystemen bereitgestellt, um die Skalierbarkeit zu gewährleisten und die Verfügbarkeit zu verbessern. Möglicherweise führen Sie beispielsweise Portal Server-Instanzen auf mehreren Computern zusammen mit einem Lastenausgleichsprogramm aus, um die Last zu verteilen.

Für Portal Server-Instanzen mit Lastenausgleich können Sie ein sogenanntes Rolling Upgrade durchführen, bei dem Sie alle Portal Server-Instanzen nacheinander aktualisieren, ohne den Dienst zu unterbrechen, wie nachstehend beschrieben. Für dieses Verfahren gelten folgende Einschränkungen: Portal Server Release 3 funktioniert nicht mit Verzeichnisdaten aus Portal Server Release 5.

Zur Durchführung eines Rolling Upgrade von Portal Server Release 3 auf Release 5 gehen Sie wie unter „[Aktualisierung mehrerer Instanzen](#)“ auf [Seite 373](#) beschrieben vor. Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 3. Außerdem müssen Sie Access Manager aktualisieren, wie unter [Schritt 1 auf Seite 375](#) beschrieben.

# Aktualisieren von Portal Server von Java ES Release 2

Dieser Abschnitt enthält Informationen zum Aktualisieren von Java ES 2004Q2 (Release 2) Portal Server auf Release 5. Das Aktualisierungsverfahren ähnelt dem für das Aktualisieren von Release 4 Portal Server auf Release 5 mit Ausnahme von einigen Änderungen, die in den nachfolgenden Abschnitten erläutert sind:

- [Aufgaben vor der Aktualisierung von Release 2](#)
- [Aktualisieren von Release 2 Portal Server](#)
- [Aufgaben nach der Aktualisierung von Release 2](#)
- [Aktualisierung mehrerer Instanzen](#)

## Aufgaben vor der Aktualisierung von Release 2

Die Aufgaben vor der Aktualisierung von Portal Server von Release 2 sind mit den in [„Aufgaben vor der Aktualisierung von Release 4“ auf Seite 349](#) beschriebenen identisch, mit Ausnahme der Aktualisierung der Portal Server-Abhängigkeiten.

Bei der Aktualisierung von Portal Server von Release 2 müssen Sie *sowohl* Access Manager als auch die Webcontainer (Webserver oder Anwendungsserver) auf Release 4 oder Release 5 aktualisieren, bevor Sie Portal Server aktualisieren. Sie können weder Abhängigkeiten in Release 2 belassen noch lediglich bestimmte Abhängigkeiten auf Release 4 aktualisieren. Weitere Informationen finden Sie unter [„Selektive Aktualisierung“ auf Seite 344](#).

Insbesondere muss die Webcontainer-Software von Release 2 aktualisiert werden, was bedeutet, dass nur Szenario 2 und Szenario 5 in [Tabelle 15-4 auf Seite 345](#) bei Ausführung des Skripts psupgrade unterstützt werden.

Die folgenden Abhängigkeiten müssen in der unten gezeigten Reihenfolge aktualisiert werden.

1. **Gemeinsam genutzte Komponenten.** Anleitungen für die Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie in [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#).
2. **Directory Server.** Anleitungen für die Aktualisierung von Directory Server auf Release 4 finden Sie in [„Aktualisieren von Directory Server von Java ES Release 2“ auf Seite 126](#).

3. **Webcontainer-Software.** Anweisungen zur Aktualisierung von Webserver und Anwendungsserver finden Sie in [Kapitel 7, „Webserver“](#) auf Seite 143 bzw. [Kapitel 11, „Anwendungsserver“](#) auf Seite 219.

---

**HINWEIS** Die Aktualisierung von Drittanbieter-Webcontainern, wie beispielsweise Webcontainer von WebLogic und WebSphere, kann dazu führen, dass Portal Server nicht ordnungsgemäß funktioniert, da Anpassungen hinsichtlich dieser Container für die Unterstützung von Portal Server bei der Container-Aktualisierung überschrieben werden. In diesem Fall müssen Sie Portal Server erneut installieren und für die aktualisierte Container-Umgebung erneut konfigurieren.

---

4. **Access Manager (Access Manager SDK).** Anweisungen zur Aktualisierung von Access Manager auf Release 5 finden Sie in [Kapitel 14, „Access Manager“](#) auf Seite 281.

## Aktualisieren von Release 2 Portal Server

Das Verfahren für die Aktualisierung von Portal Server Release 2 auf Release 5 hängt von dem Webcontainer ab, in dem die Portal Server-Software bereitgestellt werden soll, wie in den nachfolgenden Abschnitten beschrieben.

### Aktualisieren der Release 2-Version von Portal Server: Webserver-Webcontainer

Um die Release 2-Version von Portal Server auf Release 5 zu aktualisieren, wobei die Bereitstellung in einem Webserver-Webcontainer erfolgt, folgen Sie den Anweisungen unter [„Aktualisieren von Portal Server von Java ES Release 4“](#) auf Seite 346. Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 2.

Wenn Portal Server jedoch in Webserver Release 5 (Webserver 7.0) bereitgestellt wird, müssen Sie vor der Aktualisierung von Webserver Release 2 die folgenden Schritte durchführen:

1. Melden Sie sich bei der Webserver-Konsole an.
2. Klicken Sie auf "Edit Virtual Servers" (Virtuelle Server bearbeiten) > "Web Applications" (Web-Anwendungen).

3. Entfernen Sie alle bereitgestellten Webanwendungen mit einer URI, die `/portal` oder `/portalsamples`
4. Klicken Sie auf "Speichern".
5. Klicken Sie auf "Deployment Pending" (Bereitstellung ausstehend).

## Aktualisieren der Release 2-Version von Portal Server: Anwendungsserver-Webcontainer

Bei der Aktualisierung von Portal Server Release 2 auf Release 5 wurde der Anwendungsserver bei einer Bereitstellung in einem Anwendungsserver-Webcontainer von Release 2 auf Release 5 aktualisiert.

Die Anwendungsserver-Instanz von Release 2, in der Portal Server ursprünglich bereitgestellt wurde (*instanceName*), wurde bei der Aktualisierung auf Release 5 in einen vom Anwendungsserver-Aktualisierungsvorgang erstellten Knotenagenten migriert. Für die Aktualisierung von Portal Server in dieser aktualisierten Anwendungsserver-Instanz sind folgende Schritte erforderlich:

1. Melden Sie sich als Root oder Superuser an.  
`su -`
2. Synchronisieren Sie alle gemeinsam genutzten Komponenten auf Release 5, sofern dies noch nicht erfolgt ist.

Anweisungen hierzu erhalten Sie unter [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“](#) auf Seite 71.

Dieser Schritt ist eine erforderliche Voraussetzung für die Ausführung des Skripts `psupgrade` in [Schritt 9 auf Seite 385](#).

3. Stoppen Sie etwaige Instanzen von Portal Server Secure Remote Access Gateway, Rewriter-Proxy oder Netlet-Proxy, die möglicherweise lokal ausgeführt werden.

```
PortalServer6-base/bin gateway stop
PortalServer6-base/bin netletd stop
PortalServer6-base/bin rwproxycd stop
```

Überprüfen Sie, ob die Prozesse angehalten wurden. Beispiel:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

4. Vergewissern Sie sich, dass Access Manager ausgeführt wird, wenn es in einem anderen Webcontainer bereitgestellt wird als dem, in dem Portal Server bereitgestellt wird.

5. Starten Sie Portal Server, sofern es nicht bereits ausgeführt wird, indem Sie den Webcontainer starten, in dem es bereitgestellt wird.

- a. Starten Sie den Domain Administration Server (DAS), falls dieser noch nicht gestartet wurde.

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
--password password domainName
```

- b. Starten Sie die aktualisierte Anwendungsserver-Instanz, in der Portal Server bereitgestellt wurde (*instanceName*), wenn diese Serverinstanz nicht bereits ausgeführt wird.

Starten Sie hierfür den Knotenagenten, in den die aktualisierte Anwendungsserver-Instanz migriert wurde.

```
AppServer8-base/bin/asadmin start-node-agent --user admin_ID
--password password nodeagentName
```

In den oben genannten Befehlen und in den folgenden Schritten werden folgende Konventionen verwendet:

- wobei *nodeagentName* der Form *hostName\_domainName* entspricht, jedoch standardmäßig nur *hostName* lautet.
- Der Standard für *domainName* lautet *domain1*.
- Der Standard für *instanceName* lautet *server1*.

6. Heben Sie die Bereitstellung der Portal Server-Komponenten auf.

```
AppServer8-base/bin/asadmin undeploy --user admin_ID
--password password --target instanceName portal
```

```
AppServer8-base/bin/asadmin undeploy --user admin_ID
--password password --target instanceName portletsamples
```

7. Setzen Sie die zwei Umgebungsvariablen (ANT\_HOME und JAVA\_HOME), die vom Skript *psupgrade* benötigt werden. Beispiel:

Solaris-Betriebssystem:

```
export ANT_HOME=/usr/sfw
export JAVA_HOME=/usr/jdk/entsys-j2se
```

Linux-Betriebssystem:

```
export ANT_HOME=/opt/sun
export JAVA_HOME=/usr/jdk/entsys-j2se
```

8. Stellen Sie sicher, dass auf Ihrem Computer ausreichend Swap-Speicher zur Verfügung steht.

Der Swap-Speicher sollte grundsätzlich die doppelte Größe des physikalischen RAM aufweisen.

9. Führen Sie das Skript `psupgrade` über die Java ES Release 5-Verteilung aus.

```
cd os_arch/Products/portal_svr/Tools/upgrade/bin
./psupgrade
```

wobei *os\_arch* der Plattform entspricht, wie z. B. *Solaris\_sparc*.

- 
- HINWEIS** Sollten Sie `psupgrade` versehentlich vom falschen *os\_arch*-Verzeichnis aus gestartet haben, müssen Sie das Verfahren folgendermaßen rückgängig machen:
- a. Wechseln Sie in das richtige *os\_arch*-Verzeichnis.
  - b. Machen Sie die Änderungen an den Portal Server-Daten rückgängig.  
  

```
./psupgrade rollback
```

Geben Sie die erforderlichen Parameter und Passwörter an.
  - c. Führen Sie `psupgrade` erneut aus.
- 

Das Skript `psupgrade` ruft das Java ES-Installationsprogramm auf, um neue Pakete zu installieren, und weist das System an, Speicherort, Anschlussnummer und andere Informationen zum Webcontainer zu erkennen, in dem Sie Portal Server-Webanwendungen bereitstellen. Je nach Webcontainer-Aktualisierungsszenario (siehe [Tabelle 15-4 auf Seite 345](#)), in diesem Fall Szenario 5, fordert das Skript Sie auf, Informationen einzugeben, die für die Bereitstellung von Portal Server für den entsprechenden Webcontainer erforderlich sind.

[Tabelle 15-6 auf Seite 351](#) enthält die erforderlichen Informationen, wenn Anwendungsserver Release 2 auf Release 5 aktualisiert wurde (Szenario 5).

---

**HINWEIS** Achten Sie darauf, die richtigen Werte für die psupgrade-Parameter einzugeben, denn Sie können nicht zurückgehen und sie ändern. Des Weiteren ist es sehr schwierig, vom Skript psupgrade vorgenommene Änderungen rückgängig zu machen. Zum Rückgängig machen von Änderungen an Portal Server-Daten müssen Sie

`./psupgrade rollback`

ausführen, bevor Sie psupgrade erneut ausführen.

---

10. Beenden Sie den Domain Administration Server (DAS) und den in [Schritt 5 auf Seite 384](#) gestarteten Knotenagenten.

```
AppServer8-base/bin/asadmin stop-domain --user admin_ID
--password password domainName
```

```
AppServer8-base/bin/asadmin stop-node-agent --user admin_ID
--password password nodeagentName
```

11. Starten Sie den Domain Administration Server (DAS), den Knotenagenten und die in [Schritt 10](#) angehaltene Serverinstanz neu.

---

**HINWEIS** Starten Sie den Knotenagent separat mithilfe der Option `startinstances=false`, bevor die Serverinstanz wie unten dargestellt gestartet wird.

---

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
--password password domainName
```

```
AppServer8-base/bin/asadmin start-node-agent --port DASportNumber
--startinstances=false --user admin_ID --password password
nodeagentName
```

```
AppServer8-base/bin/asadmin start-instance --port DASportNumber
--user admin_ID --password password instanceName
```

Der Standardwert für `DASportNumber` lautet 4848.



## Aufgaben nach der Aktualisierung von Release 2

Bei der Aktualisierung von Portal Server von Release 2 auf Release 5 müssen Sie zusätzlich zu den unter [„Aufgaben nach der Aktualisierung von Release 4“](#) auf [Seite 364](#) beschriebenen Verfahren nach der Aktualisierung die Verfahren für die folgenden Situationen durchführen:

- [Single Sign-On-Konfiguration](#)
- [Aktivieren des URLScrapper-Kanals](#)
- [Löschen des Gateway-Diensteintrags](#)

### Single Sign-On-Konfiguration

Nach der Aktualisierung von Portal Server von Release 2 schlagen Desktop-Kommunikationskanäle wie Mail, Kalender und Adressbuch, die mittels der ssoadapter-Meta-Vorlage auf einen Back-End-Server zugreifen, fehl.

Wenn Sie beispielsweise die ssoadapter-Mail-Meta-Vorlage SUN-UWC-MAIL in Release 2 geändert, d. h. speziell für Ihren Messaging-Server eingestellt haben, gibt es nach der Aktualisierung auf Release 5 zwei ssoadapter-Meta-Vorlagen SUN-UWC-MAIL: Eine ist die unveränderte Version in Release 2, die andere die neue in Release 5. Doppelte ssoadapter-Meta-Vorlagen sind in der Portal Server-Konsole und der Befehlszeilenschnittstelle psadmin vorhanden; sie haben beide denselben Namen.

Kanäle, die die ssoadapter-Meta-Vorlagen verwenden, können keine Verbindung zum Back-End-Server aufbauen und Daten abrufen.

Zur Behebung dieses Problems müssen Sie die Daten der ssoadapter-Meta-Vorlagen abrufen, die doppelten Einträge umbenennen und die geänderten Daten anschließend ersetzen. Gehen Sie folgendermaßen vor:

1. Exportieren Sie die Daten der ssoadapter-Meta-Vorlagen.

Verwenden Sie das Programm amadmin folgendermaßen zum Exportieren der Access Manager-Dienstdaten:

- a. Erstellen Sie eine amadmin-Anforderungsdatei /tmp/ssoadapter-template-gets.xml.

Diese Datei wird vom Programm zum Abrufen der Daten der ssoadapter-Meta-Vorlagen verwendet:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE Requests
 PUBLIC "-//iPlanet//iDSAME 5.0 Admin CLI DTD//EN"
 "jar://com/iplanet/am/admin/cli/amAdmin.dtd"
>
<Anforderungen>
 <SchemaRequests serviceName="SunSSOAdapterService"
 SchemaType="global">
 <GetServiceDefaultValues>
 <Attribute name="sunConfigurationTemplates" />
 </GetServiceDefaultValues>
 </SchemaRequests>
</Requests>
```

- b. Führen Sie folgenden asadmin-Befehl aus:

```
AccessManager-base/bin/amadmin -u amadminUser -w password
-t ssoadapter-templates-get.xml > /tmp/ssoadapter-templates.xml
```

Die Ausgabe des Befehls wird in /tmp/ssoadapter-templates.xml gespeichert.

Die Datei /tmp/ssoadapter-templates.xml hat das folgende Format:

```
sunConfigurationTemplates=
[<ssoadapter meta-template1>, <ssoadapter meta-template2>, ...]
```

und jede <ssoadapter-Meta-Vorlage> hat die folgende Syntax:

```
default|imap:/?configName=SUN-UWC-MAIL
&proxyAdminPassword=%5BPROXY-ADMIN_PASSWORD%5D&subType=sun-one
&enableProxyAuth=false ...
```

2. Ändern Sie die Datei /tmp/ssoadapter-templates.xml, um die doppelten ssoadapter-Meta-Vorlagen umzubenennen.

- a. Suchen Sie alle Vorlagen in der Datei /tmp/ssoadapter-templates.xml.

Suchen Sie die Zeichenfolge default|imap:/?configName= .

- b. Ersetzen Sie die Namen der doppelten ssoadapter-Meta-Vorlagen durch einmalige Werte.

Wenn beispielsweise zwei ssoadapter-Meta-Vorlagen mit dem Namen SUN-UWC-MAIL vorliegen, ersetzen Sie den Wert configName einer der Vorlagen durch SUN-UWC-MAIL2. Hierdurch entstehen anschließend zwei Vorlagen mit einmaligem Namen:

```
default|imap:/?configName=SUN-UWC-MAIL ...
default|imap:/?configName=SUN-UWC-MAIL2 ...
```

3. Erstellen Sie eine amadmin-Anforderungsdatei, die die geänderten ssoadapter-Meta-Vorlagen importiert und die ursprünglichen Daten überschreibt.

- a. Kopieren Sie /tmp/ssoadapter-templates.xml in /tmp/ssoadapter-new-templates.xml
- b. Ersetzen Sie in /tmp/ssoadapter-new-templates.xml die Zeichenfolge:

```
sunConfigurationTemplates=[
```

durch:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE Requests
 PUBLIC "-//iPlanet//iDSAME 5.0 Admin CLI DTD//EN"
 "jar://com/iplanet/am/admin/cli/amAdmin.dtd"
>
<Anforderungen>
 <SchemaRequests serviceName="SunSSOAdapterService"
 SchemaType="Global">
 <ModifyDefaultValues>
 <AttributeValuePair>
 <Attribute name="sunConfigurationTemplates" />
 </AttributeValuePair>
 </ModifyDefaultValues>
 </SchemaRequests>
</Anforderungen>
```

- c. Ersetzen Sie alle UND-Zeichen ("&") durch "&amp;".

So würde beispielsweise die Zeile:

```
default|imap:/?configName=SUN-UWC-MAIL
&proxyAdminPassword=%5BPROXY-ADMIN_PASSWORD%5D
&subType=sun-one&enableProxyAuth=false...
```

anschließend so aussehen:

```
default|imap:/?configName=SUN-UWC-MAIL
&proxyAdminPassword=%5BPROXY-ADMIN_PASSWORD%5D
&subType=sun-one&enableProxyAuth=false ...
```

- d. Entfernen Sie die Kommas (",") am Ende einer jeden ssoadapter-Meta-Vorlage.
- e. Umbrechen Sie jede ssoadapter-Meta-Vorlage mit einem Anfangs-Tag `<Wert>` und einem End-Tag `</Wert>`.

Beispiel:

```
<Wert>default|imap:/?configName=SUN-UWC-MAIL
&proxyAdminPassword=%5BPROXY-ADMIN_PASSWORD%5D
&subType=sun-one&enableProxyAuth=false ...</Wert>
```

- f. Entfernen Sie die eckige Schließungsklammer ("]") aus der letzten ssoadapter-Meta-Vorlage.
- g. Fügen Sie an das Ende der Datei die folgenden Zeilen an:

```
</AttributeValuePair>
</ModifyDefaultValues>
</SchemaRequests>
</Requests>
```

Die entstandene Datei `ssoadapter-new-templates.xml` für die in den obigen Schritten verwendete Vorlage sollte folgendermaßen aussehen:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE Requests
PUBLIC "-//iPlanet//iDSAME 5.0 Admin CLI DTD//EN"
"jar://com/iplanet/am/admin/cli/amAdmin.dtd"
>
<Anforderungen>
 <SchemaRequests serviceName="SunSSOAdapterService"
 SchemaType="Global">
 <ModifyDefaultValues>
 <AttributeValuePair>
 <Attribute name="sunConfigurationTemplates" />
 <Wert>default|imap:/?configName=SUN-UWC-MAIL
&proxyAdminPassword=%5BPROXY-ADMIN_PASSWORD%5D
&subType=sun-one&enableProxyAuth=false ...</Wert>
 </AttributeValuePair>
 </ModifyDefaultValues>
 </SchemaRequests>
</Requests>
```

4. Importieren Sie die neue Datei `ssoadapter-new-templates.xml`.

```
AccessManager-base/bin/amadmin -u amadminUser -w password -v
-t ssoadapter-new-templates.xml
```

Nun können Sie auf die ssoadapter-Registerkarte in der Portal Server-Konsole zugreifen, um Einblick in die geänderten ssoadapter zu erhalten.

## Aktivieren des URLScrapper-Kanals

Beim Aktualisieren von Release 3 auf Release 5 müssen Sie den URLScrapper-Kanal aktivieren. Siehe auch „[Aktivieren des URLScrapper-Kanals](#)“ auf Seite 368.

## Löschen des Gateway-Diensteintrags

Der Benutzereintrag `amService-srapGateway` muss beim Aktualisieren von Portal Server von Release 2 manuell gelöscht werden, da die Portal Server Secure Remote Access-Gateway-Komponente nach der Aktualisierung ansonsten nicht gestartet werden kann. Führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei der Access Manager-Konsole an.
2. Listen Sie alle Benutzer im Organisations-DN auf.
3. Löschen Sie den Benutzer `amService-srapGateway`.

## Aktualisierung mehrerer Instanzen

Rolling Upgrades mehrerer Instanzen (siehe „[Aktualisierung mehrerer Instanzen](#)“ auf Seite 373) werden bei der Aktualisierung von Portal Server Release 2 auf Release 5 nicht unterstützt.

# Aktualisieren von Portal Server von der Interim Feature Release 7.0

Dieser Abschnitt enthält Informationen zur Aktualisierung von Portal Server von der Interim Feature Release (IFR) 7.0 2005Q4 auf Java ES 5 (Release 5).

In diesem Abschnitt werden folgende Themen behandelt:

- [Portal Server Einführung in die IFR-Aktualisierung](#)
- [Portal Server Aktualisierung von IFR 7.0](#)
- [Aktualisierung mehrerer Instanzen](#)

## Portal Server Einführung in die IFR-Aktualisierung

Berücksichtigen Sie bei der Aktualisierung von Portal Server IFR 7.0 auf Release 5 Portal Server die folgenden Aspekte des Aktualisierungsvorgangs:

- Die Portal Server-IFR wird in Anwendungsserver 7.x nicht unterstützt, daher trifft das Aktualisierungsszenario 5 in [Tabelle 15-4 auf Seite 345](#) nicht zu.
- Das Skript `psupgrade`, das zur Aktualisierung der Portal Server-IFR auf Release 5 verwendet wird, installiert, anders als bei der Aktualisierung von Release 4, keine neuen Pakete. Stattdessen müssen Sie für die Aktualisierung die folgenden Patches anwenden:

**Tabelle 15-8** Patches<sup>1</sup> für die Aktualisierung der Portal Server-IFR auf Release 5

| Beschreibung                        | Patch-ID: Solaris 9 & 10 | Patch-ID: Linux |
|-------------------------------------|--------------------------|-----------------|
| Portal Server 7.1                   | 121465-10 (SPARC)        | 121467-10       |
|                                     | 121466-10 (x86)          |                 |
| Portal Server 7.1<br>-Lokalisierung | 123254-02 (SPARC)        | 123255-02       |
|                                     | 124590-02 (x86)          |                 |

1. Diese Patch-Versionsnummern sind für die Aktualisierung auf Java ES Release 5 mindestens erforderlich. Wenn neuere Versionen verfügbar sind, verwenden Sie anstelle der in dieser Tabelle genannten Versionen die neueren Versionen.

- Das Skript `psupgrade` unterstützt die Aktualisierung der Portal Server-IFR auf Release 5 für Webserver Release 5 nicht. Es stehen zwei Möglichkeiten zur Verfügung:
  - Wenn Webserver bereits auf Release 5 aktualisiert wurde, können Sie die Portal Server-IFR-Software, die im früheren Webserver-Container bereitgestellt wurde, nicht aktualisieren. Daher wird das Webcontainer-Aktualisierungsszenario 2 in [Tabelle 15-6](#) nicht unterstützt.
  - Wenn Webserver *noch nicht* und Access Manager ebenfalls noch nicht auf Release 5 aktualisiert wurde, können Sie zuerst die Portal Server-IFR-Software im früheren Webserver (6.x)-Container und anschließend Webserver (und Access Manager) auf Release 5 aktualisieren. Wenn dies Ihr Aktualisierungsszenario ist, finden Sie weitere Anweisungen unter „[Aktualisierung in Release 5 Webserver \(7.0\) Web Container](#)“ auf Seite 404.

## Portal Server Aktualisierung von IFR 7.0

In diesem Abschnitt wird die Aktualisierung von Portal Server von der IFR auf Java ES Release 5 unter Solaris und Linux beschrieben. Plattformspezifische Vorgänge sind durch die Angabe des jeweiligen Betriebssystems, auf das sich der Vorgang bezieht, gekennzeichnet. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung der IFR 7](#)
- [Aktualisieren der Portal Server-IFR 7.0 \(Solaris\)](#)
- [Aktualisieren der Portal Server-IFR 7 \(Linux\)](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung der IFR 7](#)
- [Aufheben der Aktualisierung \(Solaris\)](#)
- [Aufheben der Aktualisierung \(Linux\)](#)

### Aufgaben vor der Aktualisierung der IFR 7

Die Aufgaben vor der Aktualisierung der IFR 7 sind identisch mit denen für die Aktualisierung von Release 4 upgrade (siehe „[Aufgaben vor der Aktualisierung von Release 4](#)“ auf Seite 349), mit Ausnahme von „[Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)“ auf Seite 351 im Hinblick auf Informationen, die vom Skript `psupgrade` benötigt werden.

Die Portal Server-IFR wird in Anwendungsserver 7.x nicht unterstützt, daher trifft das Webcontainer-Aktualisierungsszenario 5 in [Tabelle 15-6 auf Seite 351](#) nicht zu.

## Aktualisieren der Portal Server-IFR 7.0 (Solaris)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren der Portal Server-IFR haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung der IFR 7 (Solaris)*

Bei der Aktualisierung der Portal Server-IFR auf Java ES Release 5 sind dieselben Aspekte zu berücksichtigen wie bei der Aktualisierung von Release 4 (siehe „[Zu berücksichtigende Aspekte bei der Aktualisierung \(Solaris\)“ auf Seite 355](#)).

Informationen zu aufgetretenen Problemen finden Sie außerdem unter „[Portal Server Einführung in die IFR-Aktualisierung“ auf Seite 392](#).

### *IFR 7-Aktualisierungsverfahren (Solaris)*

Das im Folgenden beschriebene Verfahren ist für Portal Server auf dem Computer anzuwenden, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

`su -`

2. Stoppen Sie etwaige Instanzen von Portal Server Secure Remote Access Gateway, Rewriter-Proxy oder Netlet-Proxy, die möglicherweise lokal ausgeführt werden.

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t gateway -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t rwproxy -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t nlproxy -N gatewayProfileName
```

Überprüfen Sie, ob die Prozesse angehalten wurden. Beispiel:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

3. Vergewissern Sie sich, dass Access Manager ausgeführt wird, wenn es in einem anderen Webcontainer bereitgestellt wird als dem, in dem Portal Server bereitgestellt wird.



4. Starten Sie Portal Server, sofern es nicht bereits ausgeführt wird, indem Sie den Webcontainer starten, in dem es bereitgestellt wird.

Webserver 6.x:

```
WebServer-base/https-instanceName/start
```

Webserver 7.0:

Admin Server--

```
WebServer7Config-base/admin-server/bin/startserv
```

Instance Server--

```
WebServer7Config-base/https-configName/bin/startserv
```

Anwendungsserver 8.x:

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
--password password domainName
```

5. Beziehen Sie den in [Tabelle 15-8 auf Seite 392](#) angegebenen erforderlichen Patch.

Verwenden Sie immer die aktuellste, verfügbare Patch-Revision, es sei denn, Sie werden angewiesen, eine bestimmte Revision zu verwenden.

Patches zum Download in das /tmp-Verzeichnis erhalten Sie unter:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

6. Wenden Sie zunächst den entsprechenden Portal Server-Patch und bei Bedarf das Lokalisierungs-Patch aus [Tabelle 15-8](#) an.

```
patchadd /tmp/patch_ID
```

7. Stellen Sie sicher, dass die Patch-Aktualisierungen erfolgreich durchgeführt wurden:

```
showrev -p | grep patch_ID
```

Die Ausgabe sollte die Versionen der in [Schritt 6](#) angewendeten Patch-IDs zurückgeben.

8. Falls die Lokalisierungs-Patches in [Schritt 6](#) aktualisiert wurden, setzen Sie das Gebietsschema der Portal Server-Konsolen-JVM auf UTF-8.

```
export LC_ALL=ja_JP.UTF-8
```

```
export LANG=ja_JP.UTF-8
```

9. Setzen Sie die zwei Umgebungsvariablen (ANT\_HOME und JAVA\_HOME), die vom Skript psupgrade benötigt werden:

```
export ANT_HOME=/usr/sfw
```

```
export JAVA_HOME=/usr/jdk/entsys-j2se
```

10. Stellen Sie sicher, dass auf Ihrem Computer ausreichend Swap-Speicher zur Verfügung steht.

Der Swap-Speicher sollte grundsätzlich die doppelte Größe des physikalischen RAM aufweisen.

11. Führen Sie das Skript `psupgrade` aus.

```
cd PortalServer7-base/bin
./psupgrade
```

Das `psupgrade`-Skript wird nicht aus der Java ES Release 5-Verteilung ausgeführt und ruft nicht das Java ES-Installationsprogramm auf (auf die Pakete wurden bereits Patches angewendet).

Das Skript weist das System an, Speicherort, Anschlussnummer und weitere Informationen zum Webcontainer zu erkennen, in dem Sie Portal Server-Webanwendungen bereitstellen. Je nach Webcontainer-Aktualisierungsszenario (siehe [Tabelle 15-4 auf Seite 345](#)) fordert das Skript Sie auf, zusätzliche Informationen einzugeben, die für die Bereitstellung von Portal Server für den entsprechenden Webcontainer erforderlich sind.

[Tabelle 15-6 auf Seite 351](#) enthält die Informationen, die für die verschiedenen Webcontainer-Aktualisierungsszenarios in [Tabelle 15-4 auf Seite 345](#) erforderlich sind.

---

**HINWEIS** Achten Sie darauf, die richtigen Werte für die `psupgrade`-Parameter einzugeben, denn Sie können nicht zurückgehen und sie ändern. Des Weiteren ist es sehr schwierig, vom Skript `psupgrade` vorgenommene Änderungen rückgängig zu machen.

---

12. Halten Sie den Webcontainer an und starten Sie ihn erneut.

Ein Neustart des Webcontainers ist zwar nicht in jedem Fall erforderlich, dadurch wird jedoch sichergestellt, dass der Status von Portal Server beim Start eindeutig ist.

## Aktualisieren der Portal Server-IFR 7 (Linux)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Portal Server haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung von IFR 7 (Linux)*

Bei der Aktualisierung der Portal Server-IFR-Software auf Release 5 unter Linux sind dieselben Aspekte wie unter Solaris zu berücksichtigen (siehe „[Zu berücksichtigende Aspekte bei der Aktualisierung der IFR 7 \(Solaris\)](#)“ auf [Seite 394](#)), jedoch werden die vorherigen RPMs bei der Installation der Patches von Release 5 unter Linux entfernt.

### *IFR 7-Aktualisierungsverfahren (Linux)*

Das im Folgenden beschriebene Verfahren ist für Portal Server auf dem Computer anzuwenden, auf dem die Aktualisierung durchgeführt wird.

---

**VORSICHT** Eine Aktualisierung der Portal Server-IFR auf Release 5 unter Linux kann nicht rückgängig gemacht werden. Stellen Sie sicher, dass Sie Ihr System sicher, *bevor* Sie das folgende Verfahren durchführen.

---

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Stoppen Sie etwaige Instanzen von Portal Server Secure Remote Access Gateway, Rewriter-Proxy oder Netlet-Proxy, die möglicherweise lokal ausgeführt werden.

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t gateway -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t rwproxy -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t nlproxy -N gatewayProfileName
```

Überprüfen Sie, ob die Prozesse angehalten wurden. Beispiel:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

3. Vergewissern Sie sich, dass Access Manager ausgeführt wird, wenn es in einem anderen Webcontainer bereitgestellt wird als dem, in dem Portal Server bereitgestellt wird.
4. Starten Sie Portal Server, sofern es nicht bereits ausgeführt wird, indem Sie den Webcontainer starten, in dem es bereitgestellt wird.

Webserver 6.x:

```
WebServer-base/https-instanceName/start
```

Webserver 7.0:

Admin Server--

*WebServer7Config-base/admin-server/bin/startserv*

Instance Server--

*WebServer7Config-base/https-configName/bin/startserv*

Anwendungsserver 8.x:

*AppServer8-base/bin/asadmin start-domain --user admin\_ID*

*--password password domainName*

5. Der erforderliche Patch lässt sich anhand der entsprechenden Patch-Nummern und RPM-Namen aus [Tabelle 15-8 auf Seite 392](#) entnehmen.

Verwenden Sie immer die aktuellste, verfügbare Patch-Revision, es sei denn, Sie werden angewiesen, eine bestimmte Revision zu verwenden.

Patches zum Download in das /tmp-Verzeichnis erhalten Sie unter:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

6. Wenden Sie zunächst den Portal Server-Patch und anschließend bei Bedarf die Lokalisierungs-RPMs für Portal Server aus [Tabelle 15-8 auf Seite 392](#) an.

Lesen Sie die Readme-Datei zum Portal Server-Patch; hierin ist beschrieben, wie Sie ein Skript zur Anwendung der RPMs des Patch verwenden:

```
cd /tmp
```

Dabei ist /tmp das Verzeichnis, in das Sie den Patch herunterladen.

```
./upgradeportalrpm
```

Das Aktualisierungsskript installiert die RPMs.

Installieren Sie die einzelnen RPMs für das Lokalisierungs-Patch mit folgendem Befehl:

```
rpm -Fvh patchName-version.rpm
```

7. Stellen Sie sicher, dass die Patch-Aktualisierung erfolgreich durchgeführt wurde:

```
rpm -qa | grep sun-portal
```

Die Aktualisierungs-Revisionsnummern der RPMs sollten zurückgegeben werden.

8. Falls die Lokalisierungs-Patches in [Schritt 6](#) aktualisiert wurden, setzen Sie das Gebietsschema der Portal Server-Konsolen-JVM auf UTF-8.

```
export LC_ALL=ja_JP.UTF-8
export LANG=ja_JP.UTF-8
```

9. Setzen Sie die zwei Umgebungsvariablen (ANT\_HOME und JAVA\_HOME), die vom Skript psupgrade benötigt werden:

```
export ANT_HOME=/opt/sun
export JAVA_HOME=/usr/jdk/entsys-j2se
```

10. Stellen Sie sicher, dass auf Ihrem Computer ausreichend Swap-Speicher zur Verfügung steht.

Der Swap-Speicher sollte grundsätzlich die doppelte Größe des physikalischen RAM aufweisen.

11. Führen Sie das Skript psupgrade aus.

```
cd PortalServer7-base/bin
./psupgrade
```

Das psupgrade-Skript wird nicht aus der Java ES Release 5-Verteilung ausgeführt und ruft nicht das Java ES-Installationsprogramm auf (auf die Pakete wurden bereits Patches angewendet).

Das Skript weist das System an, Speicherort, Anschlussnummer und weitere Informationen zum Webcontainer zu erkennen, in dem Sie Portal Server-Webanwendungen bereitstellen. Je nach Webcontainer-Aktualisierungsszenario (siehe [Tabelle 15-4 auf Seite 345](#)) fordert das Skript Sie auf, zusätzliche Informationen einzugeben, die für die Bereitstellung von Portal Server für den entsprechenden Webcontainer erforderlich sind.

[Tabelle 15-6 auf Seite 351](#) enthält die Informationen, die für die verschiedenen Webcontainer-Aktualisierungsszenarien in [Tabelle 15-4 auf Seite 345](#) erforderlich sind.

---

**HINWEIS** Achten Sie darauf, die richtigen Werte für die psupgrade-Parameter einzugeben, denn Sie können nicht zurückgehen und sie ändern. Des Weiteren ist es sehr schwierig, vom Skript psupgrade vorgenommene Änderungen rückgängig zu machen.

---

**12. Halten Sie den Webcontainer an und starten Sie ihn erneut.**

Ein Neustart des Webcontainers ist zwar nicht in jedem Fall erforderlich, dadurch wird jedoch sichergestellt, dass der Status von Portal Server beim Start eindeutig ist.

## Überprüfen der Aktualisierung

Sie können die Anwendung der Patches der Portal Server-Pakete von Release 5 mithilfe des folgenden Befehls überprüfen:

```
PortalServer7-base/bin/psadmin --version --adminuser admin_ID
-f adminpasswordfile.
```

Ausgabewerte finden Sie in [Tabelle 15-5 auf Seite 349](#).

Zur Überprüfung der gesamten Aktualisierung vergewissern Sie sich, dass der Portal-Desktop angezeigt wird und das Administrationsprogramm psadmin wie dokumentiert funktioniert.

Sie können im Verzeichnis `/var/sadm/install/logs` auch die folgenden Aktualisierungs-Protokolldateien überprüfen:

- `Sun_Java_System_Portal_Server_upgrade.log`
- `Sun_Java_System_Portal_Server_upgrade.log_ant_xxx.log`  
wobei `xxx` `preupgrade`, `upgrade` oder `postupgrade` sein kann.

## Aufgaben nach der Aktualisierung der IFR 7

Bei der Aktualisierung von Portal Server von der IFR 7 auf Release 5 müssen Sie folgende Verfahren nach der Aktualisierung für die folgenden Situationen durchführen:

- [Konfiguration von Common Agent Container](#)
- [Aktivieren des Java ES Monitoring Framework](#)
- [Aktualisierung im Anwendungsserver-Webcontainer](#)
- [Aktualisierung in Release 5 Webserver \(7.0\) Web Container](#)
- [Erneutes Bereitstellen von benutzerdefinierten Portlet-Anwendungen](#)
- [Migrieren von benutzerdefinierten Portlet-Anwendungen](#)
- [Manuelle Migration von Struts-basierten Portlets](#)

## Konfiguration von Common Agent Container

Common Agent Container ist eine gemeinsam genutzte Komponente, die Containerdienste für Java ES-Überwachungs- und Administrationsagenten bietet. Portal Server-Administrationstools wie die Portal Server-Konsole und die Befehlszeilenschnittstelle `psadmin` verwenden eine Reihe von Überwachungs- und Administrationsagenten, zusammengefasst Portal Administration Server genannt, die in Common Agent Container bereitgestellt werden.

Wenn gemeinsam genutzte Java ES-Komponenten vor der Aktualisierung der Portal Server-IFR 7.0 auf Release 5 aktualisiert wurden, müssen Sie die folgenden zusätzlichen Schritte durchführen, um sich bei der Portal Server Release 5-Konsole anzumelden und die Befehlszeilenschnittstelle `psadmin` zu verwenden. (Wenn gemeinsam genutzte Java ES-Komponenten *nicht* vor der Aktualisierung der Portal Server-IFR 7.0 auf Release 5 aktualisiert wurden, können Sie die folgenden zusätzlichen Schritte ignorieren.)

1. Konfigurieren Sie Common Agent Container neu.

`PortalServer7-base/bin/psconfig PortalServer7-base/samples/example2.xml`

Die Datei `example2.xml` enthält Informationen zur Neukonfiguration. Sie müssen zuerst die Datei `example2.xml` bearbeiten, um die erforderlichen Passwörter anzugeben, bevor Sie den Befehl `psconfig` ausführen. Wenn Sie keine Standard-Speicherorte für Portal Server verwenden, müssen Sie auch die richtigen Verzeichnisse angeben.

2. Bearbeiten Sie den classpath des Webcontainers so, dass er auf Common Agent Container verweist.

Der classpath des Webcontainers enthält einen Verweis auf den Speicherort der früheren Common Agent Container-Version:  
(`rel4CAC-base-dir/lib/cacao_cacao.jar`).

Ersetzen Sie diesen Verweis durch den Speicherort von Release 5:  
(`rel5CAC-admin-dir/lib/cacao_cacao.jar`).

3. Erstellen Sie im Verzeichnis `PortalServer7Config-base` eine Eigenschaftsdatei `pasconnect.properties` mit dem folgenden Eigenschafts-Wertepaar:

`pas.host=.`

4. Starten Sie Common Agent Container neu.

```
rel5CAC-admin-dir/bin/cacaoadm start
```

### ***Aktivieren des Java ES Monitoring Framework***

Durch Aktivieren des Java ES Monitoring Framework (gemeinsam genutzte MFWK-Komponenten) werden Portal Server-Administrationstools wie die Portal Server-Konsole und die Befehlszeilenschnittstelle psadmin angewiesen, Metriken wie z. B. die Anzahl der Besucher und die von ihnen besuchten Portale zu protokollieren. So aktivieren Sie MFWK:

1. Suchen Sie die folgenden beiden Dateien:

```
MFWK-base/template/jesmf/desktopmfwk.properties
MFWK-base/template/jesmf/com.sun.cmm.ps.xml
```

wobei *MFWK-base* dem folgenden Pfad entspricht:

```
/opt/SUNWmfwk (Solaris)
/opt/sun/mfwk (Linux)
```

2. Kopieren Sie die beiden Dateien in das folgende Verzeichnis:

```
PortalServer7Data-base/portals/portal_ID/config/Portal_Instance/
```

3. Ersetzen Sie in der Datei desktopmfwk.properties

```
com.sun.portal.ProductCollectionId=%PS_DIR%
mit
```

```
com.sun.portal.ProductCollectionId=Portal_Installed_Location
```

4. Fügen Sie die folgenden beiden JAR-Dateien:

```
MFWK-base/lib/mfwk_instrum_tk.jar
MFWK-base/lib/mfwk_agent.jar
```

dem classpath des entsprechenden Containers hinzu (Datei `server.xml` für Webserver und `domain.xml` für Anwendungsserver).

5. Starten Sie den entsprechenden Webcontainer neu.

### ***Aktualisierung im Anwendungsserver-Webcontainer***

Wenn Portal Server in einem Anwendungsserver-Webcontainer bereitgestellt wird, müssen Sie das folgende zusätzliche Verfahren durchführen, um Portal Server erfolgreich erneut bereitzustellen:



1. Suchen Sie den Abschnitt, in dem die psconsole-Einstellungen in der Datei *AppServer8Config-base/domains/domainName/config/server.policy* definiert sind:

2. Fügen Sie an das Ende des Abschnitts die folgende Zeile an:

```
permission java.lang.RuntimePermission „getProtectionDomain“
```

3. Stellen Sie die Datei *portal.war* erneut bereit.

```
PortalServer7-base/bin psadmin redeploy -p portal_ID
```

4. Starten Sie die Anwendungsserver-Instanz neu.

```
AppServer8-base/bin/asadmin start-domain --user admin_ID
--password passworddomainName
```

```
AppServer8-base/bin/asadmin start-node-agent --user admin_ID
--password password nodeagentName
```

wobei *nodeagentName* der Form *hostName\_domainName* entspricht, jedoch standardmäßig nur *hostName* lautet.

### *Verbindungen bleiben im Anwendungsserver-Webcontainer hängen*

Wenn der aktualisierte Portal Server in einem Anwendungsserver-Webcontainer bereitgestellt wird, kann es vorkommen, dass die Portalanwendungen beim Warten auf Java DB-Verbindungen hängenbleiben. Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

1. Entfernen Sie die Einstellungen in *PortalServer7Data-base/derby/derby.properties* zu den folgenden beiden Parametern:

```
derby.drda.maxThreads
derby.drda.timeslice
```

2. Starten Sie Java DB neu.

```
ANT_HOME/bin/ant
-DPS_CONFIG=PortalServer7Config-base/PSConfig.properties
-buildfile PortalServer7-base/lib/derby.xml
[stop-instance|start-instance]
```

wobei *ANT\_HOME* */usr/sfw* (unter Solaris) und */opt/sun* (unter Linux) entspricht.

3. Ändern Sie die Java DB-Konfigurationseinstellungen für Anwendungsserver.

Ändern Sie mithilfe der Anwendungsserver-Konsole die Attributwerte zu den folgenden Verbindungspool-Ressourcen: `communitymcPool`, `FileSharingDBPool`, `PointBasePool`, `SurveyDBPool`.

Ändern Sie die folgenden Attributwerte wie folgt:

```
Idle Timeout in 300 oder mehr
Resource Type in javax.sql.ConnectionPoolDataSource
Datasource classname in
 org.apache.derby.jdbc.ClientConnectionPoolDataSource
```

4. Starten Sie die Anwendungsserver-Instanz neu, in der Portal Server bereitgestellt wird.

### *Aktualisierung in Release 5 Webserver (7.0) Web Container*

Wenn Sie die Portal Server-IFR in einem Webserver aktualisiert haben, der *noch nicht* auf Release 5 aktualisiert wurde, weil das Skript `psupgrade` die Aktualisierung der Portal Server-IFR in Webserver Release 5 nicht unterstützt (siehe „[Portal Server Einführung in die IFR-Aktualisierung](#)“ auf Seite 392), müssen Sie die folgenden zusätzlichen Verfahren nach der Aktualisierung durchführen:

1. Aktualisieren Sie Webserver (und Access Manager) auf Release 5.
2. Konfigurieren Sie Common Agent Container neu.

Gehen Sie wie unter „[Konfiguration von Common Agent Container](#)“ auf Seite 401 beschrieben vor.

3. Konfigurieren Sie die von der Portal Server-Konsole benötigten Webserver-Containerwerte und die Befehlszeilenschnittstelle `psadmin` neu.

- a. Öffnen Sie einen LDAP-Browser.

Die Konfigurationswerte werden in Directory Server gespeichert.

- b. Suchen Sie unter DN nach:  
`sunPortalAdminPortalDomainID=defaultDomain`  
`->sunPortalAdminPortalDomainPortalID=portal1`  
`->sunPortalAdminPortalDomainPortalServerInstanceIn=host-port`

- c. Bearbeiten Sie Werte wie `InstallDir`, `WebContainerInstanceDir`, `WebContainerType`, `DocRoot` und andere Parameter in [Tabelle 15-6 auf Seite 351](#) so, dass sie den Werten in Webserver Release 5 (7.0) entsprechen.

#### 4. Erstellen Sie eine Portal Server Release 5-Instanz.

```
PortalServer7-base/bin/psadmin create-instance newInstance_ID
```

Wenn der Wert von *newInstance\_ID* bereits vorhanden ist, wird ein Fehler ausgegeben, daher ist es von Vorteil, diesen Schritt vor dem nachstehenden [Schritt 5](#) durchzuführen.

#### 5. Löschen Sie die Portal Server-IFR-Instanz.

```
PortalServer7-base/bin/psadmin delete-instance oldInstance_ID
```

#### *Erneutes Bereitstellen von benutzerdefinierten Portlet-Anwendungen*

Wenn Sie benutzerdefinierte Portlet-Anwendungen erstellt und bereitgestellt haben, müssen diese Portlets Portal Server Release 5 nach der Aktualisierung manuell erneut bereitgestellt werden. Zwar sind Anzeige-Profileinträge vorhanden und der Kanalname wird angezeigt, der Inhalt ist jedoch erst zu sehen, nachdem Sie die benutzerdefinierten Portlets erneut bereitgestellt haben.

Stellen Sie die Portlets mit dem folgenden Befehl erneut bereit:

```
PortalServer7-base/bin/psadmin deploy-portlet
```

Sie können die erneute Bereitstellung überprüfen, indem Sie die entsprechenden .war- und XML-Dateien im folgenden Verzeichnis suchen:

```
PortalServer7Data-base/portals/Upgraded/war
```

#### *Migrieren von benutzerdefinierten Portlet-Anwendungen*

Portlet-Anwendungen, die auf dem von Sun Java Web Console (SJWC) gelieferten Benutzerschnittstellen-Framework basieren, müssen manuell in Release 5 migriert und erneut bereitgestellt werden.

Diese Anforderung betrifft insbesondere vier Webanwendungen, die mit Portal Server als Beispiel-Portlet-Anwendungen verteilt werden, welche dazu gedacht sind, angepasst und in einem Portal installiert zu werden: *filesharing*, *surveys*, *wiki*, *rssportlet*. Bei der Aktualisierung werden fehlerkorrigierte Versionen dieser Beispiel-Portlet-Anwendungen im Bereich der Portlet-Anwendungen auf dem Datenträger platziert. Wenn Sie diese Portlet-Anwendungen für Ihren Gebrauch angepasst haben, müssen Sie sie manuell in Release 5 migrieren und erneut bereitstellen; sie werden nicht vom Portal Server-Aktualisierungsprozess erfasst.

Standardmäßig werden einige dieser Portlet-Anwendungen (*filesharing* und *surveys*) bereitgestellt und dem Benutzer zugänglich gemacht, wenn eine Community erstellt wird.

Sie können SJWC-basierende Portlet-Anwendungen folgendermaßen aktualisieren, anpassen und erneut bereitstellen. Die Portlet-Anwendung `filesharing` dient hierbei als Beispiel:

1. Extrahieren Sie die SJWC-JAR-Dateien von Release 5.
  - a. `mkdir /tmp/lh`
  - b. `cd /tmp/lh`
  - c. `/usr/jdk/entsys-j2se/bin/jar xvf`  
`PortalServer7-base/portlet/communityportlets.war`  
`WEB-INF/lib/commons-beanutils.jar`  
`WEB-INF/lib/commons-collections-3.1.jar`  
`WEB-INF/lib/commons-digester.jar`  
`WEB-INF/lib/commons-logging.jar`  
`WEB-INF/lib/dataprovider.jar` `WEB-INF/lib/jsf-api.jar`  
`WEB-INF/lib/jsf-impl.jar` `WEB-INF/lib/webui.jar`
  - d. Benennen Sie eine dieser Dateien um.  
`mv WEB-INF/lib/commons-collections-3.1.jar`  
`WEB-INF/lib/commons-collections.jar`
2. Suchen Sie die Portlet-Anwendung `filesharing`.  
`cd PortalServer7Config-base/portals/portal1/portletapps/filesharing`
3. Geben Sie die aktualisierten SJWC-Bibliotheken ein.  
`jar uvf src/filesharing.war.tokenized -C /tmp/lh WEB-INF`
4. Passen Sie die Portlet-Anwendung `filesharing` an.  
`ant customize`
5. Stellen Sie die Portlet-Anwendung `filesharing` erneut bereit.
  - a. `PortalServer7-base/bin/psadmin undeploy-portlet -u amadmin`  
`-f passwordfile -p portal_id -i instance_id -g filesharing`
  - b. `ant deploy`

- c. Gehen Sie zum folgenden Verzeichnis (je nach Webcontainer):

*Anwendungsserver 8.x:*

*AppServer8Config-base/domains/domain1/applications/j2ee-modules/  
communityportlets/WEB-INF*

*Webserver 6.x:*

*WebServer6-base/https-instanceName/webapps/https-instanceName/  
communityportlets/WEB-INF*

*Webserver 7.x:*

*WebServer7Config-base/https-configName/web-app/https-configName/  
communityportlets/WEB-INF*

- d. Öffnen Sie die Datei `sun-web.xml` und fügen Sie unmittelbar vor der letzten Zeile (d. h. vor dem End-Tag `sun-web-app`) die folgende Zeile hinzu:

```
<class-loader delegate="false"/>
```

- e. Wiederholen Sie [Schritt c](#) und [Schritt d](#) für die Datei `sun-web.xml` unter `filesharing/WEB-INF`.
6. Wiederholen Sie [Schritt 2](#) bis [Schritt 5](#) für surveys und alle weiteren auf dem SJWC-Framework basierenden benutzerdefinierten Portlet-Anwendungen.
7. Starten Sie den Webcontainer neu.

### *Manuelle Migration von Struts-basierten Portlets*

Wenn Sie über benutzerdefinierte Portlets verfügen, die auf dem Struts-Framework basierende Codes verwenden, müssen diese Portlets manuell aktualisiert werden, damit die in Portal Server Release 5 enthaltene Datei `struts.jar` verwendet werden kann. Gehen Sie folgendermaßen vor:

1. Heben Sie die Bereitstellung der Struts-basierten Portlet-Anwendung auf.
2. Aktualisieren Sie die war-Datei mit der richtigen Version der Datei `struts.jar`.

Kopieren Sie *PortalServer7-base/lib/struts.jar* in *strutsbasedPortlet/WEB-INF/lib/struts.jar*

wobei *strutsbasedPortlet* dem Verzeichnis entspricht, in dem sich die Struts-basierten Portlet-Dateien befinden.

3. Erstellen Sie ein .war-Archiv des Verzeichnisses *strutsbasedPortlet*.
4. Stellen Sie die Portlet-Anwendung erneut bereit.

*PortalServer7-base/bin psadmin deploy-portlet*

## Aufheben der Aktualisierung (Solaris)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Verfahren zum Aufheben der Aktualisierung Portal Server haben, sowie eine Beschreibung des eigentlichen Verfahrens zum Aufheben der Aktualisierung.

### *Zu berücksichtigende Aspekte beim Aufheben der Aktualisierung (Solaris)*

Beim Aufheben der Aktualisierung auf Release 5 wird die IFR-Installation in *PortalServer6-base* wiederhergestellt und die Webanwendungen der IFR werden erneut bereitgestellt.

### *Verfahren zum Aufheben der Aktualisierung (Solaris)*

1. Melden Sie sich als Root oder Superuser an.

`su -`

2. Stellen Sie den Zustand von Directory Server vor der Aktualisierung wieder her.

Verwenden Sie die Directory Server-Sicherungs-/Wiederherstellungs-Befehlszeile und die GUI-Programme. Lesen Sie hierzu das Kapitel "Directory Server Backup and Restore" im *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*, <http://docs.sun.com/doc/819-0995>.

3. Heben Sie die Bereitstellung der Webanwendungen in Portal Server Release 5 auf, die während der Aktualisierung auf Release 5 erneut bereitgestellt wurden.

Verwenden Sie die Administrationsprogramme des Webcontainers (Befehlszeile oder Konsole) zum Aufheben der Bereitstellung der folgenden Pakete:

```
portal
psconsole
search1
wsssoportlet
guessnumber
portletsamples
```

4. Beenden Sie Portal Server, indem Sie seinen Webcontainer beenden.

Webserver 6.x:

*WebServer-base/https-instanceName/stop*

Webserver 7.0:

Admin Server--

*WebServer7Config-base/admin-server/bin/stopserv*

Instance Server--

*WebServer7Config-base/https-configName/bin/stopserv*

Anwendungsserver 8.x:

*AppServer8-base/bin/asadmin stop-domain --user admin\_ID  
--password password domainName*

5. Heben Sie das Portal Server 7.1-Patch aus [Tabelle 15-8](#) auf.

*patchrm patch\_ID*

6. Starten Sie Portal Server neu, indem Sie seinen Webcontainer neu starten.

Webserver 6.x:

*WebServer-base/https-instanceName/start*

Webserver 7.0:

Admin Server--

*WebServer7Config-base/admin-server/bin/startserv*

Instance Server--

*WebServer7Config-base/https-configName/bin/startserv*

Anwendungsserver 8.x:

*AppServer8-base/bin/asadmin start-domain --user admin\_ID  
--password password domainName*

7. Stellen Sie die Portal Server-IFR-Webanwendungen mithilfe der folgenden Befehle erneut bereit:

```
cd PortalServer7-base/bin
./psupgrade rollback
```

wobei *os\_arch* der Plattform entspricht, wie z. B. *Solaris\_sparc*.

Mit dem Befehl `psupgrade rollback` wird die Bereitstellung der Webanwendungen von Portal Server Release 5 aufgehoben und die Webanwendungen der Portal Server-IFR werden erneut bereitgestellt.

Mit dem Befehl wird der Inhalt aus *PortalServer7-base/web-src* erneut in */var/PortalServer7-base/https-hostName/deploy-dir/web-apps* bereitgestellt. Anpassungen der Portal Server-Webanwendung sollten daher zuerst in */web-src* vorgenommen und anschließend in */web-apps* bereitgestellt werden. Änderungen, die Sie unter */web-apps* vornehmen, sollten in */web-src* repliziert werden, *bevor* Sie den `deploy`-Befehl ausführen. Andernfalls werden diese Änderungen überschrieben.

8. Halten Sie den Webcontainer an und starten Sie ihn erneut.

Ein Neustart des Webcontainers ist zwar nicht in jedem Fall erforderlich, dadurch wird jedoch sichergestellt, dass der Status von Portal Server beim Start eindeutig ist.

## Aufheben der Aktualisierung (Linux)

Da für das Aktualisieren auf Release 5 die Binärdateien der IFR-RPMs entfernt werden müssen, gestaltet sich das Aufheben der Aktualisierung unter Linux sehr schwierig.

Eine Möglichkeit zum Aufheben der Aktualisierung besteht darin, *vor* der Aktualisierung ein paralleles System zu erstellen und dieses System vor der Aktualisierung zu testen. Wenn Sie die Aktualisierung aufheben müssen, können Sie zu diesem parallelen System zurückkehren.

## Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen wird Portal Server auf mehreren Computersystemen bereitgestellt, um die Skalierbarkeit zu gewährleisten und die Verfügbarkeit zu verbessern. Möglicherweise führen Sie beispielsweise Portal Server-Komponenten auf mehreren Computern zusammen mit einem Lastenausgleichsprogramm aus, um die Last zu verteilen.



Für Portal Server-Instanzen mit Lastenausgleich können Sie ein sogenanntes Rolling Upgrade durchführen, bei dem Sie alle Portal Server-Instanzen nacheinander aktualisieren, ohne den Dienst zu unterbrechen. Dabei werden die verschiedenen Portal Server-Instanzen einzeln aktualisiert, während die übrigen Instanzen weiter ausgeführt werden. Zur Durchführung eines Rolling Upgrade von der IFR auf Release 5 gehen Sie wie unter „[Aktualisierung mehrerer Instanzen](#)“ auf Seite 373 beschrieben vor. Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch die IFR.



# Portal Server Secure Remote Access

In diesem Kapitel wird die Aktualisierung von Portal Server Secure Remote Access auf Java ES 5 (Release 5) beschrieben: Sun Java System Portal Server Secure Remote Access 7.1.

Das Kapitel enthält einen Überblick über die Aspekte der verschiedenen Aktualisierungswege, die von Release 5 unterstützt werden. Es wird sowohl die Aktualisierung unter dem Solaris- als auch unter dem Linux-Betriebssystem berücksichtigt:

- „Überblick über Aktualisierungen von Portal Server Secure Remote Access“ auf Seite 415
- „Aktualisieren von Portal Server Secure Remote Access von Java ES Release 4“ auf Seite 420
- „Aktualisieren von Portal Server Secure Remote Access von Java ES Release 3“ auf Seite 441
- „Aktualisieren von Portal Server Secure Remote Access von Java ES Release 2“ auf Seite 443
- „Aktualisieren von Portal Server Secure Remote Access von Interim Feature Release 7.0“ auf Seite 446

---

**HINWEIS** Die in diesem Kapitel angegebenen Speicherorte von Dateien beziehen sich auf die Verzeichnispfade, die im Folgenden als *PortalServer6-base* and *PortalServer6Config-base* (Portal Server 6.x) und *PortalServer7-base* and *PortalServer7Config-base* (Portal Server 7.x) angegeben werden. Wenn Portal Server erstmalig installiert wurde, wurden diese Pfade mindestens teilweise als Installationsverzeichnis angegeben. Wenn nicht, wurde vom Java ES-Installationsprogramm ein Standardwert zugewiesen.

Die Standardwerte für diese Verzeichnispfade sind in der folgenden Tabelle aufgelistet.

---

**Tabelle 16-1** Portal Server Secure Remote Access Verzeichnispfade

| Variable des Pfadnamens         | Solaris OS          | Linux OS            |
|---------------------------------|---------------------|---------------------|
| <i>PortalServer6-base</i>       | /opt/SUNWps         | /opt/sun/portal     |
| <i>PortalServer6Config-base</i> | /etc/opt/SUNWps     | /etc/opt/sun/portal |
| <i>PortalServer6Data-base</i>   | /var/opt/SUNWps     | /var/opt/sun/portal |
| <i>ortalServer7-base</i>        | /opt/SUNWportal     | /opt/sun/portal     |
| <i>PortalServer7Config-base</i> | /etc/opt/SUNWportal | /etc/opt/sun/portal |
| <i>PortalServer7Data-base</i>   | /var/opt/SUNWportal | /var/opt/sun/portal |

# Überblick über Aktualisierungen von Portal Server Secure Remote Access

In diesem Abschnitt werden die folgenden allgemeinen Aspekte bezüglich der Aktualisierung von Portal Server Secure Remote Access auf Java ES 5 (Release 5) beschrieben:

- [Über Java ES Release 5 Portal Server Secure Remote Access](#)
- [Wegweiser für die Aktualisierung von Portal Server Secure Remote Access](#)
- [Portal Server Secure Remote Access-Daten](#)
- [Vorgehensweise zur Aktualisierung von Portal Server Secure Remote Access](#)

## Über Java ES Release 5 Portal Server Secure Remote Access

Portal Server Secure Remote Access (bestehend aus Gateway-, Rewriter Proxy- und Netlet Proxy-Komponenten) ist zwar eng mit Portal Server verbunden, wird jedoch üblicherweise auf Computern bereitgestellt, die nicht als Host für Portal Server dienen. Portal Server Secure Remote Access-Komponenten verwenden dieselbe Verwaltungsinfrastruktur wie Portal Server und interagieren mit Servlets und Applets, die sich auf dem Computer befinden, der als Host für Portal Server dient.

Java ES Release 5 Portal Server Secure Remote Access stellt in Bezug auf Release 4 ein größeres Release dar und zahlreiche neue Erweiterungen und Funktionen. Viele der Änderungen wurden in einem vorläufigen Release (Interim Feature Release, IFR) vorgenommen, das nach Release 4 eingeführt wurde. Release 5 enthält in Bezug auf das IFR nur kleine Funktionsänderungen. Weitere Informationen über Erweiterungen und neue Funktionen des IFR finden Sie in den *Sun Java System Portal Server 7.1 Release Notes* (<http://docs.sun.com/doc/820-0901/6n4l3f365?a=view>). Insbesondere wurde die Release 4-Befehlszeilenschnittstelle für die Verwaltung durch den Befehl `psadmin` ersetzt.

# Wegweiser für die Aktualisierung von Portal Server Secure Remote Access

Tabelle 16-2 zeigt die unterstützten Wege für die Aktualisierung von Portal Server Secure Remote Access auf Java ES Release 5. Die Tabelle gilt sowohl für das Solaris- als auch für das Linux-Betriebssystem.

**Tabelle 16-2** Wege für die Aktualisierung auf Java ES 5 (Release 5): Portal Server Secure Remote Access 7.1

| Java ES Release               | Portal Server Secure Remote Access Version                        | Allgemeiner Ansatz                                                                                                                                      | Neukonfiguration erforderlich |
|-------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Interim Feature Release (IFR) | Sun Java System Portal Server Secure Remote Access IFR 7.0 2005Q4 | Direkte Aktualisierung:<br>Durch Anwendung von Patches und anschließender Verwendung eines Aktualisierungsskripts.                                      | Keine.                        |
| Release 4                     | Sun Java System Portal Server Secure Remote Access 6.3.1 2005Q4   | Direkte Aktualisierung:<br>Durch Anwendung eines Aktualisierungsskripts.                                                                                | Keine.                        |
| Release 3                     | Sun Java System Portal Server Secure Remote Access 6.3.1 2005Q1   | Direkte Aktualisierung:<br>Durch Anwendung eines Aktualisierungsskripts.                                                                                | Keine.                        |
| Release 2                     | Sun Java System Portal Server Secure Remote Access 6.3 2004Q2     | Direkte Aktualisierung:<br>Durch Anwendung eines Aktualisierungsskripts.                                                                                | Keine.                        |
| Release 1                     | Sun ONE Portal Server Secure Remote Access 6.2 (2003Q4)           | Keine direkte Aktualisierung:<br>Kann jedoch durch Aktualisierung auf Release 3 und anschließender Aktualisierung von Release 3 auf Release 5 erfolgen. | Konfigurationsdaten           |
| Versionen vor Java ES         |                                                                   | Keine direkte Aktualisierung.                                                                                                                           |                               |

## Portal Server Secure Remote Access-Daten

Die folgende Tabelle enthält die Datentypen, die von einer Aktualisierung der Portal Server Secure Remote Access-Software betroffen sein können.

**Tabelle 16-3** Portal Server Secure Remote Access Verwendung der Daten

| Datentyp                                                  | Standort                         | Verwendung                                                                                                                                                           |
|-----------------------------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Konfigurationsdaten                                       | <i>PortalServer6Config-base/</i> | Konfiguration von Portal Server Secure Remote Access.                                                                                                                |
| Directory-Schema<br>Dienstekonfiguration<br>Benutzerdaten | Directory Server                 | Portal Server Secure Remote Access hängt von Dienstkonfigurationen ab (z. B. Portal-Desktop) und von Benutzerprofildaten, die in einem Verzeichnis gespeichert sind. |
| Dynamische Anwendungsdaten                                | Keine                            | Anwendungsdaten, wie beispielsweise zum Sitzungsstatus, werden von Portal Server Secure Remote Access nicht dauerhaft gespeichert.                                   |

## Vorgehensweise zur Aktualisierung von Portal Server Secure Remote Access

Die Vorgehensweise zur Aktualisierung von Portal Server Secure Remote Access hängt im Grunde von den verschiedenen Aspekten ab, die in [Kapitel 1, „Planung hinsichtlich der Aktualisierungen“](#) besprochen wurden: Aktualisierungsweg, Abhängigkeiten zwischen den Java ES-Komponenten, selektive Aktualisierung im Vergleich zur Aktualisierung aller Komponenten, Bereitstellung mehrerer Instanzen usw.

In diesem Abschnitt wird im Detail auf Portal Server Secure Remote Access eingegangen, indem Themen besprochen werden, die Ihre Aktualisierungspläne von Portal Server Secure Remote Access beeinflussen können.

### Kompatibilität

Portal Server Secure Remote Access Release 5 führt Änderungen für öffentliche Schnittstellen im Befehl `psadmin` ein, der zum Starten und Anhalten der Gateway-, Rewriter Proxy- und Netlet Proxy-Komponenten verwendet wird. Weitere Informationen finden Sie in *Sun Java System Portal Server 7.1 Command-Line Reference* (<http://docs.sun.com/doc/819-5030>).

Einzelne Portal Server Secure Remote Access-Komponenten (einschließlich Gateway, Rewriter Proxy und Netlet Proxy) sind nicht rückwärts kompatibel mit früheren Versionen. Sämtliche dieser Komponenten müssen zusammen mit Portal Server selbst auf Java ES Release 5 synchronisiert werden. Diese Anforderung gilt sowohl für lokale als auch für verteilte Portal Server Secure Remote Access-Komponenten.

Des Weiteren besteht eine Inkompatibilität zwischen den Directory Server-Datenstrukturen, die von Portal Server in Release 5 und früheren Portal Server-Versionen verwendet werden. Diese Inkompatibilität hat Auswirkung auf die parallele Aktualisierung mehrerer Portal Server-Instanzen mit denselben Directory Server-Daten.

## Portal Server Secure Remote Access-Abhängigkeiten

Portal Server Secure Remote Access ist eng mit Portal Server verbunden. Es hängt von der Software ab, die in Portal Server enthalten ist, und wird auf demselben Computer wie Portal Server ausgeführt.

Portal Server Secure Remote Access hängt jedoch auch von anderen Java ES-Komponenten ab. Diese Abhängigkeiten beeinflussen möglicherweise das Verfahren für die Aktualisierung und Neukonfiguration der Portal Server Secure Remote Access-Software. Änderungen der Portal Server Secure Remote Access-Schnittstellen oder -Funktionen könnten beispielsweise eine aktualisierte Version der Komponenten erforderlich machen, von denen Portal Server Secure Remote Access abhängig ist. Welche dieser Komponenten aktualisiert werden müssen, hängt von dem jeweiligen Aktualisierungsweg ab.

Für Portal Server Secure Remote Access-Komponenten bestehen Abhängigkeiten zu folgenden Java ES-Komponenten:

- **Gemeinsam genutzte Komponenten.** Portal Server Secure Remote Access-Komponenten sind von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)).
- **Für Portal Server** Portal Server Secure Remote Access-Komponenten besteht eine zwingende Abhängigkeit zu Portal Server, einschließlich lokaler Komponenten, die für die Unterstützung der Portal Server Secure Remote Access-Funktionen erforderlich sind.
- **Access Manager (oder Access Manager SDK).** Für Portal Server Secure Remote Access besteht eine zwingende Abhängigkeit zu Access Manager, um Authentifizierungs- und Autorisierungsdienste für Endbenutzer, einschließlich Single-Sign-On, bereitzustellen. Wenn Access Manager auf einem Remote-Computer ausgeführt wird, muss Access Manager SDK lokal vorhanden sein.



- **Directory Server.** Für Portal Server Secure Remote Access besteht eine zwingende Abhängigkeit zu Directory Server, das Grundfunktionen zur Verfügung stellt. Daher sind bei einer Aktualisierung von Portal Server Secure Remote Access möglicherweise Erweiterungen des Directory-Schemas erforderlich.

## Selektive Aktualisierung

Java ES Release 5 unterstützt zwar grundsätzlich eine selektive Aktualisierung für alle Komponenten auf einem Computer, Portal Server Secure Remote Access muss jedoch aktualisiert werden, wenn Portal Server aktualisiert wird, da Portal Server Secure Remote Access eng mit Portal Server verbunden ist. Ebenso ist bei einer Aktualisierung von Portal Server Secure Remote Access eine Aktualisierung von Portal Server erforderlich.

Daher gelten für eine Aktualisierung von Portal Server Secure Remote Access dieselben Einschränkungen wie für eine Aktualisierung von Portal Server (siehe Portal Server „[Selektive Aktualisierung](#)“ auf Seite 344): Sie können entweder Portal Server Secure Remote Access und *alle* Abhängigkeiten der Produktkomponenten auf Release 5 aktualisieren, oder Sie aktualisieren nur Portal Server Secure Remote Access und Portal Server auf Release 5 und belassen somit alle anderen Abhängigkeiten der Produktkomponenten bei Release 4.

# Aktualisieren von Portal Server Secure Remote Access von Java ES Release 4

Dieser Abschnitt enthält Informationen zur Aktualisierung von Portal Server Secure Remote Access von Java ES 2005Q4 (Release 4) auf Java ES 2005Q5 (Release 5).

In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisierung der Release 4-Version von Portal Server Secure Remote Access](#)
- [Aktualisierung mehrerer Instanzen](#)

## Einführung

Berücksichtigen Sie bei der Aktualisierung von Java ES von Portal Server Secure Remote Access Release 4 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

- **Allgemeiner Aktualisierungsansatz.** Die Aktualisierung erfolgt durch die Verwendung des Aktualisierungsskripts `psupgrade`. Das Skript entfernt alte Pakete, installiert neue Pakete und migriert gegebenenfalls Konfigurationsdaten.
- **Aktualisierungsabhängigkeiten.** Portal Server ist von bestimmten gemeinsam genutzten Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)). Während Portal Server für Release 5 mit der Release 4-Version dieser gemeinsam genutzten Komponenten kompatibel ist, ist eine Aktualisierung der gemeinsam genutzten Komponenten dennoch erforderlich, da das für die Aktualisierung von Portal Server verwendete Aktualisierungsskript `psupgrade` die Release 5-Version der gemeinsam genutzten ANT-Komponente erfordert.

Des Weiteren ist Portal Server für Release 5 von einem Webcontainer, Access Manager und Directory Server abhängig, wie unter „[Portal Server Secure Remote Access-Abhängigkeiten](#)“ auf [Seite 418](#) beschrieben. Es werden zwei Ansätze zur Aktualisierung dieser Abhängigkeiten unterstützt (siehe „[Selektive Aktualisierung](#)“ auf [Seite 419](#)):

- **Aktualisierungsabhängigkeiten.** Portal Server Secure Remote Access ist zwar von einer Reihe gemeinsam genutzter Java ES-Komponenten abhängig (siehe [Tabelle 1-7 auf Seite 51](#)), Portal Server Secure Remote Access für Release 5 ist jedoch mit der Release 3-Version dieser Komponenten kompatibel. Eine Aktualisierung dieser gemeinsam genutzten Komponenten ist daher hinsichtlich der Aktualisierung von Portal Server Secure Remote Access auf Release 5 optional.

Für Portal Server Secure Remote Access für Release 5 besteht jedoch nur eine zwingende Aktualisierungsabhängigkeit zu Portal Server. Des Weiteren besteht für Portal Server Secure Remote Access für Release 5 eine nicht zwingende Abhängigkeit von Access Manager und Directory Server, wie unter [„Portal Server Secure Remote Access-Abhängigkeiten“ auf Seite 418](#) beschrieben.

Es werden zwei Ansätze zur Aktualisierung dieser Abhängigkeiten von Produktkomponenten unterstützt (siehe [„Selektive Aktualisierung“ auf Seite 419](#)):

- Alle Abhängigkeiten, die von Release 4-Komponenten erfüllt werden (*keine* der Komponenten, mit Ausnahme von Portal Server, werden auf Release 5 aktualisiert).
- Alle Abhängigkeiten, die von Release 5-Komponenten erfüllt werden (*alle* Komponenten werden auf Release 5 aktualisiert.)

Der für die Aktualisierung von Portal Server Secure Remote Access gewählte Ansatz muss auch für die Aktualisierung von Portal Server verwendet werden.

- **Rückwärtskompatibilität.** Die Rückwärtskompatibilität von Portal Server Secure Remote Access Release 5 zu Release 4 ist gewährleistet.
- **Aufheben der Aktualisierung.** Das Zurücksetzen der Release 5-Aktualisierung von Portal Server Secure Remote Access auf Release 4 besteht im Wiederherstellen der Release 4-Pakete und der Release 4-Verzeichnisdaten.
- **Plattformspezifische Aspekte.** Der allgemeine Ansatz für die Aktualisierung von Portal Server Secure Remote Access ist für das Solaris- und Linux-Betriebssystem identisch; Portal Server Secure Remote Access für Release 5 wird auf einem Solaris-System jedoch unter einem neuen Pfad installiert, während auf einem Linux-Betriebssystem der Pfad aus Release 4 verwendet wird.

# Aktualisierung der Release 4-Version von Portal Server Secure Remote Access

In diesem Abschnitt wird die Aktualisierung von Portal Server Secure Remote Access von Java ES Release 4 auf Java ES Release 5 unter Solaris und Linux beschrieben. Plattformspezifische Vorgänge sind durch die Angabe des jeweiligen Betriebssystems, auf das sich der Vorgang bezieht, gekennzeichnet. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung von Release 4](#)
- [Aktualisieren der Release 4-Version von Portal Server Secure Remote Access \(Solaris\)](#)
- [Aktualisieren der Release 4-Version von Portal Server Secure Remote Access \(Linux\)](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung von Release 4](#)
- [Aufheben der Aktualisierung \(Solaris\)](#)
- [Aufheben der Aktualisierung \(Linux\)](#)

## Aufgaben vor der Aktualisierung von Release 4

Bevor Sie mit der Aktualisierung von Portal Server Secure Remote Access beginnen, führen Sie die folgenden Aufgaben durch:

- [Aktuelle Versionsinformationen überprüfen](#)
- [Portal Server Secure Remote Access-Aktualisierungsabhängigkeiten](#)
- [Konfigurationsinformationen von Portal Server Secure Remote Access Release 4 sichern](#)
- [Konfiguration des Lastenausgleichsprogramms entfernen](#)
- [Konfiguration entfernen von Directory Proxy Server](#)
- [Erforderliche Konfigurationsinformationen und Passwörter abrufen](#)

### *Aktuelle Versionsinformationen überprüfen*

Sie können die aktuelle Version von Portal Server Secure Remote Access mithilfe des folgenden Befehls überprüfen:

```
PortalServer6-base/bin/version
```

**Tabelle 16-4** Portal Server Secure Remote Access Ausgaben der Versionsüberprüfung

| Java ES Release | Portal Server Secure Remote Access-Versionsnummer |
|-----------------|---------------------------------------------------|
| Release 2       | 6.3                                               |
| Release 3       | 6.3.1                                             |
| Release 4       | 6.3.1 <sup>1</sup>                                |
| IFR             | 7.0                                               |
| Release 5       | 7.1                                               |

1. Release 3 und Release 4 unterscheiden sich lediglich durch einen Patch. Sie können nach Release 4-Patches suchen, indem Sie den Solaris-Befehl `showrev -p grep patch_ID` bzw. den Linux-Befehl `rpm -qa sun-portal-core` verwenden und die Versionen mit der im *Aktualisierungshandbuch* für Java ES Release 4 aufgelisteten Versionen vergleichen.

### *Portal Server Secure Remote Access-Aktualisierungsabhängigkeiten*

Es wird grundsätzlich empfohlen, alle Java ES-Komponenten auf einem Computersystem (und in einer Netzwerkumgebung) auf Java ES Release 5 zu aktualisieren.

Während Portal Server Secure Remote Access für Release 5 mit der Release 4-Version der gemeinsam genutzten Java ES-Komponenten kompatibel ist, ist eine Aktualisierung der gemeinsam genutzten Komponenten dennoch erforderlich, da das für die Aktualisierung von Portal Server Secure Remote Access verwendete Aktualisierungsskript `psupgrade` die Release 5-Version der gemeinsam genutzten ANT-Komponente erfordert.

Portal Server Secure Remote Access erfordert außerdem die Aktualisierung von Portal Server. Die Aktualisierung anderer Abhängigkeiten von Java ES Release 4-Produktkomponenten ist jedoch nicht erforderlich.

Der Ansatz für die Aktualisierung der Abhängigkeiten ist derselbe Ansatz, der für Portal Server gewählt wird: Wenn eine der Abhängigkeiten auf Release 5 aktualisiert wird, müssen alle Abhängigkeiten aktualisiert werden (siehe [„Selektive Aktualisierung“ auf Seite 344](#)). Da für Portal Server Secure Remote Access jedoch eine Abhängigkeit zu Portal Server besteht, werden mit der Aktualisierung von Portal Server auch die Portal Server Secure Remote Access-Abhängigkeiten aktualisiert, mit Ausnahme der gemeinsam genutzten Komponenten.

Wenn Sie Portal Server Secure Remote Access-Abhängigkeiten auf Release 5 aktualisieren, sollten Sie in der unten angegebenen Reihenfolge vorgehen (unter Auslassung der bereits aktualisierten Abhängigkeiten), bevor Sie Portal Server Secure Remote Access aktualisieren.

1. **Gemeinsam genutzte Komponenten.** Anweisungen zur Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie unter [„Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71.](#)
2. **Portal Server.** Anweisungen zur Aktualisierung von Portal Server finden Sie in [Kapitel 15, „Portal Server“ auf Seite 337.](#)

### *Konfigurationsinformationen von Portal Server Secure Remote Access Release 4 sichern*

Bei der Aktualisierung von Portal Server Secure Remote Access auf Release 5 ist eine Neukonfiguration der Portal Server Secure Remote Access-Software nicht erforderlich. Als Vorsichtsmaßnahme sichert jedoch das Skript `psupgrade` die folgenden Verzeichnisse mit Konfigurationsinformationen:

*PortalServer6Config-base/*

### *Konfiguration des Lastenausgleichsprogramms entfernen*

In Fällen, in denen der Zugriff auf Portal Server Secure Remote Access-Instanzen über ein Lastenausgleichsprogramm erfolgt, kann der Wert der für diesen Zugriff verwendeten Eigenschaft `LOAD_BALANCER_URL` die Aktualisierung von Portal Server Secure Remote Access beeinträchtigen. Diese Einstellung muss daher vor der Aktualisierung einer Portal Server Secure Remote Access-Komponente geändert werden. So ändern Sie die Einstellung der Eigenschaft `LOAD_BALANCER_URL`

1. Notieren Sie, welche der folgenden Konfigurationsdateien lokal vorhanden sind (manche der Dateien unterstützen möglicherweise lokal installierte Portal Server-Komponenten):

*PortalServer6Config-base/PSConfig.properties* (wenn Portal Server lokal vorhanden ist)

*PortalServer6Config-base/GWConfig.properties* (wenn Gateway lokal vorhanden ist)

*PortalServer6Config-base/RWPCConfig.properties* (wenn Rewriter Proxy lokal vorhanden ist)

*PortalServer6Config-base/NLPCConfig.properties* (wenn Netlet Proxy lokal vorhanden ist)

2. Notieren Sie den aktuellen Wert der Eigenschaft `LOAD_BALANCER_URL` in diesen Konfigurationsdateien.

3. Ändern Sie den Wert der Eigenschaft `LOAD_BALANCER_URL` so, dass diese auf die entsprechende zu aktualisierende Portal Server Secure Remote Access-Instanz zeigt:

`LOAD_BALANCER_URL=hostName:port/portal`

4. Stellen Sie sicher, dass die folgenden Konfigurationsinformationen (falls vorhanden) auf die entsprechende Portal Server Secure Remote Access-Komponente (und *nicht* auf das Lastenausgleichsprogramm) verweisen, wie in folgendem Beispiel gezeigt:

In der Datei *PortalServer6Config-base/platform.conf.default*:

`gateway.host=Gateway_hostName`

In der Datei *PortalServer6Config-base/GWConfig.properties* und *PortalServer6Config-base/GWConfig-default.properties*:

`GW_HOST=Gateway_hostName`

`GW_IP=Gateway_hostIP`

In der Datei *PortalServer6Config-base/RWPCConfig.properties* und *PortalServer6Config-base/RWPCConfig-default.properties*:

`RWP_HOST=RewriterProxy_hostName`

`RWP_IP=RewriterProxy_hostIP`

In der Datei *PortalServer6Config-base/NLPConfig.properties* und *PortalServer6Config-base/NLPConfig-default.properties*:

`NLP_HOST=NetLetProxy_hostName`

`NLP_IP=NetLetProxy_hostIP`

### *Konfiguration entfernen von Directory Proxy Server*

In Fällen, in denen der Zugriff der Portal Server Secure Remote Access-Instanzen auf Directory Server über eine Directory Proxy Server-Instanz erfolgt, müssen die Einstellungen des Hosts und der Portnummer für Directory Proxy Server vor der Aktualisierung geändert und nach der Aktualisierung wieder auf die ursprünglichen Werte festgelegt werden.

So ändern Sie die entsprechenden Einstellungen

1. Notieren Sie den aktuellen Wert der Eigenschaft `DS_HOST` und `DS_PORT` in den folgenden Access Manager-Konfigurationsdateien:

*AccessManagerConfig-base/config/AMConfig.properties*

2. Ändern Sie den Wert der Eigenschaft `DS_HOST` und `DS_PORT` so, dass diese direkt auf die entsprechende Directory Server-Instanz zeigen.

### *Erforderliche Konfigurationsinformationen und Passwörter abrufen*

Je nach Aktualisierungsszenario ist bei der Ausführung des Skripts `psupgrade` die Eingabe von Informationen zu folgenden Administratorkonten erforderlich:

- Administrator-ID und -Passwort für Directory Server
- Administrator-ID und -Passwort für Access Manager
- `amldapuser`-ID und -Passwort für Directory Server

### **Aktualisieren der Release 4-Version von Portal Server Secure Remote Access (Solaris)**

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Portal Server Secure Remote Access haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung (Solaris)*

Bei der Aktualisierung der Portal Server Secure Remote Access-Software auf Release 5 müssen folgende Aspekte berücksichtigt werden:

- Die Portal Server Secure Remote Access-Software besteht aus Unterkomponenten, die eine Reihe verschiedener Rollen übernehmen, jedoch alle zusammen auf Release 5 aktualisiert werden müssen:
  - **Portal-base.** Beinhaltet administrative Mbeans und zugehörige Verwaltungssoftware, Logging Framework und Software bezüglich Überwachung. Sämtliche dieser Bestandteile sind im SUNWportal-base-Paket enthalten.
  - **Secure Remote Access-Anwendungen.** Enthalten Gateway, Netlet Proxy und Rewriter Proxy. Diese Anwendungen werden in der Regel auf einem oder mehreren Computern bereitgestellt, die nicht als Host für den eigentlichen Portal Server dienen. Secure Remote Access-Anwendungen erfordern keinen Webcontainer.
- Wenn Gateway, Rewriter Proxy und Netlet Proxy nicht auf demselben Computer bereitgestellt werden, muss Rewriter Proxy und Netlet Proxy vor der Aktualisierung von Gateway aktualisiert werden.
- Alle Portal Server Secure Remote Access-Unterkomponenten entsprechen demselben installierten Portal Server Secure Remote Access-Image und werden gleichzeitig aktualisiert, wenn sich die Unterkomponenten auf dem zu aktualisierenden Computer befinden.



- Das `psupgrade`-Skript erkennt automatisch die auf dem Hostcomputer installierten Portal Server Secure Remote Access-Unterkomponenten und aktualisiert diese.

### *Aktualisierungsverfahren (Solaris)*

Das im Folgenden beschriebene Verfahren ist für die Portal Server Secure Remote Access-Komponente auf dem Computer anzuwenden, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Synchronisieren Sie alle gemeinsam genutzten Komponenten auf Release 5, sofern dies noch nicht erfolgt ist.

Anweisungen hierzu erhalten Sie unter [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“](#) auf Seite 71.

Dieser Schritt ist eine erforderliche Voraussetzung für die Ausführung des Skripts `psupgrade` in [Schritt 8 auf Seite 428](#).

3. Halten Sie alle lokal ausgeführten Gateway-, Rewriter Proxy- und Netlet Proxy-Instanzen an.

```
PortalServer6-base/bin gateway stop
PortalServer6-base/bin netletd stop
PortalServer6-base/bin rwproxycd stop
```

Überprüfen Sie, ob die Prozesse angehalten wurden. Beispiel:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

4. Stellen Sie sicher, dass Access Manager ausgeführt wird.
5. Legen Sie die zwei vom Skript `psupgrade` benötigten Umgebungsvariablen fest (`ANT_HOME` und `JAVA_HOME`). Beispiel:

```
export ANT_HOME=/usr/sfw
export JAVA_HOME=/usr/jdk/entsys-j2se
```

6. Stellen Sie sicher, dass auf Ihrem Computer ausreichend Swap-Speicher zur Verfügung steht.

Der Swap-Speicher sollte grundsätzlich die doppelte Größe des physikalischen RAM aufweisen.

7. Wenn die zu aktualisierende Portal Server Secure Remote Access-Komponente zu Portal Server remote ist, kopieren Sie die ausführbare Datei `dpadmin` von dem Computer, der als Host für Portal Server dient, auf den Computer, der als Host für die Portal Server Secure Remote Access-Komponente dient.

Die ausführbare Datei „dpadmin“ befindet sich im folgenden Verzeichnis:

*PortalServer7-base/SUNWps.bak/bin/dpadmin*, wenn Portal Server bereits aktualisiert wurde.

*PortalServer6-base/bin/dpadmin*, wenn Portal Server noch nicht aktualisiert wurde.

8. Führen Sie das Skript `psupgrade` aus der Java ES Release 5-Verteilung aus.

```
cd os_arch/Products/portal_svr/Tools/upgrade/bin
./psupgrade
```

wobei *os\_arch* der Plattform entspricht, wie z. B. *Solaris\_sparc*.

Das Skript `psupgrade` ruft das Java ES-Installationsprogramm auf, um die neuen Pakete zu installieren und folgende Informationen anzufordern:

- Administrator-ID und -Passwort für Directory Server
- Administrator-ID und -Passwort für Access Manager
- `amldapuser`-ID und -Passwort für Directory Server

9. Starten Sie die in [Schritt 3 auf Seite 427](#) angehaltenen Gateway-, Rewriter Proxy- und Netlet Proxy-Instanzen.

```
PortalServer7-base/bin/psadmin start-sra-instance -u amadminUser
-f passwordFile --name default --type gateway
```

```
PortalServer7-base/bin/psadmin start-sra-instance -u amadminUser
-f passwordFile --name default --type nlproxy
```

```
PortalServer7-base/bin/psadmin start-sra-instance -u amadminUser
-f passwordFile --name default --type rwproxy
```

Wenn die oben genannten Befehle fehlschlagen, müssen Sie zuerst die Portal Server Secure Remote Access-Komponenten registrieren (aktivieren):

```
PortalServer7-base/bin/psadmin provision-sra -u amadminUser
-f passwordFile -p Portal_ID --gateway-profile profileName --enable
```

## Aktualisieren der Release 4-Version von Portal Server Secure Remote Access (Linux)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Portal Server Secure Remote Access haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung (Linux)*

Bei der Aktualisierung der Portal Server Secure Remote Access-Software auf Release 5 unter Linux sind dieselben Aspekte wie unter Solaris zu berücksichtigen (siehe „[Zu berücksichtigende Aspekte bei der Aktualisierung \(Solaris\)](#)“ auf [Seite 426](#)). Allerdings wird Portal Server Secure Remote Access für Release 5 unter demselben Pfad wie für Release 4 auf dem Linux-Betriebssystem installiert. Daher entfernt das Skript psupgrade bei der Installation der RPMs für Release 5 die vorherigen RPMs.

### *Aktualisierungsverfahren (Linux)*

Das im Folgenden beschriebene Verfahren ist für Portal Server Secure Remote Access auf dem Computer anzuwenden, auf dem die Aktualisierung durchgeführt wird.

---

**VORSICHT** Eine Aktualisierung von Java ES Release 4 auf Release 5 unter Linux kann nicht rückgängig gemacht werden. Stellen Sie sicher, dass Sie Ihr System sicher, *bevor* Sie das folgende Verfahren durchführen.

---

1. Melden Sie sich als Root oder Superuser an.

su -

2. Synchronisieren Sie alle gemeinsam genutzten Komponenten auf Release 5, sofern dies noch nicht erfolgt ist.

Anweisungen hierzu erhalten Sie unter [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“](#) auf [Seite 71](#).

Dieser Schritt ist eine erforderliche Voraussetzung für die Ausführung des Skripts psupgrade in [Schritt 8 auf Seite 430](#).

3. Halten Sie alle lokal ausgeführten Gateway-, Rewriter Proxy- und Netlet Proxy-Instanzen an.

```
PortalServer6-base/bin gateway stop
PortalServer6-base/bin netletd stop
PortalServer6-base/bin rwproxyd stop
```

Überprüfen Sie, ob die Prozesse angehalten wurden. Beispiel:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

4. Stellen Sie sicher, dass Access Manager ausgeführt wird.
5. Legen Sie die zwei vom Skript `psupgrade` benötigten Umgebungsvariablen fest (`ANT_HOME` und `JAVA_HOME`). Beispiel:

```
export ANT_HOME=/opt/sun
export JAVA_HOME=/usr/jdk/entsys-j2se
```

6. Stellen Sie sicher, dass auf Ihrem Computer ausreichend Swap-Speicher zur Verfügung steht.

Der Swap-Speicher sollte grundsätzlich die doppelte Größe des physikalischen RAM aufweisen.

7. Wenn die zu aktualisierende Portal Server Secure Remote Access-Komponente zu Portal Server remote ist, kopieren Sie die ausführbare Datei `dpadmin` von dem Computer, der als Host für Portal Server dient, auf den Computer, der als Host für die Portal Server Secure Remote Access-Komponente dient.

Die ausführbare Datei „`dpadmin`“ befindet sich im folgenden Verzeichnis:

*PortalServer7-base/SUNWps.bak/bin/dpadmin*, wenn Portal Server bereits aktualisiert wurde.

*PortalServer6-base/bin/dpadmin*, wenn Portal Server noch nicht aktualisiert wurde.

8. Führen Sie das Skript `psupgrade` aus der Java ES Release 5-Verteilung aus.

```
cd os_arch/Products/porta_l_svr/Tools/upgrade/bin
./psupgrade
```

wobei `os_arch` der Plattform entspricht, wie z. B. `Solaris_sparc`.

Das Skript `psupgrade` ruft das Java ES-Installationsprogramm auf, um die neuen Pakete zu installieren und folgende Informationen anzufordern:

- Administrator-ID und -Passwort für Directory Server
- Administrator-ID und -Passwort für Access Manager

- o amldapuser-ID und -Passwort für Directory Server

## Überprüfen der Aktualisierung

Wenn die zu aktualisierende Portal Server Secure Remote Access-Komponente zu Portal Server remote ist, können Sie die Installation der Release 5-Pakete anhand der Versionsinformationen in folgender Datei überprüfen:

*PortalServer7-base/lib/PSversion.properties*

Wenn sich die zu aktualisierende Portal Server Secure Remote Access-Komponente jedoch auf demselben Computer befindet wie Portal Server, können Sie die Aktualisierung mit folgendem Befehl überprüfen:

```
PortalServer7-base/bin/psadmin --version --adminuser admin_ID
-f adminpasswordfile.
```

Ausgabewerte finden Sie in [Tabelle 16-4 auf Seite 423](#).

Sie können auch die Protokolldateien der Aktualisierung im folgenden Verzeichnis überprüfen:

*/var/sadm/install/logs/Sun\_Java\_System\_Portal\_Server\_upagrede.log*

## Aufgaben nach der Aktualisierung von Release 4

Bei einer Aktualisierung von Portal Server Secure Remote Access auf Release 5 müssen keine Aufgaben durchgeführt werden, mit Ausnahme in folgenden Fällen:

- [Konfiguration des Lastenausgleichsprogramms wiederherstellen](#)
- [Konfiguration wiederherstellen von Directory Proxy Server](#)
- [Lokalisierte Release 4-Anbieter löschen](#)

### **Konfiguration des Lastenausgleichsprogramms wiederherstellen**

Wenn der Zugriff auf die Portal Server Secure Remote Access-Instanzen über ein Lastenausgleichsprogramm erfolgt, führen Sie nach der Aktualisierung folgende Schritte durch, um die Konfiguration des Lastenausgleichsprogramms wiederherzustellen:

1. Legen Sie die folgenden Parameter in der Datei *PortalServer7Config-base/platform.conf.default* fest:

```
gateway.virtualhost=loadBalancer_hostName loadBalancer_hostIP
gateway.external.ip=loadBalancer_hostIP
gateway.dsame.agent=http\://loadBalancer_hostName\:
80/portal/RemoteConfigServlet
```

2. Legen Sie die folgenden Parameter in der Datei *PortalServer7Config-base/GWConfig-default.properties* fest:  
  
`gateway.ipaddress=Gateway_hostIP`
3. Legen Sie die jeweiligen Parameter aus [Schritt 1](#) und [Schritt 2](#) für Rewriter Proxy und Netlet Proxy fest, wenn diese Instanzen auf Computern bereitgestellt werden, die zum Portal Server-Host remote sind.
4. Starten Sie die Portal Server-Instanzen und die Portal Server Secure Remote Access-Instanzen mit Lastenausgleich neu.

### **Konfiguration wiederherstellen von Directory Proxy Server**

Wenn Portal Server Secure Remote Access-Instanzen über eine Directory Proxy Server-Instanz auf Directory Server zugegriffen haben, müssen die Einstellungen des Hosts und der Portnummer für Directory Proxy Server wieder auf ihre ursprünglichen Werte (wie vor der Aktualisierung) festgelegt werden. Siehe [„Konfiguration entfernen von Directory Proxy Server“ auf Seite 425](#). In diesem Abschnitt wurden die Werte dieser Eigenschaften in Vorbereitung auf die Aktualisierung geändert.

### **Lokalisierte Release 4-Anbieter löschen**

Lokalisierte Proxylet-Dienste werden erst geladen, wenn Sie die lokalisierten Release 4-Anbieter wie folgt löschen:

1. Wechseln Sie in das Verzeichnis  
*PortalServer7Data-base/portals/Upgraded/desktop*.
2. Löschen Sie alle Verzeichnisse und Dateien aus *default\_Locale* mit Ausnahme folgender Verzeichnisse und Dateien:
  - Von Ihnen erstellte Dateien und Verzeichnisse (nicht im Lieferumfang von Portal Server Secure Remote Access enthalten).
  - Die Datei *message.properties*
  - Die folgenden Verzeichnisse:  
AddressBookProvider  
BookmarkProvider  
CalendarProvider  
LoginProvider  
LotusNotesAddressBookProvider  
LotusNotesCalendarProvider  
LotusNotesMailProvider  
MSExchangeAddressBookProvider  
MSExchangeCalendarProvider

```

MSExchangeMailProvidervMailProvider
NotesProvider
PersonalNoteProvider
Register
SampleRSS
SampleURLScraper
SampleXML
TemplateEditContainerProvider
TemplateTabContainerProvider
URLScraperProvider
UWCAddressBookProvider
UserInfo
UserInfoProvider
XMLProvider
error

```

3. Starten Sie den Webcontainer, in dem Portal Server bereitgestellt ist, neu.

### Aufheben der Aktualisierung (Solaris)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Verfahren zum Aufheben der Aktualisierung Portal Server Secure Remote Access haben, sowie eine Beschreibung des eigentlichen Verfahrens zum Aufheben der Aktualisierung.

#### *Zu berücksichtigende Aspekte beim Aufheben der Aktualisierung (Solaris)*

Das Verfahren zum Aufheben der Aktualisierung auf Release 5 erfolgt durch das Zurückkehren zur Release 4-Installation in *PortalServer6-base*.

#### *Verfahren zum Aufheben der Aktualisierung (Solaris)*

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Stellen den ursprünglichen Zustand von Directory Server wie vor der Aktualisierung wieder her.

Verwenden Sie das Directory Server-Befehlszeilenprogramm zum Sichern und Wiederherstellen und die GUI-Dienstprogramme. Weitere Informationen finden Sie im Kapitel über das Sichern und Wiederherstellen von Directory Server im *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide* (<http://docs.sun.com/doc/819-0995>)

3. Entfernen Sie die Release 5 Portal Server Secure Remote Access-Pakete.

- a. Starten Sie das Java ES-Deinstallationsprogramm.  
`/var/sadm/prod/SUNWentsys5/uninstall`
  - b. Wählen Sie alle installierten Portal Server Secure Remote Access-Komponenten aus.
  - c. Bestätigen Sie Ihre Auswahl für die Deinstallation.
  - d. Beenden Sie das Java ES-Deinstallationsprogramm.
4. Stellen Sie die Verzeichnisse *PortalServer6-base* und *PortalServer6Config-base* an ihren ursprünglichen Speicherorten wieder her.

Diese Verzeichnisse wurden bei der Aktualisierung in Verzeichnisse mit der Erweiterung `.bak` verschoben.



## Aufheben der Aktualisierung (Linux)

Da für die Aktualisierung auf Release 5 die binären Release 4-Dateien entfernt werden müssen, ist das Aufheben der Aktualisierung unter Linux sehr aufwändig.

Eine Möglichkeit zum Aufheben der Aktualisierung besteht darin, *vor* der Aktualisierung ein paralleles System zu erstellen und dieses System vor der Aktualisierung zu testen. Wenn Sie die Aktualisierung aufheben müssen, können Sie zu diesem parallelen System zurückkehren.

## Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen werden Portal Server Secure Remote Access-Komponenten (z. B. Gateway) auf mehreren Computersystemen bereitgestellt, um Skalierbarkeit und Sicherheit zu gewährleisten und die Verfügbarkeit zu verbessern. Möglicherweise führen Sie beispielsweise Gateway-Komponenten auf mehreren Computern zusammen mit einem Lastenausgleichsprogramm aus, um die Last zu verteilen.

Für Gateway-Instanzen mit Lastenausgleich können Sie ein sogenanntes Rolling Upgrade durchführen, bei dem Sie alle Gateway-Instanzen nacheinander aktualisieren, ohne den Dienst zu unterbrechen. Für dieses Verfahren gelten folgende Einschränkungen: Einzelne Portal Server Secure Remote Access-Komponenten sind nicht rückwärts kompatibel mit früheren Versionen. Sämtliche dieser Komponenten müssen zusammen mit Portal Server selbst auf Java ES Release 5 synchronisiert werden. Bei einem Rolling Upgrade können jedoch die Release 4 Portal Server Secure Remote Access-Instanzen während der Aktualisierung der Portal Server-Instanzen weiter ausgeführt werden.

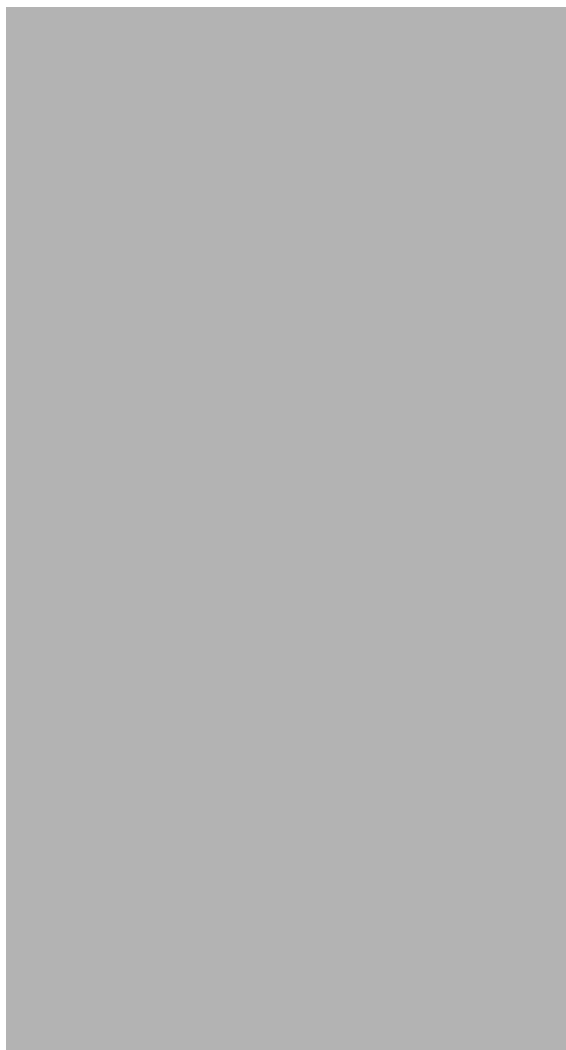
Die in [Abbildung 16-1 auf Seite 436](#) dargestellte Bereitstellungsarchitektur erläutert die Vorgehensweise bei einem Rolling Upgrade.

In dieser Architektur erfolgt der Zugriff auf mehrere Portal Server-Instanzen über Gateway-Instanzen von Portal Server Secure Remote Access. Sowohl die Portal Server-Instanzen als auch die Gateway-Instanzen werden mit Lastenausgleich ausgeführt, um Verfügbarkeit und Skalierbarkeit zu gewährleisten.

Die Portal Server-Instanzen wiederum greifen über ein Lastenausgleichsprogramm auf die Access Manager-Instanzen zu. Die Access Manager- und Access Manager SDK-Instanzen greifen auf ein Verzeichnis zu, das für die Multimaster-Replikation (MMR) eingerichtet wurde. Während andere Directory Server-Replikationsschemata möglich sind, ist MMR repräsentativ für hochverfügbare und skalierbare Directory-Dienste.

In [Abbildung 16-1](#) werden die verschiedenen Instanzen von Gateway, Portal Server, Access Manager und Directory Server gruppiert dargestellt, um den Aktualisierungsvorgang zu erläutern. Portal Server 2 stellt beispielsweise die zweite bis n-te Instanz von Portal Server dar.

**Abbildung 16-1** Beispiel für Bereitstellungsarchitektur für mehrere Portal Server-Instanzen



Ein Rolling Upgrade von Gateway (und Portal Server) von Release 4 auf Release 5 wird wie folgt durchgeführt:

1. Wenn Sie Access Manager von Release 4 auf Release 5 aktualisieren, führen Sie das Rolling Upgrade wie unter [„Aktualisierung mehrerer Instanzen“ auf Seite 309](#) beschrieben durch. Beachten Sie, dass bei einer Aktualisierung von Gateway oder Portal Server der Release 4-Version auf Release 5 keine Aktualisierung der Release 4-Version von Access Manager auf Release 5 erforderlich ist.
2. Ändern Sie die Konfiguration der Portal Server- und Gateway-Instanzen wie folgt.
  - a. Konfigurieren Sie Portal Server 2 mit einem Verweis auf Directory Server 2 statt auf Directory Server 1.  
  
Um die Anweisungen zu verkürzen, bedeutet „Portal Server 2“ gleich Portal Server 2 durch Portal Server n.
  - b. Konfigurieren Sie Gateway 2 mit einem Verweis auf Directory Server 2 statt auf Directory Server 1.  
  
Um die Anweisungen zu verkürzen, bedeutet „Gateway 2“ in diesem und den folgenden Schritten Gateway 2 bis Gateway n.
3. Aktualisieren Sie Portal Server 1..
  - a. Deaktivieren Sie Portal Server 1 im Lastenausgleichsprogramm B.  
Anfragen werden nicht mehr an Portal Server 1 weitergeleitet.
  - b. Deaktivieren Sie Directory Server MMR.  
Directory Server 2Anfragen werden nicht mehr an Directory Server 1. weitergeleitet.
  - c. Aktualisieren Sie Access Manager SDK 1B auf Release 5.  
  
Führen Sie hierzu das unter [„Ausschließliche Aktualisierung der Release 4-Version von Access Manager SDK“ auf Seite 311](#) beschriebene Verfahren durch.
  - d. Aktualisieren Sie Portal Server 1 auf Release 5.  
  
Führen Sie die Aktualisierung der einzelnen Portal Server-Instanzen wie unter [„Aktualisierung der Release 4-Version von Portal Server Secure Remote Access“ auf Seite 422](#) beschrieben durch. Beachten Sie dabei Folgendes:
    - Die folgende Aufgabe muss vor der Aktualisierung durchgeführt werden: [„Konfiguration des Lastenausgleichsprogramms entfernen“ auf Seite 424.](#)

- Stellen Sie vor der Aktualisierung sicher, dass der Wert für `am.encrypted.pwd` in der Datei `AccessManagerConfig-base/config/AMConfig.properties` für das lokale Access Manager SDK und für die zugehörigen Remote-Instanzen von Access Manager identisch ist.
- Stellen Sie sicher, dass Sie in jeder zu aktualisierenden Portal Server-Instanz für den vom Skript `psupgrade` angeforderten Parameter `Portal-Instanz-ID` einen eindeutigen Wert angeben, der nicht Null ist.

Die Portal Server-Daten für Directory Server 1 werden auf Release 5 aktualisiert.

#### 4. Aktualisieren Sie Gateway 1.

- a. Deaktivieren Sie Gateway 1 im Lastenausgleichsprogramm C.

Anfragen werden nicht mehr an Gateway 1 weitergeleitet.

- b. Aktualisieren Sie Access Manager SDK 1A auf Release 5.

Führen Sie hierzu das unter „[Ausschließliche Aktualisierung der Release 4-Version von Access Manager SDK](#)“ auf Seite 311 beschriebene Verfahren durch.

- c. Aktualisieren Sie Gateway 1 auf Release 5.

Führen Sie die Aktualisierung von Gateway wie unter „[Aktualisierung der Release 4-Version von Portal Server Secure Remote Access](#)“ auf Seite 422 beschrieben durch. Beachten Sie dabei Folgendes:

- Die folgende Aufgabe muss vor der Aktualisierung durchgeführt werden: „[Konfiguration des Lastenausgleichsprogramms entfernen](#)“ auf Seite 424.
- Stellen Sie vor der Aktualisierung sicher, dass der Wert für `am.encrypted.pwd` in der Datei `AccessManagerConfig-base/config/AMConfig.properties` für das lokale Access Manager SDK und für die zugehörigen Remote-Instanzen von Access Manager identisch ist.

#### 5. Aktivieren Sie das zuvor deaktivierte Portal Server 1 und Gateway 1 im jeweiligen Lastenausgleichsprogramm wie folgt:

- a. Aktivieren Sie Portal Server 1 im Lastenausgleichsprogramm B.

Anfragen werden wieder an Portal Server 1 weitergeleitet.

- b. Aktivieren Sie Gateway 1 im Lastenausgleichsprogramm C.  
Anfragen werden wieder an Gateway 1 weitergeleitet.
6. Deaktivieren Sie Portal Server 2 und Gateway 2 im jeweiligen Lastenausgleichsprogramm wie folgt:
  - a. Deaktivieren Sie Portal Server 2 im Lastenausgleichsprogramm B.  
Anfragen werden nicht mehr an Portal Server 2 weitergeleitet.
  - b. Deaktivieren Sie Gateway 2 im Lastenausgleichsprogramm C.  
Anfragen werden nicht mehr an Gateway 2 weitergeleitet.
7. Aktualisieren Sie Portal Server 2..
  - a. Stellen Sie die Konfiguration von Portal Server 2 wieder her, sodass auf Directory Server 1 verwiesen wird.
  - b. Aktualisieren Sie Access Manager SDK 2B auf Release 5.  
Führen Sie hierzu das unter „[Ausschließliche Aktualisierung der Release 4-Version von Access Manager SDK](#)“ auf Seite 311 beschriebene Verfahren durch.
  - c. Aktualisieren Sie Portal Server 2 auf Release 5.  
Verwenden Sie dasselbe Verfahren wie bei der Aktualisierung von Portal Server 1, [Schritt d auf Seite 437](#).
  - d. Aktivieren Sie Portal Server 2 im Lastenausgleichsprogramm B.  
Anfragen werden wieder an Portal Server 2 weitergeleitet.
8. Aktualisieren Sie Gateway 2.
  - a. Stellen Sie die Konfiguration von Gateway 2 wieder her, sodass auf Directory Server 1 verwiesen wird.
  - b. Aktualisieren Sie Access Manager SDK 2A auf Release 5.  
Führen Sie hierzu das unter „[Ausschließliche Aktualisierung der Release 4-Version von Access Manager SDK](#)“ auf Seite 311 beschriebene Verfahren durch.
  - c. Aktualisieren Sie Gateway 2 auf Release 5.  
Verwenden Sie dasselbe Verfahren wie bei der Aktualisierung von Gateway 1 in [Schritt c auf Seite 438](#).

- d. Aktivieren Sie Gateway 2 im Lastenausgleichsprogramm C.

Anfragen werden wieder an Gateway 2 weitergeleitet.

9. Aktivieren Sie Directory Server MMR.

Die Portal Server-Daten für Directory Server 2 werden mit Directory Server 1 synchronisiert.

---

**HINWEIS** In Rolling Upgrade-Szenarios, in denen Portal Server-Instanzen auf Release 5 aktualisiert werden, während frühere Releases der Gateway-Komponente aktiv bleiben (d. h. *nicht* das oben beschriebene Szenario), und in denen auf Gateway-Instanzen über ein Lastenausgleichsprogramm zugegriffen wird, müssen Sie überprüfen, ob für alle Gateway-Instanzen in der Datei *PortalServer6Config-base/GWConfig.properties* und *GWConfig-default.properties* folgende Konfigurationseigenschaften auf das Gateway, und nicht auf das Lastenausgleichsprogramm verweisen:

```
GW_IP=Gateway_hostIP
GW_HOST=Gateway_hostName
```

Wenn diese Eigenschaften auf das Lastenausgleichsprogramm verweisen, greift Gateway nicht mehr auf aktualisierte Portal Server-Instanzen zu.

---

# Aktualisieren von Portal Server Secure Remote Access von Java ES Release 3

Das Verfahren zur Aktualisierung von Java ES 2005Q1 (Release 3) Portal Server Secure Remote Access auf Release 5 ist mit dem Verfahren zur Aktualisierung von Portal Server Secure Remote Access Release 4 auf Release 5 identisch, mit Ausnahme folgender Aspekte:

- [Aktualisierung der Portal Server Secure Remote Access-Abhängigkeiten](#)
- [Aktualisieren von Release 3 Portal Server Secure Remote Access](#)
- [Aktualisierung mehrerer Instanzen](#)

## Aktualisierung der Portal Server Secure Remote Access-Abhängigkeiten

Wenn Sie jedoch Portal Server Secure Remote Access Release 3 aktualisieren, müssen Sie Access Manager auf Release 4 oder Release 5 vor der Aktualisierung von Portal Server Secure Remote Access aktualisieren. Sie können außerdem weder andere Abhängigkeiten bei Release 3 belassen noch einige der Abhängigkeiten auf Release 4 und andere auf Release 5 aktualisieren. Weitere Informationen finden Sie unter [„Selektive Aktualisierung“ auf Seite 419](#).

Die folgenden Abhängigkeiten müssen in der unten gezeigten Reihenfolge aktualisiert werden.

1. **Gemeinsam genutzte Komponenten.** Anweisungen zur Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie in [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#).
2. **Directory Server.** Anleitungen für die Aktualisierung von Directory Server auf Release 4 finden Sie in [„Aktualisieren von Directory Server von Java ES Release 2“ auf Seite 126](#).
3. **Access Manager (Access Manager SDK).** Anweisungen zur Aktualisierung von Access Manager auf Release 5 finden Sie in [Kapitel 14, „Access Manager“ auf Seite 281](#).
4. **Portal Server.** Anweisungen zur Aktualisierung von Portal Server finden Sie in [Kapitel 15, „Portal Server“ auf Seite 337](#).

## Aktualisieren von Release 3 Portal Server Secure Remote Access

Um die Release 3-Version von Portal Server Secure Remote Access auf Release 5 zu aktualisieren, folgen Sie den Anweisungen unter [„Aktualisieren von Portal Server Secure Remote Access von Java ES Release 4“ auf Seite 420](#). Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 3.

## Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen werden Portal Server Secure Remote Access-Komponenten (z. B. Gateway) auf mehreren Computersystemen bereitgestellt, um Skalierbarkeit und Sicherheit zu gewährleisten und die Verfügbarkeit zu verbessern. Möglicherweise führen Sie beispielsweise Gateway-Komponenten auf mehreren Computern zusammen mit einem Lastenausgleichsprogramm aus, um die Last zu verteilen.

Wenn Sie mehrere Portal Server Secure Remote Access-Instanzen der Release 3-Version aktualisieren, folgen Sie dem unter [„Aktualisierung mehrerer Instanzen“ auf Seite 435](#) beschriebenen Verfahren. Ersetzen Sie in den Anweisungen jedoch Verweise auf „Release 4“ durch „Release 3“. Sie müssen ebenfalls Access Manager wie in [Schritt 1 auf Seite 437](#) beschrieben aktualisieren.



# Aktualisieren von Portal Server Secure Remote Access von Java ES Release 2

Dieser Abschnitt enthält Informationen zur Aktualisierung von Java ES 2004Q2 (Release 2) Portal Server Secure Remote Access auf Release 5. Das Verfahren ist ähnlich wie das Verfahren für die Aktualisierung von Release 4 Portal Server Secure Remote Access auf Release 5, wie in den folgenden Abschnitten dargestellt:

- [Aufgaben vor der Aktualisierung von Release 2](#)
- [Aktualisieren von Release 2 Portal Server Secure Remote Access](#)
- [Aufgaben nach der Aktualisierung von Release 2](#)
- [Aktualisierung mehrerer Instanzen](#)

## Aufgaben vor der Aktualisierung von Release 2

Die Aufgaben, die vor der Aktualisierung von Portal Server Secure Remote Access Release 2 durchgeführt werden müssen, sind mit denen unter [„Aufgaben vor der Aktualisierung von Release 4“ auf Seite 422](#) beschriebenen Aufgaben identisch, mit Ausnahme folgender Aufgaben:

- [Aktualisierung der Portal Server Secure Remote Access-Abhängigkeiten](#)
- [Löschen des Gateway-Diensteintrags](#)

### Aktualisierung der Portal Server Secure Remote Access-Abhängigkeiten

Wenn Sie Portal Server Secure Remote Access Release 2 aktualisieren, müssen Sie Access Manager auf Release 4 oder Release 5 vor der Aktualisierung von Portal Server Secure Remote Access aktualisieren. Sie können außerdem weder andere Abhängigkeiten bei Release 2 belassen noch einige der Abhängigkeiten auf Release 4 und andere auf Release 5 aktualisieren. Weitere Informationen finden Sie unter [„Selektive Aktualisierung“ auf Seite 419](#).

Die folgenden Abhängigkeiten müssen in der unten gezeigten Reihenfolge aktualisiert werden.

1. **Gemeinsam genutzte Komponenten.** Anweisungen zur Aktualisierung der gemeinsam genutzten Java ES-Komponenten auf Release 5 finden Sie in [Kapitel 2, „Aktualisieren der gemeinsam genutzten Java ES-Komponenten“ auf Seite 71](#). Wenn jedoch die gemeinsam genutzten Komponenten noch nicht aktualisiert wurden, werden diese automatisch vom Skript psupgrade aktualisiert.
2. **Directory Server.** Anleitungen für die Aktualisierung von Directory Server auf Release 4 finden Sie in [„Aktualisieren von Directory Server von Java ES Release 2“ auf Seite 126](#).
3. **Access Manager (Access Manager SDK).** Anweisungen zur Aktualisierung von Access Manager auf Release 5 finden Sie in [Kapitel 14, „Access Manager“ auf Seite 281](#).
4. **Portal Server.** Anweisungen zur Aktualisierung von Portal Server finden Sie in [Kapitel 15, „Portal Server“ auf Seite 337](#).

Um die Release 2-Version von Portal Server Secure Remote Access auf Release 5 zu aktualisieren, folgen Sie den Anweisungen unter [„Aktualisieren von Portal Server Secure Remote Access von Java ES Release 4“ auf Seite 420](#). Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 2.

## Löschen des Gateway-Diensteintrags

Der Benutzereintrag `amService-srapGateway` muss bei einer Aktualisierung von Portal Server Release 2 manuell gelöscht werden, andernfalls kann Gateway nach der Aktualisierung nicht gestartet werden. Führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei Access Manager Console an.
2. Listen Sie alle Benutzer im Organisations-DN auf.
3. Löschen Sie den Benutzer `amService-srapGateway`.

## Aktualisieren von Release 2 Portal Server Secure Remote Access

Das Verfahren zur Aktualisierung von Java ES 2004Q2 (Release 2) Portal Server Secure Remote Access auf Release 5 ist mit dem Verfahren zur Aktualisierung von Portal Server Secure Remote Access Release 4 auf Release 5 identisch.

Um die Release 2-Version von Portal Server Secure Remote Access auf Release 5 zu aktualisieren, folgen Sie den Anweisungen unter [„Aktualisieren von Portal Server Secure Remote Access von Java ES Release 4“ auf Seite 420](#). Ersetzen Sie in den Anweisungen jedoch Verweise auf Release 4 durch Release 2.

## Aufgaben nach der Aktualisierung von Release 2

Die Aufgaben, die nach der Aktualisierung von Release 2 durchgeführt werden müssen, sind mit denen unter [„Aufgaben nach der Aktualisierung von Release 4“ auf Seite 431](#) beschriebenen Aufgaben identisch, mit Ausnahme folgender Aufgabe:

- [Festlegen der Portal Server-Domäne für Proxylet-Dienst](#)

### Festlegen der Portal Server-Domäne für Proxylet-Dienst

Nach der Aktualisierung von Release 2 Portal Server Secure Remote Access auf Release 5 müssen Sie den richtigen Portal Server-Domänenwert festlegen.

1. Melden Sie sich bei Portal Server Console an und navigieren Sie unter „Secure Remote Access“ zur Registerkarte „Proxylet“.
2. Wählen Sie den eindeutigen Namen (Distinguished Name, DN) der Organisation aus, in der sich der Proxylet-Dienst befindet.
3. Ersetzen Sie im Feld „Domänen“ für Proxylet-Regeln SERVER\_DOMAIN durch den Namen der Domäne, in der Portal Server installiert ist.
4. Wiederholen Sie obigen Schritt für alle Organisationen, in denen sich der Proxylet-Dienst befindet.

## Aktualisierung mehrerer Instanzen

Ein Rolling Upgrade mehrerer Instanzen (siehe [„Aktualisierung mehrerer Instanzen“ auf Seite 435](#)) wird bei einer Aktualisierung von Release 2 Portal Server Secure Remote Access-Komponenten (oder Portal Server) auf Release 5 nicht unterstützt.

# Aktualisieren von Portal Server Secure Remote Access von Interim Feature Release 7.0

Dieser Abschnitt enthält Informationen zur Aktualisierung von Portal Server Secure Remote Access von Interim Feature Release (IFR) 7.0 2005Q4 auf Java ES 5 (Release 5).

In diesem Abschnitt werden folgende Themen behandelt:

- [Einführung](#)
- [Aktualisieren von Portal Server Secure Remote Access IFR 7.0](#)
- [Aktualisierung mehrerer Instanzen](#)

## Einführung

Berücksichtigen Sie bei der Aktualisierung von Portal Server Secure Remote Access IFR 7.0 auf Release 5 folgende Aspekte des Aktualisierungsvorgangs:

Das Skript `psupgrade` für die Aktualisierung von Portal Server Secure Remote Access IFR auf Release 5 installiert keine neuen Pakete (wie bei einer Aktualisierung von Release 4). Stattdessen müssen Sie beim Aktualisierungsvorgang folgende Patches anwenden:

**Tabelle 16-5** Patches<sup>1</sup> für die Aktualisierung von Portal Server Secure Remote Access IFR auf Release 5

| Beschreibung                        | Patch-ID: Solaris 9 & 10             | Patch-ID: Linux |
|-------------------------------------|--------------------------------------|-----------------|
| Portal Server 7.1                   | 121465-10 (SPARC)<br>121466-10 (x86) | 121467-10       |
| Portal Server 7.1<br>-Lokalisierung | 123254-02 (SPARC)<br>124590-02 (x86) | 123255-02       |

1. Diese Patch-Versionsnummern sind für die Aktualisierung auf Java ES Release 5 mindestens erforderlich. Wenn neuere Versionen verfügbar sind, verwenden Sie anstelle der in dieser Tabelle genannten Versionen die neueren Versionen.

# Aktualisieren von Portal Server Secure Remote Access IFR 7.0

In diesem Abschnitt wird die Aktualisierung von Portal Server Secure Remote Access von IFR auf Java ES Release 5 unter Solaris und Linux beschrieben. Plattformspezifische Vorgänge sind durch die Angabe des jeweiligen Betriebssystems, auf das sich der Vorgang bezieht, gekennzeichnet. In diesem Abschnitt werden folgende Themen behandelt:

- [Aufgaben vor der Aktualisierung](#)
- [Aktualisieren von Portal Server Secure Remote Access IFR 7.0 \(Solaris\)](#)
- [Aktualisieren von Portal Server Secure Remote Access IFR 7.0 \(Linux\)](#)
- [Überprüfen der Aktualisierung](#)
- [Aufgaben nach der Aktualisierung](#)
- [Aufheben der Aktualisierung \(Solaris\)](#)
- [Aufheben der Aktualisierung \(Linux\)](#)

## Aufgaben vor der Aktualisierung

Die Aufgaben, die vor der Aktualisierung von IFR durchgeführt werden müssen, sind mit denen für eine Release 4-Aktualisierung identisch (siehe [„Aufgaben vor der Aktualisierung von Release 4“ auf Seite 422](#)).

## Aktualisieren von Portal Server Secure Remote Access IFR 7.0 (Solaris)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Portal Server Secure Remote Access haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung von IFR 7 (Solaris)*

Bei der Aktualisierung der Portal Server Secure Remote Access IFR auf Release 5 müssen dieselben Aspekte berücksichtigt werden wie bei einer Aktualisierung von Release 4 (siehe [„Zu berücksichtigende Aspekte bei der Aktualisierung \(Solaris\)“ auf Seite 426](#)).

### *IFR 7-Aktualisierungsverfahren (Solaris)*

Das im Folgenden beschriebene Verfahren ist für Portal Server Secure Remote Access auf dem Computer anzuwenden, auf dem die Aktualisierung durchgeführt wird.

1. Melden Sie sich als Root oder Superuser an.

```
su -
```

2. Halten Sie alle lokal ausgeführten Gateway-, Rewriter Proxy- und Netlet Proxy-Instanzen an.

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t gateway -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t rwproxy -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t nlproxy -N gatewayProfileName
```

Überprüfen Sie, ob die Prozesse angehalten wurden. Beispiel:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

3. Stellen Sie sicher, dass Access Manager ausgeführt wird.
4. Beziehen Sie die in [Tabelle 16-5 auf Seite 446](#) angegebenen erforderlichen Patches.

Verwenden Sie immer die aktuellste, verfügbare Patch-Revision, es sei denn, Sie werden angewiesen, eine bestimmte Revision zu verwenden.

Patches zum Download in das /tmp-Verzeichnis erhalten Sie unter:  
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

5. Wenden Sie zunächst den entsprechenden Portal Server-Patch und bei Bedarf die Lokalisierungs-Patches aus [Tabelle 16-5](#) an.

```
patchadd patch_ID
```

6. Stellen Sie sicher, dass die Patch-Aktualisierung erfolgreich durchgeführt wurde:

```
showrev -p | grep patch_ID
```

Die Ausgabe sollte die Versionen der in [Schritt 5](#) angewendeten Patch-IDs zurückgeben.

7. Wenn in [Schritt 5](#) Lokalisierungspakete aktualisiert wurden, legen Sie für die Portal Server Console-JVM das Gebietsschema „UTF-8“ fest.

```
export LC_ALL=ja_JP.UTF-8
export LANG=ja_JP.UTF-8
```

8. Legen Sie die zwei vom Skript `psupgrade` benötigten Umgebungsvariablen fest (`ANT_HOME` und `JAVA_HOME`):

```
export ANT_HOME=/usr/sfw
export JAVA_HOME=/usr/jdk/entsys-j2se
```

9. Stellen Sie sicher, dass auf Ihrem Computer ausreichend Swap-Speicher zur Verfügung steht.

Der Swap-Speicher sollte grundsätzlich die doppelte Größe des physikalischen RAM aufweisen.

10. Führen Sie das Skript `psupgrade` aus.

```
cd PortalServer7-base/bin
./psupgrade
```

Das `psupgrade`-Skript wird nicht aus der Java ES Release 5-Verteilung ausgeführt und ruft nicht das Java ES-Installationsprogramm auf (auf die Pakete wurden bereits Patches angewendet).

## Aktualisieren von Portal Server Secure Remote Access IFR 7.0 (Linux)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Aktualisierungsverfahren von Portal Server Secure Remote Access haben, sowie eine Beschreibung des eigentlichen Aktualisierungsverfahrens.

### *Zu berücksichtigende Aspekte bei der Aktualisierung von IFR 7 (Linux)*

Bei der Aktualisierung der Portal Server Secure Remote Access-Software auf Release 5 unter Linux sind dieselben Aspekte wie unter Solaris zu berücksichtigen (siehe „[Zu berücksichtigende Aspekte bei der Aktualisierung \(Solaris\)](#)“ auf [Seite 426](#)). Die Release 5-Patches für Linux entfernen jedoch vorherige RPMs.

### *IFR 7-Aktualisierungsverfahren (Linux)*

Das im Folgenden beschriebene Verfahren ist für Portal Server Secure Remote Access auf dem Computer anzuwenden, auf dem die Aktualisierung durchgeführt wird.

---

**VORSICHT** Eine Aktualisierung von Portal Server Secure Remote Access IFR auf Release 5 unter Linux kann nicht rückgängig gemacht werden. Stellen Sie sicher, dass Sie Ihr System sicher, *bevor* Sie das folgende Verfahren durchführen.

---

1. Melden Sie sich als Root oder Superuser an.

`su -`

2. Halten Sie alle lokal ausgeführten Gateway-, Rewriter Proxy- und Netlet Proxy-Instanzen an.

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t gateway -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t rwproxy -N gatewayProfileName
```

```
PortalServer7-base/bin/psadmin stop-sra-instance -u amadminUser
-f passwordFile -t nlproxy -N gatewayProfileName
```

Überprüfen Sie, ob die Prozesse angehalten wurden. Beispiel:

```
ps -ef|grep `cat PortalServer6Data-base/.gw.pid.default`
```

3. Stellen Sie sicher, dass Access Manager ausgeführt wird.
4. Der erforderliche Patch lässt sich anhand der entsprechenden Patch-Nummern und RPM-Namen aus [Tabelle 16-5 auf Seite 446](#) entnehmen.

Verwenden Sie immer die aktuellste, verfügbare Patch-Revision, es sei denn, Sie werden angewiesen, eine bestimmte Revision zu verwenden.

Patches zum Download in das /tmp-Verzeichnis erhalten Sie unter:  
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

5. Wenden Sie zunächst den Portal Server-Patch und anschließend bei Bedarf die Lokalisierungs-RPMs für Portal Server aus [Tabelle 16-5](#) an.

Lesen Sie die Readme-Datei zum Portal Server-Patch; hierin ist beschrieben, wie Sie ein Skript zur Anwendung der RPMs des Patch verwenden:

```
cd /tmp
```

Dabei ist /tmp das Verzeichnis, in das Sie den Patch herunterladen.

```
./update
```

Das Aktualisierungsskript installiert die RPMs.

Installieren Sie die einzelnen RPMs für das Lokalisierungs-Patch mit folgendem Befehl:

```
rpm -Fvh patchName-version.rpm
```



6. Stellen Sie sicher, dass die Patch-Aktualisierung erfolgreich durchgeführt wurde:  

```
rpm -qa | grep sun-portal-core
```

Die Aktualisierungs-Revisionsnummern der RPMs sollten zurückgegeben werden.
7. Wenn in [Schritt 5](#) Lokalisierungspakete aktualisiert wurden, legen Sie für die Portal Server Console-JVM das Gebietsschema „UTF-8“ fest.  

```
export LC_ALL=ja_JP.UTF-8
export LANG=ja_JP.UTF-8
```
8. Legen Sie die zwei vom Skript `psupgrade` benötigten Umgebungsvariablen fest (`ANT_HOME` und `JAVA_HOME`):  

```
export ANT_HOME=/opt/sun
export JAVA_HOME=/usr/jdk/entsys-j2se
```
9. Stellen Sie sicher, dass auf Ihrem Computer ausreichend Swap-Speicher zur Verfügung steht.  

Der Swap-Speicher sollte grundsätzlich die doppelte Größe des physikalischen RAM aufweisen.
10. Führen Sie das Skript `psupgrade` aus.  

```
cd PortalServer7-base/bin
./psupgrade
```

Das `psupgrade`-Skript wird nicht aus der Java ES Release 5-Verteilung ausgeführt und ruft nicht das Java ES-Installationsprogramm auf (auf die Pakete wurden bereits Patches angewendet).

## Überprüfen der Aktualisierung

Sie können die mithilfe der Patches durchgeführte Aktualisierung der Portal Server Secure Remote Access-Pakete auf Release 5 mit folgendem Befehl überprüfen:

```
PortalServer7-base/bin/psadmin --version --adminuser admin_ID
-f adminpasswordfile.
```

Ausgabewerte finden Sie in [Tabelle 16-4 auf Seite 423](#).

Sie können auch die Protokolldateien der Aktualisierung im folgenden Verzeichnis überprüfen:

```
/var/sadm/install/logs/Sun_Java_System_Portal_Server_upagrede.log
```

## Aufgaben nach der Aktualisierung

Nach einer Aktualisierung von Portal Server Secure Remote Access auf Release 5 müssen keine Aufgaben durchgeführt werden.

## Aufheben der Aktualisierung (Solaris)

Dieser Abschnitt enthält eine Beschreibung der Aspekte, die Einfluss auf das Verfahren zum Aufheben der Aktualisierung Portal Server Secure Remote Access haben, sowie eine Beschreibung des eigentlichen Verfahrens zum Aufheben der Aktualisierung.

### *Zu berücksichtigende Aspekte beim Aufheben der Aktualisierung (Solaris)*

Das Verfahren zum Aufheben der Aktualisierung auf Release 5 erfolgt durch das Zurückkehren zur Release 4-Installation in *PortalServer7-base*.

### *Verfahren zum Aufheben der Aktualisierung (Solaris)*

1. Melden Sie sich als Root oder Superuser an.

`su -`

2. Stellen den ursprünglichen Zustand von Directory Server wie vor der Aktualisierung wieder her.

Verwenden Sie das Directory Server-Befehlszeilenprogramm zum Sichern und Wiederherstellen und die GUI-Dienstprogramme. Weitere Informationen finden Sie im Kapitel über das Sichern und Wiederherstellen von Directory Server im *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide* (<http://docs.sun.com/doc/819-0995>).

3. Machen Sie den in [Tabelle 16-5 auf Seite 446](#) angegebenen Portal Server 7.1-Patch rückgängig.

`patchrm patch_ID`

## Aufheben der Aktualisierung (Linux)

Unter Linux steht kein Verfahren zum Aufheben der Aktualisierung zur Verfügung.

## Aktualisierung mehrerer Instanzen

In manchen Bereitstellungsarchitekturen wird Portal Server Secure Remote Access auf mehreren Computersystemen bereitgestellt, um die Skalierbarkeit zu gewährleisten und die Verfügbarkeit zu verbessern. Möglicherweise führen Sie beispielsweise Portal Server Secure Remote Access-Komponenten auf mehreren Computern zusammen mit einem Lastenausgleichsprogramm aus, um die Last zu verteilen.

Für Portal Server Secure Remote Access-Instanzen mit Lastenausgleich können Sie ein sogenanntes Rolling Upgrade durchführen, bei dem Sie alle Portal Server Secure Remote Access-Instanzen nacheinander aktualisieren, ohne den Dienst zu unterbrechen. Dabei werden die verschiedenen Portal Server Secure Remote Access-Instanzen einzeln aktualisiert, während die übrigen Instanzen weiter ausgeführt werden. Unter [„Aktualisieren von Portal Server Secure Remote Access IFR 7.0“ auf Seite 447](#) wird beschrieben, wie Sie die Aktualisierung der einzelnen Instanzen durchführen.

Wenn Sie mehrere Portal Server Secure Remote Access-Instanzen der IFR-Version aktualisieren, folgen Sie dem unter [„Aktualisierung mehrerer Instanzen“ auf Seite 435](#) beschriebenen Verfahren. Ersetzen Sie in den Anweisungen jedoch Verweise auf „Release 4“ durch „IFR“. Sie müssen ebenfalls Access Manager wie in [Schritt 1 auf Seite 437](#) beschrieben aktualisieren.



# Java Enterprise System-Versionsinhalte

In diesem Anhang werden die Inhalte der verschiedenen Java Enterprise System-Releases aufgeführt. Es besteht aus folgenden Abschnitten:

- „Java ES 2003Q4 (Release 1)“ auf Seite 456
- „Java ES 2004Q2 (Release 2)“ auf Seite 458
- „Java ES 2005Q1 (Release 3)“ auf Seite 461
- „Java ES 2005Q4 (Release 4)“ auf Seite 466
- „Java ES 5 (Release 5)“ auf Seite 471

# Java ES 2003Q4 (Release 1)

In diesem Abschnitt werden die Inhalte von Java Enterprise System 2003Q4 aufgelistet.

## Release 1: Im Installationsprogramm auswählbare Komponenten

Die Produktkomponenten Sun Open Network Environment (Sun ONE) und Sun Cluster bieten Infrastrukturdienste, die zur Unterstützung verteilter Unternehmensanwendungen erforderlich sind. Folgende Produktkomponenten stehen zur Verfügung:

- Sun Cluster 3.1 und Sun Cluster Agents für Sun ONE
- Sun ONE Administration Server 5.2
- Sun ONE Anwendungsserver 7, Update 1
- Sun ONE Calendar Server 6.0
- Sun ONE Directory Server 5.2
- Sun ONE Directory Proxy Server 5.2
- Sun ONE Identity Server 6.1
- Sun ONE Instant Messaging 6.1
- Sun ONE Message Queue 3.0.1 Service Pack 2
- Sun ONE Messaging Server 6.0
- Sun ONE Portal Server 6.2
- Sun ONE Portal Server, Secure Remote Access 6.2
- Sun ONE Webserver 6.1

## Release 1: Gemeinsam genutzte Komponenten

Gemeinsam genutzte Komponenten bieten die Unterstützung der lokalen Dienste und Technologien, von denen die Produktkomponenten abhängen. Bei der Installation der Produktkomponenten installiert das Java ES-Installationsprogramm automatisch die erforderlichen gemeinsam genutzten Komponenten, sofern sie nicht bereits installiert sind.

Java Enterprise System umfasst die folgenden gemeinsam genutzten Komponenten:

- ANT (auf Jakarta ANT Java/XML basierendes Tool)
- Apache Commons Logging
- ICU (International Components for Unicode)
- J2SE™ Platform 1.4.1\_06 (Java 2 Platform, Standard Edition)
- JAF (JavaBeans™ Activation Framework)
- JATO (Sun ONE Application Framework)
- JavaHelp™ Runtime
- JAXM (Java-API für XML-Messaging) Client Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java API for XML Registries)
- JAX-RPC (Java-APIs für XML-basierten Remote Procedure Call)
- JSS (Java Security Services)
- KT Search Engine
- LDAP C Language SDK
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)
- SAAJ (SOAP mit Anhangs-API für Java)
- SASL (Simple Authentication and Security Layer)
- XML C Library (libxml)

---

**HINWEIS** Perl ist zudem für Anwendungsserver und Directory Server auf Ihrem System erforderlich, wird aber nicht automatisch als gemeinsam genutzte Java ES-Komponente installiert.

---

## Java ES 2004Q2 (Release 2)

In diesem Abschnitt werden die Inhalte von Java Enterprise System 2004Q2 aufgelistet.

### Release 2: Im Installationsprogramm auswählbare Komponenten

Produktkomponenten bieten die erforderlichen Infrastrukturdienste für die Unterstützung verteilter Unternehmensanwendungen. Bei der Installation von Java Enterprise System auf einem bestimmten Host wählen Sie entsprechend Ihrer allgemeinen Bereitstellungsarchitektur aus, welche Produktkomponenten auf diesem Host installiert werden sollen.

Java Enterprise System 2004Q2 enthält folgende Produktkomponenten:

#### **Communication & Collaboration Services**

- Sun Java System Messaging Server 6 2004Q2
- Sun Java System Calendar Server 6 2004Q2
- Sun Java System Instant Messaging 6 2004Q2
- Sun Java System Portal Server 2004Q2
- Sun Java System Portal Server Mobile Access 2004Q2
- Sun Java System Portal Server Secure Remote Access 2004Q2
- Sun Java System Communications Express 6 2004Q2

#### **Web & Application Services**

- Sun Java System Anwendungsserver 7.0 Update 3 (Standard und Platform Edition)
- Sun Java System Webserver 6 2004Q2 Update 1 Service Pack 2
- Sun Java System Message Queue 3.5 SP1 (Platform und Enterprise Edition)



**Directory & Identity Services**

- Sun Java System Identity Server 6.2 2004Q2, einschließlich  
Sun Java System Communications Services 6 2004Q2 User Management Utility
- Sun Java System Directory Server 5 2004Q2
- Sun Java System Directory Proxy Server 5 2004Q2

**Verfügbarkeitsdienste**

- Sun Cluster 3.1 4/04 und Sun Cluster Agents für Sun Java System

**Administrative Services**

- Sun Java System Administration Server 5 2004Q2
- Sun Remote Services Net Connect 3.5

Beachten Sie, dass Sun Cluster, Sun Cluster Agents und Sun Remote Services Net Connect auf dem Linux-Betriebssystem nicht zur Verfügung stehen.

## Release 2: Gemeinsam genutzte Komponenten

Gemeinsam genutzte Komponenten bieten die Unterstützung der lokalen Dienste und Technologien, von denen die Produktkomponenten abhängen. Bei der Installation der Produktkomponenten installiert das Java ES-Installationsprogramm automatisch die erforderlichen gemeinsam genutzten Komponenten, sofern sie nicht bereits installiert sind.

Java Enterprise System 2004Q2 umfasst die folgenden gemeinsam genutzten Komponenten:

- Ant (auf Jakarta ANT Java/XML basierendes Tool)
- Apache Commons Logging
- Apache SOAP (Simple Object Access Protocol)
- ICU (International Components for Unicode)
- J2SE™ Platform 1.4.2\_04 (Java 2 Platform, Standard Edition)
- JAF (JavaBeans™ Activation Framework)
- JATO (Java Application Framework)
- JavaHelp™ Runtime
- JAXB (Java Architecture for XML Binding)

- JAXM (Java-API für XML-Messaging) Client Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java API for XML Registries)
- JAX-RPC (Java-APIs für XML-basierten Remote Procedure Call)
- JCAPAPI (Java Calendar API)
- JSS (Java Security Services)
- KT Search Engine
- LDAP C Language SDK
- LDAP Java SDK
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)
- Perl LDAP, einschließlich NSPERL
- SAAJ (SOAP mit Anhangs-API für Java)
- SAML (Security Assertions Markup Language)
- SASL (Simple Authentication and Security Layer)
- SNMP (Simple Network Management Protocol) Peer
- Sun Explorer Data Collector
- XML C Library (libxml)

# Java ES 2005Q1 (Release 3)

In diesem Abschnitt werden die Inhalte von Java Enterprise System 2005Q1 aufgelistet.

## Release 3: Im Installationsprogramm auswählbare Komponenten

Auf der Seite für die Komponentenauswahl des Java ES-Installationsprogramms werden die auswählbaren Komponenten anhand der Dienste gruppiert, deren Bereitstellung sie unterstützen. Die folgende Liste enthält auch die Unterkomponenten, die mit der jeweiligen Komponente installiert werden.

### **Communication & Collaboration Services**

- Sun Java System Messaging Server 6 2005Q1
- Sun Java System Calendar Server 6 2005Q1
- Sun Java System Instant Messaging 7 2005Q1
  - Instant Messaging Server Core: Enthält Server- und Multiplexer-Software.
  - Instant Messaging-Ressourcen
  - Access Manager Instant Messaging Service
- Sun Java System Portal Server 6 2005Q1
- Sun Java System Portal Server Secure Remote Access 6 2005Q1
  - Secure Remote Access Core
  - Gateway
  - Netlet Proxy
  - Rewriter Proxy
- Sun Java System Communications Express 2005Q1
- Sun Java System Directory Preparation Tool

## **Web & Application Services**

- Sun Java System Anwendungsserver Enterprise Edition 8.1 2005Q1
  - Domain Administration Server
  - Anwendungsserver-Knotenagent
  - Befehlszeilen-Administrations-Tool
  - Load Balancer-Plug-In

Kann entweder mit Webserver oder Apache Webserver (bei Konfiguration wählbar) verwendet werden. Der Standard ist Webserver.

  - PointBase
  - Beispielanwendungen
- Sun Java System Webserver 6 2005Q1 Update 1 Service Pack 4
- Sun Java System Message Queue 3 2005Q1

## **Directory & Identity Services**

- Sun Java System Access Manager 6.3 2005Q1

Delegierter Administrator-Bereitstellungstools für Portal Server und Messaging Server werden automatisch mit Access Manager installiert.

  - Identity Management und Policy Services Core (umfasst Delegierter Administrator-Dienstprogramm)
  - Access Manager-Administrationskonsole
  - Common Domain Services for Federation Management
  - Access Manager SDK
- Sun Java System Directory Server 5 2005Q1
- Sun Java System Directory Proxy Server 5 2005Q1

## Verfügbarkeitsdienste

- Sun Cluster 3.1 9/04
  - Sun Cluster Core
- Sun Cluster Agents für Sun Java System
  - HA/Scalable Sun Java System Webserver
  - HA Sun Java System Message Queue
  - HA Sun Java System Portal Server
  - HA Sun Java System Administration Server
  - HA Sun Java System Directory Server
  - HA Sun Java System Messaging Server
- HADB (wird für Hochverfügbarkeits-Sitzungsspeicher verwendet)

## Administrative Services

- Sun Java System Administration Server 5 2005Q1
- Sun<sup>SM</sup> Remote Services Net Connect 3.1.1

---

**HINWEIS** Sun Cluster, Sun Cluster Agents und Sun Remote Services Net Connect sind unter Solaris 10 oder Linux nicht verfügbar.

Sun Remote Services Net Connect ist auf der Solaris x86-Plattform nicht verfügbar.

---

## Release 3: Gemeinsam genutzte Komponenten

Die gemeinsam genutzten Komponenten stellen lokale Dienste und Technologien für die auswählbaren Komponenten bereit. Bei der Installation der Java ES-Komponenten installiert das Installationsprogramm automatisch die erforderlichen gemeinsam genutzten Komponenten, sofern sie nicht bereits installiert sind.

Dieses Release von Java ES umfasst die folgenden gemeinsam genutzten Komponenten:

- Ant (auf Jakarta ANT Java/XML basierendes Tool)
- Apache SOAP (Simple Object Access Protocol) Runtime
- Berkeley Datenbank
- Common Agent Container
- ICU (International Components for Unicode)
- J2SE™ (Java 2 Platform, Standard Edition) Platform 5.0
- JAF (JavaBeans™ Activation Framework)
- JATO (Java Studio Web Application Framework)
- JavaHelp™ Runtime
- JavaHelp™ Runtime
- JAXB (Java Architecture for XML Binding ) Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java-API für XML-Registrierungen) Runtime
- JAX-RPC (Java-API für XML-basierten Remote Procedure Call) Runtime
- JCAPI (Java Calendar API)
- JDMK (Java Dynamic Management™ Kit) Runtime
- JSS (Java Security Services)
- KTSE (KT Search Engine)
- LDAP C SDK
- LDAP Java SDK
- NSPR (Netscape Portable Runtime)

- NSS (Network Security Services)
- Perl LDAP, einschließlich NSPERL
- SAAJ (SOAP mit Anhangs-API für Java)
- SAML (Security Assertions Markup Language)
- SASL (Simple Authentication and Security Layer)
- SNMP (Simple Network Management Protocol) Peer
- Sun Explorer Data Collector (nur Solaris)
- Sun Java Monitoring Framework
- Sun Java Web Console
- Tomcat Servlet JSP Container
- XML C Library (libxml)
- WSCL (Web Services Common Library)

# Java ES 2005Q4 (Release 4)

In diesem Abschnitt werden die Inhalte von Java Enterprise System 2005Q4 aufgelistet.

## Release 4: Im Installationsprogramm auswählbare Komponenten

Auf der Seite für die Komponentenauswahl des Java ES-Installationsprogramms werden die auswählbaren Komponenten anhand der Dienste gruppiert, deren Bereitstellung sie unterstützen. Die folgende Liste enthält auch die Unterkomponenten, die mit der jeweiligen Komponente installiert werden.

### **Communication & Collaboration Services**

- Sun Java System Messaging Server 6.2 2005Q4
- Sun Java System Calendar Server 6.2 2005Q4
- Sun Java System Instant Messaging 7.0.1 2005Q4
  - Instant Messaging Server Core: Enthält Server- und Multiplexer-Software.
  - Instant Messaging-Ressourcen
  - Access Manager Instant Messaging Service
- Sun Java System Portal Server 6.3.1 2005Q4
- Sun Java System Portal Server Secure Remote Access 6.3.1 2005Q4
  - Secure Remote Access Core
  - Gateway
  - Netlet Proxy
  - Rewriter Proxy
- Sun Java System Communications Express 6.2 2005Q4
- Sun Java System Directory Preparation Tool 6.3 2005Q4
- Sun Java System Communications Services Delegierter Administrator 6.3 2005Q4
  - Delegierter Administrator-Konsole und -Dienstprogramm
  - Delegierter Administrator Server



## Web & Application Services

- Sun Java System Anwendungsserver Enterprise Edition 8.1 2005Q4
  - Domain Administration Server
  - Anwendungsserver-Knotenagent
  - Befehlszeilen-Administrations-Tool
  - Load Balancer-Plug-In

Kann entweder mit Webserver oder Apache Webserver (bei Konfiguration wählbar) verwendet werden. Der Standard ist Webserver.

  - PointBase-Datenbank
  - Beispielanwendungen
- Sun Java System Webserver 6.1 Service Pack 5 2005Q4
- Sun Java Web Proxy Server 4.0.1 2005Q4
- Sun Java System Message Queue Enterprise Edition 3.6 SP3 2005Q4
- Sun Java Service Registry 3.0

## Directory & Identity Services

- Sun Java System Access Manager 7.0 2005Q4
  - Identity Management und Policy Services Core
  - Access Manager-Administrationskonsole
  - Common Domain Services for Federation Management
  - Access Manager SDK
- Sun Java System Directory Server 5.2 2005Q4
- Sun Java System Directory Proxy Server 5.2 2005Q4

## **Verfügbarkeitsdienste**

- Sun Cluster 3.1 8/05
  - Sun Cluster Core
  - Sun Cluster Agents für Sun Java System
    - HA Sun Java System Directory Server
    - HA Sun Java System Administration Server
    - HA/Scalable Sun Java System Webserver
    - HA Sun Java System Message Queue
    - HA Sun Java System Anwendungsserver
    - HA Sun Java System Messaging Server
    - HA Sun Java System Calendar Server
    - HA Sun Java System Instant Messaging
- High Availability Session Store (HADB) 4.4.2

## **Administrative Services**

- Sun Java System Administration Server 5.2 2005Q4

---

**HINWEIS** Sun Cluster und Sun Cluster Agents werden auf dem Solaris-Betriebssystem, nicht jedoch auf dem Linux-Betriebssystem unterstützt.

---

## Release 4: Gemeinsam genutzte Komponenten

Die gemeinsam genutzten Komponenten stellen lokale Dienste und Technologien für die auswählbaren Komponenten bereit. Bei der Installation der Java ES-Komponenten installiert das Installationsprogramm automatisch die erforderlichen gemeinsam genutzten Komponenten, sofern sie nicht bereits installiert sind.

Dieses Release von Java ES umfasst die folgenden gemeinsam genutzten Komponenten:

- ANT (auf Jakarta ANT Java/XML basierendes Tool)
- ACL (Apache Commons Logging)
- BDB (Berkeley Datenbank)
- CAC (Common Agent Container)
- Derby Datenbank
- ICU (International Components for Unicode)
- IM-SDK (Instant Messenger SDK)
- J2SE™ (Java 2 Platform, Standard Edition) Platform 5.0
- JAF (JavaBeans™ Activation Framework)
- JATO (Java Studio Web Application Framework)
- JavaHelp™ Runtime
- JavaHelp™ Runtime
- JAXB (Java Architecture for XML Binding ) Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java-API für XML-Registrierungen) Runtime
- JAX-RPC (Java-API für XML-basierten Remote Procedure Call) Runtime
- JCAP (Java Calendar API)
- JDMK (Java Dynamic Management™ Kit) Runtime
- JSS (Java Security Services)
- KTSE (KT Search Engine)
- LDAP C SDK

- LDAP Java SDK
- MA (Mobile Access) Core
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)
- SAAJ (SOAP-Runtime mit Anhangs-API für Java)
- SASL (Simple Authentication and Security Layer)
- SEDC (Sun Explorer Data Collector, nur Solaris)
- MFWK (Java ES Monitoring Framework)
- SJWC (Sun Java Web Console)
- WSCL (Web Services Common Library)

# Java ES 5 (Release 5)

In diesem Abschnitt werden die Inhalte von Java Enterprise System 5 aufgelistet.

## Release 2: Im Installationsprogramm auswählbare Komponenten

Auf der Seite für die Komponentenauswahl des Java ES-Installationsprogramms werden die auswählbaren Komponenten anhand der Dienste gruppiert, deren Bereitstellung sie unterstützen. Die folgende Liste enthält auch die Unterkomponenten, die mit der jeweiligen Komponente installiert werden. Beachten Sie, dass Communication Services-Komponenten nicht mehr vom Java ES-Installationsprogramm unterstützt werden.

### Collaboration Services

- Sun Java System Portal Server 7.1
- Sun Java System Portal Server Secure Remote Access 7.1
  - Gateway
  - Netlet Proxy
  - Rewriter Proxy

### Web & Application Services

- Sun Java System Anwendungsserver Enterprise Edition 8.2
  - Domain Administration Server
  - Anwendungsserver-Knotenagent
  - Befehlszeilen-Administrations-Tool
  - Load Balancer-Plug-In
    - Kann entweder mit Webserver oder Apache Webserver (bei Konfiguration wählbar) verwendet werden. Der Standard ist Webserver.
  - Beispielanwendungen
- Sun Java System Webserver 7.0
  - Webserver 7.0 CLI
  - Webserver 7.0 Core

- Webserver 7.0 Beispiele
- Sun Java Web Proxy Server 4.0.4
- Sun Java System Message Queue 3.7UR1
- Service Registry 3.1
  - Service Registry Client-Support
  - Service Registry Bereitstellungs-Support

### **Directory & Identity Services**

- Sun Java System Access Manager 7.1
  - Identity Management und Policy Services Core
  - Access Manager-Administrationskonsole
  - Common Domain Services for Federation Management
  - Access Manager SDK
  - Dezentrale Authentifizierung
  - Client-SDK
  - Sitzungs-Failover-Client
- Sun Java System Directory Server Enterprise Edition 6
  - Java Enterprise System Directory Server 6 Core Server
  - Java Enterprise System Directory Service Control Center
  - Sun Java System Directory Server Enterprise Edition 6-Befehlszeilenprogramme
  - Sun Java System Directory Proxy Server 6 Core Server

### **Verfügbarkeitsdienste**

- Sun Cluster 3.1
  - Sun Cluster Core
- Sun Cluster Geographic Edition 3.1 2006Q4
- Sun Cluster Agents 3.1
  - HA Sun Java System Anwendungsserver
  - HA Sun Java System Message Queue

- HA Sun Java System Directory Server
- HA Sun Java System Messaging Server
- HA Sun Java System Application Server EE (HADB)
- HA/Scalable Sun Java System Webserver
- HA Instant Messaging
- HA Sun Java System Calendar Server
- ...
- Sun Java System High Availability Session Store 4.4.3

### **Gemeinsam genutzte Dienste**

- Alle freigegebenen Komponenten  
 Siehe „[Release 5: Gemeinsam genutzte Komponenten](#)“ auf Seite 474.
- Sun Java System Monitoring Console 1.0
- Java DB
  - Java DB Client
  - Java DB Server

---

**HINWEIS** Sun Cluster und Sun Cluster Agents werden auf dem Solaris-Betriebssystem, nicht jedoch auf dem Linux-Betriebssystem unterstützt.

---

## Release 5: Gemeinsam genutzte Komponenten

Die gemeinsam genutzten Komponenten stellen lokale Dienste und Technologien für die auswählbaren Komponenten bereit. Bei der Installation der Java ES-Komponenten installiert das Installationsprogramm automatisch die erforderlichen gemeinsam genutzten Komponenten, sofern sie nicht bereits installiert sind.

Dieses Release von Java ES umfasst die folgenden gemeinsam genutzten Komponenten:

- ANT (auf Jakarta ANT Java/XML basierendes Tool)
- ACL (Apache Commons Logging)
- BDB (Berkeley Datenbank)
- CAC (Common Agent Container), nur für Sun Cluster
- CAC (Common Agent Container)
- FIS (FastInfoSet)
- ICU (International Components for Unicode)
- IM-SDK (Instant Messenger SDK)
- J2SE™ (Java 2 Platform, Standard Edition) Platform 5.0
- JAF (JavaBeans™ Activation Framework)
- JATO (Java Studio Web Application Framework)
- JavaHelp™ Runtime
- JavaHelp™ Runtime
- JAXB (Java Architecture for XML Binding ) Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java-API für XML-Registrierungen) Runtime
- JAX-RPC (Java-API für XML-basierten Remote Procedure Call) Runtime
- JAXWS (Java-API für Webservices) Runtime
- JDMK (Java Dynamic Management™ Kit) Runtime
- JSS (Java Security Services)
- JSTL (JSP Standard Library Template)



- KTSE (KT Search Engine)
- LDAP C SDK
- LDAP Java SDK
- MA (Mobile Access) Core
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)
- SAAJ (SOAP-Runtime mit Anhangs-API für Java)
- SASL (Simple Authentication and Security Layer)
- SEDC (Sun Explorer Data Collector, nur Solaris)
- MFWK (Java ES Monitoring Framework)
- SJWC (Sun Java Web Console)
- WSCL (Web Services Common Library)
- XWSS (XML Web Services Security)



# Index

## A

Abhängigkeiten  
  Produktkomponente, von gemeinsam genutzten  
    Komponenten [49](#)  
  zwischen gemeinsam genutzten  
    Komponenten [53](#)  
  zwischen Produktkomponenten [56](#)  
Access Manager  
  Abhängigkeiten der Produktkomponenten [56](#)  
  Abhängigkeiten zu gemeinsam genutzten  
    Komponenten [51](#)  
  Abkürzung [30](#)  
  Aktualisierungsansatz [36](#)  
  Unterkomponenten [467, 472](#)  
*AccessManager-base-Pfad* [282](#)  
*AccessManagerConfig-base-Pfad* [282](#)  
ACL, gemeinsam genutzte Komponente  
  in Abhängigkeitstabelle [51](#)  
  Vollständiger Name [31](#)  
amconfig-Skript (Access Manager) [300](#)  
ampre71upgrade script (Access Manager) [297, 326](#)  
amupgrade-Skript (Access Manager) [305, 333](#)  
ANT, gemeinsam genutzte Komponente  
  in Abhängigkeitstabelle [51](#)  
  Vollständiger Name [31](#)  
ANT\_HOME (Umgebungsvariable) [357, 361, 384, 395, 399, 427, 430, 449, 451](#)  
Anwendungsserver  
  Abhängigkeiten der Produktkomponenten [57](#)  
  Abhängigkeiten zu gemeinsam genutzten  
    Komponenten [51](#)  
  Abkürzung [30](#)

  Aktualisierungsansatz [37](#)  
  Konfiguration nach der Installation [240](#)  
  Unterkomponenten [467, 471](#)  
Apache Commons Logging, *siehe* ACL  
*AppServer7-base -Pfad* [220](#)  
*AppServer7Config-base -Pfad* [220](#)  
*AppServer8-base-Pfad* [220](#)  
*AppServer8Config-base -Pfad* [220](#)  
*AppServer8Install-base -Pfad* [220](#)  
Auf Jakarta ANT Java/XML basierendes Tool, *siehe*  
  ANT

## B

BDB, gemeinsam genutzte Komponente  
  in Abhängigkeitstabelle [51](#)  
  Vollständiger Name [31](#)  
Berkeley Datenbank, *siehe* BDB

## C

CAC, gemeinsam genutzte Komponente  
  in Abhängigkeitstabelle [51](#)  
  Vollständiger Name [31](#)  
Common Agent Container, *siehe* CAC

## D

- db2bak, Dienstprogramm [293](#)
- Derby Datenbank, gemeinsam genutzte Komponente [469](#)
- Directory Proxy Server
  - Abhängigkeiten der Produktkomponenten [57](#)
  - Abhängigkeiten zu gemeinsam genutzten Komponenten [51](#)
  - Abkürzung [30](#)
  - Aktualisierungsansatz [37](#)
- Directory Server
  - Abhängigkeiten der Produktkomponenten [57](#)
  - Abhängigkeiten zu gemeinsam genutzten Komponenten [51](#)
  - Abkürzung [30](#)
  - Aktualisierungsansatz [37](#)
- DirServer-base-Pfad (Directory Server 6.0) [110](#), [128](#)

## F

- FastInfoSet, *siehe* FIS
- FIS, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [51](#)
  - Vollständiger Name [31](#)

## G

- Gemeinsam genutzte Komponenten
  - abhängige Produktkomponenten [49](#)
  - gegenseitige Abhängigkeiten [53](#)
- Java ES 2003Q4 (Release 1) [457](#)
- Java ES 2004Q2 (Release2) [459](#)
- Java ES 2005Q1 (Release 3) [464](#)
- Java ES 2005Q4 (Release 4) [469](#)
- Java ES 5 (Release 5) [474](#)

## H

- HADB-base-Pfad [179](#), [180](#)

- High Availability Session Store (HADB)
  - Abhängigkeiten der Produktkomponenten [57](#)
  - Abhängigkeiten zu gemeinsam genutzten Komponenten [51](#)
  - Abkürzung [31](#)
  - Aktualisierungsansatz [37](#)

## I

- ICU, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [51](#)
  - Vollständiger Name [31](#)
- IM-SDK, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [51](#)
  - Vollständiger Name [31](#)
- Instant Messenger SDK, *siehe* IM-SDK
- International Components für Unicode, *siehe* ICU

## J

- JAF, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [51](#)
  - Vollständiger Name [32](#)
- JATO, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [51](#)
  - Vollständiger Name [32](#)
- Java 2 Platform, Standard Edition, *siehe* J2SE
- Java API für XML-Registrierungen, *siehe* JAXR
- Java API für XML-Verarbeitung, *siehe* JAXP
- Java Architecture for XML Binding, *siehe* JAXB
- Java Calendar API, *siehe* JCAPI
- Java DB
  - Abhängigkeiten der Produktkomponenten [57](#)
  - Abhängigkeiten zu gemeinsam genutzten Komponenten [51](#)
  - Abkürzung [31](#)
  - Aktualisierungsansatz [37](#)
- Java Dynamic Management Kit, *siehe* JDMK
- Java ES 2003Q4 (Release 1)
  - Gemeinsam genutzte Komponenten [457](#)
  - Produktkomponenten [456](#)

Java ES 2004Q2 (Release 2)  
     Gemeinsam genutzte Komponenten [459](#)  
     Produktkomponenten [458](#)  
 Java ES 2005Q1 (Release 3)  
     Gemeinsam genutzte Komponenten [464](#)  
     Produktkomponenten [461](#)  
 Java ES 2005Q4 (Release 4)  
     Gemeinsam genutzte Komponenten [469](#)  
     Produktkomponenten [466](#)  
 Java ES 5 (Release 5)  
     Gemeinsam genutzte Komponenten [474](#)  
     Produktkomponenten [471](#)  
 Java ES Monitoring Framework, *siehe* MFWK  
 Java SE, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [31](#)  
 Java Security Services, *siehe* JSS  
 Java Studio Web Application Framework, *siehe* JATO  
 JAVA\_HOME [384](#), [395](#), [399](#), [427](#), [430](#), [449](#), [451](#)  
 JAVA\_HOME Umgebungsvariable [302](#), [330](#), [357](#),  
     [361](#)  
 Java-APIs für XML-basierten Remote Procedure  
     Call, *siehe* JAX-RPC  
 JavaBeans Activation Framework, *siehe* JAF  
 JavaHelp, *Siehe* JHELP  
 JavaMail, *Siehe* JMAIL  
 JAXB, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)  
 JAXP, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)  
 JAXR, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)  
 JAX-RPC, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)  
 JAXWS, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)  
 JCAPI, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)

JDMK, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)  
 JHELP, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name  
 JMAIL, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name  
 JSP Standard Library Template, *siehe* JSTL  
 JSP-Dateien, benutzerdefiniert [285](#), [294](#), [300](#), [328](#)  
 JSS, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)  
 JSTL, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)

## K

Konventionen  
     Symbol [23](#)  
     Typografisch [23](#)  
 KT Search Engine, *siehe* KTSE  
 KTSE, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)

## L

LDAP C Language SDK gemeinsam genutzte  
     Komponente [475](#)  
 LDAP C SDK, gemeinsam genutzte Komponente  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)  
 LDAP J SDK, gemeinsam genutzte Komponente [475](#)  
     in Abhängigkeitstabelle [51](#)  
     Vollständiger Name [32](#)

## M

- MA Core, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [51](#)
  - Vollständiger Name [32](#)
- Message Queue
  - Abhängigkeiten der Produktkomponenten [57](#)
  - Abhängigkeiten zu gemeinsam genutzten Komponenten [51](#)
  - Abkürzung [31](#)
  - Aktualisierungsansatz [37](#)
- MessageQueue-base*-Pfad [193](#)
- MFWK, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [51](#)
  - Vollständiger Name [32](#)
- Mobile Access Core, *siehe* MA Core
- Monitoring Console
  - Abkürzung [31](#)
- mqupgrade-Skript (Message Queue) [213](#), [215](#)

## N

- Netscape Portable Runtime, *siehe* NSPR
- Network Security Services, *siehe* NSS
- NSPR, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [52](#)
  - Vollständiger Name [32](#)
- NSS, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [52](#)
  - Vollständiger Name [32](#)

## P

- Pfad *PortalServer6-base* [338](#), [414](#)
- Pfad *PortalServer6Config-base* [338](#), [414](#)
- Pfad *PortalServer7-base* [338](#), [414](#)
- Pfad *PortalServer7Config-base* [338](#), [414](#)
- Pfad *PortalServer7Data-base* [338](#), [414](#)
- Pfad *RegistryDomainR4-base* [249](#)
- Pfad *RegistryDomainR5-base* [250](#)
- Pfad *rel4CAC-base-dir* [80](#)

- Pfad *rel5CAC-admin-dir* [80](#)
- Pfad *ServiceRegistryR4-base* [171](#), [249](#)
- Pfad *ServiceRegistryR5-base* [250](#)
- Portal Server
  - Abhängigkeiten der Produktkomponenten [58](#)
  - Abhängigkeiten zu gemeinsam genutzten Komponenten [51](#)
  - Abkürzung [31](#)
  - Aktualisierungsansatz [37](#)
- Portal Server Secure Remote Access
  - Abhängigkeiten der Produktkomponenten [58](#)
  - Abhängigkeiten zu gemeinsam genutzten Komponenten [51](#)
  - Abkürzung [31](#)
  - Aktualisierungsansatz [37](#)
- postInstall-Skript (Application Server) [241](#)
- Produktkomponenten
  - Abhängigkeit von gemeinsam genutzten Komponenten [49](#)
  - gegenseitige Abhängigkeiten [56](#)
  - Java ES 2003Q4 (Release 1) [456](#)
  - Java ES 2004Q2 (Release 2) [458](#)
  - Java ES 2005Q1 (Release 3) [461](#)
  - Java ES 2005Q4 (Release 4) [466](#)
  - Java ES 5 (Release 5) [471](#)

## S

- SAAJ, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [52](#)
  - Vollständiger Name [32](#)
- SAML [308](#), [335](#)
- SASL, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [52](#)
  - Vollständiger Name [32](#)
- Security Assertion Markup Language, *siehe* SAML
- SEDC, gemeinsam genutzte Komponente
  - in Abhängigkeitstabelle [52](#)
  - Vollständiger Name [32](#)
- serverRoot*-Pfad (Directory Server 5.x) [109](#), [128](#)
- Service Registry
  - Abhängigkeiten der Produktkomponenten [59](#)

Abhängigkeiten zu gemeinsam genutzten  
 Komponenten [51](#)  
 Abkürzung [31](#)  
 Aktualisierungsansatz [37](#)  
 Simple Authentication and Security Layer, *siehe*  
 SASL  
 SJWC, gemeinsam genutzte Komponente  
 in Abhängigkeitstabelle [52](#)  
 Vollständiger Name [32](#)  
 Skripten  
   amconfig (Access Manager) [300](#)  
   ampre71upgrade (Access Manager) [297](#), [326](#)  
   amupgrade (Access Manager) [305](#), [333](#)  
   mqmigrate (Message Queue) [215](#)  
   mqupgrade (Message Queue) [213](#)  
   postInstall (Application Server) [241](#)  
 SML Web Services Security, *siehe* XWSS  
 SOAP-Runtime mit Anhangs-API für Java, *siehe*  
 SAAJ  
 Sun Cluster  
   Abhängigkeiten der Produktkomponenten [59](#)  
   Abhängigkeiten zu gemeinsam genutzten  
   Komponenten [51](#)  
   Abkürzung [31](#)  
   Aktualisierungsansatz [38](#)  
 Sun Cluster Geographic Edition  
   Abhängigkeiten der Produktkomponenten [59](#)  
   Abhängigkeiten zu gemeinsam genutzten  
   Komponenten [51](#)  
   Abkürzung [31](#)  
   Aktualisierungsansatz [38](#)  
 Sun Explorer Data Collector, *siehe* SEDC  
 Sun Java Web Console, *siehe* SJWC  
*SunClusterGeo-base-Pfad* [97](#)  
 Symbolkonventionen [23](#)

## T

Typografische Konventionen [23](#)

## W

Web Proxy Server  
   Abhängigkeiten der Produktkomponenten [59](#)  
   Abhängigkeiten zu gemeinsam genutzten  
   Komponenten [51](#)  
   Abkürzung [31](#)  
   Aktualisierungsansatz [38](#)  
 Web services Common Library, *siehe* WSCL  
*WebProxyServer-base-Pfad* [263](#)  
 Webserver  
   Abhängigkeiten der Produktkomponenten [59](#)  
   Abhängigkeiten zu gemeinsam genutzten  
   Komponenten [51](#)  
   Abkürzung [31](#)  
   Aktualisierungsansatz [38](#)  
*WebServer6-base-Pfad* [144](#)  
*WebServer7-base-Pfad* [144](#)  
*WebServer7Config-base-Pfad* [144](#)  
 WSCL, gemeinsam genutzte Komponente  
 in Abhängigkeitstabelle [52](#)  
 Vollständiger Name [32](#)

## X

XWSS, gemeinsam genutzte Komponente  
 in Abhängigkeitstabelle [52](#)  
 Vollständiger Name [32](#)





# Index of Fonts

Courier @ 10.0 pt 23–28, 30, 35–36, 47, 64–65, 68–70, 75, 77, 79–81, 84–85, 88–89, 91–92, 94–95, 103, 105–107, 111, 114, 117–124, 132, 137–140, 144, 149, 151–155, 157–158, 160–167, 175–178, 185–190, 196, 199–200, 202–205, 207–216, 220, 228, 231–232, 234, 236, 238–244, 255, 257–262, 268, 270–273, 275–276, 278, 282, 287, 289–290, 292–302, 304–308, 310–311, 313–314, 318–319, 321–335, 339, 342, 345–346, 349–377, 379–381, 383–410, 415, 417, 420, 422–434, 436–440, 444–446, 448–452, 465

Courier @ 7.0 pt 136, 195, 223, 349, 352, 423

Courier @ 7.5 pt 2

Courier @ 8.25 pt 23–26, 36–38, 43–44, 78–80, 85–86, 91, 97, 109–110, 112, 128, 130, 144, 146–147, 155–156, 158–160, 162, 171, 179–180, 182, 193, 195–196, 220, 222–224, 249–250, 252, 256, 263, 265, 268, 271–272, 275, 282, 284–285, 296–298, 301–306, 325–326, 330–331, 333, 338, 340–341, 349, 351–352, 354, 414, 417, 423

Courier @ 9.0 pt 18–20, 102, 117–118, 120–122, 135–136, 155, 158–159, 162, 164, 166, 175, 201, 211, 229, 256, 292, 301–302, 304–305, 330, 333, 351

Courier @ 9.5 pt 24, 79–81, 102, 117–118, 124, 135, 149, 216, 402

Helvetica @ 10.0 pt 45, 60, 67, 79, 85, 93, 97, 104, 106, 109–110, 123–124, 127–128, 143, 171, 179, 193, 219–220, 224, 226, 237, 240–241, 249, 263, 272, 281–282, 294, 309, 315–316, 329, 334, 337, 343, 346, 350, 352, 358, 360, 362, 374, 379, 382, 385–386, 396–397, 399, 414, 429, 440, 449, 458, 463, 468, 473

Helvetica @ 11.0 pt 34–35, 91–94, 102–105, 117–119, 135–137, 149–150, 153, 164–167, 175–176, 185–187, 200–202, 211–212, 228–230, 236–239, 244, 255–257, 260, 268–271, 273, 275–276, 292–296, 308, 324–325, 349, 351–352, 354–356, 360, 364–365, 367–368, 371, 394, 397, 401–405, 407–408, 422–427, 429, 431–433, 447, 449, 452

Helvetica @ 12.0 pt 34, 36, 47–49, 66–67, 69–70, 79, 87, 89, 93–95, 100, 102, 104, 107–108, 114, 117–118, 124–125, 132–133, 135–136, 139–140, 146–147, 149–150, 163–164, 167, 173, 175–178, 185–186, 189–191, 197, 200, 202–204, 208–212, 214, 216–217, 225, 228, 230, 232, 235, 238, 243–244, 252–253,

255, 257, 260–261, 266, 268–269, 271–273, 275–276, 278–279, 286–288, 291, 295, 307–308, 312–314, 321–323, 334–335, 342, 344, 349, 355, 360, 363–364, 371, 373, 379, 382–383, 387, 391, 393–394, 396–397, 400, 408, 410, 417–419, 422, 426, 429, 431, 433, 435, 443–445, 447, 449, 451–452

Helvetica @ 14.0 pt 29, 71, 83, 97, 109, 127, 143, 171, 179, 193, 219, 249, 263, 281, 337, 413, 455

Helvetica @ 15.0 pt 477–481

Helvetica @ 16.0 pt 1

Helvetica @ 17.0 pt 22–26, 30–31, 33, 38, 41–42, 45–47, 49, 55, 64–66, 68–69, 72–76, 78, 80, 84–89, 98–99, 101, 111, 113–114, 116–117, 124, 129, 131, 134–135, 140, 144–146, 148–149, 172–175, 178, 181–185, 194–197, 199–200, 205, 207–208, 210, 221, 224–225, 227–228, 234–235, 251–252, 254–255, 262, 264–265, 267–268, 274–275, 282–283, 285–286, 290–291, 309, 311, 315, 320, 323, 335, 339–341, 346, 348, 373, 378–382, 387, 391–393, 410, 415–417, 420, 422, 435, 441–447, 453, 456–459, 461, 464, 466, 469, 471, 474

Helvetica @ 20.0 pt 22, 25, 27–28, 30, 33, 39–40, 49, 60, 64–65, 72, 77, 84, 88, 98, 100, 111, 116, 125–126, 129, 134, 141–142, 144, 148, 169–170, 172, 174, 181, 184, 192, 194, 199, 206–207, 221, 227, 233–234, 245, 251, 254, 264, 267, 274, 282, 290, 315, 320, 339, 346, 378, 381, 392, 415, 420, 441, 443, 446, 456, 458, 461, 466, 471

Helvetica @ 22.0 pt 1, 5, 17, 21, 29, 71, 83, 97–98, 109, 127, 129, 143, 171–172, 179, 193, 219, 249, 251, 263, 281, 337, 413, 455, 477, 1, 1, 1, 3, 7, 17, 19, 49

Helvetica @ 7.0 pt 5–56

Helvetica @ 8.0 pt 1

Helvetica @ 8.25 pt 23–26, 30–32, 36–40, 43–44, 46, 51–53, 56–59, 64, 78–80, 85–86, 91, 97, 99, 102, 109–113, 117–118, 128, 130–131, 135–136, 144–147, 149, 155–156, 158–160, 162–164, 166, 171–173, 175, 179–182, 185–187, 193, 195–196, 201, 211, 220, 222–224, 229, 249, 251–252, 256, 263–265, 268, 270–271, 275, 282–286, 288–289, 292, 296–298, 301–306, 309, 316, 325–326, 330–331, 333, 338, 340–341, 345, 349, 351–352, 354, 375, 392, 414, 416–417, 423, 436, 446

Helvetica @ 9.0 pt 1, 5–16, 23–25, 30–31, 36, 39, 43, 46, 48, 51, 53, 56, 60–64, 77–81, 85–86, 91, 94–95, 97, 99, 102–107, 109, 111, 113, 117, 119–122, 124, 128, 130–131, 135–139, 144–147, 149, 153–155, 157–159, 161–168, 171–173, 175–177, 179, 181–182, 185, 187–190, 193, 195–196, 201–205, 211–216, 220, 222–224, 229–232, 236–243, 246–247, 249, 251–252, 256–265, 268, 270–273, 275–278, 282–283, 285, 288, 292–293, 295–302, 304–311, 313, 316, 318–319, 321–334, 338, 340, 345, 349–351, 354–363, 365–368, 371–373, 375–392, 394–410, 414, 416–417, 423–425, 427–434, 436–441, 444–446, 448–452, 468

Palatino @ 10.0 pt 21–31, 33–36, 38–43, 45–50, 52–56, 60–95, 97–111, 113–129, 131–155, 157–158, 160–179, 181–217, 219–221, 224–247, 249–279, 281–283, 285–302, 304–335, 337, 339–368, 371–411, 413–453, 455–475, 1–3, 1, 3–5, 7–17, 19–47, 49–55

Palatino @ 6.0 pt 23–25, 30–31, 36, 39, 43, 45–46, 51, 56, 60, 64, 67, 78–80, 85–86, 91, 93, 97, 99, 102, 104, 106, 109, 111, 113, 117, 121–124, 127–128, 130–131, 135, 143–147, 149, 155, 158–159, 162, 164,

166, 171–173, 175, 179, 181–182, 185, 187, 193, 195–196, 201, 211, 219–220, 222–224, 226, 229, 237, 240–241, 249, 251–252, 256, 263–265, 268, 270–272, 275, 281–283, 285, 288, 292, 294, 296–297, 301–302, 304–305, 309, 315–316, 325–326, 329–330, 333–334, 337–338, 340, 343, 345–346, 349–352, 354, 358, 360, 362, 374, 379, 382, 385–386, 392, 396–397, 399, 414, 416–417, 423, 429, 440, 446, 449, 458, 463, 468, 473

Palatino @ 7.0 pt 52, 60, 64, 86, 91, 136, 146, 195, 223, 270–271, 296, 298, 303–304, 306, 325–326, 331, 333, 349, 352, 392, 423, 446

Palatino @ 7.5 pt 2–3

Palatino @ 8.0 pt 2

Palatino @ 8.25 pt 24–26, 43–44, 80, 109, 112, 128, 130, 144, 146–147, 158–160, 162, 171, 173, 179–180, 193, 195–196, 220, 222, 224, 252, 263, 265, 271, 282, 284–285, 288–289, 297–298, 301–305, 326, 330–331, 333, 338, 340–341, 345, 351, 354, 398, 414, 417, 450

Palatino @ 9.0 pt 5–20, 23–25, 30–31, 36, 39, 43, 51, 53, 56, 64, 78–80, 85–86, 91, 97, 99, 102, 109, 111, 113, 117, 121–122, 128, 130–131, 135, 144–147, 149, 155, 158–159, 162, 164, 166, 171–173, 175, 179, 181–182, 185, 187, 193, 195–196, 201, 211, 220, 222–224, 229, 249, 251–252, 256, 263–265, 268, 270–271, 275, 282–283, 285, 288, 292, 296–297, 301–302, 304–305, 309, 316, 325–326, 330, 333, 338, 340, 345, 349, 351, 354, 375, 392, 414, 416–417, 423, 436, 446, 477–481

Palatino @ 9.5 pt 79–81, 117, 124, 135, 149, 401–402

ZapfDingbats @ 5.0 pt 30, 68–69, 150–153, 160, 184, 242, 294, 300, 305, 307, 313, 328–329, 333, 348, 355–356, 384, 393, 421, 426, 428, 430–432, 461–463, 466–468, 471–473



# List of Conditional Text



# List of Marker Text for Alternative Text

|                     |                |                                                                                                                                                                                                                                                             |     |
|---------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ImageAltText:       | Abbildung 1-1  | Das Diagramm listet die Abhängigkeiten zw. gemeinsam genutzten Komponenten. Diese werden in zwei Gruppen aufgeteilt: gegenseitige JAX-Abhängigkeiten, und für Anzeige- und Sicherheitszwecke verwendete, von denen die meisten von J2SE oder NSPR abhängen. | 53  |
| ImageLongDescByRef: | Abbildung 1-1  | <a href="#">longdesc-fig1-1.html</a>                                                                                                                                                                                                                        | 53  |
| ImageAltText:       | Abbildung 14-1 | Bereitstellungsarchitektur für mehrere Access Manager-Instanzen (Diagramm)                                                                                                                                                                                  | 309 |
| ImageAltText:       | Abbildung 14-2 | Bereitstellungsarchitektur für mehrere Access Manager-Instanzen (Diagramm)                                                                                                                                                                                  | 316 |
| ImageAltText:       | Abbildung 15-1 | Beispiel-Bereitstellungsarchitektur für mehrere Portal Server-Instanzen, die auf mehrere Access Manager-Instanzen zugreifen (Diagramm).                                                                                                                     | 375 |
| ImageAltText:       | Abbildung 16-1 | Diagramm einer Beispielbereitstellungsarchitektur für mehrere Gateway-Instanzen, die auf mehrere Portal Server-Instanzen mit Zugriff auf mehrere Access Manager-Instanzen zugreifen                                                                         | 436 |





# List of Table Summaries Marker Text

|                     |              |                                                                                                      |     |
|---------------------|--------------|------------------------------------------------------------------------------------------------------|-----|
| TableSummary:       | Tabelle 1    | Schriftartkonventionen in diesem Handbuch                                                            | 23  |
| TableSummary:       | Tabelle 2    | Symbolkonventionen in diesem Handbuch.                                                               | 23  |
| TableSummary:       | Tabelle 3    | Shell-Eingabeaufforderungen in diesem Handbuch.                                                      | 24  |
| TableSummaryNotReq: | Tabelle 4    | Dokumentation                                                                                        | 25  |
| TableSummary:       | Tabelle 1-8  | Abhängigkeiten von Produktkomponenten                                                                | 56  |
| TableSummary:       | Tabelle 3-1  | In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt.   | 85  |
| TableSummary:       | Tabelle 4-2  | In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt.   | 99  |
| TableSummary:       | Tabelle 5-2  | In dieser Tabelle wird der Wegweiser für die Aktualisierung von Directory Server 2006Q3 dargestellt. | 111 |
| TableSummary:       | Tabelle 6-2  | In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt.   | 130 |
| TableSummary:       | Tabelle 7-2  | In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt.   | 145 |
| TableSummary:       | Tabelle 8-2  | In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt.   | 172 |
| TableSummary:       | Tabelle 9-2  | In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt.   | 181 |
| TableSummary:       | Tabelle 10-2 | In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt.   | 195 |

|                     |                               |                                                                                                                                                                                                                  |
|---------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TableSummaryNotReq: | <a href="#">Tabelle 10-3</a>  | <a href="#">196</a>                                                                                                                                                                                              |
| TableSummary:       | <a href="#">Tabelle 11-2</a>  | <a href="#">In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt. 222</a>                                                                                           |
| TableSummary:       | <a href="#">Tabelle 11-3</a>  | <a href="#">In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt. 223</a>                                                                                           |
| TableSummary:       | <a href="#">Tabelle 12-2</a>  | <a href="#">In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt. 251</a>                                                                                           |
| TableSummary:       | <a href="#">Tabelle 13-2</a>  | <a href="#">In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt. 264</a>                                                                                           |
| TableSummary:       | <a href="#">Tabelle 13-5</a>  | <a href="#">In dieser Tabelle werden die erforderlichen Patches für die Aktualisierung und das Aufheben von Administration Server, Directory Server und Directory Proxy Server unter Solaris aufgeführt. 270</a> |
| TableSummary:       | <a href="#">Tabelle 13-6</a>  | <a href="#">In dieser Tabelle werden die erforderlichen Patches für die Aktualisierung von Administration Server unter Linux dargestellt. 271</a>                                                                |
| TableSummary:       | <a href="#">Tabelle 14-2</a>  | <a href="#">In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt. 283</a>                                                                                           |
| TableSummary:       | <a href="#">Tabelle 14-4</a>  | <a href="#">In dieser Tabelle werden die erforderlichen Patches für die Aktualisierung und das Aufheben von Administration Server, Directory Server und Directory Proxy Server unter Solaris aufgeführt. 288</a> |
| TableSummary:       | <a href="#">Tabelle 14-6</a>  | <a href="#">In dieser Tabelle werden die erforderlichen Patches für die Aktualisierung und das Aufheben von Administration Server, Directory Server und Directory Proxy Server unter Solaris aufgeführt. 296</a> |
| TableSummary:       | <a href="#">Tabelle 14-13</a> | <a href="#">In dieser Tabelle werden die erforderlichen Patches für die Aktualisierung und das Aufheben von Administration Server, Directory Server und Directory Proxy Server unter Solaris aufgeführt. 325</a> |
| TableSummary:       | <a href="#">Tabelle 15-2</a>  | <a href="#">In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt. 340</a>                                                                                           |
| TableSummary:       | <a href="#">Tabelle 15-4</a>  | <a href="#">In dieser Tabelle werden die erforderlichen Patches für die Aktualisierung und das Aufheben von Administration Server, Directory Server und Directory Proxy Server unter Solaris aufgeführt. 345</a> |

|               |              |                                                                                                                                                                                                  |
|---------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TableSummary: | Tabelle 15-8 | In dieser Tabelle werden die erforderlichen Patches für die Aktualisierung und das Aufheben von Administration Server, Directory Server und Directory Proxy Server unter Solaris aufgeführt. 392 |
| TableSummary: | Tabelle 16-2 | In dieser Tabelle wird der Wegweiser für die Aktualisierung von Access Manager 2005Q1 dargestellt. 416                                                                                           |
| TableSummary: | Tabelle 16-5 | In dieser Tabelle werden die erforderlichen Patches für die Aktualisierung und das Aufheben von Administration Server, Directory Server und Directory Proxy Server unter Solaris aufgeführt. 446 |



# List of Markers That Insert URLs and Links in HTML Output Files

Starts Link Type13: <http://www.sun.com/patents> 2

Ends Link Type14: aufgelisteten 2

Starts Link Type13: <http://www.sun.com/patents> 2

Ends Link Type14: et 2

Starts Link Type13: <http://docs.sun.com> 25

Ends Link Type14: SM 25

Starts Link Type13: <http://docs.sun.com> 25

Ends Link Type14: 25

Starts Link Type13: <http://docs.sun.com/coll/1695.1> 25

Ends Link Type14: 25

Starts Link Type13: <http://docs.sun.com/doc/820-0448> 25

Ends Link Type14: 25

Starts Link Type13: <http://docs.sun.com/doc/820-0887> 25

Ends Link Type14: 25

Starts Link Type13: <http://docs.sun.com/doc/819-3454> 26

Ends Link Type14: 26

Starts Link Type13: <http://docs.sun.com/doc/820-0080> 26

Ends Link Type14: 26

Starts Link Type13: <http://docs.sun.com/doc/820-0098> 26

Ends Link Type14: 26

Starts Link Type13: <http://docs.sun.com/doc/820-0584> 26

Ends Link Type14: 26

Starts Link Type13: <http://docs.sun.com/doc/820-0894> 26

Ends Link Type14: 26

Starts Link Type13: <http://docs.sun.com/doc/820-1587> 26

Ends Link Type14: 26

Starts Link Type13: <http://docs.sun.com/doc/819-4626> 26

Ends Link Type14: 26

Starts Link Type13: [java.sun.com](http://java.sun.com) 27

Ends Link Type14: , 27

Starts Link Type13: [www.sun.com](http://www.sun.com) 27

Ends Link Type14: , 27

Starts Link Type13: [developers.sun.com](http://developers.sun.com) 27

Ends Link Type14: ) 27

Starts Link Type13: <http://www.sun.com/software/download/> 27

Ends Link Type14: 27

Starts Link Type13: <http://www.sun.com/service/sunjavasystem/sjsservicessuite.html> 27

Ends Link Type14: 27

Starts Link Type13: <http://sunsolve.sun.com/> 27

Ends Link Type14: 27

Starts Link Type13: <http://developers.sun.com/prodtech/index.html> 27  
Ends Link Type14: 27

Starts Link Type13: <http://www.sun.com/software/javaenterprisesystem/index.html> 27  
Ends Link Type14: 27

Starts Link Type13: <http://www.sun.com/service/contacting> 27  
Ends Link Type14: . 27

Starts Link Type13: <http://docs.sun.com> 28  
Ends Link Type14: auf 28

Starts Link Type13: <http://docs.sun.com/doc/819-3588> 30  
Ends Link Type14: beschrieben 30

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>  
35  
Ends Link Type14: 35

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>  
36  
Ends Link Type14: 36

Starts Link Type13: <http://docs.sun.com/doc/820-0448> 43  
Ends Link Type14: dokumentiert 43

Starts Link Type13: <http://docs.sun.com/doc/820-0448> 43  
Ends Link Type14: dokumentiert 43

Starts Link Type13: <http://docs.sun.com/doc/819-2232> 44  
Ends Link Type14: beschrieben 44

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>  
47  
Ends Link Type14: 47

Starts Link Type13: <https://www.redhat.com/apps/download/> 47

Ends Link Type14: . 47

Starts Link Type13: <http://docs.sun.com/doc/820-0080> 65

Ends Link Type14: . 65

Starts Link Type13: <http://docs.sun.com/doc/820-0080> 68

Ends Link Type14: . 68

Starts Link Type13: <http://docs.sun.com/doc/820-0080> 68

Ends Link Type14: beschrieben 68

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnncr?a=view> 80

Ends Link Type14: ) 80

Starts Link Type13: <http://docs.sun.com/doc/819-4351> 80

Ends Link Type14: ) 80

Starts Link Type13: <http://docs.sun.com/doc/819-1405/6n3p13hac?a=view> 84

Ends Link Type14: ) 84

Starts Link Type13: <http://docs.sun.com/doc/819-4351> 84

Ends Link Type14: . 84

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnncr?a=view> 89

Ends Link Type14: . 89

Starts Link Type13: <http://docs.sun.com/doc/819-4351> 89

Ends Link Type14: . 89

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnncr?a=view> 92

Ends Link Type14: . 92

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnncr?a=view> 92

Ends Link Type14: . 92

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnncr?a=view> 94

Ends Link Type14: . 94



Starts Link Type13: <http://docs.sun.com/doc/819-4351> 94  
Ends Link Type14: . 94

Starts Link Type13: <http://docs.sun.com/doc/816-3381/6m9lratq9?a=view#gcpom> 94  
Ends Link Type14: . 94

Starts Link Type13: <http://docs.sun.com/doc/819-0420/6n2rlnnrc?a=view> 95  
Ends Link Type14: . 95

Starts Link Type13: <http://docs.sun.com/doc/817-7501> 105  
Ends Link Type14: . 105

Starts Link Type13: <http://docs.sun.com/doc/817-7500> 105  
Ends Link Type14: . 105

Starts Link Type13: <http://docs.sun.com/doc/817-7500> 106  
Ends Link Type14: . 106

Starts Link Type13: <http://docs.sun.com/doc/817-7501> 107  
Ends Link Type14: . 107

Starts Link Type13: <http://docs.sun.com/doc/820-0284> 111  
Ends Link Type14: . 111

Starts Link Type13: <http://docs.sun.com/doc/819-2232> 112  
Ends Link Type14: . 112

Starts Link Type13: <http://docs.sun.com/doc/819-2232> 112  
Ends Link Type14: . 112

Starts Link Type13: <http://docs.sun.com/doc/819-0994> 114  
Ends Link Type14: . 114

Starts Link Type13: <http://docs.sun.com/doc/819-0995> 122  
Ends Link Type14: . 122

Starts Link Type13: <http://docs.sun.com/doc/819-0994> 123

|             |         |                                                                                                                   |     |
|-------------|---------|-------------------------------------------------------------------------------------------------------------------|-----|
| Ends Link   | Type14: | .                                                                                                                 | 123 |
| Starts Link | Type13: | <a href="http://docs.sun.com/doc/819-2232">http://docs.sun.com/doc/819-2232</a>                                   | 130 |
| Ends Link   | Type14: | .                                                                                                                 | 130 |
| Starts Link | Type13: | <a href="http://docs.sun.com/doc/819-2232">http://docs.sun.com/doc/819-2232</a>                                   | 130 |
| Ends Link   | Type14: | .                                                                                                                 | 130 |
| Starts Link | Type13: | <a href="http://docs.sun.com/doc/819-0994">http://docs.sun.com/doc/819-0994</a>                                   | 132 |
| Ends Link   | Type14: | .                                                                                                                 | 132 |
| Starts Link | Type13: | <a href="http://docs.sun.com/doc/819-0995">http://docs.sun.com/doc/819-0995</a>                                   | 139 |
| Ends Link   | Type14: | .                                                                                                                 | 139 |
| Starts Link | Type13: | <a href="http://docs.sun.com/doc/819-0994">http://docs.sun.com/doc/819-0994</a>                                   | 139 |
| Ends Link   | Type14: | .                                                                                                                 | 139 |
| Starts Link | Type13: | <a href="http://docs.sun.com/doc/819-2629">http://docs.sun.com/doc/819-2629</a>                                   | 144 |
| Ends Link   | Type14: | .                                                                                                                 | 144 |
| Starts Link | Type13: | <a href="http://docs.sun.com/doc/819-2625">http://docs.sun.com/doc/819-2625</a>                                   | 153 |
| Ends Link   | Type14: | .                                                                                                                 | 153 |
| Starts Link | Type13: | <a href="http://docs.sun.com/doc/819-3283">http://docs.sun.com/doc/819-3283</a>                                   | 158 |
| Ends Link   | Type14: | .                                                                                                                 | 158 |
| Starts Link | Type13: | <a href="http://docs.sun.com/doc/819-4740/6n4r9qo7n?a=view">http://docs.sun.com/doc/819-4740/6n4r9qo7n?a=view</a> | 187 |
| Ends Link   | Type14: |                                                                                                                   | 187 |
| Starts Link | Type13: | <a href="http://docs.sun.com/819-4467/6n6k98brl?a=view">http://docs.sun.com/819-4467/6n6k98brl?a=view</a>         | 196 |
| Ends Link   | Type14: | .                                                                                                                 | 196 |
| Starts Link | Type13: | <a href="http://docs.sun.com/doc/819-4467">http://docs.sun.com/doc/819-4467</a>                                   | 203 |
| Ends Link   | Type14: | .                                                                                                                 | 203 |
| Starts Link | Type13: | <a href="http://docs.sun.com/doc/819-4467">http://docs.sun.com/doc/819-4467</a>                                   | 209 |
| Ends Link   | Type14: | )                                                                                                                 | 209 |

Starts Link Type13: <http://docs.sun.com/doc/819-4467> 210  
Ends Link Type14: ) 210

Starts Link Type13: <http://docs.sun.com/doc/819-4467> 212  
Ends Link Type14: . 212

Starts Link Type13: <http://docs.sun.com/doc/819-4467> 216  
Ends Link Type14: . 216

Starts Link Type13: <http://docs.sun.com/doc/819-3651> 220  
Ends Link Type14: . 220

Starts Link Type13: <http://docs.sun.com/doc/819-2232> 222  
Ends Link Type14: ) 222

Starts Link Type13: <http://docs.sun.com/doc/819-4733> 241  
Ends Link Type14: . 241

Starts Link Type13: <http://docs.sun.com/doc/819-4740> 241  
Ends Link Type14: ) 241

Starts Link Type13: <http://docs.sun.com/doc/819-3651> 242  
Ends Link Type14: [sowie](#) 242

Starts Link Type13: <http://docs.sun.com/doc/819-4737/6n6sao3ju?a=view> 242  
Ends Link Type14: . 242

Starts Link Type13: <http://docs.sun.com/doc/819-4737> 244  
Ends Link Type14: ) 244

Starts Link Type13: <http://docs.sun.com/doc/817-4640> 257  
Ends Link Type14: . 257

Starts Link Type13: <http://docs.sun.com/doc/817-4640> 259  
Ends Link Type14: . 259

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access> 270

Ends Link Type14: 270

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access> 272

Ends Link Type14: 272

Starts Link Type13: <http://docs.sun.com/doc/819-5492> 278

Ends Link Type14: . 278

Starts Link Type13: <http://docs.sun.com/doc/819-5494> 278

Ends Link Type14: . 278

Starts Link Type13: <http://docs.sun.com/doc/820-0360> 282

Ends Link Type14: . 282

Starts Link Type13: <http://docs.sun.com/doc/819-2232> 284

Ends Link Type14: ) 284

Starts Link Type13: <http://docs.sun.com/doc/820-0360> 287

Ends Link Type14: ) 287

Starts Link Type13: <http://docs.sun.com/doc/8197-0995> 293

Ends Link Type14: ) 293

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access> 296

Ends Link Type14: 296

Starts Link Type13: <http://docs.sun.com/doc/819-4675> 300

Ends Link Type14: ) 300

Starts Link Type13: <http://docs.sun.com/doc/819-4670> 300

Ends Link Type14: ) 300

Starts Link Type13: <http://docs.sun.com/doc/819-4670> 308

Ends Link Type14: ) 308

Ends Link Type14: http 321

Starts Link Type13: http://docs.sun.com/doc/819-7561 321

Starts Link Type13: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access  
325

Ends Link Type14: 325

Starts Link Type13: http://docs.sun.com/doc/819-4675 328

Ends Link Type14: ) 328

Starts Link Type13: http://docs.sun.com/doc/819-4670 335

Ends Link Type14: ) 335

Starts Link Type13: http://docs.sun.com/doc/820-0901/6n4l3f365?a=view 339

Ends Link Type14: zu 339

Starts Link Type13: http://docs.sun.com/doc/819-5030 342

Ends Link Type14: ) 342

Starts Link Type13: http://docs.sun.com/doc/819-7561 351

Ends Link Type14: . 351

Starts Link Type13: http://docs.sun.com/doc/819-0995 371

Ends Link Type14: . 371

Starts Link Type13: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access  
395

Ends Link Type14: 395

Starts Link Type13: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access  
398

Ends Link Type14: 398

Starts Link Type13: http://docs.sun.com/doc/819-0995 408

Ends Link Type14: . 408

Starts Link Type13: <http://docs.sun.com/doc/820-0901/6n4l3f365?a=view> 415

Ends Link Type14: ) 415

Starts Link Type13: <http://docs.sun.com/doc/819-5030> 417

Ends Link Type14: ) 417

Starts Link Type13: <http://docs.sun.com/doc/819-0995> 433

Ends Link Type14: ) 433

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>  
448

Ends Link Type14: 448

Starts Link Type13: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>  
450

Ends Link Type14: 450

Starts Link Type13: <http://docs.sun.com/doc/819-0995> 452

Ends Link Type14: ) 452

# List of Imported Graphics

|       |                                                                                                |     |
|-------|------------------------------------------------------------------------------------------------|-----|
| Dir & | Filename ..../Final/SJESUMG/820-0894/frame-src/figures/sha<br>redCompDependencies.eps. . . . . | 53  |
| Dir & | Filename ..../Final/SJESUMG/820-0894/frame-src/figures/red<br>undacyArch-AM.eps . . . . .      | 309 |
| Dir & | Filename ..../Final/SJESUMG/820-0894/frame-src/figures/red<br>undacyArch-AM.eps . . . . .      | 316 |
| Dir & | Filename ..../Final/SJESUMG/820-0894/frame-src/figures/red<br>undacyArch-PS.eps . . . . .      | 375 |
| Dir & | Filename ..../Final/SJESUMG/820-0894/frame-src/figures/red<br>undacyArch-PS-SRA.eps . . . . .  | 436 |





# List of Markers

12326: Head1: Who Should Use This Book 22  
48092: Head1: Conventions Used in This Book 22  
18195: Head1: Related Documentation 25  
20210: TableCaptionP: Sun ONE Application Server documentation roadmap 25  
39375: Head1: Accessing Sun Resources Online 27  
60891: Head1: Contacting Sun Technical Support 27  
94390: Head1: Related Third-Party Web Site References 28  
18048: Head1: Sun Welcomes Your Comments 28  
84055: ChapNumber: Chapter 8 29  
75725: ChapTitle: Planning for Upgrades 29  
64237: Head1: Java ES 5 Components 30  
94762: TableCaption: Table 1-1 Java ES Release 4 Product Components 30  
57330: Head2: Release 4 Shared Components 31  
32712: TableCaption: Table 1-2 Java ES Release 4 Shared Components 31  
53515: Head1: Upgrade Planning 33  
19005: Head3: Using the Upgrade Option of the Java ES Release 5 Installer 34  
26271: Head3: Performing a Fresh Install of the Component 35  
28798: Head3: Running a Component-specific Upgrade Script 35  
97158: Head3: Patching Existing Component Packages 35

|                                                                                     |    |
|-------------------------------------------------------------------------------------|----|
| 47583: Head2: Shared Component Upgrades                                             | 38 |
| 95877: Head1: The Upgrade Process                                                   | 39 |
| 87930: Head1: Upgrade Planning                                                      | 40 |
| 96243: Head2: Upgrade Dependencies                                                  | 41 |
| 96632: Head2: Upgrade Paths                                                         | 42 |
| 23983: TableCaptionWide: Table 1-4 Upgrade Paths to Java ES 2005Q4 (Release 4)      | 43 |
| 48275: Head2: Selective Upgrade or Upgrade All                                      | 45 |
| 77667: Head4: Component Redundancy                                                  | 46 |
| 99494: Head2: Operating System Issues                                               | 47 |
| 55223: Head3: Required Operating System Patches                                     | 47 |
| 65555: Head3: Dual Upgrades: Java ES and Operating System Software                  | 48 |
| 40351: Step1: 1. Backing up all Java ES configuration files and customizations.     | 48 |
| 49654: Head1: Java ES Component Dependencies                                        | 49 |
| 83054: Head2: Dependencies on Shared Components                                     | 49 |
| 86783: TableCaption: Table 1-2 Shared Component Dependencies of Product Componets   | 51 |
| 80863: FigureCaption: Figure 1-1 Shared Component Inter-dependencies                | 53 |
| 17819: Head3: Infrastructure Dependencies                                           | 55 |
| 26535: TableCaption: Table 1-3 Java ES Product Component Dependencies               | 56 |
| 53904: Head1: Preparing for Upgrades                                                | 60 |
| 88510: Head1: Special Cases                                                         | 64 |
| 13934: TableCaptionIndent: Table 6-3 Patches to Upgrade Messaging Server on Solaris | 64 |
| 22989: Head1: Java ES Release 5 and Solaris 10 Zones                                | 65 |
| 14735: Head2: Zone Support in the Java ES Release 5 Installer                       | 66 |
| 64070: Head2: Recommended Upgrade Practices                                         | 68 |
| 20835: Head2: Special Cases or Exceptions                                           | 69 |
| 66239: Head3: Product Component Special Cases                                       | 69 |
| 18126: Head3: Shared Component Special Cases                                        | 70 |
| 74193: ChapTitle: Upgrading System Components                                       | 71 |
| 89815: Procedure: % Applying Patches                                                | 72 |

|                                                                                                      |    |
|------------------------------------------------------------------------------------------------------|----|
| 79265: Head2: General Considerations                                                                 | 72 |
| 65274: Head2: Synchronizing Shared Components                                                        | 73 |
| 94148: Head2: Synchronizing All Shared Components                                                    | 74 |
| 40353: Head2: Solaris 10 Zone Considerations                                                         | 75 |
| 22759: Head1: Shared Component Upgrade Procedure                                                     | 77 |
| 24723: Head1: Special Upgrade Procedures                                                             | 77 |
| 81664: Head2: Upgrading J2SE Packages                                                                | 78 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                       | 79 |
| 38561: Head3: Common Agent Container (CACAO)                                                         | 80 |
| 68144: Step1: 1. If the current installation uses custom configuration settings (for example,        | 80 |
| 62821: Step1+: 5. Apply any custom configuration settings previously captured in Step 1 on           | 81 |
| 70527: Step1+: 8. FOOIf you upgraded J2SE to J2SE Version 5, run the rebuild-dependencies            | 81 |
| 47678: Head1: Manual Upgrade Procedures                                                              | 82 |
| 74193: ChapTitle: Upgrading System Components                                                        | 83 |
| 17885: Head1: Preparing for Upgrades                                                                 | 84 |
| 41290: Head1: Upgrading Shared Components                                                            | 84 |
| 34673: Procedure: % Patch Contents                                                                   | 84 |
| 73321: Head1: Message Queue Upgrade Information                                                      | 84 |
| 23459: Head1: Upgrading to Administration Server 5.2                                                 | 84 |
| 15541: Head2: About Java ES Release 4 Access Manager                                                 | 84 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                         | 85 |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0)<br>2005Q1 | 85 |
| 26267: Head2: Access Manager Data                                                                    | 86 |
| 18668: Head2: Sun Cluster Upgrade Strategy                                                           | 87 |
| 26959: Head2: Compatibility Issues                                                                   | 87 |
| 43330: Head2: Access Manager Dependencies                                                            | 87 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                        | 88 |
| 46384: Head2: Introduction                                                                           | 88 |

|                                                                                                      |     |
|------------------------------------------------------------------------------------------------------|-----|
| 93913: Head2: Full Access Manager Upgrade                                                            | 89  |
| 90948: Head2: Before You Upgrade                                                                     | 89  |
| 35243: Head4: Verify Current Version Information                                                     | 91  |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                       | 91  |
| 57504: Head4: Prepare the Cluster Node for Upgrade                                                   | 91  |
| 49065: Head4: Upgrade the Operating System                                                           | 92  |
| 44778: Head3: Upgrading Access Manager Dependencies                                                  | 92  |
| 39931: Head3: Obtain the Required Information                                                        | 93  |
| 49530: Head2: Access Manager Upgrade Procedures                                                      | 93  |
| 34640: Head4: Upgrade Considerations                                                                 | 93  |
| 19412: Head4: Upgrade Procedure                                                                      | 94  |
| 79521: Head2: Verifying the Upgrade                                                                  | 94  |
| 95616: Head2: Post-Upgrade Tasks                                                                     | 95  |
| 71706: Head2: Upgrade Rollback                                                                       | 95  |
| 44595: ChapTitle: Directory Proxy Server                                                             | 97  |
| 69359: Note: Note                                                                                    | 97  |
| 17885: Head1: Preparing for Upgrades                                                                 | 98  |
| 41290: Head1: Upgrading Shared Components                                                            | 98  |
| 34673: Procedure: % Patch Contents                                                                   | 98  |
| 73321: Head1: Message Queue Upgrade Information                                                      | 98  |
| 23459: Head1: Upgrading to Administration Server 5.2                                                 | 98  |
| 15541: Head2: About Java ES Release 4 Access Manager                                                 | 98  |
| 46544: Head2: Access Manager Upgrade Roadmap                                                         | 98  |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0)<br>2005Q1 | 99  |
| 26267: Head2: Access Manager Data                                                                    | 99  |
| 23608: Head2: Portal Server Upgrade Strategy                                                         | 99  |
| 26959: Head2: Compatibility Issues                                                                   | 100 |
| 43330: Head2: Access Manager Dependencies                                                            | 100 |

|                                                                                   |     |
|-----------------------------------------------------------------------------------|-----|
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                     | 100 |
| 46384: Head2: Introduction                                                        | 101 |
| 87678: Head2: Versions 3.1 Sun Cluster Geo Upgrade                                | 101 |
| 90948: Head2: Before You Upgrade                                                  | 102 |
| 30517: Head4: Verify Current Version Information                                  | 102 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs    | 102 |
| 94955: Head4: Prepare a Cluster for an Upgrade                                    | 102 |
| 86699: Step1: 1. Ensure that eh cluster is functioning properly.                  | 103 |
| 74111: Step1+: 3. Remove all application resource groups from protection groups.  | 103 |
| 44778: Head3: Upgrading Access Manager Dependencies                               | 103 |
| 32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared | 104 |
| 19147: Head3: Back Up Directory Server                                            | 104 |
| 39931: Head3: Obtain the Required Information                                     | 104 |
| 49530: Head2: Access Manager Upgrade Procedures                                   | 104 |
| 34640: Head4: Upgrade Considerations                                              | 104 |
| 19412: Head4: Upgrade Procedure                                                   | 105 |
| 34896: Step1: 1. Log in as root or become superuser.                              | 105 |
| 90067: Step1+: 2. Shut down Sun Cluster Geo 3.1.                                  | 105 |
| 74138: Step1+: 6. Install all the required Sun Cluster Geo patches.               | 106 |
| 61615: Step1+: 6. Re-start Release 5 Sun Cluster Geo.                             | 107 |
| 79521: Head2: Verifying the Upgrade                                               | 107 |
| 95616: Head2: Post-Upgrade Tasks                                                  | 107 |
| 71706: Head2: Upgrade Rollback                                                    | 108 |
| 74193: ChapTitle: Upgrading System Components                                     | 109 |
| 17885: Head1: Preparing for Upgrades                                              | 111 |
| 41290: Head1: Upgrading Shared Components                                         | 111 |
| 34673: Procedure: % Patch Contents                                                | 111 |
| 73321: Head1: Message Queue Upgrade Information                                   | 111 |
| 23459: Head1: Upgrading to Administration Server 5.2                              | 111 |

|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| 15541: Head2: About Java ES Release 4 Access Manager                                              | 111 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                      | 111 |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1 | 111 |
| 26267: Head2: Access Manager Data                                                                 | 113 |
| 23608: Head2: Portal Server Upgrade Strategy                                                      | 114 |
| 26959: Head2: Compatibility Issues                                                                | 114 |
| 43330: Head2: Access Manager Dependencies                                                         | 114 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                     | 116 |
| 46384: Head2: Introduction                                                                        | 116 |
| 93913: Head2: Full Access Manager Upgrade                                                         | 117 |
| 90948: Head2: Before You Upgrade                                                                  | 117 |
| 34684: Head4: Verify Current Version Information                                                  | 117 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                    | 117 |
| 44778: Head3: Upgrading Access Manager Dependencies                                               | 118 |
| 39931: Head3: Obtain the Required Information                                                     | 118 |
| 56542: Head4: Create DS Image (Optional)                                                          | 118 |
| 49530: Head2: Access Manager Upgrade Procedures                                                   | 118 |
| 34640: Head4: Upgrade Considerations                                                              | 119 |
| 19412: Head4: Upgrade Procedure                                                                   | 119 |
| 79283: Step1+: 7. Create a Directory Server instance.                                             | 122 |
| 28818: Step1+: 8. Migrate Release 4 data to the Release 5 Directory Server instance.              | 122 |
| 69359: Note: Note                                                                                 | 123 |
| 79521: Head2: Verifying the Upgrade                                                               | 124 |
| 95616: Head2: Post-Upgrade Tasks                                                                  | 124 |
| 71706: Head2: Upgrade Rollback                                                                    | 124 |
| 12921: Head1: Multiple Instance Upgrades                                                          | 124 |
| 41813: Head2: Upgrading Directory Server as a Data Service in a Cluster                           | 125 |
| 70823: Head1: Upgrading Directory Server from Java ES Release 3                                   | 125 |

|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| 19472: Head1: Upgrading Access Manager from Java ES Release 2                                     | 126 |
| 44595: ChapTitle: Directory Proxy Server                                                          | 127 |
| 17885: Head1: Preparing for Upgrades                                                              | 129 |
| 41290: Head1: Upgrading Shared Components                                                         | 129 |
| 34673: Procedure: % Patch Contents                                                                | 129 |
| 73321: Head1: Message Queue Upgrade Information                                                   | 129 |
| 23459: Head1: Upgrading to Administration Server 5.2                                              | 129 |
| 15541: Head2: About Java ES Release 4 Access Manager                                              | 129 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                      | 129 |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1 | 130 |
| 26267: Head2: Access Manager Data                                                                 | 131 |
| 23608: Head2: Portal Server Upgrade Strategy                                                      | 131 |
| 26959: Head2: Compatibility Issues                                                                | 132 |
| 43330: Head2: Access Manager Dependencies                                                         | 133 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                     | 134 |
| 46384: Head2: Introduction                                                                        | 134 |
| 93913: Head2: Full Access Manager Upgrade                                                         | 135 |
| 90948: Head2: Before You Upgrade                                                                  | 135 |
| 10228: Head4: Verify Current Version Information                                                  | 135 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                    | 135 |
| 44778: Head3: Upgrading Access Manager Dependencies                                               | 136 |
| 32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared                 | 136 |
| 39931: Head3: Obtain the Required Information                                                     | 136 |
| 49530: Head2: Access Manager Upgrade Procedures                                                   | 136 |
| 34640: Head4: Upgrade Considerations                                                              | 137 |
| 19412: Head4: Upgrade Procedure                                                                   | 137 |
| 86649: Step1+: 3. Shut down all Java ES components dependent on the Directory Server,             | 137 |
| 24850: Step1+: 4. Create a Directory Proxy Server instance.                                       | 139 |

|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| 26229: Step1+: 5. If desired, map Release 4 configuration attributes to the Release 5 Directory   | 139 |
| 79521: Head2: Verifying the Upgrade                                                               | 139 |
| 95616: Head2: Post-Upgrade Tasks                                                                  | 139 |
| 71706: Head2: Upgrade Rollback                                                                    | 140 |
| 12921: Head1: Multiple Instance Upgrades                                                          | 140 |
| 21426: Head1: Upgrading Directory Proxy Server from Java ES Release 3                             | 141 |
| 19472: Head1: Upgrading Access Manager from Java ES Release 2                                     | 142 |
| 74193: ChapTitle: Upgrading System Components                                                     | 143 |
| 17885: Head1: Preparing for Upgrades                                                              | 144 |
| 41290: Head1: Upgrading Shared Components                                                         | 144 |
| 34673: Procedure: % Patch Contents                                                                | 144 |
| 73321: Head1: Message Queue Upgrade Information                                                   | 144 |
| 23459: Head1: Upgrading to Administration Server 5.2                                              | 144 |
| 15541: Head2: About Java ES Release 4 Access Manager                                              | 144 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                      | 145 |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1 | 145 |
| 26267: Head2: Access Manager Data                                                                 | 145 |
| 23608: Head2: Portal Server Upgrade Strategy                                                      | 146 |
| 26959: Head2: Compatibility Issues                                                                | 146 |
| 63673: TableCaption: Table 7-3 Web Server Default Names                                           | 147 |
| 43330: Head2: Access Manager Dependencies                                                         | 147 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                     | 148 |
| 46384: Head2: Introduction                                                                        | 148 |
| 93913: Head2: Full Access Manager Upgrade                                                         | 149 |
| 90948: Head2: Before You Upgrade                                                                  | 149 |
| 23715: Head4: Verify Current Version Information                                                  | 149 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                    | 149 |
| 44778: Head3: Upgrading Access Manager Dependencies                                               | 150 |



|                                                                                               |     |
|-----------------------------------------------------------------------------------------------|-----|
| 19147: Head3: Back Up Directory Server                                                        | 150 |
| 39931: Head3: Obtain the Required Information                                                 | 150 |
| 49530: Head2: Access Manager Upgrade Procedures                                               | 150 |
| 34640: Head4: Upgrade Considerations                                                          | 150 |
| 19412: Head4: Upgrade Procedure                                                               | 153 |
| 91177: Step1+: 3. Stop all running instances of Web Server and the Administration Server.     | 153 |
| 89234: Step2+: e. If you choose configure now                                                 | 154 |
| 37914: Step2+: f. If you choose configure later:                                              | 155 |
| 54074: Step3+: II. Run the configureServer script.                                            | 157 |
| 91653: Step1+: 4. Start the Web Server Administration Server service.                         | 157 |
| 34612: Step1+: 5. Migrate Release 4 Web Server instances to Release 5 configurations.         | 157 |
| 17030: TableCaptionIndent: Table 6-4 wadm migrate-server Command Options and Arguments        | 158 |
| 59476: TableCaptionIndent: Table 6-5 wadm migrate-server Command Options                      | 159 |
| 92706: Step2+: c. If the target instance already exists as the default instance, then you can | 162 |
| 93575: TableCaptionIndent: Table 6-7 wadm deploy-cofig Command Options and Operands           | 162 |
| 71778: Step1+: 7. Start each Release 5 instance.                                              | 163 |
| 79521: Head2: Verifying the Upgrade                                                           | 163 |
| 95616: Head2: Post-Upgrade Tasks                                                              | 164 |
| 62873: Head4: Migrating Web Server 6.1 docroot content                                        | 164 |
| 71158: Head4: Migrating webdav collection information                                         | 165 |
| 10590: Head4: Migrating Log files                                                             | 165 |
| 85187: Head4: Migrating 3rd party NSAPI plug-ins                                              | 165 |
| 39918: Head4: Changing the search collection document root                                    | 166 |
| 70227: Head4: Customizing command-line scripts                                                | 167 |
| 71706: Head2: Upgrade Rollback                                                                | 167 |
| 19472: Head1: Upgrading Access Manager from Java ES Release 2                                 | 169 |
| 24060: Head1: Upgrading Web Server from Java ES Release 2                                     | 170 |
| 44595: ChapTitle: Directory Proxy Server                                                      | 171 |

|                                                                                                      |     |
|------------------------------------------------------------------------------------------------------|-----|
| 69359: Note: Note                                                                                    | 171 |
| 17885: Head1: Preparing for Upgrades                                                                 | 172 |
| 41290: Head1: Upgrading Shared Components                                                            | 172 |
| 34673: Procedure: % Patch Contents                                                                   | 172 |
| 73321: Head1: Message Queue Upgrade Information                                                      | 172 |
| 23459: Head1: Upgrading to Administration Server 5.2                                                 | 172 |
| 15541: Head2: About Java ES Release 4 Access Manager                                                 | 172 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                         | 172 |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0)<br>2005Q1 | 172 |
| 26267: Head2: Access Manager Data                                                                    | 173 |
| 23608: Head2: Portal Server Upgrade Strategy                                                         | 173 |
| 26959: Head2: Compatibility Issues                                                                   | 173 |
| 43330: Head2: Access Manager Dependencies                                                            | 173 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                        | 174 |
| 46384: Head2: Introduction                                                                           | 174 |
| 93913: Head2: Full Access Manager Upgrade                                                            | 175 |
| 90948: Head2: Before You Upgrade                                                                     | 175 |
| 77155: Head4: Verify Current Version Information                                                     | 175 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                       | 175 |
| 44778: Head3: Upgrading Access Manager Dependencies                                                  | 176 |
| 19147: Head3: Back Up Directory Server                                                               | 176 |
| 39931: Head3: Obtain the Required Information                                                        | 176 |
| 49530: Head2: Access Manager Upgrade Procedures                                                      | 176 |
| 19412: Head4: Upgrade Procedure                                                                      | 176 |
| 79521: Head2: Verifying the Upgrade                                                                  | 177 |
| 95616: Head2: Post-Upgrade Tasks                                                                     | 178 |
| 71706: Head2: Upgrade Rollback                                                                       | 178 |
| 12921: Head1: Multiple Instance Upgrades                                                             | 178 |

|                                                                                                      |     |
|------------------------------------------------------------------------------------------------------|-----|
| 74193: ChapTitle: Upgrading System Components                                                        | 179 |
| 17885: Head1: Preparing for Upgrades                                                                 | 181 |
| 41290: Head1: Upgrading Shared Components                                                            | 181 |
| 34673: Procedure: % Patch Contents                                                                   | 181 |
| 73321: Head1: Message Queue Upgrade Information                                                      | 181 |
| 23459: Head1: Upgrading to Administration Server 5.2                                                 | 181 |
| 15541: Head2: About Java ES Release 4 Access Manager                                                 | 181 |
| 36281: Head2: HADB Upgrade Roadmap                                                                   | 181 |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1    | 181 |
| 29711: Head2: HADB Data                                                                              | 182 |
| 23608: Head2: Portal Server Upgrade Strategy                                                         | 182 |
| 26959: Head2: Compatibility Issues                                                                   | 182 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                        | 184 |
| 46384: Head2: Introduction                                                                           | 184 |
| 93913: Head2: Full Access Manager Upgrade                                                            | 185 |
| 90948: Head2: Before You Upgrade                                                                     | 185 |
| 43372: Head4: Verify Current Version Information                                                     | 185 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                       | 185 |
| 44778: Head3: Upgrading Access Manager Dependencies                                                  | 186 |
| 19147: Head3: Back Up Directory Server                                                               | 186 |
| 39931: Head3: Obtain the Required Information                                                        | 186 |
| 49530: Head2: Access Manager Upgrade Procedures                                                      | 186 |
| 34640: Head4: Upgrade Considerations                                                                 | 186 |
| 32630: TableCaption: Table 2-2 Package Versions for Upgrading Shared Components on Solaris Platforms | 187 |
| 79521: Head2: Verifying the Upgrade                                                                  | 189 |
| 95616: Head2: Post-Upgrade Tasks                                                                     | 190 |
| 71706: Head2: Upgrade Rollback                                                                       | 191 |
| 88733: Head1: Upgrading HADB from Java ES Release 3                                                  | 192 |

|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| 74193: ChapTitle: Upgrading System Components                                                     | 193 |
| 17885: Head1: Preparing for Upgrades                                                              | 194 |
| 41290: Head1: Upgrading Shared Components                                                         | 194 |
| 34673: Procedure: % Patch Contents                                                                | 194 |
| 73321: Head1: Message Queue Upgrade Information                                                   | 194 |
| 23459: Head1: Upgrading to Administration Server 5.2                                              | 194 |
| 15541: Head2: About Java ES Release 4 Access Manager                                              | 194 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                      | 195 |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1 | 195 |
| 26267: Head2: Access Manager Data                                                                 | 196 |
| 20617: TableCaptionWide: Table 8-2 Message Queue Data Usage (Solaris OS)                          | 196 |
| 23608: Head2: Portal Server Upgrade Strategy                                                      | 197 |
| 26959: Head2: Compatibility Issues                                                                | 197 |
| 43330: Head2: Access Manager Dependencies                                                         | 197 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                     | 199 |
| 46384: Head2: Introduction                                                                        | 199 |
| 93913: Head2: Full Access Manager Upgrade                                                         | 200 |
| 90948: Head2: Before You Upgrade                                                                  | 200 |
| 67437: Head4: Verify Current Version Information                                                  | 200 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                    | 201 |
| 44778: Head3: Upgrading Access Manager Dependencies                                               | 201 |
| 32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared                 | 201 |
| 49130: Head4: Back Up Message Queue                                                               | 202 |
| 49530: Head2: Access Manager Upgrade Procedures                                                   | 202 |
| 79521: Head2: Verifying the Upgrade                                                               | 203 |
| 95616: Head2: Post-Upgrade Tasks                                                                  | 203 |
| 71706: Head2: Upgrade Rollback                                                                    | 204 |
| 12921: Head1: Multiple Instance Upgrades                                                          | 205 |

|                                                                                                                         |     |
|-------------------------------------------------------------------------------------------------------------------------|-----|
| 62991: Head1: Upgrading Message Queue from Java ES Release 3                                                            | 206 |
| 19472: Head1: Upgrading Access Manager from Java ES Release 2                                                           | 207 |
| 57508: Head2: Compatibility Issues                                                                                      | 208 |
| 12331: Head3: Protocol Compatibility                                                                                    | 208 |
| 28321: Head3: Broker Compatibility                                                                                      | 208 |
| 16480: Head3: Administered Objects                                                                                      | 209 |
| 95774: Head3: Administration Tool Compatibility                                                                         | 210 |
| 76701: Head3: Client Compatibility                                                                                      | 210 |
| 36929: Head2: Release 2 Message Queue Upgrade                                                                           | 210 |
| 86655: Head4: Verify Current Version Information (Solaris Systems)                                                      | 211 |
| 38575: Head4: Upgrade Message Queue Dependencies                                                                        | 211 |
| 90377: Head4: Back Up Message Queue                                                                                     | 212 |
| 60583: Head3: Upgrading Release 2 Message Queue (Solaris)                                                               | 212 |
| 59119: Head3: Upgrading Release 2 Message Queue (Linux)                                                                 | 214 |
| 95739: Step1+: 6. Migrate broker instance data using the following command:                                             | 215 |
| 45153: Step1+: 7. Run the mqupgrade script.                                                                             | 215 |
| 79935: Head3: Installing the sun-mq-compat Package                                                                      | 216 |
| 61002: Head3: Verifying the Message Queue Upgrade                                                                       | 216 |
| 54290: Head3: Post-Upgrade Tasks                                                                                        | 216 |
| 76601: Head3: Rolling Back the Upgrade                                                                                  | 217 |
| 74193: ChapTitle: Upgrading System Components                                                                           | 219 |
| 34104: Head1: Overview of Application Server Upgrades                                                                   | 221 |
| 15541: Head2: About Java ES Release 4 Access Manager                                                                    | 221 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                                            | 221 |
| 33786: TableCaptionWide: Table 11-2 Upgrade Paths to Java ES 5 (Release 5): Application Server Enterprise Edition 8.2   | 222 |
| 30603: TableCaptionWide: Table 11-3 Upgrade Paths for Application Server Versions Bundled with Solaris Operating System | 223 |
| 26267: Head2: Access Manager Data                                                                                       | 224 |
| 80642: TableCaptionWide: Table 10-3 Application Server Data Usage                                                       | 224 |

|                                                                                       |     |
|---------------------------------------------------------------------------------------|-----|
| 23608: Head2: Portal Server Upgrade Strategy                                          | 225 |
| 26959: Head2: Compatibility Issues                                                    | 225 |
| 43330: Head2: Access Manager Dependencies                                             | 225 |
| 16247: Note: Note                                                                     | 226 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                         | 227 |
| 46384: Head2: Introduction                                                            | 227 |
| 93913: Head2: Full Access Manager Upgrade                                             | 228 |
| 90948: Head2: Before You Upgrade                                                      | 228 |
| 88295: Head4: Verify Current Version Information                                      | 228 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs        | 229 |
| 44778: Head3: Upgrading Access Manager Dependencies                                   | 229 |
| 32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared     | 229 |
| 19147: Head3: Back Up Directory Server                                                | 230 |
| 39931: Head3: Obtain the Required Information                                         | 230 |
| 49530: Head2: Access Manager Upgrade Procedures                                       | 230 |
| 34640: Head4: Upgrade Considerations                                                  | 230 |
| 19412: Head4: Upgrade Procedure                                                       | 230 |
| 86649: Step1+: 3. Shut down all Java ES components dependent on the Directory Server, | 231 |
| 79521: Head2: Verifying the Upgrade                                                   | 232 |
| 95616: Head2: Post-Upgrade Tasks                                                      | 232 |
| 71706: Head2: Upgrade Rollback                                                        | 232 |
| 84321: Head1: Upgrading Application Server from Java ES Release 3                     | 233 |
| 19472: Head1: Upgrading Access Manager from Java ES Release 2                         | 234 |
| 20329: Head2: Introduction                                                            | 234 |
| 69047: Head2: Release 2 Application Server Upgrade                                    | 235 |
| 13674: Head4: Solaris Only: Manually Remove the Application Server Packages Bundled   | 236 |
| 26914: Head4: Verify Current Version Information                                      | 236 |
| 47180: Head4: Upgrade Application Server Dependencies                                 | 237 |
| 58344: Head4: Back Up Application Server Data                                         | 238 |

|                                                                                                  |     |
|--------------------------------------------------------------------------------------------------|-----|
| 98757: Head4: Obtain Required Configuration Information and Passwords                            | 238 |
| 81692: Head3: Upgrading Release 2 Application Server                                             | 238 |
| 16801: Head4: Upgrade Procedure                                                                  | 239 |
| 96166: Step1+: 2. If Java ES shared components have been upgraded to Release 5 (in particular    | 239 |
| 41022: Step1+: 3. Stop all Application Server and related processes.                             | 239 |
| 51295: Step1+: 3. Install Release 4 Application Server using the Java ES installer, choosing the | 239 |
| 25486: Step2+: c. Select Application Server from the component selection panel.                  | 240 |
| 23402: Step2+: d. Specify an installation directory different from that in which Release 2 was   | 240 |
| 40237: Step1+: 5. Perform the following post-install procedure:                                  | 240 |
| 53630: Step1+: 5. Run the asupgrade utility.                                                     | 242 |
| 86242: Step1+: 4. Identify both target and source installation directories, for example:         | 242 |
| 36701: Step1+: 9. Start the Domain Administration Server (DAS).                                  | 243 |
| 49085: Step1+: 10. Restart upgraded Application Server instances.                                | 243 |
| 23993: Head3: Upgrading Release 2 Application Server (Linux)                                     | 243 |
| 47178: Head3: Post-Upgrade Tasks                                                                 | 244 |
| 24193: Head4: Correct the Reference to JSS                                                       | 244 |
| 35947: Head4: Migration of Release 2 J2EE Components                                             | 244 |
| 95586: Head3: Rolling Back the Upgrade                                                           | 244 |
| 14447: Head2: 7. An Illustrative Example: Install Application Server in a Sparse Root Zone       | 245 |
| 44595: ChapTitle: Directory Proxy Server                                                         | 249 |
| 69359: Note: Note                                                                                | 249 |
| 17885: Head1: Preparing for Upgrades                                                             | 251 |
| 41290: Head1: Upgrading Shared Components                                                        | 251 |
| 34673: Procedure: % Patch Contents                                                               | 251 |
| 73321: Head1: Message Queue Upgrade Information                                                  | 251 |
| 23459: Head1: Upgrading to Administration Server 5.2                                             | 251 |
| 15541: Head2: About Java ES Release 4 Access Manager                                             | 251 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                     | 251 |

|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1 | 251 |
| 26267: Head2: Access Manager Data                                                                 | 252 |
| 23608: Head2: Portal Server Upgrade Strategy                                                      | 252 |
| 26959: Head2: Compatibility Issues                                                                | 252 |
| 43330: Head2: Access Manager Dependencies                                                         | 253 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                     | 254 |
| 46384: Head2: Introduction                                                                        | 254 |
| 93913: Head2: Full Access Manager Upgrade                                                         | 255 |
| 90948: Head2: Before You Upgrade                                                                  | 255 |
| 24956: Head4: Verify Current Version Information                                                  | 255 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                    | 256 |
| 44778: Head3: Upgrading Access Manager Dependencies                                               | 256 |
| 32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared                 | 256 |
| 19147: Head3: Back Up Directory Server                                                            | 257 |
| 39931: Head3: Obtain the Required Information                                                     | 257 |
| 49530: Head2: Access Manager Upgrade Procedures                                                   | 257 |
| 19412: Head4: Upgrade Procedure                                                                   | 257 |
| 61791: Step1+: 6. Upgrade and configure the Release 5 Service Registry.                           | 258 |
| 79521: Head2: Verifying the Upgrade                                                               | 260 |
| 95616: Head2: Post-Upgrade Tasks                                                                  | 261 |
| 71706: Head2: Upgrade Rollback                                                                    | 261 |
| 12921: Head1: Multiple Instance Upgrades                                                          | 262 |
| 74193: ChapTitle: Upgrading System Components                                                     | 263 |
| 17885: Head1: Preparing for Upgrades                                                              | 264 |
| 41290: Head1: Upgrading Shared Components                                                         | 264 |
| 34673: Procedure: % Patch Contents                                                                | 264 |
| 73321: Head1: Message Queue Upgrade Information                                                   | 264 |
| 23459: Head1: Upgrading to Administration Server 5.2                                              | 264 |



|                                                                                                      |     |
|------------------------------------------------------------------------------------------------------|-----|
| 15541: Head2: About Java ES Release 4 Access Manager                                                 | 264 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                         | 264 |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1    | 264 |
| 26267: Head2: Access Manager Data                                                                    | 265 |
| 23608: Head2: Portal Server Upgrade Strategy                                                         | 265 |
| 26959: Head2: Compatibility Issues                                                                   | 266 |
| 43330: Head2: Access Manager Dependencies                                                            | 266 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                        | 267 |
| 78545: Head2: Release 4 Web Proxy Server Upgrade                                                     | 268 |
| 88643: Head4: Verify Current Version Information                                                     | 268 |
| 93575: TableCaption: Table 11-3 Web Proxy Server Version Verification Outputs                        | 268 |
| 95242: Head4: Upgrade Web Proxy Server Dependencies                                                  | 269 |
| 49984: Head4: Back Up Web Proxy Server Data                                                          | 269 |
| 57637: Head4: Obtain Required Configuration Information and Passwords                                | 269 |
| 93656: Head3: Upgrading Release 4 Web Proxy Server (Solaris)                                         | 269 |
| 16936: TableCaptionIndent: Table 4-3 Patches to Upgrade Administration Server, Directory Server, and | 270 |
| 93280: Head4: Upgrade Procedure (Solaris)                                                            | 270 |
| 91177: Step1+: 3. Stop all running instances of Web Server and the Administration Server.            | 270 |
| 69482: Step2: a. Apply the Administration Server patches.                                            | 270 |
| 69739: Head3: Upgrading Web Server (Linux)                                                           | 271 |
| 14399: Head4: Upgrade Considerations (Linux)                                                         | 271 |
| 54062: TableCaptionIndent: Table 4-4 Patches to Upgrade Administration Server Directory Server, and  | 271 |
| 97364: Head4: Upgrade Procedure (Linux)                                                              | 271 |
| 84274: Head3: Rolling Back the Upgrade (Solaris)                                                     | 273 |
| 64922: Step1+: 2. Stop all running instances of Web Proxy Server and the Administration Server.      | 273 |
| 29419: Head1: Upgrading Web Proxy Server from Version 3.6                                            | 274 |

|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| 46384: Head2: Introduction                                                                        | 274 |
| 55960: Head2: Version 3.6 Web Proxy Server Upgrade                                                | 275 |
| 90948: Head2: Before You Upgrade                                                                  | 275 |
| 39518: Head4: Verify Current Version Information                                                  | 275 |
| 29676: TableCaption: Table 11-6 Web Proxy Server Version Verification Outputs                     | 275 |
| 44778: Head3: Upgrading Access Manager Dependencies                                               | 276 |
| 19147: Head3: Back Up Directory Server                                                            | 276 |
| 39931: Head3: Obtain the Required Information                                                     | 276 |
| 49530: Head2: Access Manager Upgrade Procedures                                                   | 276 |
| 34640: Head4: Upgrade Considerations                                                              | 276 |
| 19412: Head4: Upgrade Procedure                                                                   | 276 |
| 97789: Step2+: d. Click the Migrate button.                                                       | 278 |
| 79521: Head2: Verifying the Upgrade                                                               | 278 |
| 95616: Head2: Post-Upgrade Tasks                                                                  | 278 |
| 71706: Head2: Upgrade Rollback                                                                    | 279 |
| 74193: ChapTitle: Upgrading System Components                                                     | 281 |
| 17885: Head1: Preparing for Upgrades                                                              | 282 |
| 41290: Head1: Upgrading Shared Components                                                         | 282 |
| 34673: Procedure: % Patch Contents                                                                | 282 |
| 73321: Head1: Message Queue Upgrade Information                                                   | 282 |
| 23459: Head1: Upgrading to Administration Server 5.2                                              | 282 |
| 15541: Head2: About Java ES Release 4 Access Manager                                              | 282 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                      | 283 |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0) 2005Q1 | 283 |
| 26267: Head2: Access Manager Data                                                                 | 285 |
| 22953: TableCaptionWide: Table 11-2 Access Manager Data Usage                                     | 285 |
| 23608: Head2: Portal Server Upgrade Strategy                                                      | 286 |
| 26959: Head2: Compatibility Issues                                                                | 286 |

|                                                                                                    |     |
|----------------------------------------------------------------------------------------------------|-----|
| 43330: Head2: Access Manager Dependencies                                                          | 287 |
| 23141: TableCaption: Table 11-3 Web Container Upgrade Scenarios for Access Manager Upgrade         | 288 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                      | 290 |
| 46384: Head2: Introduction                                                                         | 290 |
| 93913: Head2: Full Access Manager Upgrade                                                          | 291 |
| 90948: Head2: Before You Upgrade                                                                   | 291 |
| 23760: Head4: Verify Current Version Information                                                   | 292 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                     | 292 |
| 44778: Head3: Upgrading Access Manager Dependencies                                                | 292 |
| 32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared                  | 293 |
| 19147: Head3: Back Up Directory Server                                                             | 293 |
| 27083: Head4: Back Up Release 4 Access Manager Configuration Information                           | 293 |
| 61806: Head2: Backing up Web Container Files                                                       | 294 |
| 53828: Head3: Backing Up Access Manager Release 3                                                  | 294 |
| 81910: Head4: Back Up Custom Localization Files                                                    | 295 |
| 39931: Head3: Obtain the Required Information                                                      | 295 |
| 49530: Head2: Access Manager Upgrade Procedures                                                    | 295 |
| 16910: Step1+: 2. Remove the Java ES Release 4 Version of Access Manager. Use the                  | 295 |
| 31541: Step1+: 7. Update the directory structure and schema. Use the amupgrade script.             | 296 |
| 30579: Step1+: 3. Upgrade mobile access software.                                                  | 296 |
| 13934: TableCaptionIndent: Table 6-3 Patches to Upgrade Messaging Server on Solaris                | 296 |
| 93040: Head3: Remove the Java ES Release 3 Version of Access Manager                               | 297 |
| 35655: Step1+: 2. If the upgrade to Release 5 needs to be localized, remove Release 4 localization | 298 |
| 24529: Step2: a. Check for localization packages.                                                  | 298 |
| 78467: Head3: Install Java ES Release 4 Version of Access Manager                                  | 299 |
| 91206: Head3: Re-apply Customized JSPs for Access Manager                                          | 300 |
| 49148: Head3: Re-deploy Access Manager Web Applications                                            | 300 |
| 62405: Step2+: d. If Access Manager is deployed in Release 5 Web Server, disable all Java ES       | 301 |

15015: Head3: Upgrade the Directory Schema 305

93497: Step1+: 2. Run the amupgrade script. 306

79521: Head2: Verifying the Upgrade 307

95616: Head2: Post-Upgrade Tasks 307

78316: Head4: Migrating to Realm Mode 308

55903: Head4: Security Assertion Markup Language 308

97810: Head4: Update Patches 308

71706: Head2: Upgrade Rollback 308

12921: Head1: Multiple Instance Upgrades 309

31938: FigureCaption: Figure 14-1 Typical Deployment Architecture for Multiple Access Manager Instances 309

66117: Head2: Access Manager SDK-only Upgrades 311

94723: Head2: Access Manager SDK Upgrade Procedures 313

62989: Head2: Verifying the Access Manager SDK Upgrade 313

56774: Head1: Upgrading Access Manager from Java ES Release 3 315

23590: Head2: Release 3 Access Manager Upgrade 315

59477: Head2: Multiple Instance Release 3 Access Manager Upgrade 315

16251: FigureCaption: Figure 14-2 Example Deployment Architecture for Multiple Access Manager Instances 316

19472: Head1: Upgrading Access Manager from Java ES Release 2 320

19884: Head2: Pre-Upgrade Tasks 320

24162: Head3: Upgrade Access Manager Dependencies 321

95303: Head3: Upgrade Directory Schema 321

21940: Head3: Re-index the Directory 322

35795: Head2: Release 2 Access Manager Upgrade 323

24401: Head3: Upgrading Messaging Server (Solaris) 323

60105: Head3: Upgrading Access Manager: Application Server Web Container 323

77541: Step1: 1. Upgrade Access Manager mobile access software. 325

83145: Step1+: 2. Remove the Java ES Release 2 Version of Access Manager. 326

18497: Step1+: 3. If the upgrade to Release 5 needs to be localized, remove the Release 2 327

|                                                                                                       |     |
|-------------------------------------------------------------------------------------------------------|-----|
| 63603: Step1+: 4. Install the Java ES Release 5 Version of Access Manager.                            | 327 |
| 12988: Step1+: 6. Check that Directory Server is running.                                             | 329 |
| 49202: Step1+: 7. Start the following Application Server instances:                                   | 329 |
| 78174: Step1+: 8. Undeploy Access Manager, reconfigure, and re-deploy into the Application            | 329 |
| 13868: Step1+: 9. Verify that Access Manager classpath-suffix and server-classpath                    | 332 |
| 72142: Step1+: 12. Update the directory structure and schema.                                         | 332 |
| 32139: Step1+: 10. Stop the Domain Administration Server (DAS) and node agent that were               | 334 |
| 61227: Step1+: 11. Restart the the Domain Administration Server (DAS), node agent, and server         | 334 |
| 86085: Head2: Multiple Instance Upgrade                                                               | 335 |
| 74193: ChapTitle: Upgrading System Components                                                         | 337 |
| 17885: Head1: Preparing for Upgrades                                                                  | 339 |
| 41290: Head1: Upgrading Shared Components                                                             | 339 |
| 34673: Procedure: % Patch Contents                                                                    | 339 |
| 73321: Head1: Message Queue Upgrade Information                                                       | 339 |
| 23459: Head1: Upgrading to Administration Server 5.2                                                  | 339 |
| 15541: Head2: About Java ES Release 4 Access Manager                                                  | 339 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                          | 339 |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0)<br>2005Q1  | 340 |
| 26267: Head2: Access Manager Data                                                                     | 340 |
| 23608: Head2: Portal Server Upgrade Strategy                                                          | 341 |
| 26959: Head2: Compatibility Issues                                                                    | 342 |
| 43330: Head2: Access Manager Dependencies                                                             | 342 |
| 49667: Head3: Selective Upgrade Issues                                                                | 344 |
| 77725: TableCaptionIndent: Table 17-5 Portal Server Upgrade Scenarios for Different Web<br>Containers | 345 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                         | 346 |
| 46384: Head2: Introduction                                                                            | 346 |
| 93913: Head2: Full Access Manager Upgrade                                                             | 348 |

|                                                                                                     |     |
|-----------------------------------------------------------------------------------------------------|-----|
| 90948: Head2: Before You Upgrade                                                                    | 349 |
| 86427: Head4: Verify Current Version Information                                                    | 349 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                      | 349 |
| 44778: Head3: Upgrading Access Manager Dependencies                                                 | 349 |
| 32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared                   | 350 |
| 39931: Head3: Obtain the Required Information                                                       | 351 |
| 67657: TableCaptionIndent: Table 17-5 Information Requested by psupgrade Script for Various Upgrade | 351 |
| 16146: Head4: Back Up Release 4 Portal Server Configuration Information                             | 352 |
| 60248: Head4: Note Java Virtual Machine (JVM) Settings                                              | 352 |
| 24690: Head4: Remove Configuration for Load Balancer                                                | 354 |
| 57135: Head4: Remove Configuration for Directory Proxy Server                                       | 355 |
| 49530: Head2: Access Manager Upgrade Procedures                                                     | 355 |
| 34640: Head4: Upgrade Considerations                                                                | 355 |
| 19412: Head4: Upgrade Procedure                                                                     | 356 |
| 56828: Step1+: 3. If not already running, start Portal Server by starting the web container to      | 357 |
| 41845: Step1+: 4. Set two environment variables needed by the psupgrade script:                     | 357 |
| 89837: Step1+: 4. Run the psupgrade script.                                                         | 357 |
| 69739: Head3: Upgrading Web Server (Linux)                                                          | 360 |
| 14399: Head4: Upgrade Considerations (Linux)                                                        | 360 |
| 97364: Head4: Upgrade Procedure (Linux)                                                             | 360 |
| 94383: Step1+: 5. If not already running, start Portal Server by starting the web container to      | 361 |
| 14016: Step1+: 8. Run the psupgrade script from the Java ES Release 5 distribution.                 | 362 |
| 79521: Head2: Verifying the Upgrade                                                                 | 363 |
| 95616: Head2: Post-Upgrade Tasks                                                                    | 364 |
| 95668: Head4: Migrate Custom web-src Data                                                           | 364 |
| 27601: Head4: Redeploy Custom Portlet Applications                                                  | 365 |
| 63225: Head4: Migrate Customized Portlet Applications                                               | 365 |
| 13908: Step1+: 2. Locate the filesharing portlet application.                                       | 366 |

|                                                                                                         |     |
|---------------------------------------------------------------------------------------------------------|-----|
| 69773: Step1+: 5. Redeploy the filesharing portlet application.                                         | 366 |
| 59153: Step2+: c. Go to the following directory (depending on web container):                           | 366 |
| 98193: Step2+: d. Open the sun-web.xml file and add the following line just before the last             | 367 |
| 80829: Head4: Correct Access to Search Server                                                           | 367 |
| 46403: Head4: Restore Configuration for Directory Proxy Server                                          | 367 |
| 75598: Head3: Manually Register Portal Server Secure Remote Access                                      | 368 |
| 13217: Head3: Enabling URLScrapper Channel                                                              | 368 |
| 78603: Step1+: 4. Locate the entire XML portion starting from:                                          | 368 |
| 66019: Head4: Logout Page                                                                               | 371 |
| 71706: Head2: Upgrade Rollback                                                                          | 371 |
| 79353: Head3: Rolling Back the Upgrade (Linux)                                                          | 373 |
| 12921: Head1: Multiple Instance Upgrades                                                                | 373 |
| 31938: FigureCaption: Figure 14-1 Typical Deployment Architecture for Multiple Access Manager Instances | 375 |
| 72247: Step1: 1. If you are upgrading Release 4 Access Manager to Release 5, perform a rolling          | 375 |
| 16198: Step2+: c. Upgrade Access Manager SDK 1B to Release 5.                                           | 376 |
| 45043: Step2+: d. Upgrade Portal Server 1 to Release 5.                                                 | 376 |
| 32637: Head1: Upgrading Portal Server from Java ES Release 3                                            | 378 |
| 24651: Head2: Release 3 Pre-Upgrade Task: Upgrading Portal Server Dependencies                          | 378 |
| 36852: Head2: Release 3 Portal Server Upgrade                                                           | 379 |
| 19573: Head2: Release 3 Post-Upgrade Tasks                                                              | 379 |
| 76092: Head3: Subscribing a Discussion                                                                  | 379 |
| 88282: Head2: Multiple Instance Upgrades                                                                | 380 |
| 73569: Head1: Upgrading Portal Server from Java ES Release 2                                            | 381 |
| 33156: Head2: Pre-Upgrade Tasks                                                                         | 381 |
| 79129: Head2: Upgrading Release 2 Portal Server                                                         | 382 |
| 24401: Head3: Upgrading Messaging Server (Solaris)                                                      | 382 |
| 60105: Head3: Upgrading Access Manager: Application Server Web Container                                | 383 |
| 47403: Step1+: 4. If not already running, start Portal Server by starting the web container to          | 384 |

|                                                                                                    |     |
|----------------------------------------------------------------------------------------------------|-----|
| 30452: Step1+: 9. Run the psupgrade script from the Java ES Release 5 distribution.                | 385 |
| 32139: Step1+: 10. Stop the Domain Administration Server (DAS) and node agent that were            | 386 |
| 64787: Head2: Release 2 Post-Upgrade Tasks                                                         | 387 |
| 78956: Head3: Single Sign-on Configuration                                                         | 387 |
| 26757: Head3: Enabling the URLScrapper Channel                                                     | 391 |
| 65685: Head3: Delete Gateway Service Entry                                                         | 391 |
| 99094: Head2: Multiple Instance Upgrades                                                           | 391 |
| 18474: Head1: Upgrading Portal Server from the Interim Feature                                     | 392 |
| 20105: Head2: Introduction                                                                         | 392 |
| 71392: TableCaptionIndent: Table 17-6 Patches to Upgrade Portal Server IFR to Release 5 on Solaris | 392 |
| 66302: Head2: Portal Server IFR 7.0 Upgrade                                                        | 393 |
| 20319: Head3: Pre-Upgrade Tasks                                                                    | 393 |
| 86903: Head3: Upgrading Portal Server IFR 7.0 (Solaris)                                            | 394 |
| 93710: Head4: Upgrade Considerations (Solaris)                                                     | 394 |
| 15809: Head4: IFR 7 Upgrade Procedure (Solaris)                                                    | 394 |
| 56479: Step1+: 4. If not already running, start Portal Server by starting the web container to     | 395 |
| 21387: Step1+: 4. Obtain the required patch, based on Table 17-6.                                  | 395 |
| 69482: Step2: a. Apply the Administration Server patches.                                          | 395 |
| 10785: Step1+: 6. Confirm that the patch upgrade was successful:                                   | 395 |
| 12340: Step1+: 11. Run the psupgrade script.                                                       | 396 |
| 42263: Head3: Upgrading IFR 7 Portal Server (Linux)                                                | 396 |
| 59024: Head3: Upgrading Portal Server IFR 7.0 (Linux)                                              | 397 |
| 77944: Step1+: 4. If not already running, start Portal Server by starting the web container to     | 397 |
| 30186: Step1+: 11. Run the psupgrade script.                                                       | 399 |
| 25105: Head3: Verifying the Upgrade                                                                | 400 |
| 22792: Head3: Post-Upgrade Tasks                                                                   | 400 |
| 96066: Head4: Configuration of Common Agent Container Shared Component                             | 401 |
| 48904: Head4: Enabling the Java ES Monitoring Framework                                            | 402 |



|                                                                                                      |     |
|------------------------------------------------------------------------------------------------------|-----|
| 84419: Head4: Upgrade in Application Server Web Container                                            | 402 |
| 19754: Head4: Upgrade in Web Server Web Container                                                    | 404 |
| 82941: Step1+: 4. Delete the Portal Server IFR instance.                                             | 405 |
| 82315: Head4: Redeploy Custom Portlet Applications                                                   | 405 |
| 41727: Head4: Migrate Customized Portlet Applications                                                | 405 |
| 72947: Head4: Manual Migration of Struts-based Portlets                                              | 407 |
| 78568: Head3: Rolling Back the Upgrade (Solaris)                                                     | 408 |
| 91734: Head3: Rolling Back the Upgrade (Linux)                                                       | 410 |
| 94840: Head2: Multiple Instance Upgrades                                                             | 410 |
| 74193: ChapTitle: Upgrading System Components                                                        | 413 |
| 17885: Head1: Preparing for Upgrades                                                                 | 415 |
| 41290: Head1: Upgrading Shared Components                                                            | 415 |
| 34673: Procedure: % Patch Contents                                                                   | 415 |
| 73321: Head1: Message Queue Upgrade Information                                                      | 415 |
| 23459: Head1: Upgrading to Administration Server 5.2                                                 | 415 |
| 15541: Head2: About Java ES Release 4 Access Manager                                                 | 415 |
| 46544: Head2: Access Manager Upgrade Roadmap                                                         | 416 |
| 57034: TableCaptionWide: Table 3-1 Upgrade Paths to Java ES Release 4 Access Manager (7.0)<br>2005Q1 | 416 |
| 26267: Head2: Access Manager Data                                                                    | 416 |
| 23608: Head2: Portal Server Upgrade Strategy                                                         | 417 |
| 26959: Head2: Compatibility Issues                                                                   | 417 |
| 43330: Head2: Access Manager Dependencies                                                            | 418 |
| 23142: Head3: Selective Upgrade Issues                                                               | 419 |
| 18756: Head1: Upgrading Access Manager from Java ES Release 3                                        | 420 |
| 46384: Head2: Introduction                                                                           | 420 |
| 21678: Bullet1: • Upgrade Dependencies. While Portal Server has dependencies on a number             | 421 |
| 93913: Head2: Full Access Manager Upgrade                                                            | 422 |
| 90948: Head2: Before You Upgrade                                                                     | 422 |

|                                                                                                                    |     |
|--------------------------------------------------------------------------------------------------------------------|-----|
| 47076: Head4: Verify Current Version Information                                                                   | 422 |
| 29469: TableCaption: Table 6-3 Application Server version verification outputs                                     | 423 |
| 44778: Head3: Upgrading Access Manager Dependencies                                                                | 423 |
| 32303: Step1: 1. Shared Components. Instructions for synchronizing Java ES shared                                  | 424 |
| 43322: Head4: Back Up Release 4 Portal Server Secure Remote Access Configuration                                   | 424 |
| 24690: Head4: Remove Configuration for Load Balancer                                                               | 424 |
| 57135: Head4: Remove Configuration for Directory Proxy Server                                                      | 425 |
| 39931: Head3: Obtain the Required Information                                                                      | 426 |
| 49530: Head2: Access Manager Upgrade Procedures                                                                    | 426 |
| 34640: Head4: Upgrade Considerations                                                                               | 426 |
| 19412: Head4: Upgrade Procedure                                                                                    | 427 |
| 92871: Step1+: 3. Stop any instances of the Gateway, Rewriter Proxy, or Netlet Proxy that are                      | 427 |
| 41845: Step1+: 4. Set two environment variables needed by the psupgrade script:                                    | 427 |
| 35135: Step1+: 8. Run the psupgrade script from the Java ES Release 5 distribution.                                | 428 |
| 69739: Head3: Upgrading Web Server (Linux)                                                                         | 429 |
| 14399: Head4: Upgrade Considerations (Linux)                                                                       | 429 |
| 97364: Head4: Upgrade Procedure (Linux)                                                                            | 429 |
| 17364: Step1+: 8. Run the psupgrade script from the Java ES Release 5 distribution.                                | 430 |
| 79521: Head2: Verifying the Upgrade                                                                                | 431 |
| 95616: Head2: Post-Upgrade Tasks                                                                                   | 431 |
| 92269: Head4: Restore Configuration for Load Balancer                                                              | 431 |
| 44296: Step1+: 2. Set the following parameters in the<br>PortalServer7Config-base/platform.conf.default file:      | 431 |
| 90189: Step1+: 3. Set the following parameter in the<br>PortalServer7Config-base/GWConfig-default.properties file. | 432 |
| 15493: Head4: Restore Configuration for Directory Proxy Server                                                     | 432 |
| 71826: Head4: Delete Release 4 Localized Providers                                                                 | 432 |
| 71706: Head2: Upgrade Rollback                                                                                     | 433 |
| 79353: Head3: Rolling Back the Upgrade (Linux)                                                                     | 435 |
| 12921: Head1: Multiple Instance Upgrades                                                                           | 435 |

|                                                                                                         |     |
|---------------------------------------------------------------------------------------------------------|-----|
| 31938: FigureCaption: Figure 14-1 Typical Deployment Architecture for Multiple Access Manager Instances | 436 |
| 19021: Step1: 1. If you are upgrading Release 4 Access Manager to Release 5, perform a rolling          | 437 |
| 92027: Step1+: 3. Upgrade Portal Server 1.                                                              | 437 |
| 16198: Step2+: c. Upgrade Access Manager SDK 1B to Release 5.                                           | 437 |
| 45043: Step2+: d. Upgrade Portal Server 1 to Release 5.                                                 | 437 |
| 55497: Step2+: b. Upgrade Access Manager SDK 1A to Release 5.                                           | 438 |
| 80225: Step2+: c. Upgrade Gateway 1 to Release 5.                                                       | 438 |
| 32637: Head1: Upgrading Portal Server from Java ES Release 3                                            | 441 |
| 57991: Head2: Upgrading Portal Server Secure Remote Access Dependencies                                 | 441 |
| 70112: Head2: Upgrading Release 3 Portal Server Secure Remote Access                                    | 442 |
| 15015: Head2: Multiple Instance Upgrades                                                                | 442 |
| 73569: Head1: Upgrading Portal Server from Java ES Release 2                                            | 443 |
| 61860: Head2: Release 2 Pre-Upgrade Tasks                                                               | 443 |
| 43743: Head3: Upgrading Portal Server Dependencies.                                                     | 443 |
| 65685: Head3: Delete Gateway Service Entry                                                              | 444 |
| 79129: Head2: Upgrading Release 2 Portal Server                                                         | 444 |
| 76339: Head2: Release 2 Post-Upgrade Tasks                                                              | 445 |
| 64945: Head3: Set PS Domain                                                                             | 445 |
| 25975: Head2: Multiple Instance Upgrades                                                                | 445 |
| 18474: Head1: Upgrading Portal Server from the Interim Feature                                          | 446 |
| 20105: Head2: Introduction                                                                              | 446 |
| 33932: TableCaption: Table 16-5 Patches to Upgrade Portal Server Secure Remote Access IFR to Release 5  | 446 |
| 66302: Head2: Portal Server IFR 7.0 Upgrade                                                             | 447 |
| 20319: Head3: Pre-Upgrade Tasks                                                                         | 447 |
| 86903: Head3: Upgrading Portal Server IFR 7.0 (Solaris)                                                 | 447 |
| 21387: Step1+: 4. Obtain the required patch, based on Table 17-6.                                       | 448 |
| 69482: Step2: a. Apply the Administration Server patches.                                               | 448 |
| 10785: Step1+: 6. Confirm that the patch upgrade was successful:                                        | 448 |

|                                                                 |     |
|-----------------------------------------------------------------|-----|
| 19861: Step1+: 10. Run the psupgrade script.                    | 449 |
| 59024: Head3: Upgrading Portal Server IFR 7.0 (Linux)           | 449 |
| 83840: Step1+: 10. Run the psupgrade script.                    | 451 |
| 25105: Head3: Verifying the Upgrade                             | 451 |
| 22792: Head3: Post-Upgrade Tasks                                | 452 |
| 78568: Head3: Rolling Back the Upgrade (Solaris)                | 452 |
| 91734: Head3: Rolling Back the Upgrade (Linux)                  | 452 |
| 94840: Head2: Multiple Instance Upgrades                        | 453 |
| 30617: ChapNumberA: Appendix B                                  | 455 |
| 68152: ChapTitleA: Previous Java Enterprise System Releases     | 455 |
| 33080: Head1: Java ES 2003Q4                                    | 456 |
| 72105: Head3: Sun ONE Administration Server 5.2                 | 456 |
| 44958: Head3: Sun ONE Application Server 7, Update 1            | 456 |
| 97608: Head3: Sun ONE Calendar Server 6.0                       | 456 |
| 71661: Head3: Sun ONE Directory Server 5.2                      | 456 |
| 25410: Head3: Sun ONE Directory Proxy Server 5.2                | 456 |
| 51933: Head3: Sun ONE Identity Server 6.1                       | 456 |
| 67613: Head3: Sun ONE Instant Messaging 6.1                     | 456 |
| 30041: Head3: Sun ONE Message Queue 3.0.1 Service Pack 2        | 456 |
| 80042: Head3: Sun ONE Messaging Server 6.0                      | 456 |
| 92032: Head3: Sun ONE Portal Server 6.2                         | 456 |
| 18544: Head3: Sun ONE Portal Server, Secure Remote Access 6.2   | 456 |
| 40736: Head3: Sun ONE Web Server 6.1                            | 456 |
| 18017: Head1: Java ES 2004Q2                                    | 458 |
| 18631: Head1: Java ES 2005Q1                                    | 461 |
| 98851: Head2: What Are the Component Products?                  | 461 |
| 52849: Head2: What Are the Shared Components?                   | 464 |
| 46890: Head1: How Do I Get the Java Enterprise System Software? | 465 |
| 39670: Head1: Java ES 2005Q4 (Release 4)                        | 466 |

|                                           |     |
|-------------------------------------------|-----|
| 62421: Head2: Release 4 Shared Components | 469 |
| 81363: Head1: Java ES 2006Q4 (Release 5)  | 471 |
| 80020: Head2: Release 5 Shared Components | 474 |



# List of External Cross-References

|                |                                                                            |    |
|----------------|----------------------------------------------------------------------------|----|
| Dir & Filename | applicationSvr.fm (Head2: Release 2 Application Server Upgrade) . . . . .  | 34 |
| Dir & Filename | sharedComps.fm (Head2: Synchronizing All Shared Components) . . . . .      | 39 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .           | 54 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .           | 60 |
| Dir & Filename | sunCluster.fm (ChapTitle: Upgrading System Components) . . . . .           | 61 |
| Dir & Filename | sunCluster-Geo.fm (ChapTitle: Directory Proxy Server) . . . . .            | 61 |
| Dir & Filename | directorySvr.fm (ChapTitle: Upgrading System Components) . . . . .         | 61 |
| Dir & Filename | directoryProxySvr.fm (ChapTitle: Directory Proxy Server) . . . . .         | 61 |
| Dir & Filename | webSvr.fm (ChapTitle: Upgrading System Components) . . . . .               | 61 |
| Dir & Filename | javaDB.fm (ChapTitle: Directory Proxy Server) . . . . .                    | 62 |
| Dir & Filename | highAvailabilityDB.fm (ChapTitle: Upgrading System Components) . . . .     | 62 |
| Dir & Filename | messageQueue.fm (ChapTitle: Upgrading System Components) . . . . .         | 62 |
| Dir & Filename | applicationSvr.fm (ChapTitle: Upgrading System Components) . . . . .       | 62 |
| Dir & Filename | serviceRegistry.fm (ChapTitle: Directory Proxy Server) . . . . .           | 62 |
| Dir & Filename | webProxySvr.fm (ChapTitle: Upgrading System Components) . . . . .          | 62 |
| Dir & Filename | accessMgr.fm (ChapTitle: Upgrading System Components). . . . .             | 63 |
| Dir & Filename | portalSvr.fm (ChapTitle: Upgrading System Components) . . . . .            | 63 |
| Dir & Filename | portalSvrSRA.fm (ChapTitle: Upgrading System Components). . . . .          | 63 |
| Dir & Filename | portalSvr.fm (Head1: Upgrading Portal Server from the Interim Feature) . . | 65 |

|                |                                                                                                            |     |
|----------------|------------------------------------------------------------------------------------------------------------|-----|
| Dir & Filename | sharedComps.fm (Head2: Synchronizing All Shared Components) . . . . .                                      | 67  |
| Dir & Filename | applicationSvr.fm (Head4: Solaris Only: Manually Remove the Application Server Packages Bundled) . . . . . | 70  |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                                   | 72  |
| Dir & Filename | planning.fm (Head2: Operating System Issues) . . . . .                                                     | 72  |
| Dir & Filename | planning.fm (Head1: Preparing for Upgrades) . . . . .                                                      | 72  |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                                   | 87  |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets) . . . . .         | 87  |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets) . . . . .         | 88  |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components) . . . . .                                          | 92  |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                                   | 99  |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets) . . . . .         | 100 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets) . . . . .         | 101 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components) . . . . .                                          | 104 |
| Dir & Filename | sunCluster.fm (ChapTitle: Upgrading System Components) . . . . .                                           | 104 |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                                   | 114 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets) . . . . .         | 114 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets) . . . . .         | 116 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets) . . . . .         | 126 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components) . . . . .                                          | 126 |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                                   | 131 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets) . . . . .         | 133 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets) . . . . .         | 134 |



|                |                                                                                                   |     |
|----------------|---------------------------------------------------------------------------------------------------|-----|
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 136 |
| Dir & Filename | directorySvr.fm (ChapTitle: Upgrading System Components) . . . . .                                | 136 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 142 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 142 |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                          | 146 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 147 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 148 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 150 |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                          | 173 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 173 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 174 |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                          | 182 |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                          | 197 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 197 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 199 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 201 |
| Dir & Filename | sunCluster.fm (ChapTitle: Upgrading System Components) . . . . .                                  | 201 |
| Dir & Filename | directorySvr.fm (ChapTitle: Upgrading System Components) . . . . .                                | 201 |
| Dir & Filename | WebSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                      | 202 |
| Dir & Filename | ApplicationSvr.fm (ChapTitle: Upgrading System Components) . . . . .                              | 202 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 212 |
| Dir & Filename | sunCluster.fm (ChapTitle: Upgrading System Components) . . . . .                                  | 212 |
| Dir & Filename | directorySvr.fm (ChapTitle: Upgrading System Components) . . . . .                                | 212 |
| Dir & Filename | WebSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                      | 212 |

|                |                                                                                                       |     |
|----------------|-------------------------------------------------------------------------------------------------------|-----|
| Dir & Filename | ApplicationSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                  | 212 |
| Dir & Filename | planning.fm (Head3: Dual Upgrades: Java ES and Operating System Software) .<br>214                    |     |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                              | 225 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of<br>Product Componets) . . . . . | 225 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of<br>Product Componets) . . . . . | 227 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components) . . . . .                                     | 229 |
| Dir & Filename | messageQueue.fm (ChapTitle: Upgrading System Components) . . . . .                                    | 229 |
| Dir & Filename | highAvailabilityDB.fm (ChapTitle: Upgrading System Components) . . .                                  | 229 |
| Dir & Filename | javaDB.fm (ChapTitle: Directory Proxy Server) . . . . .                                               | 230 |
| Dir & Filename | webSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                          | 230 |
| Dir & Filename | planning.fm (Head3: Dual Upgrades: Java ES and Operating System Software) .<br>235                    |     |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components) . . . . .                                     | 237 |
| Dir & Filename | messageQueue.fm (Head1: Upgrading Access Manager from Java ES Release 2).<br>. . . . .                | 238 |
| Dir & Filename | webSvr.fm (Head1: Upgrading Web Server from Java ES Release 2) . . . .                                | 238 |
| Dir & Filename | messageQueue.fm (Head2: Release 2 Message Queue Upgrade) . . . . .                                    | 240 |
| Dir & Filename | planning.fm (Head3: Dual Upgrades: Java ES and Operating System Software) .<br>243                    |     |
| Dir & Filename | planning.fm (Head1: Java ES Release 5 and Solaris 10 Zones) . . . . .                                 | 245 |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                              | 252 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of<br>Product Componets) . . . . . | 253 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of<br>Product Componets) . . . . . | 254 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components) . . . . .                                     | 256 |
| Dir & Filename | javaDB.fm (ChapTitle: Directory Proxy Server) . . . . .                                               | 256 |
| Dir & Filename | ApplicationSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                  | 256 |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                              | 265 |

|                |                                                                                                   |     |
|----------------|---------------------------------------------------------------------------------------------------|-----|
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 266 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 267 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 269 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 270 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 276 |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                          | 286 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 288 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 290 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 292 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 293 |
| Dir & Filename | directorySvr.fm (ChapTitle: Upgrading System Components) . . . . .                                | 293 |
| Dir & Filename | webSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                      | 293 |
| Dir & Filename | applicationSvr.fm (ChapTitle: Upgrading System Components) . . . . .                              | 293 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 321 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 321 |
| Dir & Filename | directorySvr.fm (Head1: Upgrading Access Manager from Java ES Release 2) .<br>321                 |     |
| Dir & Filename | webSvr.fm (Head1: Upgrading Access Manager from Java ES Release 2) .                              | 321 |
| Dir & Filename | applicationSvr.fm (Head1: Upgrading Access Manager from Java ES Release 2)<br>321                 |     |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                          | 341 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 342 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 346 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 350 |

|                |                                                                                                       |     |
|----------------|-------------------------------------------------------------------------------------------------------|-----|
| Dir & Filename | directorySvr.fm (ChapTitle: Upgrading System Components) . . . . .                                    | 350 |
| Dir & Filename | webSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                          | 350 |
| Dir & Filename | applicationSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                  | 350 |
| Dir & Filename | accessMgr.fm (ChapTitle: Upgrading System Components) . . . . .                                       | 350 |
| Dir & Filename | portalSvrSRA.fm (ChapTitle: Upgrading System Components) . . . . .                                    | 350 |
| Dir & Filename | javaDB.fm (ChapTitle: Directory Proxy Server) . . . . .                                               | 350 |
| Dir & Filename | serviceRegistry.fm (ChapTitle: Directory Proxy Server) . . . . .                                      | 351 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components) . . . . .                                     | 356 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components) . . . . .                                     | 360 |
| Dir & Filename | portalSvrSRA.fm (Head1: Multiple Instance Upgrades) . . . . .                                         | 374 |
| Dir & Filename | accessMgr.fm (Head1: Multiple Instance Upgrades) . . . . .                                            | 375 |
| Dir & Filename | accessMgr.fm (Head2: Access Manager SDK-only Upgrades). . . . .                                       | 376 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components) . . . . .                                     | 378 |
| Dir & Filename | directorySvr.fm (ChapTitle: Upgrading System Components) . . . . .                                    | 378 |
| Dir & Filename | webSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                          | 378 |
| Dir & Filename | applicationSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                  | 378 |
| Dir & Filename | accessMgr.fm (ChapTitle: Upgrading System Components) . . . . .                                       | 379 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components) . . . . .                                     | 381 |
| Dir & Filename | directorySvr.fm (Head1: Upgrading Access Manager from Java ES Release 2) . .<br>381                   |     |
| Dir & Filename | webSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                          | 382 |
| Dir & Filename | applicationSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                  | 382 |
| Dir & Filename | accessMgr.fm (ChapTitle: Upgrading System Components) . . . . .                                       | 382 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components) . . . . .                                     | 383 |
| Dir & Filename | planning.fm (ChapTitle: Planning for Upgrades) . . . . .                                              | 417 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of<br>Product Componets) . . . . . | 418 |
| Dir & Filename | portalSvr.fm (Head3: Selective Upgrade Issues) . . . . .                                              | 419 |
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of<br>Product Componets) . . . . . | 420 |

|                |                                                                                                   |     |
|----------------|---------------------------------------------------------------------------------------------------|-----|
| Dir & Filename | planning.fm (TableCaption: Table 1-2 Shared Component Dependencies of Product Componets). . . . . | 421 |
| Dir & Filename | portalSvr.fm (Head3: Selective Upgrade Issues). . . . .                                           | 423 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 424 |
| Dir & Filename | portalSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                   | 424 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 427 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 429 |
| Dir & Filename | accessMgr.fm (Head1: Multiple Instance Upgrades) . . . . .                                        | 437 |
| Dir & Filename | accessMgr.fm (Head2: Access Manager SDK-only Upgrades). . . . .                                   | 437 |
| Dir & Filename | accessMgr.fm (Head2: Access Manager SDK-only Upgrades). . . . .                                   | 438 |
| Dir & Filename | accessMgr.fm (Head2: Access Manager SDK-only Upgrades). . . . .                                   | 439 |
| Dir & Filename | accessMgr.fm (Head2: Access Manager SDK-only Upgrades). . . . .                                   | 439 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 441 |
| Dir & Filename | directorySvr.fm (Head1: Upgrading Access Manager from Java ES Release 2) .<br>441                 |     |
| Dir & Filename | accessMgr.fm (ChapTitle: Upgrading System Components). . . . .                                    | 441 |
| Dir & Filename | portalSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                   | 441 |
| Dir & Filename | sharedComps.fm (ChapTitle: Upgrading System Components). . . . .                                  | 444 |
| Dir & Filename | directorySvr.fm (Head1: Upgrading Access Manager from Java ES Release 2) .<br>444                 |     |
| Dir & Filename | accessMgr.fm (ChapTitle: Upgrading System Components). . . . .                                    | 444 |
| Dir & Filename | portalSvr.fm (ChapTitle: Upgrading System Components) . . . . .                                   | 444 |

