Oracle® ILOM - Sicherheitshandbuch - Firmwarereleases 3.0, 3.1 und 3.2

Teilenr.: E40363-04
Oktober 2015

ORACLE

Teilenr.: E40363-04

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

- **Überblick** - Stellt Web- und CLI-Informationen zu Richtlinien für Oracle ILOM-Sicherheitsaufgaben bereit. Verwenden Sie dieses Handbuch zusammen mit anderen Handbüchern in der Oracle ILOM-Dokumentationsbibliothek.
- **Zielgruppe** - Techniker, Systemadministratoren und autorisierte Oracle-Serviceprovider, die Erfahrung bei der Verwaltung von Systemhardware haben.
- **Erforderliche Kenntnisse** – Erfahrung mit dem Konfigurieren und Verwalten von Oracle-Servern.

Produktdokumentationsbibliothek

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

Feedback

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

Sicherheitsfunktionen pro Oracle ILOM-Firmware-Version

Anhand der folgenden Tabelle können Sie die Firmware-Version ermitteln, in der eine Oracle ILOM-Sicherheitsfunktion verfügbar wurde.

Verfügbarkeit der Firmware-Version	Sicherheitsfunktion	Einzelheiten finden Sie unter:
Alle	Authentifizierung und Autorisierung	■ „Sichern des Oracle ILOM-Benutzerzugriffs“ [25]
Alle	Dedizierte, sichere Verwaltungsverbindung	■ „Sichern der physischen Verwaltungsverbindung“ [15] ■ „Aufrechterhalten einer sicheren Verwaltungsverbindung“ [57]
Alle	Verschlüsselte vorkonfigurierte Netzwerkports	■ „Vorkonfigurierte Services und Netzwerkports“ [20]
Alle	IPMI 2.0 - Sichere Verwaltung	■ „Konfigurieren des IPMI-Verwaltungszugriffs für maximale Sicherheit“ [51]
Alle	Secure Shell-Schlüsselverschlüsselungskonfiguration	■ Verwenden von serverseitigen Schlüsseln zum Verschlüsseln von SSH-Verbindungen [47] ■ Anhängen von SSH-Schlüsseln an Benutzerkonten für automatisierte CLI-Authentifizierung [48]
Alle	SNMP 3.0 - Sichere Verwaltung	■ „Konfigurieren des SNMP-Verwaltungszugriffs für maximale Sicherheit“ [49]
Alle	SSL-Protokolle und -Zertifikate	■ Hochladen eines benutzerdefinierten SSL-Zertifikats und privaten Schlüssels in Oracle ILOM [41] ■ Abrufen eines SSL-Zertifikats und privaten Schlüssels mit OpenSSL [39] ■ Aktivieren der sichersten SSL- und TLS-Verschlüsselungseigenschaften [42]
Alle	Verschlüsselung der Remotekonsole und sichere Protokolle	■ „Sicheres Verwenden von Remote KVMS“ [61]
3.0.4 und höher	KVMS-Hostsperrkonfiguration	■ Sperren des Hostzugriffs nach Beenden einer KVMS-Sitzung [34]
3.0.4 und höher	Sitzungstimeoutkonfiguration	■ Festlegen eines Timeoutintervalls für inaktive Websitzungen [43] ■ Festlegen eines Timeoutintervalls für inaktive CLI-Sitzungen [46]
3.0.12 und höher	Authentifizierte Interconnect-Sitzungen für lokalen Host	■ „Interconnect-Zugriff auf bevorzugten authentifizierten Host“ [58]

Verfügbarkeit der Firmware-Version	Sicherheitsfunktion	Einzelheiten finden Sie unter:
3.0.8 und höher	Anmeldebannerkonfiguration	Sicherer Systemzugriff mit Anmeldebanner (3.0.8 und höher) [36]
3.0.8 bis 3.1.2	Sicherer WS-Management-Zugriff	■ „Konfigurieren des WS-Management-Zugriffs für maximale Sicherheit“ [54]
3.1.0 und höher	Separates Auditlog	■ „Überwachen von Auditereignissen zum Auffinden nicht autorisierter Zugriffe“ [67]
3.1.0 und höher	Prüfung auf physische Sicherheitspräsenz	■ „Physische Sicherheitspräsenz zum Zurücksetzen des Standardpassworts des `root`-Kontos“ [65]
3.2.4 und höher	Konfigurierbare IPMI 1.5-Eigenschaft	■ „Konfigurieren des IPMI-Verwaltungszugriffs für maximale Sicherheit“ [51]
3.2.4 und höher	TLS-Protokollversionen 1.1 und 1.2	■ Aktivieren der sichersten SSL- und TLS-Verschlüsselungseigenschaften [42]
3.2.4 und höher	KVMS-Sitzungsanzahl	■ Einschränken anzeigbarer KVMS-Sitzungen für Remote System Console Plus (3.2.4 oder höher) [35]
3.2.4 und höher	Unterstützung für FIPS-Konformitätsverschlüsselung	■ „Festlegen, ob der FIPS-Modus beim Deployment konfiguriert werden soll“ [16] ■ „Nicht unterstützte Funktionen bei aktiviertem FIPS-Modus“ [19] ■ „Überlegungen nach dem Deployment zum Sichern des Benutzerzugriffs“ [63]
3.2.5 und höher	SSH-Serverstatus und schwache Ciphers	■ Verwaltung von SSH-Serverstatus und schwachen Ciphers (3.2.5 und höher) [45]
3.2.5 und höher	Passwortrichtlinien für lokale Benutzerkonten	■ Einschränkungen der Passwortrichtlinie für alle lokalen Benutzer festlegen (3.2.5 und höher) [30]

Zusätzliche Sicherheitsinformationen

Zusätzliche Informationen zum Sichern von Oracle ILOM finden Sie in den folgenden Abschnitten in diesem Handbuch:

- Best Practice-Checklisten zur Sicherheit für Oracle ILOM
- Sicherheits-Best Practices zum Deployment für Oracle ILOM
- Sicherheits-Best Practices nach dem Deployment für Oracle ILOM

Best Practice-Checklisten zur Sicherheit für Oracle ILOM

Oracle Integrated Lights Out Manager (ILOM) ist ein vorinstallierter Serviceprozessor (SP) in allen Oracle-Servern und den meisten Legacy-Sun-Servern. Systemadministratoren können mit der Benutzeroberfläche von Oracle ILOM Remoteserver-Verwaltungsaufgaben sowie Überwachungsvorgänge zur Serverintegrität in Echtzeit ausführen.

Um sicherzustellen, dass die Sicherheits-Best Practices für Oracle ILOM für Ihre Umgebung implementiert werden, sollten Systemadministratoren die in den folgenden Checklisten empfohlenen Sicherheitsaufgaben berücksichtigen.

- „Sicherheitscheckliste für Server-Deployment“ [11]
- „Sicherheitscheckliste nach Server-Deployment“ [12]

Zusätzliche Informationen

- Sicherheits-Best Practices zum Deployment für Oracle ILOM .
- Sicherheits-Best Practices nach dem Deployment für Oracle ILOM
- Sicherheitsfunktionen pro Oracle ILOM-Firmware-Version [9]

Sicherheitscheckliste für Server-Deployment

Um zu bestimmen, welche Oracle ILOM-Sicherheitsverfahren am besten geeignet sind, wenn das Deployment eines neuen Servers geplant wird, müssen Systemadministratoren die in der folgenden Tabelle 1, „Checkliste - Konfigurieren der Oracle ILOM-Sicherheit beim Server-Deployment “ empfohlenen Sicherheitsaufgaben berücksichtigen.

TABELLE 1 Checkliste - Konfigurieren der Oracle ILOM-Sicherheit beim Server-Deployment

✓	Sicherheitsaufgabe	Zutreffende Firmware-Version (en)	Einzelheiten finden Sie unter:
	Sichere, dedizierte Verwaltungsverbindung mit Oracle ILOM herstellen.	Alle Firmware-Versionen	■ „Sichern der physischen Verwaltungsverbindung“ [15]

✓	Sicherheitsaufgabe	Zutreffende Firmware-Version (en)	Einzelheiten finden Sie unter:
	Festlegen, ob die FIPS 140-2-Sicherheitskonformität beim oder nach dem Deployment oder überhaupt nicht erforderlich ist.	Firmware-Versionen ab 3.2.4	■ „Festlegen, ob der FIPS-Modus beim Deployment konfiguriert werden soll“ [16] ■ „Nicht unterstützte Funktionen bei aktiviertem FIPS-Modus“ [19]
	Passwortrichtlinie für alle lokalen Benutzerkonten festlegen	Firmwareversion 3.2.5 und höher	■ Einschränkungen der Passwortrichtlinie für alle lokalen Benutzer festlegen (3.2.5 und höher) [30]
	Standardpasswort für das vorkonfigurierte Administratoren-`root`-Konto ändern.	Alle Firmware-Versionen	■ „Vermeiden der Erstellung gemeinsam verwendeter Benutzerkonten“ [25] ■ Ändern des Standardpassworts für `root`-Konto bei erster Anmeldung [31]
	Festlegen, ob die vorkonfigurierten Oracle ILOM-Services und deren offenen Netzwerkports auf Ihre Zielumgebung anwendbar sind.	Alle Firmware-Versionen	■ „Sichern von Services und offenen Netzwerkports“ [19]
	Benutzerzugriff auf Oracle ILOM konfigurieren.	Alle Firmware-Versionen	■ „Sichern des Oracle ILOM-Benutzerzugriffs“ [25] ■ Erstellen lokaler Benutzerkonten mit rollenbasierten Berechtigungen [33]
	Festlegen, ob der Zugriff auf das Hostbetriebssystem beim Beenden einer Remote-KVMS-Sitzung gesperrt werden soll.	Firmwareversionen ab 3.0.4	■ Sperren des Hostzugriffs nach Beenden einer KVMS-Sitzung [34]
	Festlegen, ob verhindert werden soll, dass andere SP-Benutzer Remote-KVMS-Sitzungen anzeigen, die mit dem SP gestartet wurden.	Firmware-Versionen ab 3.2.4	■ Einschränken anzeigbarer KVMS-Sitzungen für Remote System Console Plus (3.2.4 oder höher) [35]
	Festlegen, ob eine Sicherheitsbannermeldung bei der Benutzeranmeldung oder sofort nach der Benutzeranmeldung angezeigt werden soll.	Firmware-Versionen ab 3.0.8	■ Sicherer Systemzugriff mit Anmeldebanner (3.0.8 und höher) [36]
	Sicherstellen, dass die maximalen Sicherheitseigenschaften für alle Oracle ILOM-Benutzeroberflächen festgelegt wurden.	Alle Firmware-Versionen	■ „Konfigurieren der Oracle ILOM-Benutzeroberflächen für maximale Sicherheit“ [38]

Sicherheitscheckliste nach Server-Deployment

Um zu bestimmen, welche Oracle ILOM-Sicherheitsverfahren am besten für vorhandene Server in der Umgebung geeignet sind, müssen Systemadministratoren die in der folgenden Tabelle 2, „Checkliste - Aufrechterhalten der Oracle ILOM-Sicherheit nach dem Server-Deployment “ empfohlenen Sicherheitsaufgaben berücksichtigen.

TABELLE 2 Checkliste - Aufrechterhalten der Oracle ILOM-Sicherheit nach dem Server-Deployment

✓	Sicherheitsaufgabe	Zutreffende Firmware-Version (en)	Einzelheiten finden Sie unter:
	Sichere Verwaltungsverbindung mit Oracle ILOM aufrechterhalten	Alle Firmware-Versionen	■ „Verhindern von nicht authentifiziertem Host-KCS-Gerätezugriff“ [57]

✓	**Sicherheitsaufgabe**	**Zutreffende Firmware-Version (en)**	**Einzelheiten finden Sie unter:**
			■ „Interconnect-Zugriff auf bevorzugten authentifizierten Host“ [58] ■ „Verwenden von IPMI 2.0-Verschlüsselung zum Sichern des Kanals“ [59]
	Sicherstellen, dass Remote KVMS und serielle textbasierte Sitzungen sicher von Oracle ILOM aus gestartet werden.	Alle Firmware-Versionen	■ „KVMS-Remotekommunikation und -Verschlüsselung“ [61] ■ „Schutz vor gemeinsamem Remote- KVMS-Zugriff“ [62] ■ „Schutz vor gemeinsamem Zugriff auf serielle Hostkonsole“ [63]
	Benutzerzugriff auf Oracle ILOM verwalten und verfolgen.	Alle Firmware-Versionen	■ „Überlegungen nach dem Deployment zum Sichern des Benutzerzugriffs“ [63]
	Erforderliche Sicherheitsaktionen zum Zurücksetzen eines vergessenen Passworts für das vorkonfigurierte Admin-`root`-Konto.	Firmware-Versionen ab 3.1	■ „Physische Sicherheitspräsenz zum Zurücksetzen des Standardpassworts des `root`-Kontos“ [65]
	Erforderliche Sicherheitsaktionen, wenn der FIPS 140-2-Konformitätsmodus in Oracle ILOM nach dem Server-Deployment geändert werden muss.	Firmware-Versionen ab 3.2.4	■ Ändern des FIPS-Modus nach dem Deployment [68] ■ „Nicht unterstützte Funktionen bei aktiviertem FIPS-Modus“ [19]
	Sicherstellen, dass die Software und Firmware auf dem Server auf dem neuesten Stand ist.	Alle Firmware-Versionen	■ „Durchführen von Updates auf die aktuellste Software und Firmware“ [70]

Sicherheits-Best Practices zum Deployment für Oracle ILOM

Anhand der folgenden Themen können Sie die besten Oracle ILOM-Sicherheitsverfahren ermitteln, die beim Server-Deployment implementiert werden müssen.

Zusätzliche Informationen

- Best Practice-Checklisten zur Sicherheit für Oracle ILOM.
- Sicherheits-Best Practices nach dem Deployment für Oracle ILOM
- Sicherheitsfunktionen pro Oracle ILOM-Firmware-Version [9]

Sichern der physischen Verwaltungsverbindung

Oracle ILOM ist ein Out-of-Band-(OOB-)Verwaltungstool, das Oracle-Server in einem dedizierten Verwaltungskanal verwaltet und überwacht. Im Gegensatz zu Servern mit In-Band-Verwaltungstools sind Oracle-Server bereits mit integrierten Verwaltungsfunktionen ausgestattet, mit denen Systemadministratoren über einen separaten dedizierten Netzwerk-Connector im Serviceprozessor sicheren Zugriff auf Oracle ILOM erhalten. Die Verwaltungsfunktionen von Oracle ILOM bieten Systemadministratoren zwar spezifische Funktionen zur Überwachung und Verwaltung von Oracle-Servern, Oracle ILOM ist jedoch nicht als allgemeine Rechen-Engine oder für den Zugriff von ungeschützten, nicht vertrauenswürdigen Netzwerkverbindungen konzipiert.

Unabhängig davon, ob Sie eine physische Verwaltungsverbindung zu Oracle ILOM über den lokalen seriellen Port, den dedizierten Netzwerkverwaltungsport oder den Standarddaten-Netzwerkport herstellen, muss dieser physische Port auf dem Server oder dem Chassis

Monitoring Module (CMM) immer mit einem internen vertrauenswürdigen Netzwerk oder einem dedizierten sicheren Verwaltungs- oder privaten Netzwerk verbunden sein. Weitere Richtlinien zum Aufbau einer physischen Verwaltungsverbindung zu Oracle ILOM finden Sie in der folgenden Tabelle.

Verwaltungsverbindung über physischen Port zu Oracle ILOM	Unterstützte Oracle-Hardware	Sicherheitsrichtlinien für Verwaltungsverbindung
Dedizierte Verbindung	■ Server (Port: `NET MGT`) ■ CMM (Port: `NET MGT`)	Trennen Sie den Serviceprozessor (SP) vom allgemeinen Datennetzverkehr, indem Sie ihn in ein internes dediziertes Netzwerk integrieren. Weitere Einzelheiten zum Aufbau einer Verwaltungsverbindung zu Oracle ILOM über ein dediziertes Netzwerk finden Sie unter ■ Dedicated Network Management Connection im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)*
Lokale Verbindung	■ Server (Port: `SER MGT`) ■ CMM (Port: `SER MGT`)	Greifen Sie mit einer lokalen seriellen Verwaltungsverbindung direkt vom physischen Server oder CMM auf Oracle ILOM zu. Weitere Einzelheiten zum Aufbau einer lokalen seriellen Verwaltungsverbindung zu Oracle ILOM finden Sie unter: ■ Local Serial Network Management Connection to Oracle ILOM im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)*
Seitenbandverbindung	Server (Ports: `NET0`, `NET1`, `NET2`, `NET3`)	Greifen Sie gegebenenfalls mit einem gemeinsamen Ethernet-Datennetzwerk auf den Serviceprozessor (SP) zu. So wird die Kabelführung und Netzwerkkonfiguration einfacher, da zwei separate Netzwerkverbindungen entfallen. Weitere Einzelheiten zum Aufbau einer Seitenband-Verwaltungsverbindung zu Oracle ILOM finden Sie unter ■ Sideband Management Connection im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)* **Anmerkung -** Die Seitenbandverwaltung wird auf den meisten Oracle-Servern unterstützt.

Anmerkung - Als Schutzmaßnahme gegen Sicherheitsangriffe sollten **Sie den Oracle ILOM SP niemals an ein öffentliches Netzwerk** wie das Internet anschließen. Führen Sie den Oracle ILOM-SP-Verwaltungsdatenverkehr auf einem separaten Verwaltungsnetzwerk, auf das nur Systemadministratoren Zugriff haben.

Festlegen, ob der FIPS-Modus beim Deployment konfiguriert werden soll

Ab Oracle ILOM-Firmwarerelease 3.2.4 bieten die Oracle ILOM-CLI und -Webbenutzeroberfläche einen konfigurierbaren Modus für die Federal Information Processing

Standards (FIPS) Level 1-Konformität. Wenn dieser Modus aktiviert ist, verwendet Oracle kryptografische Algorithmen gemäß den FIPS 140-2-Sicherheitsstandards zum Sichern von sensiblen oder wertvollen Systemdaten.

Systemadministratoren, die Server mit Firmware 3.2.4 oder höher bereitstellen, müssen entscheiden, ob der FIPS-Modus vor der Konfiguration anderer Oracle ILOM-Eigenschaften konfiguriert werden soll. Standardmäßig ist der FIPS-Konformitätsmodus in Oracle ILOM deaktiviert. Bei Änderungen am FIPS-Konformitätsmodus werden alle Konfigurationsdaten auf ihre werkseitigen Standardwerte zurückgesetzt.

Informationen zum Aktivieren der FIPS-Moduskonformität beim Deployment (vor dem Konfigurieren der Oracle ILOM-Eigenschaften) finden Sie unter Aktivieren des FIPS-Modus beim Deployment [17]. Wenn bereits benutzerdefinierte Konfigurationseigenschaften in Oracle ILOM festgelegt wurden und Sie die FIPS-Eigenschaft ändern müssen, lesen Sie „Aktionen nach dem Deployment zum Ändern des FIPS-Modus“ [68].

▼ Aktivieren des FIPS-Modus beim Deployment

Anmerkung - Der FIPS-Konformitätsmodus in Oracle ILOM wird durch die Eigenschaften "State" und "Status" angegeben. Die Zustandseigenschaft steht für den konfigurierten Modus in Oracle ILOM und die Statuseigenschaft für den Betriebsmodus in Oracle ILOM. Wenn die Eigenschaft "FIPS State" geändert wird, wirkt sich diese Änderung bis zum nächsten Neustart von Oracle ILOM nicht auf den Betriebsmodus (Eigenschaft "FIPS Status") aus.

Bevor Sie beginnen

- Die Eigenschaften zum FIPS-Zustand und -Status sind standardmäßig deaktiviert.
- Wenn FIPS aktiviert ist (konfiguriert und betriebsfähig), werden einige Funktionen in Oracle ILOM nicht unterstützt. Eine Liste der nicht unterstützten Funktionen bei aktiviertem FIPS finden Sie unter Tabelle 3, „Nicht unterstützte Funktionen Oracle ILOM bei aktiviertem FIPS-Modus“.
- Die Rolle Admin (a) ist erforderlich, um die FIPS-Zustandseigenschaft zu ändern.
- Die konfigurierbare Eigenschaft für die FIPS-Konformität ist ab Firmwarerelease 3.2.4 in Oracle ILOM verfügbar. In älteren Firmwarereleases als 3.2.4 gibt es in Oracle ILOM keine konfigurierbare Eigenschaft für die FIPS-Konformität.
- Alle benutzerdefinierten Konfigurationseinstellungen werden auf ihre Standardeinstellungen zurückgesetzt, wenn die Zustands- und die Statuseigenschaft des FIPS-Modus in Oracle ILOM geändert werden.

1. **Klicken Sie in der Oracle ILOM-Webbenutzeroberfläche auf "ILOM Administration" -> "Management Access" -> "FIPS".**

2. **Führen Sie auf der FIPS-Seite folgende Aktionen aus:**

a. **Aktivieren Sie das Kontrollkästchen "FIPS State", um die konfigurierte FIPS-Eigenschaft zu aktiveren.**

b. **Klicken Sie auf "Save", um die Änderung anzuwenden.**

Zusätzliche Konfigurationsdetails erhalten Sie, indem Sie auf der FIPS-Webseite auf den Link `More details`.... klicken.

3. **Um den FIPS-Betriebsmodusstatus in Oracle ILOM zu ändern, führen Sie die folgenden Schritte aus, um Oracle ILOM neu zu starten.**

a. **Klicken Sie in der Webbenutzeroberfläche auf "ILOM Administration" -> "Maintenance" -> "SP Reset".**

b. **Klicken Sie auf der Seite "SP Reset" auf die Schaltfläche "SP Reset".**

Nach dem Neustart von Oracle ILOM wird Folgendes ausgeführt:

- Der letzte konfigurierte FIPS-Zustand (aktiviert) wird auf das System angewendet.
- Alle benutzerdefinierten Konfigurationseinstellungen, die zuvor in Oracle ILOM konfiguriert waren, werden auf ihre werkseitigen Standardwerte zurückgesetzt.
- Die Eigenschaft "FIPS Status" wird aktualisiert, um den derzeit aktivierten Betriebszustand in Oracle ILOM widerzuspiegeln.

  Eine vollständige Liste und Beschreibung der FIPS-Statusmeldungen erhalten Sie, indem Sie auf der FIPS-Seite auf den Link `More details` klicken.
- Ein FIPS-Schildsymbol wird im Titelbereich der Webbenutzeroberfläche angezeigt.
- Alle nicht unterstützten FIPS-Funktionen werden entweder deaktiviert oder aus der CLI und Webbenutzeroberfläche entfernt.

  Eine vollständige Liste und Beschreibung der nicht unterstützten FIPS-Funktionen erhalten Sie, indem Sie auf der FIPS-Seite auf den Link `More details` klicken.

Zusätzliche Informationen

- „Nicht unterstützte Funktionen bei aktiviertem FIPS-Modus“ [19]
- „Aktionen nach dem Deployment zum Ändern des FIPS-Modus“ [68]
- Configure FIPS Mode Properties im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (3.2.x)*.

Nicht unterstützte Funktionen bei aktiviertem FIPS-Modus

Wenn Sie die FIPS-Konformität in Oracle ILOM aktivieren, werden die folgenden nicht kompatiblen FIPS 140-2-Funktionen in Oracle ILOM nicht unterstützt.

TABELLE 3 Nicht unterstützte Funktionen Oracle ILOM bei aktiviertem FIPS-Modus

Nicht unterstützte Funktion im FIPS-Modus	Beschreibung
IPMI 1.5	Wenn der FIPS-Modus aktiviert ist und im System ausgeführt wird, wird die IPMI 1.5-Konfigurationseigenschaft von der Oracle ILOM-CLI und -Webbenutzeroberfläche entfernt. Der IPMI 2.0-Service wird automatisch in Oracle ILOM aktiviert. IPMI 2.0 unterstützt sowohl FIPS-konforme als auch nicht konforme Modi.
Firmware-Kompatibilität für Remotekonsole des Oracle ILOM-Systems	Im FIPS-Modus in Oracle ILOM sind die früheren Firmware-Versionen von Oracle ILOM Remote System Console nicht mit den späteren Firmware-Versionen von Oracle ILOM Remote System Console kompatibel. Beispiel: Die Firmware-Version 3.2.4 des Oracle ILOM Remote System Console-Clients ist mit der Firmware-Version 3.2.3 und früheren Versionen von Oracle ILOM Remote System Console abwärtskompatibel. Die Firmware-Version 3.2.2 und frühere Versionen des Oracle ILOM Remote System Console-Clients sind allerdings nicht mit der Firmware-Version 3.2.4 und höher von Oracle ILOM Remote System Console aufwärtskompatibel. **Anmerkung -** Diese Einschränkung der Firmware-Kompatibilität gilt nicht für Oracle ILOM Remote System Console Plus. Oracle ILOM Remote System Console Plus wird auf neueren Serviceprozessorsystemen, wie SPARC T5 und späteren Systemen und/oder Oracle Server x4-4, x4-8 und späteren Systemen, bereitgestellt. Oracle ILOM Remote System Console wird auf älteren Serviceprozessorsystemen, wie SPARC T3 und T4 und Sun Server x4-2/2L/2B und früheren Systemen, bereitgestellt.
LDAP (Lightweight Directory Access Protocol)	Wenn der FIPS-Modus aktiviert ist und im System ausgeführt wird, werden die LDAP-Konfigurationseigenschaften in Oracle ILOM automatisch von der Oracle ILOM-CLI und -Webbenutzeroberfläche entfernt. **Anmerkung -** Die folgenden Remote-Authentifizierungsservices werden sowohl in FIPS-konformen als auch in nicht konformen Modi unterstützt: Active Directory und LDAP/SSL.
RADIUS (Remote Authentication Dial-In User Service)	Wenn der FIPS-Modus aktiviert ist und im System ausgeführt wird, werden die RADIUS-Konfigurationseigenschaften in Oracle ILOM automatisch von der Oracle ILOM-CLI und -Webbenutzeroberfläche entfernt. **Anmerkung -** Die folgenden Remote-Authentifizierungsservices werden sowohl in FIPS-konformen als auch in nicht konformen Modi unterstützt: Active Directory und LDAP/SSL.
SNMP (Simple Network Management Protocol) DES und MD5	Wenn der FIPS-Modus aktiviert ist und im System ausgeführt wird, werden die SNMP-Konfigurationseigenschaften für das DES-Datenschutzprotokoll und das MD5-Authentifizierungsprotokoll nicht in der Oracle ILOM-CLI und -Webbenutzeroberfläche unterstützt.

Sichern von Services und offenen Netzwerkports

Die folgenden Themen enthalten Informationen zur ordnungsgemäßen Konfiguration von Services und den jeweiligen Netzwerkports in Oracle ILOM:

- „Vorkonfigurierte Services und Netzwerkports“ [20]
- „Verwaltung von unerwünschten Services und offenen Ports“ [20]

- „Konfigurieren von Services und Netzwerkports“ [22]

Vorkonfigurierte Services und Netzwerkports

Bei der Oracle ILOM-Vorkonfiguration sind die meisten Services standardmäßig aktiviert. Dadurch kann Oracle ILOM einfach und unkompliziert bereitgestellt werden. Böswillige Benutzer können jedoch über jeden offenen Servicenetzwerkport auf dem Server Zugriff erhalten. Aus diesem Grund ist es wichtig, sich über die ursprünglichen Oracle ILOM-Einstellungen und deren Verwendungszweck zu informieren und die für ein bereitgestelltes System erforderlichen Services auszuwählen. Aktivieren Sie zur Gewährleistung eines möglichst hohen Maßes an Sicherheit nur die erforderlichen Oracle ILOM-Services.

In der folgenden Tabelle sind die in Oracle ILOM standardmäßig aktivierten Services aufgeführt.

TABELLE 4 Standardmäßig aktivierte Services und Ports

Service	Port
HTTP-Umleitung zu HTTPS	80
HTTPS	443
IPMI	623
Remote-KVMS für Oracle ILOM-Remotekonsole	5120, 5121, 5122, 5123, 5555, 5556, 7578, 7579
Remote-KVMS für Oracle ILOM-Remotekonsole Plus	5120, 5555
Servicetag	6481
SNMP	161
Single Sign-On	11626
SSH	22

In der folgenden Tabelle sind die in Oracle ILOM standardmäßig deaktivierten Services aufgeführt.

TABELLE 5 Standardmäßig deaktivierte Services und Ports

Service	Port
HTTP	80

Verwaltung von unerwünschten Services und offenen Ports

Alle Oracle ILOM-Services können bei Bedarf deaktiviert werden, wodurch die entsprechenden offenen Netzwerkports für diese Services geschlossen werden. Sie erreichen eine höhere

Sicherheit in der Oracle ILOM-Umgebung, indem Sie einige Funktionen der standardmäßig aktivierten Services deaktivieren oder deren Standardeinstellungen ändern. Zwar können alle Oracle ILOM-Services deaktiviert werden, jedoch stehen dann weniger Funktionen zur Verfügung. Generell sollten nur diejenigen Services aktiviert werden, die für die bereitgestellte Umgebung erforderlich sind. Hierbei muss zwischen dem Verlust an Funktionen und der Erhöhung der Sicherheit durch weniger aktivierte Netzwerkservices abgewogen werden.

In der folgenden Tabelle werden die Folgen der Aktivierung bzw. Deaktivierung der einzelnen Services beschrieben.

TABELLE 6 Deaktivierte Services

Service	Beschreibung	Folge der Aktivierung/Deaktivierung
HTTP	Unverschlüsseltes Protokoll für den Zugriff auf die Oracle ILOM-Webbenutzeroberfläche	Die Aktivierung dieses Service bewirkt eine schnellere Ausführung als bei verschlüsseltem HTTP (HTTPS). Jedoch können dadurch sensible Daten unverschlüsselt über das Internet gesendet werden.
HTTPS	Verschlüsseltes Protokoll für den Zugriff auf die Oracle ILOM-Webbenutzeroberfläche	Durch die Aktivierung dieses Service wird eine sichere Kommunikation zwischen Webbrowseroberfläche und Oracle ILOM gewährleistet. Dafür ist jedoch ein offener Oracle ILOM-Netzwerkport erforderlich, wodurch das System anfälliger für Sicherheitsrisiken wie Denial-of-Service-Angriffe wird.
Servicetag	Oracle-Erkennungsprotokoll zur Serveridentifizierung und Erleichterung von Serviceanfragen	Durch die Deaktivierung dieses Service kann Oracle ILOM von Oracle Enterprise Manager Ops Center nicht mehr erkannt und nicht in andere automatische Oracle-Servicelösungen integriert werden. Der Servicetag-Zustand kann nur mit der Oracle ILOM-CLI konfiguriert werden. Beispiel: Geben Sie Folgendes ein, um die servicetag-Zustandseigenschaft zu ändern: `set /SP/services/servicetag state=`*enabled*|*disabled*
IPMI	Standardverwaltungsprotokoll	Durch die Deaktivierung dieses Service können möglicherweise Oracle Enterprise Manager Ops Center und einige Oracle-Verwaltungsanschlüsse zu Software von Fremdherstellern das System nicht mehr verwalten.
SNMP	Standardverwaltungsprotokoll für die Überwachung des Zustands von Oracle ILOM und empfangener Trap-Benachrichtigungen	Durch die Deaktivierung dieses Service können möglicherweise Oracle Enterprise Manager Ops Center und einige Oracle-Verwaltungsanschlüsse zu Software von Fremdherstellern das System nicht mehr verwalten.
KVMS	Protokollsatz, mit dem Tastatur, Video, Maus und Speicherplatz per Remote-Zugriff verwendet können.	Durch die Deaktivierung dieses Service können die Hostkonsole und der Remote-Speicherplatz und dadurch die Anwendungen Oracle ILOM Remote Console (oder Oracle ILOM Remote System Console Plus) und CLI Storage Redirection nicht mehr verwendet werden.
SSH	Sicheres Protokoll für den Zugriff auf eine Remote-Shell	Die Deaktivierung dieses Service bewirkt eine Sperrung des Netzwerkzugriffs über die Befehlszeilenschnittstelle und kann dazu führen, dass Oracle ILOM von Oracle Enterprise Manager Ops Center nicht mehr erkannt wird.
SSO	Single Sign-On-Funktion, durch die die Anzahl der erforderlichen Eingaben von Benutzername und Passwort reduziert wird	Die Deaktivierung dieses Service bewirkt, dass beim Start von KVMS das Passwort nicht erneut eingegeben werden muss. Außerdem ist ein Drilldown von einem CMM (Chassis Monitoring Module) in einen Blade-SP ohne erneute Passworteingabe möglich.

Informationen zum Aktivieren und Deaktivieren individueller Netzwerkservices finden Sie im folgenden Thema „Konfigurieren von Services und Netzwerkports“ [22].

Konfigurieren von Services und Netzwerkports

Anweisungen zum Konfigurieren von Verwaltungsservices und den zugehörigen Netzwerkports in Oracle ILOM finden Sie in den folgenden Verfahren.

Sie können Services und die zugehörigen Netzwerkports mit der Befehlszeilenschnittstelle (CLI) oder Webbenutzeroberfläche von Oracle ILOM deaktivieren oder aktivieren. Die Verfahren in diesem Abschnitt liefern webbasierte Navigationsanweisungen für alle Oracle ILOM-Firmware-Versionen. Die CLI-Anweisungen bzw. zusätzliche Details zu Konfigurationseigenschaften finden Sie in der entsprechenden Dokumentation im Abschnitt "Zusätzliche Informationen" im Anschluss an jedes Verfahren.

▼ Ändern von Zuständen und Ports für Protokollverwaltungsservice

Bevor Sie beginnen

- Bestimmen Sie anhand der folgenden Tabellen, welche Protokollservices und Netzwerkports standardmäßig in Oracle ILOM aktiviert oder deaktiviert sind.
  - Tabelle 4, „Standardmäßig aktivierte Services und Ports“ Services and Ports Enabled by Default
  - Tabelle 5, „Standardmäßig deaktivierte Services und Ports“ Services and Ports Disabled by Default
- Die Rolle Admin (a) ist in Oracle ILOM erforderlich, um die Zustandseigenschaft von Protokollservices zu ändern.

Gehen Sie wie folgt vor, um die Zustandseigenschaft eines Netzwerkservice zu ändern.

1. **Navigieren Sie in der Oracle ILOM-Webbenutzeroberfläche zu den Services für den Verwaltungszugriff.**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "Configuration" -> "System Management Access".**
   - **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "ILOM Administration" -> "Management Access".**

2. **Klicken Sie auf eine der unten aufgeführten Management Access-Serviceregisterkarten:**

Management Access ->	Beschreibung
Web Server	Auf der Seite "Web Server" können Sie den Servicezustand und die Portzuweisungen für den HTTP- und HTTPS-Protokollverwaltungszugriff verwalten.
IPMI	Auf der Seite "IPMI" können Sie den Servicezustand und die Porteigenschaften für den IPMI-Protokollverwaltungszugriff verwalten.
SNMP	Auf der Seite "SNMP" können Sie den Servicezustand und die Porteigenschaften für den SNMP-Verwaltungszugriff verwalten.
SSH	Auf der Seite "SSH" können Sie die Servicezustandseigenschaft für den Secure Shell-Verwaltungszugriff verwalten.

3. **Ändern Sie die Eigenschaft "State" auf der jeweiligen Management Access-Serviceseite, und klicken Sie dann auf "Save", um die Änderung anzuwenden.**

   Hinweis: Wenn Sie die Eigenschaft "State" eines Protokollservice deaktivieren, wird der zugehörige Netzwerkport des Protokollservice geschlossen, und der Protokollservice kann nicht mit Oracle ILOM verwendet werden.

Zusätzliche Informationen

- Management Services and Network Default Properties im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Management Services and Network Default Properties im *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Konfigurieren von Netzwerkeinstellungen in *Oracle ILOM 3.0 - Allgemeine Verwaltung - CLI-Prozeduren - Handbuch*
- Konfigurieren von Netzwerkeinstellungen, *Oracle ILOM 3.0 - Allgemeine Verwaltung - Webprozeduren - Handbuch*

▼ Ändern von Zustand und Ports für KVMS-Service

Bevor Sie beginnen

- Die Zustandseigenschaft des KVMS-Service ist standardmäßig in Oracle ILOM aktiviert. Eine Liste der offenen Netzwerkports, die mit dem KVMS-Service verknüpft sind, finden Sie in Tabelle 4, „Standardmäßig aktivierte Services und Ports“.
- Die Rolle Admin (a) ist erforderlich, um die KVMS-Zustandseigenschaft in Oracle ILOM zu ändern.

1. **Navigieren Sie zur Registerkarte "KVMS" in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "Remote Control" -> "KVMS".**

- **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "Remote Console" -> "KVMS".**

2. **Ändern Sie in der Registerkarte "KVMS" die Eigenschaft "KVMS State", und klicken Sie dann auf "Save", um die Änderung anzuwenden.**

   Beachten Sie, dass die Deaktivierung der Eigenschaft "State" dazu führt, dass die jeweiligen offenen KVMS-Servicenetzwerkports geschlossen werden. Dadurch wird die Verwendung von Folgendem verhindert: a) der Remotehostkonsole und b) von Oracle ILOM Remote Console und Oracle ILOM Remote Storage CLI oder von Oracle ILOM Remote Console Plus.

Zusätzliche Informationen

- Configure Local Client KVMS Settings im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Konfigurieren von lokalen Client-KVMS-Einstellungen, *Oracle ILOM 3.1 - Konfigurations- und Wartungshandbuch*
- Anfangssetup in *Oracle ILOM 3.0 Remote Redirection Console - Web- und CLI-Handbuch*

▼ Ändern von Zustand und Port für Single Sign-On-Service

Bevor Sie beginnen

- Die Zustandseigenschaft des Single Sign-On-(SSO-)Service und der zugehörige Netzwerkport (1126) sind standardmäßig in Oracle ILOM aktiviert.
- Die Rolle Admin (a) ist in Oracle ILOM erforderlich, um die Zustandseigenschaft des SSO-Service zu ändern.

1. **Navigieren Sie zur Registerkarte "User Account" in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "User Management" -> "User Account".**

   - **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "ILOM Administration" -> "User Account".**

2. **Ändern Sie auf der Seite "User Account" die Eigenschaft "SSO State", und klicken Sie dann auf "Save", um die Änderung anzuwenden.**

   Beachten Sie, dass die Deaktivierung der Eigenschaft "SSO State" in Oracle ILOM zu Folgendem führt : a) Der offene SSO-Netzwerkport wird geschlossen; b) Benutzer werden aufgefordert, ihr Passwort beim Starten einer KVMS-Konsole erneut einzugeben und c) CMM-Benutzer können zu einem Blade-Server-SP navigieren, ohne ihr Passwort erneut eingeben zu müssen.

Zusätzliche Informationen

- Single Sign-On Service im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Single Sign-On Service im *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Configure Single Sign-On in *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Configure Single Sign-On in *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Sichern des Oracle ILOM-Benutzerzugriffs

Informationen zum Sichern des Benutzerzugriffs in Oracle ILOM finden Sie in den folgenden Themen:

Vermeiden der Erstellung gemeinsam verwendeter Benutzerkonten

Gewährleisten Sie eine sichere Umgebung, indem Sie die Erstellung von gemeinsamen Konten vermeiden. Gemeinsame Konten sind Benutzerkonten, die dasselbe Passwort verwenden. Anstelle von gemeinsam genutzten Konten empfiehlt es sich, ein eindeutiges Passwort für jeden Benutzer zu erstellen, der auf Oracle ILOM Zugriff hat. Stellen Sie sicher, dass die jeweilige Kombination aus Benutzerkonto und Passwort nur einem Benutzer bekannt ist.

Anmerkung - Oracle ILOM unterstützt bis zu 10 lokale Benutzerkonten. Wenn mehr Benutzer Zugriff auf Oracle ILOM erhalten sollen, können Sie Verzeichnisservices wie LDAP oder Active Directory konfigurieren, sodass mehr Konten eine zentrale Datenbank verwenden können. Einzelheiten dazu finden Sie unter „Remote-Authentifizierungsservices und Sicherheitsprofile“ [29].

Nach der Einrichtung individueller Benutzerkonten mit eindeutigen Passwörtern muss der Systemadministrator sicherstellen, dass ein eindeutiges Passwort dem vorkonfigurierten Administratorkonto `root` zugewiesen wurde. Wenn das vorkonfigurierte Administratorkonto `root` kein eindeutiges Passwort aufweist, wird es als gemeinsam genutztes Konto betrachtet. Um sicherzustellen, dass keine unautorisierten Benutzer das vorkonfigurierte Administratorkonto `root` verwenden, müssen Sie das Passwort ändern oder das vorkonfigurierte `root`-Konto von Oracle ILOM entfernen. Weitere Einzelheiten zum

vorkonfigurierten Administratorkonto `root` finden Sie unter Ändern des Standardpassworts für `root`-Konto bei erster Anmeldung [31].

Weitere Anweisungen zum Einrichten von sicheren Konten mit eindeutigen Passwörtern finden Sie unter „Sicherheitsrichtlinien zum Verwalten von Benutzerkonten und Passwörtern“ [27].

Informationen zur Benutzerkontenkonfiguration finden Sie unter „Konfigurieren des Benutzerzugriffs für maximale Sicherheit“ [30].

Zuweisung rollenbasierter Berechtigungen

Sämtliche Oracle ILOM-Benutzerkonten umfassen einen Satz von rollenbasierten Berechtigungen. Diese rollenbasierten Berechtigungen bieten Zugriff auf diskrete Oracle ILOM-Funktionen. Das Benutzerkonto kann so konfiguriert werden, dass der Benutzer das System überwachen, aber die Konfiguration nicht ändern kann. Alternativ können Sie einem Benutzer die Änderung der meisten Konfigurationsoptionen mit Ausnahme der Erstellung und Änderung von Benutzerkonten ermöglichen. Außerdem können Sie die Steuerung der Stromversorgung des Servers und den Zugriff auf die Remote-Konsole einschränken. Gründliche Kenntnisse der Berechtigungsstufen sind wichtig für die Zuweisung zu den richtigen Benutzern in der Organisation.

Die folgende Tabelle enthält eine Liste von Berechtigungen, die Sie einem einzelnen Oracle ILOM-Benutzerkonto zuweisen können.

TABELLE 7 Beschreibungen der Berechtigungen für Benutzerkonten

Rolle	Beschreibung
`Admin` (a)	Ein Benutzer kann sämtliche Oracle ILOM-Konfigurationsoptionen ändern. Ausnahme: Konfigurationsoptionen, die ausdrücklich durch andere Berechtigungen (beispielsweise Benutzerverwaltung) autorisiert wurden.
`Benutzerverwaltung` (u)	Ermöglicht Benutzern das Hinzufügen und Entfernen anderer Benutzer, Änderungen an Benutzerpasswörtern sowie das Konfigurieren von Authentifizierungsservices. Da ein Benutzer mit dieser Rolle ein zweites Benutzerkonto mit allen Berechtigungen erstellen kann, verfügt diese Rolle über die höchste Berechtigungsstufe aller Benutzerrollen.
`Konsole` (c)	Ermöglicht dem Benutzer den Remote-Zugriff auf die Hostkonsole. Dadurch kann der Benutzer das BIOS oder OBP (OpenBoot PROM) aufrufen und das Boot-Verhalten ändern, um Zugriff auf das System zu erhalten.
`Zurücksetzen und Hoststeuerung` (r)	Der Benutzer kann die Stromversorgungszustände des Hosts steuern und Oracle ILOM zurücksetzen.
`Schreibgeschützt` (o)	Ermöglicht dem Benutzer den schreibgeschützten Zugriff auf die Oracle ILOM-Benutzeroberfläche. Alle Benutzer verfügen über diese Zugriffsmöglichkeit, mit der sie Protokolle und Umgebungsinformationen lesen sowie Konfigurationseinstellungen anzeigen können.

Weitere Informationen zum Erstellen eines lokalen Benutzerkontos und Zuweisen von rollenbasierten Berechtigungen finden Sie unter Erstellen lokaler Benutzerkonten mit rollenbasierten Berechtigungen [33].

Sicherheitsrichtlinien zum Verwalten von Benutzerkonten und Passwörtern

Beachten Sie die folgenden Sicherheitsrichtlinien beim Verwalten von Oracle ILOM-Benutzerkonten und -Passwörtern:

Richtlinien für die Verwaltung von Benutzerkonten

Richtlinie für die Benutzerkontenverwaltung	Beschreibung
Fördern Sie niemals die gemeinsame Nutzung von Benutzerkonten	Für jeden Oracle ILOM-Benutzer sollte ein separates Konto erstellt werden. Oracle ILOM unterstützt maximal 10 lokale Benutzerkonten. Wenn Sie einen größeren Standort verwalten und mehr als 10 Benutzerkonten benötigen, sollten Sie den Authentifizierungsservice eines Drittanbieters wie LDAP oder Active Directory verwenden. Weitere Informationen zur Implementierung der Benutzerauthentifizierung in Oracle ILOM über einen externen Authentifizierungsservice finden Sie unter „Remote-Authentifizierungsservices und Sicherheitsprofile“ [29].
Wählen Sie konforme Namen für lokale Benutzerkonten	Benutzernamen für ein lokales Oracle ILOM-Benutzerkonto müssen die folgenden Anforderungen erfüllen: ■ Zwischen 4 und 16 Zeichen lang sein (das erste Zeichen muss ein Buchstabe sein). ■ Innerhalb Ihres Unternehmens eindeutig sein ■ Keine Leerzeichen, Punkte (.) oder Doppelpunkte (:) enthalten
Wählen Sie konforme Passwörter für lokale Benutzerkonten	Passwörter für ein lokales Oracle ILOM-Benutzerkonto müssen die folgenden Anforderungen erfüllen: ■ Sicher und als stark eingestuft sein und höchstens 16 Zeichen umfassen ■ Eine Kombination aus Klein- und Großbuchstaben sowie ein oder zwei Sonderzeichen enthalten, um das Passwort sicher und komplex zu machen ■ Keine Leerzeichen, Punkte (.) oder Doppelpunkte (:) enthalten ■ Konform zu den im Unternehmen gültigen Richtlinien zur Passwortverwaltung sein Weitere Einzelheiten zur Passwortverwaltung in Oracle ILOM finden Sie unter „Sicherheitsrichtlinien zum Verwalten von Benutzerkonten und Passwörtern“ [27].
Schränken Sie die Benutzerkontoberechtigungen auf Basis der Jobrolle ein (*Grundsatz der niedrigstmöglichen Berechtigung*)	Der für optimale Sicherheit verfolgte Grundsatz der niedrigstmöglichen Berechtigung gibt vor, Benutzern stets nur die zur Ausführung ihrer Arbeit notwendigen Berechtigungen zuzuweisen. Eine zu ambitionierte Zuweisung von Verantwortlichkeiten und Rollen (insbesondere in der Anfangsphase einer Organisation) kann die Tür für Missbrauch öffnen. Überprüfen Sie die Benutzerberechtigungen regelmäßig, um ihre Relevanz für aktuelle Verantwortungsbereiche zu ermitteln. Oracle ILOM ermöglicht es Ihnen, die Berechtigungen sämtlicher Benutzer zu kontrollieren. Stellen Sie sicher, dass den einzelnen Benutzerkonten die geeigneten der Tätigkeitsrolle entsprechenden Berechtigungen zugewiesen sind. Einzelheiten zum Erstellen eines Benutzerkontos mit rollenbasierten Berechtigungen finden Sie unter Erstellen lokaler Benutzerkonten mit rollenbasierten Berechtigungen [33].

Richtlinien für die Passwortverwaltung

Richtlinie für die Passwortverwaltung	Beschreibung
Ändern des Standard-`root`-Passwortes (`changeme`) unmittelbar nach der ersten Anmeldung	Für die erstmalige Anmeldung und den ersten Zugriff auf Oracle ILOM wird ein lokales Administrator-`root`-Konto im System bereitgestellt. Um eine sichere Umgebung aufzubauen, ändern Sie das bereitgestellte Administratorpasswort (`changeme`) nach der ersten Anmeldung bei Oracle ILOM. Wenn Benutzer ohne Autorisierung Zugriff auf das `root`-Konto für Administratoren erhalten, können sie uneingeschränkt auf alle Oracle ILOM-Funktionen zugreifen. Aus diesem Grund sollten unbedingt sichere Passwörter festgelegt werden.
Regelmäßiges Ändern aller Oracle ILOM-Kontopasswörter	Um böswillige Aktivitäten zu verhindern und sicherzustellen, dass Passwörter den aktuellen Passwortrichtlinien entsprechen, müssen Sie alle Oracle ILOM-Passwörter regelmäßig ändern.
Gängige Vorgehensweisen zum Erstellen sicherer, komplexer Passwörter	Setzen Sie die folgenden gängigen Vorgehensweisen zur Erstellung komplexer Passwörter durch: ■ Erstellen Sie kein Passwort, das kürzer als 16 Zeichen ist. ■ Erstellen Sie keine Passwörter, die den Benutzernamen, den Mitarbeiternamen oder den Namen eines Familienmitglieds enthalten. ■ Wählen Sie keine Passwörter, die sich einfach erraten lassen. ■ Erstellen Sie keine Passwörter, die eine aufeinander folgende Zeichenfolge von Zahlen enthalten, wie 12345. ■ Erstellen Sie keine Passwörter, die Wörter oder Zeichenfolgen enthalten, die sich durch einfache Internetrecherchen herausfinden lassen. ■ Sorgen Sie dafür, dass Benutzer dasselbe Passwort nicht in mehreren Systemen wiederverwenden können. ■ Sorgen Sie dafür, dass Benutzer ältere Passwörter nicht wiederverwenden können. ■ Für maximale Sicherheit müssen Sie neue Passworteinträge in der CLI immer mit der folgenden Syntax maskieren: **`set [`***SP*|*CMM*`**`]`**`/users/root password=`**[*Kennwort nicht eingeben, Eingabetaste drücken*] - oder- **`set [`***SP*|*CMM*`**`]`**`/users/newuser password=`**[*Kennwort nicht eingeben, Eingabetaste drücken*] Die CLI fordert Sie zur Eingabe des neuen Passwortwertes auf, wobei das Passwort in der Anzeige maskiert wird.
Einschränkungen der Passwortrichtlinie für lokale Benutzer festlegen (Ab Firmware 3.2.5 und höher verfügbar)	Setzen Sie eine Passwortrichtlinie für alle lokalen Benutzerkonten durch. Weitere Einzelheiten finden Sie unter Einschränkungen der Passwortrichtlinie für alle lokalen Benutzer festlegen (3.2.5 und höher) [30]
Fragen Sie den IT-Sicherheitsbeauftragten nach den für die Passwortverwaltung gültigen Richtlinien.	Wenden Sie sich an Ihren IT-Sicherheitsbeauftragten, um sicherzustellen, dass die Passwortanforderungen und -richtlinien Ihres Unternehmens erfüllt werden.

Remote-Authentifizierungsservices und Sicherheitsprofile

Oracle ILOM kann so konfiguriert werden, dass ein externer, zentraler Benutzerspeicher an die Stelle einer Konfiguration von lokalen Benutzern für jede Oracle ILOM-Instanz tritt. Auf diese Weise können die Zugangsdaten von Benutzern für den Zugriff auf verschiedene Systeme zentral erstellt und geändert werden.

Bevor Sie einen Authentifizierungsservice auswählen und konfigurieren, machen Sie sich mit der Funktionsweise und den Anforderungen an die Konfiguration dieser Services vertraut. Neben der Authentifizierung bietet jeder unterstützte Service die Möglichkeit der Konfiguration von Autorisierungsregeln, um die Art und Weise der Zuweisung von Oracle ILOM-Benutzerberechtigungen für einen bestimmten Remote-Benutzer zu definieren. Vergewissern Sie sich, dass die richtige Benutzerrolle bzw. -berechtigung zugewiesen wird.

In der folgenden Tabelle werden die von Oracle ILOM unterstützten Benutzerauthentifizierungsservices beschrieben.

TABELLE 8 Remote-Authentifizierungsservices und Sicherheitsprofile

Servicename	Sicherheitsprofil	Information
Active Directory	Hoch	■ Dieser Service ist standardmäßig sicher. ■ Für den strikten Zertifikatsmodus ist ein Zertifikatsserver erforderlich, durch den jedoch eine zusätzliche Sicherheitsebene zur Verfügung steht.
LDAP/SSL (Lightweight Directory Access Protocol/ Secure Socket Layer)	Hoch	■ Dieser Service ist standardmäßig sicher. ■ Für den strikten Zertifikatsmodus ist ein Zertifikatsserver erforderlich, durch den jedoch eine zusätzliche Sicherheitsebene zur Verfügung steht.
Legacy-LDAP	Niedrig	■ Verwenden Sie diesen Service für private, sichere Netzwerke, in denen sich keine verdächtigen, böswilligen Benutzer befinden.
RADIUS (Remote Authentication Dial In User Service)	Niedrig	■ Verwenden Sie diesen Service für private, sichere Netzwerke, in denen sich keine verdächtigen, böswilligen Benutzer befinden.

Services mit dem Sicherheitsprofil "Hoch" können in sehr stark abgesicherten Umgebungen verwendet werden, da sie durch Zertifikate und andere sichere Verschlüsselungsmethoden zum Schutz des Kanals geschützt sind. Die Services mit dem Sicherheitsprofil "Niedrig" sind standardmäßig deaktiviert. Aktivieren Sie diese Sicherheitsprofile nur dann, wenn Sie sich über die Einschränkungen durch eine solch niedrige Sicherheitsstufe im Klaren sind und sie akzeptieren.

Einzelheiten zur Konfiguration von Remote-Authentifizierungsservices finden Sie in der entsprechenden Oracle ILOM-Dokumentation weiter unten:

- Setting Up and Maintaining User Accounts im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*

- Setting Up and Maintaining User Accounts im Oracle ILOM 3.1 *Configuration and Maintenance Guide*
- Managing User Accounts in *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Managing User Accounts in *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Konfigurieren des Benutzerzugriffs für maximale Sicherheit

Die folgenden Themen enthalten Informationen zur optimalen Konfiguration des Oracle ILOM-Benutzerzugriffs für maximale Sicherheit.

Sie können Benutzerzugriffseigenschaften in Oracle ILOM mit der Befehlszeilenschnittstelle (CLI) oder Webbenutzeroberfläche konfigurieren. Die Verfahren in diesem Abschnitt liefern webbasierte Navigationsanweisungen für alle Oracle ILOM-Firmware-Versionen. Die CLI-Anweisungen bzw. zusätzliche Details zu Konfigurationseigenschaften finden Sie in der entsprechenden Dokumentation im Abschnitt "Zusätzliche Informationen" nach jedem Verfahren.

▼ Einschränkungen der Passwortrichtlinie für alle lokalen Benutzer festlegen (3.2.5 und höher)

Ab Firmwarerelease 3.2.5 setzt Oracle ILOM eine Passwortrichtlinie für alle lokalen Benutzerkonten durch. Die Passwortrichtlinie ist in einem Standardset von Einschränkungen für Passwortrichtlinien enthalten. Systemadministratoren können die Standardeigenschaften unverändert verwenden oder sie entsprechend ihren Anforderungen an Passwortrichtlinien ändern.

Anmerkung - Änderungen an den Eigenschaften der Passwortrichtlinie müssen vor dem Erstellen von lokalen Benutzerkonten festgelegt werden. Falls die Eigenschaften der Passwortrichtlinie geändert werden, nachdem lokale Benutzerkonten konfiguriert wurden, führt Oracle ILOM automatisch folgende Schritte aus: 1) Die Konfiguration aller lokalen Benutzerkonten wird entfernt, und 2) das Standard-Root-Konto, das anfänglich mit dem System bereitgestellt wurde, wird wiederhergestellt.

Bevor Sie beginnen

- Die Rolle Admin (a) ist erforderlich, um die Eigenschaften der Passwortrichtlinie zu konfigurieren.
- Die Passwortrichtlinie wird nur für lokale Benutzerkonten angewendet. Sie hat keine Auswirkungen auf Konten von Remote-Benutzerauthentifizierungsservices wie LDAP oder Active Directory.
- Nachdem Änderungen an den Eigenschaften der Passwortrichtlinie gespeichert wurden, geschieht Folgendes:
  - Alle Konfigurationen von lokalen Benutzerkonten werden aus Oracle ILOM gelöscht.
  - Das mit dem System gelieferte lokale Standardbenutzerkonto (root) wird wiederhergestellt.
  - Nach der anfänglichen Anmeldung von Root, wird der Root-Benutzer aufgefordert, das "root-account"-Passwort zu ändern.

Verwenden Sie die folgenden webbasierten Anweisungen, um eine Passwortrichtlinie für alle lokalen Benutzer festzulegen:

Anmerkung - Für Anweisungen zur CLI-Passwortrichtlinie klicken Sie auf die Referenz für das "Oracle ILOM - Administrationshandbuch" im Abschnitt "Zusätzliche Informationen" für diese Prozedur.

---

1. **Zur Anzeige der aktuellen Einschränkungen der Passwortrichtlinie in Oracle ILOM klicken Sie auf "ILOM Administration > User Management > Password Policy".**
2. **Zur Änderung der Einschränkungen der Passwortrichtlinie klicken Sie auf den Link "More Details..." auf der Seite "Password Policy", um weitere Anweisungen aufzurufen.**
3. **Um die Änderungen zu speichern, klicken Sie auf "Save".**

Zusätzliche Informationen

- „Modify Password Policy Restrictions for Local Users“ im *Oracle ILOM - Administratorhandbuch für Konfiguration und Wartung (Firmwarerelease 3.2.x)*

▼ Ändern des Standardpassworts für root-Konto bei erster Anmeldung

Für die erstmalige Anmeldung und den ersten Zugriff auf Oracle ILOM werden ein vorkonfiguriertes Administrator-root-Konto und ein Standardpasswort (changme) im

System bereitgestellt. Um den unautorisierten Zugriff auf Oracle ILOM zu verhindern, muss das Standardpasswort (changeme) des vorkonfigurierten root-Kontos bei der ersten Anmeldung geändert werden. Andernfalls fungieren das vorkonfigurierte root-Konto und das Standardpasswort (changeme) als gemeinsam genutztes Konto, über das jeder Benutzer Administratorzugriff erhält.

Ändern Sie das Standardpasswort (changeme) des vorkonfigurierten Administrator-root-Kontos anhand des folgenden webbasierten Verfahrens.

Anmerkung - Wenn Sie keinen Zugriff auf das vorkonfigurierte root-Konto haben, aber Zugriff auf die Oracle ILOM-Administratorfunktionen benötigen, bitten Sie den Systemadministrator um ein Benutzerkonto mit Administratorberechtigungen.

Bevor Sie beginnen

- Lesen Sie den Abschnitt „Sicherheitsrichtlinien zum Verwalten von Benutzerkonten und Passwörtern“ [27].

  Anmerkung - Sie müssen unbedingt ein komplexes, sicheres Passwort für das root-Konto erstellen, um den unautorisierten Zugriff auf Oracle ILOM-Funktionen zu verhindern. Ein sicheres Passwort besteht aus einer Kombination aus Kleinbuchstaben, Großbuchstaben und mindestens einem Sonderzeichen, z.B. % oder $.

- Die Rolle Benutzerverwaltung (u) ist erforderlich, um die Passwörter der lokalen Benutzerkonten in Oracle ILOM zu ändern.

1. **Navigieren Sie zur Seite "User Account" in der Oracle ILOM-Webbenutzeroberfläche.**
   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "User Management" -> "User Accounts".**
   - **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "User Management" -> "User Accounts".**

2. **Klicken Sie auf der Seite "User Account" beim root-Konto auf "Edit".**
   Das Dialogfeld "Edit: User Root" wird angezeigt.

3. **Führen Sie im Dialogfeld "Edit: User Root" die folgenden Aktionen aus:**

   - **Geben Sie ein eindeutiges Passwort in das Textfeld "New Password" ein, und wiederholen Sie dieses Passwort dann im Textfeld "Confirm New Password".**

- **Klicken Sie auf "Save", um die Änderung anzuwenden.**

Zusätzliche Informationen

- Configuring a Local User Account im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Configuring a Local User Account im *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Modify a User Account in *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Modify a User Account in *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*
- „Physische Sicherheitspräsenz zum Zurücksetzen des Standardpassworts des `root`-Kontos“ [65]

▼ Erstellen lokaler Benutzerkonten mit rollenbasierten Berechtigungen

Bevor Sie beginnen

Oracle ILOM unterstützt die Erstellung und Speicherung von bis zu 10 lokalen Benutzerkonten auf einem einzelnen SP oder Chassis Monitoring Module (CMM). Oracle ILOM-Benutzer erhalten einen Satz aus Berechtigungen, über den sie mit den Funktionen arbeiten können, die gemäß ihrem konfigurierten Konto für sie verfügbar sind.

Anmerkung - Alternativ dazu können Systemadministratoren Oracle ILOM so konfigurieren, dass zusätzliche Benutzerkonten über einen Remote-Authentifizierungsservice unterstützt werden. Bei der Konfiguration eines Remote-Authentifizierungsservice werden Anmeldenamen, Passwörter und Berechtigungen von einem externen Benutzerspeicher abgeleitet. Einzelheiten dazu finden Sie unter „Remote-Authentifizierungsservices und Sicherheitsprofile“ [29].

Im Folgenden erhalten Sie webbasierte Anweisungen zum Konfigurieren eines lokalen Benutzerkontos mit rollenbasierten Zugriffsberechtigungen.

Bevor Sie beginnen

- Lesen Sie den Abschnitt „Sicherheitsrichtlinien zum Verwalten von Benutzerkonten und Passwörtern“ [27].
- Prüfen Sie Tabelle 7, „Beschreibungen der Berechtigungen für Benutzerkonten“ Unterstützte Webbrowser für Oracle ILOM.
- Die Rolle Benutzerverwaltung (u) ist in Oracle ILOM erforderlich, um ein lokales Benutzerkonto mit Berechtigungen zu erstellen.

1. **Navigieren Sie zur Seite "User Account" in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

- **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "User Management" -> "User Accounts".**
- **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "User Management" -> "User Accounts".**

2. **Klicken Sie auf der Seite "User Account" auf "Add".**

   Das Dialogfeld "Add User" wird angezeigt.

3. **Führen Sie im Dialogfeld "Add User" die folgenden Aktionen aus:**

   a. **Geben Sie den Namen des Benutzers im Textfeld "User Name" an.**

   b. **Wählen Sie in der Dropdown-Liste "Roles" das entsprechende Benutzerrollenprofil ("Administrator", "Operator" oder "Advanced").**

   c. **Geben Sie ein eindeutiges Passwort in das Textfeld "New Password" ein, und wiederholen Sie dieses Passwort dann im Textfeld "Confirm New Password".**

   d. **Klicken Sie auf "Save", um die Änderungen anzuwenden.**

Zusätzliche Informationen

- Create User Account and Assign User Role im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Create User Account and Assign User Role im *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Add User Account and Assign Roles in *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Add User Account and Assign Roles in *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

▼ Sperren des Hostzugriffs nach Beenden einer KVMS-Sitzung

Die Hostkonsole fungiert bei der Verwendung von Remote KVMS als gemeinsam genutzte Netzwerkressource. Wenn sich also ein Benutzer bei der Hostkonsole anmeldet und die Anwendung Oracle ILOM Remote System Console, Remote System Console Plus oder CLI Storage Redirection schließt, ohne sich vom Hostbetriebssystem abzumelden, kann ein anderer Benutzer, der über Remote KVMS mit derselben Konsole eine Verbindung herstellt, die zuvor authentifizierte Betriebssystemsitzung verwenden. Aus diesem Grund bietet Oracle ILOM die Möglichkeit, das Hostbetriebssystem automatisch immer dann zu sperren, wenn eine Remote

KVMS-Sitzung unterbrochen wird. Aktivieren oder konfigurieren Sie diese Oracle ILOM-Funktion, um ein Höchstmaß an Sicherheit zu erreichen.

Im Folgenden finden Sie webbasierte Anweisungen zum Sperren des Remotehostdesktops nach Beenden einer KVMS-Sitzung. Weitere Informationen zum Aktivieren der Hostsperrfunktion finden Sie im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*.

Bevor Sie beginnen

- Die Rolle Konsole (c) ist erforderlich, um die Eigenschaft für den Hostsperrmodus in Oracle ILOM zu ändern.
- Firmware 3.0.4 oder höher ist erforderlich, um die Funktion für den Hostsperrmodus in Oracle ILOM zu verwenden.
- Die Funktion für den Hostsperrmodus ist standardmäßig deaktiviert.

1. **Navigieren Sie zur Seite "KVMS" in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "Remote Console" -> "KVMS".**
   - **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "Remote Control" -> "KVMS".**

2. **Führen Sie im Abschnitt "Host Lock Settings" der Seite "KVMS" eine der folgenden Aktionen aus.**

   - **Geben Sie einen Sperrmodus an ("Windows", "Custom" oder "Disabled").**
   - **Klicken Sie auf "Save", um die Änderung anzuwenden.**

Zusätzliche Informationen

- Lock Host Desktop im *Oracle ILOM Administrator Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Lock Host Desktop in *Oracle ILOM 3.1 Configuration and Maintenance*
- KVMS Lock in *Oracle ILOM 3.0 Remote Redirection Consoles CLI and Web Guide*

▼ Einschränken anzeigbarer KVMS-Sitzungen für Remote System Console Plus (3.2.4 oder höher)

Ab Firmwarerelease 3.2.4 kann ein primärer Remote System Console Plus-Benutzer verhindern, dass andere angemeldete Sitzungsbenutzer am SP vertrauliche Daten anzeigen,

die während einer Videoumleitungssitzung eingegeben wurden. Dazu wird die maximale Anzahl Clientsitzungen auf einen (1) Sitzungsbetrachter eingeschränkt. Standardmäßig ist die Eigenschaft für die maximale Anzahl Clientsitzungen für Oracle ILOM Remote System Console Plus auf vier Sitzungsbetrachter gesetzt.

Im Folgenden finden Sie webbasierte Anweisungen zum Ändern der Eigenschaft für die maximale Anzahl Clientsitzungen für Oracle ILOM Remote System Console Plus.

Bevor Sie beginnen

- Die KVMS-Eigenschaft für die maximale Anzahl Clientsitzungen für Oracle ILOM Remote System Console Plus ist ab Firmwarerelease 3.2.4 verfügbar.

Anmerkung - Die KVMS-Eigenschaft für die maximale Anzahl Clientsitzungen kann auf Systemen, die Oracle ILOM Remote Console unterstützen, nicht konfiguriert werden.

- Oracle ILOM Remote System Console Plus ist nur auf neu veröffentlichten SP-Systemen ab Firmwarerelease 3.2.1 verfügbar.
- Die Rolle Konsole (c) ist in Oracle ILOM erforderlich, um die KVMS-Eigenschaft zur maximalen Anzahl Clientsitzungen zu ändern.
- Nach dem Zurücksetzen der Eigenschaft für die maximale Anzahl Clientsitzungen in Oracle ILOM werden alle aktiven Oracle ILOM Remote System Console Plus-Videositzungen am SP beendet.
- Standardmäßig können höchstens vier Remote System Console Plus-Videoumleitungssitzungen pro SP von der Umleitungsseite in Oracle ILOM gestartet werden.

1. **Navigieren Sie zur Seite "KVMS" in der Oracle ILOM-Webbenutzeroberfläche, indem Sie auf "Remote Console" -> "KVMS" klicken.**
2. **Ändern Sie auf der Seite "KVMS" die Eigenschaft "Maximum Client Session Count" (mögliche Werte: *4* (Standard)|*1*|*2*|*3*).**
3. **Klicken Sie auf "Save", um die Änderung anzuwenden.**

Zusätzliche Informationen

- Eigenschaften der Remotegeräteumleitung, *Oracle ILOM - Administratorhandbuch für Konfiguration und Wartung (Firmware 3.2.x)*

▼ Sicherer Systemzugriff mit Anmeldebanner (3.0.8 und höher)

Ab Firmwarerelease 3.0.8 können Systemadministratoren in Oracle ILOM eine Bannermeldung für alle Benutzer anzeigen, die sich bei der Oracle ILOM-CLI und -Webbenutzeroberfläche anmelden. Ein Anmeldebanner kann zum Schutz vor unautorisiertem Systemzugriff mit

Remotegeräten dienen und autorisierte und berechtigte Benutzer auf ihre Pflichten in Bezug auf die angemessene Nutzung des Systems hinweisen.

Die verwendete Bannermeldung muss Ihrer Informationssicherheitsrichtlinie entsprechen. Weitere Richtlinien zur verfassten Meldung erhalten Sie beim Siteadministrator oder Sicherheitsbeauftragten.

Im Folgenden finden Sie webbasierte Anweisungen zum Anzeigen einer Bannermeldung für alle Benutzer bei der Anmeldung oder nach der Anmeldung.

Bevor Sie beginnen

- Die Rolle Admin (a) ist erforderlich, um eine Bannermeldung zu erstellen.
- Die Bannermeldung kann ab Oracle ILOM-Firmwarerelease 3.0.8 konfiguriert werden.
- Administratoren können die Bannermeldung so konfigurieren, dass sie entweder auf der Anmeldeseite angezeigt wird oder in einem Dialogfeld, das unmittelbar nach der Anmeldung bei Oracle ILOM eingeblendet wird.

1. **Navigieren Sie zur Seite "Banner Message" in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "System Information" -> "Banner Messages".**
   - **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "ILOM Administration" -> "Management Access" -> "Banner Messages".**

2. **Klicken Sie auf der Seite "Banner Message" auf den Link** *More Details...*, **um zu bestimmen, wie eine Bannermeldung konfiguriert werden soll.**

   CLI-Anweisungen finden Sie im entsprechenden *Oracle ILOM - Administrationshandbuch*, das im Abschnitt "Zusätzliche Informationen" für diese Prozedur aufgeführt wird.

3. **Klicken Sie auf Speichern, um die Änderungen anzuwenden.**

Zusätzliche Informationen

- „Management of Banner Messages at Log-In“ im *Oracle ILOM - Administratorhandbuch für Konfiguration und Wartung (Firmware 3.2.x)*
- Verwalten von Bannermeldungen, *Oracle ILOM - Administratorhandbuch für Konfiguration und Wartung (Firmware 3.2.x)*
- Eigenschaften der Konfiguration von Bannermeldungen, *Oracle ILOM 3.1 - Konfigurations- und Wartungshandbuch*
- Anzeigen der Bannermeldung, *Oracle ILOM 3.0 - Allgemeine Verwaltung - CLI-Prozeduren - Handbuch*
- Anzeigen der Bannermeldung, *Oracle ILOM 3.0 - Allgemeine Verwaltung - Webprozeduren - Handbuch*

Konfigurieren der Oracle ILOM-Benutzeroberflächen für maximale Sicherheit

Die folgenden Themen enthalten Informationen zum Konfigurieren der Oracle ILOM-Benutzeroberflächen für maximale Sicherheit:

Konfigurieren der Webbenutzeroberfläche für maximale Sicherheit

Die folgenden Themen enthalten Informationen zur optimalen Konfiguration der Oracle ILOM-Webbenutzeroberfläche für maximale Sicherheit.

Anmerkung - Sie können die Eigenschaften der Webverwaltungsoberfläche in Oracle ILOM mit der Befehlszeilenschnittstelle (CLI) oder der Webbenutzeroberfläche konfigurieren. Die Verfahren in diesem Abschnitt liefern webbasierte Navigationsanweisungen für alle Oracle ILOM-Firmware-Versionen. Die CLI-Anweisungen bzw. zusätzliche Details zu Konfigurationseigenschaften finden Sie in der entsprechenden Dokumentation im Abschnitt "Zusätzliche Informationen" nach jedem Verfahren.

Verbessern der Sicherheit durch Verwendung eines vertrauenswürdigen SSL-Zertifikats und privaten Schlüssels

SSL-Zertifikate (Secure Socket Layer) werden sowohl zur Verschlüsselung von Netzwerkkommunikation als auch Authentifizierung eines Servers oder Clients verwendet. Oracle ILOM umfasst ein selbstsigniertes SSL-Zertifikat, mit dem das HTTPS-Protokoll Out-of-the-Box verwendet werden kann, ohne dass ein Zertifikat hochgeladen werden muss. Wenn zum ersten Mal eine Verbindung mit der Oracle ILOM-Webbenutzeroberfläche hergestellt wird, erhält der Benutzer eine Meldung, dass ein selbstsigniertes Zertifikat verwendet wird. Er

wird aufgefordert, die Verwendung dieses Zertifikats zu akzeptieren. Durch die Verwendung dieses Zertifikats wird die komplette Kommunikation zwischen Webbrowser und Oracle ILOM verschlüsselt.

Es ist jedoch möglich, stattdessen ein vertrauenswürdiges Zertifikat zu erstellen und hochzuladen, um die Sicherheit zu erhöhen. Ein Zertifikat ist vertrauenswürdig, wenn es von einer vertrauenswürdigen Certificate Authority ausgegeben wird. Ein vertrauenswürdiges Zertifikat von einer bekannten Certificate Authority trägt zur Authentizität des Oracle ILOM-Webservers bei. Durch Verwendung nicht vertrauenswürdiger, d.h. selbstsignierter, Zertifikate besteht die Gefahr, Ziel eines MITM-Angriffs (Man in the Middle) zu werden.

In den folgenden Themen finden Sie Informationen zum Erhalten und Hochladen eines temporären selbstsignierten oder von einer Certificate Authority signierten Zertifikats.

- Abrufen eines SSL-Zertifikats und privaten Schlüssels mit OpenSSL [39]
- Hochladen eines benutzerdefinierten SSL-Zertifikats und privaten Schlüssels in Oracle ILOM [41]

▼ Abrufen eines SSL-Zertifikats und privaten Schlüssels mit OpenSSL

Dieses Verfahren stellt eine vereinfachte Beschreibung davon dar, wie Sie ein SSL-Zertifikat und einen privaten Schlüssel mit dem OpenSSL-Toolkit erstellen.

Anmerkung - Es ist in Oracle ILOM *nicht* erforderlich, SSL-Zertifikate mit OpenSSL zu generieren. OpenSSL wird in diesem Verfahren lediglich zu Demonstrationszwecken eingesetzt. Sie können SSL-Zertifikate auch mit anderen Tools generieren.

Ob die Verwendung eines temporären selbstsignierten oder von einer Certificate Authority signierten Zertifikats erforderlich ist, sollte vom Siteadministrator oder Sicherheitsbeauftragten bestimmt werden. Sollten Sie ein SSL-Zertifikat (ob temporär selbstsigniert oder von Certificate Authority signiert) benötigen, können Sie den unten stehenden OpenSSL-Beispielanweisungen für die Befehlszeile folgen.

Anmerkung - Wenn weitere OpenSSL-Anweisungen erforderlich sind, um das SSL-Zertifikat zu generieren, schlagen Sie in der Benutzerdokumentation für das OpenSSL-Toolkit nach.

---

1. **Erstellen Sie eine Netzwerkfreigabe oder ein lokales Verzeichnis, um das Zertifikat und den privaten Schlüssel zu speichern.**

2. **Um einen neuen privaten RSA-Schlüssel mit dem OpenSSL-Toolkit zu erstellen, geben Sie Folgendes ein:**

   ```
   openssl genrsa -out <foo>.key 2048
   ```

   Dabei entspricht <*foo*> dem Namen des privaten Schlüssels.

Anmerkung - Dieser private Schlüssel ist ein 2048-Bit-RSA-Schlüssel, der im PEM-Format gespeichert ist, damit er als ASCII-Text gelesen werden kann.

3. **Um eine Zertifikatssignieranforderung (Certificate Signing Request, CSR) mit dem OpenSSL-Toolkit zu generieren, geben Sie Folgendes ein:**

   `openssl req -new -key <`*foo*`>.key -out <`*foo*`>.csr`

   Dabei entspricht <*foo*> dem Namen der Zertifikatssignieranforderung.

   Anmerkung - Bei der Generierung der CSR müssen Sie verschiedene Informationen angeben.

   Die Datei <*foo*>`.csr` sollte nun im aktuellen Arbeitsverzeichnis angezeigt werden.

4. **Führen Sie eine der folgenden Aktionen aus, um ein SSL-Zertifikat zu generieren:**

   - **Generieren Sie ein temporäres selbstsigniertes Zertifikat (365 Tage gültig).**

     Das selbstsignierte SSL-Zertifikat wird aus dem privaten `server.key`-Schlüssel und den `server.csr`-Dateien generiert.

     Geben Sie Folgendes in das OpenSSL-Toolkit ein:

     `openssl x509 -req -days 365 -in <`*foo*`>.csr`

     `-signkey <`*foo*`>.key -out <`*foo*`>.cert`

     Dabei entspricht <*foo*> dem Namen des privaten Schlüssels (`.key`) oder Zertifikats (`.cert`).

     Anmerkung - Bei diesem temporären Zertifikat wird ein Fehler im Clientbrowser generiert, der angibt, dass die signierende Certificate Authority unbekannt und nicht vertrauenswürdig ist. Wenn dieser Fehler nicht akzeptabel ist, müssen Sie die Ausstellung eines signierten Zertifikats bei der Certificate Authority anfordern.

   - **Rufen Sie ein offiziell signiertes Zertifikat von einem Certificate Authority-Provider ab.**

     Leiten Sie die Zertifikatssignieranforderung (<*foo*>`.csr`) an einen SSL-Certificate Authority-Provider weiter. Bei den meisten Certificate Authority-Providern müssen Sie die CSR-Ausgabe ausschneiden und in den Bildschirm einer Webanwendung einfügen. Es kann normalerweise bis zu sieben Werktage dauern, bis Sie das signierte Zertifikat erhalten.

5. **Laden Sie das neue SSL-Zertifikat und den privaten Schlüssel in Oracle ILOM hoch.**

Anweisungen dazu finden Sie unter Hochladen eines benutzerdefinierten SSL-Zertifikats und privaten Schlüssels in Oracle ILOM [41].

▼ Hochladen eines benutzerdefinierten SSL-Zertifikats und privaten Schlüssels in Oracle ILOM

Bevor Sie beginnen

- Die Rolle Admin (a) ist erforderlich, um die Webservereigenschaften in Oracle ILOM zu ändern.
- Rufen Sie das neue (temporäre selbstsignierte oder von einer Certificate Authority signierte) HTTPS-Zertifikat und den privaten Schlüssel ab. Anweisungen zur Verwendung des OpenSSL-Toolkits finden Sie unter Abrufen eines SSL-Zertifikats und privaten Schlüssels mit OpenSSL [39].
- Stellen Sie sicher, dass Sie über Ihr Netzwerk oder lokales Dateisystem auf das neue HTTPS-Zertifikat und den privaten Schlüssel zugreifen können.

1. **Navigieren Sie zur Seite "SSL Certificate" in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "Configuration" -> "System Management Access" -> "SSL Certificate".**
   - **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "ILOM Administration" -> "Management Access" -> "SSL Certificate".**

2. **Führen Sie auf der Seite "SSL Server" folgende Aktionen aus:**

   a. **Klicken Sie auf die Schaltfläche "Load Certificate", um die benutzerdefinierte Zertifikatsdatei hochzuladen, die in den Eigenschaften der Dateiübertragungsmethode angegeben ist.**

   b. **Klicken Sie auf die Schaltfläche "Load Custom Private Key", um die Datei des benutzerdefinierte privaten Schlüssels hochzuladen, die in den Eigenschaften der Dateiübertragungsmethode angegeben ist.**

   c. **Klicken Sie auf "Save", um die Änderungen anzuwenden.**

Zusätzliche Informationen

- SSL Certificate and Private Key Configuration Properties im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*

- SSL Certificate and Private Key Configuration Properties im *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Hochladen des SSL-Zertifikats, *Oracle ILOM 3.0 - Allgemeine Verwaltung - CLI-Prozeduren - Handbuch*
- Hochladen des SSL-Zertifikats, *Oracle ILOM 3.0 - Allgemeine Verwaltung - Webprozeduren - Handbuch*

▼ Aktivieren der sichersten SSL- und TLS-Verschlüsselungseigenschaften

Oracle ILOM unterstützt die sichersten Secure Socket Layer-Verschlüsselungsprotokolle (SSLv3 und TLS v1.0, v1.1 und v1.2) mit den sichersten Ciphers. In einigen Fällen müssen Sie aber möglicherweise SSLv2 oder schwächere Ciphers aktivieren, damit ältere Webbrowser verwenden werden können.

Mit dieser Prozedur können Sie die SSL- und TLS-Eigenschaften in Oracle ILOM festlegen, damit sie Ihren Anforderungen an die Sicherheitsrichtlinien entsprechen.

Anmerkung - SSL und TLSv1.0 werden ab Firmwarerelease 3.1.0 unterstützt. TLS v1.1 und v1.2 werden ab Firmwarerelease 3.2.4 in Oracle ILOM unterstützt.

Bevor Sie beginnen

- Die Rolle Admin (a) ist erforderlich, um die Webservereigenschaften in Oracle ILOM zu ändern.
- Die Standardeinstellung für die TLS-Eigenschaft in Oracle ILOM hängt von der Firmwareversion ab, die aktuell auf dem Server installiert ist.

Firmware	TLS-Standardwert
3.1.x, 3.2.1.x, 3.2.2.x und 3.2.3.x	TLS v1.0 aktiviert
3.2.4 und höher	TLS v1.0, v1.1 und v1.2 aktiviert

- Für Oracle ILOM-Firmwarereleases *vor* 3.2.4 ist die SSLv3-Eigenschaft standardmäßig aktiviert.

Anmerkung - Aufgrund einer Sicherheitslücke, die bei SSLv3 ermittelt wurde, müssen Sie SSLv3 deaktivieren, bis ein Fix verfügbar ist. Weitere Einzelheiten finden Sie unter Oracle: MOS SSLv3 Vulnerability Article.

- Bei Oracle ILOM-Firmwarerelease 3.2.4.x und höher hängt die SSLv3-Standardeinstellung von dem Servermodell und der installierten 3.2.4.x-Firmwareversion ab.

Servermodell	Firmware	SSLv3-Standardwert
SPARC T3, T4, T5, M5, M6	3.2.4.1	SSLv 3 deaktiviert
X4-2 X4-2L X4-2B	3.2.4.20 (x4-2) 3.2.4.22 (x4-2L) 3.2.24.24 (X4-2B)	SSLv3 aktiviert Weitere Einzelheiten finden Sie unter: MOS SSLv3 Vulnerability Article.
X4-4 X4-8	3.2.4.18	SSLv3 aktiviert Weitere Einzelheiten finden Sie unter: MOS SSLv3 Vulnerability Article.
X5-2 X5-2L	3.2.4.10 (x5-2) 3.2.4.12 (x5-2L)	SSLv3 deaktiviert

- Die Eigenschaften "SSLv2" und "Schwache Ciphers" in Oracle ILOM sind standardmäßig deaktiviert

Im Folgenden finden Sie webbasierte Anweisungen zum Anzeigen oder Ändern der SSL- oder TLS-Webserver-Sicherheitseigenschaften in Oracle ILOM.

1. **Klicken Sie in der Oracle ILOM-Webbenutzeroberfläche auf "ILOM Administration" -> "Management Access" -> "Web Server".**
2. **Zeigen Sie auf der Seite "Web Server" die Websicherheitseigenschaften für SSL, TLS oder schwache Ciphers an, oder ändern Sie diese.**
3. **Klicken Sie auf "Save", um die Änderungen anzuwenden.**

Zusätzliche Informationen

- Web Server Configuration Properties im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Web Server Configuration Properties im *Oracle ILOM 3.1 Configuration and Maintenance Guide*

▼ Festlegen eines Timeoutintervalls für inaktive Websitzungen

Die Timeoutintervalle für Oracle ILOM-Websitzungen bieten Sicherheit für Webzugriffsbenutzer, die sich nicht abmelden. Mit den Timeoutintervallen für Websitzungen können Sie bestimmen, wie viele Minuten bis zur automatischen Abmeldung von einer inaktiven HTTP- oder HTTPS-Websitzung verstreichen können. Diese Funktion reduziert das Risiko, dass nicht autorisierte Benutzer einen unbeaufsichtigten Computer auffinden, auf dem eine authentifizierte Oracle ILOM-Websitzung ausgeführt wird.

Im Folgenden finden Sie webbasierte Anweisungen zum Anzeigen oder Ändern der festgelegten Timeoutintervalle für HTTP- und HTTPS-Websitzungen.

Bevor Sie beginnen

- Das standardmäßig festgelegte Timeoutintervall für HTTP- und HTTPS-Websitzungen beträgt 15 Minuten.

Anmerkung - Ein kürzeres Sitzungstimeout hätte zur Folge, dass Benutzer während einer bestehenden Sitzung Benutzername und Passwort möglicherweise häufiger erneut eingeben müssen. Bei einem kürzeren Sitzungstimeout bleiben unbeaufsichtigte authentifizierte Websitzungen allerdings auch weniger lang aktiv.

- Die Rolle Admin (a) ist erforderlich, um die Webservereigenschaften zu ändern.
- Die Timeoutintervalleigenschaften für HTTP- und HTTPS-Sitzungen können in Oracle ILOM nur für Server-SPs mit Firmware-Version 3.0.4 oder höher konfiguriert werden.

1. **Navigieren Sie zur Seite "Web Server".**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "Configuration" -> "System Management Access" -> "Web Server".**
   - **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "ILOM Administration" -> "Management Access" -> "Web Server".**

2. **Führen Sie auf der Seite "Web Server" folgende Aktionen aus:**

   a. **Navigieren Sie zur Eigenschaft für den HTTP- oder HTTP-Sitzungstimeout.**

   b. **Geben Sie eine Zahl zwischen 1 und 720 Minuten ein, um anzugeben, wie viele Minuten bis zur automatischen Abmeldung von einer inaktiven Websitzung verstreichen können.**

   c. **Klicken Sie auf "Save", um die Änderungen anzuwenden.**

Zusätzliche Informationen

- Web Server Configuration Properties im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Web Server Configuration Properties im *Oracle ILOM 3.1 Configuration and Maintenance Guide*

- Festlegen des Sitzungstimeouts, *Oracle ILOM 3.0 - Allgemeine Verwaltung - Webprozeduren - Handbuch*

Konfigurieren der CLI für maximale Sicherheit

Die folgenden Themen enthalten Informationen zur optimalen Konfiguration der Oracle ILOM-Befehlszeilenschnittstelle (CLI) für maximale Sicherheit.

Sie können die CLI-Verwaltungseigenschaften in Oracle ILOM mit der Befehlszeilenschnittstelle (CLI) oder der Webbenutzeroberfläche konfigurieren. Die Verfahren in diesem Abschnitt liefern webbasierte Navigationsanweisungen für alle Oracle ILOM-Firmware-Versionen. Die CLI-Anweisungen bzw. zusätzliche Details zu Konfigurationseigenschaften finden Sie in der entsprechenden Dokumentation im Abschnitt "Zusätzliche Informationen" nach jedem Verfahren.

▼ Verwaltung von SSH-Serverstatus und schwachen Ciphers (3.2.5 und höher)

Ab Firmwarerelease 3.2.5 sind die Eigenschaften "SSH-Serverstatus" und "Schwache Ciphers" in der Oracle ILOM-CLI und Webbenutzeroberfläche konfigurierbar. Im Hinblick auf maximale Sicherheit ist die Eigenschaft "SSH-Serverstatus" aktiviert und die Eigenschaft "Schwache Ciphers" deaktiviert. In den folgenden webbasierten Anweisungen wird beschrieben, wie diese Eigenschaften für den Zugriff auf die SSH-Verwaltung geändert werden.

1. **Klicken Sie in der Oracle ILOM-Webbenutzeroberfläche auf "ILOM Administration" -> "Management Access" -> "SSH Server".**
2. **Klicken Sie auf der Seite "SSH Server" auf den Link** *More Details...*, **um weitere Anweisungen zu erhalten.**
3. **Klicken Sie auf Speichern, um die Änderungen anzuwenden.**

Zusätzliche Informationen

- Verwaltung von SSH-Serverstatus und schwachen Ciphers, *Oracle ILOM - Administratorhandbuch für Konfiguration und Wartung (Firmware 3.2.x)*

▼ Festlegen eines Timeoutintervalls für inaktive CLI-Sitzungen

Auf die Oracle ILOM-CLI kann über eine Oracle ILOM-Verbindung über das Secure Shell-(SSH-)Protokoll oder mit einer seriellen Verbindung zugegriffen werden. Sie unterstützt ein konfigurierbares Timeoutintervall für inaktive CLI-Sitzungen. Wenn Sie diese Funktion konfigurieren, wird das Risiko verringert, dass unautorisierte Benutzer einen unbeaufsichtigten Computer finden, auf dem eine authentifizierte Oracle ILOM-CLI-Sitzung ausgeführt wird.

Aus Sicherheitsgründen sollten Sie ein Timeoutintervall für CLI-Sitzungen in allen Umgebungen konfigurieren, in denen die Oracle ILOM-CLI auf einer gemeinsam genutzten Konsole verwendet wird. Optimal wäre ein Timeoutintervall für CLI-Sitzungen von höchstens 15 Minuten.

Im Folgenden finden Sie webbasierte Anweisungen zum Anzeigen oder Ändern der festgelegten Timeoutintervalleigenschaft für inaktive Oracle ILOM-CLI-Sitzungen.

Bevor Sie beginnen

- Die Rolle Admin (a) ist erforderlich, um die CLI-Eigenschaften zu ändern.
- Das standardmäßige CLI-Sitzungs-Timeoutintervall für SSH-Verbindungen ist deaktiviert und auf 0 (Null) Minuten gesetzt.

Anmerkung - Wenn das CLI-Timeoutintervall auf 0 (Null) gesetzt ist, werden inaktive CLI-Sitzungen nicht von Oracle ILOM geschlossen, unabhängig davon, wie lange sie inaktiv bleiben.

- Die Timeoutintervalleigenschaft für CLI-Sitzungen kann in Oracle ILOM nur für Server-SPs mit Firmware-Version 3.0.4 oder höher konfiguriert werden.

1. **Navigieren Sie zur Seite "CLI" in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "Configuration" -> "System Management Access" -> "CLI".**
   - **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "ILOM Administration" -> "Management Access" -> "CLI".**

2. **Legen Sie auf der Seite "CLI" ein Timeoutintervall für CLI-Sitzungen fest, indem Sie folgende Aktionen ausführen.**

   a. **Aktivieren Sie das Kontrollkästchen "Enable".**

   b. **Geben Sie eine Zahl zwischen 1 und 1440 Minuten ein, um anzugeben, wie viele Minuten bis zur automatischen Abmeldung von einer inaktiven Befehlszeilensitzung verstreichen können.**

c. **Klicken Sie auf "Save", um die Änderungen anzuwenden.**

Zusätzliche Informationen

- CLI Session Time-Out Configuration Properties im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- CLI Session Time-Out Configuration Properties im *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Set a CLI Session Time-Out in *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*

▼ Verwenden von serverseitigen Schlüsseln zum Verschlüsseln von SSH-Verbindungen

Die in Oracle ILOM integrierte SSH-Serverfunktion (Secure Shell) bietet die Möglichkeit einer sicheren Verbindung zwischen Remoteclients und Oracle ILOM, sodass Oracle ILOM über eine Befehlszeilenschnittstelle verwaltet werden kann. Das SSH-Protokoll verwendet serverseitige Schlüssel, um den Verwaltungskanal zu verschlüsseln und die gesamte Kommunikation zu sichern. SSH-Clients verwenden diese Schlüssel auch zur Überprüfung der Authentizität des SSH-Servers.

Oracle ILOM generiert einen Satz eindeutiger SSH-Schlüssel beim Erststart eines Standardsystems mit werkseitigen Einstellungen. Falls neue serverseitige Schlüssel benötigt werden, können in Oracle ILOM zusätzliche serverseitige SSH-Schlüssel manuell generiert werden.

Im Folgenden finden Sie webbasierte Anweisungen zum Anzeigen oder manuellen Generieren von serverseitigen SSH-Verschlüsselungsschlüsseln.

Bevor Sie beginnen

- Die Rolle Admin (a) ist erforderlich, um die SSH-Servereigenschaften zu ändern.

1. **Navigieren Sie zur Seite "SSH Server" in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "System Management" -> "SSH Server".**
   - **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "ILOM Administration" -> "Management Access" -> "SSH Server".**

2. **Prüfen Sie auf der Seite "SSH Server" die Informationen zu den generierten RSA- und DSA-Schlüsseln, oder führen Sie folgende Aktionen aus:**

   a. **Klicken Sie auf "Generate RSA Key", um einen neuen Schlüssel zu generieren.**

   b. **Klicken Sie auf "Generate DSA Key", um einen neuen Schlüssel zu generieren.**

Zusätzliche Informationen

- SSH Server Configuration Properties im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- SSH Server Configuration Properties im *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Generate a New SSH Key in *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*
- Generate a New SSH Key in *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*

▼ Anhängen von SSH-Schlüsseln an Benutzerkonten für automatisierte CLI-Authentifizierung

Individuell generierte SSH-Schlüsselpaare (DSA oder RSA) können für einzelne Benutzerkonten verwendet werden, wobei der öffentliche Schlüssel in Oracle ILOM hochgeladen wird. Dies ist bei der Verwendung von Skripten nützlich, die ohne manuelle Eingriffe ausgeführt werden und keine eingebetteten Klartextpasswörter enthalten. Benutzer können Skripte erstellen, mit denen Serviceprozessorbefehle über eine netzwerkbasierte SSH-Verbindung von einem Remotesystem aus automatisch oder regelmäßig ausgeführt werden.

Im Folgenden finden Sie webbasierte Anweisungen zum Hochladen und Anhängen eines generierten öffentlichen SSH-Schlüssels an ein Oracle ILOM-Konto.

Bevor Sie beginnen

- Generieren Sie den die privaten und öffentlichen SSH-Schlüssel mit einem SSH-Konnektivitätstool, wie ssh-keygen, und speichern Sie die generierten SSH-Schlüsseldateien dann in einem Remote-SSH-System.
- Die Rolle Benutzerverwaltung (u) ist erforderlich, um öffentliche SSH-Schlüssel an andere Benutzerkonten anzuhängen.
- Die Rolle Schreibgeschützt (o) ist erforderlich, um einen öffentlichen SSH-Schlüssel an Ihr eigenes Benutzerkonto anzuhängen.

1. **Navigieren Sie zur Seite "User Account" in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

- **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "User Management" -> "User Accounts".**
- **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "ILOM Administration" ->"User Management" -> "User Accounts".**

2. **Führen Sie auf der Seite "User Account" folgende Aktionen aus:**

   a. **Blättern Sie zum Abschnitt "SSH Keys", und klicken Sie auf "Add".**

   b. **Wählen Sie ein Benutzerkonto in der Benutzerliste.**

   c. **Wählen Sie eine Übertragungsmethode in der Liste, und geben Sie dann die erforderlichen Übertragungsmethodeneigenschaften zum Hochladen des öffentlichen SSH-Schlüssels an.**

3. **Klicken Sie auf "Load", um den öffentlichen SSH-Schlüssel hochzuladen und an das gewählte Benutzerkonto anzuhängen.**

Zusätzliche Informationen

- CLI Authentication Using Local SSH Key im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- CLI Authentication Using Local SSH Key im *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Managing User Accounts in *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*
- Managing User Accounts in *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*

Konfigurieren des SNMP-Verwaltungszugriffs für maximale Sicherheit

SNMP ist ein Standardprotokoll, das zur Systemüberwachung oder -verwaltung verwendet wird. Oracle ILOM bietet eine SNMP-Lösung, die nach entsprechender Konfiguration sowohl zur Überwachung als auch Verwaltung geeignet ist. Es ist wichtig, dass Sie sich vor der Konfiguration des Service über die Auswirkungen auf die Sicherheit der einzelnen SNMP-Optionen informieren, die Benutzer konfigurieren können. Einzelheiten dazu finden Sie in den folgenden Informationen:

- Verwenden von SNMPv3-Verschlüsselung und Benutzerauthentifizierung [50]
- „Sun-SNMP-MIBs, die konfigurierbare Objekte unterstützen“ [51]

▼ Verwenden von SNMPv3-Verschlüsselung und Benutzerauthentifizierung

SNMPv1 und SNMPv2c bieten keine Verschlüsselung und führen die Authentifizierung anhand von Communityzeichenfolgen durch. Communityzeichenfolgen werden über das Netzwerk in Klartext übertragen und üblicherweise von einer Gruppe gemeinsam und nicht von einem einzelnen Benutzer privat genutzt. Bei SNMPv3 hingegen werden die Verschlüsselung zum Erreichen eines sicheren Kanals sowie individuelle Benutzernamen und Passwörter verwendet. SNMPv3-Benutzerpasswörter sind lokalisiert, sodass sie sicher auf Verwaltungsstationen abgespeichert werden können.

SNMPv1, SNMPv2c und SNMPv3 werden von Oracle ILOM unterstützt und können einzeln aktiviert bzw. deaktiviert werden. Außerdem können "Sätze" aktiviert oder deaktiviert werden, um eine zusätzliche Sicherheitsebene bereitzustellen. Durch diese konfigurierbare Option wird bestimmt, ob der SNMP-Service das Festlegen von konfigurierbaren SNMP-MIB-Eigenschaften zulässt. Das Deaktivieren von Sätzen bewirkt, dass der SNMP-Service nur für die Überwachung effektiv eingesetzt werden kann.

SNMPv1 und SNMPv2c sind standardmäßig deaktiviert. SNMPv3 ist zwar standardmäßig aktiviert, es muss aber vor der Verwendung mindestens ein SNMP-Benutzer erstellt werden. Es sind keine vorkonfigurierten SNMPv3-Benutzer vorhanden.

Im Folgenden finden Sie webbasierte Anweisungen zum Konfigurieren der SNMP-Verwaltung in Oracle ILOM.

Bevor Sie beginnen

- Wenn Sie die höchstmögliche SNMP-Sicherheit erreichen möchten, verwenden Sie SNMPv1 und SNMPv2c nur für die Überwachung, und aktivieren Sie keine Sätze, wenn diese beiden Protokolle, die nicht das Maximum an Sicherheit bieten, aktiviert sind.
- Aktivieren Sie SNMP-Sätze nur für die SNMPv3-Verwaltung. Die Eigenschaft "SNMP Set" ist standardmäßig deaktiviert.
- SNMPv3-Sätze erfordern die Konfiguration von SNMPv3-Benutzerkonten. Es sind keine vorkonfigurierten SNMPv3-Benutzerkonten verfügbar.
- Die SNMP-Serviceeigenschaft "State" ist standardmäßig aktiviert.
- Berechtigungen der Rolle Admin (a) sind erforderlich, um die SNMP-Eigenschaften zu ändern.
- Berechtigungen für die Benutzerverwaltung (u) sind erforderlich, um SNMPv3-Benutzerkonten hinzuzufügen oder zu ändern.

1. **Navigieren Sie zur Seite "SNMP" in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "System Management Access" -> "SNMP".**

- **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "ILOM Administration" -> "Management Access" -> "SNMP".**

2. **Ändern Sie auf der Seite "SNMP" die SNMP-Eigenschaften, und klicken Sie dann auf "Save", um die Änderungen anzuwenden.**

   Weitere Anweisungen finden Sie in der entsprechenden Dokumentation im Abschnitt "Zusätzliche Informationen" für dieses Verfahren. Benutzer mit Firmware-Version 3.2 oder höher erhalten weitere Informationen durch Klicken auf den Link `More details` auf der SNMP-Seite.

Zusätzliche Informationen

- Configuring SNMP Settings im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Configuring SNMP Settings in der *Oracle ILOM Protocol Management Reference for SNMP and IPMI (Firmware 3.2.x)*
- Configuring SNMP Settings in der *Oracle ILOM 3.1 SNMP, IPMI, CIM, and WS-Man Protocol Management Reference*
- Configuring SNMP Settings in der *Oracle ILOM 3.0 SNMP, IPMI, CIM, and WS-Man Protocol Management Reference*

Sun-SNMP-MIBs, die konfigurierbare Objekte unterstützen

Sun-MIBs von Oracle, die konfigurierbare Objekte unterstützen und bei denen "Sätze" angewendet werden können, lauten wie folgt:

- `SUN-HW-CTRL-MIB` – Mit dieser MIB werden Hardwarerichtlinien, wie beispielsweise Stromverwaltungsrichtlinien, konfiguriert.
- `SUN-ILOM-CONTROL-MIB` – Mit dieser MIB werden Oracle ILOM-Funktionen wie Benutzererstellung und Servicekonfiguration konfiguriert.

Anmerkung - Sie können ein MIB-Objekt festlegen, wenn: 1) das MIB-Objekt Modifizierungen unterstützt; 2) das `MAX-ACCESS`-Element für das MIB-Objekt auf `read-write` festgelegt ist, und 3) der Benutzer, der versucht, den Satz auszuführen, dafür autorisiert ist.

Konfigurieren des IPMI-Verwaltungszugriffs für maximale Sicherheit

Die folgenden Themen enthalten Informationen zur optimalen Konfiguration des Oracle ILOM IPMI-Verwaltungszugriffs für maximale Sicherheit.

▼ Verwenden von IPMI v2.0 für erweiterte Authentifizierung und Paketverschlüsselung

Oracle ILOM unterstützt zwar IPMI 1.5 und 2.0 für Remoteverwaltung, jedoch sollten Systemadministratoren immer die IPMI 2.0 -l lanplus-Schnittstelle verwenden, um Oracle-Server sicher verwalten zu können. Die -l lanplus-Schnittstelle bietet erweiterte Authentifizierungs- und Datenintegrationsprüfungen ab IPMI-Version 2.0.

Ab Firmware-Version 3.2.4 bietet Oracle ILOM eine konfigurierbare Eigenschaft für die Aktivierung oder Deaktivierung von IPMI v1.5-Sitzungen. Für ein hohes Maß an Sicherheit ist die IPMI v1.5-Eigenschaft standardmäßig deaktiviert. Wenn die IPMI v1.5-Eigenschaft deaktiviert ist, werden alle IPMI v1.5-Sitzungsverbindungen mit Oracle ILOM verhindert (blockiert).

Im Folgenden finden Sie Informationen zum Anzeigen oder Ändern der IPMI-Serviceeigenschaft "State" oder der konfigurierbaren IPMI v1.5-Eigenschaft, die ab Firmware-Version 3.2.4 verfügbar ist.

Bevor Sie beginnen

- Die Rolle Admin (a) ist erforderlich, um IPMI-Eigenschaften in Oracle ILOM zu ändern.
- Die IPMI-Serviceeigenschaft "State" ist standardmäßig aktiviert. Vor der Verwendung müssen Benutzerkonten mit den richtigen rollenbasierten Berechtigungen (Administrator, Operator) in Oracle ILOM konfiguriert sein, um IPMI-Verwaltungsfunktionen ausführen zu können.
- Bei SPs mit Oracle ILOM-Firmware-Version 3.2.4 oder höher werden IPMI v2.0-Verwaltungssitzungen unterstützt, und IPMI v1.5-Verwaltungssitzungen werden standardmäßig nicht unterstützt. Die IPMI v1.5-Eigenschaft kann in Oracle ILOM konfiguriert werden.

Anmerkung - Wenn IPMI v1.5-Sitzungen in Oracle ILOM deaktiviert sind, müssen Benutzer von IPMItool die IPMI 2.0 -I lanplus-Option verwenden.

- Bei SPs mit Oracle ILOM-Firmware-Version 3.2.3 oder älter werden IPMI v2.0- und v1.5-Verwaltungssitzungen von Oracle ILOM unterstützt. Die IPMI v1.5-Eigenschaft kann nicht in Oracle ILOM konfiguriert werden.

Anmerkung - Bei IPMI v1.5-Sitzungen wird keine erweiterte Authentifizierung oder Paketverschlüsselung unterstützt. Für die erweiterte Authentifizierung und IPMI-Paketverschlüsselung müssen Sie IPMI v2.0 verwenden.

1. **Navigieren Sie zur Seite "IPMI" in der Oracle ILOM-Webbenutzeroberfläche.**
   Beispiele:

   - **Klicken Sie in der 3.0-Webbenutzeroberfläche auf "Configuration" -> "System Management Access" -> "IPMI".**
   - **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "ILOM Administration" -> "Management Access" -> "IPMI".**

2. **Zeigen Sie auf der Seite "IPMI" die IPMI-Eigenschaften an, und konfigurieren Sie diese bei Bedarf. Klicken Sie dann auf "Save", um die Änderungen anzuwenden.**
   Zusätzliche IPMI-Konfigurationsanweisungen finden Sie in der entsprechenden Dokumentation im Abschnitt "Zusätzliche Informationen" weiter unten.

Zusätzliche Informationen

- Server Management Using IPMI in der *Oracle ILOM Protocol Management Reference for SNMP and IPMI (Firmware 3.2.x)*
- Server Management Using IPMI in der *Oracle ILOM 3.1 SNMP, IPMI, CIM, WS-MAN Protocol Management Reference*
- Server Management Using IPMI in der *Oracle ILOM 3.0 SNMP, IPMI, CIM, WS-MAN Protocol Management Reference*
- „IPMI-Sicherheitsrichtlinien und Best Practices“ [53]
- „Unterstützung von IPMI 2.0-Authentifizierung über Cipher Suite“ [54]

IPMI-Sicherheitsrichtlinien und Best Practices

Um sicherzustellen, dass eingerichtete IPMI-Systemverwaltungssitzungen sicher und nicht anfällig für Cyber-Angriffe sind, sollten Systemadministratoren:

- niemals IPMI-Remote-Verwaltungssitzungen mit IPMI-Version 1.5 (`-I lan` IPMItool-Schnittstelle) einrichten. Sie sollten die IPMI-Version 2.0 explizit mit Befehlszeilenutilitys wie IPMItools (`-I lanplus` IPMItool-Schnittstelle) verwenden.
- Ihr ILMI-Passwort regelmäßig ändern. Stellen Sie sicher, dass der Lebenszyklus von Oracle ILOM-Benutzerkonten angemessen verwaltet wird.

  Weitere Einzelheiten finden Sie unter „Sichern des Oracle ILOM-Benutzerzugriffs“ [25].

- Netzwerkzugriff von außen einschränken. Kommunizieren Sie über den dedizierten Ethernet-Verwaltungskanal mit Oracle ILOM.

  Weitere Einzelheiten dazu finden Sie unter „Sichern der physischen Verwaltungsverbindung“ [15].
- Zusammen mit dem IT-Sicherheitsbeauftragten eine Gruppe von Best Practices und Policys zu Serververwaltung und zur IPMI-Sicherheit erstellen

Unterstützung von IPMI 2.0-Authentifizierung über Cipher Suite

Authentifizierung, Vertraulichkeit und Integritätsprüfungen in IPMI Version 2.0 werden über Cipher Suites unterstützt. Diese Cipher Suites verwenden das RMCP+ Authenticated Key-Exchange Protocol wie in der IPMI 2.0-Spezifikation beschrieben.

Oracle ILOM unterstützt die folgenden Schlüsselalgorithmen der Cipher Suite, um sichere IPMI 2.0-Sitzungen zwischen Client und Server einzurichten.

- **Cipher Suite 2** – Cipher Suite 2 verwendet Authentifizierungs- und Integritätsalgorithmen.
- **Cipher Suite 3** – Cipher Suite 3 verwendet alle drei Algorithmen für Authentifizierung, Vertraulichkeit und Integrität.

Anmerkung - Um sicherzustellen, dass der gesamte IPMI 2.0-Datenverkehr verschlüsselt wird, implementiert Oracle ILOM keine Unterstützung für IPMI 2.0 Cipher Type 0 (unverschlüsselter Betriebsmodus).

Konfigurieren des WS-Management-Zugriffs für maximale Sicherheit

Zwischen Firmware-Version 3.0.8 und Firmware-Version 3.1.2 bietet Oracle ILOM eine standardmäßige Webservice-Schnittstelle zur Überwachung der Serverintegrität und zum Bereitstellen von Bestandsinformationen anhand des Protokolls WS-Management (WS-MAN).

Die WS-MAN-Schnittstelle von Oracle ILOM ermöglicht außerdem die Peerkontrolle des Hosts und das Zurücksetzen des Oracle ILOM-SP. Bei WS-MAN handelt es sich um ein SOAP-(Simple Object Access Protocol-)basiertes Protokoll, das die Protokolle HTTP und HTTPS verwendet. Die WS-MAN-Schnittstelle von Oracle ILOM kann in Verbindung mit HTTP oder HTTPS als Transport verwendet werden. Bei HTTPS wird der Kanal mithilfe eines SSL-Zertifikats verschlüsselt. Informationen zu den Vorteilen der Verwendung von SSL-Zertifikaten für die Sicherheit sowie zum Unterschied zwischen selbstsignierten und vertrauenswürdigen Zertifikaten finden Sie unter ??„Verbessern der Sicherheit durch Verwendung eines vertrauenswürdigen SSL-Zertifikats und privaten Schlüssels“ [38].

Verwenden Sie diese Webservice-Schnittstelle nur, wenn SSL-Zertifikate verwendet werden. Um ein Höchstmaß an Sicherheit zu gewährleisten, verwenden Sie HTTPS als Transportmechanismus. Weitere Informationen zum Konfigurieren der Webservereigenschaften finden Sie unter „Konfigurieren der Webbenutzeroberfläche für maximale Sicherheit“ [38].

Sicherheits-Best Practices nach dem Deployment für Oracle ILOM

Anhand der folgenden Themen können Sie die besten Oracle ILOM-Sicherheitsverfahren ermitteln, die nach dem Server-Deployment implementiert werden müssen.

Zusätzliche Informationen

- Sicherheits-Best Practices zum Deployment für Oracle ILOM
- Best Practice-Checklisten zur Sicherheit für Oracle ILOM

Aufrechterhalten einer sicheren Verwaltungsverbindung

Die folgenden Themen enthalten Informationen zum Aufrechterhalten einer sicheren Verwaltungsverbindung mit Oracle ILOM.

Verhindern von nicht authentifiziertem Host-KCS-Gerätezugriff

Bei Oracle-Servern wird eine langsame Standardverbindung, die KCS-(Keyboard Controller Style-)Schnittstelle, zwischen dem Host und Oracle ILOM unterstützt. Diese unterstützte KCS-

Schnittstelle ist mit der IPMI-Version 2.0 (Intelligent Platform Management Interface) voll kompatibel und kann ebenfalls nicht deaktiviert werden.

Während der KCS-Gerätezugriff eine praktische Art darstellen kann, Oracle ILOM vom Host aus zu konfigurieren, birgt diese Zugriffsart auch Sicherheitsrisiken, da alle Betriebssystembenutzer mit Kernel- oder Treiberzugriff auf das physische KCS-Gerät ohne Authentifizierung die Oracle ILOM-Einstellungen ändern können. Normalerweise können nur `root`- oder Administratorbenutzer auf das KCS-Gerät zugreifen. Die meisten Betriebssysteme können jedoch so konfiguriert werden, dass diese Benutzerbeschränkung erweitert wird.

Beispiel: Ein Betriebssystembenutzer mit KCS-Zugriff kann folgende Aktionen ausführen:

- Oracle ILOM-Benutzer hinzufügen oder erstellen
- Benutzerpasswörter ändern,
- auf die Oracle ILOM-CLI als ILOM-Administrator zugreifen,
- Protokolle und Hardwaredaten aufrufen.

Üblicherweise lautet der Name des Geräts unter Linux oder Oracle Solaris `/dev/kcs0` oder `/dev/bmc` und unter Microsoft Windows `ipmidrv.sys` oder `imbdrv.sys`. Der Zugriff auf dieses Gerät, auch als BMC-Treiber (Baseboard Management Controller) oder IPMI-Treiber bezeichnet, muss mithilfe entsprechender Zugriffskontrollmechanismen sorgsam kontrolliert werden, die Teil des Hostbetriebssystems sind.

Als Alternative zum Host-IPMI-KCS-Gerät können Sie Oracle ILOM-Einstellungen auch mit der Oracle ILOM Interconnect-Schnittstelle konfigurieren. Einzelheiten dazu finden Sie unter „Interconnect-Zugriff auf bevorzugten authentifizierten Host“ [58].

Weitere Informationen zum Kontrollieren oder Sichern des Zugriffs auf Hardwaregeräte, wie das KCS-Gerät, finden Sie in der Dokumentation für das Hostbetriebssystem.

Interconnect-Zugriff auf bevorzugten authentifizierten Host

Eine schnellere Alternative zur KCS-Schnittstelle ist die interne High-Speed Interconnect-Verbindung, über die Clients auf dem Hostbetriebssystem mit Oracle ILOM kommunizieren können. Das Interconnect wird durch eine interne Ethernet-USB-Verbindung implementiert und es wird ein IP-Stack ausgeführt. Oracle ILOM erhält eine interne, nicht routingfähige IP-Adresse, mit der ein Client auf dem Host eine Verbindung zu Oracle ILOM herstellen kann.

Anders als bei der KCS-Schnittstelle, für die ein geschützter Zugriff auf ein Hardwaregerät erforderlich ist, können standardmäßig alle Betriebssystembenutzer das LAN-Interconnect verwenden. Daher ist für die Verbindung mit Oracle ILOM über das LAN-Interconnect genau wie für eine Netzwerkverbindung mit dem Oracle ILOM-Verwaltungsanschluss eine Authentifizierung erforderlich.

Außerdem stehen dem Host über das LAN-Interconnect alle im Verwaltungsnetzwerk bekannten Services und Protokolle zur Verfügung. Sie können die Oracle ILOM-Webbenutzeroberfläche aufrufen, indem Sie einen Webbrowser auf dem Host verwenden, oder mithilfe eines Secure Shell-Clients eine Verbindung mit der Oracle ILOM-Befehlszeilenschnittstelle aufbauen. In allen Fällen ist ein gültiger Benutzername und ein gültiges Passwort für das LAN-Interconnect erforderlich.

Das LAN-Interconnect ist standardmäßig deaktiviert. Bei Deaktivierung wird dem Hostbetriebssystem kein Ethernet-Gerät und kein vorhandener Kanal angezeigt. Oracle Hardware Management Pack unterstützt Sie bei der Bereitstellung und Konfiguration des LAN-Interconnect.

Informationen zur Verwaltung von Oracle ILOM über eine sichere, dedizierte Host-Interconnect-Verbindung finden Sie in einem der folgenden Themen:

- Bei Firmware-Versionen ab 3.2: Dedicated Interconnect SP Management Connection im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2x)*
- Bei Firmware-Versionen 3.1.x: Dedicated Interconnect SP Management Connection im *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Bei Firmware-Versionen 3.0.12 bis 3.0.16: Configuring Local Host Interconnect im *Oracle ILOM 3.0 Web Procedures Guide*.

Verwenden von IPMI 2.0-Verschlüsselung zum Sichern des Kanals

Die IPMI-Version 2.0 (Intelligent Platform Management Interface) unterstützt das verschlüsselte Netzwerkprotokoll RMCP+ (Remote Management and Control Protocol+). Dieses Protokoll verschlüsselt den Kanal mithilfe eines symmetrischen, schlüsselbasierten Anfrage/Antwort-Mechanismus. Durch diesen Mechanismus wird sichergestellt, dass keine sensiblen Daten unverschlüsselt über das Netzwerk gesendet werden und für die Ver- und Entschlüsselung des Datenverkehrs ein Benutzerpasswort erforderlich ist. Um sicherzustellen, dass der gesamte IPMI 2.0-Verkehr verschlüsselt ist, implementiert Oracle ILOM keine Unterstützung für den Betriebsmodus IPMI 2.0 Cipher Type 0 (unverschlüsselt).

Geben Sie bei IPMItool mithilfe des Kennzeichens `-I lanplus` an, dass eine verschlüsselte RMCP+-Sitzung gestartet werden muss.

Weitere Informationen finden Sie in der Dokumentation zu `ipmitool`.

Anmerkung - Ab Firmware-Version 3.2.4 bietet Oracle ILOM eine konfigurierbare Eigenschaft für IPMI 1.5. Standardmäßig ist die IPMI 1.5-Eigenschaft deaktiviert. Einzelheiten dazu finden Sie unter Verwenden von IPMI v2.0 für erweiterte Authentifizierung und Paketverschlüsselung [52].

Verwenden sicherer Protokolle für Remoteverwaltung

Oracle ILOM unterstützt eine Reihe von verschiedenen Remote-Verwaltungsprotokollen. In manchen Fällen werden sowohl verschlüsselte als auch unverschlüsselte Versionen desselben Protokolls unterstützt. Verwenden Sie wenn möglich aus Sicherheitsgründen immer das sicherste verfügbare Protokoll. Die folgende Tabelle enthält eine Liste der unterstützten verschlüsselten und unverschlüsselten Protokolle.

TABELLE 9 Unterstützte sichere Protokolle

Kategorie	Sicher/Verschlüsselt	Unverschlüsselt
Webbrowserzugriff	HTTPS	HTTP
Zugriff über die Befehlszeilenschnittstelle	SSH	Nicht unterstützt
IPMI-Zugriff	IPMI v2.0	IPMI v1.5
Protokollzugriff	SNMPv3	SNMPv1/v2c

Aufbauen einer sicheren, vertrauenswürdigen Netzwerk-Verwaltungsverbindung

Alle Oracle-Server, auf denen Oracle ILOM ausgeführt wird, verfügen über einen dezidierten Verwaltungsport, der für die Netzwerkverbindung mit Oracle ILOM verwendet wird. Der dezidierte Verwaltungsport bietet ein privates, sicheres Netzwerk für die Verwaltung. Einige Systeme unterstützen auch Seitenbandverwaltung, bei der Host und Oracle ILOM über die Standardserverdatenports zugänglich sind. Mit der Seitenbandverwaltung werden Kabelführung und Netzwerkkonfiguration einfacher, da der Bedarf an zwei separaten Netzwerkverbindungen entfällt. Das bedeutet aber auch, dass der Oracle ILOM-Datenverkehr theoretisch über ein nicht vertrauenswürdiges Netzwerk gesendet werden könnte, wenn der dedizierte oder Seitenband-Verwaltungsport nicht mit einem vertrauenswürdigen Netzwerk verbunden ist.

Um eine möglichst zuverlässige und sichere Umgebung für Oracle ILOM beizubehalten, muss der dedizierte Netzwerkverwaltungsport oder Seitenband-Verwaltungsport am Server immer mit einem internen, vertrauenswürdigen Netzwerk oder einem dedizierten, sicheren Verwaltungs-/privaten Netzwerk verbunden sein.

Aufbauen einer sicheren, lokalen seriellen Verwaltungsverbindung

Sie können einen Terminalserver oder einen Dumpterminal über den physischen seriellen Verwaltungsport am Server lokal mit Oracle ILOM verbinden. Um eine sichere lokale

Verwaltungsverbindung mit Oracle ILOM aufrecht zu erhalten, verbinden Sie Terminalgeräte nicht mit dem lokalen seriellen Verwaltungsport, wenn das Gerät auch mit einem internen oder privaten Netzwerk verbunden ist.

Sicheres Verwenden von Remote KVMS

Oracle ILOM bietet die Möglichkeit der Remote-Umleitung von Tastatur, Video und Maus des Hostservers zu einem Remote-Client und des Einhängens von Remote-Speicherplatz. Diese Funktionen werden alle als "Remote KVMS" bezeichnet. Remote-KVMS ermöglicht Ihnen die Anzeige der grafischen Konsole des Hostbetriebssystems auf dem Server, indem Sie die Java-Anwendungen Oracle ILOM Remote Console, Remote Console Plus und CLI Storage Redirection auf einem Clientrechner ausführen.

In den folgenden Themen enthalten Sie Informationen zum Sicherstellen, dass Remote KVMS und serielle textbasierte Sitzungen sicher von Oracle ILOM aus gestartet werden:

- „KVMS-Remotekommunikation und -Verschlüsselung“ [61]
- „Schutz vor gemeinsamem Remote- KVMS-Zugriff“ [62]
- „Schutz vor gemeinsamem Zugriff auf serielle Hostkonsole“ [63]

KVMS-Remotekommunikation und -Verschlüsselung

Die Anwendungen Oracle ILOM Remote System Console, Remote System Console Plus und CLI Storage Redirection verwenden eine Reihe von Netzwerkprotokollen für die Remotekommunikation mit Oracle ILOM. Mit diesen Java-Anwendungen können Sie Hosttastatur und -maus steuern sowie ein lokales Speichergerät (CD- oder DVD-Laufwerk) auf dem Remoteserver einhängen.

In der folgenden Tabelle wird die Netzwerkübertragung von Remote-KVMS-Daten genauer beschrieben.

TABELLE 10 KVMS-Funktionen und -Verschlüsselung

KVMS-Funktion	Verschlüsselt oder unverschlüsselt	Beschreibung
Mausumleitung	Verschlüsselt	Ihre Mauskoordinaten werden sicher über das Netzwerk an Oracle ILOM übertragen.
Tastaturumleitung	Verschlüsselt	Eingaben am Clientrechner werden an Oracle ILOM mithilfe eines verschlüsselten Protokolls übertragen.
Videoumleitung	Verschlüsselt	Videodaten werden mithilfe eines verschlüsselten Protokolls zwischen Java-Client und Oracle ILOM übertragen.

KVMS-Funktion	Verschlüsselt oder unverschlüsselt	Beschreibung
Speicherplatzumleitung	Unverschlüsselt	Auf ein Speichergerät geschriebene und von dort lesbare Daten werden ohne Verschlüsselung über das Netzwerk an Oracle ILOM übertragen.

Eine Liste der Netzwerkports, die von Remote-KVMS aktiviert sind, finden Sie unter Tabelle 4, „Standardmäßig aktivierte Services und Ports“.

Schutz vor gemeinsamem Remote- KVMS-Zugriff

Durch eine Remote KVMS-Videokonsole wird das umgeleitet, was Sie auf einem physischen, mit diesem Server verbundenen Bildschirm sehen würden. Da in der Regel nur ein Videoausgang pro Server vorhanden ist, übertragen alle Sitzungen trotz unterschiedlicher mit Oracle ILOM verbundener Remote-Clients dasselbe Videobild.

So können andere KVMS-Benutzer, die mit demselben Rechner verbunden sind, Ihre Bildschirmeingaben während einer Remote KVMS-Sitzung sehen. In diesem Zusammenhang ist es wichtig zu wissen, dass wenn sich ein Benutzer beim Hostbetriebssystem innerhalb der Anwendungen Oracle ILOM Remote Console, Remote Console Plus und CLI Storage Redirection als berechtigter Benutzer anmeldet, alle anderen KVMS-Benutzer an dieser authentifizierten Sitzung teilnehmen können. Vergessen Sie also nicht, dass die Remote-KVMS-Funktion gemeinsam genutzte Verbindungen zulässt.

Zum Schutz von authentifizierten Betriebssystemsitzungen, die nach Beenden einer Remote KVMS-Umleitungssitzung inaktiv bleiben, sollten Sie:

- Oracle ILOM so konfigurieren, dass das Hostbetriebssystem nach Beenden einer Remote KVMS-Umleitungssitzung automatisch gesperrt wird.

  Anweisungen dazu finden Sie unter Sperren des Hostzugriffs nach Beenden einer KVMS-Sitzung [34].
- ein Timeoutintervall im Hostbetriebssystem festlegen, um unbeaufsichtigte authentifizierte Benutzersitzungen automatisch zu schließen.

  Anweisungen dazu finden Sie in der Benutzerdokumentation für Ihr Hostbetriebssystem.

Wenn Sie Oracle ILOM Remote System Console Plus verwenden und die Anzahl der anzeigbaren KVMS-Sitzungen einschränken möchten, die von Oracle ILOM gestartet werden, lesen Sie Einschränken anzeigbarer KVMS-Sitzungen für Remote System Console Plus (3.2.4 oder höher) [35].

Schutz vor gemeinsamem Zugriff auf serielle Hostkonsole

Die Hostkonsole ist bei den meisten Betriebssystemen auch als textbasierte, serielle Konsole verfügbar. Rufen Sie diese Konsole auf, indem Sie den Befehl `start /HOST/console` in der Befehlszeile der Oracle ILOM-CLI ausführen. Ähnlich wie bei der grafischen Konsole steht allen Oracle ILOM-Benutzern nur eine einzelne serielle Konsole zur Verfügung. Aus diesem Grund ist sie eine Ressource, die gemeinsam genutzt werden kann. Wenn sich ein Benutzer von der seriellen Konsole aus beim Hostbetriebssystem anmeldet und die Konsole beendet, ohne sich vorher abzumelden, kann ein anderer Benutzer der seriellen Konsole die zuvor authentifizierte Betriebssystemsitzung verwenden.

Oracle ILOM sendet ein DTR-Signal (Data Transfer Request) an das Hostbetriebssystem, wenn eine Konsolenumleitungssitzung beendet wird. Bei zahlreichen Betriebssystemen wird ein Benutzer bei Empfang dieses Signals automatisch abgemeldet. Nicht alle Betriebssysteme unterstützen diese Funktion allerdings:

- Bei Oracle Linux 5 ist das DTR-Signal standardmäßig aktiviert.
- Oracle Linux 6 bietet Unterstützung für DTR, die aber manuell aktiviert werden muss.
- Oracle Solaris unterstützt das DTR-Signal nicht. Benutzer können zur Verringerung von Sicherheitsrisiken im Hostbetriebssystem eine Zeitüberschreitung für die Sitzung konfigurieren.

Im Folgenden finden Sie Richtlinien zum Schutz von authentifizierten Betriebssystemsitzungen, die nach Beenden einer seriellen Hostumleitungssitzung inaktiv bleiben:

- Bestimmen Sie, ob das DTR-Signal im Hostbetriebssystem unterstützt wird. Wenn ja, stellen Sie sicher, dass diese Funktion standardmäßig aktiviert ist.

  Informationen zum DTR-Signal finden Sie in der Benutzerdokumentation für Ihr Hostbetriebssystem.
- Konfigurieren Sie ein Sitzungstimeoutintervall im Hostbetriebssystem.

  Informationen zum Festlegen eines Sitzungstimeoutintervalls im Hostbetriebssystem finden Sie in der Benutzerdokumentation für Ihr Hostbetriebssystem.
- Implementieren Sie eine Sicherheitsrichtlinie, um sicherzustellen, dass Benutzer eine serielle Remote-Hostkonsole niemals unbeaufsichtigt lassen. Benutzer müssen sich immer bei allen Remote-Hostkonsolensitzungen abmelden, wenn keine Sitzungen verwendet werden.

Überlegungen nach dem Deployment zum Sichern des Benutzerzugriffs

In den folgenden Themen erhalten Sie Informationen zum Aufrechterhalten eines sicheren Benutzerzugriffs:

Durchsetzen der Passwortverwaltung

Ändern Sie sämtliche Oracle ILOM-Passwörter regelmäßig. Dadurch unterbinden Sie böswillige Aktivitäten und stellen sicher, dass Passwörter den aktuellen Passwortrichtlinien entsprechen.

Normalerweise ändern die Benutzer ihre eigenen Passwörter. Systemadministratoren mit Benutzerverwaltungsberechtigungen können allerdings auch Passwörter für andere Benutzerkonten ändern.

Im Folgenden finden Sie webbasierte Anweisungen zum Ändern des Passworts für ein Oracle ILOM-Benutzerkonto.

Anmerkung - Die CLI-Anweisungen bzw. andere Details zu Benutzerverwaltungs-Konfigurationseigenschaften finden Sie in der entsprechenden Dokumentation im Abschnitt "Zusätzliche Informationen" im folgenden Verfahren.

▼ Ändern des Passworts eines lokalen Benutzerkontos

Bevor Sie beginnen

- Lesen Sie den Abschnitt „Sicherheitsrichtlinien zum Verwalten von Benutzerkonten und Passwörtern“ [27].
- Die Rolle Benutzerverwaltung (u) ist erforderlich, um Passwörter oder Berechtigungen von anderen Benutzerkonten zu ändern.
- Mit der Rolle Operator (o) können Benutzer das Passwort für ihr eigenes Konto ändern.

1. **Navigieren Sie zur Seite "User Account" in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "User Management" -> "User Accounts".**
   - **Klicken Sie in Version 3.1 und höher der Webbenutzeroberfläche auf "User Management" -> "User Accounts".**

2. **Klicken Sie auf der Seite "User Account" beim Konto, das Sie ändern möchten, auf "Edit".**
   Das Dialogfeld "Edit: User Name" wird angezeigt.

3. **Führen Sie im Dialogfeld "Edit: User Name" die folgenden Aktionen aus:**

   - **Geben Sie ein eindeutiges Passwort in das Textfeld "New Password" ein, und wiederholen Sie dieses Passwort dann im Textfeld "Confirm New Password".**
   - **Klicken Sie auf "Save", um die Änderung anzuwenden.**

Zusätzliche Informationen

- Einschränkungen der Passwortrichtlinie für alle lokalen Benutzer festlegen (3.2.5 und höher) [30]
- Configuring a Local User Account im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Konfigurieren eines lokalen Benutzerkontos, Oracle ILOM 3.1 - *Konfigurations- und Wartungshandbuch*
- Modify a User Account in *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Modify a User Account in *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Physische Sicherheitspräsenz zum Zurücksetzen des Standardpassworts des `root`-Kontos

Das `root`-Benutzerpasswort für Oracle ILOM kann bei Verlust wiederhergestellt werden. Setzen Sie das `root`-Passwort zurück, indem Sie mithilfe des seriellen Ports eine Verbindung mit Oracle ILOM herstellen. Anders als in den meisten Fällen, in denen für eine Verbindung zum seriellen Oracle ILOM-Port der physische Zugang zum System erforderlich ist, kann die serielle Konsole mit einem Terminalserver verbunden werden. Der Terminalserver bietet quasi den Netzwerkzugang zum physischen seriellen Port.

Bei den meisten Servern gibt es eine Funktion zur Überprüfung der physischen Anwesenheit, um zu verhindern, dass bei Verwendung eines Terminalservers das `root`-Passwort über das Netzwerk zurückgesetzt werden kann. Dazu muss auf dem Server eine Taste gedrückt werden, um zu bestätigen, dass ein physischer Zugang zum Server möglich ist. Vergewissern Sie sich, dass die Physical Presence-Funktion im Falle einer bestehenden Verbindung zwischen dem seriellen Oracle ILOM-Port und einem Terminalserver aktiviert ist, um ein Höchstmaß an Sicherheit zu gewährleisten.

Im Folgenden finden Sie webbasierte Anweisungen zum Anzeigen oder Ändern der Prüfungsfunktion zur physischen Präsenz.

Anmerkung - Die CLI-Anweisungen bzw. andere Details zu den `root`-Kontoeigenschaften finden Sie in der entsprechenden Dokumentation im Abschnitt "Zusätzliche Informationen" im folgenden Verfahren.

▼ Festlegen der Prüfung auf physische Präsenz

Bevor Sie beginnen

- Der Modus zur Prüfung der physischen Präsenz ist standardmäßig in Oracle ILOM aktiviert.
- Firmware-Version 3.1 oder höher ist erforderlich, um den Modus zur Prüfung der physischen Präsenz in Oracle ILOM zu verwenden.

1. **Klicken Sie in der Oracle ILOM-Webbenutzeroberfläche auf "ILOM Administration" -> "Identification".**
2. **Navigieren Sie auf der Seite "Identification" zur Eigenschaft "Physical Presence Check", und führen Sie dann eine der folgenden Aktionen aus:**

   - **Aktivieren Sie das Kontrollkästchen "Physical Presence". Nach der Aktivierung muss der Locator-Schalter am physischen System gedrückt werden, um das Oracle ILOM-Standardpasswort wiederherzustellen.**

     -oder-

   - **Deaktivieren Sie das Kontrollkästchen "Physical Presence". Nach der Deaktivierung kann das Standardpasswort für das Oracle ILOM-Administrator-root-Konto zurückgesetzt werden, ohne dass der Locator-Schalter am physischen System gedrückt werden muss.**

3. **Klicken Sie auf "Save", um die Änderung anzuwenden.**

Zusätzliche Informationen

- Device Identification Configuration Properties im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*.
- Device Identification Configuration Properties im *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Password Recovery for `root` Account im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*.
- Password Recovery for `root` Account im *Oracle ILOM 3.1 Configuration and Maintenance Guide*

Überwachen von Auditereignissen zum Auffinden nicht autorisierter Zugriffe

Im Oracle ILOM-Auditprotokoll werden alle Anmeldevorgänge und Änderungen an der Konfiguration erfasst. Jeder Auditprotokolleintrag zeichnet den Benutzer und den dem Ereignis zugeordneten Zeitstempel auf. Auditereignisse sind nützlich für die Verfolgung von Änderungen und die Ermittlung unautorisierter Änderungen und Zugriffe auf Oracle ILOM.

Im Folgenden finden Sie webbasierte Anweisungen zum Anzeigen von Ereignissen im Oracle ILOM-Auditlog.

Anmerkung - Die CLI-Anweisungen bzw. andere Details zum Auditlog finden Sie in der entsprechenden Dokumentation im Abschnitt "Zusätzliche Informationen" im folgenden Verfahren.

▼ Anzeigen des Auditlogs

Bevor Sie beginnen

- Das Auditlog ab Firmware-Version 3.1 in Oracle ILOM verfügbar. Vor der Firmware-Version 3.1 wurden Auditereignisse im Oracle ILOM-Ereignislog erfasst.
- Die Berechtigungen der Rolle Admin (a) sind in Oracle ILOM erforderlich, um Einträge im Auditlog zu löschen.

1. **Klicken Sie in der Webbenutzeroberfläche auf "ILOM Administration" -> "Logs" -> "Audit".**

2. **Verwenden Sie die Steuerelemente auf der Auditlogseite, um die Logeinträge zu filtern oder Ereignisse im Log zu löschen.**

   Benutzer mit Firmware-Version 3.2 oder höher erhalten weitere Informationen durch Klicken auf den Link `More details` auf der Auditseite.

Zusätzliche Informationen

- Verwalten von Oracle ILOM-Logeinträgen, *Oracle ILOM - Benutzerhandbuch für Systemüberwachung und Diagnose (Firmware 3.2.x)*
- Verwalten von Oracle ILOM-Logeinträgen, *Oracle ILOM 3.1 - Benutzerhandbuch*

Aktionen nach dem Deployment zum Ändern des FIPS-Modus

Ab Firmwarerelease 3.2.4 bietet Oracle ILOM eine konfigurierbare Eigenschaft für die FIPS Level 1-Konformität. Standardmäßig ist diese Eigenschaft deaktiviert. Nach der Änderung des Betriebsstatus der FIPS-Konformität in Oracle ILOM werden alle benutzerdefinierten Konfigurationseigenschaften auf ihre werkseitigen Standardwerte zurückgesetzt. Um zu verhindern, dass benutzerdefinierte Konfigurationseinstellungen in Oracle ILOM verloren gehen, sollte die FIPS-Konformität geändert werden, bevor andere Oracle ILOM-Einstellungen konfiguriert werden. Im Folgenden finden Sie Anweisungen, mit denen verhindert werden kann, dass benutzerdefinierte Einstellungen verloren gehen, wenn Sie die FIPS-Konformität nach dem Deployment der Oracle ILOM-Konfiguration ändern müssen.

Anmerkung - Oracle verwendet kryptografische Algorithmen gemäß den FIPS 140-2-Sicherheitsstandards zum Sichern von sensiblen oder wertvollen Systemdaten.

▼ Ändern des FIPS-Modus nach dem Deployment

Gehen Sie wie folgt vor, wenn Sie den Betriebszustand des FIPS-Modus nach einem Firmwareupdate oder der Angabe von benutzerdefinierten Konfigurationseigenschaften in Oracle ILOM ändern müssen.

Anmerkung - Der FIPS-Konformitätsmodus in Oracle ILOM wird durch die Eigenschaften "State" und "Status" angegeben. Die Zustandseigenschaft steht für den konfigurierten Modus in Oracle ILOM und die Statuseigenschaft für den Betriebsmodus in Oracle ILOM. Wenn die Eigenschaft "FIPS State" geändert wird, wirkt sich diese Änderung bis zum nächsten Neustart von Oracle ILOM nicht auf den Betriebsmodus (Eigenschaft "FIPS Status") aus.

Bevor Sie beginnen

- Die konfigurierbare Eigenschaft für die FIPS Level 1-Konformität ist ab Firmwarerelease 3.2.4 in Oracle ILOM verfügbar. In älteren Firmwarereleases als 3.2.4 gibt es in Oracle ILOM keine konfigurierbare Eigenschaft für die FIPS Level 1-Konformität.
- Wenn FIPS aktiviert ist (konfiguriert und betriebsfähig), werden einige Funktionen in Oracle ILOM nicht unterstützt. Eine Liste der nicht unterstützten Funktionen bei aktiviertem FIPS finden Sie unter „Nicht unterstützte Funktionen bei aktiviertem FIPS-Modus“ [19].
- Die Rolle Admin (a) ist erforderlich, um dieses Verfahren auszuführen.

1. **Erstellen Sie ein Backup der Oracle ILOM-Konfiguration in der Oracle ILOM-Webbenutzeroberfläche.**

   Beispiele:

a. **Klicken Sie auf "ILOM Administration" -> "Configuration Management" -> "Backup/Restore".**

b. **Klicken Sie auf der Seite "Backup/Restore" auf den Link "More details...", um weitere Anweisungen zu erhalten.**

Anmerkung - Um die erneute Verbindung zu Oracle ILOM nach dem Firmware-Update zu erleichtern, aktivieren Sie die Firmware-Updateoptionen zum Beibehalten der Konfiguration.

Anmerkung - Wenn Sie Schritt 2 vor Schritt 1 ausführen, müssen Sie die gesicherte XML-Konfigurationsdatei bearbeiten und die FIPS-Einstellung entfernen. Andernfalls kommt es zu einer inkonsistenten Konfiguration zwischen der gesicherten Oracle ILOM-XML-Datei und dem Zustand des FIPS-Betriebsmodus auf dem Server. Dies ist nicht zulässig.

---

2. **Führen Sie die folgenden Schritte aus, wenn ein Firmware-Update erforderlich ist:**

   a. **Klicken Sie auf "ILOM Administration" -> "Maintenance" -> "Firmware Update".**

   b. **Klicken Sie auf der Seite "Firmware Update" auf den Link "More details...", um weitere Anweisungen zu erhalten.**

3. **Ändern Sie den FIPS-Konformitätsmodus in Oracle ILOM wie folgt:**

   a. **Klicken Sie auf "ILOM Administration" -> "Management Access" -> "FIPS".**

   b. **Klicken Sie auf der Seite "FIPS" auf den Link `More details`, um Anweisungen dazu zu erhalten, wie Sie:**

      - **die Konfiguration des FIPS-Zustands ändern**
      - **den FIPS-Betriebsstatus auf einem System durch Zurücksetzen des SP aktualisieren**

4. **Stellen Sie die gesicherte Oracle ILOM-Konfiguration wie folgt wieder her:**

   a. **Klicken Sie auf "ILOM Administration" -> "Configuration Management" -> "Backup/Restore".**

   b. **Klicken Sie auf der Seite "Backup/Restore" auf den Link `More details`, um weitere Anweisungen zu erhalten.**

Zusätzliche Informationen

- „Festlegen, ob der FIPS-Modus beim Deployment konfiguriert werden soll“ [16]
- „Nicht unterstützte Funktionen bei aktiviertem FIPS-Modus“ [19]
- Configure FIPS Mode Properties im *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*

Durchführen von Updates auf die aktuellste Software und Firmware

Bringen Sie die Software- und Firmware-Versionen Ihrer Server immer auf den neuesten Stand.

- Suchen Sie regelmäßig auf My Oracle Support nach Updates.
- Nutzen Sie Bugfixes und Verbesserungen, indem Sie stets die aktuellste verfügbare Version der Software oder Firmware für Ihren Server installieren.
- Installieren Sie alle erforderlichen Sicherheitspatches für die gesamte installierte Software.

Im Folgenden finden Sie Anweisungen zum Aktualisieren der Oracle ILOM-Firmware auf Ihrem Server.

▼ Update der Oracle ILOM-Firmware

Bevor Sie beginnen

- Die Rolle Admin (a) ist in Oracle ILOM erforderlich, um die Oracle ILOM-Firmware zu aktualisieren.
- Benachrichtigen Sie alle Oracle ILOM-Benutzer über das geplante Firmware-Update, und bitten Sie sie, alle Clientsitzungen zu schließen, bis das Firmware-Update abgeschlossen ist.
- Der Firmware-Updateprozess nimmt mehrere Minuten in Anspruch. Während dieser Zeit dürfen keine anderen Oracle ILOM-Aufgaben ausgeführt werden.

1. **Laden Sie das aktuellste verfügbare Softwareupdate für Ihren Server von der My Oracle Support-(MOS-)Website herunter.**
   Bei Bedarf finden Sie in der Dokumentation zu Ihrem Server Anweisungen zum Abrufen von Softwareupdates von MOS.

   Anmerkung - Die aktuellste verfügbare Oracle ILOM-Firmware-Version für Ihren Server ist im letzten Softwarepatch enthalten, der auf MOS für Ihren Server veröffentlicht wurde.

2. **Speichern Sie das Firmware-Image in einem lokalen Laufwerk oder einer Netzwerkfreigabe.**

3. **Navigieren Sie in der Webbenutzeroberfläche zur Seite "Firmware Update".**

   Beispiele:

   - **Klicken Sie in der 3.0.x-Webbenutzeroberfläche auf "Maintenance" -> "Firmware".**
   - **Klicken Sie in Version 3.1 oder höher der Webbenutzeroberfläche auf "ILOM Administration" -> "Maintenance" -> "Firmware Upgrade".**

4. **Klicken Sie auf der Seite "Firmware Upgrade" auf "Enter Firmware Upgrade mode", und befolgen Sie dann die Anweisungen.**

   Benutzer mit Oracle ILOM-Firmware 3.2 oder höher klicken auf den Link `More details` auf der Seite "Firmware Upgrade".