Sicherheitshandbuch zu Oracle® ZFS Storage Appliance

ORACLE®

Überblick über die Oracle ZFS Storage Appliance-Sicherheit

In diesem Handbuch werden die Sicherheitsbetrachtungen behandelt, geprüft und hervorgehoben, die zum Erstellen eines sicheren Speichersystems und für ein teamübergreifendes Verständnis Ihrer jeweiligen Sicherheitsziele erforderlich sind. Wir empfehlen Ihnen, dieses Handbuch vor der Konfiguration von Appliances zu lesen, damit Sie die verfügbaren Sicherheitsfunktionen nutzen und die benötigten Sicherheitslevel einrichten können.

Sie können dieses Handbuch auch als Referenz verwenden, um nähere Einzelheiten zu Sicherheitsbetrachtungen der verschiedenen Funktionen und Fähigkeiten der Oracle ZFS Storage Appliance (ZFSSA) zu erhalten. Vorgehensweisen zur Appliance-Konfiguration finden Sie im Oracle ZFS Storage System Administration Guide.

In den folgenden Abschnitten finden Sie eine Beschreibung der ZFSSA-Sicherheitsfunktionen:

- **Erstinstallation** – Beschreibt die Festlegung des Admin-Zugangs, die Einrichtung des Root-Kontos sowie die Auswirkungen einer Zurücksetzung der ZFSSA auf die Werkseinstellungen.
- **Physische Sicherheit** – Beschreibt die physische Sicherheitsumgebung der ZFSSA.
- **Administratives Modell** – Beschreibt die Einschränkung des Zugriffs auf die CLI und BUI, das System-Patching-Modell, verzögerte Updates, Support-Bundles und das Konfigurationsbackup.
- **ZFSSA-Benutzer** – Beschreibt, wer über administrative Rollen die ZFSSA verwalten darf und wie Benutzerberechtigungen verwaltet werden.
- **Access Control-Listen (ACL)** – Beschreibt den Mechanismus, mit dem Zugriff auf Dateien und Verzeichnisse gewährt oder verweigert werden kann.
- **Storage Area Network (SAN)** – Beschreibt LUNs (Logical Unit Numbers) und deren zugehörige Inititatorgruppen sowie Initiatorauthentifizierungsoptionen und Standardeinstellungen.
- **Datenservices** – Beschreibt die von der ZFSSA unterstützten Datenservices und die von den verschiedenen Datenservices bereitgestellte Sicherheit.
- **Directory Services** – Beschreibt die Directory Services, die auf der ZFSSA konfiguriert werden können, und deren Sicherheitsauswirkungen.
- **Systemeinstellungen** – Beschreibt die Systemeinstellungen zu Phone Home, Servicetags, SMTP, SNMP, Syslog, Systemidentität, Datenträgerbereinigung und Verhinderung der endgültigen Löschung.
- **Remote-Admin-Zugriff** – Beschreibt den Remote-Zugriff über die BUI und CLI.
- **Protokolle** – Beschreibt die sicherheitsbezogenen Protokolltypen.

Erstinstallation

Die ZFSSA wird mit werkseitig vorinstallierter ZFSSA-Software ausgeliefert. Eine weitere Softwareinstallation ist nicht erforderlich, und es sind keine Medien im Lieferumfang enthalten.

Die Erstinstallation erfolgt mit dem Standardkontonamen und -passwort. Das Standard-Root-Passwort muss nach der Installation geändert werden. Wird die ZFSSA auf die Werkseinstellungen zurückgesetzt, wird dadurch auch das Root-Passwort sowohl für die ZFSSA als auch für den Serviceprozessor auf die Standardeinstellung zurückgesetzt.

Während der Erstinstallation einer ZFSSA liegt ein Standardkontoname und -passwort vor, das mit dem Serviceprozessor des Systems verknüpft ist. Mithilfe dieses Standardkontos erhält der Systemadministrator erstmals Zugriff auf die ZFSSA und muss dann im System die zur Erstinstallation erforderlichen Schritte

vornehmen. Einer dieser erforderlichen Schritte besteht in der Einrichtung eines neuen Admin-Passworts für die ZFSSA. Das Standardpasswort des Serviceprozessors wird dabei automatisch auf denselben Wert festgelegt.

Physische Sicherheit

Um den Zugriff auf das System zu steuern, müssen Sie die physische Sicherheit Ihrer Computerumgebung gewährleisten. Beispielsweise stellen Systeme, die nach der Anmeldung unbeaufsichtigt gelassen werden, Sicherheitsrisiken dar. Die Umgebung und die Hardware des Computers müssen physisch jederzeit vor unberechtigtem Zugriff geschützt werden.

Die ZFSSA unterliegt Zugangsbeschränkungen. Der Zugang wird mithilfe eines Sicherheitsmechanismus kontrolliert (z.B. einem Schlüssel, einer Sperre, einem Tool oder eines Werksausweises), und das autorisierte Zugangspersonal wurde über die Gründe für die Beschränkungen und die zu treffenden Sicherheitsmaßnahmen unterrichtet.

Administratives Modell

In diesem Abschnitt wird die Sicherheit für die administrativen ZFSSA-Modelle beschrieben.

Beschränkter Zugriff (CLI und BUI)

Administrativer Zugriff auf die Browserbenutzeroberfläche (Browser User Interface, BUI) und die Befehlszeilenschnittstelle (Command Line Interface, CLI) ist begrenzt auf den Root-Benutzer, lokale Administratoren mit den entsprechenden Berechtigungen und diejenigen, die über Identity Server wie beispielsweise Lightweight Directory Access Protocol (LDAP) und Network Information Service (NIS) autorisiert wurden.

Die Verwaltung erfolgt über eine SSL-(Secure Sockets Layer-)Befehlszeilenanmeldung bzw. eine sichere HTTP-(HTTPS-)Browsersitzung. HTTPS-Sitzungen werden mit einem selbstsignierten Zertifikat verschlüsselt, das bei der Erstinstallation speziell für jede ZFSSA generiert wird. HTTPS-Sitzungen besitzen ein vom Benutzer definierbares Standardsitzungs-Timeout von 15 Minuten.

Systemupdates

Systemupdates werden als vollständige binäre Ersetzung der Systemsoftware eingespielt. Vor dem Update wird ein Snapshot des laufenden Systempools aufgenommen. Damit können Administratoren bei Bedarf zur vorherigen Version zurückkehren.

Verzögerte Updates

Bei einem verzögerten Update wird ein Feature oder Teil einer Funktion, das Teil eines Systemupdates ist, bei Ausführung des Systemupdates nicht aktiviert. Es bleibt dem Administrator überlassen, ob und wann verzögerte Updates eingespielt werden sollen. Bei einem Systemupdate nicht eingespielte Updates stehen bei nachfolgenden Systemupdates weiterhin zur Verfügung. Bei Wahl eines verzögerten Updates können Sie keine einzelnen Updates zur Einspielung auswählen – Sie können nur entweder alle oder keine Updates einspielen. Nach dem Einspielen eines Updates können Sie nicht zu einer früheren Version der Systemsoftware zurückkehren.

Support-Bundles

Wenn in Ihrem System die Funktion "Phone Home" bei wesentlichen Ausfällen registriert ist, wird Ihr Systemstatus an My Oracle Support gesendet, wo er von unserem technischen Betreuungsteam untersucht und ein Support-Bundle erstellt werden kann. In den an My Oracle Support gesendeten Informationen zum Systemstatus sind keinerlei Benutzerdaten enthalten. Es werden lediglich Konfigurationsinformationen gesendet.

Konfigurationsbackup

Systemkonfigurationen können zwecks späterer Wiederherstellung lokal gespeichert werden. In diesen Backups sind keinerlei Benutzerdaten enthalten. Es werden lediglich Konfigurationseinstellungen gespeichert.

ZFSSA-Benutzer

Es gibt zwei Arten von ZFSSA-Benutzern:

- **Datenservicebenutzer** – Clients, die über unterstützte Protokolle wie NFS, SMB, Fibre Channel, iSCSI, HTTP und FTP auf Datei- und Blockressourcen zugreifen.
- **Benutzer mit Administratorrechten** – Benutzer, die die Konfiguration und Services auf der ZFSSA verwalten. Dieser Abschnitt bezieht sich nur auf Benutzer mit Administratorrechten.

Benutzer mit Administratorrechten - Rollen

Durch Zuweisung benutzerdefinierter Rollen können Administratoren Berechtigungen erteilt werden. Eine Rolle ist eine Zusammenfassung von Berechtigungen, die Sie einem Administrator zuweisen können. Es empfiehlt sich, verschiedene Administrator- und Operatorrollen mit unterschiedlichen Berechtigungsstufen zu erstellen. Mitarbeitern werden dann Rollen entsprechend ihren Anforderungen zugewiesen. Eine Zuweisung unnötiger Berechtigungen sollte vermieden werden.

Die Verwendung von Rollen ist sicherer als die gemeinsame Verwendung von Admin-Passwörtern für einen Vollzugriff, bei dem beispielsweise jedem Benutzer das Root-Passwort mitgeteilt wird. Rollen schränken Benutzer auf definierte Berechtigungsmengen ein. Darüber hinaus können Benutzerrollen in den Auditprotokollen auf bestimmte Benutzernamen zurückverfolgt werden. Standardmäßig ist eine Rolle namens "Basic administration" ("Allgemeine Verwaltung") vorhanden, die einen Mindestsatz an Berechtigungen enthält.

Bei Benutzern mit Administratorrechten kann es sich um folgende Arten von Benutzern handeln:

- Lokale Benutzer – Alle Kontoinformationen werden in der ZFSSA gespeichert.
- Verzeichnisbenutzer – Vorhandene NIS- oder LDAP-Konten werden verwendet, und zusätzliche Berechtigungseinstellungen werden in der ZFSSA gespeichert. Dadurch können vorhandene NIS-/LDAP-Benutzer sich anmelden und die ZFSSA verwalten, ohne sich jedoch standardmäßig bei der ZFSSA anmelden zu können. Der Zugang zur ZFSSA muss explizit erteilt werden.

Administrative Geltungsbereiche

Mithilfe von Berechtigungen können Benutzer bestimmte Aufgaben ausführen, wie beispielsweise das Erstellen von Shares, den Neustart der ZFSSA oder das Update der Systemsoftware. Berechtigungsgruppen

werden als Geltungsbereiche bezeichnet. Jeder Geltungsbereich kann einen Satz optionaler Filter besitzen, die die Anzahl der Berechtigungen eingrenzen. Beispiel: Anstatt eine Berechtigung zum Neustart aller Services zu vergeben, kann über einen Filter festgelegt werden, dass die Berechtigung nur zum Neustart des HTTP-Service befugt.

Access Control-Listen (ACL)

ZFSSA stellt Dateizugriffskontrolle über so genannte Access Control-Listen (ACLs) bereit. Eine Access Control-Liste ist ein Mechanismus, mit dem der Zugriff auf eine bestimmte Datei oder ein bestimmtes Verzeichnis erteilt oder verweigert wird.

Das von der ZFSSA bereitgestellte ACL-Modell basiert auf dem NFSv4 ACL-Modell, das sich von der Windows-ACL-Semantik ableitet. Es handelt sich dabei um ein umfassendes ACL-Modell, das feingranulierten Zugriff auf Dateien und Verzeichnisse bietet. Jede Datei und jedes Verzeichnis innerhalb der Speicher-ZFSSA besitzt eine eigene ACL. Sowohl für SMB als auch für NFS durchlaufen sämtliche ACL-Entscheidungen denselben Algorithmus zur Bestimmung, wem Zugriff auf Dateien und Verzeichnisse gewährt und wem er verweigert wird.

Eine ACL setzt sich aus einem oder mehreren ACEs (Access Control Entries) zusammen. Jeder ACE enthält einen Eintrag für die Berechtigungen, die der ACE erteilt oder verwehrt, für wen der ACE gilt und welche Übernahmekennzeichen verwendet werden.

ACL-Übernahme

In NFSv4 ACLs können einzelne ACEs von neu erstellten Dateien und Verzeichnissen übernommen werden. Die ACE-Übernahme wird über mehrere Kennzeichen zu Übernahmeebenen gesteuert, die der Administrator bei der anfänglichen Einrichtung der ACL festlegt.

ACL-Zugriff bestimmen

NFSv4 ACLs sind reihenfolgenabhängig und werden von oben nach unten verarbeitet. Eine einmal erteilte Berechtigung kann von einem nachfolgenden ACE nicht entzogen werden. Eine einmal verwehrte Berechtigung kann von einem nachfolgenden ACE nicht erteilt werden.

ACL mit SMB Share-Ebene

Eine ACL mit einer SMB Share-Ebene ist eine ACL, die zusammen mit einer Datei- oder Verzeichnis-ACL im Share bestimmt, welche Berechtigungen für eine Datei gelten. Die Share-Ebenen-ACL bietet eine weitere Stufe der Zugriffskontrolle über die der Datei-ACLs hinaus und stellt noch detailliertere Zugriffskontrollkonfigurationen bereit. Share-Ebenen-ACLs werden beim Export des Dateisystems über das SMB-Protokoll eingerichtet. Wird das Dateisystem nicht über das SMB-Protokoll exportiert, hat eine Einrichtung der Share-Ebenen-ACL keine Auswirkungen. Standardmäßig erteilen Share-Ebenen-ACLs allen Benutzern Vollzugriff.

ZFS ACL-Eigenschaften

ACL-Verhaltens- und Übernahmeeigenschaften gelten nur für NFS-Clients. SMB-Clients verwenden eine strenge Windows-Semantik und haben Priorität gegenüber ZFS-Eigenschaften. Der Unterschied besteht

darin, dass NFS im Gegensatz zu SMB-Clients POSIX-Semantik verwendet. Die Eigenschaften sind größtenteils mit POSIX kompatibel.

Storage Area Network (SAN)

In einem SAN definieren Ziel- und Initiatorgruppen Sets aus Zielen und Initiatoren, die mit einer LUN (Logical Unit Number) verknüpft werden können. Auf eine mit einer Zielgruppe verknüpfte LUN kann nur über die Ziele dieser Gruppe zugegriffen werden. Auf eine mit einer Initiatorgruppe verknüpfte LUN können nur die Initiatoren dieser Gruppe zugreifen. Initiator- und Zielgruppen werden auf eine LUN bei ihrer Erstellung angewendet. Eine LUN kann nur erfolgreich erstellt werden, wenn mindestens eine Zielgruppe und eine Initiatorgruppe definiert wird.

Abgesehen von der Authentifizierung über das Challenge-Handshake Authentication Protocol (CHAP), welches nur für einen iSCSI/iSER-Initiatorzugriff gewählt werden kann, findet keine Authentifizierung statt.

HINWEIS: Eine Verwendung der Standardinitiatorgruppe kann dazu führen, dass die LUN unerwünschten oder Konflikte verursachenden Initiatoren ausgesetzt wird.

Datenservices

TABELLE 1 Datenservices

SERVICE	BESCHREIBUNG	VERWENDETE PORTS
NFS	Dateisystemzugriff über die Protokolle NFSv3 und NFSv4	111 und 2049
iSCSI	LUN-Zugriff über das iSCSI-Protokoll	3260 und 3205
SMB	Dateisystemzugriff über das SMB-Protokoll	SMB-over-NetBIOS 139
		SMB-over-TCP 445
		NetBIOS Datagram 138
		NetBIOS Name Service 137
FTP	Dateisystemzugriff über das FTP-Protokoll	21
HTTP	Dateisystemzugriff über das HTTP-Protokoll	80
NDMP	NDMP-Hostservice	10000
Remote-Replikation	Remote-Replikation	216
Schattenmigration	Schattendatenmigration	
SFTP	Dateisystemzugriff über das SFTP-Protokoll	218
SRP	Blockzugriff über das SRP-Protokoll	
TFTP	Dateisystemzugriff über das TFTP-Protokoll	
Virenscan	Virenscan des Dateisystems	

Mindestens benötigte Ports:

Um für Sicherheit in einem Netzwerk zu sorgen, können Sie Firewalls erstellen. Portnummern werden für die Erstellung von Firewalls verwendet und identifizieren eine Transaktion über ein Netzwerk eindeutig, indem der Host und Service angegeben werden.

In der folgenden Liste sind die mindestens für die Erstellung von Firewalls benötigten Ports aufgeführt:

Eingehende Ports

- icmp/0-65535 (PING)
- tcp/1920 (EM)
- tcp/215 (BUI)
- tcp/22 (SSH)
- udp/161 (SNMP)

Zusätzliche eingehende Ports, wenn gemeinsamer Dateizugriff über http verwendet wird (in der Regel ist dies nicht der Fall)

- tcp/443 (SSL WEB)
- tcp/80 (WEB)

Ausgehende Ports

- tcp/80 (WEB)

Hinweis: Verwenden Sie bei der Replikation Generic Routing Encapsulation-Tunnels (GRE-Tunnels), wenn möglich. So kann der Verkehr über die Back-End-Schnittstellen abgewickelt werden, und es sind keine Firewalls erforderlich, die den Verkehr verlangsamen. Wenn keine GRE-Tunnels auf dem NFS-Core zur Verfügung stehen, muss die Replikation über die Front-End-Schnittstelle durchgeführt werden. In diesem Fall muss Port 216 ebenfalls geöffnet sein.

NFS-Authentifizierung und Verschlüsselungsoptionen

NFS Shares werden standardmäßig mit AUTH_SYS RPC-Authentifizierung zugewiesen. Sie können sie auch zur Freigabe mit Kerberos-Sicherheit konfigurieren. Mit der AUTH_SYS-Authentifizierung werden die UNIX UID und GID des Clients ohne Authentifizierung vom NFS-Server an das Netzwerk übergeben. Dieser Authentifizierungsmechanismus kann auf einem Client leicht durch jeden Benutzer mit Root-Zugriff ausgehoben werden. Es ist daher besser, einen der anderen verfügbaren Sicherheitsmodi zu verwenden.

Zusätzliche Zugriffskontrollen können für jedes Share einzeln angegeben werden, um Zugriff auf die Shares für bestimmte Hosts, DNS-Domänen oder Netzwerke zu erteilen bzw. zu verweigern.

Sicherheitsmodi

Sicherheitsmodi werden für jedes Share einzeln festgelegt. In der folgenden Liste werden die verfügbaren Kerberos-Sicherheitseinstellungen beschrieben.

- krb5 - Endbenutzerauthentifizierung über Kerberos V5
- krb5i - krb5 plus Integritätsschutz (Datenpakete sind vor Manipulation geschützt)
- krb5p - krb5i plus Datenschutz (Datenpakete sind vor Manipulation geschützt und verschlüsselt)

In der Sicherheitsmoduseinstellung können auch Kombinationen verschiedener Kerberos-Typen angegeben werden. Mit den kombinierten Sicherheitsmodi können Clients mit beliebigen der aufgeführten Kerberos-Typen gemountet werden.

Kerberos-Typen

- sys - Systemauthentifizierung

- krb5 - nur Kerberos v5, Clients müssen mit diesem Typ mounten.
- krb5:krb5i - Kerberos v5, mit Integrität, Clients können mit beliebigen der aufgelisteten Typen mounten.
- krb5i - nur Kerberos v5-Integrität, Clients müssen mit diesem Typ mounten.
- krb5:krb5i:krb5p - Kerberos v5, mit Integrität oder Datenschutz, Clients können mit beliebigen der aufgelisteten Typen mounten.
- krb5p - nur Kerberos v5-Datenschutz, Clients müssen mit diesem Typ mounten.

iSCSI

Wenn Sie eine LUN auf der ZFSSA konfigurieren, können Sie dieses Volume über ein iSCSI-(Internet Small Computer System Interface-)Ziel exportieren. Mit dem iSCSI-Service können iSCSI-Initiatoren über das iSCSI-Protokoll auf Ziele zugreifen.

Dieser Service unterstützt Discovery, Verwaltung und Konfiguration mittels iSNS-Protokoll. Der iSCSI-Service unterstützt sowohl unidirektionale (Ziel authentifiziert Initiator) als auch bidirektionale (Ziel und Initiator authentifizieren sich gegenseitig) Authentifizierung über CHAP. Darüber hinaus unterstützt der Service die Verwaltung von CHAP-Authentifizierungsdaten in einer RADIUS-Datenbank.

Das System führt in zwei voneinander unabhängigen Schritten zuerst die Authentifizierung und anschließend die Autorisierung durch. Wenn der lokale Initiator einen CHAP-Namen und ein CHAP Secret besitzt, nimmt das System die Authentifizierung vor. Besitzt der lokale Initiator keine CHAP-Eigenschaften, führt das System keine Authentifizierung durch, sodass alle Initiatoren autorisierungsberechtigt sind.

Mit dem iSCSI-Service können Sie eine globale Initiatorenliste angeben, die Sie innerhalb der Initiatorengruppen verwenden können. Bei der Verwendung der iSCSI- und CHAP-Authentifizierung kann RADIUS als das iSCSI-Protokoll dienen, das alle CHAP-Authentifizierungen dem gewählten RADIUS-Server überlässt.

RADIUS-Unterstützung

RADIUS (Remote Authentication Dial-In User Service) ist ein System, bei dem ein zentralisierter Server zur Ausführung von CHAP-Authentifizierungen für Speicherknoten eingesetzt wird. Wenn Sie iSCSI- und CHAP-Authentifizierung verwenden, können Sie RADIUS als iSCSI-Protokoll wählen. Dadurch wird sowohl iSCSI als auch iSER (iSCSI Extensions for RDMA) angewendet, und alle CHAP-Authentifizierungen werden an den gewählten RADIUS-Server gesendet.

Damit die ZFSSA eine CHAP-Authentifizierung mittels RADIUS ausführen kann, müssen folgende Angaben gemacht werden:

- Die ZFSSA muss die Adresse des RADIUS-Servers und ein Secret angeben, das zur Kommunikation mit diesem RADIUS-Server eingesetzt werden soll.
- Der RADIUS-Server muss (beispielsweise in seiner Clientdatei) einen Eintrag aufweisen, der die Adresse der ZFSSA und dasselbe Secret wie oben erwähnt angibt.
- Der RADIUS-Server muss (beispielsweise in seiner Benutzerdatei) einen Eintrag aufweisen, der für jeden Initiator den CHAP-Namen und das zugehörige CHAP Secret angibt.
- Wenn der Initiator seinen IQN-Namen als CHAP-Namen verwendet (empfohlene Konfiguration) und die ZFSSA keinen separaten Initiatoreintrag für jedes Initiatorfeld erfordert, kann der RADIUS-Server alle Authentifizierungsschritte durchführen.
- Verwendet der Initiator einen anderen CHAP-Namen, muss die ZFSSA einen Initiatoreintrag für den Initiator haben, der die Zuordnung zwischen IQN-Name und CHAP-Name angibt. In diesem Initiatoreintrag muss das CHAP Secret für den Initiator NICHT angegeben werden.

SMB (Server Message Block)

Das SMB-Protokoll (auch als CIFS (Common Internet File System) bezeichnet) bietet hauptsächlich gemeinsamen Zugriff auf Dateien in einem Microsoft Windows-Netzwerk. Außerdem führt es eine Authentifizierung durch.

Folgende SMB-Optionen haben Auswirkungen auf die Sicherheit:

- **Restrict Anonymous Access to share list** (Anonymen Zugriff auf Share-Liste einschränken) – Bei Auswahl dieser Option müssen sich Clients über SMB authentifizieren, um eine Share-Liste abrufen zu können. Ist diese Option deaktiviert, können anonyme Clients auf die Share-Liste zugreifen. Diese Option ist standardmäßig deaktiviert.
- **SMB Signing Enabled** (SMB-Signaturfunktion aktiviert) – Mit dieser Option wird Interoperabilität mit SMB-Clients aktiviert, die die SMB-Signaturfunktion verwenden. Wenn die Option aktiviert ist, werden Signaturen von unterzeichneten Paketen überprüft. Ist die Option deaktiviert, werden nicht unterzeichnete Pakete ohne Signaturüberprüfung akzeptiert. Diese Option ist standardmäßig deaktiviert.
- **SMB Signing Required** (SMB-Signatur erforderlich) – Diese Option kann verwendet werden, wenn eine SMB-Signatur erforderlich ist. Ist die Option deaktiviert, müssen alle SMB-Pakete unterzeichnet sein, da sie ansonsten abgelehnt werden. Clients, die die SMB-Signaturfunktion nicht unterstützen, können sich nicht am Server anmelden. Diese Option ist standardmäßig deaktiviert.
- **Enable Access-based Enumeration** (Zugriffsbasierte Enumeration aktivieren) – Wenn Sie diese Option aktivieren, werden Verzeichniseinträge basierend auf den Zugangsdaten des Clients gefiltert. Hat der Client keinen Zugriff auf eine Datei oder ein Verzeichnis, wird diese Datei aus der Liste der an den Client zurückgegebenen Einträge ausgelassen. Diese Option ist standardmäßig deaktiviert.

Authentifizierung im Active Directory-(AD-)Domänenmodus

Im Domänenmodus werden Benutzer in Active Directory definiert. SMB-Clients können sich über Kerberos oder NTLM-Authentifizierung bei der ZFSSA anmelden.

Wenn sich ein Benutzer über einen vollqualifizierten ZFSSA-Hostnamen anmeldet, verwenden Windows-Clients in derselben oder einer vertrauenswürdigen Domäne die Kerberos-Authentifizierung. Ansonsten verwenden sie die NTLM-Authentifizierung.

Verwendet ein SMB-Client die NTLM-Authentifizierung zur Anmeldung bei der ZFSSA, werden die Zugangsdaten des Benutzers zur Authentifizierung an den AD-Domänencontroller weitergeleitet. Dies wird als Passthrough-Authentifizierung bezeichnet.

Sind Windows-Sicherheitsrichtlinien definiert, die die NTLM-Authentifizierung einschränken, müssen sich Windows-Clients über einen vollqualifizierten Hostnamen bei der ZFSSA anmelden. Weitere Informationen finden Sie im folgenden MSDN-Artikel: http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx.

Nach der Authentifizierung wird für die SMB-Sitzung des Benutzers ein so genannter "Sicherheitskontext" eingerichtet. Der durch den Sicherheitskontext repräsentierte Benutzer besitzt eine eindeutige SID (Sicherheitsdeskriptor). Die SID gibt den Dateieigentümer an und wird zur Bestimmung von Dateizugriffsrechten verwendet.

Authentifizierung im Arbeitsgruppenmodus

Im Arbeitsgruppenmodus werden Benutzer lokal auf der ZFSSA definiert. Meldet sich ein SMB-Client im Arbeitsgruppenmodus bei einer ZFSSA an, wird dieser Benutzer lokal über seine Benutzernamen- und Passwort-Hashes authentifiziert.

Über die LAN Manager-(LM-)Kompatibilitätsebene wird das Protokoll angegeben, das verwendet werden soll, wenn sich die ZFSSA im Arbeitsgruppenmodus befindet.

In der folgenden Liste wird angezeigt, wie sich die ZFSSA für die einzelnen LM-Kompatibilitätsebenen verhält:

- Ebene 2: Akzeptiert LM-, NTLM- und NTLMv2-Authentifizierung
- Ebene 3: Akzeptiert LM-, NTLM- und NTLMv2-Authentifizierung
- Ebene 4: Akzeptiert NTLM- und NTLMv2-Authentifizierung
- Ebene 5: Akzeptiert nur NTLMv2-Authentifizierung.

Sobald der Arbeitsgruppenbenutzer erfolgreich authentifiziert wurde, wird ein Sicherheitskontext eingerichtet. Für die in der ZFSSA definierten Benutzer wird eine eindeutige SID aus einer Kombination der Rechner-SID und der Benutzer-UID erstellt. Alle lokalen Benutzer werden als UNIX-Benutzer definiert.

Lokale Gruppen und Berechtigungen

Lokale Gruppen sind Domänenbenutzergruppen, die den darin enthaltenen Benutzern zusätzliche Rechte einräumen. Administratoren können Dateiberechtigungen umgehen, um das Eigentümerrecht von Dateien zu ändern. Backupoperatoren können Dateizugriffskontrollen umgehen, um für Dateien Backups zu erstellen und Dateien wiederherzustellen.

Administrative Vorgänge über die Microsoft Management Console (MMC)

Um sicherzustellen, dass administrative Vorgänge nur von Benutzern mit den entsprechenden Berechtigungen vorgenommen werden können, gibt es einige Zugriffsbeschränkungen für Vorgänge, die remote über die MMC vorgenommen werden.

In der folgenden Liste sind die Benutzer und die für sie zulässigen Vorgänge aufgeführt:

- Normale Benutzer – Shares auflisten
- Mitglieder der Administratorengruppe – Dateiöffnungen und -schließungen auflisten, Benutzerverbindungen trennen, Services und Ereignisprotokoll anzeigen
- Mitglieder der Administratorengruppen können außerdem die Share-Ebenen-ACLs festlegen/ändern
- Mitglieder der Administratorengruppe – Dateiöffnungen und -schließungen auflisten, Benutzerverbindungen trennen, Services und Ereignisprotokoll anzeigen

Virenscan

Mit dem Virenscanservice können Sie auf Dateisystemebene nach Viren suchen. Bei einem Zugriff auf eine Datei über ein beliebiges Protokoll scannt der Virenscanservice zunächst die Datei. Wird ein Virus erkannt, verweigert der Service den Zugriff auf die Datei und stellt sie unter Quarantäne. Der Scan erfolgt über eine von der ZFSSA aufgerufene externe Engine. Die externe Engine ist nicht im Lieferumfang der ZFSSA-Software enthalten.

Sobald eine Datei mit der neuesten Virusdefinition gescannt wurde, wird sie erst nach der nächsten Änderung erneut gescannt. Virenscans werden hauptsächlich für SMB-Clients angeboten, die einem hohen Virenrisiko ausgesetzt sind. NFS-Clients können ebenfalls Virenscans durchführen. Aufgrund der Funktionsweise des NFS-Protokolls werden Viren jedoch möglicherweise nicht so schnell wie beim SMB-Client erkannt.

Verzögerungs-Engine für Timing-Angriffe

In SMB ist keine Verzögerungs-Engine zur Abwehr von Timing-Angriffen implementiert. SMB basiert auf dem kryptografischen Solaris-Framework.

Datenverschlüsselung bei Kabelverbindungen

Der SMB-Service verwendet Version 1 des SMB-Protokolls, welches keine Datenverschlüsselung bei Kabelverbindungen unterstützt.

FTP (File Transfer Protocol)

FTP ermöglicht FTP-Clients den Zugriff auf das Dateisystem. Beim FTP-Service sind keine anonymen Anmeldungen zulässig, und Benutzer müssen sich mit dem konfigurierten Namensservice authentifizieren.

FTP unterstützt die folgenden Sicherheitseinstellungen. Diese Einstellungen gelten für alle Dateisysteme, für die der FTP-Protokollzugriff aktiviert ist:

- Enable SSL/TLS (SSL/TLS aktivieren) – Lässt SSL-/TLS-verschlüsselte FTP-Verbindungen zu und stellt sicher, dass die FTP-Transaktion verschlüsselt ist. Diese Option ist standardmäßig deaktiviert.
- Permit root login (Anmeldung des Root-Benutzers zulassen) – Lässt FTP-Anmeldungen für den Root-Benutzer zu. Diese Option ist standardmäßig deaktiviert, da die FTP-Authentifizierung im Klartext erfolgt, was für das Netzwerk eine potentielle Gefährdung durch Sniffer-Angriffe darstellt.
- Maximum number of allowable login attempts (Maximale Anzahl zulässiger Anmeldeversuche) – Die Anzahl nicht erfolgreicher Anmeldeversuche, bevor eine FTP-Verbindung getrennt wird und der Benutzer sich erneut anmelden muss. Der Standardwert ist 3.
- Logging level (Protokollierungsebene) – Der Ausführlichkeitsgrad des Protokolls.

FTP unterstützt die folgenden Protokolle:

- proftpd – FTP-Ereignisse einschließlich erfolgreiche und nicht erfolgreiche Anmeldeversuche
- proftpd_xfer – Dateiübertragungsprotokoll
- proftpd_tls – FTP-Ereignisse, die sich auf die SSL-/TLS-Verschlüsselung beziehen

HTTP (Hypertext Transfer Protocol)

HTTP bietet Zugriff auf Dateisysteme über die Protokolle HTTP und HTTPS sowie die HTTP-Erweiterung WebDAV (Web based Distributed Authoring and Versioning). Dadurch können Clients über einen Webbrowser oder – sofern ihre Clientsoftware dies unterstützt – als lokales Dateisystem auf gemeinsam genutzte Dateisysteme zugreifen. Der HTTPS-Server verwendet ein selbstsigniertes Sicherheitszertifikat.

Folgende Eigenschaften stehen zur Verfügung:

- Require client login (Clientanmeldung erforderlich) – Clients müssen sich vor dem Zugriff auf das Share authentifizieren und erhalten Eigentümerrechte an den von ihnen erstellten Dateien. Wenn diese Option nicht aktiviert ist, gehen die Eigentümerrechte an erstellten Dateien an den HTTP-Service mit dem Benutzer "nobody”.
- Protocols (Protokolle) – Wählen Sie, welche Zugriffsmethoden unterstützt werden sollen: HTTP, HTTPS oder beide.
- HTTP Port (for incoming connections) (HTTP-Port (für eingehende Verbindungen)) – HTTP-Port. Der Standardport lautet 80.

- HTTPS Port (for incoming secure connections) (HTTPS-Port (für eingehende sichere Verbindungen)) – HTTP-Port. Der Standardport lautet 443.

Ist die Option "Require Client Login" aktiviert, verweigert die ZFSSA den Zugriff auf Clients, die keine gültigen Authentifizierungszugangsdaten für einen lokalen Benutzer, einen NIS-Benutzer oder einen LDAP-Benutzer bereitstellen. Die Active Directory-Authentifizierung wird nicht unterstützt. Es wird nur die HTTP-Basisauthentifizierung unterstützt. Sofern HTTPS nicht verwendet wird, erfolgt die Übertragung von Benutzername und Passwort hier unverschlüsselt, was nicht für alle Umgebungen angemessen sein mag. Ist die Option "Require Client Login" deaktiviert, unternimmt die ZFSSA keinen Authentifizierungsversuch.

Unabhängig von der Authentifizierung werden Berechtigungen nicht vor erstellten Dateien und Verzeichnissen maskiert. Auf neu erstellte Dateien haben alle Benutzer Schreib- und Lesezugriff. Auf neu erstellte Verzeichnisse haben alle Benutzer Schreib-, Lese- und Ausführungszugriff.

NDMP (Network Data Management Protocol)

NDMP ermöglicht der ZFSSA die Teilnahme an NDMP-basierten Backup- und Wiederherstellungsvorgängen, die von einem als DMA (Data Management Application) bezeichneten Remote-NDMP-Client gesteuert werden. Über NDMP können ZFSSA-Benutzerdaten (Beispiel: Daten, die in von einem Administrator erstellten Shares auf der ZFSSA gespeichert sind) in lokal angebundenen Geräten wie Bandlaufwerken und Remote-Systemen gesichert und wiederhergestellt werden. Lokal angebundene Geräte können auch über DMA gesichert und wiederherstellt werden.

Remote-Replikation

Die Remote-Replikationsfunktion der ZFSSA erleichtert die Replikation von Projekten und Shares. Mit diesem Service können Sie ZFSSAs anzeigen, die Daten auf diese ZFSSA repliziert haben, und konfigurieren, auf welche ZFSSAs diese ZFSSA Daten replizieren darf.

Wenn dieser Service aktiviert ist, erhält die ZFSSA Replikationsupdates von anderen ZFSSAs und kann Replikationsupdates für lokale Projekte und Shares je nach deren konfigurierten Aktionen senden. Wenn der Service deaktiviert ist, können keine Replikationsupdates empfangen werden, und es werden keine lokalen Projekte und Shares repliziert.

Um Remote-Replikationsziele für die ZFSSA konfigurieren zu können, ist das Root-Passwort für die Remote-ZFSSA erforderlich. Diese Ziele werden zur Einrichtung einer Replikations-Peer-Verbindung verwendet, mit deren Hilfe die ZFSSAs kommunizieren können.

Während der Zielerstellung wird das Root-Passwort zur Echtheitsbestätigung der Anforderung sowie zur Generierung und zum Austausch von Sicherheitsschlüsseln verwendet, über die die ZFSSAs in nachfolgenden Kommunikationen identifiziert werden.

Die generierten Schlüssel werden als Teil der ZFSSA-Konfiguration dauerhaft gespeichert. Das Root-Passwort wird nie dauerhaft gespeichert. Das Root-Passwort wird nie unverschlüsselt übermittelt. Alle ZFSSA-Kommunikationen, einschließlich des anfänglichen Identitätsaustauschs, werden über SSL geschützt.

Schattenmigration

Eine Schattenmigration ermöglicht eine automatische Datenmigration von externen oder internen Quellen und steuert die automatische Migration im Hintergrund. Unabhängig davon, ob der Service aktiviert ist oder nicht, werden Daten für In-Band-Anforderungen synchron migriert. Hauptzweck dieses Service ist es, eine Einstellungsmöglichkeit zu bieten, wie viele Threads dediziert für die Migration im Hintergrund bereitgestellt werden können.

NFS-Mounts auf einer NFS-Quelle können nicht vom ZFSSA-Benutzer gesteuert werden. Daher können Schattenmigrationmounts nicht sicher sein; wenn der Server eine Kerberos- oder eine ähnliche Anforderung erwartet, wird der Quellmount abgelehnt.

SFTP (SSH File Transfer Protocol)

SFTP ermöglicht SFTP-Clients den Zugriff auf das Dateisystem. Anonyme Anmeldungen sind nicht zulässig, sodass sich Benutzer mit dem konfigurierten Namensservice authentifizieren müssen.

Wenn Sie einen SFTP-Schlüssel erstellen, müssen Sie die Benutzereigenschaft mit einer gültigen Benutzerzuweisung aufnehmen. SFTP-Schlüssel sind nach Benutzer gruppiert und werden über SFTP mit dem Namen des Benutzers authentifiziert.

HINWEIS: Aus Sicherheitsgründen sollten Sie vorhandene SFTP-Schlüssel, die die Benutzereigenschaft nicht enthalten, neu erstellen, auch wenn damit eine Authentifizierung möglich ist.

TFTP (Trivial File Transfer Protocol)

TFTP ist ein einfaches Protokoll für die Übertragung von Dateien. Es ist auf Kompaktheit und einfache Implementierung ausgelegt, ihm fehlen jedoch die meisten Sicherheitsfunktionen von FTP. TFTP führt nur Lese- und Schreibvorgänge zu und von einem Remote-Server aus. Es kann keine Verzeichnisse auflisten und bietet derzeit keine Möglichkeit der Benutzerauthentifizierung.

Directory Services

NIS (Network Information Service)

NIS ist ein Namensservice für eine zentralisierte Verzeichnisverwaltung. Die ZFSSA kann als NIS-Client für Benutzer und Gruppen fungieren, sodass sich NIS-Benutzer bei FTP und HTTP/WebDAV anmelden können. NIS-Benutzer können auch Berechtigungen zur ZFSSA-Administration erhalten. Die ZFSSA ergänzt die NIS-Informationen mit ihren eigenen Berechtigungseinstellungen.

LDAP (Lightweight Directory Access Protocol)

Die ZFSSA verwendet LDAP zur Authentifizierung von Admin-Benutzern wie auch einigen Datenservicebenutzern (FTP, HTTP). LDAP over SSL-Sicherheit wird von der ZFSSA unterstützt. Über LDAP werden Informationen zu Benutzern und Gruppen abgerufen. Es bietet folgende Funktionen:

- Stellt Benutzerschnittstellen bereit, die Namen für Benutzer und Gruppen akzeptieren und anzeigen.
- Ordnet für Datenprotokolle wie NFSv4, die Namen verwenden, Namen von Benutzern und Gruppen zu.
- Definiert Gruppenmitgliedschaft zur Verwendung in der Zugriffskontrolle.
- Kann optional Authentifizierungsdaten zur Admin- und Datenzugriffsauthentifizierung übertragen.

LDAP-Verbindungen können als Authentifizierungsmechanismus verwendet werden. Beispiel: Bei einem Versuch eines Benutzers, sich bei der ZFSSA zu authentifizieren, kann die ZFSSA ihrerseits versuchen, sich als dieser Benutzer beim LDAP-Server zu authentifizieren, um die Authentifizierung zu überprüfen.

Zur LDAP-Verbindungssicherheit stehen eine Reihe an Steuerelementen zur Verfügung:

- Authentifizierung von der Appliance zum Server:
  - Die Appliance ist anonym
  - Die Appliance authentifiziert sich über die Kerberos-Zugangsdaten des Benutzers
  - Die Appliance authentifiziert sich über den angegebenen "Proxy"-Benutzer und das zugehörige Passwort
- Authentifizierung vom Server zur Appliance (zur Sicherstellung, dass der korrekte Server kontaktiert wurde):
  1. Nicht gesichert
  2. Der Server wird über Kerberos authentifiziert
  3. Der Server wird über ein TLS-Zertifikat authentifiziert

Über eine LDAP-Verbindung übertragene Daten werden verschlüsselt, sofern Kerberos oder TLS verwendet werden; ansonsten nicht. Bei Verwendung von TLS wird die erste Verbindung zur Konfigurationszeit nicht gesichert. Zu diesem Zeitpunkt wird das Serverzertifikat erfasst und bei späteren Production-Verbindungen zur Authentifizierung verwendet.

Zertifikate einer Certificate Authority können nicht zur Authentifizierung mehrerer LDAP-Server importiert werden. Ebenso wenig kann das Zertifikat eines bestimmten LDAP-Servers manuell importiert werden.

Es werden nur TLS-(LDAPS-)Daten vom Typ RAW unterstützt. STARTTLS-Verbindungen, die auf einer nicht gesicherten LDAP-Verbindung starten und dann in eine gesicherte Verbindung übergehen, werden nicht unterstützt. LDAP-Server, für die ein Clientzertifikat erforderlich ist, werden nicht unterstützt.

Identitätszuordnung

Clients können auf Dateiressourcen auf der ZFSSA über SMB oder NFS zugreifen. Jeder Client verfügt über eine eindeutige Benutzer-ID. SMB-/Windows-Benutzer besitzen SIDs (Security Descriptors), während UNIX-/Linux-Benutzer UIDs (User IDs) besitzen. Benutzer können auch Mitglieder von Gruppen sein, die über Gruppen-SIDs (für Windows-Benutzer) bzw. Gruppen-IDs (GIDs) für Unix-/Linux-Benutzer gekennzeichnet sind.

In Umgebungen, in denen über beide Protokolle auf Dateiressourcen zugegriffen wird, ist es häufig ratsam, Identitätsentsprechungen einzurichten, sodass ein UNIX-Benutzer beispielsweise einem bestimmten Active Directory-Benutzer entspricht. Dies ist zur Bestimmung der Zugriffsrechte auf Dateiressourcen auf der ZFSSA von Bedeutung.

Es gibt verschiedene Arten der Identitätszuordnung, die Directory Services wie Active Directory, LDAP und NIS einbeziehen. Für den verwendeten Directory Service sollten nach Möglichkeit in Bezug auf Sicherheitsverfahren Best Practices zum Einsatz kommen.

IDMU

Microsoft bietet eine Funktion namens Identity Management for UNIX (IDMU). Diese Software ist für Windows Server 2003 verfügbar und ist in Windows Server 2003 R2 und höher eingebunden. Diese Funktion ist Teil der vormals als Services for UNIX bezeichneten Services in entbündelter Form.

IDMU dient hauptsächlich zur Unterstützung von Windows als NIS-/NFS-Server. Mit IDMU kann der Administrator eine Reihe UNIX-bezogener Parameter angeben: UID, GID, Anmeldeshell, Home-Verzeichnis und Ähnliches für Gruppen. Diese Parameter werden mit AD über ein Schema bereitgestellt, das dem in RFC2307 beschriebenen ähnelt, sowie über den NIS-Service.

Im IDMU-Zuordnungsmodus verwendet der Identitätszuordnungsservice diese UNIX-Attribute zur Herstellung von Zuordnungen zwischen Windows- und UNIX-Attributen. Dieser Ansatz weist starke

Ähnlichkeiten mit der verzeichnisbasierten Zuordnung auf, nur dass der Identitätszuordnungsservice das von der IDMU-Software eingerichtete Eigenschaftsschema abfragt, anstatt ein benutzerdefiniertes Schema zuzulassen. Bei Verwendung dieses Ansatzes darf keine weitere verzeichnisbasierte Zuordnung verwendet werden.

Verzeichnisbasierte Zuordnung

Bei der verzeichnisbasierten Zuordnung werden an ein LDAP- oder Active Directory-Objekt Informationen darüber angehängt, wie dessen Identität einer entsprechenden Identität auf der gegenüberliegenden Plattform zuzuordnen ist. Diese zusätzlichen, mit dem Objekt verknüpften Attribute müssen konfiguriert werden.

Namensbasierte Zuordnung

Bei der namensbasierten Zuordnung werden verschiedene Regeln erstellt, die die Identitäten nach Namen zuordnen. Diese Regeln stellen Entsprechungen zwischen Windows- und UNIX-Identitäten her.

Flüchtige Zuordnung

Gelten für einen bestimmten Benutzer keine namensbasierten Zuordnungsregeln, erhält dieser Benutzer über eine flüchtige Zuordnung temporäre Zugangsdaten, es sei denn, er ist durch eine Zuordnungsverweigerungssperre blockiert. Erstellt ein Windows-Benutzer mit einem flüchtigen UNIX-Namen eine Datei im System, wird Windows-Clients, die auf die Datei über SMB zugreifen, diese Windows-Identität als Eigentümer der Datei angezeigt. NFS-Clients hingegen wird als Eigentümer der Benutzer "nobody" angezeigt.

Systemeinstellungen

In den folgenden Abschnitten werden die verfügbaren Systemsicherheitseinstellungen beschrieben.

Phone Home

Mit dem Phone Home-Service werden die ZFSSA-Registrierung sowie der Remote-Supportservice von Phone Home verwaltet. In diesen Meldungen werden keine Benutzerdaten oder Metadaten übertragen.

- Bei der Registrierung wird Ihre ZFSSA mit dem Bestandsportal von Oracle verbunden, über das Sie Ihre Oracle-Geräte verwalten können. Die Verwendung des Phone Home-Service setzt eine Registrierung zwingend voraus.
- Der Phone Home-Service kommuniziert mit Oracle Support, um folgende Funktionen anzubieten:
  - Fehlermeldung – Das System meldet aktive Probleme an Oracle und erhält eine automatische Serviceantwort. Je nach Art des Fehlers wird eventuell ein Supportfall geöffnet.
  - Taktüberwachung – Taktüberwachungsmeldungen werden täglich an Oracle gesendet, um anzuzeigen, dass das System hochgefahren und gestartet ist. Oracle Support benachrichtigt möglicherweise den technischen Ansprechpartner für einen Kunden, wenn eines der aktivierten Systeme zu lange kein Taktsignal sendet.
  - Systemkonfiguration – In regelmäßigen Abständen werden Meldungen mit den aktuellen Software- und Hardwareversionen und Konfigurationen sowie mit Informationen zur Speicherkonfiguration an Oracle gesendet.

Servicetags

Servicetags erleichtern die Produktbestandsaufnahme und den Support, da mit ihnen die ZFSSA beispielsweise auf folgende Daten abgefragt werden kann:

- Systemseriennummer
- Systemtyp
- Softwareversionsnummern

Sie können die Servicetags bei Oracle Support registrieren und somit leicht den Überblick über Ihre Oracle-Geräte behalten und Serviceanfragen beschleunigen. Servicetags sind standardmäßig aktiviert.

SMTP

SMTP versendet alle von der ZFSSA generierten Mails, üblicherweise als Antwort auf Alarmmeldungen entsprechend der Konfiguration. SMTP nimmt keine externen Mails an, sondern sendet nur Mails, die von der ZFSSA selbst automatisch generiert wurden.

Standardmäßig verwendet der SMTP-Service DNS (MX-Datensätze), um zu bestimmen, wohin die Mails gesendet werden sollen. Wenn DNS nicht für die Domäne der ZFSSA konfiguriert ist oder für die Zieldomäne für ausgehende Mails keine DNS MX-Datensätze ordnungsgemäß eingerichtet sind, kann die ZFSSA so konfiguriert werden, dass alle Mails über einen ausgehenden Mailserver weitergeleitet werden.

SNMP (Simple Network Management Protocol)

SNMP stellt zwei Funktionen für die ZFSSA bereit: die Bereitstellung von ZFSSA-Statusinformationen und die Konfiguration von Alarmmeldungen zur Versendung von SNMP-Traps. Verfügbar sind die beiden SNMP-Versionen 1 und 2c.

Syslog

Eine Syslog-Meldung ist eine kleine Ereignismeldung, die von der ZFSSA an ein oder mehrere Remote-Systeme übertragen wird. Syslog stellt zwei ZFSSA-Funktionen bereit:

- Alarmkonfiguration zur Versendung von Syslog-Meldungen an ein oder mehrere Remote-Systeme
- Weiterleitung von Syslog-Meldungen an Remote-Systeme für Syslog-fähige Services auf der ZFSSA

Syslog-Meldungen können für das klassische in RFC 3164 beschriebene Ausgabeformat oder das neuere, in RFC 5424 beschriebene versionierte Ausgabeformat konfiguriert werden. Syslog-Meldungen werden als UDP-Datagramme übermittelt. Daher können sie vom Netzwerk verworfen werden oder werden möglicherweise gar nicht gesendet, wenn im Ausgangssystem wenig Arbeitsspeicher zur Verfügung steht oder das Netzwerk ausgelastet ist. Administratoren sollten daher davon ausgehen, dass bei einem komplexen Fehlerszenario in einem Netzwerk einige Meldungen möglicherweise fehlen oder verworfen wurden.

Die Meldung enthält folgende Elemente:

- Eine Funktion, die die Art der Systemkomponente angibt, welche die Meldung gesendet hat
- Ein Schweregrad, der den Schweregrad der mit der Bedingung verknüpften Meldung beschreibt
- Ein Zeitstempel, der die Uhrzeit des verknüpften Ereignisses in UTC angibt
- Ein Hostname mit dem kanonischen Namen der ZFSSA
- Ein Tag, das den Namen der Systemkomponente angibt, welche die Meldung gesendet hat
- Eine Meldung mit einer Beschreibung des Ereignisses selbst

Systemidentität

Dieser Service dient zur Konfiguration von Systemname und Speicherort. Wenn die ZFSSA an eine andere Stelle im Netzwerk verschoben oder einem anderen Zweck zugeführt wird, müssen diese Angaben möglicherweise geändert werden.

Datenträgerbereinigung

Eine Datenträgerbereinigung sollte in regelmäßigen Abständen vorgenommen werden, damit die ZFSSA beschädigte Daten auf dem Datenträger erkennen und korrigieren kann. Die Datenträgerbereinigung ist ein Prozess im Hintergrund, bei dem Datenträger während Leerlaufphasen gelesen werden, um nicht behebbare Lesefehler in Bereichen zu erkennen, auf die selten zugegriffen wird. Eine zeitige Erkennung solch latenter Bereichsfehler ist zur Reduktion von Datenverlusten von hoher Bedeutung.

Verhinderung der endgültigen Löschung

Wenn die Funktion "Prevent Destruction" (Endgültige Löschung verhindern) aktiviert ist, kann das Share oder Projekt nicht endgültig gelöscht werden. Dies umfasst die endgültige Löschung eines Shares über abhängige Klons, die endgültige Löschung eines Shares innerhalb eines Projekts sowie die endgültige Löschung eines Replikationspackage. Shares, die über Replikationsupdates endgültig gelöscht wurden, sind davon jedoch nicht betroffen. Wird ein Share auf einer ZFSSA, die als Replikationsquelle dient, endgültig gelöscht, wird das entsprechende Share auf dem Ziel ebenfalls endgültig gelöscht, auch wenn diese Eigenschaft eingerichtet ist.

Um das Share endgültig zu löschen, muss die Eigenschaft zuerst in einem separaten Schritt explizit deaktiviert werden. Diese Eigenschaft ist standardmäßig deaktiviert.

Remote-Admin-Zugriff

In diesem Abschnitt wird die Remote-Zugriffssicherheit für die ZFSSA beschrieben.

Browserbenutzeroberfläche (Browser User Interface, BUI)

Auf den Bildschirmen "BUI Services" können Sie die Remote-Zugriffsservices und -einstellungen anzeigen und ändern.

SSH (Secure Shell)

Mit SSH können sich Benutzer über die Befehlszeilenschnittstelle (Command Line Interface, CLI) bei der ZFSSA anmelden und einen Großteil der Admin-Aktionen ausführen, die auch in der BUI ausgeführt werden können. SSH kann auch zur Ausführung automatisierter Skripte von einem Remote-Host, beispielsweise zum täglichen Abruf von Protokollen oder Analysestatistiken, verwendet werden.

Protokolle

In diesem Abschnitt werden auf die Sicherheit bezogene Protokollierungsfunktionen beschrieben.

Audit

Das Auditprotokoll zeichnet Aktivitätsereignisse auf, einschließlich BUI- und CLI-Anmeldungen- und Abmeldungen sowie Admin-Aktionen. In der folgenden Tabelle sind Beispiele für Auditprotokolleinträge dargestellt, wie sie in der BUI angezeigt würden:

TABELLE 2 Auditprotokolldatensatz

Uhrzeit	Benutzer	Host	Zusammenfassung	Sitzungsanmerkung
2009-10-12 05:20:24	Root	Galaxy	FTP-Service deaktiviert	
2009-10-12 03:17:05	Root	Galaxy	Benutzer angemeldet	
2009-10-11 22:38:56	Root	Galaxy	Timeout in Browsersitzung aufgetreten	
2009-10-11 21:13:35	Root	<console>	FTP-Service aktiviert	

Phone Home

Bei Verwendung der Funktion "Phone Home" zeigt dieses Protokoll Kommunikationsereignisse mit Oracle Support an. Die folgende Tabelle zeigt ein Beispiel für einen Phone Home-Eintrag, wie er in der BUI angezeigt würde:

TABELLE 3 Phone Home - Protokolldatensatz

Uhrzeit	Beschreibung	Ergebnis
2009-10-12 05:24:09	Datei "cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz" an Oracle Support hochgeladen	OK

Weitere Informationen

Kontextbezogene Onlinehilfe zu den einzelnen Seiten der ZFSSA-Browserbenutzeroberfläche (BUI) erhalten Sie, wenn Sie oben links auf der jeweiligen Seite auf die Schaltfläche "Hilfe" klicken.

Vollständige Produktinformationen für die Oracle ZFS Storage Appliance finden Sie unter folgendem Link:

www.oracle.com/us/products/servers-storage/storage/nas/overview

Dokumentationszuordnung

Über die nachfolgenden Tabellen finden Sie detaillierte Dokumentationen zu den einzelnen Services, Konfigurationen oder sonstigen Funktionen der ZFSSA. Wenn Sie eine ZFSSA über die BUI konfigurieren, können Sie über den Link "HELP" (HILFE) oben rechts im Bildschirm Hilfe zu dem jeweiligen Bildschirm aufrufen.

TABELLE 4 Services

Service	Dokumentation zu finden unter
Active Directory	Services:Active_Directory

Service	Dokumentation zu finden unter
Identitätszuordnung	Services:Identity_Mapping
DNS	Services:DNS
Dynamisches Routing	Services:Dynamic_Routing
IPMP	Services:IPMP
NTP	Services:NTP
Phone Home	Services:Phone_Home
Servicetags	Services:Service_Tags
SMTP	Services:SMTP
SNMP	Services:SNMP
Syslog	Services:Syslog
Systemidentität	Services:System_Identity
SSH	Services:SSH

TABELLE 5 Konfiguration

Konfiguration	Dokumentation zu finden unter
SAN	Configuration:SAN
SAN: FC	Configuration:SAN:FC
SAN: iSCSI	Configuration:SAN:iSCSI
SAN: SRP	Configuration:SAN:SRP
Cluster	Configuration:Cluster
Benutzer	Configuration:Users
Voreinstellungen	Configuration:Preferences
Alarme	Configuration:Alerts
Speicherung	Configuration:Storage

TABELLE 6 Speicherung

Speicherung	Dokumentation zu finden unter
Shares	Shares
Konzepte	Shares:Concepts
Schattenmigration	Shares:Shadow_Migration
Speicherverwaltung	Shares:Space_Management
Dateisystem - Namespace	Shares:File system_Namespace
Shares	Shares:Shares
Allgemein	Shares:Shares:General
Protokolle	Shares:Shares:Protocols
Zugang	Shares:Shares:Access
Snapshots	Shares:Shares:Snapshots

Speicherung	Dokumentation zu finden unter
Projekte	Shares:Projects
Projekte: Allgemein	Shares:Projects:General
Projekte: Protokolle	Shares:Projects:Protocols
Projekte: Replikation	Shares:Projects:Replication
Schema	Shares:Schema

ORACLE®