# Oracle SuperCluster M7 Series - Sicherheitshandbuch

**Teilenr.: E69653-01**
Februar 2016

**Teilenr.: E69653-01**

Copyright © 2016, Oracle und/oder verbundene Unternehmen. All rights reserved. Alle Rechte vorbehalten.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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

**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

# Verwenden dieser Dokumentation

- **Überblick** – Enthält Informationen zur Planung, Konfiguration und Wartung einer sicheren Umgebung für Oracle SuperCluster M7 Series-Systeme.
- **Zielgruppe** – Techniker, Systemadministratoren und autorisierte Serviceprovider
- **Erforderliche Kenntnisse** – Umfassende Erfahrung mit UNIX und Datenbankverwaltung.

## Produktdokumentationsbibliothek

Dokumentation und Ressourcen für dieses Produkt und verwandte Produkte sind verfügbar unter http://www.oracle.com/goto/sc-m7/docs.

## Feedback

Auf folgender Website können Sie Feedback zu dieser Dokumentation angeben http://www.oracle.com/goto/docfeedback.

# Sicherheitsgrundsätze

Diese Dokumentation enthält Informationen zur Planung, Konfiguration und Wartung einer sicheren Umgebung für Oracle SuperCluster M7 Series-Systeme.

In diesem Abschnitt werden folgende Themen behandelt:

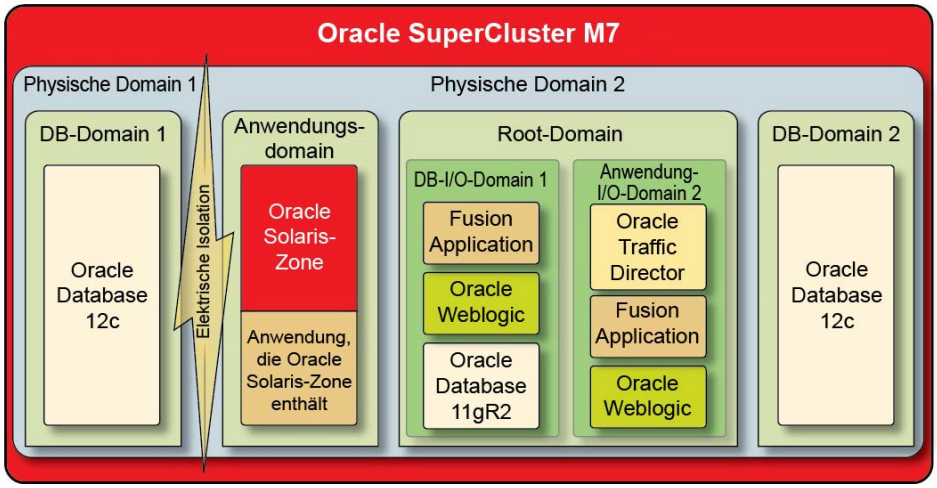


## Sichere Isolation

SuperCluster M7 unterstützt eine Vielzahl von Isolationsstrategien, die Cloud-Provider basierend auf ihren Sicherheits- und Versicherungsanforderungen auswählen können. Aufgrund dieser Flexibilität können Cloud-Provider eine benutzerdefinierte, sichere mehrmandantenfähige Architektur erstellen, die auf ihr Unternehmen zugeschnitten ist.

SuperCluster M7 unterstützt eine Reihe von Workload-Isolationsstrategien, jede mit ihren eigenen eindeutigen Möglichkeiten. Während jede Implementierungsstrategie unabhängig verwendet werden kann, können die Strategien auch in einer Hybridlösung gemeinsam verwendet werden, mit der Cloud-Provider Architekturen bereitstellen können, mit denen sie die Sicherheits-, Performance-, Verfügbarkeitsanforderungen usw. effizienter ausgleichen können.

**ABBILDUNG 1** Sichere Isolation mit einer dynamischen Mandantenkonfiguration




Cloud-Provider können physische Domains (auch als PDomains bezeichnet) in Fällen verwenden, in denen auf Mandantenhosts Anwendungen und Datenbanken ausgeführt werden, die physisch von anderen Workloads getrennt werden müssen. Dedizierte physische Ressourcen sind möglicherweise wegen der Wichtigkeit für das Unternehmen, der Vertraulichkeit der enthaltenen Informationen, der Complianceanforderungen oder einfach deshalb für ein Deployment erforderlich, weil die Datenbank- oder Anwendungs-Workload die Ressourcen eines ganzen physischen Systems voll ausschöpft.

Bei Unternehmen, die eine hypervisor-vermittelte Isolation erfordern, werden Oracle VM Server for SPARC-Domains, die als dedizierte Domains bezeichnet werden, für das Erstellen virtueller Umgebungen verwendet, die Anwendungs- und/oder Datenbankinstanzen isolieren. Im Rahmen der SuperCluster-Installation erstellt, führt jede dedizierte Domain ihre eigene Instanz des Oracle Solaris-BS aus. Der Zugriff auf physische Ressourcen wird über die hardwaregestützten Hypervisor vermittelt, die in den SPARC-Prozessoren integriert sind.

Außerdem können Sie mit SuperCluster zusätzliche Domains erstellen, die als Root-Domains bezeichnet werden und die SR-IOV-(Single Root-I/O-Virtualisierungs-)Technologie nutzen. Root-Domains verfügen über ein oder zwei IB-HCAs und 10 GbE-NICs. Sie können zusätzliche Domains, die als I/O-Domains bezeichnet werden, basierend auf Root-Domains erstellen. SuperCluster M7 umfasst ein browserbasiertes Tool, mit dem diese erstellt und verwaltet werden können.

Innerhalb jeder dieser Domains können Cloud-Consumermandanten die Oracle Solaris Zones-Technologie nutzen, um zusätzliche isolierte Umgebungen zu erstellen. Mit Zonen können einzelne Anwendungs- oder Datenbankinstanzen oder Gruppen von Anwendungs- oder Datenbankinstanzen in einem oder mehreren virtualisierten Containern bereitgestellt werden, die aufbauend auf einem einzelnen BS-Kernel kollektiv ausgeführt werden. Diese einfache Virtualisierungslösung wird verwendet, um eine stärkere Sicherheitsgrenze um bereitgestellte Services zu errichten.

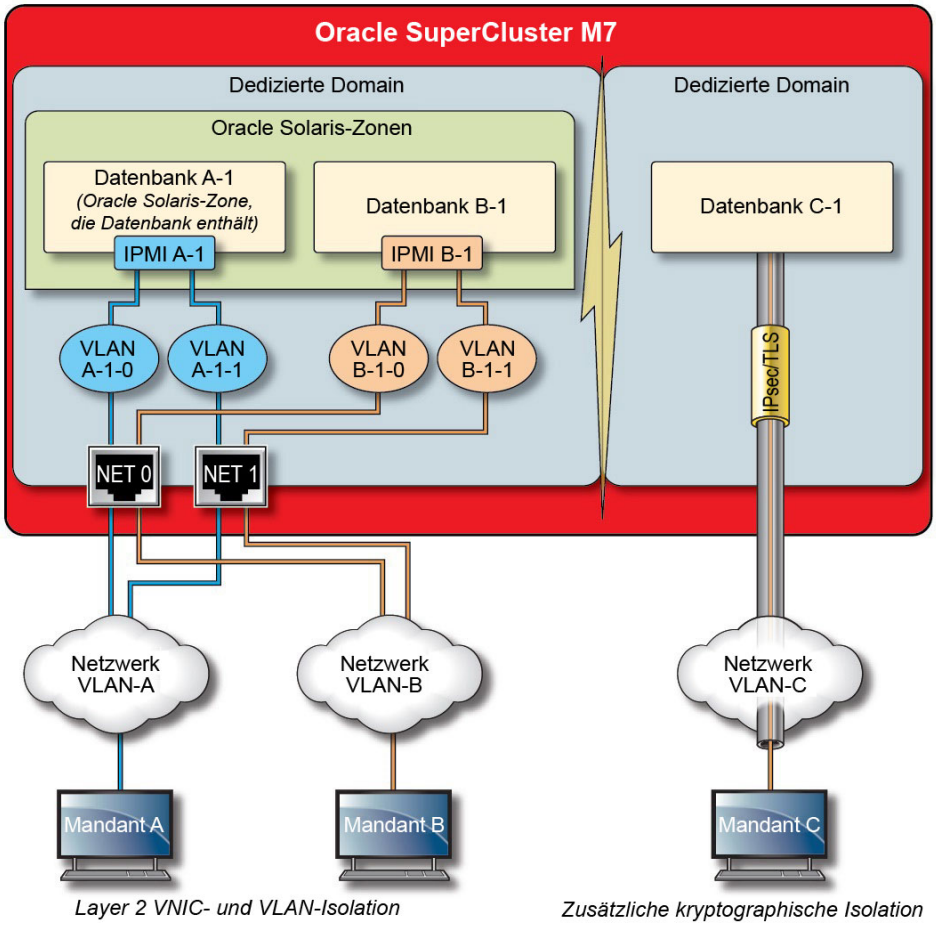
Mandanten, die mehrere Anwendungen und Datenbanken in SuperCluster hosten, können auch eine Hybridlösung nutzen, indem eine Kombination von Isolationsstrategien basierend auf Oracle Solaris Zones, I/O-Domains und dedizierten Domains verwendet wird, um flexible und dennoch robuste Architekturen zu erstellen, die ihren Anforderungen an die Cloud-Infrastruktur gerecht werden. Mit einer Reihe von Virtualisierungsoptionen können in der Cloud gehostete Mandanten mit SuperCluster sicher auf der Hardwareebene isoliert werden; außerdem stehen Oracle Solaris Zones für erweiterte Sicherheit und weitere Isolation in der Laufzeitumgebung bereit.

Die Gewährleistung, dass einzelne Anwendungen, Datenbanken, Benutzer und Prozesse in ihrem Host-BS isoliert sind, ist ein erster wichtiger Schritt. Die drei primären Netzwerke, die in SuperCluster verwendet werden, sind jedoch mindestens genauso wichtig; außerdem muss geprüft werden, wie die Netzwerkisolationsmöglichkeiten und Kommunikationen über das Netzwerk geschützt werden.

- 10 GbE-Clientzugriffsnetzwerk
- Privates IB-Servicenetzwerk
- Managementnetzwerk

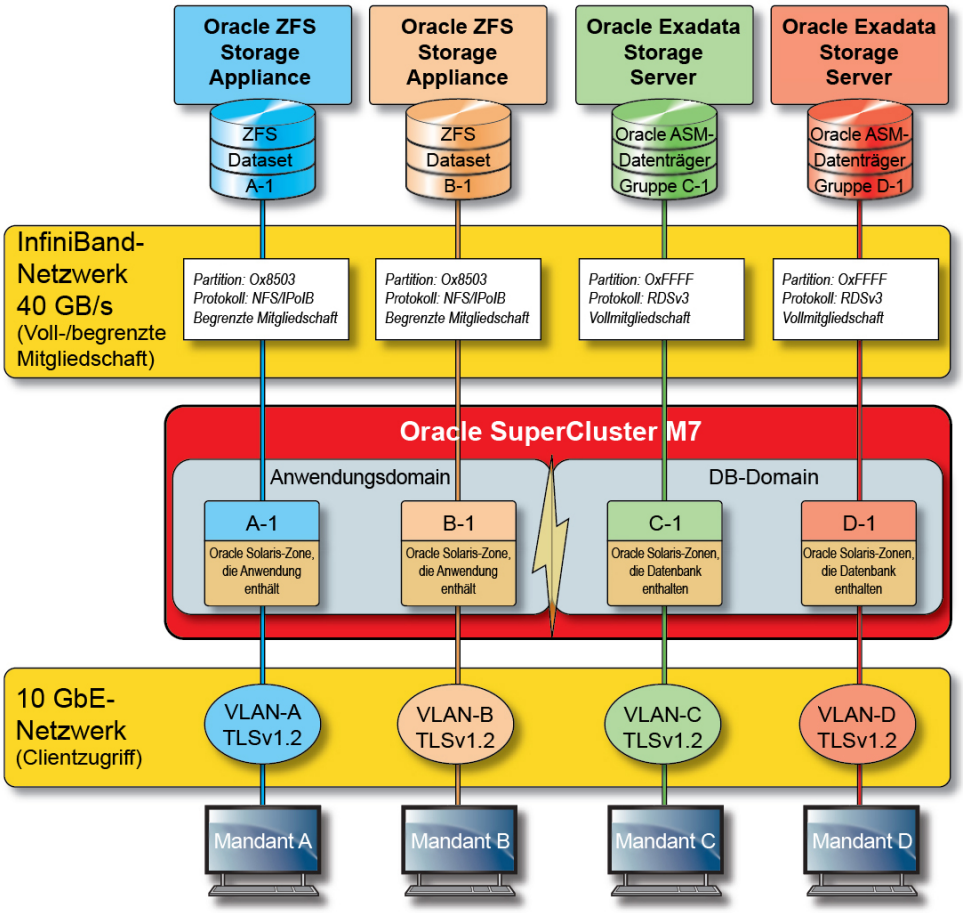
Der Netzwerkverkehr, der über das SuperCluster-Clientzugriffsnetzwerk fließt, kann mit verschiedenen Techniken isoliert werden. In dieser Abbildung wird eine mögliche Konfiguration dargestellt, in der vier Datenbankinstanzen so konfiguriert sind, dass sie in drei eindeutigen virtuellen LANs (VLANs) ausgeführt werden. Wenn die Netzwerkschnittstellen von SuperCluster zur Verwendung von VLANs konfiguriert werden, kann der Netzwerkverkehr zwischen für Oracle VM Server for SPARC dedizierten Domains sowie zwischen Oracle Solaris Zones isoliert werden.

**ABBILDUNG 2** Sichere Netzwerkisolation über das Clientzugriffsnetzwerk




SuperCluster umfasst ein privates IB-Netzwerk, das von Datenbankinstanzen für den Zugriff auf die Informationen verwendet wird, die in Exadata Storage Servern und der ZFS Storage Appliance gespeichert sind, sowie zur Ausführung der internen Kommunikation, die für Clustering und High Availability erforderlich ist. In dieser Abbildung wird eine sichere Netzwerkisolation in SuperCluster M7 dargestellt.

**ABBILDUNG 3** Sichere Netzwerkisolation bei dem 40 GBit/s IB-Netzwerk




Standardmäßig wird das SuperCluster-IB-Netzwerk während der Installation und Konfiguration in sechs eindeutige Partitionen partitioniert. Sie können zwar die Standardpartitionen nicht ändern, Oracle unterstützt jedoch das Erstellen und Verwenden von zusätzlichen dedizierten Partitionen in Fällen, in denen eine weitere Segmentierung des IB-Netzwerks erforderlich ist. Außerdem unterstützt das IB-Netzwerk das Konzept der begrenzten und vollen Partitionsmitgliedschaft. Begrenzte Mitglieder können nur mit Vollmitgliedern kommunizieren, während Vollmitglieder mit allen Knoten in der Partition kommunizieren können. Die Anwendungs-I/O-Domains und Oracle Solaris 11 Zones können als begrenzte Mitglieder der jeweiligen IB-Partitionen konfiguriert werden, sodass sichergestellt ist, dass sie nur mit der

ZFS Storage Appliance kommunizieren können, die als Vollmitglied konfiguriert ist, und nicht mit anderen begrenzten Mitgliedschaftsknoten, die möglicherweise in derselben Partition vorhanden sind.

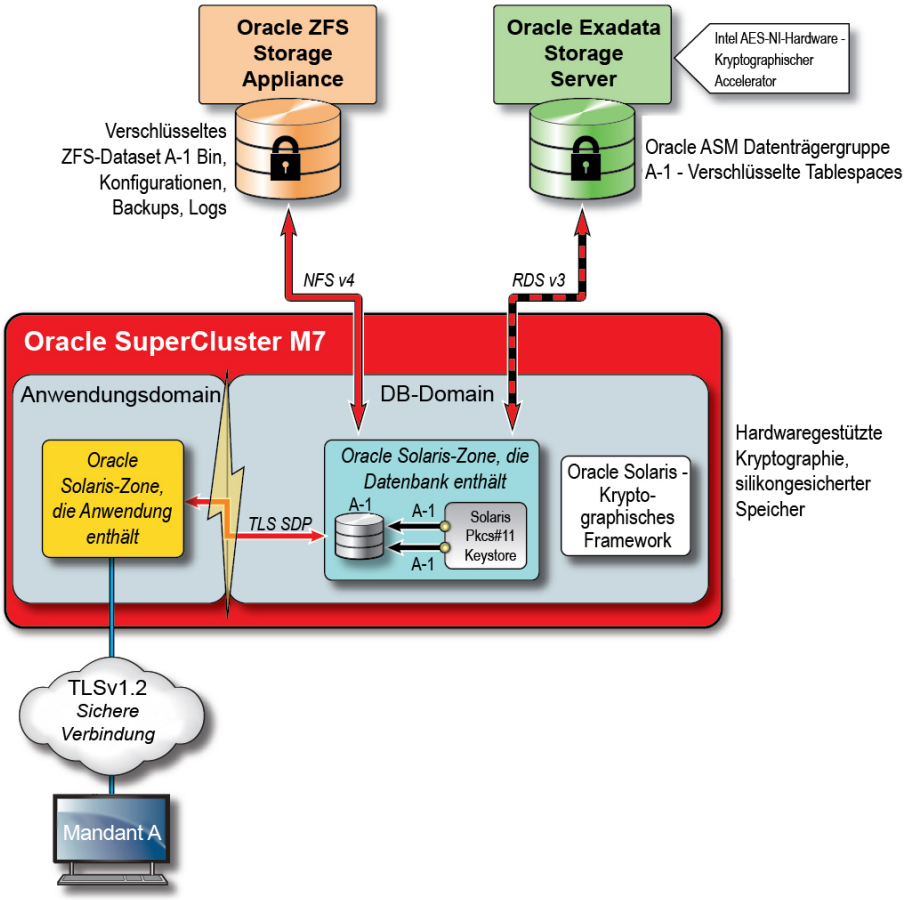
SuperCluster umfasst auch ein dediziertes Managementnetzwerk, über das alle Core-Komponenten verwaltet und konfiguriert werden können. Durch diese Strategie werden vertrauliche Management- und Überwachungsfunktionen von den Netzwerkpfaden isoliert gehalten, die zur Verarbeitung von Clientanforderungen verwendet werden. Durch die Isolation der Managementfunktionen in diesem Managementnetzwerk kann SuperCluster die Netzwerkangriffsfläche weiter reduzieren, die über den Clientzugriff und die IB-Netzwerke geboten wird. Es wird unbedingt empfohlen, dass Cloud-Provider diese empfohlene Vorgehensweise befolgen und Verwaltung, Überwachung und zugehörige Funktionen isolieren, damit nur aus dem Managementnetzwerk auf diese zugegriffen werden kann.

# Datenschutz

Für Cloud-Provider ist der Datenschutz das Kernstück ihrer Sicherheitsstrategie. Aufgrund der Bedeutung von Datenschutz- und Complianceanforderungen sollten Unternehmen, die mehrmandantenfähige Architekturen ins Auge fassen, unbedingt die Verwendung von Kryptografie zum Schutz der Informationen in Betracht ziehen, die in und aus ihren Datenbanken fließen. Die Verwendung von kryptografischen Services zum Datenschutz wird systematisch angewendet, um die Vertraulichkeit und Integrität von Informationen zu gewährleisten, die über das Netzwerk fließen und auf Datenträgern gespeichert werden.

Der SPARC M7-Prozessor in SuperCluster vereinfacht die hardwaregestützten High-Performance-Verschlüsselungen für die Datenschutzanforderungen sensibler IT-Umgebungen. Der SPARC M7-Prozessor umfasst außerdem die Silicon-Secured-Memory-Technologie, die böswillige Angriffe auf Anwendungsebene verhindert, wie Speicher-Scraping, lautlose Arbeitsspeicherbeschädigung, Pufferüberlauf und ähnliche Angriffe.

**ABBILDUNG 4** Datenschutz durch hardwaregestützte krytografische Beschleunigung und Schutz vor Speicherangriffen




Bei sicheren mehrmandantenfähigen Architekturen, bei denen Datenschutz bei nahezu jedem Aspekt der Architektur eine Rolle spielt, können Unternehmen mit SuperCluster und der unterstützenden Software ihre Sicherheits- und Complianceziele erreichen, ohne dass sich dies auf die Performance auswirkt. SuperCluster nutzt on-core-basierte kryptografische Anweisungen und Silicon-Secured-Memory-Funktionen, die in dem SPARC M7-Prozessor integriert sind, um kryptografische Vorgänge zu beschleunigen und Schutz vor Speicherangriffen zu bieten, ohne dass sich dies auf die Performance auswirkt. Diese Möglichkeiten führen zu verbesserter kryptografischer Performance und lassen die Prüfung

auf Speicherangriffe zu. Außerdem verbessern sie die Gesamtperformance, weil mehr Rechenressourcen für Mandanten-Workloads dediziert werden können.

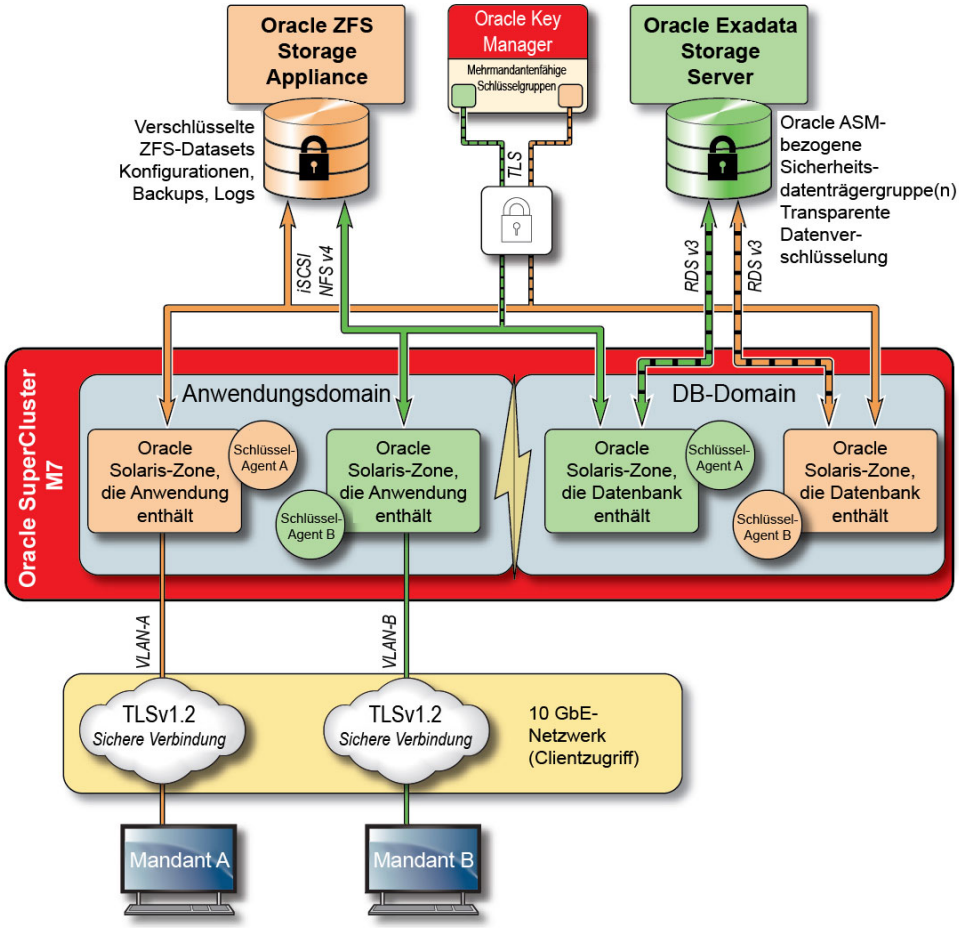
Der SPARC-Prozessor unterstützt die hardwaregestützte kryptografische Beschleunigung für mehr als 16 kryptografische Algorithmen gemäß Branchenstandard. Gemeinsam unterstützen diese Algorithmen die modernsten kryptografischen Anforderungen, einschließlich Public Key-Verschlüsselung, Symmetric Key-Verschlüsselung, Zufallszahlengenerierung sowie Berechnung und Verifizierung digitaler Signaturen und Message Digests. Außerdem ist auf BS-Ebene die kryptografische Hardwarebeschleunigung standardmäßig für die meisten Core-Services aktiviert, einschließlich Secure Shell, IPSec/IKE und verschlüsselten ZFS-Datasets.

Oracle Database und Oracle Fusion Middleware identifizieren automatisch das Oracle Solaris-BS und den SPARC-Prozessor, der von SuperCluster verwendet wird. Dadurch können Datenbank und Middleware automatisch die kryptografischen Hardwarebeschleunigungsmöglichkeiten der Plattform für TLS-, WS-Security- und Tablespace-Verschlüsselungsvorgänge verwenden. Außerdem kann die Silicon-Secured-Memory-Funktion für den Speicherschutz verwendet werden, und die Integrität der Anwendungsdaten wird sichergestellt, ohne dass eine Endbenutzerkonfiguration erforderlich ist. Für den Schutz der Vertraulichkeit und Integrität der mandantenspezifischen IP-basierten Kommunikation zwischen Zonen über das IB-Netzwerk verwenden Sie IPSec (IP Security) und IKE (Internet Key Exchange).

Jede Diskussion über Kryptografie wäre unvollständig ohne die Angabe, wie Verschlüsselungsschlüssel verwaltet werden. Die Generierung und Verwaltung von Verschlüsselungsschlüsseln, insbesondere bei großen Sammlungen von Services, war immer eine der größten Herausforderungen für Unternehmen, und die Herausforderungen werden bei einer cloud-basierten mehrmandantenfähigen Umgebung noch größer. Bei SuperCluster kann die ZFS-Datasetverschlüsselung und die transparente Datenverschlüsselung von Oracle Database einen Oracle Solaris PKCS#11-Keystore nutzen, um den Masterschlüssel sicher zu schützen. Bei Verwendung des Oracle Solaris PKCS#11-Keystores wird automatisch die hardwaregestützte kryptografische Beschleunigung von SPARC für Vorgänge mit Masterschlüsseln aktiviert. Auf diese Weise kann SuperCluster die Performance der Verschlüsselungs- und Entschlüsselungsvorgänge wesentlich verbessern, die mit der Verschlüsselung von ZFS-Datasets, der Verschlüsselung von Oracle Database Tablespaces, verschlüsselten Datenbankbackups (mit Oracle Recovery Manager [Oracle RMAN]), verschlüsselten Datenbankexporten (mit der Data Pump-Funktion von Oracle Database) und Redo-Logs (mit Oracle Active Data Guard) verknüpft sind

Mandanten, die eine Shared-Wallet-Lösung verwenden, können mit ZFS Storage Appliance ein Verzeichnis erstellen, das über alle Knoten in einem Cluster hinweg gemeinsam verwendet werden kann. Mit einem freigegebenen, zentralisierten Keystore können Mandanten die Schlüssel in geclusterten Datenbankarchitekturen, wie Oracle RAC-Clustern, besser verwalten, warten und rotieren, weil die Schlüssel auf allen Knoten in dem Cluster synchronisiert werden.

**ABBILDUNG 5** Datenschutz über ein mehrmandantenfähiges Schlüsselverwaltungsszenario mit Oracle Key Manager




Um die Komplexität und die Probleme der Schlüsselverwaltung bei mehreren Hosts und Anwendungen in einer cloud-basierten mehrmandantenfähigen Umgebung zu lösen, verwenden Sie den optionalen Oracle Key Manager als eine Appliance, die im Managementnetzwerk integriert ist. Oracle Key Manager autorisiert, sichert und verwaltet den Zugriff auf Verschlüsselungsschlüssel zentral, die von Oracle Database, Oracle Fusion Applications, Oracle Solaris und ZFS Storage Appliance verwendet werden. Oracle Key Manager unterstützt auch die StorageTek-Verschlüsselungsbandlaufwerke von Oracle. Durch Verschlüsselungsrichtlinien

und Schlüsselverwaltung auf ZFS-Datasetebene (Dateisystemebene) wird sichergestellt, dass Mandantendateisysteme durch Zerstörung der Schlüssel gelöscht werden.

Oracle Key Manager ist eine umfassende Schlüsselverwaltungs-Appliance, die Schlüsselverwaltungsvorgänge während des Lebenszyklus der Schlüssel und vertrauenswürdige Schlüsselspeicherung unterstützt. Bei der Konfiguration mit einer zusätzlichen Sun Crypto Accelerator 6000 PCIe-Karte von Oracle bietet Oracle Key Manager FIPS 140-2 Level 3-zertifizierte Schlüsselspeicherung von AES 256-Bit-Verschlüsselungsschlüsseln sowie FIPS 186-2–konforme Zufallszahlengenerierung. In SuperCluster können alle Datenbank- und Anwendungsdomains, einschließlich deren globalen und nicht-globalen Zonen, zur Verwendung von Oracle Key Manager bei der Verwaltung von Schlüsseln konfiguriert werden, die mit Anwendungen, Datenbanken und verschlüsselten ZFS-Datasets verknüpft sind. Oracle Key Manager kann Schlüsselverwaltungsvorgänge unterstützen, die mit einzelnen oder mehreren Datenbankinstanzen, Oracle RAC, Oracle Active Data Guard, Oracle RMAN und der Data Pump-Funktion von Oracle Database verknüpft sind.

Schließlich hat jeder Mandant durch die von Oracle Key Manager durchgesetzte Aufgabentrennung vollständige Kontrolle über seine Verschlüsselungsschlüssel mit konsistentem Einblick in alle Schlüsselverwaltungsvorgänge. Aufgrund der Wichtigkeit von Schlüsseln für den Informationsschutz müssen Mandanten unbedingt die erforderlichen Ebenen der rollenbasierten Zugriffskontrolle und des Auditings implementieren, um sicherzustellen, dass die Schlüssel während ihrer Gültigkeitsdauer ordnungsgemäß geschützt sind.

## Zusätzliche Informationen

- „Oracle Key Manager“ [130]

# Zugriffskontrolle

Für Unternehmen, die sich für eine cloud-gehostete Umgebungsstrategie entscheiden, ist die Zugriffskontrolle eine der wichtigsten Herausforderungen, die gelöst werden müssen. Mandanten müssen das Vertrauen haben, dass in der freigegebenen Infrastruktur gespeicherte Informationen geschützt und nur für autorisierte Hosts, Services, Einzelpersonen, Gruppen und Rollen verfügbar sind. Autorisierte Hosts, Einzelpersonen und Services müssen weiter nach dem Prinzip der geringsten Berechtigung begrenzt werden, indem sie nur die Rechte und Berechtigungen erhalten, die für einen bestimmten Vorgang erforderlich sind.

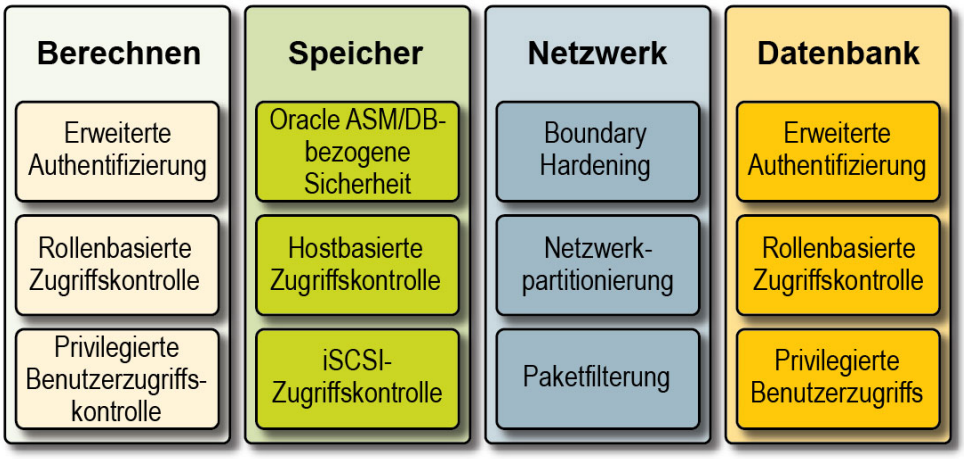
SuperCluster vereinfacht eine flexible, geschichtete Zugriffskontrollarchitektur, die jede Ebene des Stacks abdeckt und eine Vielzahl von Rollen unterstützt, einschließlich Endbenutzern,

Datenbankadministratoren und Systemadministratoren. Auf diese Weise können Unternehmen Richtlinien definieren, die Hosts, Anwendungen und Datenbanken individuell schützen und die zugrundliegende Rechen-, Speicher- und Netzwerkinfrastruktur schützen, auf der diese Services ausgeführt werden.

Auf den Virtualisierungs- und BS-Ebenen beginnt die Zugriffskontrolle mit der Reduzierung der Anzahl von Services, die in dem Netzwerk verfügbar gemacht werden. Auf diese Weise kann der Zugriff auf Oracle VM Server for SPARC-Konsolen, -Domains und -Zonen kontrolliert werden. Durch Reduzierung der Anzahl von Einsprungstellen, über die auf das System zugegriffen werden kann, kann auch die Anzahl von Zugriffskontrollrichtlinien reduziert und während des Lebenszyklus des System einfacher verwaltet werden.

Innerhalb des Oracle Solaris-BS werden Zugriffskontrollen durch eine Kombination von POSIX-Berechtigungen zusammen mit der rollenbasierten Zugriffskontrollfunktion (RBAC) von Oracle Solaris implementiert. Genauso wichtig ist der Schutz der Hosts, Anwendungen, Datenbanken und zugehörigen Services, die in SuperCluster ausgeführt werden, vor netzwerkbasierten Angriffen. Hierzu müssen die Mandanten zuerst sicherstellen, dass nur genehmigte Netzwerkservices ausgeführt werden und auf eingehende Netzwerkverbindungen horchen können. Nachdem die Angriffsfläche des Netzwerks minimiert wurde, konfigurieren Mandanten die restlichen Services, sodass diese nur über genehmigte Netzwerke und Schnittstellen auf eingehende Verbindungen horchen. Durch diese einfache Vorgehensweise kann auf Managementprotokolle, wie Secure Shell, ausschließlich über das Managementnetzwerk zugegriffen werden.

**ABBILDUNG 6** Zusammenfassung der End-to-End-Zugriffskontrolle



Außerdem können Mandanten eine host-basierte Firewall implementieren, wie den IP-Filterservice von Oracle Solaris. Hostbasierte Firewalls sind insofern nützlich, als sie Hosts umfassendere Möglichkeiten zur Kontrolle des Zugriffs auf Netzwerkservices bieten. Beispiel: IP-Filter unterstützt die zustandsbehaftete Paketfilterung und kann Pakete nach IP-Adresse, Port, Protokoll, Netzwerkschnittstelle und Richtung des Datenverkehrs filtern. Diese Möglichkeiten sind für Plattformen wie SuperCluster wichtig, die mit vielen Netzwerkschnittstellen arbeiten und eine Vielzahl von eingehenden und ausgehenden Netzwerkkommunikationen unterstützen.

Bei SuperCluster kann IP-Filter innerhalb einer Oracle VM Server for SPARC-Domain konfiguriert oder aus einer Oracle Solaris-Zone ausgeführt werden. Dadurch kann die Richtlinie für die Netzwerkzugriffskontrolle in demselben BS-Container durchgesetzt werden, in dem die Datenbankservices bereitgestellt werden. In einem mehrmandantenfähigen Szenario ist der Umfang der ausgehenden Netzwerkaktivität wahrscheinlich minimal und kann einfach kategorisiert werden, sodass eine Richtlinie erstellt werden kann, die die Kommunikation zu bestimmten Netzwerkschnittstellen und Zielen begrenzt. Der gesamte andere Datenverkehr würde abgelehnt und als Teil einer "Default Deny"-Richtlinie protokolliert, um nicht autorisierte Kommunikationen, sowohl eingehend als auch ausgehend, zu blockieren.

Mit Oracle End User Security können Mandanten ihre Anwendungen und Datenbanken mit ihren vorhandenen Identitätsverwaltungsservices integrieren, um Single Sign-On (SSO) und zentralisierte Benutzer- und Rollenverwaltung zu unterstützen. Insbesondere zentralisiert Oracle End User Security folgende Vorgänge: (1) Provisioning und Deprovisioning von Datenbankbenutzern und -Administratoren, (2) Passwortverwaltung und Selfservice-Passwortrücksetzung und (3) Verwaltung von Autorisierungen durch globale Datenbankrollen. Unternehmen, die Mehrfaktor-Authentifizierungsmethoden erfordern, wie Kerberos oder PKI, können Oracle Advanced Security nutzen.

Die Oracle Exadata Storage Server-Technologie unterstützt ein vordefiniertes Set von Benutzerkonten, jedes mit eindeutigen Berechtigungen. Administratoren, die die Oracle Exadata Storage Server-Administration durchführen, müssen eine dieser vordefinierten Rollen für den Zugriff auf das System verwenden. ZFS Storage Appliance hingegen unterstützt das Erstellen von lokalen und Remote-Administrationskonten, die beide die individuelle Zuweisung von Rollen und Berechtigungen unterstützen können.

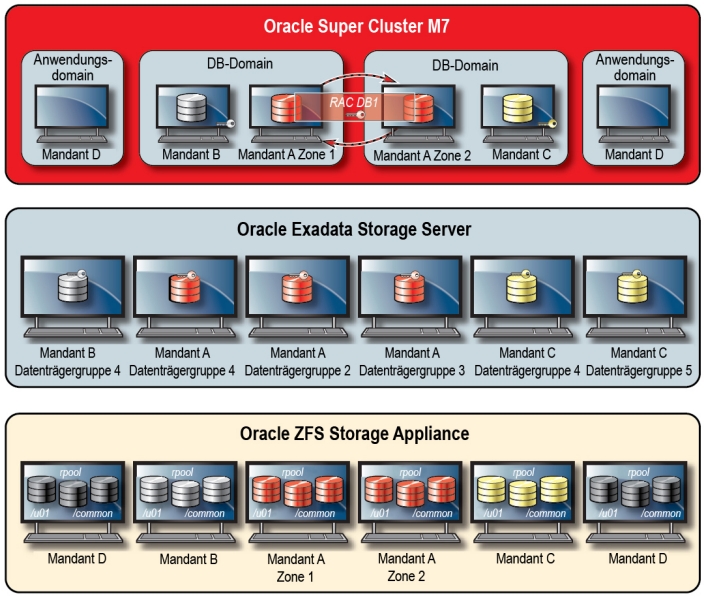
Standardmäßig wird auf die Oracle Exadata Storage Server, die in SuperCluster verwendet werden, von den Datenbankdomains mit der Oracle Automatic Storage Management-Funktion zugegriffen. Mit dieser Funktion können Cloud-Provider eindeutige Datenträgergruppen für jeden Mandanten erstellen, die dessen Anforderungen an Kapazität, Performance und Verfügbarkeit erfüllen. Was die Zugriffskontrolle betrifft, unterstützt Oracle Automatic Storage Management drei Zugriffskontrollmodi: Offene Sicherheit, Oracle Automatic Storage Management–bezogene Sicherheit und datenbankbezogene Sicherheit.

In einem mehrmandantenfähigen Szenario wird die datenbankbezogene Sicherheit empfohlen, weil sie die feingranulierteste Ebene der Zugriffskontrolle bietet. In diesem Modus können

Datenträgergruppen so konfiguriert werden, dass nur eine einzelne Datenbank auf sie zugreifen kann. Dies bedeutet insbesondere, dass sowohl Datenbankadministratoren als auch Datenbankbenutzer nur auf die Grid Disks zugreifen können, die Informationen enthalten, für die sie Zugriffsberechtigungen haben. Bei Datenbankkonsolidierungsszenarios, bei denen einzelne Datenbanken möglicherweise unterschiedliche Unternehmen oder Mandanten unterstützen können, ist es wichtig, dass jeder Mandant nur auf seinen eigenen Speicher zugreifen und diesen verwalten kann. Insbesondere bei der Kombination mit Workload- und Datenbankisolationsstrategien, die vorher beschrieben wurden, können Mandanten den Zugriff auf einzelne Datenbanken begrenzen.

Die datenbankbezogene Sicherheit ist ein effizientes Tool zur Begrenzung des Zugriffs auf Oracle ASM Grid Disks. In dieser Abbildung wird die Oracle ASM-bezogene Sicherheit zusammen mit der ZFS-Sicherheit dargestellt. In Fällen, in denen eine große Anzahl von Oracle Database-Instanzen in der SuperCluster-Plattform bereitgestellt wird, ist eine Oracle ASM-bezogene Sicherheitsstrategie pro Mandant möglicherweise sinnvoller, weil sie die Anzahl von Schlüsseln wesentlich reduziert, die erstellt, zugewiesen und verwaltet werden müssen. Weil die datenbankbezogene Sicherheit erfordert, das separate Datenträgergruppen für jede Datenbank erstellt werden, reduziert diese Lösung außerdem die Anzahl von separaten Grid Disks wesentlich, die in einem Exadata Storage Server erstellt werden müssen.

**ABBILDUNG 7** Oracle ASM-bezogene Sicherheit pro Mandant



SuperCluster nutzt den Oracle Solaris-Datenlinkschutz, mit dem potenzielle Beschädigungen des Netzwerks durch böswillige virtuelle Mandantenmaschinen verhindert werden sollen. Diese integrierte Oracle Solaris-Funktion bietet Schutz vor den folgenden allgemeinen Bedrohungen: Spoofing von IP- und MAC-Adressen sowie L2-Frame Spoofing (Beispiel: BPDU-(Bridge Protocol Data Unit-)Angriffe). Oracle Solaris-Datenlinkschutz muss individuell für alle nicht-globalen Oracle Solaris-Zonen angewendet werden, die in der mehrmandantenfähigen Umgebung bereitgestellt sind.

Weil einzelne Mandanten niemals Administrationszugriff oder Zugriff auf Hostebene für die Exadata Storage Server anfordern sollten, wird unbedingt empfohlen, dass dieser Zugriff eingeschränkt wird. Die Exadata Storage Server müssen so konfiguriert werden, dass der direkte Zugriff auf nicht-globale Mandantenzonen und Datenbank-I/O-Domains verhindert wird, während der Zugriff von SuperCluster-Datenbankdomains (die vom Cloud-Provider betrieben werden) weiter zugelassen ist. Dadurch wird sichergestellt, dass die Exadata Storage Server nur aus vertrauenswürdigen Verzeichnissen im Managementnetzwerk verwaltet werden können.

Nachdem die Sicherheitskonfiguration der Mandanten definiert und implementiert wurde, können Serviceprovider zusätzlich mandantenspezifische globale und nicht-globale Zonen als unveränderliche schreibgeschützte Umgebungen konfigurieren. Unveränderliche Zonen erstellen eine robuste Betriebsumgebung mit hoher Integrität, in der Mandanten ihre eigenen Services verwenden können. Aufbauend auf den inhärenten Sicherheitsfunktionen von Oracle Solaris stellen unveränderliche Zonen sicher, dass einige (oder alle) BS-Verzeichnisse und -Dateien ohne Eingriff des Cloud-Serviceproviders nicht verändert werden können. Die Durchsetzung dieser schreibgeschützten Vorgehensweise kann nicht autorisierte Änderungen verhindern, stärkere Change Management-Prozeduren fördern und das Einschleusen sowohl von Kernel- als auch von benutzerbasierter Schadsoftware verhindern.

# Überwachung und Complianceauditing

Proaktive Überwachung und Logging in einer Cloud-Umgebung sind sehr wichtig und helfen in vielen Fällen, von Sicherheitslücken ausgehende Angriffe zu vermeiden. Ob für Complianceberichte oder Antworten auf Vorfälle, Überwachung und Auditing ist eine wichtige Funktion für den Cloud-Provider; Mandantenunternehmen müssen eine ordnungsgemäß definierte Logging- und Auditing-Richtlinie durchsetzen, damit sie immer Einblick in ihre Hostingumgebung haben. Der Grad, bis zu dem Überwachung und Auditing eingesetzt werden, basiert häufig auf dem Risiko oder der kritischen Natur der zu schützenden Umgebung.

Die SuperCluster-Cloud-Architektur nutzt das Oracle Solaris-Auditsubsystem zur Erfassung, Speicherung und Verarbeitung von Auditereignisinformationen. Jede mandantenspezifische nicht-globale Zone generiert Auditdatensätze, die lokal in jeder der dedizierten SuperCluster-

Domains (globale Zone) gespeichert werden. Diese Lösung stellt sicher, dass einzelne Mandanten ihre Auditingrichtlinien, -konfigurationen oder aufgezeichneten Daten nicht ändern können, weil die Verantwortung bei dem Cloud-Serviceprovider liegt. Die Oracle Solaris-Auditingfunktion überwacht alle administrativen Aktionen, Befehlsaufrufe und sogar individuelle Systemaufrufe auf Kernelebene sowohl in Mandantenzonen als auch in Domains. Diese Funktion ist hoch konfigurierbar und bietet globale Auditingrichtlinien pro Zone und sogar pro Benutzer. Bei der Konfiguration zur Verwendung von Mandantenzonen können Auditdatensätze für jede Zone in der globalen Zone gespeichert werden, um sie vor Manipulation zu schützen. Dedizierte Domains und I/O-Domains nutzen die systemeigene Oracle Solaris-Auditingfunktion ebenfalls zur Aufzeichnung von Aktionen und Ereignissen, die mit Virtualisierungsereignissen und Domainverwaltung verknüpft sind.

Exadata Storage Server und ZFS Storage Appliance unterstützen Anmeldungs-, Hardware- und Konfigurationsauditing. Dadurch können Unternehmen feststellen, wer auf ein Gerät zugegriffen hat und welche Aktionen ausgeführt wurden. Das Oracle Solaris-Auditing ist zwar nicht direkt für Endbenutzer zugänglich, stellt jedoch den zugrundeliegenden Inhalt für Informationen bereit, die von ZFS Storage Appliance dargestellt werden.

Ähnlich stellt das Exadata Storage Server-Audit eine umfassende Sammlung von Systemereignissen bereit, die zusammen mit Hardware- und Konfigurations-Alert-Informationen verwendet werden können, die von der Exadata Storage Server-Software bereitgestellt werden. Mit der IP-Filterfunktion von Oracle Solaris kann der Cloud-Provider selektiv sowohl eingehende als auch ausgehende Netzwerkkommunikationen aufzeichnen; diese Möglichkeit kann auf Domain- und nicht-globaler Zonenebene angewendet werden. Dadurch können Unternehmen ihre Netzwerkrichtlinien segmentieren und Aktivitätsdatensätze prüfen. Optional kann die Oracle Audit Vault and Database Firewall Appliance bereitgestellt werden, mit der Auditinformationen aus einer Vielzahl von Oracle- und Nicht-Oracle-Datenbanken sowie Auditinformationen von Oracle Solaris aggregiert und analysiert werden können.

Durch die Integration mit Oracle Enterprise Manager kann SuperCluster verschiedene Cloud-Selfservicevorgänge unterstützen. Cloud-Provider können Pools mit Ressourcen definieren, einzelnen Mandanten Pools und Quota zuweisen, Servicekataloge identifizieren und veröffentlichen und schließlich Überwachung und Logging von Anwendungs- und Datenbankressourcen unterstützen.

# Zusätzliche Informationen

- Auditing auf Compliance [123]
- „Überwachen der Sicherheit“ [133]

# Zusätzliche Ressourcen für Best Practices bei SuperCluster-Sicherheit

Zusätzliche Informationen zu SuperCluster-Sicherheit, -Architektur und Best Practices finden Sie in diesen Ressourcen:

- Oracle SuperCluster M7 - Grundlagen und Möglichkeiten der Plattformsicherheit

  http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf
- Oracle SuperCluster M7 - Sichere private Cloud-Architektur

  http://www.oracle.com/technetwork/server-storage/engineered-systems/oracle-supercluster/documentation/supercluster-secure-multi-tenancy-2734706.pdf
- Umfassender Datenschutz bei Oracle SuperCluster

  https://community.oracle.com/docs/DOC-918251
- Sichere Datenbankkonsolidierung in Oracle SuperCluster

  http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf
- Oracle SuperCluster und PCI-Compliance

  http://www.oracle.com/technetwork/server-storage/engineered-systems/sparc-supercluster/supercluster-pci-dss-compliance-2372543.pdf
- Oracle SuperCluster - Security Technical Implementation Guide (STIG) - Validierung und Best Practices

  http://www.oracle.com/technetwork/server-storage/hardware-solutions/stig-sparc-supercluster-1841833.pdf
- Developer’s Guide to Oracle Solaris 11 Security

  https://docs.oracle.com/cd/E36784_01/html/E36855/index.html
- Oracle Solaris 11 und PCI-Compliance

  http://www.oracle.com/us/products/servers-storage/solaris/solaris11/solaris11-pci-dss-wp-1937938.pdf
- Oracle Solaris 11 Audit - Kurzanleitung

  http://www.oracle.com/technetwork/articles/servers-storage-admin/sol-audit-quick-start-1942928.html
- Oracle Solaris 11 - Sicherheitsbestimmungen

  http://docs.oracle.com/cd/E53394_01/html/E54807/index.html
- Oracle Database 12c Release 1 (12.1) - Sicherheitshandbuch

  https://docs.oracle.com/database/121/DBSEG/E48135-11.pdf

# Prüfen der Standardsicherheitskonfiguration

In diesen Themen wird die Standardsicherheitskonfiguration für SuperCluster M7 beschrieben.



## Standardsicherheitseinstellungen

SuperCluster M7-Software ist mit vielen Standardsicherheitseinstellungen installiert. Wenn möglich verwenden Sie die Standardsicherheitseinstellungen:

- Passwortrichtlinien setzen eine Mindestpasswortkomplexität voraus.
- Nicht erfolgreiche Anmeldeversuche führen nach einer festgelegten Anzahl von nicht erfolgreichen Versuchen zu einer Sperre.
- Alle Standardsystemkonten in dem BS werden gesperrt, eine Anmeldung ist nicht möglich.
- Begrenzte Möglichkeit zur Verwendung des Befehls `su` ist konfiguriert.
- Nicht erforderliche Protokolle und Module sind im BS-Kernel deaktiviert.
- Bootloader ist passwortgeschützt.
- Alle nicht erforderlichen Systemservices sind deaktiviert, einschließlich `inetd` (Internet-Service-Daemon).
- Softwarefirewall ist in den Speicherzellen konfiguriert.
- Restriktive Dateiberechtigungen sind für wichtige sicherheitsbezogene Konfigurationsdateien und ausführbare Dateien festgelegt.
- SSH-Listening-Ports sind auf Management- und private Netzwerke begrenzt.
- SSH ist auf v2-Protokoll begrenzt.
- Unsichere SSH-Authentifizierungsverfahren sind deaktiviert.
- Spezifische kryptografische Ciphers sind konfiguriert.
- Die Switches sind im System von dem Datenverkehr im Netzwerk getrennt.

# Standardbenutzerkonten und Passwörter

In dieser Tabelle werden die Standardbenutzerkonten und Passwörter für SuperCluster M7 aufgeführt. Zusätzliche Anweisungen zur Änderung der Standardkennwörter werden in nachfolgenden Kapiteln für jede Komponente bereitgestellt.

| Komponente | Benutzername | Passwort | Informationen zu Benutzerkonto und Passwort |
|---|---|---|---|
| Oracle ILOM in:<br>■ SPARC M7 Series-Server<br>■ Exadata Storage Server<br>■ ZFS Storage Appliance | ■ `root` | `welcome1` | Hierzu wird auf "Konfiguration und Wartung" in der Oracle ILOM-Dokumentation unter: `http://docs.oracle.com/cd/E24707_01/html/E24528` verwiesen. |
| SPARC M7 Series-Server | ■ `root`<br>■ `oracle`<br>■ `grid` | `welcome1`<br>`welcome1`<br>`welcome1` | Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].<br>Außerdem wird auf folgende Ressourcen verwiesen:<br>■ **Oracle Solaris 11** – Hierzu wird auf die Sicherheitsdokumentation für Oracle Solaris 11 unter: `http://www.oracle.com/goto/Solaris11/docs` verwiesen.<br>■ **Oracle Solaris 10** – Hierzu wird auf *Oracle Solaris Administration: Basic Administration* unter `http://docs.oracle.com/cd/E26505_01` verwiesen. |
| Exadata Storage Server | ■ `root`<br>■ `celladmin`<br>■ `cellmonitor` | `welcome1`<br>`welcome`<br>`welcome` | Siehe Ändern von Storage Server-Passwörtern [96]. |
| Oracle ZFS Storage ZS3-ES | ■ `root` | `welcome1` | Siehe Andern des `root`-Passwortes von ZFS Storage Appliance [85].<br>Hierzu wird auf den Abschnitt "Benutzer" in *Oracle ZFS Storage Appliance - Administrationshandbuch* unter: `http://www.oracle.com/goto/ZS3-ES/docs` verwiesen. |
| InfiniBand-Switches | ■ `root`<br>■ `nm2user` | `welcome1`<br>changeme | Siehe Ändern der `root-` und `nm2user`-Passwörter [113].<br>Hierzu wird auf "Controlling the Chassis" in *Sun Datacenter InfiniBand Switch 36 HTML Document Collection for Firmware Version 2.1* unter: `http://docs.oracle.com/cd/E36265_01` verwiesen. |
| InfiniBand Oracle ILOM | ■ `ilom-admin`<br>■ `ilom-operator` | ilom-admin<br>ilom-operator | Siehe Ändern von IB-Switch-Passwörtern (Oracle ILOM) [114].<br>Außerdem wird auf die InfiniBand-Dokumentation unter: `http://docs.oracle.com/cd/E36265_01` verwiesen. |
| Ethernet-Management-Switch | ■ `admin` | `welcome1` | Siehe Ändern des Ethernet-Switch-Passwortes [121] |

| Komponente | Benutzername | Passwort | Informationen zu Benutzerkonto und Passwort |
|---|---|---|---|
| Oracle I/O Domain Creation-Tool | ■ `admin` | welcome1 | Hierzu wird auf *Oracle I/O-Domain - Administrationshandbuch* unter: `http://www.oracle.com/goto/sc-m7/docs` verwiesen. |
| Oracle Engineered Systems Hardware Manager | ■ `admin`<br>■ Service | welcome1<br>welcome1 | Hierzu wird auf *Oracle SuperCluster M7 Series - Eigentümerhandbuch: Administration* unter: `http://www.oracle.com/goto/sc-m7/docs` verwiesen. |

**Anmerkung -** Wenn das `root`- oder `admin`-Passwort für diese Komponente geändert wird, muss es auch in Oracle Engineered Systems Hardware Manager geändert werden. Weitere Anweisungen finden Sie in *Oracle SuperCluster M7 Series - Eigentümerhandbuch: Administration*. Siehe auch „Passwörter, die Oracle Engineered Systems Hardware Manager bekannt sind“ [31]

# Passwörter, die Oracle Engineered Systems Hardware Manager bekannt sind

Oracle Engineered Systems Hardware Manager muss mit den Konten und Passwörtern für die Komponenten in dieser Tabelle konfiguriert werden.

**Anmerkung -** Oracle Engineered Systems Hardware Manager muss die Passwörter für logische Domains oder Zonen nicht kennen.

| Komponente | Konto |
|---|---|
| Alle Oracle ILOMs | `root` |
| Exadata Storage Server - BS | `root` |
| ZFS Storage Controller - BS | `root` |
| IB-Switches | `root` |
| Ethernet-Management-Switch | `admin` |
| PDUs | `admin` |

Informationen zu Oracle Engineered Systems Hardware Manager finden Sie in „Oracle Engineered Systems Hardware Manager“ [131]; außerdem wird auf *Oracle SuperCluster M7 Series - Administrationshandbuch* unter `http://www.oracle.com/goto/sc-m7/docs` verwiesen.

# Sichern der Hardware

In diesen Abschnitten werden die Sicherheitsrichtlinien zur Sicherung der Hardware beschrieben.



## Zugriffsbeschränkungen

- Installieren Sie Oracle SuperCluster M7 Series-Systeme und die zugehörige Ausrüstung in einem abgeschlossenen Raum mit Zugangskontrolle.
- Verschließen Sie die Racktüren, es sei denn, die Komponenten in dem Rack müssen gewartet werden. Dadurch wird der Zugang zu austauschbaren oder im laufenden Betrieb austauschbaren Geräten, sowie zu USB-Ports, Netzwerkports und Systemkonsolen eingeschränkt.
- Lagern Sie nicht verwendete FRUs (Field Replaceable Units) oder CRUs (Customer Replaceable Units) in einem abschließbaren Schrank. Nur autorisiertes Personal sollte Zugang zu diesem Schrank haben.
- Prüfen Sie regelmäßig den Zustand und die Integrität der Verriegelungen am Rack und am Ersatzteilschrank, um Manipulation oder versehentlich unverschlossene Türen zu verhindern oder zu entdecken.
- Bewahren Sie Schrankschlüssel an einem sicheren Ort mit eingeschränktem Zugang auf.
- Schränken Sie den Zugriff auf USB-Konsolen ein. Geräte wie Systemcontroller, Steckdosenleisten (Power Distribution Units, PDUs) und Netzwerk-Switches weisen USB-Anschlüsse auf. Die Einschränkung des physischen Zugriffs ist eine sicherere Methode, auf eine Komponente zuzugreifen, da sie dabei keinen netzwerkbasierten Angriffen ausgesetzt ist.

# Seriennummern

- Schreiben Sie die Seriennummern der Komponenten in SuperCluster M7 Series-Systemen auf.
- Versehen Sie alle wichtigen Komponenten der Computerhardware, wie z.B. Ersatzteile, mit einer Sicherheitskennzeichnung. Verwenden Sie spezielle UV-Stifte oder geprägte Beschriftungen.
- Bewahren Sie Aufzeichnungen der Hardwareaktivierungsschlüssel und Lizenzen an einem sicheren Ort auf, der im Systemnotfall für den Systemverwalter einfach zugänglich ist. Die ausgedruckten Dokumente sind möglicherweise Ihr einziger Eigentumsnachweis.
- Bewahren Sie alle Informationsblätter sorgfältig auf, die mit dem System geliefert werden.

# Laufwerke

Festplattenlaufwerke und Solid-State-Laufwerke werden häufig zur Speicherung vertraulicher Daten verwendet. Um diese Informationen vor unberechtigter Weitergabe zu schützen, müssen Laufwerke vor der Wiederverwendung, Außerbetriebnahme oder Entsorgung bereinigt werden.

- Verwenden Sie Tools zum Bereinigen von Datenträgern, wie den Oracle Solaris-Befehl `format(1M)`, um alle Daten vollständig aus dem Laufwerk zu löschen.
- Unternehmen sollten anhand ihrer Datenschutzrichtlinien die am ehesten geeignete Methode zum Bereinigen von Festplatten bestimmen.
- Nutzen Sie bei Bedarf den Oracle Customer Data and Device Retention-Service. Dazu wird auf folgendes Dokument verwiesen: `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`

**Achtung -** Einige Daten auf modernen Laufwerken können möglicherweise nicht von Software zum Bereinigen von Datenträgern gelöscht werden. Dies liegt an der Art, wie sie den Datenzugriff verwalten.

# OBP

Standardmäßig ist der OBP von SPARC M7 Series nicht passwortgeschützt. Sie können die Sicherheit des Systems erhöhen, indem Sie den Zugriff auf den OBP wie folgt einschränken:

- Passwortschutz implementieren.
- Auf nicht erfolgreiche OBP-Anmeldungen prüfen.
- Bereitstellen eines OBP-Einschaltbanners.

# Zusätzliche Hardwareressourcen

Alle Sicherheitsbestimmungen, die in *SPARC M7 Series Systems Server - Sicherheitshandbuch* dargelegt werden, gelten auch für die SPARC M7-Server in SuperCluster. Dieses Sicherheitshandbuch ist unter: `http://www.oracle.com/goto/M7/docs` verfügbar.

# Sichern von Oracle ILOM

Oracle ILOM stellt erweiterte Serviceprozessorhardware und -software bereit, mit der Oracle SuperCluster-Komponenten verwaltet und überwacht werden können, einschließlich Rechenserver, Storage Server, ZFS Storage Appliance und IB-Switches.

Mit Oracle ILOM können Sie die zugrundeliegenden Server und Geräte unabhängig vom BS-Status verwalten und überwachen, sodass eine verlässliche Lights Out Management-Funktion bereitgestellt wird.

Zur vollen Sicherung von Oracle ILOM in SuperCluster M7 müssen Sie Konfigurationseinstellungen für alle Oracle ILOM-fähigen Komponenten individuell anwenden. Folgende Komponenten verfügen über Oracle ILOM:

- Rechenserver
- Storage Server
- ZFS Storage Appliance
- IB-Switches

Führen Sie die folgenden Aufgaben zur Sicherung von Oracle ILOM aus:



## ▼ Anmelden bei der Oracle ILOM-CLI

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**

In diesem Beispiel ersetzen Sie *ILOM_SP_ipaddress* durch die IP-Adresse von Oracle ILOM für die Komponente, auf die Sie zugreifen möchten:

- Rechenserver
- Storage Server
- ZFS Storage Appliance
- IB-Switches

IP-Adressen für Ihre Konfiguration werden in der Deployment-Zusammenfassung aufgeführt, die Ihnen von Oracle-Mitarbeitern zur Verfügung gestellt wird.

```
% ssh root@ILOM_SP__ipaddress
```

2. **Geben Sie das Oracle ILOM Root-Passwort ein.**

   Siehe „Standardkonten und -passwörter (Oracle ILOM)“ [40].

# Bestimmen der Oracle ILOM-Version

Um die neuesten Features, Funktionen und Sicherheitserweiterungen nutzen zu können, updaten Sie die Oracle ILOM-Software auf die neueste unterstützte Version.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**

   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Zeigen Sie die Oracle ILOM-Version an.**

   In diesem Beispiel ist die Oracle ILOM-Software Version 3.2.4.1.b.

```
-> version
SP firmware 3.2.4.1.b
SP firmware build number: 94529
SP firmware date: Thu Nov 13 16:41:19 PST 2014
SP filesystem version: 0.2.10
```

**Anmerkung -** Um die Version von Oracle ILOM in einer der SuperCluster-Komponenten zu aktualisieren, installieren Sie das neueste SuperCluster Quarterly Full Stack Download Patch, das in My Oracle Support unter `https://support.oracle.com` verfügbar ist.

**Anmerkung -** Bei Oracle Engineered Systems, wie SuperCluster, gibt es Einschränkungen für die Versionen von Oracle ILOM, die verwendet werden können und wie sie verwendet werden können. Für weitere Einzelheiten wenden Sie sich an Ihren Oracle-Ansprechpartner.

# (Falls erforderlich) Aktivieren eines FIPS-140-konformen Vorgangs (Oracle ILOM)

Kunden der US-Bundesregierung müssen FIPS-140-validierte Kryptografie verwenden.

Standardmäßig arbeitet Oracle ILOM nicht mit FIPS 140-validierter Kryptografie. Die Verwendung von FIPS 140-validierter Kryptografie kann jedoch falls erforderlich aktiviert werden.

Einige Oracle ILOM-Features und -Funktionen sind bei einer Konfiguration für FIPS 140-konforme Vorgänge nicht verfügbar. Eine Liste dieser Funktionen finden Sie in *Oracle ILOM - Sicherheitshandbuch* in dem Abschnitt über nicht unterstützte Features, wenn der FIPS-Modus aktiviert ist (siehe „Zusätzliche Oracle ILOM-Ressourcen“ [52]).

Siehe auch „FIPS-140-2 Level 1-Compliance“ [126].

**Achtung -** In dieser Aufgabe müssen Sie Oracle ILOM zurücksetzen Eine Rücksetzung führt zum Verlust aller benutzerkonfigurierten Einstellungen. Deshalb müssen Sie einen FIPS 140-konformen Vorgang vor zusätzlichen sitespezifischen Änderungen aktivieren, die an Oracle ILOM vorgenommen werden. Bei Systemen, bei denen sitespezifische Änderungen vorgenommen wurden, erstellen Sie ein Backup der Oracle ILOM-Konfiguration, damit sie nach der Zurücksetzung von Oracle ILOM wiederhergestellt werden kann; sonst sind die Konfigurationsänderungen verloren.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**

   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Bestimmen Sie, ob Oracle ILOM für FIPS 140-konforme Vorgänge konfiguriert ist.**

```
-> show /SP/services/fips state status
/SP/services/fips
Properties:
state = enabled
status = enabled
```

   Der FIPS 140-konforme Modus in Oracle ILOM wird mit den Eigenschaften `state` und `status` dargestellt. Die `state`-Eigenschaft steht für den konfigurierten Modus in Oracle ILOM und die `status`-Eigenschaft für den Betriebsmodus in Oracle ILOM. Wenn die FIPS-Eigenschaft `state` geändert wird, wirkt sich diese Änderung bis zum nächsten Neustart von Oracle ILOM nicht auf den Betriebsmodus der FIPS-Eigenschaft `status` aus.

3. **Aktivieren Sie den FIPS 140-konformen Vorgang.**

```
-> set /SP/services/fips state=enabled
```

4. **Starten Sie den Oracle ILOM-Serviceprozessor neu.**

   Der Oracle ILOM-SP muss neu gestartet werden, damit diese Änderung wirksam wird.

```
-> reset /SP
```

# Standardkonten und -passwörter (Oracle ILOM)

| Konto | Typ | Standardpasswort | Beschreibung |
|---|---|---|---|
| `root` | Administrator | `welcome1` | Dies ist das Standardkonto, das für diese Komponente bereitgestellt und aktiviert wird. Dieses Konto wird zur Ausführung der anfänglichen Konfiguration verwendet und ermöglicht das Erstellen von zusätzlichen, nicht freigegebenen administrativen Konten.<br><br>Ändern Sie das Standardpasswort aus Sicherheitsgründen. |

# Verfügbar gemachte Standardnetzwerkservices (Oracle ILOM)

In dieser Tabelle werden die Standardnetzwerkservices aufgeführt, die erneut von Oracle ILOM verfügbar gemacht werden

Weitere Informationen zu diesen Services finden Sie in *Oracle ILOM - Sicherheitshandbuch* (siehe „Zusätzliche Oracle ILOM-Ressourcen“ [52]).

| Servicename | Protokoll | Port | Beschreibung |
|---|---|---|---|
| SSH | TCP | 22 | Wird von dem integrierten Secure Shell-Service verwendet, um den administrativen Zugriff auf Oracle ILOM mit einer CLI zu aktivieren. |
| HTTP (BUI) | TCP | 80 | Wird von dem integrierten HTTP-Service verwendet, um den administrativen Zugriff auf Oracle ILOM mit einer Browseroberfläche zu aktivieren. Während TCP/80 im Allgemeinen für den Klartextzugriff verwendet wird, leitet Oracle ILOM standardmäßig eingehende Anforderungen automatisch an die sichere Version dieses Service um, die unter TCP/443 ausgeführt wird. |
| NTP | UDP | 123 | Wird vom integrierten Network Time Protocol-(NTP-) (Nur Client-)Service zur Synchronisierung der lokalen Zeituhr mit einer oder mehreren externen Zeitquellen verwendet. |

| Servicename | Protokoll | Port | Beschreibung |
|---|---|---|---|
| SNMP | UDP | 161 | Wird von dem integrierten SNMP-Service verwendet, um eine Managementoberfläche zur Überwachung der Integrität von Oracle ILOM und zur Überwachung empfangener Trap-Benachrichtigungen bereitzustellen. |
| HTTPS (BUI) | TCP | 443 | Wird von dem integrierten HTTPS-Service verwendet, um den administrativen Zugriff auf Oracle ILOM über einen verschlüsselten (SSL/TLS-)Kanal mit einer Browseroberfläche zu aktivieren. |
| IPMI | TCP | 623 | Wird von dem integrierten IPMI-(Intelligent Platform Management Interface-)Service verwendet, um eine Rechnerschnittstelle für verschiedene Überwachungs- und Managementfunktionen bereitzustellen. Dieser Service darf nicht deaktiviert werden, weil er von Oracle Enterprise Manager Ops Center zur Erfassung von Hardwarebestandsdaten, FRU-Beschreibungen, Hardwaresensorinformationen und Informationen zum Hardwarekomponentenstatus verwendet wird. |
| Remote KVMS | TCP | 5120<br>5121<br>5123<br>5555<br>5556<br>7578<br>7579 | Gemeinsam stellen die Remote-KVMS-Ports ein Set von Protokollen für Remote-Tastatur-, Video-, Maus- und Speicherfunktionen bereit, die mit Oracle Integrated Lights Out Manager verwendet werden können |
| ServiceTag | TCP | 6481 | Wird vom Oracle ServiceTag-Service verwendet. Dies ist ein Oracle-Erkennungsprotokoll zur Serveridentifizierung und Erleichterung von Serviceanfragen. Dieser Service wird von Produkten wie Oracle Enterprise Manager Ops Center verwendet, um Oracle ILOM-Software zu ermitteln und mit anderen automatischen Oracle-Servicelösungen zu integrieren. |
| WS-MAN über HTTP | TCP | 8888 | Wird von dem integrierten WS-Man-Service verwendet, um eine auf Standards basierende Webserviceschnittstelle bereitzustellen, mit der Oracle ILOM über das HTTPS-Protokoll verwaltet wird. Wenn dieser Service deaktiviert wird, kann Oracle ILOM nicht mit diesem Protokoll verwaltet werden. Ab Oracle ILOM Version 3.2 ist dieser Service nicht mehr enthalten. |
| WS-MAN über HTTP | TCP | 8889 | Dieser Port wird von dem integrierten WS-Man-Service verwendet, um eine auf Standards basierende Webserviceschnittstelle bereitzustellen, mit der Oracle ILOM über das HTTPS-Protokoll verwaltet wird. Wenn dieser Service deaktiviert wird, kann Oracle ILOM nicht mit diesem Protokoll verwaltet werden. Ab Oracle ILOM Version 3.2 ist dieser Service nicht mehr enthalten. |
| Single Sign-on | TCP | 11626 | Dieser Port wird von der integrierten Single Sign-On-Funktion verwendet, mit der ein Benutzer seinen Benutzernamen und sein Passwort nicht mehr so häufig eingeben muss. Wenn dieser Service deaktiviert wird, kann KVMS nicht mehr ohne erneute Eingabe eines Passwortes gestartet werden. |

# Härten der Oracle ILOM-Sicherheitskonfiguration

In diesen Themen wird beschrieben, wie Oracle ILOM über verschiedene Konfigurationseinstellungen gesichert wird.

# ▼ Deaktivieren nicht erforderlicher Services (Oracle ILOM)

Deaktivieren Sie Services, die zur Unterstützung der Betriebs- und Managementanforderungen der Plattform nicht erforderlich sind.

Standardmäßig nutzt Oracle ILOM eine Secure-by-Default-Netzwerkkonfiguration, bei der nicht wesentliche Services bereits deaktiviert sind. Je nach Ihren Sicherheitsrichtlinien und Sicherheitsbestimmungen müssen möglicherweise weitere Services deaktiviert werden.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**

   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Bestimmen Sie die Liste der Services, die von Oracle ILOM unterstützt werden.**

   ```
   -> show /SP/services
   ```

3. **Prüfen Sie, ob ein bestimmter Service aktiviert ist.**

   Ersetzen Sie *servicename* durch den Namen des Service, der in Schritt 2 identifiziert wird.

   ```
   -> show /SP/services/servicename servicestate
   ```

   Während die meisten Services den Parameter `servicestate` zur Aufzeichnung, ob der Service aktiviert oder deaktiviert ist, erkennen und verwenden, gibt es einige wenige Services, wie `servicetag`, `ssh`, `sso` und `wsman`, die einen Parameter namens `state` verwenden. Ungeachtet des

tatsächlich verwendeten Parameters ist ein Service aktiviert, wenn der Parameter `servicestate` oder `state` einen Wert `enabled` zurückgibt, wie in diesen Beispielen dargestellt:

```
-> show /SP/services/https servicestate
/SP/services/https
Properties:
servicestate = enabled
```

```
-> show /SP/services/ssh state
/SP/services/ssh
Properties:
state = enabled
```

4. **Um einen Service zu deaktivieren, der nicht erforderlich ist, legen Sie den Servicestatus auf `disabled` fest.**

```
-> set /SP/services/http servicestate=disabled
```

5. **Prüfen Sie, ob einer dieser Services deaktiviert werden muss.**

   Je nach den verwendeten Tools und Methoden können diese zusätzlichen Services deaktiviert werden, wenn sie nicht erforderlich sind oder nicht verwendet werden.

   - **Bei einer administrativen Browseroberfläche (HTTP, HTTPS) geben Sie Folgendes ein:**

     ```
     -> set /SP/services/http servicestate=disabled
     -> set /SP/services/http secureredirect=disabled
     -> set /SP/services/https servicestate=disabled
     ```

   - **Bei Tastatur-, Video-, Mausservices (KVMS) geben Sie Folgendes ein:**

     ```
     -> set /SP/services/kvms servicestate=disabled
     ```

   - **Bei Webservices-Management (WS-Man über HTTP/HTTPS) - (Oracle ILOM Version 3.1 und älter) geben Sie Folgendes ein:**:

     ```
     -> set /SP/services/wsman state=disabled
     ```

   - **Bei Single Sign-On-Services (SSO) geben Sie Folgendes ein:**

     ```
     -> set /SP/services/sso state=disabled
     ```

## ▼ Konfigurieren der HTTP-Umleitung zu HTTPS (Oracle ILOM)

Standardmäßig ist Oracle ILOM so konfiguriert, dass eingehende HTTP-Anforderungen an den HTTPS-Service umgeleitet werden, um sicherzustellen, dass die gesamte browserbasierte Kommunikation zwischen Oracle ILOM und dem Administrator verschlüsselt ist.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**

   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Prüfen Sie, ob die sichere Umleitung aktiviert ist.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **Wenn der Standardwert geändert wurde, können Sie die sichere Umleitung aktivieren.**

```
-> set /SP/services/http secureredirect=enabled
```

4. **Prüfen Sie die Einstellung, indem Sie Schritt 2 wiederholen.**

# Deaktivieren nicht genehmigter Protokolle

In diesen Themen wird beschrieben, wie nicht genehmigte Protokolle deaktiviert werden:

- Deaktivieren des SLv2-Protokolls für HTTPS [44]
- Deaktivieren des SLv3-Protokolls für HTTPS [45]

## ▼ Deaktivieren des SLv2-Protokolls für HTTPS

Standardmäßig ist das SSLv2-Protokoll für den HTTPS-Service deaktiviert.

Aus Sicherheitsgründen muss SSLv2 unbedingt deaktiviert sein.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**

   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Prüfen Sie, ob das SSLv2-Protokoll für den HTTP-Service deaktiviert ist.**

```
-> show /SP/services/https sslv2
/SP/services/https
Properties:
sslv2 = disabled
```

3. **Wenn der Service aktiviert ist, deaktivieren Sie das SSLv2-Protokoll.**

```
-> set /SP/services/https sslv2=disabled
```

4. **Prüfen Sie die Einstellung, indem Sie Schritt 2 wiederholen.**

## ▼ Deaktivieren des SLv3-Protokolls für HTTPS

Standardmäßig ist das SSLv3-Protokoll für den HTTPS-Service aktiviert.

Deaktivieren Sie das SSLv3-Protokoll aus Sicherheitsgründen.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**
   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Prüfen Sie, ob das SSLv3-Protokoll für den HTTP-Service deaktiviert ist.**

```
-> show /SP/services/https sslv3
/SP/services/https
Properties:
sslv3 = enabled
```

3. **Deaktivieren Sie das SSLv3-Protokoll.**

```
-> set /SP/services/https sslv3=disabled
```

4. **Prüfen Sie die Einstellung, indem Sie Schritt 2 wiederholen.**

# ▼ Deaktivieren nicht genehmigter TLS-Protokolle für HTTPS

Standardmäßig sind die TLSv1.0-, TLSv1.1- und TLSv1.2-Protokolle für den HTTPS-Service. aktiviert

Sie können ein oder mehrere TLS-Protokollversionen deaktivieren, die nicht mit Ihren Sicherheitsrichtlinien konform sind.

Aus Sicherheitsgründen verwenden Sie TLSv1.2, es sei denn, die Unterstützung älterer Versionen des TLS-Protokolls ist erforderlich.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**
   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Prüfen Sie die Liste der TLS-Protokollversionen, die für den HTTPS-Service aktiviert sind.**

```
-> show /SP/services/https tlsv1 tlsv1_1 tlsv1_2
/SP/services/https
Properties:
tlsv1 = enabled
tlsv1_1 = enabled
tlsv1_2 = enabled
```

3. **Deaktivieren Sie TLSv1.0.**

```
-> set /SP/services/https tlsv1_0=disabled
```

4. **Deaktivieren Sie TLSv1.1.**

```
-> set /SP/services/https tlsv1_1=disabled
```

5. **Prüfen Sie die Einstellung, indem Sie Schritt 2 wiederholen.**

# ▼ Deaktivieren von unsicheren und mittelsicheren SSL-Verschlüsselungsverfahren für HTTPS

Standardmäßig deaktiviert Oracle ILOM die Verwendung von unsicheren und mittelsicheren Verschlüsselungsverfahren für den HTTPS-Service.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**
   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Prüfen Sie, ob unsichere oder mittelsichere Verschlüsselungsverfahren deaktiviert sind.**

```
-> show /SP/services/https weak_ciphers
/SP/services/https
Properties:
weak_ciphers = disabled
```

3. **Wenn der Standard deaktiviert wurde, können Sie die Verwendung von unsicheren und mittelsicheren Verschlüsselungsverfahren deaktivieren.**

```
-> set /SP/services/https weak_ciphers=disabled
```

4. **Prüfen Sie die Einstellung, indem Sie Schritt 2 wiederholen.**

# ▼ Deaktivieren nicht genehmigter SNMP-Protokolle (Oracle ILOM)

Standardmäßig ist nur das SNMPv3-Protokoll für den SNMP-Service aktiviert, der zur Überwachung und Verwaltung von Oracle ILOM verwendet wird. Stellen Sie sicher, dass ältere Versionen des SNMP-Protokolls deaktiviert bleiben, es sei denn, sie müssen aktiviert werden.

Einige Oracle- und Fremdprodukte begrenzen die Unterstützung für neuere SNMP-Protokolle. In der Produktdokumentation für diese Komponenten wird beschrieben, ob bestimmte SNMP-Protokollversionen unterstützt werden. Stellen Sie sicher, dass Oracle ILOM zur Unterstützung von Protokollversionen konfiguriert ist, die von diesen Komponenten benötigt werden.

---

**Anmerkung -** Ab Version 3 des SNMP-Protokolls wird das benutzerbasierte Sicherheitsmodell (User-based Security Model (USM)) unterstützt. Diese Funktionalität ersetzt die üblichen SNMP-Communityzeichenfolgen durch tatsächliche Benutzerkonten, die mit bestimmten Berechtigungen, Authentifizierungs- und Datenschutzprotokollen und Passwörtern konfiguriert werden können. Standardmäßig umfasst Oracle ILOM keine USM-Konten. Konfigurieren Sie SNMPv3 USM-Konten entsprechend Ihren Deployment-, Management- und Überwachungsanforderungen.

---

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**
   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Bestimmen Sie den Status jedes der SNMP-Protokolle.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = disabled
v2c = disabled
v3 = enabled
```

3. **Falls erforderlich deaktivieren Sie SNMPv1 und SNMPv2c.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

4. **Prüfen Sie die Einstellung, indem Sie Schritt 2 wiederholen.**

# ▼ Konfigurieren von SNMP v1- und v2c-Communityzeichenfolgen (Oracle ILOM)

Diese Aufgabe ist nur anwendbar, wenn SNMP v1 oder SNMPv2c zur Verwendung aktiviert und konfiguriert ist.

Damit SNMP ordnungsgemäß arbeiten kann, müssen ein Client und ein Server die Communityzeichenfolge vereinbaren, die zur Authentifizierung des Zugriffs verwendet wird. Wenn also SNMP-Communityzeichenfolgen geändert werden, müssen Sie sicherstellen, dass die neue Zeichenfolge sowohl für Oracle ILOM als auch für alle Komponenten konfiguriert ist, die versuchen, mit dem SNMP-Protokoll eine Verbindung zu Oracle ILOM herzustellen.

Weil SNMP häufig zur Überwachung der Integrität des Geräts verwendet wird, müssen die SNMP-Standardcommunityzeichenfolgen, die von dem Gerät verwendet werden, durch vom Kunden definierte Werte ersetzt werden.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**

   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Erstellen Sie eine neue SNMP-Communityzeichenfolge.**

   In diesem Beispiel ersetzen Sie die folgenden Elemente in der Befehlszeile:

   - *string* – Ersetzen Sie diese Zeichenfolge durch einen vom Kunden definierten Wert, der den Sicherheitsbestimmungen des US-Verteidigungsministeriums entspricht, was den Aufbau der SNMP-Communityzeichenfolgen betrifft.
   - *access* – Ersetzen Sie diesen Wert durch `ro` oder `rw`, je nachdem, ob es sich um eine schreibgeschützte oder nicht schreibgeschützte Zugriffszeichenfolge handelt.

```
-> create /SP/services/snmp/communities/string permission=access
```

   Nachdem neue Communityzeichenfolgen erstellt wurden, müssen die Standardcommunityzeichenfolgen entfernt werden.

3. **Entfernen Sie die SNMP-Standardcommunityzeichenfolgen.**

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

4. **Prüfen Sie die SNMP-Communityzeichenfolgen.**

```
-> show /SP/services/snmp/communities
```

# Ersetzen von selbstsignierten Zertifikaten (Oracle ILOM)

Oracle ILOM verwendet selbstsignierte Zertifikate, um die Out-of-the-Box-Verwendung der SSL- und TLS-Protokolle zu aktivieren. Wenn möglich ersetzen Sie selbstsignierte Zertifikate durch Zertifikate, die zur Verwendung in Ihrer Umgebung genehmigt und von einer anerkannten Certificate Authority signiert sind.

Oracle ILOM unterstützt eine Vielzahl von Methoden, die für den Zugriff auf das digitale Zertifikat und den Private Key verwendet werden können, einschließlich HTTPS, HTTP, SCP, FTP, TFTP und dem Einfügen von Informationen direkt in eine Webbrowseroberfläche. Weitere Informationen finden Sie in *Oracle ILOM - Konfigurations- und Wartungshandbuch* (siehe „Zusätzliche Oracle ILOM-Ressourcen“ [52]).

1. **Prüfen Sie, ob Oracle ILOM ein selbstsigniertes Standardzertifikat verwendet.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

2. **Installieren Sie das Zertifikat Ihres Unternehmens.**

```
-> set /SP/services/https/ssl/custom_cert load_uri=URI_method
-> set /SP/services/https/ssl/custom_key load_uri=URI_method
```

# Konfigurieren des Inaktivitätstimeouts der administrativen Browseroberfläche

Oracle ILOM unterstützt die Trennung und Abmeldung von administrativen Sessions, die während mehr als einer vordefinierten Anzahl von Minuten inaktiv waren. Standardmäßig wird die Session der Browseroberfläche nach 15 Minuten wegen Timeouts abgebrochen.

Die Sessiontimeoutparameter für die HTTPS- und HTTP-Services werden unabhängig voneinander festgelegt und verwaltet. Sie müssen den `sessiontimeout`-Parameter für jeden Service unbedingt festlegen.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**

   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Prüfen Sie den Parameter für den Inaktivitätstimeout des HTTPS-Service.**

```
-> show /SP/services/https sessiontimeout
/SP/services/https
Properties:
sessiontimeout = 15
```

3. **Legen Sie den Parameter für den Inaktivitätstimeout fest.**

   Ersetzen Sie *n* durch einen Wert in Minuten.

```
-> set /SP/services/https sessiontimeout=n
```

4. **Prüfen Sie den Parameter für den Inaktivitätstimeout des HTTP-Service.**

```
-> show /SP/services/http sessiontimeout
/SP/services/http
Properties:
sessiontimeout = 15
```

5. **Legen Sie den Parameter für den Inaktivitätstimeout fest.**

   Ersetzen Sie *n* durch einen Wert in Minuten.

```
-> set /SP/services/http sessiontimeout=n
```

6. **Prüfen Sie die Einstellung, indem Sie Schritt 2 und Schritt 4 wiederholen.**

# ▼ Konfigurieren des Timeouts der Administrationsoberfläche (Oracle ILOM CLI)

Oracle ILOM unterstützt die Trennung und Abmeldung von CLI-Administrationssessions, die während mehr als einer vordefinierten Anzahl von Minuten inaktiv waren.

Standardmäßig ist für die SSH-CLI kein Timeoutwert angegeben, und somit bleiben Benutzer mit Administrationsberechtigung, die auf diesen Service zugreifen, endlos angemeldet.

Legen Sie diesen Parameter aus Sicherheitsgründen so fest, dass er mit dem Wert für die Browserbenutzeroberfläche übereinstimmt. Dies könnte ein Wert von 15 Minuten oder ein anderer Wert sein.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**

   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Prüfen Sie den Parameter für den Inaktivitätstimeout der CLI.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **Legen Sie den Parameter für den Inaktivitätstimeout fest.**

   Ersetzen Sie *n* durch einen Wert in Minuten.

```
-> set /SP/cli timeout=n
```

4. **Prüfen Sie die Einstellung, indem Sie Schritt 2 wiederholen.**

# Konfigurieren von Anmeldewarnungsbannern (Oracle ILOM)

Oracle ILOM unterstützt die Anzeige von kundenspezifischen Meldungen bevor und nachdem ein Administrator die Verbindung zu dem Gerät hergestellt hat.

Die Oracle-ILOM-Verbindungsmeldung wird vor der Authentifizierung angezeigt, während die Anmeldemeldung nach der Authentifizierung angezeigt wird.

Optional können Sie Oracle ILOM so konfigurieren, dass die Anmeldemeldung akzeptiert werden muss, bevor Zugriff auf die Oracle ILOM-Funktionen erteilt wird. Sowohl die Verbindungs- und Anmeldemeldungen als auch die optionale Annahme werden in den Browser- und Befehlszeilenzugriffsoberflächen implementiert.

Oracle ILOM unterstützt Verbindungs- und Anmeldemeldungen mit einer Länge von bis zu 1.000 Zeichen.

1. **Melden Sie sich im Managementnetzwerk bei Oracle ILOM an.**

   Siehe Anmelden bei der Oracle ILOM-CLI [37].

2. **Prüfen Sie, ob Verbindungs- und Anmeldemeldungen konfiguriert sind.**

```
-> show /SP/preferences/banner connect_message login_message
/SP/preferences/banner
Properties:
connect_message = (none)
login_message = (none)
```

3. **Legen Sie eine Verbindungs- oder Anmeldemeldung fest.**

```
-> set /SP/preferences/banner connect_message="Authorized Use Only"
-> set /SP/preferences/banner login_message="Authorized Use Only"
```

4. **Prüfen Sie, ob die Annahme der Anmeldemeldung aktiviert ist.**

```
-> show /SP/preferences/banner login_message_acceptance
/SP/preferences/banner
Properties:
login_message_acceptance = disabled
```

5. **(Optional) Setzen Sie die Annahme der Anmeldemeldung durch.**

**Achtung -** Wenn die Annahme der Anmeldemeldung gefordert wird, kann sich dies auf den einwandfreien Ablauf der automatisierten Managementprozesse auswirken, die SSH verwenden, weil diese möglicherweise nicht in der Lage sind, auf die Annahmeanforderung zu antworten, oder nicht dafür konfiguriert sind. Deshalb können diese Verbindungen blockiert oder wegen Timeouts abgebrochen werden, weil Oracle ILOM die Verwendung der CLI erst zulässt, nachdem die Anforderung der Meldungsannahme erfüllt wurde.

```
-> set /SP/preferences/banner login_message_acceptance=enabled
```

6. **Prüfen Sie die Einstellung, indem Sie Schritt 2 und Schritt 4 wiederholen.**

# Zusätzliche Oracle ILOM-Ressourcen

Weitere Informationen zu den Oracle ILOM-Administrations- und Sicherheitsprozeduren finden Sie in der Oracle ILOM-Dokumentationsbibliothek für die Version, die in SuperCluster M7 ausgeführt wird:

- *Oracle ILOM - Sicherheitshandbuch - Firmwarereleases 3.0, 3.1 und 3.2*:

  http://docs.oracle.com/cd/E37444_01/html/E37451
- Oracle Integrated Lights Out Manager Version 3.2.*x*:

http://docs.oracle.com/cd/E37444_01

- Oracle Integrated Lights Out Manager Version 3.1.*x*:

  http://docs.oracle.com/cd/E24707_01

- Oracle Integrated Lights Out Manager Version 3.0.*x*:

  http://docs.oracle.com/cd/E19860-01

# Sichern der Rechenserver

Ein oder zwei SPARC M7-Server (Rechenserver) sind in SuperCluster M7 installiert. Jeder Rechenserver ist in zwei Hardwarepartitionen (zwei PDomains) unterteilt. Jede PDomain enthält die Hälfte der möglichen Prozessoren, Speicher, PCIe-Erweiterungsslots in dem Gehäuse. Beide PDomains arbeiten als separater Server innerhalb desselben Gehäuses. Ein redundantes Paar von Serviceprozessormodulen (SPMs) verwaltet jede Partition.

Sie müssen jede PDomain sichern.

Dieser Abschnitt enthält ein Set von Sicherheitskontrollen für die Rechenserver.



## ▼ Anmelden bei einem Rechenserver und Ändern des Standardpasswortes

Für den Zugriff auf eine einzelne PDomain über Oracle ILOM müssen Sie sich bei dem aktiven SPM anmelden, das diese PDomain kontrolliert. Sie können eine Partition einschalten, neu starten oder verwalten, während die andere Partition weiter normal arbeitet.

Es gibt verschiedene Methoden, mit denen Sie sich bei einem SuperCluster-Rechenserver anmelden können. Bei der in dieser Aufgabe beschriebenen Methode melden Sie sich bei Oracle ILOM CLI in dem SPM des Rechenservers an. Mit dieser Methode können Sie in einem dieser Status auf den Server zugreifen:

- Standbyenergiestatus
- System eingeschaltet, Host wird jedoch nicht ausgeführt
- BS wird gebootet
- Vollständig eingeschaltet und BS wird ausgeführt

1. **Melden Sie sich im Managementnetzwerk mit dem Befehl `ssh` an.**

```
$ ssh root@compute_server_SPM_ILOM_IP-address
```

2. **Geben Sie bei entsprechender Aufforderung das Passwort ein.**

   Das werksseitige Standard-`root`-Passwort ist `welcome1`.

   Wenn Sie zur Änderung des Passwortes aufgefordert werden, ändern Sie das Passwort.

   An dieser Stelle können Sie alle Sicherheitsaufgaben für Oracle ILOM auf dem Rechenserver ausführen.

3. **Wenn Sie auf die Hostkonsole des Rechenservers zugreifen möchten, starten Sie die Hostkonsole.**

```
    -> start /Servers/PDomains/PDomain_0/HOST/console
Are you sure you want to start /Servers/PDomains/PDomain_0/HOST/console (y/n)? y

Serial console started.  To stop, type #.

root@system-identifier-pd0:~#
```

**Anmerkung -** Die PDomain-Eingabeaufforderung wird nicht angezeigt, wenn der Host nicht ausgeführt wird.

**Anmerkung -** Um zu dem Oracle ILOM-Prompt zurückzugehen, geben Sie die Escapezeichen ein (`#.` sind die Standardzeichen).

4. **Falls erforderlich übernehmen Sie eine Superuser-Rolle.**

   Mit dem Befehl `su` können Sie zu einem Benutzer wechseln, der mit der `root`-Rolle konfiguriert ist.

# Standardkonten und -passwörter (Rechenserver)

| Konto | Standardpasswort | Beschreibung |
|---|---|---|
| `Root` | `welcome1` | Oracle ILOM fordert, dass das Standardpasswort sofort nach der ersten erfolgreichen Anmeldung geändert wird. |
| `oracle` | `welcome1` | |
| `grid` | `welcome1` | |

## ▼ Bestimmen der SuperCluster-Softwareversion

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Geben Sie diesen Befehl ein.**

```
# svcprop -p configuration/build svc:/system/oes/id:default
```

   In der Ausgabe stellen die an `ssc` angehängten Zahlen die Softwareversion dar.

   Um die Version der SuperCluster-Software zu aktualisieren, installieren Sie das neueste SuperCluster Quarterly Full Stack Download Patch, das in My Oracle Support unter `https://support.oracle.com` verfügbar ist.

---

**Anmerkung -** Bei SuperCluster können zusätzliche Einschränkungen die Softwareversionen, die verwendet werden können, und die Art der Aktualisierung dieser Versionen begrenzen. Wenden Sie sich in diesen Fällen an Ihren Oracle-Ansprechpartner.

---

## ▼ Konfigurieren des Secure Shell-Service

Durch Ausführung dieser Aufgabe kann die Secure Shell-Sicherheitskonfiguration verbessert werden, die in Oracle SuperCluster bereitgestellt ist.

Die Datei `/etc/ssh/sshd_config` ist eine systemweit gültige Konfigurationsdatei, in der Sie Parameter für den Secure Shell-Service konfigurieren.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**
   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Bearbeiten Sie die Datei `/etc/ssh/sshd_config`.**

3. **Konfigurieren Sie den Parameter `ListenAddress`, um sicherzustellen, dass nur Verbindungen von dem SuperCluster-Clientzugriffsnetzwerk akzeptiert werden.**
   Stellen Sie sicher, dass die IP-Adresse `ListenAddress` auf das Clientnetzwerk festgelegt ist. Dadurch wird sichergestellt, dass Secure Shell-Verbindungen nicht erfolgreich zwischen Komponenten über die Management- oder IB-Netzwerke ausgelöst werden können.

4. **Prüfen Sie andere `sshd_config`-Parameter, und legen Sie diese entsprechend den Siteanforderungen fest.**
   Diese Einstellungen sichern den Secure Shell-Service:

```
Protocol 2
Banner /etc/issue
PermitEmptyPasswords no
PermitRootLogin no
StrictModes yes
IgnoreRhosts yes
PrintLastLog yes
X11Forwarding no
ClientAliveInterval 600
ClientAliveCountMax 0
```

5. **Speichern Sie die Datei `sshd_config`.**

6. **Starten Sie den Service neu.**
   Sie müssen den Service neu starten, damit die Änderungen übernommen werden.

```
# svcadm restart ssh
```

## ▼ Prüfen, ob `root` eine Rolle ist

Standardmäßig ist Oracle Solaris so konfiguriert, dass `root` eine Rolle und kein Benutzerkonto ist. Außerdem lässt die SuperCluster-Konfiguration keine anonymen `root`-Benutzeranmeldungen zu. Stattdessen müssen sich alle Benutzer als regulärer Benutzer anmelden, bevor die Root-Rolle übernommen werden kann. Alle SuperCluster-Administrationsvorgänge müssen mit `root` als Rolle ausgeführt werden.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole auf.**

Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Prüfen Sie, ob `root`-Attribute auf `type=role` festgelegt sind.**

```
# grep root /etc/user_attr
root::::type=role
```

3. **(Optional) Weisen Sie einem regulären Benutzer die `root`-Rolle zu.**

```
# usermod -R root user_name
```

# Verfügbar gemachte Standardnetzwerke (Rechenserver)

In dieser Tabelle werden die Standardnetzwerkservices aufgeführt, die erneut auf Rechenservern verfügbar gemacht werden.

| Servicename | Protokoll | Port | Beschreibung |
|---|---|---|---|
| SSH | TCP | 22 | Wird von dem integrierten Secure Shell-Service verwendet, um den administrativen Zugriff auf die Rechenserver mit einer CLI zu aktivieren. |
| HTTP (BUI) | TCP | 80 | Wird von dem integrierten HTTP-Service verwendet, um den administrativen Zugriff auf die Rechenserver mit einer Browseroberfläche zu aktivieren. |
| HTTPS (BUI) | TCP | 443 | Wird von dem integrierten HTTPS-Service verwendet, um den administrativen Zugriff auf die Rechenserver über einen verschlüsselten (SSL/TLS-)Kanal mit einer Browseroberfläche zu aktivieren. |
| SNMP | UDP | 161 | Wird von dem integrierten SNMP-Service verwendet, um eine Managementoberfläche zur Überwachung der Integrität der Rechenserver und zur Überwachung empfangener Trap-Benachrichtigungen bereitzustellen. |

# Härten der Sicherheitskonfiguration des Rechenservers

In diesen Themen wird beschrieben, wie die Rechenserver sicher konfiguriert werden.

# ▼ Aktivieren des `intrd`-Service

Der Interrupt Balancer-(`intrd`-)Service überwacht die Zuweisungen zwischen Interrupts und CPUs, um optimale Performance sicherzustellen. Weitere Einzelheiten finden Sie in der `intrd (1M)`-Manpage.

Dieser Service wird nur in der globalen Zone ausgeführt.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Starten Sie den Service.**

```
# svcadm enable intrd
```

# ▼ Deaktivieren nicht erforderlicher Services (Rechenserver)

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Deaktivieren Sie die NFS-Statusüberwachung, wenn das System kein NFS-Client oder -Server ist.**

   Dieser Service kommuniziert mit `lockd(1M)`, um die Crash- und Recovery-Funktionen für die Sperrservices auf NFS bereitzustellen

   ```
   # svcadm disable svc:/network/nfs/status
   ```

3. **Deaktivieren Sie den NFS-Lock-Manager-Service, wenn Sie NFS überhaupt nicht verwenden oder NFS v4 verwenden.**

   Der NFS-Lock-Manager unterstützt Vorgänge zur Datensatzsperre bei NFS-Dateien in NFSv2 und NFSv3.

   ```
   # svcadm disable svc:/network/nfs/nlockmgr
   ```

4. **Wenn das System keine Dateien einhängt, können Sie den NFS-Clientservice deaktivieren oder dessen Package deinstallieren.**

   Der NFS-Clientservice wird nur benötigt, wenn das System Dateien von einem NFS-Server einhängt. Weitere Informationen finden Sie in der `mount_nfs(1M)`-Manpage.

   ```
   # svcadm disable svc:/network/nfs/client
   ```

5. **Deaktivieren Sie den NFS-Serverservice in einem System, das kein NFS-Dateiserver ist.**

   Der NFS-Serverservice verwaltet Clientdateisysteme über NFS-Versionen 2, 3 und 4. Wenn dieses System kein NFS-Server ist, deaktivieren Sie den Service.

   ```
   # svcadm disable svc:/network/nfs/server
   ```

6. **Wenn Sie FedFS für DNS-SRV-Datensätze oder LDAP-basierte Referrals nicht verwenden, deaktivieren Sie den Service.**

   Der Federated File System-(FedFS-)Clientservice verwaltet Standardwerte und Verbindungsinformationen für LDAP-Server, in denen FedFS-Informationen, gespeichert werden

```
# svcadm disable svc:/network/nfs/fedfs-client
```

7. **Deaktivieren Sie den `rquota`-Service.**

   Der `Remote`-Quotaserver gibt Quota für einen Benutzer eines lokalen Dateisystems zurück, das über NFS eingehängt ist. Die Ergebnisse werden von `quota(1M)` verwendet, um Benutzerquota für Remote-Dateisysteme anzuzeigen. Der `rquotad(1M)`-Daemon wird im Allgemeinen von `inetd (1M)` aufgerufen. Der Daemon stellt potenziell böswilligen Benutzern Informationen über das Netzwerk bereit.

   ```
   # svcadm disable svc:/network/nfs/rquota
   ```

8. **Deaktivieren Sie den `cbd`-Service.**

   Der `cbd`-Service verwaltet Kommunikationsendpunkte für das NFS Version 4-Protokoll. Der `nfs4cbd(1M)`-Daemon wird auf dem NFS Version 4-Client ausgeführt und erstellt einen Listener-Port für Callbacks.

   ```
   # svcadm disable svc:/network/nfs/cbd
   ```

9. **Deaktivieren Sie den `mapid`-Service, wenn Sie NFSv4 nicht verwenden.**

   Der Daemon-Service zur NFS-Benutzer- und Gruppen-ID-Zuordnung nimmt die Zuordnung zu und von NFS-Version 4 `owner`- und `owner_group`-ID-Attributen und lokalen UID und GID-Nummern vor, die sowohl von dem NFS-Version 4-Client als auch dem NFS-Version 4-Server verwendet werden.

   ```
   # svcadm disable svc:/network/nfs/mapid
   ```

10. **Deaktivieren Sie den `ftp`-Service.**

    Der FTP-Service stellt einen unverschlüsselten Dateiübertragungsservice bereit und verwendet Nur-Text-Authentifizierung. Verwenden Sie das `scp(1)`-Programm (Secure Copy Program), anstelle von `ftp`, weil es verschlüsselte Authentifizierung und verschlüsselte Dateiübertragung bietet.

    ```
    # svcadm disable svc:/network/ftp:default
    ```

11. **Deaktivieren Sie den Remote Volume-Managerservice.**

    Der Wechsel-Volume-Manager ist ein HAL-fähiger Volume-Manager, der Wechselmedien und austauschbaren Speicher automatisch ein- und aushängen kann. Benutzer könnten schädliche Programme importieren oder vertrauliche Daten aus dem System übertragen. Weitere Einzelheiten finden Sie in der `rmvolmgr(1M)`-Manpage.

    Dieser Service wird nur in der globalen Zone ausgeführt.

```
# svcadm disable svc:/system/filesystem/rmvolmgr
```

**12. Deaktivieren Sie den `smserver`-Service.**

Der `smserver`-Service wird für den Zugriff auf Wechselmediengeräte verwendet.

```
# svcadm disable rpc/smserver:default
```

**13. Geben Sie `pam_deny.so.1` als Modul für den Authentifizierungsstack für die `r-protocol`-Services im Verzeichnis `/etc/pam.d` an.**

Standardmäßig werden Legacy-Services wie `r-protocols`, `rlogin(1)` und `rsh(1)` nicht installiert. Diese Services werden jedoch in `/etc/pam.d` definiert. Wenn Sie die Servicedefinitionen aus `/etc/pam.d` entfernen, verwenden die Services die anderen Services (beispielsweise SSH), falls die Legacy-Services aktiviert sind.

```
# cd /etc/pam.d
# cp rlogin rlogin.orig
# pfedit rlogin
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
# cp rsh rsh.orig
# pfedit rsh
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
```

**14. Bearbeiten Sie die Datei `/etc/default/keyserv`, um den Wert von `ENABLE_NOBODY_KEYS` in `NO` zu ändern.**

Der `keyserv`-Service kann den Benutzerschlüssel `nobody` nicht verwenden. Der Wert von `ENABLE_NOBODY_KEYS` ist standardmäßig `YES`.

```
# pfedit /etc/default/keyserv
. . .
ENABLE_NOBODY_KEYS=NO
```

**15. Fügen Sie Benutzer zu der Datei `ftpusers` hinzu, um den `ftp`-Zugriff zu begrenzen.**

FTP-Dateiübertragungen dürfen nicht für alle Benutzer verfügbar sein; nur qualifizierte Benutzer dürfen ihre Namen und Passwörter angeben. Im Allgemeinen sollte Systembenutzern die Verwendung von FTP nicht gestattet sein. Mit dieser Prüfung wird geprüft, ob Systemkonten in der Datei `/etc/ftpd/ftpusers` enthalten sind, damit diese FTP nicht verwenden dürfen.

Die Datei `/etc/ftpd/ftpusers` wird verwendet, um Benutzern die Verwendung des FTP-Service zu untersagen. Beziehen Sie mindestens alle Systembenutzer, wie `root`, `bin`, `adm` usw. ein.

```
# pfedit /etc/ftpd/ftpusers
....
root
```

```
daemon
bin
...
```

16. **Legen Sie eine starke Dateierstellungsmaske für Dateien fest, die vom FTP-Server erstellt werden.**

    Der FTP-Server verwendet nicht unbedingt die Erstellungsmaske für Systemdateien des Benutzers. Durch Festlegung von FTP umask wird sichergestellt, dass die über FTP übertragenen Dateien eine starke Dateierstellungs-umask verwenden.

    ```
    # pfedit /etc/proftpd.conf
    Umask          027
    ```

17. **Deaktivieren Sie Antworten auf Netzwerktopologieabfragen.**

    Antworten auf Echoanforderungen müssen unbedingt deaktiviert werden. ICMP-Anforderungen werden mit dem Befehl `ipadm` verwaltet.

    Diese Einstellungen unterbinden die Verteilung von Informationen über die Netzwerktopologie.

    ```
    # ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
    # ipadm set-prop -p _respond_to_echo_broadcast=0 ip
    ```

18. **Deaktivieren Sie die Umleitung von ICMP-Meldungen.**

    Router verwenden ICMP-Umleitungsmeldungen, um Hosts über direktere Routen zu einem Ziel zu informieren. Eine unzulässige ICMP-Umleitungsmeldung kann zu einem Man-in-the-Middle-Angriff führen.

    ```
    # ipadm set-prop -p _ignore_redirect=1 ipv4
    ```

19. **Deaktivieren Sie `mesg(1)`, um den `talk(1)`- und `write(1)`-Zugriff auf Remote-Terminals zu verhindern.**

    ```
    # mesg -n
    ```

20. **(Optional) Prüfen und deaktivieren Sie nicht erforderliche Services, die auf dem Netzwerk horchen.**

    Standardmäßig ist `ssh(1)` der einzige Netzwerkservice, der Netzwerkpakete senden und empfangen kann.

    ```
    # svcadm disable FMRI_of_unneeded_service
    ```

# ▼ Aktivieren von Strict Multihoming

Aktivieren Sie Strict Multihoming für Systeme, die als Gateway zu anderen Domains fungieren, zum Beispiel Firewalls oder VPN-Knoten. Die Eigenschaft `hostmodel` kontrolliert das Sende- und Empfangsbehavior für IP-Pakete in einem Multihome-System. Legen Sie das Strict

Multihoming auf `1` fest, damit Pakete nicht auf einer anderen Oberfläche akzeptiert werden. Der Standardwert ist `0`.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**
   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Legen Sie Strict Multihoming auf `1` fest.**

```
# ipadm set-prop -p _strict_dst_multihoming=1 ipv4
```

## Aktivieren von ASLR

**Anmerkung -** Aktivieren Sie ASLR nicht in Datenbankdomains oder in Datenbankzonen.

Oracle Solaris taggt viele Benutzerbinärdateien so, dass die zufällige Anordnung des Layouts des Adressraums (Address Space Layout Randomization (ASLR)) aktiviert ist. ASLR ordnet die Startadresse von Schlüsselteilen eines Adressraums zufällig an. Diese Sicherheitsabwehrmaßnahme kann verhindern, dass ROP-(Return Oriented Programming) -Angriffe erfolgreich verlaufen, wenn sie versuchen, Softwaresicherheitslücken zu nutzen. Zonen übernehmen diese zufällige Anordnung des Layouts für ihre Prozesse. Weil die Verwendung von ASLR möglicherweise nicht für alle Binärdateien optimal verläuft, ist ASLR auf Zonen- und Binärebene konfigurierbar.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**
   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Aktivieren Sie ASLR.**

```
# sxadm delcust aslr
# sxadm info
EXTENSION    STATUS                CONFIGURATION
aslr         enabled (tagged-files) System default (default)
```

## Konfigurieren von TXP-Verbindungen

Wenn der Höchstwert von halb-geöffneten TCP-Verbindungen pro IP-Adresse und pro Port auf 4096 festgelegt wird, kann die SYN-Flut von Denial-of-Service-Angriffen abgewiesen werden.

Wenn die maximale Anzahl von in der Queue gespeicherten eingehenden TCP-Verbindungen auf mindestens 1024 festgelegt wird, können bestimmte verteilte Denial-of-Service-(DDoS-) Angriffe verhindert werden.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Legen Sie die Höchstzahl von halb-geöffnete und in der Queue gespeicherten eingehenden T CP-Verbindungen fest.**

```
# ipadm set-prop -p _conn_req_max_q0=9096 tcp
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

# Festlegen von Passworthistorienlogs und Passwortrichtlinien für PCI-Compliance

Der Parameter `HISTORY` in der Datei `/etc/default/passwd` verhindert, dass Benutzer ähnliche Passwörter mit dem Wert `HISTORY` verwenden.

Wenn der Befehl `MINWEEKS` auf `3` und `HISTORY` auf `10` festgelegt ist, können Passwörter nicht 10 Monate lang wiederverwendet werden.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Bearbeiten Sie die Datei `/etc/default/passwd`, und legen Sie die Passwortparameter fest.**

```
# pfedit /etc/default/passwd
. . .
#Compliance to the PCI-DSS benchmark is 10
#HISTORY=0
HISTORY=10
MINDIFF=4
MINDIGIT=1
MINUPPER=1
MINWEEKS=3
MAXWEEKS=13
```

3. **Bearbeiten Sie die Datei `/etc/default/login`, um diese Parameter einzubeziehen.**

```
# pfedit /etc/default/login
. . .
# Compliance edit
#PASSLENGTH=6
PASSLENGTH=14
. . .
```

## Sicherstellen, dass Benutzer-Home-Verzeichnisse entsprechende Berechtigungen haben

Home-Verzeichnisse dürfen nicht schreibgeschützt sein und müssen von ihren Eigentümern durchsucht werden können. Im Allgemeinen sind andere Benutzer nicht berechtigt, diese Dateien zu ändern oder Dateien zu dem Home-Verzeichnis des Benutzers hinzuzufügen. Um dies sicherzustellen, legen Sie Berechtigungen für das Benutzerverzeichnis fest.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Legen Sie Berechtigungen für ein Benutzerverzeichnis fest.**

   ```
   # chmod 750 /export/home/user_home_directory
   ```

## Aktivieren der IP-Filterfirewall

IP-Filter ist eine hostbasierte Firewall, die zustandsbehaftete Paketfilterung und Übersetzung von Netzwerkdressen (NAT) bereitstellt. Die Paketfilterung bietet allgemeinen Schutz vor netzwerkbasierten Angriffen. Darüber hinaus bietet IP Filter eine zustandslose Paketfilterung und kann Adresspools erstellen und verwalten.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Aktivieren Sie die IP-Filterfirewall.**

```
# svcadm svc:/network/ipfilter:default
```

## Sicherstellen, dass Name-Services nur lokale Dateien verwenden

Das BS verwendet eine Reihe von Datenbanken mit Informationen zu Hosts, `ipnodes`, user (`passwd(4)`, `shadow(4)`, `user_attr(4)`) und `groups`. Daten für diese Elemente stammen aus verschiedenen Quellen. Beispiel: Hostnamen und Hostadressen können in `/etc/hosts`, NIS, LDAP, DNS oder Multicast-DNS gefunden werden. Systeme in eingeschränkten Umgebungen sind sicherer, wenn nur lokale Dateieinträge für diese Elemente verwendet werden.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Konfigurieren Sie Name-Services so, dass nur lokale Dateien verwendet werden.**

```
# svccfg -s name-service/switch setprop config/default = astring: "files"
# svccfg -s name-service/switch setprop config/host = astring: "files"
# svccfg -s name-service/switch setprop config/password = astring: "files"
# svccfg -s name-service/switch setprop config/group = astring: "files"
# svccfg -s name-service/switch:default refresh
```

## Aktivieren von Sendmail- und NTP-Services

Der Sendmail-Service muss ausgeführt werden, sonst wird wichtige Systemmail an `root` nicht zugestellt.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Aktivieren von Sendmail.**

```
# svcadm enable smtp:sendmail
```

3. **Falls erforderlich installieren Sie den NTP-Service.**

   Der `ntp`-Service muss auf allen Systemen installiert werden, auf denen Sicherheit und Compliance gewünscht wird.

```
# pkg install service/network/ntp
```

4. **Konfigurieren Sie den NTP-Service als Client, und aktivieren Sie den Service.**

   Der NTP-(Network Time Protocol-)Daemon muss aktiviert und ordnungsgemäß als Client konfiguriert sein. Die Datei `/etc/inet/ntp.conf` muss mindestens eine Serverdefinition enthalten. Die Datei muss außerdem die Zeile `restrict default ignore` enthalten, um zu verhindern, dass der Client auch als Server fungiert.

```
# vi /etc/inet/ntp.conf
. . .
server server_IP_address iburst
restrict default ignore ...
# svcadm enable ntp
```

# Deaktivieren von GSS (es sei denn, Kerberos wird verwendet)

Der generische Sicherheitsservice (`gss`) verwaltet die Generierung und Validierung der Sicherheitstoken der Generic Security Service Application Program Interface (GSS-API). Der `gssd(1M)`-Daemon arbeitet zwischen dem Kernel-`rpc` und der GSS-API.

---

**Anmerkung -** Kerberos verwendet diesen Service. Deaktivieren Sie den `rpc/gss`-Service, wenn Kerberos nicht konfiguriert ist und nicht verwendet wird.

---

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Aktivieren Sie `rpc/gss`.**

```
# svcadm enable rpc/gss
```

3. **Legen Sie einen Grenzwert für `/tmpfs` fest.**

   Die Größe des `tmpfs`-Dateisystems ist standardmäßig nicht beschränkt. Um Leistungseinbußen zu vermeiden, können Sie die Größe eines jeden `tmpfs`-Einhängevorgangs beschränken. Weitere Informationen finden Sie in den `mount_tmpfs(1M)`- und `vfstab(4)`-Manpages.

```
# pfedit /etc/vfstab
...
```

```
swap - /tmp tmpfs - yes size=sz
```

4. **Starten Sie den Rechenserver neu.**

```
# reboot
```

## Festlegen des Sticky Bits für World-Writable Files

Das Sticky Bit in einem Verzeichnis verhindert, dass Dateien in einem World-Writable-Verzeichnis nur vom Eigentümer der Datei oder der `root`-Rolle gelöscht oder verschoben werden. Dies eignet sich besonders bei Verzeichnissen, die von vielen Benutzer gemeinsam verwendet werden, wie das `/tmp`-Verzeichnis.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Legen Sie das Sticky Bit in `/tmp` und anderen World-Writable-Dateien fest.**

```
# chmod 1777 /tmp
```

## Schützen von Core-Dumps

Core-Dumps können vertrauliche Daten enthalten. Der Schutz kann Dateiberechtigungen und das Loggen von Core-Dumpereignissen umfassen. Weitere Informationen finden Sie in den `coreadm(1m)`- und `chmod(1M)`-Manpages.

Mit dem Befehl `coreadm` können Sie die aktuelle Konfiguration anzeigen und festlegen.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Zeigen Sie die aktuelle Konfiguration an.**

```
# coreadm
global core file pattern: /var/share/cores/core.%f.%p
global core file content: default
```

```
init core file pattern: core
init core file content: default
global core dumps: enabled
per-process core dumps: enabled
global setid core dumps: disabled
per-process setid core dumps: disabled
global core dump logging: enabled
```

3. **Konfigurieren Sie die Core-Dateien, und schützen Sie das Core-Dumpverzeichnis.**

```
# coreadm -g /var/cores/core_%n_%f_%u_%g_%t_%p \
          -e log -e global -e global-setid \
          -d process -d proc-setid
```

4. **Prüfen Sie die Berechtigungen.**

```
# ls -ld /var/share/cores
drwx------ 2 root root 2 Aug 2 2015 cores/
```

5. **Legen Sie die Berechtigungen für das Verzeichnis ordnungsgemäß fest.**

```
# chmod 700 /var/share/cores
```

# ▼ Durchsetzen von nicht ausführbaren Stacks

Die Aktivierung von nicht ausführbaren Stacks ist eine nützliche Technik zur Abwehr bestimmter Arten von Pufferüberlaufangriffen. Wenn Oracle Solaris `nxstack` aktiviert ist, ist das Speichersegment des Prozessstacks als nicht ausführbar markiert. Diese Erweiterung wehrt Angriffe ab, bei denen schädlicher Code eingeschleust und auf dem Stack ausgeführt wird.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Aktivieren Sie `nxstack`.**

```
# sxadm set model=all nxstack
```

3. **Prüfen Sie die Konfiguration.**

```
# sxadm get all nxstack
EXTENSION     PROPERTY     VALUE
```

```
nxstack         model        all
```

# Aktivieren von verschlüsseltem Auslagerungsbereich

Verschlüsseln Sie den Auslagerungsbereich, unabhängig davon, ob es sich um einen ZFS-Datenträger oder ein Raw Device handelt. Die Verschlüsselung stellt sicher, dass vertrauliche Daten, wie Benutzerpasswörter, geschützt werden, wenn das System diese Seiten auf einen Datenträger auslagern müssen.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**
   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Bearbeiten Sie die Datei `/etc/vfstab`, und legen Sie `swap` auf `encrypted` fest.**

```
# pfedit /etc/vfstab
...
/dev/zvol/dsk/rpool/swap - - swap - no encrypted
```

3. **Erstellen und initialisieren Sie einen PKCS #11-Keystore.**

```
# pktool setpin keystore=pkcs11
Enter token passphrase: changeme
Create new passphrase: welcome1
Re-enter new passphrase: welcome1
```

4. **Generieren Sie einen symmetrischen Schlüssel, und speichern Sie ihn in einem PKCS #11-Keystore.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=globalzone-key
```

# Auditing aktivieren

Stellen Sie sicher, dass in Auditlogs alle administrativen Aktionen erfasst werden, einschließlich Befehlen mit Argumenten.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**
   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Konfigurieren Sie die Auditfunktion.**

```
# auditconfig -setpolicy +argv
# auditconfig -setflags lo,ad,ex >& /dev/null
# auditconfig -setpolicy +zonename
```

# ▼ Aktivieren von Datenlinkschutz (Spoofing) in globalen Zonen

Oracle Solaris-Datenlinkschutz verhindert potenzielle Schäden, die durch böswillige Gast-VMs in dem Netzwerk verursacht werden können.

Die Aktivierung der Snoop Proofing-Konfiguration verbessert die Netzwerkperformance, indem der Netzwerkverkehr der virtuellen Umgebung von dem breiteren Verkehr abgetrennt wird, der von dem Hostsystem empfangen oder gesendet wird. Der Linkschutze verhindert Schäden, die durch potenziell böswillige Gast-VMs an dem Netzwerk verursacht werden können. Die Funktion bietet Schutz vor diesen grundlegenden Bedrohungen:

- IP- und MAC-Spoofing
- L2-Frame Spoofing, wie BPDU-(Bridge Protocol Data Unit-)Angriffen

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Legen Sie den Linkschutz fest.**

```
# dladm set-linkprop -p protection=mac-nospoof,restricted,ip-nospoof,dhcp-nospoof net0
```

3. **Bestätigen Sie die Konfiguration.**

```
# dladm show-linkprop -p protection net0
LINK         PROPERTY     PERM     VALUE         EFFECTIVE         DEFAULT     POSSIBLE
net0         protection     rw     mac-nospoof   mac-nospoof        --         mac-nospoof,
                                   restricted    restricted         --         restricted,
                                   ip-nospoof    ip-nospoof         --         ip-nospoof,

                                   dhcp-nospoof  dhcp-nospoof       --         dhcp-nospoof
```

4. **Legen Sie zulässige IPs für den Link fest.**

```
# dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 net0
```

# Aktivieren von Datenlinkschutz (Spoofing) in nicht-globalen Zonen

Oracle Solaris-Datenlinkschutz kann auch individuell für alle nicht-globalen Oracle Solaris-Zonen angewendet werden, die in der SuperCluster-Umgebung bereitgestellt sind.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**
   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Setzen Sie den Datenlinkschutz für eine bestimmte Netzwerkschnittstelle mit dem Befehl `zonecfg(1M)` durch.**
   Stellen Sie sicher, dass die Liste der zulässigen IP-Adressen korrekt und vollständig ist. Die Liste muss alle virtuellen IP-Adressen enthalten, die von Oracle Solaris IPMP, Oracle RAC usw. verwendet werden. Beachten Sie auch, dass Änderungen an der Konfiguration der nicht-globalen SuperCluster-Zone erst wirksam werden, nachdem die nicht-globale Zone neu gestartet wurde.

```
# zonecfg –z zonename
zonecfg:zonename> select anet linkname=network-link-name
zonecfg:zonename:anet> set allowed-address="list_of_allowed_IP_addresses"
zonecfg:zonename:anet>  set link-protection=mac-nospoof,ip-nospoof,restricted
zonecfg:zonename:anet>  set configure-allowed-address=false
zonecfg:zonename:anet>  end
zonecfg:zonename>  commit
zonecfg:zonename>  exit
```

# Erstellen von verschlüsselten ZFS-Datasets

Unternehmen, die einen Schutz *ruhender Daten* benötigen, können in Zonen bereitgestellte Anwendungen und Informationen mit verschlüsselten ZFS-Datasets weiter schützen. Um sicherzustellen, dass jede nicht-globale Zone ohne Administratoreingriff starten kann, sind die verschlüsselten ZFS-Datasets so konfiguriert, dass sie auf ZFS-Verschlüsselungsschlüssel zugreifen, die lokal in der individuellen Datenbank oder Anwendungsdomain gespeichert sind.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**
   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Erstellen von ZFS-Verschlüsselungsschlüsseln**
   Der erforderliche Schlüssel wird am einfachsten mit Befehlen wie den folgenden erstellt:

```
# zfs createzfs_pool_name/zfskeystore
$ chown root:root /zfs_pool_name/zfskeystore
$ chmod 700 /zfs_pool_name/zfskeystore
$ pktool genkey keystore=file keytype=aes keylen=256 \
outkey=/zfs_pool_name/zfskeystore/zone_name.key
```

3. **Erstellen Sie das verschlüsselte ZFS-Dataset.**

```
# zfs create -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zone_name.key \
zfs_pool_name/zone_name
```

4. **Verschlüsseln Sie die u01 und allgemeinen Datasets.**

   Dieselbe Lösung kann zur Verschlüsselung der u01- und allgemeinen Datasets verwendet werden, indem entweder derselbe (SuperCluster-spezifische) Schlüssel oder ein eindeutiger Schlüssel pro Dataset verwendet wird, je nach site-spezifischen Anforderungen und Richtlinien. In diesem Beispiel wird das allgemeine Dataset mit demselben Schlüssel erstellt, der in Schritt 3 erstellt wurde. Beachten Sie, dass zusätzliche ZFS-Konfigurationsparameter, wie Komprimierung, ebenfalls beim Erstellen dieser zusätzlichen Datasets definiert werden können.

```
# zfs create -o compression=on -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zfskeystore/zone_name.key \zfs_pool_name/u01
```

# ▼ (Optional) Festlegen einer Passphrase für den Keystore-Zugriff

Die vorherige Aufgabe,Erstellen von verschlüsselten ZFS-Datasets [74], verwendet eine lokal definierte (Raw-)Datei, die direkt in einem Dateisystem gespeichert werden muss. Eine andere Technik zum Erstellen von Keystores nutzt einen passphrase-geschützten PKCS#11-Keystore, der als *Sun Software PKCS#11 Softtoken* bezeichnet wird. Zur Verwendung dieser Methode, führen Sie die folgende Aufgabe aus:

Der PKCS#11-Keystore muss manuell entsperrt werden, bevor der Schlüssel für ZFS verfügbar gemacht wird. Am Ende bedeutet dies, dass ein manueller administrativer Eingriff erforderlich ist, um das verschlüsselte ZFS-Dataset einzuhängen (und die nicht-globale Zone zu starten, wenn die Zone auch ein verschlüsseltes ZFS-Dataset enthält). Weitere Informationen über andere Strategien zum Erstellen von Keystores finden Sie in der `zfs_encrypt(1M)`-Manpage.

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Legen Sie eine PIN (Passphrase) fest, die für den Zugriff auf den Keystore erforderlich ist.**

   Die Standard-PIN, die mit einem neuen PKCS#11-Keystore verknüpft ist, ist `changeme`. Verwenden Sie diese Passphrase beim ersten Prompt in diesem Beispiel.

```
# pktool setpin keystore=pkcs11
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

3. **Definieren Sie eine `${SOFTTOKEN}`-Umgebungsvariable zur Speicherung des Schlüssels in einem anderen Verzeichnis.**

   Das von dem PKCS#11-Softtoken verwendete Schlüsselmaterial ist standardmäßig im Verzeichnis `/var/user/ ${USERNAME}/pkcs11_softtoken` gespeichert. Die Umgebungsvariable `${SOFTTOKEN}` kann so definiert werden, dass das Schlüsselmaterial in einem anderen Verzeichnis gespeichert wird. Mit dieser Möglichkeit können Sie eine SuperCluster-spezifische Speicherung für dieses durch Passphrase geschützte Schlüsselmaterial aktivieren.

```
# export SOFTTOKEN=/<zfs_pool_name>/zfskeystore
# pktool setpin keystore=pkcs11
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

4. **Erstellen Sie einen Schlüssel.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=zone_name_rpool
Enter PIN for Sun Software PKCS#11 softtoken:
```

5. **Erstellen Sie das verschlüsselte Dataset, indem Sie den im vorherigen Schritt erstellten Schlüssel referenzieren.**

```
# zfs create -o encryption=aes-256-ccm -o keysource=raw,pkcs11:
object=<zone_name>_rpool zfs_pool_name/zone_name
Enter PKCS#11 token PIN for 'zfs_pool_name/zone_name':
```

# ▼ Erstellen unveränderlicher globaler Zonen

Durch den Schutz vor Manipulationen (Tamper-Proofing) durch Unveränderlichkeit können globale und nicht-globale Zonen eine robuste Betriebsumgebung mit hoher Integrität erstellen, in der SuperCluster-Rechenserver ihre eigenen Services ausführen. Aufbauend auf den inhärenten Sicherheitsfunktionen von globalen und nicht-globalen Oracle Solaris-Zonen stellen unveränderliche Zonen sicher, dass (einige oder alle) BS-Verzeichnisse und Dateien nicht (ohne Administratoreingriff) geändert werden können. Die Durchsetzung dieser schreibgeschützten

Vorgehensweise kann nicht autorisierte Änderungen verhindern, stärkere Change Management-Prozeduren fördern und das Einschleusen sowohl von Kernel- als auch von benutzerbasierter Schadsoftware verhindern.

---

**Anmerkung -** Nachdem die unveränderliche Zone konfiguriert wurde, ist die Aktualisierung nur noch durch die Anmeldung über einen vertrauenswürdigen Pfad möglich, oder wenn das System im nicht schreibgeschützten Modus mit `reboot -- -w` neu gestartet wird.

---

Während Sie immer sicherstellen sollten, dass die Anwendungssoftware in einer unveränderlichen Umgebung wie erwartet ausgeführt wird, beachten Sie, dass Oracle Database-Instanzen und Oracle RAC-Cluster auf korrekte Ausführung in den unveränderlichen nicht-globalen Oracle Solaris-Zonen geprüft werden.

1. **Melden Sie sich als Superuser bei der globalen Oracle Solaris-Zone an (dedizierte Domain, Root-Domain oder I/O-Domain).**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Ändern Sie die Konfiguration der globalen Oracle Solaris-Zone, indem Sie die Eigenschaft `file-mac-profile` festlegen.**

   ```
   # zonecfg -z global set file-mac-profile=fixed-configuration
   zonecfg:global> commit
   ```

3. **Starten Sie die globale Oracle Solaris-Zone neu, damit die Änderungen übernommen werden. Melden Sie sich über die ILOM-Konsole bei der Domain an.**

4. **Starten Sie die Konsole für den vertrauenswürdigen Pfad der unveränderlichen globalen Zone.**

   Während die unveränderliche globale Zone konfiguriert wird, muss die Anmeldung bei der Konsole mit einer dieser Break-Sequenzen eingeben werden.

   - **Grafische Konsole** – F1-A
   - **Serielle Konsole** – <Break> oder die alternative Break-Sequenz (CR~ Strg-b)

   ```
   trusted path console login:
   ```

5. **Melden Sie sich bei der globalen Zone der I/O-Domain an, und übernehmen Sie die `root`-Rolle zur Ausführung bestimmter Updates an dem System, danach starten Sie das System neu, damit es wieder in den schreibgeschützten Modus versetzt wird.**

   ```
   # reboot
   ```

# ▼ Konfigurieren unveränderlicher nicht-globaler Zonen

So konfigurieren Sie eine nicht-globale Oracle Solaris-Zone als unveränderlich:

---

**Anmerkung -** Das Oracle Solaris 11-BS unterstützt zusätzlich zu der in dieser Aufgabe identifizierten Konfiguration (feste Konfiguration) weitere Konfigurationen von unveränderlichen Zonen. Weitere Informationen zu diesen Optionen finden Sie in der `zonecfg (1M)`-Manpage. Es wurde jedoch nur die feste Konfigurationsoption als Teil der SuperCluster-Architektur getestet.

---

**Achtung -** Nachdem die Unveränderlichkeit der nicht-globalen Oracle Solaris-Zone aktiviert wurde, können keine Benutzerkonten oder Passwörter für Zonen hinzugefügt, geändert oder gelöscht werden, wie hier beschrieben. Dieses Problem kann jedoch gelöst werden, indem ein LDAP-Verzeichnis so bereitgestellt wird, dass es zonenspezifische Informationen enthält. wie Benutzer, Rollen. Gruppen, Berechtigungsprofile usw.

---

**Achtung -** Die Funktionalität der unveränderlichen Oracle Solaris-Zone ist auf die ZFS-Datasets begrenzt, die standardmäßig in einer nicht-globalen Oracle Solaris-Zone implementiert sind. Zusätzliche Dateisysteme, Pools oder Datasets unterliegen der Richtlinie für unveränderliche Zonen nicht, obwohl der Zugriff auf diese Dateielemente mit anderen Mitteln kontrolliert werden kann, wie der Verwendung von schreibgeschützten Loopback-Einhängungen.

---

1. **Melden Sie sich bei einem der Rechenserver an, und rufen Sie die Hostkonsole als Superuser auf.**
   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Stellen Sie sicher, dass die nicht-globale Oracle Solaris-Zone heruntergefahren ist.**
   Wenn dieser Befehl einen Wert zurückgibt, wird die nicht-globale Oracle Solaris-Zone ausgeführt, und Sie müssen sie herunterfahren.

   ---

   **Anmerkung -** Während die Zone mit dem Befehl `zoneadm(1M)` angehalten werden kann, müssen Sie die Prozedur für das ordnungsgemäße Herunterfahren befolgen, die Ihr Unternehmen festgelegt hat, um eine mögliche Serviceunterbrechung und einen möglichen Datenverlust zu vermeiden.

   ---

   ```
   # zoneadm list | grep -w "zone_name"
   ```

3. **Passen Sie die Konfiguration der nicht-globalen Oracle Solaris-Zone an, indem Sie die Eigenschaft `file-mac-profile` zur Zonenkonfiguration festlegen.**

```
# zonecfg -z zone_name set file-mac-profile=fixed-configuration
```

4. **Falls erforderlich, deaktivieren Sie die Konfiguration der nicht-globalen Zone als unveränderliche Zone.**

```
# zonecfg -z zone_name set file-mac-profile=none
```

5. **Starten Sie die nicht-globale Oracle Solaris-Zone neu, damit die Änderungen übernommen werden.**

```
# zoneadm -z zone_name boot
```

## ▼ Aktivieren des sicheren geprüften Startvorgangs (Oracle ILOM-CLI)

Mit dieser Aufgabe aktivieren Sie den sicheren geprüften Startvorgang über die Oracle ILOM-CLI. Alternativ können Sie die Oracle ILOM-Weboberfläche verwenden. Siehe „Sicherer geprüfter Startvorgang (Oracle ILOM-Weboberfläche)“ [81].

Geprüfter Startvorgang bezieht sich auf die Prüfung von Objektmodulen vor der Ausführung mittels digitalen Signaturen. Oracle Solaris schützt vor dem Laden von Rogue Kernel-Modulen. Der geprüfte Startvorgang erhöht die Sicherheit und Robustheit von Oracle Solaris, indem Kernel-Module vor der Ausführung geprüft werden.

Wenn er aktiviert ist, überprüft dieser Oracle Solaris-Startvorgang die werksseitige Signatur in einem Kernel-Modul, bevor das Modul geladen und ausgeführt wird. Bei dieser Prüfung wird eine versehentliche oder böswillige Änderung eines Moduls ermittelt. Die ergriffene Maßnahme kann konfiguriert werden; wenn sie aktiviert ist, wird entweder eine Warnmeldung ausgegeben und mit dem Laden und Ausführen des Moduls fortgefahren, oder der Vorgang verläuft nicht erfolgreich und das Modul wird nicht geladen und nicht ausgeführt.

1. **Rufen Sie Oracle ILOM auf dem Rechenserver auf.**

   Siehe Anmelden bei einem Rechenserver und Ändern des Standardpasswortes [55].

2. **Aktivieren Sie den geprüften Startvorgang.**

```
-> set /HOST/verified_boot/ module_policy=enforce
Set 'module_policy' to 'enforce'
```

3. **Rufen Sie das von Oracle bereitgestellte Zertifikat auf, und zeigen Sie es an.**

   Eine vorinstallierte geprüfte Startzertifikatsdatei, `/etc/certs/ORCLS11SE`, wird als Teil von Oracle ILOM bereitgestellt.

```
# more /etc/certs/ORCLS11SE
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----
```

4. **Starten Sie das Laden des Zertifikats.**

```
-> set /HOST/verified_boot/user_certs/1 load_uri=console
```

5. **Kopieren Sie den Inhalt der Datei `/etc/certs/ORCLS11SE`, und fügen Sie ihn in die Oracle ILOM-Konsole ein.**

   Speichern und verarbeiten Sie die Informationen mit Strg-z.

   Mit Strg-c beenden Sie den Vorgang und verwerfen die Änderungen.

```
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----^Z
Load successful.
```

6. **Prüfen Sie das Zertifikat.**

```
-> show /HOST/verified_boot/user_certs/1/
/HOST/verified_boot/user_certs/1
Targets:
Properties:
clear_action = (Cannot show property)
issuer = /C=US/O=Oracle Corporation/OU=VeriSign Trust Network/OU=Class 2 Managed PKI
 Individual
Subscriber CA/CN=Object Signing CA
load_uri = (Cannot show property)
subject = /O=Oracle Corporation/OU=Corporate Object Signing/OU=Solaris Signed Execution/
CN=Solaris 11
valid_from = Mar 1 00:00:00 2012 GMT
valid_until = Mar 1 23:59:59 2015 GMT
Commands:
cd
load
reset
show
->
```

7. **Prüfen Sie, ob der OBP-Parameter `use-nvram` auf `False` festgelegt ist.**

   Wenn Sie den geprüften Startvorgang verwenden, muss der OBP-Parameter `use-nvram` auf `False` festgelegt sein. Dadurch wird verhindert, dass OBP geändert wird, um das geprüfte Startverfahren zu deaktivieren. Der Standardwert ist False. Melden Sie sich bei Oracle Solaris an, und geben Sie Folgendes ein:

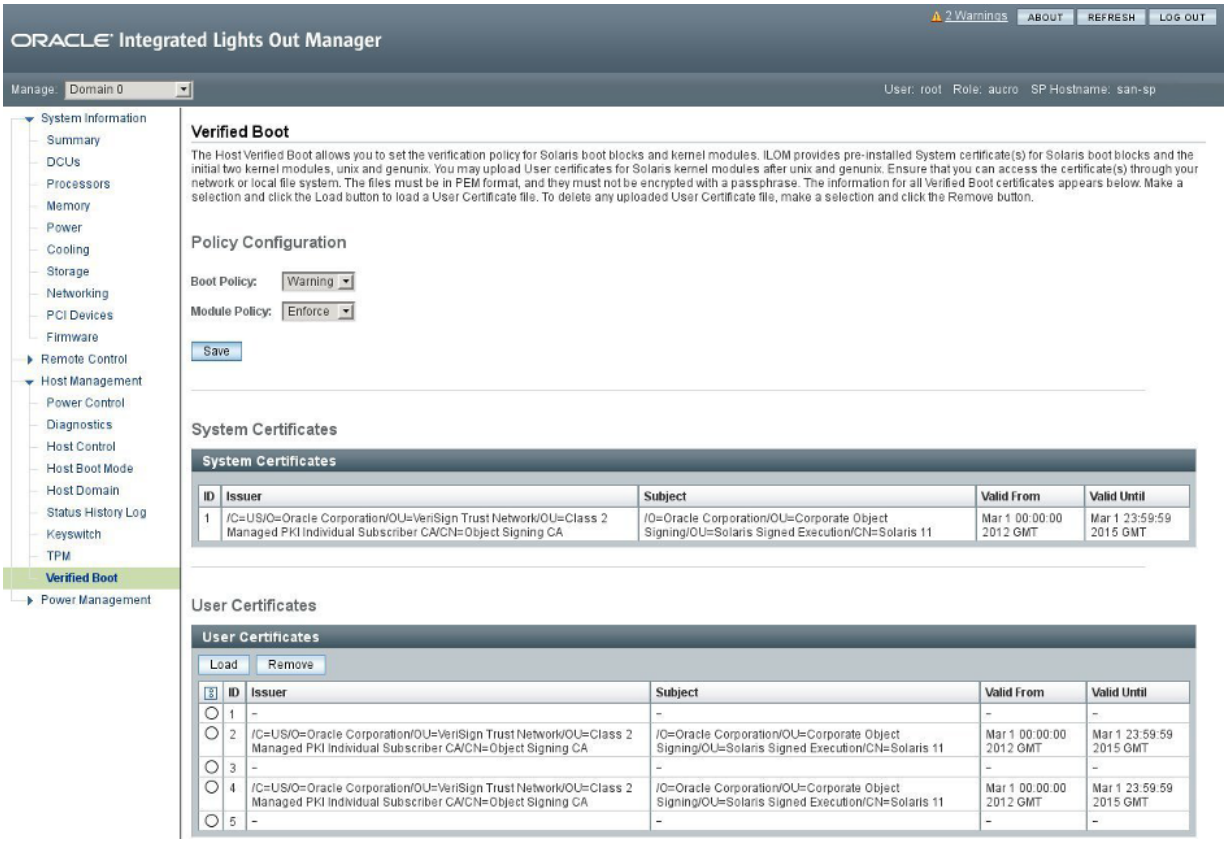
```
$ /usr/sbin/eeprom/eeprom use-nvramrc?

use-nvramrc?=false
```

# Sicherer geprüfter Startvorgang (Oracle ILOM-Weboberfläche)

Die Oracle ILOM-Weboberfläche unterstützt auch die Festlegung der Variablen der Richtlinie für den geprüften Startvorgang und die Verwaltung von Zertifikatsdateien, und stellt dabei dieselbe Funktionalität wie die CLI bereit. Navigieren Sie zu dem Link "Geprüfter Startvorgang" unter dem Navigationsmenü "Hostmanagement".

Beispiel:




# Zusätzliche Ressourcen des Rechenservers

Sicherheitsbestimmungen für Oracle Solaris-BS und Oracle Solaris-Cluster finden Sie in der Dokumentationsbibliothek für Ihre BS-Version. Die Bibliotheken sind unter `http:/docs.oracle.com/en/operating-systems` verfügbar.

Sicherheitsinformationen zu Oracle VM Server for SPARC finden Sie im Sicherheitshandbuch unter `http://docs.oracle.com/cd/E62357_01`.

Sicherheitsinformationen zur Hardware des Rechenservers finden Sie im Sicherheitshandbuch unter `http://docs.oracle.com/cd/E55211_01`.

# Sichern von ZFS Storage Appliance

ZFS Storage Appliance ist eine der SuperCluster-Komponenten; sie unterstützt die Speicherungskonsolidierung in einer Vielzahl von anspruchsvollen Workloads, einschließlich Business Intelligence, Data Warehousing, Virtualisierung, Entwicklung und Test sowie Datenschutz.

ZFS Storage Appliance umfasst zwei redundante ZFS Storage Controller. Sie müssen beide Controller sichern.

In den folgenden Abschnitten werden die Sicherheitsrichtlinien und -funktionen von ZFS Storage Appliance beschrieben:



## ▼ Anmelden bei ZFS Storage Appliance

Zur Ausführung der Sicherheitsaufgaben in diesem Abschnitt melden Sie sich über das Managementnetzwerk bei ZFS Storage Appliance an.

In dieser Aufgabe wird beschrieben, wie Sie sich über die CLI anmelden. Entsprechende Anweisungen für die Anmeldung bei der Oracle ILOM-Weboberfläche finden Sie in *Oracle ZFS Storage Appliance - Administrationshandbuch*. Siehe „Zusätzliche Ressourcen für ZFS Storage Appliance“ [93].

1. **Verwenden Sie in Ihrem Managementnetzwerk SSH zur Verbindung mit ZFS Storage Appliance.**

Wenn Sie keine anderen Benutzer zur Verwaltung der Appliance konfiguriert haben, müssen Sie sich als `root` anmelden.

```
% ssh root@ZFS_Storage_App_IPaddress_or_hostname
Password:
Last login: Mon Oct 13 15:43:05 2015
hostname:>
```

2. **Falls erforderlich rufen Sie die CLI-Hilfe auf.**

   Mit dem Befehl `help` können Sie kontextspezifische Hilfetexte aufrufen. Hilfe zu einem bestimmten Thema können Sie durch Angabe des Themas als Argument für `help` aufrufen. Verfügbare Themen werden durch Vervollständigung des Hilfebefehls mit der TAB-Taste oder durch Eingabe von `help topics` angezeigt.

# ▼ Bestimmen der ZFS Storage Appliance-Softwareversion

Mit dieser Prozedur können Sie die Softwareversion der ZFS Storage Appliance bestimmen.

1. **Melden Sie sich bei der ZFS Storage Appliance an.**

   Siehe Anmelden bei ZFS Storage Appliance [83].

2. **Zeigen Sie die Softwareversion an.**

```
hostname:> configuration version show
[...]
Appliance Product: Sun ZFS Storage 7320
Appliance Type: Sun ZFS Storage 7320
Appliance Version: 2013.06.05.2.10,1-2.1.1.1
[...]
```

In diesem Beispiel ist die Softwareversion von ZFS Storage Appliance `2013.06.05.2.10`.

Um die Version der ZFS Storage Appliance-Software zu aktualisieren, installieren Sie das neueste SuperCluster Quarterly Full Stack Download Patch, das in My Oracle Support unter `https://support.oracle.com` verfügbar ist.

---

**Anmerkung -** Bei SuperCluster können zusätzliche Einschränkungen die Versionen der ZFS Storage Appliance-Software, die verwendet werden können, und die Art der Aktualisierung dieser Versionen begrenzen. Wenden Sie sich in diesen Fällen an Ihren Oracle-Ansprechpartner.

---

# Andern des root-Passwortes von ZFS Storage Appliance

ZFS Storage Appliance selbst ist nicht im Voraus mit einem Standard-root-Passwort konfiguriert. Die anfängliche Konfiguration von ZFS Storage Appliance erfolgt über eine Konsolensession aus dem eingebetteten Oracle ILOM. Das root-Passwort für die Appliance wird während dieser anfänglichen Konfiguration festgelegt.

Wenn Sie die Konsole der Appliance das erste Mal aufrufen, wird ein Fenster zur Shell-Schnittstellenkonfiguration angezeigt. Prüfen Sie die Informationen in dem Fenster, und geben Sie die erforderlichen Werte ein. Das root-Passwort für ZFS Storage Appliance wird während dieses Prozesses festgelegt.

---

**Anmerkung -** Oracle ILOM für die Appliance verfügt über ein Standard-root-Konto und -Passwort mit der Bezeichnung welcome1. Siehe Sichern von Oracle ILOM [37].

---

Nachdem Sie ein root-Konto haben, können Sie das Passwort jederzeit ändern, wie hier beschrieben.

---

**Anmerkung -** Wenn ein Passwort für eine SuperCluster-Komponente geändert wird, die von Oracle Engineered Systems Hardware Manager verwaltet wird (wie das AFS Storage Controller-BS), müssen Sie das Passwort in Oracle Engineered Systems Hardware Manager ebenfalls ändern. Weitere Informationen finden Sie in *Oracle SuperCluster M7 Series - Administrationshandbuch*.

---

1. **Melden Sie sich bei ZFS Storage Appliance an.**

   Siehe Anmelden bei ZFS Storage Appliance [83].

2. **Ändern Sie das root-Passwort.**

   In diesem Beispiel ersetzen Sie *password* durch ein Passwort, das den Bestimmungen des US-Verteidigungsministeriums zur Passwortkomplexität entspricht.

```
hostname:> configuration users select root set initial_password=password initial_password = ************
hostname:configuration users> done
```

Weitere Informationen zur anfänglichen Installation und Konfiguration von ZFS Storage Appliance finden Sie in *Oracle ZFS Storage Appliance - Installationshandbuch*. Siehe „Zusätzliche Ressourcen für ZFS Storage Appliance“ [93].

# Verfügbar gemachte Standardnetzwerkservices (ZFS Storage Appliance)

In dieser Tabelle werden die Standardnetzwerkservices aufgeführt, die von der ZFS Storage Appliance verfügbar gemacht werden.

| Service | Protokoll | Port | Beschreibung |
|---|---|---|---|
| SSH | TCP | 22 | Wird von dem Secure Shell-Service verwendet, um den administrativen Zugriff auf ZFS Storage Appliance mit einer CLI zu aktivieren. |
| PORTMAP | TCP/UDP | 111 | Wird von dem Daemon zum RPC- (Remote-Prozeduraufruf-)Port-Mapping verwendet (auch als `rpcbind` oder `portmap` bezeichnet). Dieser Service ist zur Unterstützung von NFS Version 3 erforderlich. |
| NTP | UDP | 123 | Wird vom integrierten Network Time Protocol-(NTP-) (Nur Client-)Service zur Synchronisierung der lokalen Zeituhr mit einer oder mehreren externen Zeitquellen verwendet. |
| HTTPS (BUI) | TCP | 215 | Wird von dem integrierten HTTPS-Service verwendet, um den administrativen Zugriff auf ZFS Storage Appliance über einen verschlüsselten (SSL/TLS-)Kanal mit einer Browseroberfläche zu aktivieren. |
| Remote-Replikation | TCP | 216 | Wird von dem Remote-Datenreplikationsservice verwendet. Bei der Remote-Datenreplikation werden Projekte und Shares zwischen ZFS Storage Appliance über einen verschlüsselten (SSL-/TLS-)Kanal dupliziert und synchronisiert. |
| NFS | TCP/UDP | 2049<br>4045<br>verschiedene | Wird vom NFS-(Network File System-)Service verwendet. NFS stellt den Service für das Sharing von Netzwerkdateien bereit. Die tatsächliche Anzahl von Ports hängt von der verwendeten Version des NFS-Protokolls ab. NFS Version3 nutzt den (oben aufgeführten) RPC-Port-Mapping Daemon und dynamisch zugewiesene Ports zur Bereitstellung von Einhängung, Status, Quota und zugehörigen Services. NFS Version 4 hingegen nutzt TCP/2049. Der NFS-Sperrservice nutzt TCP/4045. |
| iSCSI / iSNS | TCP | 3260 | Wird von dem iSCSI-Service verwendet, der ein IP-basiertes Speicherungs-Networking-Protokoll zur Verknüpfung von Datenspeicherungseinrichtungen bereitstellt. Die ZFS Storage Appliance kann so konfiguriert werden, dass iSCSI-Geräte (die als LUNs bezeichnet werden) mit Netzwerkclients gemeinsam verwendet werden. |
| Servicetags | TCP | 6481 | Wird vom Oracle ServiceTag-Service verwendet. Dies ist ein Oracle-Erkennungsprotokoll zur Serveridentifizierung und Erleichterung von Serviceanfragen. Dieser Service wird von Produkten wie Oracle Enterprise Manager Ops Center verwendet, um ZFS Storage Appliance-Software zu ermitteln und mit anderen automatischen Oracle-Servicelösungen zu integrieren. |
| NDMP | TCP | 10000 | Wird vom NDMP-(Network Data Management Protocol-)Service verwendet, mit dem die ZFS Storage Appliance an remote koordinierten Backups teilnehmen kann. |

ZFS Storage Appliance unterstützt auch eine Vielzahl von anderen Services, die standardmäßig deaktiviert sind, einschließlich `HTTP`, `FTP`, `SFTP`, `TFTP`, `WebDAV` usw. Zusätzliche Netzwerkports können verfügbar gemacht werden, wenn diese Services nach der Installation aktiviert werden.

# Härten der ZFS Storage Appliance-Sicherheitskonfiguration

In diesen Themen wird beschrieben, wie die Sicherheitskonfiguration von ZFS Storage Appliance gehärtet werden kann:



## ▼ Implementieren der Härtung der Oracle ILOM-Sicherheitskonfiguration

ZFS Storage Appliance umfasst ein eingebettetes Oracle ILOM als Teil des Produkts. Wie bei anderen Oracle ILOM-Implementierungen gibt es sicherheitsrelevante Konfigurationsänderungen, die Sie implementieren können, um die Standardsicherheitskonfiguration des Geräts zu verbessern.

- **Sichern Sie die Oracle ILOM-Oberfläche der ZFS Storage Appliance, indem Sie die Prozeduren in Sichern von Oracle ILOM [37] ausführen.**

## ▼ Deaktivieren nicht erforderlicher Services (ZFS Storage Appliance)

Deaktivieren Sie Services, die zur Unterstützung der Betriebs- und Managementanforderungen der Plattform nicht erforderlich sind.

Standardmäßig verwendet ZFS Storage Appliance eine *Secure-by-Default*-Netzwerkkonfiguration, wenn nicht unbedingt erforderliche Services deaktiviert sind. Je nach

Ihren Sicherheitsrichtlinien und Sicherheitsbestimmungen müssen möglicherweise weitere Services aktiviert oder deaktiviert werden.

1. **Melden Sie sich bei ZFS Storage Appliance an.**

   Siehe Anmelden bei ZFS Storage Appliance [83].

2. **Zeigen Sie die Liste der Services an, die von ZFS Storage Appliance unterstützt werden.**

   ```
   hostname:> configuration services
   ```

3. **Prüfen Sie, ob ein bestimmter Service aktiviert ist.**

   Ersetzen Sie *servicename* durch den Namen eines Service, der in Schritt 2 identifiziert wird.

   ```
   hostname:> configuration services servicename get <status>
   ```

   Ein Service ist aktiviert, wenn der Parameter für den Servicestatus einen Wert `enabled` zurückgibt. Beispiel:

   ```
   hostname:> configuration services iscsi get <status>
   <status> = online
   ```

4. **Deaktivieren Sie einen Service, der nicht mehr benötigt wird.**

   Legen Sie den Servicestatus auf "disable" fest. Beispiel:

   ```
   hostname:> configuration services iscsi disable
   ```

# ▼ Deaktivieren des dynamischen Routings

Die ZFS Storage Appliance ist standardmäßig zur Ausführung des dynamischen Routingprotokolls konfiguriert.

Bevor Sie den dynamischen Routingservice deaktivieren, stellen Sie sicher, dass die ZFS Storage Appliance entweder direkt mit einem Netzwerk verbunden ist, mit dem sie kommunizieren muss, oder stellen Sie sicher, dass sie zur Verwendung des statischen Routings oder einer Standardroute konfiguriert wurde. Dieser Schritt ist erforderlich, um sicherzustellen, dass es zu keinem Konnektivitätsverlust kommt, wenn das dynamische Routing deaktiviert wird.

1. **Melden Sie sich bei der ZFS Storage Appliance an.**

Siehe Anmelden bei ZFS Storage Appliance [83].

2. **Deaktivieren Sie das dynamische Routing**

```
hostname:> configuration services dynrouting disable
```

3. **Um zu bestimmen, ob das dynamische Routing aktiviert ist, geben Sie Folgendes ein:**

```
hostname:> configuration services dynrouting get <status>
```

# ▼ Begrenzen des Remote-root-Zugriffs mit Secure Shell

Standardmäßig ist ZFS Storage Appliance so konfiguriert, dass der administrative Remote-Zugriff auf das root-Konto mit dem Secure Shell-(SSH-)Service zugelassen ist.

Verwenden Sie diese Prozedur, um den Remote-Root-Zugriff mit SSH zu deaktivieren.

Nachdem diese Konfigurationsänderung durchgeführt wurde, kann das root-Konto nicht mehr mit SSH auf das System zugreifen. Das root-Konto kann jedoch mit der HTTPS - Administrationsoberfläche auf dieses System zugreifen.

1. **Melden Sie sich bei ZFS Storage Appliance an.**

   Siehe Anmelden bei ZFS Storage Appliance [83].

2. **Deaktivieren Sie den Remote-root-Zugriff.**

```
hostname:> configuration services ssh set permit_root_login=false
```

3. **Prüfen Sie, ob das root-Konto nicht mehr mit SSH auf das System zugreifen kann.**

```
hostname:> configuration services ssh get permit_root_login
```

4. **Wenn der administrative SSH-Zugriff erforderlich ist, erstellen Sie mindestens ein Nicht-root-Konto.**

   Weitere Informationen finden Sie in dem *Oracle ZFS Storage Appliance - Administrationshandbuch* für das Release, das in der ZFS Storage Appliance ausgeführt wird. Siehe „Zusätzliche Ressourcen für ZFS Storage Appliance“ [93].

# Konfigurieren des Inaktivitätstimeouts für die Administrationsoberfläche (HTTPS)

Mit ZFS Storage Appliance können Administrationssessions getrennt und abgemeldet werden, die während einer vordefinierten Anzahl von Minuten inaktiv waren. Standardmäßig bricht die Browserbenutzeroberfläche (HTTPS) eine Session nach 15 Minuten wegen Timeouts ab.

---

**Anmerkung -** Es gibt keinen entsprechenden Parameter, der ein Inaktivitätstimeout in der SSH-Befehlszeilenschnittstelle der ZFS Storage Appliance durchsetzt.

---

Verwenden Sie diese Prozedur, um den Parameter für das Inaktivitätstimeout auf einen benutzerdefinierten Wert festzulegen.

1. **Melden Sie sich bei ZFS Storage Appliance an.**

   Siehe Anmelden bei ZFS Storage Appliance [83].

2. **Zeigen Sie den aktuellen Parameter für den Inaktivitätstimeout an, der mit der Browseroberfläche verknüpft ist.**

```
hostname:> configuration preferences get session_timeout
session_timeout = 15
```

3. **Konfigurieren Sie den Timeoutparameter.**

   Der Wert `session_timeout` wird in Minuten angegeben (in diesem Beispiel 10 Minuten).

```
hostname:> configuration preferences set session_timeout=10
session_timeout = 10
```

4. **Prüfen Sie den Timeoutparameter, indem Sie Schritt 2 wiederholen.**

# Deaktivieren nicht genehmigter SNMP-Protokolle

Standardmäßig sind SNMPv1 und SNMPv2c in der ZFS Storage Appliance aktiviert. Die ZFS Storage Appliance unterstützt SNMPv1/v2c auf allen unterstützten Versionen des Produkts. Ab Version 2013.1.2 unterstützt ZFS Storage Appliance auch SNMPv3.

**Anmerkung -** Ab Version 3 des SNMP-Protokolls wird das benutzerbasierte Sicherheitsmodell (User-based Security Model (USM)) unterstützt. Diese Funktionalität ersetzt die üblichen SNMP-Communityzeichenfolgen durch tatsächliche Benutzerkonten, die mit bestimmten Berechtigungen, Authentifizierungs- und Datenschutzprotokollen und Passwörtern konfiguriert werden können. Standardmäßig enthält ZFS Storage Appliance keinen Benutzernamen oder kein Passwort für das integrierte (schreibgeschützte) USM-Konto. Aus Sicherheitsgründen konfigurieren Sie die USM-Zugangsdaten und -Protokolle je nach Anforderungen an Deployment, Verwaltung und Überwachung.

Stellen Sie sicher, dass nicht verwendete oder ältere Versionen des SNMP-Protokolls deaktiviert sind, wenn sie nicht erforderlich sind.

1. **Melden Sie sich bei der ZFS Storage Appliance an.**

   Siehe Anmelden bei ZFS Storage Appliance [83].

2. **Bestimmen Sie, welche Version des SNMP-Protokolls von dem Gerät verwendet wird.**

```
hostname:> configuration services snmp get version
version = v2
```

3. **Aktivieren Sie die Verwendung von SNMPv3 (sofern verfügbar).**

   SNMPv1/v2c und SNMPv3 schließen sich gegenseitig aus, wenn Sie also SNMPv3 aktivieren, ist SNMPv1/v2c deaktiviert.

```
hostname:> configuration services snmp set version=v3
version = v3
```

4. **Prüfen Sie die Version von SNMP.**

```
hostname:> configuration services snmp get version
version = v3
```

# ▼ Konfigurieren von SNMP-Communityzeichenfolgen

Führen Sie diese Aufgabe nur aus, wenn die ZFS Storage Appliance zur Verwendung von SNMPv1 oder v2 konfiguriert ist.

Weil SNMP häufig zur Überwachung der Integrität des Geräts verwendet wird, muss die SNMP-Standardcommunityzeichenfolge, die von dem Gerät verwendet wird, in einen vom Kunden definierten Wert geändert werden.

1. **Melden Sie sich bei der ZFS Storage Appliance an.**

   Siehe Anmelden bei ZFS Storage Appliance [83].

2. **Ändern Sie die SNMP-Communityzeichenfolge.**

   Ersetzen Sie in diesem Beispiel *string* durch einen Wert, der den Sicherheitsbestimmungen des US-Verteidigungsministeriums entspricht, was den Aufbau der SNMP-Communityzeichenfolgen betrifft.

```
hostname:> configuration services snmp set community=string
community = value
```

3. **Prüfen Sie die SNMP-Communityzeichenfolge.**

```
hostname:> configuration services snmp get community
```

# ▼ Konfigurieren autorisierter SNMP-Netzwerke

Führen Sie diese Aufgabe nur aus, wenn ZFS Storage Appliance zur Verwendung von SNMPv1 oder v2 konfiguriert ist.

Um die Offenlegung von Systemkonfigurationsinformationen zu minimieren, dürfen SNMP-Abfragen nur von genehmigten Netzwerk- oder Hostquellen akzeptiert werden.

1. **Melden Sie sich bei ZFS Storage Appliance an.**

   Siehe Anmelden bei ZFS Storage Appliance [83].

2. **Konfigurieren Sie den Parameter für das autorisierte SNMP-Netzwerk.**

```
hostname:> configuration services snmp set network=127.0.0.1/8
network = 127.0.0.1/8
```

3. **Prüfen Sie den Wert des Parameters für das autorisierte SNMP-Netzwerk.**

   Wenn Sie den Netzwerkparameter in diesem Beispiel auf `127.0.0.1/8` festlegen, werden alle netzwerkbasierten SNMP-Abfragen blockiert. Der Wert muss nach Bedarf angepasst werden, um genehmigte Hosts und Netzwerke zuzulassen.

Ein Wert von `0.0.0.0/0` lässt Abfragen von jedem Netzwerkverzeichnis zu.

```
hostname:> configuration services snmp get network
network = 127.0.0.1/8
```

## ▼ Begrenzen des Managementnetzwerkzugriffs

Neben diesen Maßnahmen zur Härtung der Sicherheit müssen die Managementschnittstellen, die von ZFS Storage Appliance verfügbar gemacht werden, in einem dedizierten, isolierten Managementnetzwerk bereitgestellt werden. Mit diesem Schritt kann ZFS Storage Appliance vor unautorisiertem oder unbeabsichtigtem administrativem Netzwerkverkehr abgeschirmt werden. Sie müssen den Zugriff auf das Managementnetzwerk streng kontrollieren, indem nur den Administratoren Zugriff erteilt wird, die diese Zugriffsebene benötigen.

Außerdem kann ZFS Storage Appliance so konfiguriert werden, dass der administrative (Management-)Zugriff auf bestimmten Netzwerkschnittstellen aktiviert oder deaktiviert wird. Diese Änderung kann mit dieser Prozedur implementiert werden.

1. **Melden Sie sich bei der ZFS Storage Appliance an.**
   Siehe Anmelden bei ZFS Storage Appliance [83].

2. **Konfigurieren Sie die Managementnetzwerkschnittstellen.**
   In diesem Beispiel ersetzen Sie den Wert *interface* durch den Namen der eigentlichen Netzwerkschnittstelle, für die diese Einstellung angewendet wird.

```
hostname:> configuration net interfaces select interface set admin=false
```

# Zusätzliche Ressourcen für ZFS Storage Appliance

Zusätzliche Sicherheitsrichtlinien für die ZFS Storage Appliance finden Sie in dem Sicherheitshandbuch für das Release, das in ZFS Storage Appliance ausgeführt wird. Siehe Bestimmen der ZFS Storage Appliance-Softwareversion [84].

Diese Handbücher enthalten zusätzliche Informationen zu den Sicherheitsfunktionen, Möglichkeiten und Konfigurationsoptionen des Produkts.

- *Oracle ZFS Storage Appliance - Sicherheitshandbuch* (Release 2013.1.4.0)
  `http://docs.oracle.com//cd/E56047_01`

- *Oracle ZFS Storage Appliance - Sicherheitshandbuch* (Release 2013.1.3.0)

  http://docs.oracle.com/cd/E56021_01
- *Oracle ZFS Storage Appliance - Sicherheitshandbuch* (Release 2013.1.2.0)

  http://docs.oracle.com/cd/E51475_01

# Sichern der Exadata Storage Server

Die Exadata Storage Server (Storage Server) sind der Speicherbaustein von SuperCluster. Jeder Storage Server wird vorinstalliert und integriert als Teil von SuperCluster M7 mit allen erforderlichen Rechen-, Speicher- und Softwarekomponenten geliefert.

---

**Anmerkung -** Sie können Änderungen an der Konfiguration nur mit genehmigten Methoden, Patches oder Updates vornehmen. Eine andere Änderung der Storage Server-Software ist nicht möglich.

---

SuperCluster M7 verfügt über mindestens drei Storage Server. Zusätzliche Storage Server können im SuperCluster-Hauptrack und in optionalen Erweiterungsracks installiert werden. Sie müssen jeden einzelnen Storage Server sichern.

In diesen Themen wird beschrieben, wie die Storage Server gesichert werden:



## ▼ Anmelden bei Storage Server-BS

- **Melden Sie sich im Managementnetzwerk bei einem der Storage Server als `celladmin` an.**

  Standardpasswort wird in „Standardkonten und -passwörter“ [96] beschrieben.

```
# ssh celladmin@Storage_Server_IP_address
```

# Standardkonten und -passwörter

In dieser Tabelle werden die Standardkonten und -passwörter des Storage Servers aufgeführt.

| Kontoname | Typ | Standardpasswort | Beschreibung |
|---|---|---|---|
| `root` | Administrator | `welcome1` | Wird für den Zugriff auf das Storage Server-BS zur Ausführung allgemeiner administrativer Aktionen und zum Update der Storage Server-Software verwendet. |
| `celladmin` | Cell-Administrator | `welcome` | Wird für Setup und Konfiguration des Storage Servers verwendet. Außerdem arbeiten alle Storage-Services auf der Plattform mit diesem Passwort. |
| `cellmonitor` | Überwachen | `welcome` | Wird nur zu Überwachungszwecken verwendet. Dieses Konto nutzt die eingeschränkte Shell, um sicherzustellen, dass die Konfiguration und Objekte, die in dem Storage Server gespeichert sind, aus diesem Konto nicht geändert werden können. |

# ▼ Ändern von Storage Server-Passwörtern

Eine Liste der Standardkonten und -passwörter finden Sie in „Standardkonten und -passwörter“ [96].

---

**Anmerkung -** Wenn ein Passwort für eine SuperCluster-Komponente geändert wird, die von Oracle Engineered Systems Hardware Manager verwaltet wird (wie das Exadata Storage Server-BS), müssen Sie das Passwort in Oracle Engineered Systems Hardware Manager ebenfalls ändern. Weitere Informationen finden Sie in *Oracle SuperCluster M7 Series - Administrationshandbuch*.

---

1. **Melden Sie sich als `celladmin` bei dem Storage Server an.**
   Siehe Anmelden bei Storage Server-BS [95].

2. **Ändern Sie ein Standardpasswort mit einer der folgenden Methoden**

   - **Ändern Sie das Passwort für ein Konto auf dem Server, bei dem Sie angemeldet sind.**

     ```
     # passwd account_name
     ```

   - **Ändern Sie ein Kontopasswort für alle Storage Server.**
     `cell_group` ist eine einfache Textdatei, in der die Hostnamen aller Storage Server (einer auf jeder Zeile) aufgeführt werden.

In diesem Beispiel ersetzen Sie diese Befehlszeilenelemente:

- *new_password* – Ersetzen Sie das Passwort durch das neue Passwort, das mit den Siterichtlinien konform ist.
- *account_name* – Ersetzen Sie den Kontonamen durch den Namen des Oracle Linux-Kontos.

```
# dcli -g cell_group -l root "echo new_password | passwd --stdin account_name"
```

## ▼ Bestimmen der Exadata Storage Server-Softwareversion

1. **Melden Sie sich bei einem der Storage Server an.**

   Siehe Anmelden bei Storage Server-BS [95].

2. **Geben Sie diesen Befehl ein.**

   In diesem Beispiel ist die Storage Server-Softwareversion 12.1.2.1.1.150316.2.

   ```
   # imageinfo -ver
   12.1.2.1.1.150316.2
   ```

   Um die Version der Software zu aktualisieren, installieren Sie das neueste SuperCluster Quarterly Full Stack Download Patch, das in My Oracle Support unter `https://support.oracle.com` verfügbar ist.

   **Anmerkung -** Bei SuperCluster können zusätzliche Einschränkungen die Softwareversionen, die verwendet werden können, und die Art der Aktualisierung dieser Versionen begrenzen. Wenden Sie sich in diesen Fällen an Ihren Oracle-Ansprechpartner.

# Verfügbar gemachte Standardnetzwerke (Storage Server)

| Servicename | Protokoll | Port | Beschreibung |
|---|---|---|---|
| SSH | TCP | 22 | Wird vom Secure Shell-Service verwendet, der in der Storage Server-Software integriert ist, um den administrativen Zugriff auf das System mit einer CLI zu ermöglichen.<br><br>Standardmäßig ist der Secure Shell-Server so konfiguriert, dass er nur auf den Management-(NET 0-) und IB-(BONDIB0-)Netzwerken auf Verbindungsanforderungen antwortet. |

Der Storage Server kommuniziert auch mit Oracle Database-Domains in SuperCluster mit dem RDSv3- (Reliable Datagram Sockets-)Protokoll über RDMA-(Remote Direct Memory Access-)Schnittstellen. Diese Punkt-zu-Punkt-Kommunikation verwendet TCP/IP nicht und ist auf die interne IB-Netzwerkpartition begrenzt, in der sowohl die Oracle Database-Domains in SuperCluster als auch die Storage Server gespeichert sind.

# Härten der Sicherheitskonfiguration des Storage Servers

**Anmerkung -** Der Storage Server umfasst ein eingebettetes Oracle ILOM als Teil des Produkts. Wie bei anderen Oracle ILOM-Implementierungen gibt es sicherheitsrelevante Konfigurationsänderungen, die implementiert werden können, um die Standardsicherheitskonfiguration des Geräts zu verbessern. Weitere Informationen finden Sie in Sichern von Oracle ILOM [37].

In diesen Themen wird beschrieben, wie die Sicherheit der Storage Server gehärtet werden kann:

## Einschränkungen der Sicherheitskonfiguration

Das host_access_control-Utility ist die einzig zulässige und unterstützte Methode zur Implementierung von Änderungen der Sicherheitskonfiguration in Storage Servern. Gemäß Oracle Support-Hinweis 1068804.1 sind Sie nicht berechtigt, manuelle Änderungen an der Konfiguration dieser Geräte vorzunehmen. Bevor Sie dieses Tool verwenden, benötigen Sie außerdem zuerst die explizite Genehmigung von Oracle SuperCluster Support zur Änderung der Sicherheitskonfiguration bei den Storage Servern. Um diese Genehmigung anzufordern, öffnen Sie eine Serviceanfrage bei Oracle Support.

Der host_access_control-Befehl, der ab Exadata-Softwareversion 11.2.3.3.0 verfügbar ist, wird zur Implementierung eines begrenzten Sets von Zugriffs- und Sicherheitskonfigurationseinstellungen verwendet:

- Begrenzen des Remote Root-Zugriffs.
- Begrenzen des Netzwerkzugriffs auf bestimmte Konten.
- Implementieren von Passwortablauf- und Komplexitätsrichtlinien.
- Implementierung von Anmeldewarnungsbannern.
- Definieren von Kontosperr- und Sessiontimeoutrichtlinien.

## ▼ Anzeigen verfügbarer Sicherheitskonfigurationen mit host_access_control

Um festzustellen, welche Funktionen im host_access_control-Utility verfügbar sind, führen Sie diese Schritte aus.

1. **Melden Sie sich bei dem Storage Server-BS an.**

   Siehe Anmelden bei Storage Server-BS [95].

2. **(Optional) Zeigen Sie die host_access_control-Hilfe für weitere Einzelheiten an.**

```
# /opt/oracle.cellos/host_access_control --help
```

# Konfigurieren eines System-Bootloader-Passwortes

Sie können die Storage Server so konfigurieren, dass ein System-Bootloader-Passwort erforderlich ist, wenn ein Administrator versucht, auf den Bootloader-(GRUB-)Editor oder die Befehlsschnittstelle zuzugreifen.

1. **Melden Sie sich als `celladmin` bei dem Storage Server an.**

   Siehe Anmelden bei Storage Server-BS [95].

2. **Konfigurieren Sie ein System-Bootloader-Passwort.**

```
# /opt/oracle.cellos/host_access_control grub-password
New GRUB password: password
Retype new GRUB password: password
[...]
```

3. **Prüfen Sie die Einstellung.**

   Wenn der Befehl einen Wert wie in diesem Beispiel zurückgibt, ist ein Bootloader-Passwort installiert.

```
# grep "^password" /etc/grub.conf
password --md5 $1$Hdner/$Q2VoiZeTJwmNQsFnH9oFy.
```

# Deaktivieren des Zugriffs auf die Oracle ILOM-Systemkonsole

Jeder der Storage Server enthält einen Oracle ILOM, um die Remote-Überwachung und -Verwaltung zu aktivieren. Oracle ILOM kann auch den Remote-Zugriff auf die Systemkonsole des Storage Servers bereitstellen.

Führen Sie diese Prozedur aus, wenn Sie den Zugriff auf den Storage Server über Oracle ILOM deaktivieren möchten.

1. **Melden Sie sich als `celladmin` bei dem Storage Server an.**

   Siehe Anmelden bei Storage Server-BS [95].

2. **Deaktivieren Sie den Zugriff auf die Oracle ILOM-Systemkonsole**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --lock
```

3. **Prüfen Sie die Einstellung.**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --status
```

## Begrenzen des Remote root-Zugriffs mit SSH

Standardmäßig ist der root-Benutzer zum Remote-Zugriff auf jeden der Storage Server berechtigt.

1. **Melden Sie sich als celladmin bei dem Storage Server an.**

   Siehe Anmelden bei Storage Server-BS [95].

2. **Deaktivieren Sie den Remote root-Zugriff über SSH.**

```
# /opt/oracle.cellos/host_access_control rootssh --lock
```

3. **Prüfen Sie die Einstellung.**

```
# /opt/oracle.cellos/host_access_control rootssh --status
```

## Konfigurieren der Systemkontensperre

Standardmäßig sind die Storage Server so konfiguriert, dass Systemkonten nach fünf nicht erfolgreichen Authentifizierungsversuchen hintereinander gesperrt werden.

Führen Sie die folgenden Schritte aus, um diesen Schwellenwert zu ändern:

1. **Melden Sie sich als celladmin bei dem Storage Server an.**

   Siehe Anmelden bei Storage Server-BS [95].

2. **Ändern Sie den Schwellenwert.**

   Zur Konformität mit den Sicherheitsbestimmungen des US-Verteidigungsministeriums geben Sie einen Wert von 3 an. Falls erforderlich ersetzen Sie diesen Wert durch einen Wert, der mit den Richtlinien Ihrer lokalen Site konform ist.

```
# /opt/oracle.cellos/host_access_control pam-auth --deny 3
```

3. **Prüfen Sie die Einstellung.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep deny=
```

## Konfigurieren von Passwortkomplexitätsregeln

Standardmäßig implementieren Storage Server keine signifikanten Einschränkungen für die Komplexität der Passwörter von Systemkonten.

1. **Melden Sie sich als `celladmin` bei dem Storage Server an.**

   Siehe Anmelden bei Storage Server-BS [95].

2. **Definieren Sie eine Richtlinie zur Passwortkomplexität.**

   Syntax:

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc N0,N1,N2,N3,N4
```

   Ersetzen Sie *N0*,*N1*,*N2*,*N3*,*N4* durch eine durch Komma getrennte Gruppe mit fünf Werten. Diese fünf Werte bestimmen kollektiv die eigentliche Komplexitätsrichtlinie für das Systempasswort. Im Folgenden werden die Werte aufgeführt (sie werden auch in der `passwdqc.conf(5)`-Manpage aufgeführt):

   - *N0* – Wird für Passwörter verwendet, die nur aus einer Zeichenklasse bestehen (Ziffern, Kleinbuchstaben, Großbuchstaben und Sonderzeichen). Im Allgemeinen ist dieser Parameter auf `disabled` festgelegt, weil einfache Passwörter nicht sicher sind.
   - *N1* – Wird für Passwörter verwendet, die aus zwei Zeichenklassen bestehen, die die Anforderungen für eine Passphrase nicht erfüllen. Damit diese Regel angewendet wird, muss das Passwort eine Länge von mindestens N1 Zeichen haben.
   - *N2* – Wird für Passwörter verwendet, die aus einer Passphrase bestehen. Damit diese Regel angewendet wird, muss das Passwort eine Länge von mindestens N2 Zeichen haben und den Anforderungen an Passphrases entsprechen.
   - *N3* – Wird für Passwörter verwendet, die aus mindestens drei Zeichenklassen bestehen. Damit diese Regel angewendet wird, muss das Passwort eine Länge von mindestens N3 Zeichen haben.
   - *N4* – Wird für Passwörter verwendet, die aus mindestens vier Zeichenklassen bestehen. Damit diese Regel angewendet wird, muss das Passwort eine Länge von mindestens*N4* Zeichen haben.

Zur Konformität mit den Sicherheitsbestimmungen des US-Verteidigungsministeriums legen Sie die Parameter *N0,N1,N2,N3,N4* auf `disabled,disabled,disabled,disabled,15` fest. Dadurch wird sichergestellt, dass nur Passwörter akzeptiert werden, die aus mindestens vier Zeichenklassen (Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen) bestehen und eine Länge von mindestens 15 Zeichen haben.

---

**Anmerkung -** Großbuchstaben am Anfang des Passwortes und Ziffern am Ende des Passwortes werden bei der Berechnung der Anzahl von Zeichenklassen nicht berücksichtigt.

---

Beispiel: Um eine Passwortrichtlinie festzulegen, die den Sicherheitsbestimmungen des US-Verteidigungsministeriums entspricht, geben Sie Folgendes ein:

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc disabled,disabled,disabled,disabled,15
```

3. **Prüfen Sie den aktuellen Status dieser Einstellung.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep min=
```

## Konfigurieren einer Richtlinie zur Passworthistorie

Standardmäßig definieren Storage Server eine Richtlinie zur Passworthistorie, die verhindert, dass Benutzer ihre letzten zehn (10) Passwörter wieder verwenden.

1. **Melden Sie sich als `celladmin` bei dem Storage Server an.**

   Siehe Anmelden bei Storage Server-BS [95].

2. **Zeigen Sie die aktuelle Einstellung an.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep remember=
```

3. **Ändern Sie die Passworthistorie.**

   Zur Konformität mit den Sicherheitsbestimmungen des US-Verteidigungsministeriums und den PCI-DSS-Bestimmungen, legen Sie die Richtlinie für die Passworthistorie auf `5` fest. Dadurch wird sichergestellt, dass ein Konto keines der fünf vorherigen Passwörter wiederverwenden kann, die dem Konto zugewiesen wurden. Falls erforderlich ersetzen Sie diesen Wert durch einen Wert, der mit den Richtlinien Ihrer lokalen Site konform ist.

```
# /opt/oracle.cellos/host_access_control pam-auth --remember 5
```

4. **Zur Prüfung der Einstellung wiederholen Sie Schritt 2.**

## Konfigurieren der Sperrverzögerung bei einer nicht erfolgreichen Authentifizierung

Standardmäßig implementieren Storage Server eine Richtlinie, bei der ein Systemkonto nach einem einzigen nicht erfolgreichen Authentifizierungsversuch 10 Minuten lang gesperrt wird.

Führen Sie die folgenden Schritte aus, um diesen Schwellenwert zu ändern:

1. **Melden Sie sich als `celladmin` bei dem Storage Server an.**

   Siehe Anmelden bei Storage Server-BS [95].

2. **Zeigen Sie die aktuelle Einstellung an.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep lock_time=
```

3. **Ändern Sie den Schwellenwert.**

   Zur Konformität mit den Sicherheitsbestimmungen des US-Verteidigungsministeriums legen Sie den Wert auf 4 (Sekunden) fest. Falls erforderlich ersetzen Sie diesen Wert durch einen Wert, der mit den Richtlinien Ihrer lokalen Site konform ist.

```
# /opt/oracle.cellos/host_access_control pam-auth --lock 4
```

4. **Zur Prüfung der Einstellung wiederholen Sie Schritt 2.**

## Konfigurieren von Richtlinien zur Kontrolle des Passwortablaufs

Die Storage Server unterstützen eine Vielzahl von Kontrollen des Passwortablaufs, einschließlich Parametern zur Festlegung der Höchstanzahl von Tagen, die ein Passwort verwendet werden kann, der Mindestanzahl von Tagen zwischen Passwortänderungen und der Anzahl von Tagen, die ein Benutzer im Voraus vor dem Ablauf des Passwortes gewarnt wird.

Zur Konformität mit den Sicherheitsbestimmungen des US-Verteidigungsministeriums und den PCI-DSS-Sicherheitsbestimmungen verwenden Sie die Werte des US-Verteidigungsministeriums in dieser Tabelle:

| Richtlinie | Oracle-Standardwert | DOD-Wert |
|---|---|---|
| Maximale Gültigkeitsdauer des Passwortes | 90 Tage | 60 Tage |
| Minimale Gültigkeitsdauer des Passwortes | 1 Tag | 1 Tag |
| Minimale Passwortlänge | 8 Zeichen | 15 Zeichen |
| Warnung wegen Passwortablaufs | 7 Tage | 7 Tage |

Führen Sie die folgenden Schritte aus, um einen dieser Parameter zu ändern.

1. **Melden Sie sich als `celladmin` bei dem Storage Server an.**
   Siehe Anmelden bei Storage Server-BS [95].

2. **Zeigen Sie die aktuellen Einstellungen an.**

```
# /opt/oracle.cellos/host_access_control password-policy --status
```

3. **Konfigurieren Sie diese Richtlinien gemäß den Passwortrichtlinien für Ihre Site.**

   - **Zur Änderung des Parameters für die maximale Passwortgültigkeitsdauer geben Sie Folgendes ein:**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MAX_DAYS 60
```

   - **Zur Änderung des Parameters für die minimale Passwortgültigkeitsdauer geben Sie Folgendes ein:**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_DAYS 1
```

   - **Zur Änderung des Parameters für die Passwortlänge geben Sie Folgendes ein:**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_LEN 15
```

   - **Zur Änderung des Parameters zur Warnung wegen Passwortablaufs geben Sie Folgendes ein:**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_WARN_AGE 7
```

4. **Zur Prüfung der Einstellungen wiederholen Sie Schritt 2.**

# Konfigurieren des Timeouts bei Inaktivität der Administrationsoberfläche (Anmelde-Shell)

Der Storage Server unterstützt die Möglichkeit, administrative Sessions zu beenden, die während mehr als einer vordefinierten Anzahl von Sekunden inaktiv sind.

Führen Sie folgende Schritte aus, um das Inaktivitätstimeout für die Administrationsoberfläche einer Anmelde-Shell des Systemkontos zu definieren.

1. **Melden Sie sich als `celladmin` bei dem Storage Server an.**

   Siehe Anmelden bei Storage Server-BS [95].

2. **Zeigen Sie die aktuelle Einstellung an.**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep Shell
```

3. **Definieren Sie das Inaktivitätstimeout für die Administrationsoberfläche.**

   Zur Konformität mit den Sicherheitsbestimmungen des US-Verteidigungsministeriums und den PCI-DSS-Sicherheitsbestimmungen geben Sie einen Wert von `900` (Sekunden) an. Falls erforderlich ersetzen Sie diesen Wert durch einen Wert, der mit den Richtlinien Ihrer lokalen Site konform ist.

```
# /opt/oracle.cellos/host_access_control idle-timeout --shell 900
```

4. **Zur Prüfung der Einstellung wiederholen Sie Schritt 2.**

# Konfigurieren des Timeouts bei Inaktivität der Administrationsoberfläche (Secure Shell)

Der Storage Server unterstützt die Möglichkeit, administrative SSH-Sessions zu beenden, die während mehr als einer vordefinierten Anzahl von Sekunden inaktiv waren.

Führen Sie folgende Schritte aus, um das Inaktivitätstimeout der Administrationsoberfläche für eine SSH-Session zu definieren.

1. **Melden Sie sich als `celladmin` bei dem Storage Server an.**
   Siehe Anmelden bei Storage Server-BS [95].

2. **Zeigen Sie die aktuelle Einstellung an.**

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --status | grep SSH
   ```

3. **Definieren Sie das Inaktivitätstimeout der Administrationsoberfläche für eine SSH-Session.**
   Zur Konformität mit den Sicherheitsbestimmungen des US-Verteidigungsministeriums geben Sie einen Wert von `900` (Sekunden) an. Falls erforderlich ersetzen Sie diesen Wert durch einen Wert, der mit den Richtlinien der lokalen Site konform ist.

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --client 900
   ```

4. **Zur Prüfung der Einstellung wiederholen Sie Schritt 2.**

# ▼ Konfigurieren eines Anmeldewarnungsbanners (Storage Server)

Der Storage Server unterstützt die Möglichkeit, kundenspezifische Meldungen anzuzeigen, bevor sich ein Benutzer erfolgreich bei dem System authentifiziert.

Führen Sie die folgenden Schritte aus, um ein Anmeldewarnungsbanner vor der Authentifizierung zu definieren.

1. **Melden Sie sich als `celladmin` bei dem Storage Server an.**
   Siehe Anmelden bei Storage Server-BS [95].

2. **Ermitteln Sie die aktuelle Einstellung.**

   ```
   # /opt/oracle.cellos/host_access_control banner --status
   ```

3. **Erstellen Sie eine Textdatei, die die genehmigte Meldung des Anmeldewarnungsbanners enthält.**

4. **Definieren Sie ein Anmeldewarnungsbanner vor der Authentifizierung.**
   Zur Konformität mit den Sicherheitsbestimmungen des US-Verteidigungsministeriums ersetzen Sie *filename* durch den Pfad und Namen einer Datei, die die genehmigte Meldung für das Anmeldewarnungsbanner enthält.

```
# /opt/oracle.cellos/host_access_control banner --file filename
```

5. **Zur Prüfung der Einstellung wiederholen Sie Schritt 2.**

# Begrenzen des Remote-Netzwerkzugriffs

Sie können den eingehenden Remote-Netzwerkzugriff auf die Storage Server begrenzen, indem Sie ein Filterungsregelset implementieren. Sie können den Netzwerkzugriff auch optimieren, indem Sie ein benutzerdefiniertes Regelset definieren.

Führen Sie die folgenden Schritte aus, um den Remote-Zugriff zu begrenzen.



## Isolation des Storage Server-Managementnetzwerks

Der Storage Server wird in einem dedizierten, isolierten Managementnetzwerk bereitgestellt. Auf diese Weise kann der Storage Server vor nicht autorisiertem oder nicht beabsichtigtem Netzwerkverkehr abgeschirmt werden. Der Zugriff auf das Managementnetzwerk muss streng kontrolliert werden, wobei nur die Administratoren Zugriff erhalten, die diese Zugriffsebene benötigen.

## ▼ Begrenzen des Remote-Netzwerkzugriffs

Es gibt verschiedene Möglichkeiten, den Remote-Netzwerkzugriff bei den Storage Servern zu begrenzen. Sie können den eingehenden Netzwerkzugriff auf den Storage Server begrenzen, indem Sie ein Top-Down-Filterungsregelset implementieren, das den Zugriff nach Benutzerkonto und Ursprung definiert. Sie können auch ein benutzerdefiniertes Regelset definieren, mit dem der Zugriff gemäß den Sicherheitsbestimmungen des US-Verteidigungsministeriums und den PCI-DSS-Sicherheitsbestimmungen zugelassen oder abgelehnt wird.

**Achtung -** Gehen Sie bei der Implementierung von nicht standardmäßigen Richtlinien mit Vorsicht vor, um sicherzustellen, dass der Zugriff auf das System nicht unterbrochen wird. Wenn Sie neue individuelle Regeln hinzufügen, werden die Änderungen sofort wirksam.

Führen Sie die folgenden Schritte aus, um ein Regelset zu implementieren.

1. **Melden Sie sich als `celladmin` bei dem Storage Server an.**

   Siehe Anmelden bei Storage Server-BS [95].

2. **Prüfen Sie das aktive Regelset.**

   ```
   # /opt/oracle.cellos/host_access_control access --status
   ```

3. **Exportieren Sie das aktuelle Regelset in eine Datei, und speichern Sie es als Backupkopie.**

   Dieser Befehl exportiert das Regelset in eine ASCII-Textdatei.

   ```
   # /opt/oracle.cellos/host_access_control access-export --file filename
   ```

4. **Konfigurieren Sie das Regelset, indem Sie einen oder mehrere dieser Befehle ausführen, je nach Methode, mit der Sie das Regelset erstellen möchten.**

   - **Zur Implementierung eines offenen Regelsets, das die Einschränkungen für den eingehenden Netzwerkverkehr entfernt, geben Sie Folgendes ein:**

     ```
     # /opt/oracle.cellos/host_access_control access --open
     ```

   - **Zur Implementierung eines geschlossenen Regelsets, das den eingehenden Zugriff nur mit SSH zulässt, geben Sie Folgendes ein:**

     ```
     # /opt/oracle.cellos/host_access_control access --close
     ```

   - **Zur Änderung des vorhandenen Regelsets geben Sie folgendes ein:**

     Exportieren Sie das aktuelle Regelset in eine ASCII-Textdatei.

     ```
     # /opt/oracle.cellos/host_access_control access-export --file filename
     ```

     Verwenden Sie einen Editor, um die Textdatei zur Konfiguration des Regelsets zu konfigurieren.

     Importieren Sie das Regelset aus der Textdatei, und überschreiben Sie dabei das vorhandene Regelset:

```
# /opt/oracle.cellos/host_access_control access-import --file filename
```

- **So fügen Sie spezifische Regeln individuell hinzu:**

  Mit dieser Methode kann der Zugriff basierend auf diesen Parameter zugelassen oder abgelehnt werden:

  - **Benutzername** – Gültige Werte umfassen entweder das Schlüsselwort `all` oder mindestens einen gültigen, lokalen Kontobenutzernamen.
  - **Ursprung** – Gültige Werte umfassen entweder das Schlüsselwort `all` oder einzelne Einträge, die die Quelle des Systemzugriffs beschreiben, einschließlich Konsole, virtuelle Konsole. Oracle ILOM, IP-Adresse, Netzwerkadresse, Hostname oder DNS-Domain.

  In diesem Beispiel wird der Zugriff auf den Storage Server dem Benutzer `celladmin` erteilt, wenn die Verbindung von dem Host `trusted.example.org` oder einem beliebigen Host innerhalb der Domain `.trusted.domain.com` ausgeht.

```
# /opt/oracle.cellos/host_access_control access --add --user celladmin \
--origins trustedhost.example.org,.trusted.domain.com
```

# Zusätzliche Storage Server-Ressourcen

Hierzu wird auf "Exadata Database Machine - Sicherheitshandbuch" unter http://docs.oracle.com/cd/E50790_01/welcome.html verwiesen.

# Sichern der IB- und Ethernet-Switches

Der Oracle Sun Data Center InfiniBand Switch 36, der von SuperCluster verwendet wird, bietet die Netzwerkgrundlage für ein hoch skalierbares, vollständig redundantes High-Performance Backplane über alle internen Komponenten hinweg.

Die IB-Switches verbinden die Rechenserver, Speicherzellen und die ZFS-Storage Appliance. Die IB-Switches umfassen einen eingebetteten Oracle ILOM für erweiterte Management- und Überwachungsfunktionen. Oracle ILOM ermöglicht insbesondere die Überwachung und Kontrolle von Benutzern, Hardware, Services, Protokollen und anderen Konfigurationsparametern.

SuperCluster M7 enthält mindestens zwei IB-Switches, wobei zusätzliche IB-Switches nach Bedarf für größere Konfigurationen installiert werden können. Sie müssen jeden einzelnen IB-Switch sichern.

In den folgenden Themen wird beschrieben, wie die IB-Switches in SuperCluster M7 gesichert werden:



## ▼ Anmelden bei einem IB-Switch

In dieser Aufgabe wird beschrieben, wie Sie sich bei der Oracle ILOM-Oberfläche in dem Switch anmelden, auf der die meisten administrativen Aufgaben ausgeführt werden.

- **Melden Sie sich im Managementnetzwerk bei Oracle ILOM in dem IB-Switch als `ilom-admin` an.**

  Für Standardpasswörter wird auf „Standardkonten und -passwörter (IB-Switch)“ [113] verwiesen.

```
% ssh ilom-admin@IB_Switch_ILOM_IPaddress
->
```

# ▼ Bestimmen der Firmwareversion des IB-Switches

Damit Sie die neuesten Features, Funktionen und Sicherheitserweiterungen nutzen können, stellen Sie sicher, dass der IB-Switch mit der neuesten unterstützten Firmwareversion aktualisiert ist.

1. **Melden Sie sich bei einem IB-Switch als `ilom-admin` an.**

   Siehe Anmelden bei einem IB-Switch [111].

2. **Zeigen Sie die Firmwareversion an.**

   In diesem Beispiel hat die Firmware des IB-Switches die Version `2.1.5-1`.

```
-> version
SP firmware 2.1.5-1
SP firmware build number: 47111
SP firmware date: Sat Aug 24 16:59:14 IST 2013
SP filesystem version: 0.1.22
```

   Um die Version der IB-Switch-Firmware zu aktualisieren, installieren Sie das neueste SuperCluster Quarterly Full Stack Download Patch, das in My Oracle Support unter `https://support.oracle.com` verfügbar ist.

---

**Anmerkung -** Bei SuperCluster M7 können zusätzliche Einschränkungen die Versionen der IB-Switch-Software begrenzen, die verwendet werden kann. Diese Einschränkungen bestimmen auch, wie die Firmware aktualisiert wird. Wenden Sie sich in diesen Fällen an Ihren Oracle-Ansprechpartner.

---

# Standardkonten und -passwörter (IB-Switch)

| Kontoname | Typ | Standardpasswort | Beschreibung |
|---|---|---|---|
| `root` | Administrator | `welcome1` | Wird für den Zugriff auf das BS des IB-Switches verwendet. Dieses Konto wird im Allgemeinen zugunsten von `ilom-admin-`, `ilom-operator-` oder vom Kunden definierten Konten nicht verwendet. |
| `ilom-admin` | Administrator | `ilom-admin` | Wird zur Ausführung von administrativen Funktionen mit der eingebetteten Oracle ILOM-Software, zur Ausführung von Softwareupgrades, zur Konfiguration von Benutzern und Services und zur Ausführung von Diagnose- und Fabric-Managementfunktionen des IB-Switches verwendet. |
| `ilom-operator` | Operator | `ilom-operator` | Wird nur für Oracle ILOM-Überwachungs- und IB-Fabric-Diagnosefunktionen verwendet. |
| `nm2user` | Schreibgeschützt | `changeme` | Dieses Konto hat schreibgeschützte Berechtigungen für die administrative Befehlszeilenschnittstelle des IB-Switches. Dieses Konto wird häufig von Oracle Enterprise Manager zur Unterstützung der Überwachung von Hardware und Software des Switches verwendet. |

## ▼ Ändern der `root-` und `nm2user-`Passwörter

Der IB-Switch verwaltet zwei Systemkonten an zwei Stellen. Die `root-` und `nm2user-`Konten werden von dem zugrundeliegenden BS des Switches konfiguriert und verfügbar gemacht. Das Hinzufügen, Entfernen oder Ändern von Konten wird in dieser Layer nicht unterstützt, Sie müssen die Standardpasswörter jedoch ändern.

Für andere Konten und Passwörter wird auf Ändern von IB-Switch-Passwörtern (Oracle ILOM) [114] verwiesen.

Der IB-Switch kann Passwortkomplexität, Lebensdauer, Historie und andere Regeln nicht definieren oder durchsetzen. Sie müssen sicherstellen, dass die zugewiesenen Passwörter den Sicherheitsbestimmungen des US-Verteidigungsministeriums entsprechen, und dass Prozesse implementiert werden, mit denen sichergestellt wird, dass Passwörter gemäß den Sicherheitsbestimmungen des US-Verteidigungsministeriums aktualisiert werden.

Weitere Informationen zur Verwaltung von IB-Switch-Konten, einschließlich dem Erstellen neuer Konten, dem Zuweisen von Berechtigungen für vorhandene Konten oder dem Entfernen von Konten finden Sie in *Oracle Sun Data Center InfiniBand Switch 36 Hardware - Sicherheitshandbuch* und *Oracle Integrated Lights Out Manager - Ergänzung zu Oracle Sun Data Center InfiniBand Switch 36*. Siehe „Zusätzliche IB-Switch-Ressourcen“ [121].

**Anmerkung -** Wenn ein Passwort für eine SuperCluster-Komponente geändert wird, die von Oracle Engineered Systems Hardware Manager verwaltet wird (wie die IB-Switches), müssen Sie das Passwort in Oracle Engineered Systems Hardware Manager ebenfalls ändern. Weitere Informationen finden Sie in *Oracle SuperCluster M7 Series - Administrationshandbuch*.

1. **Melden Sie sich bei dem IB-Switch als `root` an.**

```
# ssh root@IB_Switch_IP_address
```

Für Standardpasswörter wird auf „Standardkonten und -passwörter (IB-Switch)“ [113] verwiesen.

2. **Ändern Sie das `root`-Passwort.**

```
$ passwd root
```

3. **Ändern Sie das `nm2user`-Passwort.**

```
$ passwd nm2user
```

# ▼ Ändern von IB-Switch-Passwörtern (Oracle ILOM)

Der IB-Switch verwaltet zwei Systemkonten an zwei Stellen. In diesem Abschnitt wird beschrieben, wie Passwörter in der Oracle ILOM-Oberfläche des IB-Switches geändert werden. Für andere Konten und Passwörter wird auf Ändern der `root`- und `nm2user`-Passwörter [113]verwiesen.

Standardkonten und von Kunden definierte Konten des IB-Switches werden über den eingebetteten Oracle ILOM in den IB-Switches verwaltet.

Führen Sie die folgenden Schritte aus, um Konten anzuzeigen und Passwörter zu ändern.

1. **Melden Sie sich bei einem IB-Switch als `ilom-admin` an.**

   Siehe Anmelden bei einem IB-Switch [111].

   Für Standardpasswörter wird auf „Standardkonten und -passwörter (IB-Switch)“ [113] verwiesen.

2. **Zeigen Sie konfigurierte Oracle ILO-Konten in dem IB-Switch an.**

```
-> show /SP/users
```

3. **Ändern Sie das Passwort für das `ilom-admin`-Konto.**

```
-> set /SP/users/ilom-admin password=password
```

# Netzwerkisolation bei IB-Switch

Die Managementschnittstelle des IB-Switches wird in einem dedizierten, isolierten Managementnetzwerk bereitgestellt. Dadurch wird der IB-Switch vor nicht autorisiertem oder unbeabsichtigtem Netzwerkverkehr abgeschirmt.

Der Zugriff auf dieses Managementnetzwerk muss streng kontrolliert werden, wobei nur die Administratoren Zugriff erhalten, die diese Zugriffsebene benötigen.

# Verfügbar gemachte Standardnetzwerkservices (IB-Switches)

| Servicename | Protokoll | Port | Beschreibung |
|---|---|---|---|
| SSH | TCP | 22 | Wird von dem integrierten Secure Shell-Service verwendet, um den administrativen Zugriff auf den IB-Switch mit einer CLI zu aktivieren. |
| HTTP (BUI) | TCP | 80 | Wird von dem integrierten HTTP-Service verwendet, um den administrativen Zugriff auf den IB-Switch mit einer Browseroberfläche zu aktivieren. Während TCP/80 im Allgemeinen für den Klartextzugriff verwendet wird, leitet der IB-Switch standardmäßig eingehende Anforderungen automatisch an die sichere Version dieses Service um, die unter TCP/443 ausgeführt wird. |
| NTP | UDP | 123 | Wird vom integrierten Network Time Protocol-(NTP-) (Nur Client-)Service zur Synchronisierung der lokalen Zeituhr mit einer oder mehreren externen Zeitquellen verwendet. |
| SNMP | UDP | 161 | Wird von dem integrierten SNMP-Service verwendet, um eine Managementoberfläche zur Überwachung der Integrität des IB-Switches und zur Überwachung empfangener Trap-Benachrichtigungen bereitzustellen. |
| HTTPS (BUI) | TCP | 443 | Wird von dem integrierten HTTPS-Service verwendet, um den administrativen Zugriff auf den IB-Switch über einen verschlüsselten (SSL/TLS-)Kanal mit einer Browseroberfläche zu aktivieren. |
| IPMI | TCP | 623 | Wird von dem integrierten IPMI-(Intelligence Platform Management Interface-)Service verwendet, um eine Rechnerschnittstelle für verschiedene |

| Servicename | Protokoll | Port | Beschreibung |
|---|---|---|---|
| | | | Überwachungs- und Managementfunktionen bereitzustellen. Deaktivieren Sie diesen Service nicht, weil er von Oracle Enterprise Manager Ops Center zur Erfassung von Hardwarebestandsdaten, Field Replaceable Unit-Beschreibungen, Hardwaresensorinformationen und Informationen zum Hardwarekomponentenstatus verwendet wird. |
| ServiceTag | TCP | 6481 | Wird vom Oracle ServiceTag-Service verwendet. Dies ist ein Oracle-Erkennungsprotokoll zur Serveridentifizierung und Erleichterung von Serviceanfragen. Dieser Service wird von Produkten wie Oracle Enterprise Manager Ops Center verwendet, um IB-Switch-Software zu ermitteln und mit anderen automatischen Oracle-Servicelösungen zu integrieren. |

# Härten der IB-Switch-Konfiguration

In diesen Themen wird beschrieben, wie der IB-Switch über verschiedene Konfigurationseinstellungen gesichert wird.



## ▼ Deaktivieren nicht erforderlicher Services (IB-Switch)

Deaktivieren Sie Services, die zur Unterstützung der Betriebs- und Managementanforderungen der Plattform nicht erforderlich sind. Standardmäßig nutzt der IB-Switch eine Secure-by-Default-Netzwerkkonfiguration, bei der nicht wesentliche Services bereits deaktiviert sind. Je nach Sicherheitsrichtlinien und Sicherheitsbestimmungen des Kunden müssen möglicherweise weitere Services deaktiviert werden.

1. **Melden Sie sich bei einem IB-Switch als `ilom-admin` an.**

   Siehe Anmelden bei einem IB-Switch [111].

2. **Bestimmen Sie die Liste der Services, die von dem IB-Switch unterstützt werden.**

```
-> show /SP/services
```

3. **Prüfen Sie, ob ein bestimmter Service aktiviert ist.**

   Ersetzen Sie *servicename* durch den Namen eines Service aus Schritt 2.

   ```
   -> show /SP/services/servicename servicestate
   ```

   Während die meisten Services den Parameter `servicestate` zur Aufzeichnung, ob der Service aktiviert oder deaktiviert ist, erkennen und verwenden, gibt es einige wenige Services, wie `servicetag`, `ssh`, `sso` und `wsman`, die einen Parameter namens `state` verwenden. Ungeachtet des tatsächlich verwendeten Parameters ist ein Service aktiviert, wenn der Parameter für den Servicestatus einen Wert `enabled` zurückgibt, wie in diesen Beispielen dargestellt:

   ```
   -> show /SP/services/https servicestate
   /SP/services/https
   Properties:
   servicestate = enabled
   ```

   ```
   -> show /SP/services/ssh state
   /SP/services/ssh
   Properties:
   state = enabled
   ```

4. **Um einen Service zu deaktivieren, der nicht mehr erforderlich ist, legen Sie den Servicestatus auf `disabled` fest.**

   ```
   -> set /SP/services/http servicestate=disabled
   ```

5. **Prüfen Sie, ob einer dieser Services deaktiviert werden muss.**

   Je nach den verwendeten Tools und Methoden können die HTTP- und HTTPS-Services deaktiviert werden, wenn sie nicht erforderlich sind oder nicht verwendet werden. Geben Sie Folgendes ein:

   ```
   -> set /SP/services/http servicestate=disabled
   -> set /SP/services/http secureredirect=disabled
   -> set /SP/services/https servicestate=disabled
   ```

   - Browseradministrationsoberfläche (HTTP, HTTPS):
     - -> **set /SP/services/http servicestate=disabled**
     - -> **set /SP/services/http secureredirect=disabled**
     - -> **set /SP/services/https servicestate=disabled**

# Konfigurieren der HTTP-Umleitung zu HTTPS (IB-Switch)

Standardmäßig ist der IB-Switch so konfiguriert, dass eingehende HTTP-Anforderungen an den HTTPS-Service umgeleitet werden, um sicherzustellen, dass die gesamte browserbasierte Kommunikation zwischen dem Switch und dem Administrator verschlüsselt ist.

1. **Melden Sie sich bei einem IB-Switch als `ilom-admin` an.**
   Siehe Anmelden bei einem IB-Switch [111].

2. **Prüfen Sie, ob die sichere Umleitung aktiviert ist.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **Wenn der Standardwert geändert wurde, können Sie die sichere Umleitung aktivieren.**

```
-> set /SP/services/http secureredirect=enabled
```

# Deaktivieren nicht genehmigter SNMP-Protokolle (IB-Switch)

Standardmäßig sind SNMPv1, SNMPv2c und SNMPv3 alle für den SNMP-Service aktiviert, der für Überwachung und Verwaltung des IB-Switches verwendet wird. Stellen Sie sicher, dass ältere Versionen des SNMP-Protokolls deaktiviert bleiben, es sei denn, sie müssen aktiviert werden.

---

**Anmerkung -** Ab Version 3 des SNMP-Protokolls wird das benutzerbasierte Sicherheitsmodell (User-based Security Model (USM)) unterstützt. Diese Funktionalität ersetzt die üblichen SNMP-Communityzeichenfolgen durch tatsächliche Benutzerkonten, die mit bestimmten Berechtigungen, Authentifizierungs- und Datenschutzprotokollen und Passwörtern konfiguriert werden können. Standardmäßig umfasst der IB-Switch keine USM-Konten. Konfigurieren Sie SNMPv3 USM-Konten entsprechend Ihren Deployment-, Management- und Überwachungsanforderungen.

---

1. **Melden Sie sich bei einem IB-Switch als `ilom-admin` an.**

Siehe Anmelden bei einem IB-Switch [111].

2. **Bestimmen Sie den Status jedes der SNMP-Protokolle.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = enabled
v2c = enabled
v3 = enabled
```

3. **Falls erforderlich deaktivieren Sie SNMPv1 und SNMPv2c.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

# Konfigurieren von SNMP-Communityzeichenfolgen (IB-Switch)

Diese Aufgabe ist nur anwendbar, wenn SNMP v1 oder SNMPv2c zur Verwendung aktiviert und konfiguriert ist.

Weil SNMP häufig zur Überwachung der Integrität des Geräts verwendet wird, müssen die SNMP-Standardcommunityzeichenfolgen, die von dem Gerät verwendet werden, durch vom Kunden definierte Werte ersetzt werden.

1. **Melden Sie sich bei einem IB-Switch als `ilom-admin` an.**

   Siehe Anmelden bei einem IB-Switch [111].

2. **Erstellen Sie eine neue SNMP-Communityzeichenfolge.**

   In diesem Beispiel ersetzen Sie die folgenden Elemente in der Befehlszeile:

   - *string* – Ersetzen Sie diese Zeichenfolge durch einen vom Kunden definierten Wert, der den Sicherheitsbestimmungen des US-Verteidigungsministeriums entspricht, was den Aufbau der SNMP-Communityzeichenfolgen betrifft.
   - *access* – Ersetzen Sie diesen Wert durch `ro` oder `rw`, je nachdem, ob es sich um eine schreibgeschützte oder nicht schreibgeschützte Zugriffszeichenfolge handelt.

```
-> create /SP/services/snmp/communities/string permission=access
```

   Nachdem neue Communityzeichenfolgen erstellt wurden, müssen die Standardcommunityzeichenfolgen entfernt werden.

3. **Entfernen Sie die SNMP-Standardcommunityzeichenfolgen.**

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

4. **Prüfen Sie die SNMP-Communityzeichenfolgen.**

```
-> show /SP/services/snmp/communities
```

# ▼ Ersetzen von selbstsignierten Standardzertifikaten (IB-Switch)

Die IB-Switches verwenden selbstsignierte Zertifikate, um die Out-of-the-Box-Verwendungen des HTTPS-Protokolls zu aktivieren. Als Best Practice ersetzen Sie selbstsignierte Zertifikate durch Zertifikate, die zur Verwendung in Ihrer Umgebung genehmigt und von einer anerkannten Certificate Authority signiert sind.

Der IB-Switch unterstützt eine Vielzahl von Methoden, die für den Zugriff auf das SSL/TLS-Zertifikat und den Private Key verwendet werden können, einschließlich HTTPS, HTTP, SCP, FTP, TFTP und dem Einfügen von Informationen direkt in eine Webbrowseroberfläche. Weitere Informationen finden Sie in dem *Oracle Integrated Lights Out Manager - Ergänzung zu Oracle Sun Data Center InfiniBand Switch 36-Dokument*. Siehe „Zusätzliche IB-Switch-Ressourcen“ [121].

1. **Melden Sie sich bei einem IB-Switch als `ilom-admin` an.**

   Siehe Anmelden bei einem IB-Switch [111].

2. **Prüfen Sie, ob der IB-Switch ein selbstsigniertes Standardzertifikat verwendet.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

3. **Installieren Sie das Zertifikat Ihres Unternehmens.**

```
-> load -source URI /SP/services/https/ssl/custom_cert
-> load -source URI /SP/services/https/ssl/custom_key
```

## ▼ Konfigurieren von Timeouts für administrative CLI-Sessions (IB-Switch)

Die IB-Switches unterstützen die Trennung und Abmeldung von administrativen CLI-Sessions, die während mehr als einer vordefinierten Anzahl von Minuten inaktiv waren.

Standardmäßig wird die CLI nach 15 Minuten wegen Timeouts abgebrochen.

1. **Melden Sie sich bei einem IB-Switch als `ilom-admin` an.**

   Siehe Anmelden bei einem IB-Switch [111].

2. **Prüfen Sie den Parameter für den Inaktivitätstimeout der CLI.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **Legen Sie den Parameter für den Inaktivitätstimeout fest.**

   Ersetzen Sie *n* durch einen Wert in Minuten.

```
-> set /SP/cli timeout=n
```

# Zusätzliche IB-Switch-Ressourcen

Weitere Informationen zu IB-Switch-Administrations- und Sicherheitsprozeduren finden Sie in der Sun Datacenter InfiniBand Switch 36-Dokumentationsbibliothek unter http://docs.oracle.com/cd/E36265_01.

# ▼ Ändern des Ethernet-Switch-Passwortes

**Anmerkung -** Wenn ein Passwort für eine SuperCluster-Komponente geändert wird, die von Oracle Engineered Systems Hardware Manager verwaltet wird (wie die Ethernet-Switches), müssen Sie das Passwort in Oracle Engineered Systems Hardware Manager ebenfalls ändern. Weitere Informationen finden Sie in *Oracle SuperCluster M7 Series - Administrationshandbuch*.

1. **Schließen Sie ein serielles Kabel von der Konsole des Ethernet-Switch an einem Laptop oder einem ähnlichen Gerät an.**

   Die Standardgeschwindigkeit des seriellen Ports beträgt 9600 Baud, 8 Bit, keine Parität, 1 Stoppbit und kein Handshake.

```
sscsw-adm0 con0 is now available
Press RETURN to get started.
```

2. **Versetzen Sie den Switch in den Aktivierungsmodus.**

```
sscsw-adm0> enable
```

3. **Legen Sie das Passwort fest:**

```
sscsw-adm0# configure terminal
Enter configuration commands,one per line.End with CNTL/Z.
sscsw-adm0(config)# enable password *******
sscsw-adm0(config)# enable secret *******
sscsw-adm0(config)# end
sscsw-adm0# write memory
*Apr 24 14:25:05.893:%SYS-5-CONFIG_I:Configured from console by
console
Building configuration...
Compressed configuration from 2502 bytes to 1085 bytes [OK ]
```

4. **Speichern Sie die Konfiguration.**

```
sscsw-adm0# copy running-config startup-config
```

5. **Beenden Sie die Session.**

```
sscsw-adm0# exit
```

6. **Trennen Sie den Laptop von dem Ethernet-Switch.**

# Auditing auf Compliance

Mit dem Oracle Solaris Complianceutility können Sie die Compliance eines Systems anhand einer bestimmten Benchmark bewerten und melden.

Über den Oracle Solaris `compliance`-Befehl werden die Anforderungen einer Benchmark dem Code, der Datei oder der Befehlsausgabe zugeordnet, mit dem bzw. der die Compliance mit einer bestimmten Anforderung überprüft wird. Oracle SuperCluster unterstützt aktuell zwei Benchmarkprofile für die Sicherheitscompliance:

- **Empfohlen** – Ein Profil basierend auf der Center of Internet Security-Benchmark.
- **PCI-DSS** – Ein Profil, das die Anforderungen der Payment Card Industry Data Security Standard-(PCI DSS-)Compliance prüft.

Diese Profilingtools ordnen Sicherheitskontrollen den Complianceanforderungen zu, und die daraufhin erstellten Complianceberichte können die Zeit für das Auditing wesentlich reduzieren. Außerdem stellt die Compliancefunktion Richtlinien bereit, die die Begründung für jede Sicherheitsprüfung und Schritte zur Behebung von bei der Prüfung ermittelten Fehlern enthalten. Leitfäden können auch zu Schulungszwecken und als Richtlinien für zukünftige Tests dienen. Leitfäden für die einzelnen Sicherheitsprofile werden standardmäßig bei der Installation erstellt. Der SuperCluster Solaris-Administrator kann eine Benchmark hinzufügen oder ändern und einen neuen Leitfaden erstellen.

In den folgenden Themen wird beschrieben, wie Complianceberichte ausgeführt werden; außerdem wird die FIPS-140-Compliance beschrieben:



## ▼ Generieren einer Compliancebewertung

Zur Ausführung dieser Aufgabe benötigen Sie das Berechtigungsprofil "Softwareinstallation", um dem System Packages hinzuzufügen. Zur Ausführung der meisten Compliancebefehle benötigen Administratorberechtigungen.

1. **Installieren Sie das Compliance-Package.**

```
# pkg install compliance
```

Diese Meldung gibt an, dass das Package installiert wurde:

```
No updates necessary for this image.
```

Weitere Informationen finden Sie in der Manpage`pkg(1)`.

---

**Anmerkung -** Installieren Sie das Package in jeder Zone, in der Sie Compliancetests ausführen wollen.

---

2. **Listen Sie verfügbare Benchmarks, Profile und eventuelle frühere Bewertungen auf.**

In diesem Beispiel gibt es zwei Benchmarks.

- **`pci-dss`** – Umfasst ein Profil namens `Solaris_PCI-DSS`
- **`solaris`** – Umfasst zwei Profile namens `Baseline` und `Recommended`

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
No assessments available
```

3. **Generieren Sie eine Compliancebewertung.**

Führen Sie den Befehl `compliance` mit folgender Syntax aus:

`compliance assess -b` *benchmark* `-p` *profile*

| | |
|---|---|
| `-b` | Gibt eine bestimmte Benchmark an. Wenn keine Angabe gemacht wird, wird standardmäßig der Wert `solaris` verwendet. |
| `-S` | Gibt das Profil an. Bei dem Profilnamen muss die Groß-/Kleinschreibung beachtet werden. Wenn keine Angabe gemacht wird, wird standardmäßig das erste Profil verwendet. |

Beispiele:

- Verwenden des `Recommended`-Profils.

```
# compliance assess -b solaris -p Recommended
```

Der Befehl erstellt ein Verzeichnis in `/var/share/compliance/assessments`, das die Bewertung in drei Dateien enthält: einer Logdatei, einer XML-Datei und einer HTML-Datei.

- Verwenden des PCI-DSS-Profils:

```
# compliance assess -b pci-dss
```

**Anmerkung -** Die `pci-dss`-Benchmark verfügt nur über ein Profil, sodass die Profiloption (`-p`) auf der Befehlszeile nicht angegeben werden muss.

4. **Prüfen Sie, ob Compliancedateien erstellt wurden.**

```
# cd /var/share/compliance/assessments/filename_timestamp
# ls
recommended.html
recommended.txt
recommended.xml
```

**Anmerkung -** Wenn Sie denselben `compliance`-Befehl nochmals ausführen, werden die Dateien nicht ersetzt. Sie müssen die Dateien entfernen, bevor Sie ein Bewertungsverzeichnis erneut verwenden können.

5. **(Optional) Erstellen Sie einen benutzerdefinierten Bericht.**

Sie können benutzerdefinierte Berichte wiederholt ausführen. Sie können die Bewertung jedoch nur einmal im ursprünglichen Verzeichnis ausführen.
In diesem Beispiel wird die Option `-s` verwendet, um die Ergebnistypen zu wählen, die im dem Bericht angezeigt werden sollen.
Standardmäßig werden alle Ergebnistypen in dem Bericht angezeigt, mit Ausnahme von `notselected` oder `notapplicable`. Die Ergebnistypen werden als durch Komma getrennte Liste angegeben, die zusätzlich zu dem Standardwert angezeigt werden soll. Einzelne Ergebnistypen können unterdrückt werden, indem ihnen ein `-` vorangestellt wird, wenn die Liste jedoch mit einem `=` beginnt, wird genau angegeben, welche Ergebnistypen einbezogen werden sollen. Ergebnistypen sind: `pass`, `fixed`, `notchecked`, `notapplicable`, `notselected`, `informational`, `unknown`, `error` oder `fail`.

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/filename_timestamp/report_A.html
```

Mit diesem Befehl wird ein Bericht erstellt, der nicht erfolgreiche und nicht gewählte Objekte im HTML-Format enthält. Der Bericht wird anhand der aktuellsten Bewertung ausgeführt.

6. **Zeigen Sie den vollständigen Bericht an.**

Sie können die Logdatei in einem Texteditor, die HTML-Datei in einem Browser oder die XML-Datei in einem XML-Viewer anzeigen. Beispiel: Um den benutzerdefinierten HTML-Bericht aus dem vorigen Schritt anzuzeigen, geben Sie folgenden Browsereintrag ein:

```
file:///var/share/compliance/assessments/filename_timestamp/report_A.html
```

7. **Beheben Sie alle Fehler, die Ihre Sicherheitsrichtlinie für eine erfolgreiche Bewertung erfordert.**

Wenn die Korrekturmaßnahme einen Neustart des Systems umfasst, starten Sie das System vor der erneuten Ausführung der Bewertung neu.

8. **Wiederholen Sie die Bewertung, bis keine Fehler mehr vorhanden sind.**

## ▼ (Optional) Ausführen von Complianceberichten mit einem `cron`-Job

- **Verwenden Sie als Superuser den Befehl `crontab -e`, um den entsprechenden Eintrag zu der Datei `crontab` hinzuzufügen.**

  Diese Liste enthält Beispiele für `crontab`-Einträge:

  - Führt tägliche Compliancebewertungen um 02:30 Uhr aus.

    ```
    30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
    ```

  - Führt wöchentliche Compliancebewertungen Sonntags um 01:15 Uhr aus

    ```
    15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
    ```

  - Führt monatliche Bewertungen am ersten des Monats um 04:00 Uhr aus.

    ```
    0 4 1 * * /usr/bin/compliance assess -b pci-dss
    ```

  - Führt monatliche Bewertungen am ersten Montag des Monats um 03:45 Uhr aus.

    ```
    45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
    ```

# FIPS-140-2 Level 1-Compliance

Die in SuperCluster gehosteten kryptografischen Anwendungen beruhen auf der Cryptographic Framework-Funktion von Oracle Solaris, die auf FIPS 140-2 Level 1-Compliance validiert wird. Oracle Solaris Cryptographic Framework ist der zentrale kryptografische Speicher für Oracle Solaris. Er stellt zwei FIPS 140–geprüfte Module bereit, die die Userspace- und Kernel-Level-Prozesse unterstützen. Diese Bibliotheksmodule stellen Funktionen zu Verschlüsselung, Entschlüsselung, Hashing, Signaturgenerierung und -prüfung, Zertifikatsgenerierung und -prüfung sowie Nachrichtenauthentifizierung bereit. Anwendungen auf Benutzerebene, die diese Module aufrufen, werden im FIPS-140-Modus ausgeführt.

Neben Oracle Solaris Cryptographic Framework wird das OpenSSL-Objektmodul, das mit Oracle Solaris gebündelt ist, auf FIPS 140-2 Level 1-Compliance validiert, die die Kryptografie für Anwendungen basierend auf den Secure Shell- und TLS-Protokollen unterstützt. Der Cloud-Serviceprovider kann wählen, ob Mandantenhosts mit FIPS 140–konformen Modi

aktiviert werden sollen. Bei der Ausführung in FIPS 140–konformen Modi setzen Oracle Solaris und OpenSSL, die FIPS 140-2-Provider sind, die Verwendung von FIPS 140–validierten kryptografischen Algorithmen durch.

Hierzu wird auch auf (Falls erforderlich) Aktivieren eines FIPS-140-konformen Vorgangs (Oracle ILOM) [39] verwiesen.

In dieser Tabelle werden FIPS-genehmigte Algorithmen aufgeführt, die von Oracle Solaris in SuperCluster M7 unterstützt werden.

| Schlüssel oder CSP | Zertifikatsnummer | |
|---|---|---|
| | **v1.0** | **v1.1** |
| **Symmetrischer Schlüssel** | | |
| AES: ECB-, CBC-, CFB-128-, CCM-, GMAC-, GCM- und CTR-Modi für 128-, 192- und 256-Bit-Schlüsselgrößen | #2311 | #2574 |
| AES: XTS-Modus für 256- und 512-Bit-Schlüsselgrößen | #2311 | #2574 |
| TripleDES: CBC- und ECB-Modus für Schlüsselerstellungsoption 1 | #1458 | #1560 |
| **Asymmetrischer Schlüssel** | | |
| RSA PKCS#1.5-Signaturgenerierung/-prüfung: 1024-, 2048-Bit (mit SHA-1, SHA-256, SHA-384, SHA-512) | #1194 | #1321 |
| ECDSA-Signaturgenerierung/-prüfung: P-192, -224, -256, -384, -521; K-163, -233, -283, -409, -571; B-163, -233, -283, -409, -571 | #376 | #446 |
| **Secure Hashing Standard (SHS)** | | |
| SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | #1425 | #1596 |
| **(Schlüssel-) Hash-basierte Nachrichtenauthentifizierung** | | |
| HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512 | #1425 | #1596 |
| **Zufallszahlengeneratoren** | | |
| swrand FIPS 186-2-Zufallszahlengenerator | #1154 | #1222 |
| n2rng FIPS 186-2-Zufallszahlengenerator | #1152 | #1226 |

Oracle Solaris bietet zwei Provider von kryptografischen Algorithmen, die auf FIPS 140-2 Level 1 validiert sind.

- Die Cryptographic Framework-Funktion von Oracle Solaris ist der zentrale kryptografische Speicher in einem Oracle Solaris-System; sie stellt zwei FIPS 140-Module bereit. Das Userland-Modul stellt Kryptografie für Anwendungen bereit, die im Userspace ausgeführt werden, während das Kernel-Modul Kryptografie für Kernel-Level-Prozesse bereitstellt. Diese Bibliotheksmodule stellen Funktionen zu Verschlüsselung, Entschlüsselung, Hashing, Signaturgenerierung und -prüfung, Zertifikatsgenerierung und -prüfung sowie Nachrichtenauthentifizierung bereit. Anwendungen auf Benutzerebene, die diese Module aufrufen, werden im FIPS 140-Modus ausgeführt; Beispiel: `passwd`-Befehl und IKEv2.

Kernel-Level-Consumer, beispielsweise Kerberos und IPsec, verwenden proprietäre APIs für Aufrufe im Kernel Cryptographic Framework.

- Das OpenSSL-Objektmodul stellt Kryptografie für SSH- und Webanwendungen bereit. OpenSSL ist das Open Source-Toolkit für die Secure Sockets Layer-(SSL-) und Transport Layer Security-(TLS-)Protokolle und stellt eine Kryptografiebibliothek bereit. In Oracle Solaris sind SSH und der Apache-Webserver Consumer des OpenSSL FIPS 140-Moduls. Oracle Solaris stellt eine FIPS 140-Version von OpenSSL mit Oracle Solaris 11.2 bereit, die für alle Consumer verfügbar ist, die mit Oracle Solaris 11.1 gelieferte Version ist jedoch nur für Solaris SSH verfügbar. Weil FIPS 140-2-Providermodule CPU-intensiv sind, sind sie standardmäßig nicht aktiviert. Als Administrator sind Sie für die Aktivierung der Provider im FIPS 140-Modus und die Konfiguration von Consumern verantwortlich.

Weitere Informationen zur Aktivierung von FIPS-140-Providern in Oracle Solaris finden Sie in dem Dokument *Using a FIPS 140 Enabled System in Oracle Solaris 11.2*, das unter der Überschrift "Securing the Oracle Solaris 11 Operating System" unter: `http://docs.oracle.com/cd/E36784_01` verfügbar ist.

# Schützen von SuperCluster M7 Series-Systemen

In diesen Themen werden die Funktionen von SuperCluster M7 Series beschrieben, mit denen Sie die Sicherheit während der Lebensdauer des Systems aufrecht erhalten können:



## Verwalten der SuperCluster-Sicherheit

SuperCluster M7 nutzt die Möglichkeiten der Sicherheitsverwaltung von einer Vielzahl von Produkten, einschließlich Oracle ILOM, Oracle Enterprise Manager Ops Center, Oracle Enterprise Manager und Oracle Identity Management Suite. In diesen Abschnitten werden die Einzelheiten beschrieben:



## Oracle ILOM für sichere Verwaltung

Oracle ILOM ist ein Serviceprozessor, der in vielen SuperCluster M7-Komponenten eingebettet ist. Verwenden Sie Oracle ILOM, um diese Out-of-Band-Verwaltungsaktivitäten auszuführen:

- Stellen Sie sicheren Zugriff für sicheres Lights-Out-Management der SuperCluster-Komponenten bereit. Der Zugriff umfasst den webbasierten, SSL-geschützten Zugriff, Befehlszeilenzugriff mit Secure Shell sowie IPMI v2.0- und SNMPv3-Protokolle.
- Trennen Sie Aufgaben mit einem RBAC-Modell. Weisen Sie einzelne Benutzer bestimmten Rollen zu, die die Funktionen begrenzen, die diese ausführen können.
- Bereitstellen eines Auditdatensatzes aller Anmeldungen und Konfigurationsänderungen. Jeder Auditlogeintrag enthält den Benutzer, der die Aktion ausgeführt hat, sowie einen Zeitstempel. Mit dieser Funktion können Sie nicht autorisierte Aktivitäten oder Änderungen ermitteln und diese Aktionen bestimmten Benutzern wieder zuordnen.

Weitere Informationen finden Sie in der Oracle Integrated Lights Out Manager-Dokumentation unter: http://docs.oracle.com/en/hardware/?tab=4

# Oracle Identity Management Suite

Oracle Identity Management Suite verwaltet den End-to-End-Lebenszyklus von Benutzeridentitäten und Konten in einem Unternehmen. Die Suite unterstützt Single Sign-On, webbasierte Zugriffskontrolle, Sicherheit von Webservices, Identitätsadministration, starke Authentifizierung sowie Identity und Access Governance.

Oracle Identity Management kann eine einzelne Stelle zur Verwaltung von Identität und Zugriff nicht nur für Anwendungen und Services bereitstellen, die auf Oracle SuperCluster ausgeführt werden, sondern auch für die zugrundeliegende Infrastruktur und die Services, die sie verwalten.

Weitere Informationen finden Sie in der Oracle Identity Management-Dokumentation unter:

http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

# Oracle Key Manager

Oracle Key Manager ist ein umfassendes Key Management System (KMS), das die Verwaltung und Überwachung von Verschlüsselungsschlüsseln vereinfacht, die gespeicherte Informationen schützen.

Oracle Key Manager unterstützt Unternehmensumgebungen mit einer hoch skalierbaren und verfügbaren Architektur, die Tausende von Geräten und Millionen von Schlüsseln verwalten kann. Diese Funktion wird in einer gehärteten Betriebsumgebung verwendet, setzt starke Zugriffskontrolle und Rollentrennung für Schlüsselverwaltungs- und

Überwachungsvorgänge durch, und unterstützt optional die sichere Speicherung von Schlüsseln in Sun Crypto Accelerator 6000 PCIe Card von Oracle, einem FIPS 140-2-konformen sicheren Hardwaremodul.

Im Kontext von SuperCluster kann Oracle Key Manager den Zugriff auf Verschlüsselungsschlüssel, die von Oracle StorageTek-Verschlüsselungsbandlaufwerken verwendet werden, Oracle Databases, die mit der transparenten Datenverschlüsselung verschlüsselt sind und verschlüsselten ZFS-Dateisystemen autorisieren, sichern und verwalten, die im Oracle Solaris 11-BS verfügbar sind.

Weitere Informationen finden Sie in der Oracle Key Manager-Dokumentation unter:

`http://docs.oracle.com/cd/E26076_02`

# Oracle Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager ist ein BUI-basiertes Hardwareverwaltungstool auf Rackebene für Oracle Service-Mitarbeiter. Weitere Einzelheiten finden Sie in *Oracle SuperCluster M7 Series - Eigentümerhandbuch: Administration*.

Oracle Engineered Systems Hardware Manager umfasst zwei Sets von Authentifizierungsinformationen:

- **SuperCluster M7-Komponentenpasswörter**

  Oracle Engineered Systems Hardware Manager verwaltet einen sicheren Speicher mit Passwörtern für alle werkseitigen Konten für die gesamte SuperCluster M7-Hardware. Die Software verwendet diese Passwörter zur Verwaltung der SuperCluster M7-Komponenten.

  Wenn sich eines dieser Passwörter ändert, müssen Sie die Oracle Engineered Systems Hardware Manager-Anwendung mit den neuen Passwörtern aktualisieren.
- **Lokale Authentifizierung**

  Oracle Engineered Systems Hardware Manager verfügt über zwei lokale Benutzerkonten. Mit einem Konto passen Kunden Oracle Engineered Systems Hardware Manager für ihre Umgebung an und verwalten das Servicekonto. Das andere Konto wird von Oracle Service-Mitarbeitern verwendet, um SuperCluster M7-Hardware zu konfigurieren, zu unterstützen und zu verwalten.

Oracle Engineered Systems Hardware Manager stellt die folgenden lokalen Verwaltungsressourcen bereit.

- **Passwortrichtlinie** – Die Möglichkeit, die Anwendungspasswörter entsprechend Ihren Unternehmensrichtlinien zu konfigurieren, stellt sicher, dass die Passwörter den Unternehmensstandards entsprechen.

---

**Anmerkung -** Besprechen Sie die Einstellungen für die Passwortrichtlinien mit dem Sicherheitsbeauftragten Ihres Unternehmens.

---

- **Zertifikate** – Oracle Engineered Systems Hardware Manager verwendet Zertifikate, um die Kommunikation zwischen Rechenservern und dem Oracle Engineered Systems Hardware Manager-Server und BUI zu sichern. Diese Zertifikate werden automatisch während der Installation erstellt und sind für jede SuperCluster-Instanz eindeutig, sie können jedoch durch Zertifikate und Schlüssel ersetzt werden, die vom Kunden bereitgestellt werden.
- **Ports** – Die Netzwerkports, die von Oracle Engineered Systems Hardware Manager verwendet werden, sind konfigurierbar, falls ein Konflikt mit den Unternehmensrichtlinien besteht. Die Ports 8001 bis 8004 (einschließlich) werden verwendet.

Hinweise zur Konfiguration finden Sie im *Oracle SuperCluster M7 Series - Eigentümerhandbuch: Administration*.

# Oracle Enterprise Manager

Oracle Enterprise Manager Suite ist eine umfassende und integrierte Cloud-Verwaltungslösung, die auf die Verwaltung des Lebenszyklus von Anwendungen, Middleware, Datenbanken sowie physischer und virtueller Infrastruktur (mit Oracle Enterprise Manager Ops Center) fokussiert ist. Oracle Enterprise Manager stellt die folgenden Verwaltungstechnologien bereit:

- Unterstützt detaillierte Überwachung, Ereignisbenachrichtigung, Patching, Change Management, kontinuierliche Konfiguration, Complianceverwaltung und Berichtserstellung für Anwendung, Middleware und Datenbank.
- Ermöglicht die zentrale Verwaltung von Sicherheitskonfigurationseinstellungen sowie Zugriffskontroll- und Auditingrichtlinien für Datenbankgruppen. Der Zugriff auf diese Funktionen kann auf autorisierte Einzelpersonen begrenzt werden; dadurch wird sichergestellt, dass der Verwaltungszugriff Complianceanforderungen zur Trennung von Aufgaben, geringster Berechtigung und Verantwortlichkeit unterstützt.
- Unterstützt die starke Authentifizierung mit einer Vielzahl von Methoden, feingranulierter Zugriffskontrolle und umfassendem Auditing, sodass die sichere Verwaltung der SuperCluster-Umgebung gewährleistet ist.

Weitere Informationen finden Sie in der Oracle Enterprise Manager-Dokumentation unter: `http://www.oracle.com/technetwork/oem/grid-control/documentation/oem-091904.html`

## Oracle Enterprise Manager Ops Center (Optional)

Oracle Enterprise Manager Ops Center ist eine optionale Technologie, mit der Sie einige Sicherheitsaspekte von Oracle SuperCluster verwalten können.

Als Teil der Oracle Enterprise Manager Suite ist Oracle Enterprise Manager Ops Center eine zusammengeführte Hardwareverwaltungslösung, die eine einzelne administrative Schnittstelle für Server, Betriebssysteme, Firmware, virtuelle Maschinen, Zonen, Speicher und Netzwerk-Fabrics bereitstellt.

Mit Oracle Enterprise Manager Ops Center können Sie administrativen Zugriff auf Zusammenstellungen von physischen und virtuellen Systemen zuweisen, Administratoraktivitäten überwachen, Fehler ermitteln und Alerts konfigurieren und verwalten. Oracle Enterprise Manager Ops Center unterstützt eine Vielzahl von Berichten, mit denen Sie Systeme mit bekannten Konfigurations-Baselines, Patchebenen und Sicherheitslücken vergleichen können.

Weitere Informationen finden Sie in der Oracle Enterprise Manager Ops Center-Dokumentation unter: http://docs.oracle.com/cd/E27363_01/index.htm

**Anmerkung -** Bei früheren Versionen von Oracle Enterprise Manager Ops Center wurde die Ops Center-Software im SuperCluster-System installiert und ausgeführt. Ab Oracle Enterprise Manager Ops Center 12c Release 2 (12.2.0.0.0) muss die Ops Center-Software in einem System außerhalb des SuperCluster-Systems installiert und ausgeführt werden.

# Überwachen der Sicherheit

Ob für Complianceberichte oder als Reaktion auf Vorfälle, Überwachung und Auditing sind kritische Funktionen, die Sie für einen besseren Einblick in die IT-Umgebung verwenden müssen. Der Grad, bis zu dem Überwachung und Auditing eingesetzt werden, basiert häufig auf dem Risiko oder der kritischen Natur der Umgebung.

SuperCluster M7 Series-Systeme stellen umfassende Überwachungs- und Auditingfunktionalität auf Server-, Netzwerk-, Datenbank- und Speicherebene bereit, sodass sichergestellt ist, dass Informationen für Audit- und Complianceanforderungen verfügbar gemacht werden können.

In diesen Abschnitten werden Workload- sowie Datenbanküberwachung und -auditing beschrieben:

# Workload-Überwachung

Das Oracle Solaris-BS verfügt über eine umfassende Auditingfunktion, die administrative Aktionen, Befehlszeilenaufrufe und sogar einzelne Systemaufrufe auf Kernel-Ebene überwachen kann. Diese Funktion ist hoch konfigurierbar und bietet globale Auditingrichtlinien pro Zone und sogar pro Benutzer.

Wenn das System zur Verwendung von Oracle Solaris-Zonen konfiguriert ist, können Auditdatensätze in der globalen Zone gespeichert werden, um sie vor Manipulation zu schützen.

Das Oracle Solaris-Auditing bietet die Möglichkeit, Auditdatensätze mit der Systemlog-(`syslog`)Funktion an Remote-Erfassungspunkte zu senden. Viele kommerzielle Angriffserkennungs- und Eindringschutzsysteme können Oracle Solaris-Auditdatensätze als zusätzliche Eingabe zur Analyse und Berichtserstellung verwenden.

Oracle VM Server for SPARC nutzt die systemeigene Oracle Solaris-Auditingfunktion zur Aufzeichnung von Aktionen und Ereignissen, die mit Virtualisierungsereignissen und Domainadministration verknüpft sind.

Weitere Informationen finden Sie im Abschnitt "Überwachen und Verwalten von Oracle Solaris-Sicherheit in "Oracle Solaris - Sicherheitsbestimmungen" unter:

`http://docs.oracle.com/cd/E26502_01`

# Überwachung und Auditing von Datenbankaktivitäten

Mit der Oracle Database-Unterstützung des feingranulierten Auditings können Sie Richtlinien festlegen, die selektiv bestimmen, wann Auditdatensätze generiert werden. Dank dieser Möglichkeit können Sie sich auf andere Datenbankaktivitäten konzentrieren und vermeiden den Overhead, der häufig mit Auditaktivitäten verbunden ist.

Oracle Audit Vault and Database Firewall zentralisiert die Verwaltung von Datenbankauditeinstellungen und automatisiert die Konsolidierung von Auditdaten in

einem sicheren Repository. Diese Software umfasst eine integrierte Berichtserstellung, um ein breites Spektrum an Aktivitäten zu überwachen, einschließlich privilegierter Benutzeraktivitäten und Änderungen an Datenbankstrukturen. Die von Oracle Audit Vault and Database Firewall generierten Berichte bieten Einblick in verschiedene Anwendungs- und administrative Datenbankaktivitäten und stellen detaillierte Informationen zur Unterstützung der Verantwortlichkeit von Aktionen bereit.

Oracle Audit Vault and Database Firewall aktiviert die proaktive Ermittlung und Warnung bei Aktivitäten, die auf nicht autorisierte Zugriffsversuche oder den Missbrauch von Systemberechtigungen hinweisen können. Diese Warnungen können sowohl system- als auch benutzerdefinierte Ereignisse und Bedingungen umfassen, wie das Erstellen von privilegierten Benutzerkonten oder die Änderung von Tabellen, die vertrauliche Informationen enthalten.

Die Remote-Überwachung von Oracle Audit Vault and Database Firewall ermöglicht Echtzeitüberwachung der Datenbanksicherheit. Diese Funktion fragt Datenbankverbindungen ab, um böswilligen Datenverkehr zu ermitteln, wie Umgehen von Anwendungen, nicht autorisierte Aktivitäten, Einschleusung von SQL-Befehlen und andere Bedrohungen. Mit einer präzisen, auf der SQL-Grammatik basierenden Lösung können Sie mit dieser Software verdächtige Datenbankaktivitäten schnell identifizieren.

Weitere Informationen finden Sie in der Oracle Audit Vault and Database Firewall-Dokumentation unter: http://docs.oracle.com/cd/E37100_01/index.htm

# Netzwerküberwachung

Nachdem die Netzwerke nach den neuesten Sicherheitsbestimmungen konfiguriert wurden, sind regelmäßige Prüfung und Wartung erforderlich.

Halten Sie sich an folgende Bestimmungen, um einen sicheren lokalen und Remote-Zugriff auf das System zu gewährleisten:

- Prüfen Sie die Logs auf mögliche Vorfälle, und archivieren Sie sie gemäß den Sicherheitsbestimmungen Ihres Unternehmens.
- Prüfen Sie das Clientzugriffsnetzwerk in regelmäßigen Abständen, um sicherzustellen, dass Host- und Oracle ILOM-Einstellungen weiter intakt sind.

Weitere Informationen finden Sie in den Sicherheitshandbüchern für das Oracle Solaris-BS:

- Oracle Solaris 11-BS – http://www.oracle.com/goto/Solaris11/docs
- Oracle Solaris 10-BS – http://www.oracle.com/goto/Solaris10/docs

# Updaten von Software und Firmware

Updates für das SuperCluster M7 Series-System werden in QFSDP bereitgestellt. Durch die Installation von QFSDP werden alle Komponenten gleichzeitig upgedatet. Dadurch wird sichergestellt, dass alle Komponenten weiter mit einer Kombination von Softwareversionen ausgeführt werden, die gemeinsam vollständig von Oracle getestet wurden.

Die neueste QFSDP-Software erhalten Sie in My Oracle Support unter: http://support.oracle.com

Details zu der unterstützten Software und Firmware finden Sie in *Oracle SuperCluster M7 Series - Produkthinweise*. Anweisungen für den Zugriff auf diese Produkthinweise finden Sie in MOS-Hinweis 1605591.1.

**Anmerkung -** Nehmen Sie separate Upgrades, Updates oder Patches einzelner Komponenten zur reaktiven Wartung nur unter Anleitung von Oracle Support vor.

# Index

## R



## S



## Sch



## St