

Oracle MiniCluster S7-2 - Sicherheitshandbuch

ORACLE

Teilnr.: E78272-02
Oktober 2016

Teilnr.: E78272-02

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 dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

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

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

Diese Software oder Hardware und die 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.

Barrierefreie Dokumentation

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

Zugriff auf Oracle-Support

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

Inhalt

Verwenden dieser Dokumentation	7
Produktdokumentationsbibliothek	7
Feedback	7
Sicherheitsgrundsätze	9
Minimal erforderliche Sicherheitsaufgaben	9
Kernsicherheitsgrundsätze	10
Sichere virtuelle Maschinen	11
Zugriffskontrolle	12
Datenschutz	13
Auditing und Compliance	14
Sicherheitskonfiguration	17
Integrierte Sicherheitsprofile	17
▼ Prüfen des VM-Sicherheitsprofils (CLI)	18
Schützen von Daten	21
Datenschutz mit ZFS-Dataset-Verschlüsselung	21
▼ Anzeigen der ZFS-Dataset-Verschlüsselungsschlüssel (BUI)	21
Secure Shell Service	22
▼ Ändern der SSH-Schlüssel (BUI)	22
Sichere Kommunikation mit IPsec	25
▼ Konfigurieren von IPsec und IKE	25
Zugriff kontrollieren	27
▼ Ändern der Standard-Oracle ILOM-root-Passwörter	27
▼ EEPROM-Passwörter konfigurieren	28
Benutzer-Provisioning	29
MCMU-Benutzergenehmigungsprozess	30
Rollenbasierte Zugriffskontrolle	31

Benutzerkonten	32
Benutzerauthentifizierung und Passwortrichtlinien	33
▼ Prüfen von Oracle Solaris-Benutzerrollen	33
Sicheres Löschen von VMs	34
▼ Hostbasierte Firewallregeln überprüfen	34
▼ Prüfen der Verified Boot-Umgebung	36
▼ Begrenzen des Zugriffs auf Shared Storage	37
Auditing- und Compliance-Reporting	39
▼ Prüfen der Auditrichtlinien	39
▼ Auditlogs prüfen	40
▼ Auditberichte generieren	41
▼ (Falls erforderlich) Aktivieren eines FIPS-140-konformen Vorgangs (Oracle ILOM)	43
FIPS-140-2 Level 1-Compliance	45
Bewerten der Sicherheitscompliance	47
Sicherheitscompliancebenchmarks	47
▼ Planen einer Sicherheitscompliancebenchmark (BUI)	48
▼ Anzeigen von Benchmarkberichten (BUI)	49
SPARC S7-2 Server - Sicherheitssteuerelemente	53
Hardwaresicherheit	53
Zugriffsbeschränkungen	53
Seriennummern	54
Festplatten	54
Einschränken des Zugriffs auf OpenBoot	55
▼ Aufrufen des OpenBoot Prompts	55
▼ Auf nicht erfolgreiche Anmeldungen prüfen	56
▼ Banner zum Hochfahren bereitstellen	56
Stichwortverzeichnis	57

Verwenden dieser Dokumentation

- **Überblick** - Enthält Informationen zur Planung, Konfiguration und Wartung einer sicheren Umgebung für Oracle MiniCluster S7-2-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 unter <http://www.oracle.com/goto/miniclusters7-2/docs> verfügbar

Feedback

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

Sicherheitsgrundsätze

Dieses Handbuch enthält Informationen zur Planung, Konfiguration und Wartung einer sicheren Umgebung für Oracle MiniCluster S7-2-Systeme.

In diesem Abschnitt werden folgende Themen behandelt:

- „Minimal erforderliche Sicherheitsaufgaben“ [9]
- „Kernsicherheitsgrundsätze“ [10]
- „Sichere virtuelle Maschinen“ [11]
- „Zugriffskontrolle“ [12]
- „Datenschutz“ [13]
- „Auditing und Compliance“ [14]

Minimal erforderliche Sicherheitsaufgaben

Als Engineered System ist MiniCluster werksseitig standardmäßig als hoch sicheres System mit den folgenden Sicherheitsfunktionen konfiguriert:

- Vorkonfiguriert mit voll automatisierten Sicherheitssteuerelementen für alle virtuellen Maschinen (VMs).
- Verschlüsselung ist standardmäßig aktiviert, sodass sichere Daten bei der Speicherung (Data at Rest) und bei der Übertragung (Data in Transit) gewährleistet sind.
- VMs sind automatisch mit einem gehärteten und minimierten BS mit hostbasierten Firewalls konfiguriert.
- Zugriffskontrolle erfordert rollenbasierten Zugriff mit niedrigsten Berechtigungen.
- Alle VMs verwenden die verschlüsselte ZFS-Speicherung.
- Eine zentralisierte Einrichtung zur Schlüsselverwaltung, die PKCS#11 verwendet, und Unterstützung von FIPS sind vorhanden.
- Das System umfasst eine umfassende Auditrichtlinie mit zentralisierten Auditlogs.
- Das System und alle VMs sind mit einem PCI-DSS-, CIS-äquivalenten oder DISA-STIG-Sicherheitsprofil konfiguriert. Hinweis: Das letztere Profil wird derzeit geprüft. Verwenden

Sie das DISA-STIG-Profil nur zur experimentellen Nutzung in Nicht-Production-Umgebungen.

- Es gibt ein einfach anzuzeigendes Compliance-Dashboard, das einfach auszuführende Compliancebenchmarks unterstützt.

Unmittelbar nach der MiniCluster-Installation muss der Sicherheitsadministrator zwei obligatorische Aufgaben ausführen:

- Ändern des Oracle ILOM-Root-Passwortes. Siehe [Ändern der Standard-Oracle ILOM-root-Passwörter \[27\]](#)

Außerdem müssen die Sicherheitsinformationen in diesem Handbuch gelesen werden, damit die MiniCluster-Sicherheitsfunktionen verstanden und geprüft werden.

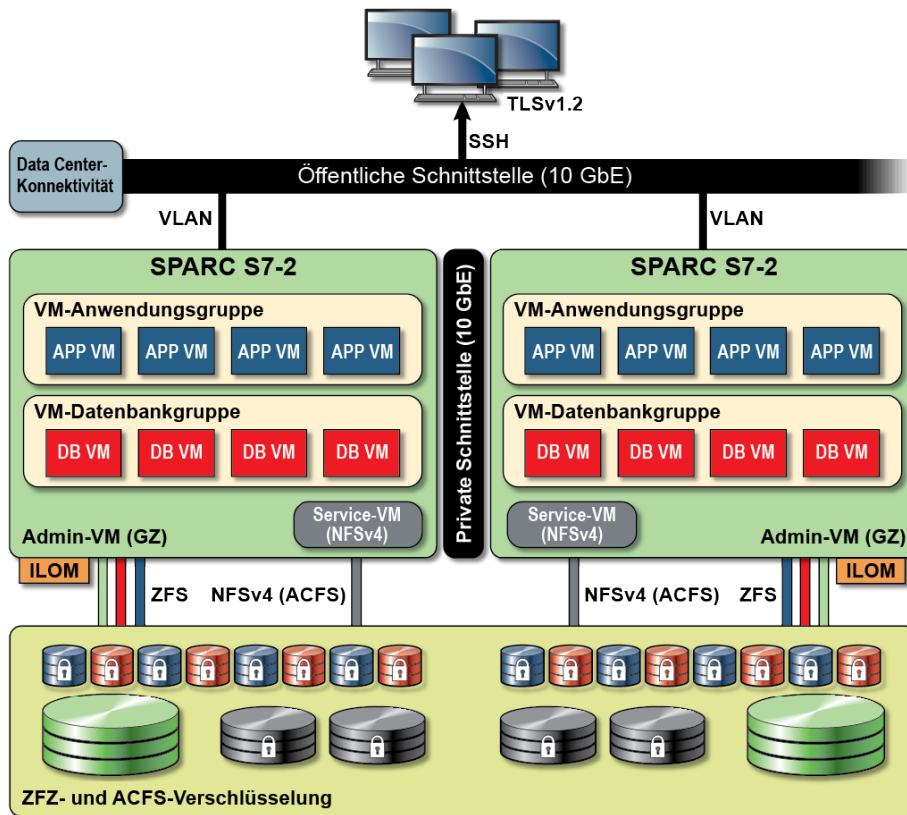
Kernsicherheitsgrundsätze

MiniCluster ist eine sichere Cloudinfrastrukturplattform zur Konsolidierung von Anwendungen und Datenbanken. Sie eignet sich besonders zur Bereitstellung von dedizierten Cloudservices, die auf Computing Infrastructure as a Service (IaaS) basieren. Als Mehrzweck-Engineered System kombiniert es die Computing-Leistung des Oracle SPARC S7-Prozessors, die effizienten Virtualisierungsmöglichkeiten von SPARC Solaris und die optimierte Datenbankleistung der Oracle-Datenbank integriert mit dediziertem Speicher. Außerdem wird ein 10GbE-Netzwerk verwendet, mit dem Clients auf Services zugreifen können, die auf MiniCluster ausgeführt werden. Schließlich stellt ein weiteres 10GbE-Netzwerk das Conduit bereit, über das die gesamte Interkommunikation zwischen der virtuellen Maschinenumgebung auf den SPARC S7-Servern und gehosteten Anwendungen läuft.

Der SPARC S7-Prozessor bietet immer aktivierte hardwaregestützte kryptografische Funktionalität, mit der in MiniCluster gehostete Entitäts ihre Informationen mit High-Performance-Datenschutz schützen können - At Rest, In-Use und In-Transit. Der Prozessor umfasst auch die silikongesicherte Speicherfunktion, die Angriffe im Zusammenhang mit Beschädigung von Speicherdaten und Speicher-Scraping ermittelt und verhindert und so die Integrität von Anwendungsdaten sicherstellt.

Standardmäßig ist MiniCluster mit mehr als 250 Out-of-Box-Sicherheitssteuerelementen vorkonfiguriert, die die Angriffsfläche des Systems reduzieren, indem Services, Ports und Protokolle deaktiviert werden, die nicht unbedingt erforderlich sind, und indem die verfügbar gemachten Services so konfiguriert werden, dass nur vertrauenswürdige Verbindungen akzeptiert werden.

Das System unterstützt eine Vielzahl von Konfigurations- und Deployment-Optionen. Diese Abbildung stellt ein typisches Deployment dar, das Oracle-Datenbank- und Anwendungsworkloads konsolidiert.



Sichere virtuelle Maschinen

Die Sicherheit innerhalb der MiniCluster-Serverknoten wird auf mehreren Ebenen bereitgestellt. Sie beginnt mit sicherem Verified Boot der Serverknoten, einem gehärteten und minimierten BS, das in Form isolierter virtueller Maschinen ausgeführt wird, um zu verhindern, dass von nicht autorisierten Benutzern und Systemen auf Workloads und Daten zugegriffen wird. Oracle Solaris Zones-Technologie wird für virtuelle Maschinen in MiniCluster verwendet, um isolierte Computing-Umgebungen zu hosten und verschiedene Anwendungen, die unter demselben Betriebssystem ausgeführt werden, wirksam und effizient zu abzugrenzen und somit vor unbeabsichtigten oder böswilligen Aktivitäten zu schützen, die in anderen virtuellen Maschinen auftreten. Auch wenn sie in demselben Kernel ausgeführt werden, haben alle Solaris-Zones ihre eigene Identität sowie Ressourcen-, Namespace- und Prozessisolation. Im Wesentlichen stellen Solaris-Zones integrierte Virtualisierung mit strenger Isolation und flexiblen Ressourcensteuerelementen mit einem kleineren CPU- und Arbeitsspeicher-Footprint bereit als übliche virtuelle Maschinen, die auf Typ 1 Hypervisoren ausgeführt werden. Jede virtuelle Maschine ist mit einem Sicherheitsprofil konfiguriert, das ein umfassendes

Set an Sicherheitssteuerelementen und -richtlinien definiert, die automatisch während des Installationsprozesses angewendet werden. Die Verwendung von ZFS-Pools und -Datasets ermöglicht eine weitere Aufteilung und Isolation des Speichers in kleinere Einheiten für virtuelle Maschinen. Sie können über ihre eigenen Sicherheitsrichtlinien verfügen.

Zugriffskontrolle

Um Anwendungsdaten, Workloads und die zugrundeliegende Infrastruktur zu schützen, auf der sie alle ausgeführt werden, bietet MiniCluster umfassende und dennoch flexible Zugriffskontrollmöglichkeiten für Benutzer und Administratoren. MiniCluster nutzt Oracle Solaris für eine Vielzahl von Zugriffskontrollmethoden für Benutzer und Anwendungen, die auf Systemservices zugreifen. Während die herkömmlichen Benutzername- und Passwortpaare weiter häufig verwendet werden, können strengere Authentifizierungsmethoden jederzeit mit der Oracle Solaris-Architektur der integrierbaren Authentifizierungsmodule (PAM) integriert werden, die die Verwendung von LDAP, Kerberos und Public Key-Authentifizierung ermöglichen. MiniCluster Computing-Umgebungen bauen auf einer umfassenden rollenbasierten Zugriffskontrollfunktion (RBAC) auf, die Unternehmen die Flexibilität geben, Benutzer- und administrativen Zugriff je nach Anforderung zu delegieren. Da der Begriff des mächtigen Superusers wegfällt, ermöglicht die RBAC-Funktion in Oracle Solaris die Aufgabentrennung und unterstützt den Begriff von administrativen Rollen, Autorisierungen, feingranulierten Berechtigungen und Rechteprofilen, die gemeinsam verwendet werden, um Benutzern und Administratoren Rechte zuzuweisen. RBAC ist mit anderen Oracle Solaris-Kernservices integriert, einschließlich Oracle Solaris Service Management Facility (SMF) und den virtuellen Maschinen und stellt so eine konsistente Architektur bereit, die alle Zugriffskontrollanforderungen auf Betriebssystemebene unterstützt. MiniCluster nutzt die RBAC-Möglichkeit von Oracle Solaris als Grundlage für seine Zugriffskontrollarchitektur, sodass Unternehmen den Zugriff auf Betriebssystem und Virtualisierungsverwaltung von einer zentralisierten Stelle aus verwalten, kontrollieren und auditieren können. Alle wichtigen Vorgänge werden mit dem Prinzip der Aufgabentrennung ausgeführt, das von einem Autorisierungsworkflow mit mehreren Personen unterstützt wird. Das System erfordert, dass zwei oder mehr Personen jeden sicherheitsrelevanten Vorgang genehmigen. Gemeinsam können diese Möglichkeiten einen hohen Grad an Sicherheit für die Identität von Benutzern und deren Handhabung von kritischen Geschäftsvorgängen bereitstellen.

Alle Geräte im MiniCluster-System enthalten die Möglichkeit, den Netzwerkzugriff auf Services zu begrenzen, indem entweder die von der Architektur bereitgestellten Methoden (beispielsweise Netzwerkisolation), Paketfilterung und/oder Zugriffskontrolllisten zur Begrenzung der Kommunikation zu, von und zwischen physischen und virtuellen Geräten sowie zu Services verwendet werden, die vom System zur Verfügung gestellt werden. MiniCluster nutzt eine "Secure-by-Default"-Haltung, bei der keine Netzwerkservices, mit Ausnahme von Secure Shell (SSH), eingehenden Netzwerkverkehr akzeptieren können. Andere aktivierte Netzwerkservices hören intern auf Anforderungen innerhalb des Oracle Solaris-Betriebssystems (virtuelle Maschine oder Zone). Dadurch wird sichergestellt, dass alle Netzwerkservices standardmäßig deaktiviert sind oder so eingestellt sind, dass sie nur

auf lokale Systemkommunikation hören. Unternehmen können diese Konfiguration je nach Anforderungen anpassen. MiniCluster ist im Voraus mit einer Netzwerk- und Transportschicht-(Stateful-)Paketfilterung konfiguriert, die die Oracle Solaris IP-Filterfunktion verwendet. IP-Filter bietet ein breites Spektrum an hostbasierten Netzwerkmöglichkeiten, einschließlich Stateful-Paketfilterung, Übersetzung von Netzwerkadressen und Übersetzung von Portadressen.

Datenschutz

Der SPARC S7-Prozessor in MiniCluster vereinfacht die hardwaregestützten High-Performance-Verschlüsselungen für die Datenschutzerfordernungen 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.

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 Betriebssystemebene die kryptografische Hardwarebeschleunigung standardmäßig für die meisten Core-Services aktiviert, einschließlich Secure Shell, IPSec/IKE und verschlüsselten ZFS-Datensets.

Oracle Database und Oracle Fusion Middleware identifizieren automatisch das Oracle Solaris-Betriebssystem und den SPARC-Prozessor, der von MiniCluster 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. MiniCluster unterstützt die Verwendung von IPSec (IP Security). IKE (Internet Key Exchange) wird empfohlen, um die Vertraulichkeit und Integrität von VM-spezifischen und Inter-VM-Kommunikationen zu schützen, die über das öffentliche und private Netzwerk fließen.

Bei MiniCluster nutzt die ZFS-Dataset-Verschlüsselung einen zentralisierten Oracle Solaris PKCS#11-Keystore, um die Wrapping Keys sicher zu schützen. Bei Verwendung des Oracle Solaris PKCS#11-Keystores wird automatisch die hardwaregestützte kryptografische Beschleunigung von SPARC für alle Verschlüsselungsvorgänge aktiviert. Auf diese Weise kann Oracle die Performance der Verschlüsselungs- und Entschlüsselungsvorgänge wesentlich verbessern, die mit der Verschlüsselung von ZFS-Datensets, der Verschlüsselung von Oracle Database Transparent Data Encryption (TDE), 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. Virtuelle Datenbankmaschinen können eine Shared-Wallet-Lösung

verwenden, indem der Oracle Solaris PKCS#11-Keystore verwendet oder ein Verzeichnis in dem ACFS Shared Storage erstellt wird, sodass das Wallet über die Datenbanken hinweg gemeinsam genutzt werden kann, die auf den virtuellen Maschinen gespeichert sind. Durch Verwendung eines zentralisierten Shared Keystore auf jedem Serverknoten kann das System die Schlüssel von Oracle TDE in Oracle Grid Infrastructure basierend auf geclusterten Datenbankarchitekturen verwalten, warten und rotieren, weil die Schlüssel über alle Knoten in dem Cluster hinweg synchronisiert werden. MiniCluster lässt auch ein sicheres Löschen von virtuellen Maschinen und verknüpften ZFS-Datasets zu, indem die Verschlüsselungsrichtlinie und Schlüsselverwaltung auf dieser ZFS-Dataset-(Dateisystem-/ZVOL-)Ebene garantierte Löschung durch Zerstörung der Schlüssel sicherstellen.

Auditing und Compliance

MiniCluster nutzt das Oracle Solaris-Auditsubsystem zur Erfassung, Speicherung und Verarbeitung von Auditereignisinformationen. Jede virtuelle Maschine (nicht-globale Zone) generiert Auditdatensätze, die lokal in jedem MiniCluster-Auditspeicher (globale Zone) gespeichert werden. Diese Lösung stellt sicher, dass einzelne virtuelle Maschinen ihre Auditingrichtlinien, -konfigurationen oder aufgezeichneten Daten nicht ändern können, weil die Verantwortung bei dem Cloudserviceprovider liegt.

Die Oracle Solaris-Auditingfunktion überwacht alle administrativen Aktionen, Befehlsaufrufe und sogar individuelle Systemaufrufe auf Kernebene in den virtuellen Maschinen. Diese Funktion ist hoch konfigurierbar und bietet globale Auditingrichtlinien pro Zone und sogar pro Benutzer. Bei der Konfiguration zur Verwendung der virtuellen Maschine können Auditdatensätze für jede virtuelle Maschine in der globalen Zone gespeichert werden, um sie vor Manipulation zu schützen. Die globale Zone nutzt auch die systemeigene Oracle Solaris-Auditingfunktion zur Aufzeichnung von Aktionen und Ereignissen, die mit Virtualisierungsereignissen und MiniCluster-Administration verknüpft sind.

MiniCluster stellt Tools bereit, die die Compliance der Oracle Solaris-Laufzeitumgebung in den virtuellen Maschinen bewerten und melden. Compliancedienstprogramme basieren auf der SCAP-(Security Content Automation Protocol-)Implementierung. MiniCluster unterstützt zwei Sicherheitscompliance-Benchmarkprofile:

- **Standardsicherheitsprofil:** Ein CIS-äquivalentes Profil (basierend auf der Center of Internet Security-Benchmark), das eher auf die gesetzlich vorgeschriebenen Anforderungen der Sicherheitscompliance ausgerichtet ist, wie HIPAA, FISMA, SOX usw.
- **PCI-DSS-Profil** - Der Payment Card Industry Data Security Standard
- **DISA STIG-Profil:** Der Defense Information System Agency - Security Technical Implementation Guidance-Standard. Dieses Profil baut auf dem Standardsicherheitsprofil auf und führt 75 weitere Sicherheitskontrollen, FIPS-140-2-Kryptografie und Unterstützung zum Festlegen eines S-Passworts ein. *Hinweis:* Dieses Profil wird derzeit geprüft. Verwenden Sie dieses Profil nur zur experimentellen Nutzung in Nicht-Production-Umgebungen.

Der MiniCluster-Administrator kann die Compliancebenchmark auf Anforderung ausführen und die Umgebung auf Compliance und Anomalien prüfen. Diese Profiling-Tools ordnen Sicherheitssteuerelemente den Complianceanforderungen zu, die von den Industriestandards auferlegt werden. Die verknüpften Complianceberichte können Auditingzeit und -kosten wesentlich reduzieren.

Ab MiniCluster v.1.1.18 umfasst das System die folgenden Auditingfunktionen:

- **Auditorrolle:** Wenn diese Rolle für einen MCMU-Benutzer angegeben ist, kann der Benutzer auf die Auditprüfungsseite in der MCMU-BUI zugreifen. Der Benutzer kann keine anderen administrativen MiniCluster-Aufgaben anzeigen oder ausführen.
- **Auditprüfungsseite:** Dies ist eine spezielle MCMU-BUI-Seite, die nur von Benutzern mit der Auditorrolle angezeigt werden kann. Auf dieser Seite können Sie den Auditpoolstatus prüfen und Auditdatensätze für alle Benutzeraktivitäten pro Zone generieren. Siehe [Auditberichte generieren \[41\]](#).

Sicherheitskonfiguration

In diesen Themen werden die MiniCluster-Sicherheitssteuerelemente beschrieben:

- [„Integrierte Sicherheitsprofile“ \[17\]](#)
- [Prüfen des VM-Sicherheitsprofils \(CLI\) \[18\]](#)

Integrierte Sicherheitsprofile

Die MiniCluster-Initialisierung wird mit der MCMU-BUI oder CLI durchgeführt. Während der Initialisierung muss das Installationsprogramm bei MCMU eines dieser Sicherheitsprofile auswählen:

- **Standardsicherheitsprofil** - Erfüllt Anforderungen, die mit Benchmarks vergleichbar und gleichbedeutend sind, die von den Center for Internet Security-(CIS-) und Security Technical Implementation Guidelines-(STIG-)Bewertungen festgelegt werden.
- **PCI-DSS-Profil** - Entspricht dem PCI DSS-(Payment Card Industry Data Security Standard-)Standard, der von dem Payment Card Industry Security Standards Council definiert wird.
- **DISA STIG-Profil**: Der Defense Information System Agency - Security Technical Implementation Guidance-Standard. Dieses Profil baut auf dem Standardsicherheitsprofil auf und führt 75 weitere Sicherheitskontrollen, FIPS-140-2-Kryptografie und Unterstützung zum Festlegen eines eeprom-Passworts ein. *Hinweis*: Dieses Profil wird derzeit geprüft. Verwenden Sie dieses Profil nur zur experimentellen Nutzung in Nicht-Production-Umgebungen.

Je nach der ausgewählten Richtlinie konfiguriert MCMU die globale Zone und nicht-globalen Zonen mit mehr als 250 Sicherheitssteuerelementen.

Nach der Initialisierung erfordert MCMU beim Erstellen der virtuellen Maschinen die Auswahl von einem der Sicherheitsprofile für jede virtuelle Maschine. Je nach Ihren Sicherheitsanforderungen können Sie eine Mischung von Sicherheitsprofilen in den virtuellen Maschinen verwenden.

▼ Prüfen des VM-Sicherheitsprofils (CLI)

Mit dieser Prozedur können Sie das Sicherheitsprofil prüfen oder identifizieren, das für die Zonen und virtuellen Maschinen konfiguriert ist.

Anmerkung - Sie müssen mit einem Benutzerkonto auf das System zugreifen, das über die `root`-Rolle zur Durchführung dieser Prozedur verfügt.

Anmerkung - Zur Identifizierung des Sicherheitsprofils, das der globalen Zone zugewiesen ist, zeigen Sie in der MCMU-BUI "System Setting -> User Input Summary" (Systemeinstellung -> Benutzereingabezusammenfassung) an. Das Sicherheitsprofil wird unten auf der Seite angezeigt.

1. Melden Sie sich bei der globalen Zone als `mcinstall` an.

Anweisungen für den Aufruf des Systems finden Sie in *Oracle MiniCluster S7-2 - Administrationshandbuch*.

2. Nehmen Sie die `root`-Rolle an.

Beispiel:

```
# su root
```

3. Bestimmen Sie den Logdateinamen für die betreffende VM.

In diesem Beispiel ist eine Logdatei für jede VM vorhanden:

```
# cd /var/opt/oracle.miniclustermcmubui/MCMU/verification_logs
# ls
verify_appvmg1-zone-1-mc4-n1.log  verify_dbvmg1-zone-3-mc4-n1.log
verify_appvmg1-zone-1-mc4-n2.log  verify_dbvmg1-zone-3-mc4-n2.log
verify_dbvmg1-zone-1-mc4-n2.log  verify_dbvmg1-zone-4-mc4-n1.log
verify_dbvmg1-zone-2-mc4-n1.log  verify_dbvmg1-zone-4-mc4-n2.log
verify_dbvmg1-zone-2-mc4-n2.log
#
```

4. Prüfen Sie die Verifizierungslogdateien.

Zeigen Sie die letzten Zeilen der Logdatei an. Wenn (PCI-DSS) angezeigt wird, ist das VM-Sicherheitsprofil PCI-DSS. Wenn kein Profil aufgeführt wird, ist das VM-Sicherheitsprofil CIS-äquivalent.

- Beispiel der letzten 22 Zeilen einer VM mit einem PCI-DSS-Profil:

```
# tail -22 verify_dbvmg1-zone-1-mc4-n2.log

(PCI-DSS) Checking /etc/cron.d/at.allow:
Passed/Configured

(PCI-DSS) Checking audit configuration (user audit flags):
```

Passed/Configured

(PCI-DSS) Checking audit configuration (non-attributable audit flags):

Passed/Configured

(PCI-DSS) Checking audit configuration (audit_binfile plugin):

Passed/Configured

(PCI-DSS) Checking audit flags on root and tadmin roles:

Passed/Configured

Check if tenant-key exists in keystore:

Passed/Configured

Check if immutability is enabled:

Failed/Not Configured

■ Beispiel der letzten 22 Zeilen einer VM mit einem CIS-äquivalenten Profil:

```
# tail -22 verify_dbvmg1-zone-1-mc4-n2.log
```

Checking if NDP routing daemon is disabled:

Passed/Configured

Checking if r-protocol services are disabled:

Passed/Configured

Checking if rpc/bind is enabled and configured correctly:

Passed/Configured

Checking if NFS v2/v3 is disabled:

Passed/Configured

Checking if GDM is enabled:

Failed/Not Configured

Check if tenant-key exists in keystore:

Passed/Configured

Check if immutability is enabled:

Failed/Not Configured

Schützen von Daten

In diesen Themen werden die MiniCluster-Datenschutztechnologien beschrieben:

- [„Datenschutz mit ZFS-Dataset-Verschlüsselung“ \[21\]](#)
- [Anzeigen der ZFS-Dataset-Verschlüsselungsschlüssel \(BUI\) \[21\]](#)
- [„Secure Shell Service“ \[22\]](#)
- [Ändern der SSH-Schlüssel \(BUI\) \[22\]](#)
- [„Sichere Kommunikation mit IPsec“ \[25\]](#)
- [Konfigurieren von IPsec und IKE \[25\]](#)

Datenschutz mit ZFS-Dataset-Verschlüsselung

In MiniCluster wird der Datenschutz bei der Speicherung (Data at Rest) automatisch mit der ZFS-Dataset-Verschlüsselung konfiguriert. Die Verschlüsselung wird wie folgt konfiguriert:

- Alle ZFS-Datasets werden in virtuellen Maschinen verschlüsselt, einschließlich den Root- und Swap-Dateisystemen.
- Alle ZFS-Datasets werden erneut in der globalen Zone verschlüsselt, mit Ausnahme der Root- und Swap-Dateisysteme.

Sie können die Verschlüsselungskonfiguration prüfen, indem Sie die Verschlüsselungsschlüssel anzeigen. Siehe [Anzeigen der ZFS-Dataset-Verschlüsselungsschlüssel \(BUI\) \[21\]](#).

▼ Anzeigen der ZFS-Dataset-Verschlüsselungsschlüssel (BUI)

Im Folgenden wird beschrieben, wie Sie Verschlüsselungsschlüsseldetails anzeigen.

- 1. Rufen Sie die MCMU-BUI auf.**

Einzelheiten für den Aufruf der MCMU-BUI finden Sie in *Oracle MiniCluster S7-2 - Administrationshandbuch*.

2. Wählen Sie im Navigationsbereich " System Settings -> Security" (Systemeinstellungen -> Sicherheit) aus.

Klicken Sie auf einen Knoten, um Details anzuzeigen.

Encryption Key Information
Encryption keys for all virtual machines and attached volumes

Node	VM Name	ZFS Pool	Key Label
Node 1			
	mc12-n1	rpool/common	gz_mc12-n1_zw;pinfile
	mc12-n1	rpool/audit_pool	gz_mc12-n1_zw;pinfile
	mc12ss01	rpool/common	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/audit_pool	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/u01	kz_mc12ss01_zw;pinfile
	mc12-n1	mcpool	mcpool-id-key
	mc12-n1	mcpool/dbzonetemplate	dbzonetemplate-id-key
	mc12-n1	mcpool/appzonetemplate	appzonetemplate-id-key
	mc12-n1	rpool/repo	repo-id-key
	mc12-n1	mcpool/mc12dbzg1-zone-1-mc12-n1u01	mc12dbzg1-zone-1-mc12-n1-id-key

Secure Shell Service

MiniCluster erfordert die Verwendung des SSH-Netzwerkprotokolls, damit Sie sich sicher bei den MiniCluster-Serverknoten (globale Zonen) und Instanzen der virtuellen Maschine (nicht-globale Zonen) anmelden können.

Wenn sich ein Benutzer das erste Mal mit SSH anmeldet, generiert das System automatisch ein neues SSH-Schlüsselpaar für den Benutzer.

▼ Ändern der SSH-Schlüssel (BUI)

Mit dieser Prozedur können Sie die SSH-Schlüssel für eine Zone oder VM mit einer der folgenden Konfigurationen ändern:

- Neuen Schlüssel einfügen, um das passwortlose SSH zu autorisieren - Bei dieser Option müssen Sie einen VM-Benutzernamen, einen VM-Maschinennamen und einen RSA-Public Key eingeben.
- Automatische Generierung von neuen Schlüsseln für VMs

Anmerkung - Die Ausführung dieser Prozedur mit der MCMU-CLI wird in *Oracle MiniCluster S7-2 - Administrationshandbuch* beschrieben.

1. Rufen Sie die MCMU-BUI auf.
2. Wählen Sie im Navigationsbereich " System Settings -> Security" (Systemeinstellungen -> Sicherheit) aus.

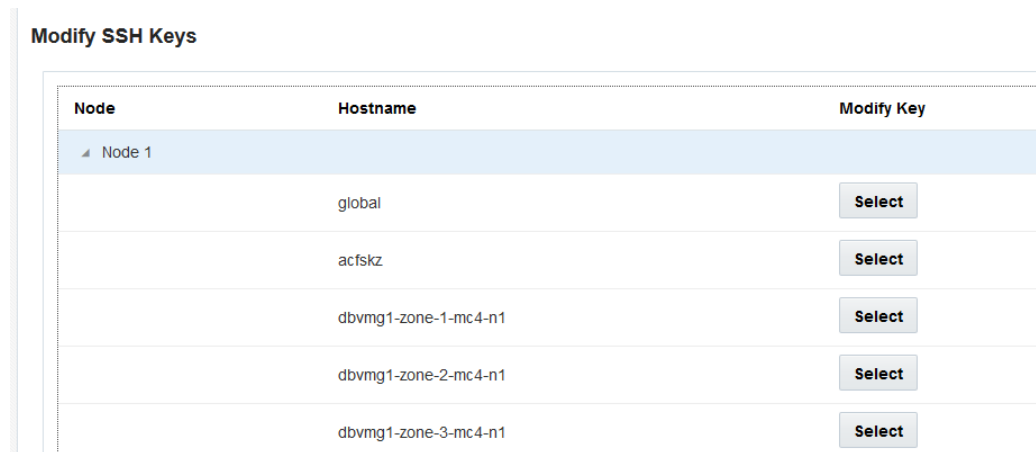
Encryption Key Information
Encryption keys for all virtual machines and attached volumes

Node	VM Name	ZFS Pool	Key Label	Encryption Key	Encryption Status	Key Source	Creation Date
▶ Node 1							
▶ Node 2							
◀ ————— ▶							

Modify SSH Keys

Node	Hostname	Modify Key
▶ Node 1		
▶ Node 2		

- Klicken Sie im Bereich "Modify SSH Keys" (SSH-Schlüssel ändern) auf einen Knoten, um die Anzeige einzublenden.**



Node	Hostname	Modify Key
Node 1		
	global	Select
	acfskz	Select
	dbvmg1-zone-1-mc4-n1	Select
	dbvmg1-zone-2-mc4-n1	Select
	dbvmg1-zone-3-mc4-n1	Select

- Klicken Sie für die VM, die Sie ändern möchten, auf "Select" (Auswählen).**
- Wählen Sie eine Option aus dem Dropdown-Menü, und klicken Sie auf "Next" (Weiter).**

Dies sind die Auswahlmöglichkeiten:

 - Neuen Schlüssel einfügen, um das passwortlose SSH zu autorisieren
 - Automatische Generierung von neuen Schlüsseln für Maschinen
- Klicken Sie auf "Next".**
- Wenn Sie die Autorisierung der passwortlosen SSH ausgewählt haben, geben Sie diese Informationen ein und klicken auf "Next".**
 - Benutzername der Maschine
 - Hostname der Maschine
 - RSA-Public Key der Maschine
- Klicken Sie auf "Setup SSH" (SSH einrichten).**

Die Änderung wird angewendet.

Sichere Kommunikation mit IPsec

Die Verwendung von IPsec (IP Security) und IKE (Internet Key Exchange) wird empfohlen, um die Vertraulichkeit und Integrität von IP-basierten Interzonenkommunikationen und NFS-Datenverkehr im Netzwerk zu schützen. IPsec wird empfohlen, weil sie Peer-Authentifizierung auf Netzwerkebene, Authentifizierung des Datenursprungs, Datenvertraulichkeit, Datenintegrität und Wiedergabeschutz unterstützt. Wenn sie auf der Oracle MiniCluster-Plattform verwendet werden, können IPsec und IKE die hardwaregestützte kryptografische Beschleunigung automatisch nutzen und so die Auswirkung der Verwendung der Kryptografie zum Schutz vertraulicher Informationen, die diesen Netzwerkkanal durchlaufen, auf die Performance verringern.

▼ Konfigurieren von IPsec und IKE

Bevor IPsec verwendet werden kann, müssen die spezifischen Hostnamen und/oder IP-Adressen definiert werden, die zwischen kommunizierenden Peers verwendet werden.

Bei dem Beispiel in dieser Prozedur werden die IP-Adressen 10.1.1.1 und 10.1.1.2 zur Angabe von zwei nicht-globalen Solaris-Zonen verwendet, die von einem einzelnen Mandanten betrieben werden. Die Kommunikation zwischen diesen beiden Adressen wird mit IPsec geschützt. Das Beispiel zeigt die Perspektive der nicht-globalen Zone, die mit IP-Adresse 10.1.1.1 verknüpft ist.

Mit den folgenden Schritten können Sie IPsec und IKE zwischen einem Paar mit angegebenen nicht-globalen Zonen (virtuellen Maschinen) konfigurieren und verwenden.

1. Definieren Sie die IPsec-Sicherheitsrichtlinie.

Definieren Sie die Sicherheitsrichtlinie, die zwischen dem Paar kommunizierender Zonen durchgesetzt wird.

In diesem Beispiel wird die gesamte Kommunikation zwischen 10.1.1.1 und 10.1.1.2 verschlüsselt:

```
{laddr 10.1.1.1 raddr 10.1.1.2}
ipsec{encr_algs aes encr_auth_algs sha256 sa shared}
```

2. Speichern Sie die Richtlinie in der Datei `/etc/inet/ipsecinit.conf`.

3. Prüfen Sie, ob die IPsec-Richtlinie syntaktisch korrekt ist.

Beispiel:

```
# ipsecconf -c -f ipsecinit.conf
```

4. Konfigurieren Sie den IKE-(Internet Key Exchange-)Service.

Konfigurieren Sie den Service gemäß den Host- und Algorithmeinstellungen in der Datei `/etc/inet/ike/config`.

```
{ label "ipsec"
local_id_type ip
remote_addr 10.1.1.2
pi_xform { auth_method preshared oakley_group 5
auth_alg sha256 encr_alg aes } }
```

5. Konfigurieren Sie den vorinstallierten Schlüssel.

Bevor IPsec aktiviert werden kann, muss Schlüsselmaterial auf beiden Peer-Knoten vorinstalliert werden, damit sie einander authentifizieren können.

Die Oracle Solaris IKE-Implementierung unterstützt eine Vielzahl von Schlüsseltypen, einschließlich vorinstallierten Schlüsseln und Zertifikaten. Der Einfachheit halber verwendet dieses Beispiel vorinstallierte Schlüssel, die in der Datei `/etc/inet/secret/ike.preshared` gespeichert sind. Unternehmen, die jedoch strengere Formen der Authentifizierung verwenden möchten, können dies tun.

Bearbeiten Sie die Datei `/etc/inet/secret/ike.preshared`, und geben Sie die vorinstallierten Schlüsselinformationen ein. Beispiel:

```
{
localidtype IP
localid 10.1.1.1
remoteid type IP
key "This is an ASCII phrAz, use str0ng p@sswords"
}
```

6. Aktivieren Sie IPsec- und IKE-Services auf beiden Peers.

Die Services müssen auf beiden kommunizierenden Peers aktiviert werden, bevor eine verschlüsselte Kommunikation möglich ist.

Beispiel:

```
# svcadm enable svc:/network/ipsec/policy:default
# svcadm enable svc:/network/ipsec/ike:default
```

Zugriff kontrollieren

In diesen Themen werden die Zugriffskontrollfunktionen in MiniCluster beschrieben:

- [Ändern der Standard-Oracle ILOM-root-Passwörter \[27\]](#)
- [EEPROM-Passwörter konfigurieren \[28\]](#)
- [„Benutzer-Provisioning“ \[29\]](#)
- [„MCMU-Benutzergenehmigungsprozess“ \[30\]](#)
- [„Rollenbasierte Zugriffskontrolle“ \[31\]](#)
- [„Benutzerkonten“ \[32\]](#)
- [„Benutzerauthentifizierung und Passworrichtlinien“ \[33\]](#)
- [Prüfen von Oracle Solaris-Benutzerrollen \[33\]](#)
- [„Sicheres Löschen von VMs“ \[34\]](#)
- [Hostbasierte Firewallregeln überprüfen \[34\]](#)
- [Prüfen der Verified Boot-Umgebung \[36\]](#)
- [Begrenzen des Zugriffs auf Shared Storage \[37\]](#)

▼ Ändern der Standard-Oracle ILOM-root-Passwörter

Bei der Lieferung des Systems sind den Oracle ILOM-Root-Konten Standardpasswörter auf beiden Knoten zugewiesen. Dadurch kann der Installationsprozess mit einem vorhersehbaren Konto für den anfänglichen Zugriff ausgeführt werden. Ändern Sie unmittelbar nach der Installation die Standardpasswörter, um optimale Sicherheit zu gewährleisten.

1. **Melden Sie sich bei Oracle ILOM auf Knoten 1 als root an.**

Mit dem Befehl `ssh` stellen Sie die Verbindung zu Oracle ILOM her.

Um die Hostnamen von Oracle ILOM abzurufen, wählen Sie in der Dienstprogramm-BUI "System Settings -> System Information" (Systemeinstellungen -> Systeminformationen) aus. Die Hostnamen werden unter der ILOM-Spalte aufgeführt.

Syntax:

```
% ssh root@node1_ILOM_hostname_or_IPaddress
```

Geben Sie das Standard-Oracle ILOM-Root-Passwort ein: `welcome1`

2. Ändern Sie das Oracle ILOM root-Passwort.

```
-> set /SP/users/root password
Enter new password: *****
Enter new password again: *****
```

3. Wiederholen Sie die Schritte, um das Oracle ILOM root-Passwort auf Knoten 2 zu ändern.

4. Aktualisieren Sie den Oracle Engineered Systems-Hardwaremanager mit den neuen Passwörtern.

Siehe „[Update Component Passwords](#)“ in *Oracle MiniCluster S7-2 Administration Guide*.

▼ EEPROM-Passwörter konfigurieren

Jeder MiniCluster-Knoten weist einen EEPROM auf (manchmal auch als OpenBoot PROM bezeichnet). Dabei handelt es sich um einfache Firmware, die einige Konfigurationsparameter und Treiber enthält, die das Booten des Systems erleichtern. Standardmäßig ist die EEPROM-Passwortfunktion deaktiviert.

In sicheren Umgebungen können Sie mit dieser Prozedur die Passwortfunktion aktivieren und ein Passwort festlegen. Das Passwort wird automatisch aktiviert und auf beide Knoten angewendet.

Diese Prozedur ersetzt ältere Methoden, bei denen das Passwort entweder in der OpenBoot ok-Eingabeaufforderung oder in Oracle Solaris mit dem `eeeprom`-Befehl festgelegt wurde.

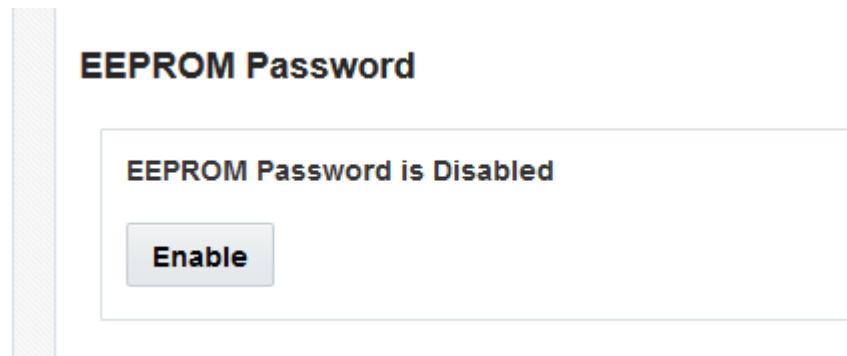


Achtung - Vergessen Sie das Passwort nicht. Wenn Sie das Passwort vergessen, müssen Sie den Support anrufen, damit das System wieder gebootet werden kann.

Anmerkung - Hier wird beschrieben, wie Sie die Passwörter über die MCMU-BUI festlegen. Sie können auch den Befehl `mcmu security -e` verwenden.

1. Melden Sie sich als primärer Admin, wie `mcinstall`, bei MCMU an.

2. Wählen Sie im Navigationsbereich "System Settings -> Security" (Systemeinstellungen -> Sicherheit).



3. Führen Sie eine der folgenden Aktionen aus:
 - Um das Passwort zu aktivieren und festzulegen: Klicken Sie auf "Enable" (Aktivieren), geben Sie das Passwort zweimal ein, und klicken Sie auf "Set Password" (Passwort festlegen).
 - Um die Funktion zu deaktivieren: Klicken Sie auf "Disable" (Deaktivieren) und dann auf "Confirm" (Bestätigen).
 - Um ein vorhandenes Passwort zu ändern: Klicken Sie auf "Change Passwort" (Passwort ändern), geben Sie das neue Passwort zweimal ein, und klicken Sie auf "Update" (Aktualisieren).

Benutzer-Provisioning

Während der Installation von MiniCluster fordert der Installationsprozess Sie auf, den ersten MCMU-Benutzer namens `mcinstall` zu erstellen und zu registrieren. Die demografischen Informationen des Benutzers, einschließlich E-Mail-Adresse und Telefonnummer werden erfasst. Der `mcinstall`-Benutzer ist das erste Primäradministratorkonto. Bei der ersten Anmeldung von `mcinstall` fordert das Dienstprogramm `mcinstall` auf, ein neues Passwort gemäß den Oracle Solaris-Passwortrichtlinien zu erstellen, die mit dem Sicherheitsprofil verknüpft sind.

Während der Registrierung des `mcinstall`-Benutzers werden Sie aufgefordert, eine Person als MCMU-Supervisor anzugeben. Der Supervisor wird nur mit einem Namen und einer E-Mail-Adresse identifiziert. Der Supervisor ist kein MCMU-Benutzer und hat keine Anmeldezugangsdaten.

Sowohl für den Supervisor als auch für die mcinstall-Benutzer sind echte Personennamen und gültige E-Mail-Adressen festgelegt.

Wenn neue MCMU-Benutzer bereitgestellt werden, wird jedes Benutzerkonto mit einer Rolle des Primäradministrators oder Sekundäradministrators zugewiesen (siehe „[Rollenbasierte Zugriffskontrolle](#)“ [31]). Bevor das neue Konto aktiviert wird, müssen der mcinstall-Benutzer und der Supervisor beide das neue Benutzerkonto über eine URL genehmigen, die ihnen in einer E-Mail zugesendet wird (siehe „[MCMU-Benutzergenehmigungsprozess](#)“ [30]). Bei der ersten Anmeldung wird der Benutzer gezwungen, ein Passwort festzulegen, das den MCMU-Passwortrichtlinien entspricht. Siehe „[Benutzerauthentifizierung und Passwortrichtlinien](#)“ [33].

MCMU-Benutzergenehmigungsprozess

Alle MCMU-Benutzerkonten müssen von zwei Personen genehmigt werden, dem MCMU-Supervisor und dem Primäradministrator. Der Prozess läuft wie folgt ab:

1. Der künftige Benutzer (oder ein MCMU-Administrator an seiner Stelle) ruft die MCMU-Registrierungsseite auf und gibt die folgenden obligatorischen Details an:
 - MCMU-Benutzername
 - E-Mail-Adresse
 - Vor- und Nachname
 - Telefonnummer
 - MCMU-Rolle
2. MCMU sendet dem MCMU-Supervisor und Primäradministrator eine E-Mail, in der sie zur Genehmigung oder Ablehnung aufgefordert werden. Die E-Mail umfasst eine URL zu der MCMU-Genehmigungs-/Ablehnungsfunktion und umfasst eine eindeutige Schlüssel-ID.
3. Wenn der Supervisor und der Primäradministrator beide das Konto genehmigen, wird das Benutzerkonto aktiviert, und MCMU sendet dem neuen Benutzer eine E-Mail, in der die Aktivierung des Kontos bestätigt wird. Der Benutzer erhält ein MCMU-Konto, auf das über die MCMU-BUI oder CLI zugegriffen werden kann. Der Benutzer erhält auch ein Oracle Solaris-Benutzerkonto. Wenn der Benutzer in einem Unternehmens-LDAP enthalten ist und MiniCluster mit einem LDAP-Client konfiguriert ist, kann der Benutzer nur LDAP für das Oracle Solaris-Konto verwenden.

Alle registrierten Benutzer sind im MCMU-Repository gespeichert. Ein MCMU-Administrator kann die Benutzer, einschließlich deren Rollen und Supervisor prüfen, indem er "MCMU System Settings -> User Accounts" (MCMU-Systemeinstellungen -> Benutzerkonten) anzeigt. Beispiel:

User Accounts

User Name ▲	Role	Date Joined	Last Login	Email	Phone	Supervisor
mcinstall	root	06-10-2016 02:02	07-10-2016 20:59	mr.smith@company.com	0000000000	mc5super
mc5super	supervisor	06-10-2016 02:03	06-10-2016 02:03	hr@company.com		
jr-admin	tadmin	07-10-2016 20:38	07-10-2016 20:51	jr.jones@company.com	4081111111	mc5super
sec-admin	auditor	07-10-2016 20:41	07-10-2016 20:41	security.boss@company.com	4082222222	mc5super
blue	root	07-10-2016 20:43	07-10-2016 20:43	blue.jeans@company.com	4083333333	mc5super
green	mcadmin	07-10-2016 20:44	07-10-2016 20:44	green.jeans@company.com	4084444444	mc5super

Die nachfolgenden Themen in diesem Abschnitt beschreiben, wie diese Aufgaben ausgeführt werden.

Rollenbasierte Zugriffskontrolle

In MiniCluster ist kein `root`-Benutzer vorhanden. Stattdessen ist `Root` eine Rolle und ist den MCMU-Benutzern zugewiesen, die als Primäradministratoren registriert sind.

Wenn Sie einen MCMU-Benutzer erstellen, weisen Sie dem Benutzer eine dieser Rollen zu:

- Primäradministrator (`root`-Rolle)** - Die `root`-Rolle definiert die Rechte und Berechtigungen von Primäradministratoren des MiniCluster-Systems, einschließlich aller Serverknoten, Netzwerke, Datenbank und Speicher. Benutzer mit der `root`-Rolle können alle Installations- und kritischen administrativen Vorgänge ohne jegliche Einschränkungen ausführen. Als Primäradministratoren können sie Vorgänge delegieren und das Hinzufügen und Löschen von Benutzern genehmigen, einschließlich neuen Primär- und Sekundäradministratoren. Der Benutzer muss sich mit seinen eigenen Zugangsdaten anmelden. Alle ausgeführten Aktionen und Vorgänge werden basierend auf der Benutzer-ID, nicht der Rollen-ID, geloggt und auditiert.
- Sekundäradministrator (`mcadmin`-Rolle)** - Diese Rolle definiert die Rechte und Berechtigungen der Sekundäradministratoren der MiniCluster-Domains und nicht-globalen Zonen. Standardmäßig ermöglicht diese Rolle nur schreibgeschützten Zugriff auf MCMU. Alle ausgeführten Aktionen und Vorgänge werden basierend auf der Benutzer-ID, nicht der Rollen-ID, geloggt und auditiert.
- Mandantenadministrator (`tadmin`-Rolle)** - Diese Rolle definiert die Rechte und Berechtigungen des Administrators einer MiniCluster-VM. Diese Rolle definiert die Rechte und Berechtigungen eines VM-Administrators, der die täglich anfallenden administrativen Vorgänge bei der Unterstützung der Anwendungsinstallationen und des Anwendungs-Deployments abwickelt. Alle Aktionen werden basierend auf Benutzer-ID und nicht auf Rollen-ID auditiert.

- Auditorrolle (auditor):** Benutzer mit dieser Rolle haben nur Zugriff auf die MCMU-BUI-Auditprüfungsseite, wo sie den Auditpoolstatus anzeigen und Berichte für Benutzeraktivitäten generieren können. Nur Benutzer mit dieser Rolle können auf die Auditprüfungsseite zugreifen. Auditoren können (mit Ausnahme der Auditseite) nicht auf MCMU zugreifen oder sich bei Kernel-Zonen oder VMs anmelden.

Benutzerkonten

MiniCluster umfasst die in dieser Tabelle aufgeführten Benutzerkonten.

Benutzer	Passwort	Rolle	Beschreibung
mcinstall	Das Passwort wird während der Installation konfiguriert. Es kann über MCMU zurückgesetzt und geändert werden.	Root	<p>Beim Installationsprozess müssen Sie <code>mcinstall</code> als primären MCMU-Administrator sowie ein Passwort erstellen. Dieses Konto ist für den primären Administrator von MCMU gedacht.</p> <p>Dieses Benutzerkonto wird für folgende Aktivitäten verwendet:</p> <ul style="list-style-type: none"> Ausführung der Systeminitialisierung bei der Installation, indem <code>installmc</code> ausgeführt wird. Administration des Systems, einschließlich VMs, über die MCMU-BUI und <code>mcmu-CLI</code>. Zur Annahme der <code>root</code>-Rolle (mit <code>su</code> zu <code>Root</code> wechseln) bei Anwendungs-VMs sowie in der globalen Zone und in Kernel-Zonen für Superuser-Berechtigungen.
MCMU-Supervisor - Kontoname wird bei der Installation bestimmt	N/V	N/V	<p>In der MiniCluster-Software ist der Supervisorbenutzer nur ein Benutzername und eine E-Mail-Adresse. Er stellt keine Anmeldezugangsdaten dar. Mit diesem Konto können Sie eine zweite Ebene im MCMU-Benutzergenehmigungsprozess bereitstellen.</p> <p>Der Benutzer erhält jedes Mal eine E-Mail, wenn ein neuer MCMU-Benutzer erstellt wird. Der neue Benutzer muss vom Supervisor und Primäradministrator genehmigt werden, damit das Benutzerkonto aktiviert wird.</p> <p>Mit diesem Konto können Sie eine zweite Schicht in dem MCMU-Benutzergenehmigungsprozess bereitstellen, indem Sie eine andere Person als den Primäradministrator als Supervisor zuweisen.</p>
(Optional) Mandantenadministrator - Kontoname wird bei der Benutzerregistrierung bestimmt	Bei anfänglicher Anmeldung bestimmt.	tadmin	<p>Dieser Benutzer kann alle Aktivitäten nach der Installation nur auf VMs ausführen.</p> <p>Dieser Benutzer kann nicht auf die globale Zone oder Kernel-Zonen zugreifen und weder die MCMU-BUI noch CLI ausführen.</p>
(Optional) Sekundäradministrator - Kontoname wird bei der Benutzerregistrierung bestimmt	Bei anfänglicher Anmeldung bestimmt.	mcadmin	<p>Wenn ein MCMU-Benutzer als sekundärer Administrator erstellt und zugewiesen wird und nur schreibgeschützten Zugriff auf nicht globale Zonen hat.</p>
oracle	Das Passwort ist identisch mit	Root	Dieses Benutzerkonto wird für folgende Aktivitäten verwendet:

Benutzer	Passwort	Rolle	Beschreibung
	dem mcinstall-Passwort.		<ul style="list-style-type: none"> ■ Wird als anfängliches Anmeldekonto für Datenbank-VMs verwendet, aus dem Sie die Datenbank-VMs mit einer Datenbank, Daten und anderen Konten nach Bedarf konfigurieren können. ■ Zur Annahme der Root-Rolle (mit <code>su</code> zu Root wechseln) in Datenbank-VMs für Superuser-Berechtigungen.

Das Standard-MCMU-Passwort, das bei der ersten Anmeldung verwendet wird, ist `welcome1`. Nachdem `welcome1` eingegeben wurde, zwingt das Dienstprogramm den Benutzer, ein neues Passwort zu erstellen, das den Passwortrichtlinien entspricht. Siehe „[Benutzerauthentifizierung und Passwortrichtlinien](#)“ [33].

Alle Aktionen, die von allen MCMU-Benutzern ausgeführt werden, werden mit der ID des Benutzers geloggt. Informationen zu Auditberichten finden Sie unter [Auditing- und Compliance-Reporting](#) [39].

Anmerkung - MCMU-Benutzerkonten werden nicht für den Routinegebrauch des Systems verwendet, wie der Verwendung von Anwendungen und Datenbanken. Diese Benutzerkonten werden über Oracle Solaris, die Anwendung, die Datenbank in den VMs und über die Namensservices Ihrer Site verwaltet.

Benutzerauthentifizierung und Passwortrichtlinien

Allen in MiniCluster bereitgestellten Benutzern wird eine Rolle mit strengen Passwortrichtlinien und Passwortverschlüsselung zugewiesen, die durch das Sicherheitsprofil durchgesetzt wird.

Die Standardsicherheitsrichtlinie legt diese MCMU-Passwortanforderungen fest:

- Muss mindestens 14 Zeichen enthalten
- Muss mindestens ein numerisches Zeichen enthalten
- Muss mindestens einen Großbuchstaben enthalten
- Muss sich um mindestens drei Zeichen von einem vorherigen Passwort unterscheiden
- Darf nicht mit den zehn vorherigen Passwörtern übereinstimmen

Alle Benutzer melden sich bei dem Oracle Solaris-Konto nur mit ihrem eigenen Passwort an.

▼ Prüfen von Oracle Solaris-Benutzerrollen

1. **Melden Sie sich bei der globalen MiniCluster-Zone an, und übernehmen Sie die Root-Rolle.**

Weitere Einzelheiten finden Sie in *Oracle MiniCluster S7-2 - Administrationshandbuch*.

2. Prüfen Sie die Liste der verfügbaren Rollen.

```
# logins -r
```

3. Prüfen Sie Benutzerrolle und Passwort für die Authentifizierung:

```
# grep root /etc/user_attr
root:::audit_flags=lo\:no;type=role;roleauth=user
mcinstall:::auths=solaris.system.maintenance;roles=root
```

Sicheres Löschen von VMs

Nur der MCMU-Primäradministrator kann VMs und VM-Gruppen löschen. Wenn eine VM-Komponente gelöscht wird, werden die entsprechenden Schlüssel automatisch gelöscht, und eine E-Mail wird an den Primäradministrator gesendet.

Um dieses Feature zu prüfen, melden Sie sich vor dem Löschen einer VM-Komponente bei der MCMU-BUI als Primäradministrator an und zeigen die Verschlüsselungsschlüssel an (System Settings -> Security) (Systemeinstellungen -> Sicherheit). Löschen Sie die VM-Komponente, und zeigen Sie die Schlüssel dann erneut an. Die VM und das verknüpfte Schlüssellabel für die gelöschte Komponente werden nicht mehr angezeigt.

▼ Hostbasierte Firewallregeln überprüfen

Alle Computing-Umgebungen, einschließlich der globalen Zonen, Kernel-Zonen und nicht-globalen Zonen werden automatisch mit IPFilter-Firewalls konfiguriert. Ein Handbuch ist nicht erforderlich.

Führen Sie die folgenden Schritte aus, um die verwendeten IPFilter zu prüfen.

1. Melden Sie sich bei der globalen Zone auf Knoten 1 als `mcinstall` an, und übernehmen Sie die `root`-Rolle.

Anweisungen zur Anmeldung bei Oracle ILOM finden Sie im *Oracle MiniCluster S7-2 - Administrationshandbuch*.

```
% ssh mcinstall@mc4-n1
Password: *****
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3      June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
```

```
Password: *****
#
```

2. Prüfen Sie die IPFilter-Konfiguration.

Stellen Sie sicher, dass die Regeln in der Datei `/etc/ipf/ipf.conf` mit der folgenden Bildschirmausgabe übereinstimmen.

```
# cat /etc/ipf/ipf.conf
block in log on all
block out log on ipmppub0 all
pass in quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 443 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1159 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1158 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port 5499 >< 5550 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1522 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1523 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp/udp from any to any port = domain keep state
pass in quick on ipmppub0 proto icmp icmp-type echo keep state
pass out quick on ipmppub0 proto icmp icmp-type echo keep state
pass in quick on ipmppub0 proto udp from any to any port = 123 keep state
pass out quick on ipmppub0 proto udp from any to any port = 123 keep state
block return-icmp in proto udp all
```

3. Prüfen Sie, ob die IPF-Services online sind.

```
# svcs | grep svc:/network/ipfilter:default
online      22:13:55 svc:/network/ipfilter:default
# ipfstat -v
bad packets:          in 0      out 0
IPv6 packets:        in 0 out 0
input packets:       blocked 2767 passed 884831 nomatch 884798 counted 0 short 0
output packets:      blocked 0 passed 596143 nomatch 595516 counted 0 short 0
input packets logged: blocked 0 passed 0
output packets logged: blocked 0 passed 0
packets logged:      input 0 output 0
log failures:        input 0 output 0
fragment state(in):  kept 0 lost 0 not fragmented 0
fragment reassembly(in): bad v6 hdr 0 bad v6 ehdr 0 failed reassembly 0
fragment state(out): kept 0 lost 0 not fragmented 0
packet state(in):    kept 0 lost 0
packet state(out):   kept 0 lost 0
ICMP replies: 0      TCP RSTs sent: 0
Invalid source(in): 0
Result cache hits(in): 0      (out): 0
IN Pullups succeeded: 0      failed: 3462
OUT Pullups succeeded: 0      failed: 0
Fastroute successes: 0      failures: 0
TCP cksum fails(in): 0      (out): 0
IPF Ticks: 92894
Packet log flags set: (0)
none
```

4. Stellen Sie sicher, dass ohne Änderung der Firewallregeln auf die Datenbanken und Anwendungen zugegriffen werden kann.

▼ Prüfen der Verified Boot-Umgebung

Oracle Solaris Verified Boot ist eine Antischadsoftware- und Integritätsfunktion, die das Risiko der Einschleusung von böswilligen oder versehentlich geänderten kritischen Boot- und Kernel-Komponenten verringert. Diese Funktion prüft die werksseitig signierten kryptografischen Signaturen von Firmware, Bootsystem und Kernel.

Standardmäßig sind globale MiniCluster-Zonen mit Oracle Solaris Verified Boot konfiguriert. Wenn Sie prüfen möchten, ob das System mit Verified Boot konfiguriert ist, führen Sie die folgenden Schritte aus.

1. Melden Sie sich auf einem der Knoten bei Oracle ILOM an.

Anweisungen zur Anmeldung bei Oracle ILOM finden Sie im *Oracle MiniCluster S7-2 - Administrationshandbuch*.

2. Prüfen Sie die Verified Boot-Konfiguration in Oracle ILOM.

Stellen Sie sicher, dass `boot_policy` auf `warning` festgelegt ist.

```
-> show /HOST/verified_boot

/HOST/verified_boot
  Targets:
    system_certs
    user_certs

  Properties:
    boot_policy = warning

  Commands:
    cd
    show
```

3. Prüfen Sie die Einstellung der Verified Boot-Richtlinie.

Stellen Sie sicher, dass `module_policy` auf `enforce` festgelegt ist.

```
-> show /HOST/verified_boot module_policy

/HOST/verified_boot
  Properties:
    module_policy = enforce
```

4. Starten Sie die Hostkonsole, um auf die globale Zone zuzugreifen.

Melden Sie sich als `mcinstall` an.

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

Serial console started. To stop, type #.

Minicuster Setup successfully configured
mc4-n1 console login: mcinstall
Password: *****
Last login: Tue Jun 28 10:17:38 2016 on rad/47
Oracle Corporation      SunOS 5.11      11.3      June 2016
```

```
Miniclustert Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall %
```

5. Prüfen Sie die globale Zone auf den Nachweis, dass das System in einer Verified Boot-Umgebung gestartet wurde.

Prüfen Sie die Datei `messages` auf die Zeichenfolge `NOTICE: Verified boot enabled; policy=warning`.

```
mcinstall % cat /var/adm/messages | grep Verified
Jun 29 11:39:15 mc4-n1 unix: [ID 402689 kern.info] NOTICE: Verified boot enabled;
policy=warning
```

▼ Begrenzen des Zugriffs auf Shared Storage

MiniCluster umfasst ein Speicherarray mit einer Mischung aus SSDs und HDDs. Die HDDs können zum Bereitstellen von Shared Storage für VMs konfiguriert werden.

MiniCluster umfasst eine Funktion für die Shared Storage-Isolierung: ein Umschalter, der die Isolierung von Shared Storage erleichtert, der nur auf globale und Kernel-Zonen angewendet wird. So können Sie eine sicherheits- und compliancefähige VM-Gruppenumgebung isolieren, sodass keine Dateien für globale und Kernel-Zonen freigegeben werden. Dadurch wird sichergestellt, dass VM-Gruppen nicht mehr NFS-Mounts zugeordnet sind und dass die NFS-Services deaktiviert werden.

Bei hochsicheren Umgebungen aktivieren Sie Shared Storage für Datenbank-VMs und Anwendungs-VMs nicht. Wenn Shared Storage aktiviert ist, muss das Dateisystem für die VMs in schreibgeschützter Form zugänglich sein. Anweisungen zum Aktivieren oder Deaktivieren des Shared Storage finden Sie im *Oracle MiniCluster S7-2 Administration Guide* unter: http://docs.oracle.com/cd/E69469_01.

Das Verzeichnis `/sharedstore` ist der Einhängpunkt für den Shared Storage:

- **Je nach Ihren Sicherheitsanforderungen konfigurieren Sie den Shared Storage unter Berücksichtigung dieser Empfehlungen:**
 - Stellen Sie sicher, dass der Shared Storage nicht für Datenbank-VMs und Anwendungs-VMs verfügbar ist, oder dass er schreibgeschützt ist.
 - In Production Deployments müssen Sie sicherstellen, dass keine Kernel-Zonen über öffentliche Netzwerke oder direkt für Clientzugriff zugänglich sind. Jeder direkte Zugriff auf Shared Storage-Services über öffentliche Netzwerke oder Clientzugriff muss beendet werden. Wenn virtuelle Maschinen Zugriff auf das `/sharedstore`-Dateisystem über NFS erfordern, stellen Sie sicher, dass sie über IPSEC/IKE-Kanäle erleichtert werden.

Auditing- und Compliance-Reporting

Diese Themen beschreiben die Auditing- und Compliance-Reporting-Funktionen, die in MiniCluster verfügbar sind:

- [Prüfen der Auditrichtlinien \[39\]](#)
- [Auditlogs prüfen \[40\]](#)
- [Auditberichte generieren \[41\]](#)
- [\(Falls erforderlich\) Aktivieren eines FIPS-140-konformen Vorgangs \(Oracle ILOM\) \[43\]](#)
- [„FIPS-140-2 Level 1-Compliance“ \[45\]](#)

▼ Prüfen der Auditrichtlinien

Die Auditrichtlinie wird während der Installation der globalen Zonen und nicht globalen Zonen bei Auswahl eines Complianceprofils (Standard-CIS-Äquivalent oder PCI-DSS) konfiguriert.

Um zu prüfen, ob Auditrichtlinien aktiviert sind, führen Sie folgende Schritte aus.

1. **Melden Sie sich bei der globalen Zone als `mcinstall` an, und nehmen Sie die `root`-Rolle an.**

Anweisungen zur Anmeldung bei Oracle ILOM finden Sie im *Oracle MiniCluster S7-2 - Administrationshandbuch*.

```
% ssh mcinstall@mc4-n1
Password: *****
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3      June 2016
Miniclustert Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: *****
#
```

2. **Prüfen Sie, ob der Auditservice online ist.**

```
# svcs | grep svc:/system/auditd
online          22:14:37  svc:/system/auditd:default
```

3. **Prüfen Sie, ob das Audit-Plug-in aktiv ist.**

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile (active)
Attributes: p_age=0h;p_dir=/var/audit;p_fsize=0;p_minfree=1
```

4. Prüfen Sie die aktiven Auditrichtlinien.

```
# auditconfig -getpolicy
configured audit policies = argv,cnt,perzone,zonename
active audit policies = argv,cnt,perzone,zonename
```

5. Prüfen Sie, ob alle Rollen für die cusa-Auditrichtlinie erfasst sind.

```
# userattr audit_flags root
cusa:no
# userattr audit_flags mcadmin
fw,fc,fd,ps,lo,ex,ua,as,cusa:no
```

▼ Auditlogs prüfen

1. Melden Sie sich bei der globalen Zone als mcinstall an, und nehmen Sie die root-Rolle an.

Anweisungen zur Anmeldung bei Oracle ILOM finden Sie im *Oracle MiniCluster S7-2 - Administrationshandbuch*.

```
% ssh mcinstall@mc4-n1
Password: *****
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation SunOS 5.11 11.3 June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: *****
#
```

2. Verwenden Sie den auditreduce-Befehl wie dargestellt.

Dies ist die Syntax zur Anzeige der Auditlogs:

```
auditreduce -z vm_name audit_file_name | praudit -s

# cd /var/share/audit
#
# ls
20160628051437.not_terminated.mc4-n1
#
# auditreduce -z dbvmg1-zone-1-mc4-n1 20160628051437.not_terminated.mc4-n1 | praudit -s
file,2016-06-27 22:58:53.000 -07:00,
header,127,2,AUE_zone_state,,mc4-n1.us.oracle.com,2016-06-27 22:58:53.354 -07:00
subject,mcinstall,root,root,root,root,26272,415120213,9462 65558 mc4-n1.us.oracle.com
text,boot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
header,88,2,AUE_zone_state,na,mc4-n1.us.oracle.com,2016-06-27 23:02:30.767 -07:00
text,reboot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
```


file, 2016-06-27 23:02:30.000 -07:00,

▼ Auditberichte generieren

Verwenden Sie diese Prozedur, um Auditberichte für einen Knoten oder für individuelle VMs und globale Zonen zu generieren.

1. Melden Sie sich als Benutzer mit Auditorrolle beim MCMU an.

Informationen zu MCMU-Benutzern und -Rollen finden Sie im *Oracle MiniCluster S7-2 Administration Guide* unter: http://docs.oracle.com/cd/E69469_01.

2. Wählen Sie im Navigationsbereich " System Settings -> Security" (Systemeinstellungen -> Sicherheit) aus.

Die Seite "Audit Review" (Auditprüfung) wird angezeigt.

Anmerkung - Nur MCMU-Benutzer mit der Auditorrolle können diese Seite anzeigen.

The screenshot shows the Oracle MiniCluster Configuration Utility interface. At the top, it says 'ORACLE MiniCluster Configuration Utility' and 'English mclauditor'. The main content area is titled 'Welcome to the MiniCluster Audit Review!' and contains two sections:

Audit Pool Status

hostname	used	available
mcl1-n1	12M	709G
mcl1-n2	6.5M	709G

Generate Audit Records

hostname	user	generate
mc1-n1		Generate Report for all users
global		Generate Report for all users
azgt1-vm1-mcl1-n1		Generate Report for all users
mc1-n2		Generate Report for all users
global		Generate Report for all users

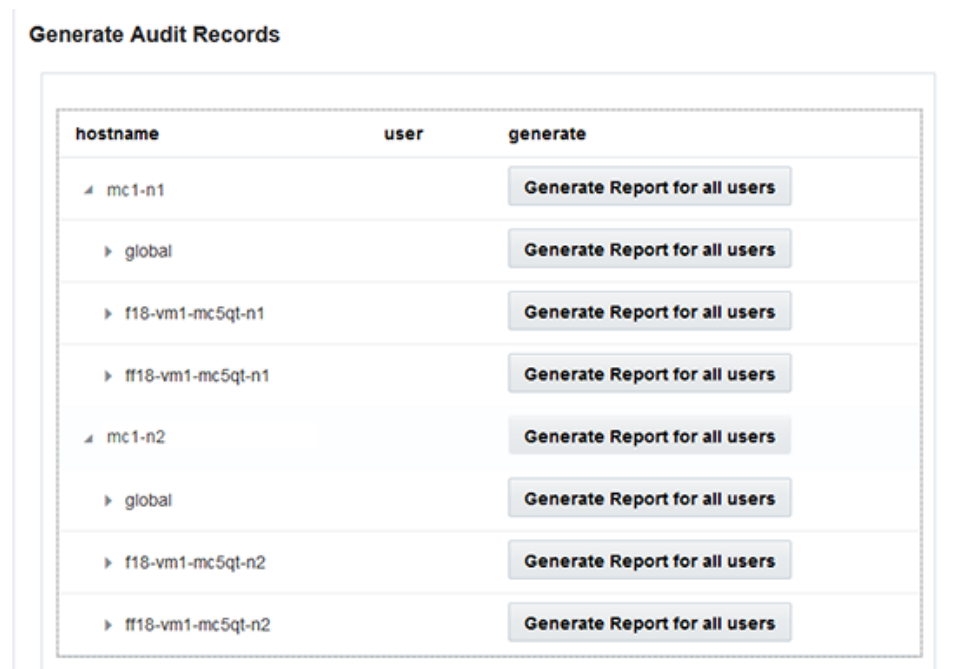
3. Prüfen Sie den Abschnitt "Audit Pool Status" (Auditpoolstatus).

Dieser Abschnitt enthält den belegten und den verfügbaren Speicherplatz für Auditpools auf jedem Knoten.

4. Um einen Bericht für den gesamten Knoten zu generieren, klicken Sie auf die Schaltfläche "Generate" (Generieren) für einen der Knoten, und gehen Sie zu Schritt 6

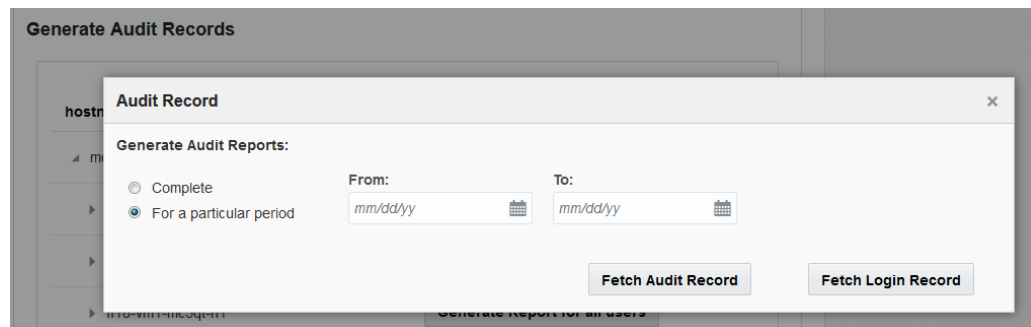
Alternativ dazu können Sie auch einen Bericht für eine bestimmte VM oder Zone generieren. Siehe [Schritt 5](#)

5. **Gehen Sie wie folgt vor, um einen Bericht für eine bestimmte VM oder globale Zone zu generieren.**
 - a. **Klicken Sie auf das Dreieck neben einem Knoten, um die Ansicht einzublenden.**



- b. **Klicken Sie für die VM oder globale Zone auf "Generate Report for all users" (Bericht für alle Benutzer generieren).**

6. Konfigurieren Sie im Dialogfeld "Audit Record" (Auditdatensatz) die Auditdatensatzparameter.



Sie haben die folgenden Optionen:

- **Complete** (Vollständig): Wählen Sie dies, wenn der Bericht alle Auditdatensätze umfassen soll.
- **For a particular period** (Für einen bestimmten Zeitraum): Wählen Sie dies, wenn Sie einen Zeitraum angeben möchten, und geben Sie dann das Anfangs- und das Enddatum ein.

7. Klicken Sie auf eine der Schaltflächen zum Abrufen.

Sie haben die folgenden Optionen:

- **Fetch Audit Record** (Auditdatensatz abrufen): Generiert einen vollständigen Auditdatensatz.
- **Fetch Login Record** (Anmeldedatensatz abrufen): Generiert Benutzeraktivitäten, wie Anmeldungen, Abmeldungen und Benutzeraktionen.

8. Klicken Sie auf die Schaltfläche "Click Here" (Hier klicken), und wählen Sie die Download-XML-Datei.

Die XML-Datei kann in Auditanalyseanwendungen, wie Oracle Audit Vault, importiert werden.

9. Klicken Sie auf "Close" (Schließen).

▼ (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 "Nicht unterstützte Funktionen bei aktiviertem FIPS-Modus".

Siehe auch „[FIPS-140-2 Level 1-Compliance](#)“ [45].



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.**
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
```

FIPS-140-2 Level 1-Compliance

Die in MiniCluster 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 Cloudserviceprovider 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 \(Oracle ILOM\) \[43\]](#) verwiesen.

In dieser Tabelle werden FIPS-genehmigte Algorithmen aufgeführt, die von Oracle Solaris in MiniCluster 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

Schlüssel oder CSP	Zertifikatsnummer	
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.

Bewerten der Sicherheitscompliance

In diesen Themen wird die MiniCluster-Sicherheitsbenchmarkfunktion beschrieben:

- „Sicherheitscompliancebenchmarks“ [47]
- Planen einer Sicherheitscompliancebenchmark (BUI) [48]
- Anzeigen von Benchmarkberichten (BUI) [49]

Sicherheitscompliancebenchmarks

Wenn das System installiert ist, wird ein Sicherheitsprofil (PCI-DSS, CIS-Äquivalent oder DISA-STiG) ausgewählt, und das System wird automatisch gemäß diesem Sicherheitsprofil konfiguriert. Um sicherzustellen, dass das System weiter gemäß den Sicherheitsprofilen arbeitet, stellt MCMU die Möglichkeit bereit, Sicherheitsbenchmarks auszuführen und auf die Benchmarkberichte zuzugreifen. Sie können die Benchmarks mit der MCMU-BUI und CLI verwalten.

Die Ausführung von Sicherheitsbenchmarks bietet folgende Vorteile:

- Sie können den aktuellen Sicherheitsstatus der Datenbank- und Anwendungs-VMs auswerten und bewerten.
- Die Sicherheitscompliancechecks unterstützen PCI-DSS-, CIS-äquivalente Standards (Standard) und DISA-STiG basierend auf der bei der Installation konfigurierten Sicherheitsebene.
- Die Sicherheitscompliancechecks werden automatisch ausgeführt, wenn das System gestartet wird und können auf Anforderung oder in geplanten Intervallen ausgeführt werden.
- Nur für MCMU-Primäradministratoren verfügbar, können Compliancebewertungen und -berichte jederzeit über die MCMU-BUI aufgerufen werden.
- Die Complianceberichte enthalten Remediation-Empfehlungen.

Anmerkung - Das DISA-STIG-Profil wird derzeit geprüft. Verwenden Sie dieses Profil nur zur experimentellen Nutzung in Nicht-Production-Umgebungen.

▼ Planen einer Sicherheitscompliancebenchmark (BUI)

Mit dieser Prozedur können Sie eine Sicherheitsbenchmark mit der MCMU-BUI planen. Wenn Sie stattdessen die MCMU-CLI verwenden möchten, finden Sie die entsprechenden Anweisungen in *Oracle MiniCluster S7-2 - Administrationshandbuch*.

1. Melden Sie sich als Primäradministrator bei der MCMU-BUI an.

Anweisungen finden Sie in *Oracle MiniCluster S7-2 - Administrationshandbuch*.

2. Scrollen Sie auf der Homepage nach unten zu dem Bereich "Complianceinformationen".

3. Klicken Sie auf einen Knoten, um dessen Details einzublenden.

Jede Zone und jede VM wurde mit einem Sicherheitsprofil (entweder CIS-Äquivalent oder PCI-DSS) konfiguriert. Wenn Sie eine Benchmark planen, wählen Sie eine Benchmark aus, die dem Sicherheitsprofil der Komponente entspricht.

Compliance Information
Assess and Report Compliance for the virtual machines in the system

Node	Hostname	Benchmark Type	Compliance Score	Date & Time	Remarks	View Repo
Node 1						
	global	pci-dss			No Reports Found	
	global	cis.equivalent			No Reports Found	
	dbvmg1-zone-1-mc4-n1	pci-dss			No Reports Found	
	dbvmg1-zone-1-mc4-n1	cis.equivalent			No Reports Found	
	dbvmg1-zone-2-mc4-n1	pci-dss			No Reports Found	
	dbvmg1-zone-2-mc4-n1	cis.equivalent			No Reports Found	
	dbvmg1-zone-3-mc4-n1	pci-dss			No Reports Found	
	dbvmg1-zone-3-mc4-n1	cis.equivalent			No Reports Found	

4. Scrollen Sie nach rechts, und klicken Sie auf eine Schaltfläche "Schedule" (Planen) für eine der VMs.

Die Seite zur Planung der Complianceausführung wird angezeigt.

5. Geben Sie Zeit und Häufigkeit an, und klicken Sie auf "Start".

Nachdem der Sicherheitscompliance-Test zur geplanten Zeit ausgeführt wurde, zeigen Sie den Bericht an. Weitere Informationen finden Sie in [Anzeigen von Benchmarkberichten \(BUI\) \[49\]](#).

▼ Anzeigen von Benchmarkberichten (BUI)

Dies sind die annehmbaren Complianceergebnisse:

	CIS-Äquivalent	PCI-DSS
Globale Zonen	ca. 88 %	ca. 88 %
VMs	ca. 90 %	ca. 93 %

Dies sind die bekannten Fehler bei Compliance-Tests aufgrund von Oracle Solaris-Problemen:

- Packageintegrität (Core-BS, Rad-Python)
- GDM
- Routing-Daemon
- SSH-Loopback-Adressen - Mitigation löst das Problem nicht.
- Naming Services erkennen DNS nicht
- LDAP-Client

Dies sind die bekannten Fehler bei Compliantests wegen Problemen bei der vom Kunden durchzuführenden MiniCluster-Konfiguration:

- NFS-Clientservices - Ausgewählte Services müssen verfügbar sein.
- Festlegen von eeprom-Passwort - Eine optionale Einstellung

1. **Melden Sie sich bei der MCMU-BUI an.**
2. **Scrollen Sie auf der Homepage nach unten zu dem Bereich "Complianceinformationen".**
3. **Klicken Sie auf "Update Reports" (Berichte aktualisieren).**
Die Aktualisierung kann etwa eine Minute dauern.
4. **Blenden Sie die Knotenanzeige ein, und identifizieren Sie den Compliancebericht.**

3-1-mc4-n1	cis.equivalent	89.83/100	2016-06-20,14:21	-	View Report
------------	----------------	-----------	------------------	---	-----------------------------

5. **Scrollen Sie nach rechts, und klicken Sie auf "View Report" (Bericht anzeigen).**
Der Benchmarkbericht wird angezeigt.

Unter "Rule Overview" (Regelüberblick) können Sie wählen, welche Testtypen basierend auf deren Ergebnissen angezeigt werden sollen. Sie können auch eine Suchzeichenfolge in das Suchfeld eingeben.

ORACLE SOLARIS Compliance Report

Oracle Solaris Security Policy

with profile **Solaris Recommended Security Policy**

Oracle Solaris Compliance baseline and recommended settings for general purpose operating systems installations.

Evaluation Characteristics

Target machine	appvmg1-zone-1-mc4-n1
Benchmark Title	Oracle Solaris Security Policy
Benchmark Version	1.13749
Benchmark Description	Oracle Solaris Compliance baseline and recommended settings for general purpose operating systems installations.
Profile ID	Recommended
Started at	2016-06-20T14:21:21
Finished at	2016-06-20T14:22:10
Performed by	

CPE Platforms

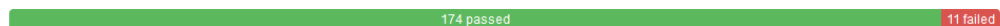
- cpe:/o:oracle:solaris:11

Addresses

Compliance and Scoring

The target system did not satisfy the conditions of 11 rules! Please review rule results and consider applying remediation.

Rule results



Severity of failed rules



- Basierend auf dem Bericht können Sie die Sicherheitssteuerelemente, Compliancebewertungen, Anomalien und Remediation-Prozeduren prüfen.
- Klicken Sie auf den Namen eines Tests, um Details und empfohlene Remediation-Informationen abzurufen.

Anmerkung - Sie können alle Details aller Tests anzeigen, indem Sie auf " Show all Result Details " (Alle Ergebnisdetails anzeigen) unten in dem Bericht klicken.

Rule ID	OSC-54005
Result	fail
Time	2016-06-20T14:21:46
Severity	high
Identifiers and References	
Description	Run 'pkg verify' to check that all installed Oracle Solaris software matches the packaging database and that ownership, permissions and content are correct.

SCE stdout

```
The following packages showed errors
pkg://solaris/system/core-os          ERROR
pkg://solaris/system/management/rad/client/rad-python  ERROR
Run 'pkg verify' to determine the nature of the errors.
```

Remediation description:

'pkg verify' has produced errors. Rerun the command and evaluate the errors. As appropriate, based on errors found, you should run 'pkg fix <package-fmri>' See the pkg(1) man page.

Remediation script:

```
# pkg verify
followed by
# pkg fix <package-fmri>
```

Service svc:/system/pkgd is enabled in global zone | medium | pass

SPARC S7-2 Server - Sicherheitssteuerelemente

In diesen Themen werden die Sicherheitssteuerelemente für die Hardware und die OpenBoot-Umgebung beschrieben.

- [„Hardwaresicherheit“ \[53\]](#)
- [„Einschränken des Zugriffs auf OpenBoot“ \[55\]](#)

Hardwaresicherheit

Physische Isolierung und Zugriffskontrolle stellen die Grundlage dar, auf der die Sicherheitsarchitektur basieren muss. Indem Sie sicherstellen, dass der physische Server in einer sicheren Umgebung aufgestellt wird, können Sie ihn vor unautorisiertem Zugriff schützen. Gleichmaßen empfiehlt es sich, alle Seriennummern aufzuzeichnen, um Diebstahl, Wiederverkauf oder Lieferkettenrisiken (also die Einführung gefälschter oder kompromittierter Komponenten in die Lieferkette Ihrer Organisation) zu vermeiden.

Diese Abschnitte enthalten allgemeine Hardwaresicherheitsrichtlinien für MiniCluster.

- [„Zugriffsbeschränkungen“ \[53\]](#)
- [„Seriennummern“ \[54\]](#)
- [„Festplatten“ \[54\]](#)

Zugriffsbeschränkungen

- Installieren Sie Server und zugehörige Komponenten in einem Raum, der abgeschlossen werden kann und zu dem nicht jeder Zutritt hat.
- Wenn sich Geräte in einem Rack mit Türverriegelung befinden, halten Sie die Tür verschlossen, wenn Sie keine Wartungsarbeiten an Komponenten im Rack vornehmen müssen. Durch Verriegeln der Türen wird auch der Zugang zu Hot-Swapping- oder Hot-Plugging-Geräten eingeschränkt.

- Lagern Sie nicht verwendete FRUs (Field Replaceable Units) oder CRUs (Customer Replaceable Units) in einem abschließbaren Schrank. Nur autorisiertes Personal darf Zugang zu diesem Schrank haben.
- Überprüfen Sie regelmäßig den Zustand und die Integrität der Verriegelungen am Rack und am Schrank der Ersatzteile, um Manipulation oder versehentlich unverschlossene Türen zu verhindern oder zu entdecken.
- Bewahren Sie Schrankschlüssel an einem sicheren Ort mit eingeschränktem Zugriff auf.
- Schränken Sie den Zugriff auf USB-Konsolen ein. Geräte wie System-Controller, Steckdosenleisten (Power Distribution Units, PDUs) und Netzwerk-Switches weisen USB-Anschlüsse auf. Der physische Zugriff ist eine sicherere Methode, auf eine Komponente zuzugreifen, da sie dabei keinen netzwerkbasierten Angriffen ausgesetzt ist.
- Schließen Sie die Konsole an ein externes KVM an, um den Remote-Konsolenzugriff zu ermöglichen. KVM-Geräte unterstützen häufig Zwei-Faktor-Authentifizierung, zentralisierte Zugriffskontrolle und Auditing. Weitere Informationen zu den Sicherheitsrichtlinien und Best Practices für KVMs finden Sie in der Dokumentation für das KVM-Gerät.

Seriennummern

- Bewahren Sie alle Hardwareseriennummern 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 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.

Durch drahtlose RFID-Lesegeräte (Radio Frequency Identification) gestaltet sich die Ressourcenüberwachung noch einfacher. Ein Oracle Whitepaper mit dem Titel *How to Track Your Oracle Sun System Assets by Using RFID* finden Sie unter:

<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf>

Festplatten

Festplatten werden häufig zum Speichern sensibler Informationen verwendet. Um die unautorisierte Offenlegung dieser Informationen zu verhindern, müssen Festplatten komplett bereinigt werden, bevor sie wiederverwendet, außer Betrieb genommen oder entsorgt werden.

- Verwenden Sie Tools zum Bereinigen von Datenträgern, wie den Oracle Solaris-Befehl `format (1M)`, um alle Daten vollständig von der Festplatte 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
<http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf>

Einschränken des Zugriffs auf OpenBoot

In diesen Themen wird beschrieben, wie Sie den Zugriff an der OpenBoot-Eingabeaufforderung einschränken.

Anweisungen zum Konfigurieren eines Passworts für OpenBoot finden Sie unter [EEPROM-Passwörter konfigurieren \[28\]](#).

- [Aufrufen des OpenBoot Prompts \[55\]](#)
- [Auf nicht erfolgreiche Anmeldungen prüfen \[56\]](#)
- [Banner zum Hochfahren bereitstellen \[56\]](#)

Informationen zum Festlegen der OpenBoot-Sicherheitsvariablen finden Sie in der OpenBoot-Dokumentation unter:

<http://www.oracle.com/goto/openboot/docs>

▼ Aufrufen des OpenBoot Prompts

In dieser Prozedur wird beschrieben, wie der OpenBoot Prompt in den MiniCluster-Serverknoten zur Konfiguration der Sicherheitssteuerelemente aufgerufen wird.

Sie müssen das System herunterfahren, um zu dem OpenBoot Prompt zu gelangen. Befolgen Sie die entsprechenden Prozeduren für das ordnungsgemäße Herunterfahren der VMs, wie in *Oracle MiniCluster S7-2 - Administrationshandbuch* beschrieben.

1. **Melden Sie sich auf einem Knoten bei Oracle ILOM an, und setzen Sie diesen Befehl ab.**

```
-> set /HOST/bootmode script="setenv auto-boot? false
-> start /HOST/console
```

Melden Sie sich auf der Hostkonsole als mcinsta11-Benutzer an, und wechseln Sie mit `su` zu `root`.

2. **Nachdem alle VMs heruntergefahren wurden, halten Sie als Root-Rolle die globale Zone an.**

```
# init 0
.
.
{0} ok
```

▼ Auf nicht erfolgreiche Anmeldungen prüfen

1. **Bestimmen Sie, ob jemand nicht erfolgreich versucht hat, auf die OpenBoot-Umgebung zuzugreifen, indem Sie den Parameter `security-#badlogins` wie im folgenden Beispiel verwenden.**

```
{0} ok printenv security-#badlogins
```

Wenn dieser Befehl einen höheren Wert als Null zurückgibt, wurde ein nicht erfolgreicher Zugriffsversuch auf die OpenBoot-Umgebung aufgezeichnet.

2. **Setzen Sie den Parameter zurück, indem Sie diesen Befehl eingeben.**

```
{0} ok setenv security-#badlogins 0
```

▼ Banner zum Hochfahren bereitstellen

Auch wenn es keine direkte Vorsichts- oder Erkennungsmaßnahme ist, kann ein Banner doch für folgende Zwecke verwendet werden:

- Eigentumsrechte ausdrücken.
 - Benutzer vor akzeptierbarer Servernutzung warnen.
 - Informieren, dass Zugriffe oder Änderungen auf bzw. am OpenBoot-Parameter nur auf autorisierte Personen beschränkt sind.
- **Mit den folgenden Befehlen können Sie eine benutzerdefinierte Warnmeldung aktivieren.**

```
{0} ok setenv oem-banner banner-message
{0} ok setenv oem-banner? true
```

Die Bannermeldung kann maximal 68 Zeichen umfassen. Alle druckbaren Zeichen sind zulässig.

Index

A

- Aktivieren FIPS-140-konformer Vorgang (Oracle ILOM), 43
- Ändern von SSH-Schlüsseln, 22
- Anmeldungen, Prüfen auf nicht erfolgreiche, OBP, 56
- Anzeigen
 - Sicherheitsbenchmarkberichte (BUI), 49
 - System Sicherheitsinformationen (BUI), 21
- Asymmetrische Schlüssel, 45
- Auditberichte, generieren, 41
- Auditing und Compliance, 14
- Auditlogs, prüfen, 40
- Auditrichtlinien, überprüfen, 39

B

- Banner, bereitstellen, 56
- Benutzer
 - Genehmigungsprozess, 30
 - Provisioning, 29
- Benutzerkonten, 32
- Benutzerkontrollen, 31
- Berechtigungen, 31
- Bereitstellen eines Banners zum Hochfahren, 56

C

- Compliance und Auditing, 14
- Compliancebenchmarks
 - Überblick, 47

D

- Datenschutz, 13
- Datenschutz mit ZFS-Dataset-Verschlüsselung, 21

- DISA STIG-Profil, 17

E

- EEPROM, Passwort konfigurieren, 28
- Einschränken des Zugriffs auf Shared Storage, 37
- Erforderliche Sicherheitsaufgaben, 9

F

- Festplatten, 54
- FIPS-140
 - Genehmigte Algorithmen, 45
 - Konformer Vorgang (Oracle ILOM), aktivieren, 43
 - Level 1-Compliance, 45
- Firewallregeln, überprüfen, 34

G

- Generieren von Auditberichten, 41
- Grundsätze, Sicherheit, 10
- Grundsätze, Sicherheits-, 9

H

- Hardware
 - Seriennummern, 54
 - Zugriffseinschränkungen, 53
- Hardwaresicherheit, verstehen, 53
- Hash-basierte Nachrichtenauthentifizierung, 45

I

- IKE, konfigurieren, 25
- IPsec, 25

IPsec, konfigurieren, 25

K

Konfigurieren

EEPROM-Passwörter, 28

IPsec und IKE, 25

kryptografische Beschleunigung, 13

M

Mandantenadministratorkonto, 32

mcinstall-Benutzerkonto, 32

MCMU-Benutzer

Genehmigungsprozess, 30

MCMU-Benutzerkonten, 32

Minimal erforderliche Sicherheitsaufgaben, 9

O

OpenBoot

Einschränken des Zugriffs auf OpenBoot, 55

Konfigurieren eines Passworts, 28

zugreifen, 55

Oracle ILOM, Root-Passwort ändern, 27

Oracle Solaris-Benutzerrollen, überprüfen, 33

P

Passwörter

ändern, in Oracle ILOM, 27

Richtlinien, 33

Standard für MCMU, 32

PCI-DSS-Profil, 17

PKCS#11, 13

Planen, Sicherheitsbenchmarks, 48

Primäres Administratorkonto, 32

Profile, Sicherheit, 17

Provisioning von Benutzern, 29

Prüfen auf nicht erfolgreiche OBP-Anmeldungen, 56

Prüfen von Auditlogs, 40

R

Rollen für MCMU-Benutzerkonten, 31

Root, Passwort ändern

, 27

S

Secure Shell-Service, 22

Sekundäres Administratorkonto, 32

Seriennummern, 54

Shared Storage, Zugriff einschränken, 37

Sichere Kommunikation mit IPsec, 25

Sichere virtuelle Maschinen, 11

Sicherer Hashing-Standard, 45

Sicheres Löschen von VMs, 34

Sicherheit

ändern, Oracle ILOM-Passwörter, 27

Benchmarkberichte (BUI) anzeigen, 49

Compliancebenchmarks, 47

Compliancebenchmarks, planen (BUI), 48

Grundsätze, 9, 10

Informationen anzeigen (BUI), 21

Profile, 17

Sicherheitsaufgaben, minimal erforderlich, 9

Sicherheitsprofile

überprüfen, 18

SSH-Netzwerkprotokoll, 22

SSH-Schlüssel, ändern, 22

Supervisorkonto, 32

Symmetrische Schlüssel, 45

Sch

Schützen von Daten, 21

St

Standardsicherheitsprofil, 17

Strategien, Sicherheit, 10

U

Überblick

Benutzergenehmigungsprozess, 30

MCMU-Benutzerkonten, 32

Überprüfen

Auditrichtlinien, 39
hostbasierte Firewallregeln, 34
Oracle Solaris-Benutzerrollen, 33
Sicherheitsprofile, 18
Verified Boot-Umgebungen, 36
Überprüfungsprotokolldateien, 18

V

Verified Boot-Umgebungen, überprüfen, 36
Verschlüsselung, 13, 21
Virtuelle Maschinen, sichere, 11
VMs, sicher löschen, 34

Z

ZFS-Dataset-Verschlüsselung, 21
Zufallszahlengeneratoren, 45
Zugreifen auf die OpenBoot-Eingabeaufforderung, 55
Zugriffseinschränkungen für Hardware, 53
Zugriffskontrolle, 12

