Oracle® ZFS Storage Appliance - Sicherheitshandbuch, Release 2013.1.4.0

Teilenr.: E61634-01
April 2015

ORACLE

Teilenr.: E61634-01

Barrierefreie Dokumentation

Informationen zu Oracles Verpflichtung zur Barrierefreiheit erhalten Sie über die Website zum Oracle Accessibility Program `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Zugriff auf Oracle-Support

Oracle-Kunden mit einem gültigen Oracle Supportvertrag haben Zugriff auf elektronischen Support über My Oracle Support. Weitere Informationen erhalten Sie unter `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` oder unter `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`, falls Sie eine Hörbehinderung haben.

Inhalt

Oracle ZFS Storage Appliance - Sicherheitshandbuch

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 von Oracle ZFS Storage Appliance zu erhalten. Vorgehensweisen zur Appliance-Konfiguration finden Sie im „Oracle ZFS Storage Appliance Administration Guide“.

In den folgenden Abschnitten werden die Sicherheitsfunktionen und -empfehlungen für Oracle ZFS Storage Appliance beschrieben:

- **Erste Schritte** - Beschreibt die Anmeldungssicherheit bei der Erstinstallation der Appliance und enthält Empfehlungen für die physische Sicherheit Ihres Systems.
- **Administratives Modell** - Beschreibt den Remote-Zugriff über BUI und CLI, die Begrenzung des Zugriffs auf BUI und CLI, das Systempatchingmodell, verzögerte Updates, Supportbündel und Backup der Konfiguration.
- **Appliance-Benutzer** – Beschreibt, wer über administrative Rollen die Appliance verwalten darf und wie Benutzerberechtigungen verwaltet werden.
- **Access Control-Listen** – Beschreibt das Verfahren, mit dem Zugriff auf Dateien und Verzeichnisse gewährt oder verweigert werden kann.
- **Datenservices** – Beschreibt die von der Appliance unterstützten Datenservices und die von den verschiedenen Datenservices bereitgestellte Sicherheit.
- **Directory Services** – Beschreibt die Directory Services, die auf der Appliance konfiguriert werden können, und deren Sicherheitsauswirkungen.
- **Systemeinstellungen** – Beschreibt die Systemeinstellungen zu Phone Home, Servicetags, SMTP, SNMP, Syslog, Systemidentität, Datenträgerbereinigung und Verhinderung der endgültigen Löschung.
- **Sicherheitslogs** - Beschreibt die Logtypen für die Sicherheit.

Erste Schritte

In diesem Abschnitt wird die Anmeldungssicherheit bei der Erstinstallation der Appliance beschrieben; er enthält außerdem Empfehlungen für die physische Sicherheit Ihres Systems.

Erstinstallation

Oracle ZFS Storage Appliance wird mit vorinstallierter Appliance-Software geliefert. 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. Wenn Oracle ZFS Storage Appliance auf die Werkseinstellungen zurückgesetzt wird, wird das Root-Kennwort ebenfalls auf den Standardwert für die Appliance und den Serviceprozessor zurückgesetzt.

Während der Erstinstallation einer Oracle ZFS Storage Appliance liegt ein Standardkontoname und -passwort vor, das mit dem Serviceprozessor des Systems verknüpft ist. Mit diesem Standardkonto erhält der Systemadministrator erstmals Zugriff auf die Appliance 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 Appliance. 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.

Oracle ZFS Storage Appliance unterliegt Zugriffsbeschränkungen. Der Zugriff wird mithilfe eines Sicherheitsmechanismus kontrolliert (z.B. einem Schlüssel, einer Sperre, einem Tool oder einem Werksausweis), 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 das administrative Modell von Oracle ZFS Storage Appliance beschrieben.

Remote-Admin-Zugriff

In diesem Abschnitt wird die Sicherheit beim Remote-Zugriff auf Oracle ZFS Storage Appliance beschrieben.

Browserbenutzeroberfläche

Die BUI (Browserbenutzeroberfläche) wird für die allgemeine Verwaltung der Appliance verwendet. Auf den Bildschirmen "BUI Services" können Sie die Remote-Zugriffsservices und -einstellungen anzeigen und ändern.

Die Verwaltung erfolgt über eine sichere HTTP- (HTTPS-)Browsersession. HTTPS-Sessions werden mit einem selbstsignierten Zertifikat verschlüsselt, das bei der Erstinstallation speziell für jede Oracle ZFS Storage Appliance generiert wird. HTTPS-Sessions haben ein vom Benutzer definierbares Standardsessiontimeout von 15 Minuten.

Befehlszeilenschnittstelle

Mit der CLI (Command Line Interface) können die meisten administrativen Aktionen ausgeführt werden, die auch in der BUI ausgeführt werden.

Mit Secure Shell (SSH) können sich Benutzer bei Oracle ZFS Storage Appliance über eine Secure Sockets Layer-(SSL-)Verbindung bei der CLI anmelden. SSH kann auch zur Ausführung automatisierter Skripte von einem Remote-Host, beispielsweise zum täglichen Abruf von Logs oder Analysestatistiken, verwendet werden.

Eingeschränkte Benutzerberechtigung

Der administrative Zugriff ist auf den Root-Benutzer, lokale Administratoren mit den entsprechenden Berechtigungen und Benutzer begrenzt, die über Identity Server wie beispielsweise Lightweight Directory Access Protocol (LDAP) und Network Information Service (NIS) autorisiert wurden.

Oracle ZFS Storage Appliance RESTful API

Mit der Oracle ZFS Storage Appliance RESTful API kann Oracle ZFS Storage Appliance verwaltet werden. Die RESTful-Architektur basiert auf einem überlagerten Client-Server-Modell, mit dem Services transparent über Standard-Hubs, Router und andere Netzwerksysteme ohne Clientkonfiguration umgeleitet werden können.

Die Oracle ZFS Storage Appliance RESTful API verwendet dieselben Authentifizierungszugangsdaten wie die BUI und CLI. Alle Anforderungen von externen Clients werden individuell mit den Appliance-Zugangsdaten authentifiziert und werden über

eine HTTPS-Verbindung zu Port 215 geführt. Die RESTful API unterstützt HTTPS-Sessions, die über ein benutzerdefinierbares Standardtimeout von 15 Minuten verfügen.

Informationen zur Verwaltung von Oracle ZFS Storage Appliance mit der RESTful API finden Sie in der Dokumentation „Oracle ZFS Storage Appliance RESTful API Guide“.

Systemupdates

Damit Sie stets die neuesten Sicherheitserweiterungen nutzen können, empfiehlt Oracle, dass Sie Ihre Systemsoftware auf dem neuesten Stand halten.

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" registriert ist und es zu einem schwerwiegenden Ausfall kommt, 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.

Appliance-Benutzer

Es gibt zwei Arten von Oracle ZFS Storage Appliance-Benutzern:

- **Datenservicebenutzer** – Clients, die mit den unterstützten Protokollen wie Network File System (NFS), Server Message Block (SMB), Fibre Channel, Internet Small Computer System Interface (iSCSI), Hypertext Transfer Protocol (HTTP) und File Transfer Protocol (FTP) auf Datei- und Blockressourcen zugreifen.
- **Benutzer mit Administratorrechten** – Benutzer, die die Konfiguration und Services auf der Appliance verwalten.

Dieser Abschnitt bezieht sich nur auf Benutzer mit Administratorrechten.

Benutzer mit Administratorrechten - Rollen

Sie erteilen Administratoren Berechtigungen, indem Sie ihnen benutzerdefinierte Rollen zuweisen. 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** – Lokale Benutzer speichern alle Kontoinformationen in Oracle ZFS Storage Appliance.
- **Directory-Benutzer** – Vorhandene NIS- oder LDAP-Konten werden verwendet, und zusätzliche Berechtigungseinstellungen werden in der Appliance gespeichert. Der Zugriff auf die Appliance muss vorhandenen NIS-/LDAP-Benutzern explizit erteilt werden, die sich dann bei der Appliance anmelden und diese verwalten können. Der Zugriff kann nicht standardmäßig erteilt werden.

Administrative Geltungsbereiche

Mithilfe von Berechtigungen können Benutzer bestimmte Aufgaben ausführen, wie beispielsweise das Erstellen von Shares, den Neustart der Appliance 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 (ACLs)

Oracle ZFS Storage Appliance gewährt den Dateizugriff über Access Control-Listen (ACLs). Mit einer ACL wird der Zugriff auf eine bestimmte Datei oder ein bestimmtes Verzeichnis gewährt oder abgelehnt.

Das von Oracle ZFS Storage Appliance 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 Storage Appliance 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 ablehnt, für wen der ACE gilt und welche Übernahmeflags verwendet werden.

ACL-Übernahme

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

Datenservices

Die folgende Tabelle enthält eine Beschreibung sowie die Ports, die für jeden Datenservice verwendet werden.

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
Virenscan	Virenscan des Dateisystems	
FTP	Dateisystemzugriff über das FTP-Protokoll	21
HTTP	Dateisystemzugriff über das HTTP-Protokoll	80
HTTPS	Für eingehende sichere Verbindungen	443
NDMP	NDMP-Hostservice	10000

SERVICE	BESCHREIBUNG	VERWENDETE PORTS
Remote-Replikation	Remote-Replikation	216 und 217
Verschlüsselung	Transparente Verschlüsselung für Dateisysteme und LUNs	
Schattenmigration	Schattendatenmigration	
SFTP	Dateisystemzugriff über das SFTP-Protokoll	218
TFTP	Dateisystemzugriff über das TFTP-Protokoll	
Storage Area Network	Storage Area Network-Ziel- und Initiatorengruppen	

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 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 Filesharing über HTTP verwendet wird (in der Regel ist das nicht der Fall):

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

Ausgehende Ports

- tcp/80 (WEB)

Anmerkung - Verwenden Sie bei der Replikation Generic Routing Encapsulation-Tunnels (GRE-Tunnels), wenn möglich. So kann der Verkehr über die Backend-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 Frontend-Schnittstelle durchgeführt werden. In diesem Fall müssen die Ports 216 und 217 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 User-ID (UID) und Gruppen-ID (GID) des Clients ohne Authentifizierung vom NFS-Server an das Netzwerk übergeben. Dieses Authentifizierungsverfahren 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-Domains 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
- **krb5** - krb5 plus Integritätsschutz (Datenpakete sind vor Manipulation geschützt)
- **krb5** - 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.
- **krb5** - 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.
- **krb5** - nur Kerberos v5-Datenschutz, Clients müssen mit diesem Typ mounten.

iSCSI-Datenservice

Wenn Sie eine LUN in Oracle ZFS Storage Appliance konfigurieren, können Sie dieses Volume über ein iSCSI-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 (Challenge-Handshake Authentication Protocol). Außerdem unterstützt der Service die CHAP-Authentifizierungsdatenverwaltung in einer RADIUS-(Remote Authentication Dial-In User Service-)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 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 Oracle ZFS Storage Appliance eine CHAP-Authentifizierung mittels RADIUS ausführen kann, müssen folgende Angaben gemacht werden:

- Die Appliance 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 Appliance 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 Appliance keinen separaten Initiatoreintrag für jedes Initiatorfeld erfordert, kann der RADIUS-Server alle Authentifizierungsschritte durchführen.
- Verwendet der Initiator einen anderen CHAP-Namen, muss die Appliance 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-Datenservice

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-Domainmodus

Im Domainmodus werden Benutzer in Microsoft Active Directory (AD) definiert. SMB-Clients können mit der Kerberos- oder NTLM-Authentifizierung Verbindung zu Oracle ZFS Storage Appliance herstellen.

Wenn sich ein Benutzer über einen vollqualifizierten Oracle ZFS Storage Appliance-Hostnamen anmeldet, verwenden Windows-Clients in derselben oder einer vertrauenswürdigen Domain die Kerberos-Authentifizierung. Ansonsten verwenden sie die NTLM-Authentifizierung.

Verwendet ein SMB-Client die NTLM-Authentifizierung zur Anmeldung bei der Appliance, werden die Zugangsdaten des Benutzers zur Authentifizierung an den AD-Domaincontroller 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 Appliance anmelden. Weitere Informationen finden Sie in folgendem Microsoft Developer Network-Artikel:

http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx

Nach der Authentifizierung wird für die SMB-Session 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 in Oracle ZFS Storage Appliance definiert. Wenn ein SMB-Client Verbindung zu einer Appliance im Arbeitsgruppenmodus herstellt, werden Benutzername- und Passwort-Hashes zur lokalen Authentifizierung des Benutzers verwendet.

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

In der folgenden Liste wird das Verhalten von Oracle ZFS Storage Appliance für jede LM-Kompatibilitätsebene aufgeführt:

- 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 Appliance 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 Domainbenutzergruppen, 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

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 Microsoft Management Console (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 und ändern.

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 wird von einer externen Engine ausgeführt, mit der Oracle ZFS Storage Appliance Verbindung aufnimmt. Die externe Engine ist nicht im Lieferumfang der Appliance-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 Oracle Solaris-Framework.

Datenverschlüsselung bei Kabelverbindungen

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

FTP-Datenservice

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. Der FTP-Server verwendet entweder ein selbstsigniertes Sicherheitszertifikat oder ein vom Kunden bereitgestelltes Zertifikat.
- **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 potenzielle 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 (Loggingebene)** – Der Ausführlichkeitsgrad des Logs.

FTP unterstützt die folgenden Logs:

- **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-Datenservice

HTTP bietet Zugriff auf Dateisysteme über die HTTP- und HTTPS-Protokolle sowie die HTTP-Erweiterung WebDAV (Web based Distributed Authoring and Versioning). Auf diese Weise können Clients auf Shared File-Systeme über einen Webbrowser oder als lokales Dateisystem zugreifen, wenn die Clientsoftware dies zulässt.

Der HTTPS-Server verwendet entweder ein selbstsigniertes Sicherheitszertifikat oder ein vom Kunden bereitgestelltes Zertifikat. Um ein vom Kunden bereitgestelltes Zertifikat zu erhalten, müssen Sie ein Certificate Signing Request (CSR) erstellen und von einer Certificate Authority (CA) signieren lassen. Nachdem das signierte Zertifikat von der CA zurückgesendet wurde, kann es auf der Appliance installiert werden. Wenn ein Zertifikat nicht von einer Root-CA signiert wird, benötigen Sie auch Zertifikate der CAs auf zweiter Ebene und höheren Ebenen. Weitere Informationen zur Zertifikatverwaltung finden Sie im *Oracle ZFS Storage Appliance - Administrationshandbuch*.

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.

Wenn die Option "Require Client Login" aktiviert ist, verweigert Oracle ZFS Storage Appliance 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. Wenn "Require Client Login" deaktiviert ist, versucht die Appliance keine Authentifizierung der Zugangsdaten.

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-Datenservice

Mit dem Network Data Management Protocol (NDMP) kann Oracle ZFS Storage Appliance an NDMP-basierten Backup- und Restore-Vorgängen teilnehmen, die von einem Remote-NDMP-Client gesteuert werden, der als Data Management Application (DMA) bezeichnet wird. Über NDMP können Appliance-Benutzerdaten (Beispiel: Daten, die in von einem Administrator erstellten Shares in der Appliance 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-Replikationsdatenservice

Die Remote-Replikation von Oracle ZFS Storage Appliance vereinfacht die Replikation von Projekten und Shares. Mit diesem Service können Sie anzeigen, welche Appliances Daten an eine bestimmte Appliance repliziert haben, und können kontrollieren, welche Appliances eine bestimmte Appliance replizieren kann.

Wenn dieser Service aktiviert ist, erhält die Appliance Replikationsupdates von anderen Appliances 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 Appliance konfigurieren zu können, ist das Root-Passwort für die Remote-Appliance erforderlich. Diese Ziele werden zur Einrichtung einer Replikations-Peer-Verbindung verwendet, mit deren Hilfe die Appliances 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 Appliances in nachfolgenden Kommunikationen identifiziert werden.

Die generierten Schlüssel werden als Teil der Appliance-Konfiguration dauerhaft gespeichert. Das Root-Passwort wird niemals dauerhaft gespeichert und auch nicht unverschlüsselt übertragen. Alle Appliance-Kommunikationen, einschließlich des anfänglichen Identitätsaustauschs, werden über SSL geschützt.

Mit der Offlinereplikationsfunktion der Oracle ZFS Storage Appliance können beim Replizieren großer Datenmengen über ein Netzwerk mit begrenzter Bandbreite Zeitaufwand, Ressourcen und mögliche Datenfehler reduziert werden. Bei der Offlinereplikation wird der Replikationsstream in eine Datei auf dem NFS-Server exportiert, die anschließend physisch an den Remote-Zielstandort verschoben oder optional für den Versand auf ein externes Medium kopiert werden kann. Am Zielstandort importiert der Administrator die Datei mit dem Replikationsstream auf die Ziel-Appliance.

Um den Zugriff auf den exportierten Replikationsstream zu begrenzen, geben Sie das NFS Share nur für die IP-Adressen der Quell- und Ziel-Appliances frei. Um die Daten zu verschlüsseln, aktivieren Sie die Verschlüsselung auf dem Datenträger für das NFS Share auf dem NFS-Server. Weitere Informationen finden Sie in der Dokumentation des NFS-Servers. Beachten Sie, dass ein exportierter Replikationsstream keinesfalls von der Appliance verschlüsselt wird.

Mit Datenverschlüsselung arbeiten

LIZENZHINWEIS: *Verschlüsselung kann kostenlos evaluiert werden, die Funktion erfordert jedoch den separaten Erwerb einer unabhängigen Lizenz zur Verwendung im Production-Betrieb. Die Verschlüsselung kann nur auf Oracle ZFS Storage ZS4-4 und Oracle ZFS Storage ZS3-4 lizenziert werden. Nach Ablauf des Evaluierungszeitraums muss diese Funktion lizenziert oder deaktiviert werden. Oracle behält sich das Recht vor, jederzeit auf Lizenzierungscompliance zu prüfen. Weitere Einzelheiten finden Sie in "Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options".*

Oracle ZFS Storage Appliance bietet transparente Datenverschlüsselung für einzelne Shares (Dateisysteme und LUNs) und Shares, die innerhalb von Projekten erstellt wurden.

Verschlüsselungsschlüssel verwalten

Die Appliance umfasst einen integrierten LOCAL-Keystore und die Möglichkeit der Verbindung zu dem OKM-(Oracle Key Manager-)System. Jedes verschlüsselte Projekt oder Share erfordert einen umschließenden Schlüssel aus dem LOCAL- oder OKM-Keystore. Die Datenverschlüsselungsschlüssel werden von der Storage Appliance verwaltet und dauerhaft von dem umschließenden Schlüssel aus dem LOCAL- oder OKM-Keystore verschlüsselt gespeichert.

OKM ist ein umfassendes Key Management System (KMS), das die schnell wachsenden Unternehmensanforderungen für speicherbasierte Datenverschlüsselung löst. Entwickelt zur Konformität mit Open Standard bietet diese Funktion die Kapazität, Skalierbarkeit und Interoperabilität zur zentralen Verwaltung von Verschlüsselungsschlüsseln über weit verteilte und heterogene Speicherungsinfrastrukturen.

OKM erfüllt die einmaligen Herausforderungen der Verwaltung von Speicherschlüsseln, einschließlich:

- **Langfristige Schlüsselaufbewahrung** - OKM stellt sicher, dass Archivdaten immer verfügbar sind, OKM bewahrt Verschlüsselungsschlüssel während des ganzen Datenlebenszyklus auf.
- **Interoperabilität** - OKM stellt die Interoperabilität bereit, die zur Unterstützung eines breiten Spektrums an Speichergeräten, die Mainframe- oder offenen System zugeordnet sind, unter einem einzigen Speicherschlüsselverwaltungsservice erforderlich ist.
- **Hohe Verfügbarkeit** - Mit aktivem N-Knoten-Clustering, dynamischem Lastausgleich und automatisiertem Failover stellt OKM hohe Verfügbarkeit bereit, unabhängig davon, ob Appliances in einer Site gruppiert oder über die ganze Welt verteilt sind.
- **Hohe Kapazität**- OKM verwaltet eine große Anzahl von Speichergeräten und sogar noch mehr Speicherschlüssel. Eine einzelne geclusterte Appliance kann Schlüsselverwaltungsservices für Tausende von Speichergeräten und Millionen von Speicherschlüsseln bereitstellen.
- **Flexible Schlüsselkonfiguration** - Schlüssel können pro OKM-Cluster automatisch generiert oder individuell für einen LOCAL- oder OKM-Keystore erstellt werden. Sicherheitsadministratoren sind für die Weitergabe von Schlüsselnamen verantwortlich, die in Kombination mit dem Keystore einen bestimmten umschließenden Schlüssel mit einem Projekt oder Share verknüpfen.

Verwaltung von Schlüsseln

Auf Shares und Projekte, die OKM-Schlüssel verwenden, die sich in einem deaktivierten Status befinden, kann weiterhin zugegriffen werden. Um zu verhindern, dass ein OKM-Schlüssel verwendet wird, muss der OKM -Administrator den Schlüssel explizit löschen.

Um sicherzustellen, dass auf verschlüsselte Shares und Projekte zugegriffen werden kann, erstellen Sie ein Backup der Appliance-Konfigurationen und der LOCAL-Keystore-Schlüsselwerte. Wenn Schlüssel nicht mehr verfügbar sind, kann auf Shares oder Projekte, die

diese Schlüssel verwenden, nicht mehr zugegriffen werden. Wenn der Schlüssel eines Projekts nicht mehr verfügbar ist, können keine neuen Shares in diesem Projekt erstellt werden.

Schlüssel können aus folgenden Gründen nicht mehr verfügbar sein:

- Schlüssel werden gelöscht
- Rollback zu einem Release, das keine Verschlüsselung unterstützt
- Rollback zu einem Release, in dem die Schlüssel nicht konfiguriert sind
- Werksseitige Rücksetzung
- Der OKM-Server ist nicht verfügbar.

Lebenszyklus des Verschlüsselungsschlüssels

Der Lebenszyklus des Verschlüsselungsschlüssels ist flexibel, weil Sie Schlüssel jederzeit ändern können, ohne Datenservices offline zu setzen.

Wenn ein Schlüssel aus dem Keystore gelöscht wird, werden alle Shares, die den Schlüssel verwenden, aufgehoben und auf ihre Daten kann nicht mehr zugegriffen werden. Das Backup von Schlüsseln im OKM-Keystore muss mit den OKM-Backupservices ausgeführt werden. Das Backup von Schlüsseln im LOCAL-Keystore ist Bestandteil des Systemkonfigurationsbackups der Appliance. Bei dem LOCAL-Keystore kann der Schlüssel beim Erstellen auch nach Wert angegeben werden, damit er in einem externen System hinterlegt wird. Dadurch ergibt sich eine alternative Backup-/Restore-Möglichkeit pro Schlüssel.

Schattenmigrationsdatenservice

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 in einer NFS-Quelle unterliegen nicht der Kontrolle des Oracle ZFS Storage Appliance-Benutzers. Daher können Schattenmigrationsmounts nicht sicher sein; wenn der Server eine Kerberos- oder eine ähnliche Anforderung erwartet, wird der Quellmount abgelehnt.

SFTP-Datenservice

Mit dem SSH File Transfer Protocol (SFTP) kann von SFTP-Clients auf das Dateisystem zugegriffen werden. 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.

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

TFTP-Datenservice

Das Trivial File Transfer Protocol (TFTP) ist ein einfaches Protokoll zur 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.

Storage Area Network

In einem SAN (Storage Area Network) 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.

Anmerkung - Die Verwendung der Standardinitiatorgruppe könnte zu unerwünschten oder nicht vereinbaren LUN-Initiatoren führen.

Directory Services

In diesem Abschnitt werden die Directory Services beschrieben, die auf der Appliance konfiguriert werden können, sowie deren Sicherheitsauswirkungen.

Network Information Service

NIS (Network Information Service) ist ein Namensservice für eine zentralisierte Verzeichnisverwaltung. Oracle ZFS Storage Appliance 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 Appliance-Administration erhalten. Die Appliance ergänzt die NIS-Informationen mit ihren eigenen Berechtigungseinstellungen.

Lightweight Directory Access Protocol

Oracle ZFS Storage Appliance verwendet Lightweight Directory Access Protocol (LDAP) zur Authentifizierung von Benutzern mit Administratorrechten und Benutzern einiger Datenservices (FTP, HTTP). LDAP-over-SSL-Sicherheit wird von der Appliance 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 Namen für und von Benutzern und Gruppen für Datenprotokolle wie NFSv4 zu, die Namen verwenden.
- Definiert die Gruppenmitgliedschaft zur Verwendung bei der Zugriffskontrolle.
- Überträgt optional Authentifizierungsdaten zur Admin- und Datenzugriffsauthentifizierung.

LDAP-Verbindungen können als Authentifizierungsverfahren verwendet werden. Beispiel: Bei einem Versuch eines Benutzers, sich bei Oracle ZFS Storage Appliance zu authentifizieren, kann die Appliance 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):
  - Nicht gesichert
  - Der Server wird über Kerberos authentifiziert
  - Der Server wird über ein TLS-Zertifikat authentifiziert

Über eine LDAP-Verbindung übertragene Daten werden verschlüsselt, sofern Kerberos oder TLS verwendet wird; 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 in Oracle ZFS Storage Appliance mit SMB oder NFS zugreifen, und jeder Client hat 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 Appliance 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.

Identity Management for UNIX

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 RFC 2307 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 Oracle ZFS Storage Appliance-Registrierung sowie der Remote-Supportservice von Phone Home verwaltet. In diesen Meldungen werden keine Benutzerdaten oder Metadaten übertragen.

Bei der Registrierung wird Ihre Oracle ZFS Storage Appliance 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 Oracle ZFS Storage Appliance 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.

Simple Mail Transport Protocol

Das Simple Mail Transport Protocol (SMTP) sendet alle von Oracle ZFS Storage Appliance generierten Mails, im Allgemeinen als Reaktion auf konfigurierte Alerts. SMTP nimmt keine externen Mails an, sondern sendet nur Mails, die von der Appliance 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 Domain der Appliance konfiguriert ist oder für die Zieldomain für ausgehende Mails keine DNS MX-Datensätze ordnungsgemäß eingerichtet sind, kann die Appliance so konfiguriert werden, dass alle Mails über einen ausgehenden Mailserver weitergeleitet werden.

SNMP (Simple Network Management Protocol)

Das Simple Network Management Protocol (SNMP) stellt zwei Funktionen in Oracle ZFS Storage Appliance bereit: Appliance-Statusinformationen können von SNMP verarbeitet werden, und Alerts können so konfiguriert werden, dass SNMP-Traps gesendet werden. Verfügbar sind die beiden SNMP-Versionen 1 und 2c.

Syslog-Meldung

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

- Alert-Konfiguration zur Versendung von Syslog-Meldungen an ein oder mehrere Remote-Systeme
- Weiterleitung von Syslog-Meldungen an Remote-Systeme für Syslog-fähige Services in der Appliance

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 Appliance
- 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. Systemname und -verzeichnis müssen möglicherweise geändert werden, wenn Oracle ZFS Storage Appliance in ein anderes Netzwerkverzeichnis verschoben oder einem anderen Zweck zugeführt wird.

Datenträgerbereinigung

Eine Datenträgerbereinigung sollte in regelmäßigen Abständen vorgenommen werden, damit Oracle ZFS Storage Appliance 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 rechtzeitige 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 Oracle ZFS Storage Appliance, 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.

Sicherheitslogs

In diesem Abschnitt werden auf die Sicherheit bezogene Loggingfunktionen beschrieben.

Auditlog

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

TABELLE 2 Auditlogdatensatz

Uhrzeit	Benutzer	Host	Zusammenfassung	Sessionanmerkung
2013-10-12 05:20:24	Root	Galaxy	FTP-Service deaktiviert	
2013-10-12 03:17:05	Root	Galaxy	Benutzer angemeldet	

Uhrzeit	Benutzer	Host	Zusammenfassung	Sessionanmerkung
2013-10-11 22:38:56	Root	Galaxy	Browsersession wegen Timeout abgebrochen	
2013-10-11 21:13:35	Root	<console>	FTP-Service aktiviert	

Phone Home-Log

Bei Verwendung der Funktion "Phone Home" zeigt dieses Log 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 - Logdatensatz

Uhrzeit	Beschreibung	Ergebnis
2013-10-12 05: 24:09	Datei "cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz" an Oracle Support hochgeladen	OK

Weitere Informationen

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

https://www.oracle.com/storage/nas/index.html

Wenn Sie die Oracle ZFS Storage Appliance über die BUI konfigurieren, können Sie über den Hilfe-Link oben rechts im Bildschirm Hilfe zu dem jeweiligen Bildschirm aufrufen. Anhand der folgenden Tabellen können Sie eine detaillierte Dokumentation für alle sicherheitsbezogenen Services, Konfigurationen und anderen Funktionen der Appliance ermitteln.

TABELLE 4 Servicedokumentation

Service	Dokumentationsverzeichnis
Active Directory	Services:Active_Directory
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

Service	Dokumentationsverzeichnis
SMTP	Services:SMTP
SNMP	Services:SNMP
Syslog	Services:Syslog
Systemidentität	Services:System_Identity
SSH	Services:SSH

TABELLE 5 Konfigurationsdokumentation

Konfiguration	Dokumentationsverzeichnis
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
Alerts	Configuration:Alerts
Speicherung	Configuration:Storage

TABELLE 6 Speicherdokumentation

Speicherung	Dokumentationsverzeichnis
Shares	Shares
Konzepte	Shares:Concepts
Schattenmigration	Shares:Shadow_Migration
Speicherplatzverwaltung	Shares:Space_Management
Dateisystem-Namespace	Shares:Filesystem_Namespace
Shares	Shares:Shares
Allgemein	Shares:Shares:General
Protokolle	Shares:Shares:Protocols
Zugriff	Shares:Shares:Access
Snapshots	Shares:Shares:Snapshots
Projekte	Shares:Projects
Projekte: Allgemein	Shares:Projects:General
Projekte: Protokolle	Shares:Projects:Protocols
Projekte: Replikation	Shares:Projects:Replication
Schema	Shares:Schema
Verschlüsselung	Shares:Encryption