

Sun Server X3-2 (früher Sun Fire X4170 M3)

Sicherheitshandbuch

Copyright © 2013 Oracle Corporation

Cette logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

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

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

U.S. GOVERNMENT END USERS:

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

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

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

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

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

Copyright © 2013, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

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

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

Inhaltsverzeichnis

| | |
|--|----|
| 1. Sicherheitshandbuch zu Sun Server X3-2 | 7 |
| Systemübersicht | 7 |
| Sicherheitsgrundsätze | 8 |
| Verwenden von Tools zur Konfiguration und Verwaltung von Servern | 9 |
| Oracle System Assistant | 9 |
| Oracle ILOM | 10 |
| Oracle Hardware Management Pack | 11 |
| Einrichten einer sicheren Umgebung | 11 |
| Oracle-Richtlinien für Betriebssysteme | 11 |
| Netzwerkports und -Switches | 12 |
| VLAN | 12 |
| InfiniBand | 13 |
| Physische Hardwaresicherheit | 13 |
| Softwaresicherheit | 13 |
| Verwalten einer sicheren Umgebung | 14 |
| Energiesteuerung der Hardware | 14 |
| Ressourcenüberwachung | 14 |
| Software- und Firmware-Aktualisierungen | 15 |
| Netzwerkzugriff | 15 |
| Datenschutz und Sicherheit | 16 |
| Protokollverwaltung | 16 |

• • • K a p i t e l 1

Sicherheitshandbuch zu Sun Server X3-2

In dem vorliegenden Dokument finden Sie allgemeine Sicherheitsanweisungen für Oracle Sun Server X3-2 einschließlich Netzwerkschnittstellen und angeschlossene Netzwerk-Switches.



Anmerkung

Sun Server X3-2 wurde früher als Sun Fire X4170 M3 bezeichnet. In der Software ist diese Bezeichnung möglicherweise noch enthalten. Die Änderung des Produktnamens hat keine Auswirkungen auf Systemmerkmale und -funktionen.

Dieses Kapitel enthält die folgenden Abschnitte:

- „Systemübersicht“ [7]
- „Sicherheitsgrundsätze“ [8]
- „Verwenden von Tools zur Konfiguration und Verwaltung von Servern“ [9]
- „Einrichten einer sicheren Umgebung“ [11]
- „Verwalten einer sicheren Umgebung“ [14]

Systemübersicht

Bei Sun Server X3-2 handelt es sich um einen für Unternehmen entwickelten 1HE-Server (one-rack unit). Unterstützt werden die folgenden Komponenten.

- Bis zu zwei Intel- Prozessoren mit folgenden Merkmalen:
 - 2,4 GHz, 4 Kerne, 80 W
 - 2,5 GHz, 6 Kerne, 95 W
 - 2,2 GHz, 8 Kerne, 95 W
 - 2,9 GHz, 8 Kerne, 135 W
- Bis zu 8 DIMMs pro Prozessor für maximal 16 DDR3-DIMMs und eine Speicherkapazität von max. 512 GB auf Dualprozessorsystemen. Die DIMM-Größen 8, 16 und 32 GB werden unterstützt.



Anmerkung

Auf Einzelprozessorsystemen werden bis zu 8 DIMMs für max. 256 GB unterstützt.

- 4 PCIe Gen3-Steckplätze auf Dualprozessorsystemen, 3 externe Steckplätze, 1 interner Steckplatz. Der PCIe-Steckplatz 1 ist ein externer Steckplatz ohne Funktion auf Einzelprozessorsystemen.
- Speicherlaufwerke können sowohl für Festplatten (HDDs) als auch Festkörper-Speichergeräte (SSDs) konfiguriert sein. Folgende Speicherlaufwerkkonfigurationen werden unterstützt:
 - Max. 4 hotplugfähige SAS-HDDs (3,5 Zoll)
 - Max. 4 hotplugfähige SAS/SATA-HDDs/-SSDs (2,5 Zoll) und DVD
 - Max. 8 hotplugfähige SAS/SATA-HDDs/-SSDs (2,5 Zoll)
- 2 redundante Hot-Plug-Netzteile
- 1 integrierter Oracle ILOM-SP (Oracle Integrated Lights Out Manager-Serviceprozessor) auf Basis des AST2300-Chips, der sichere lokale und Remote-Verwaltung bietet.
- Oracle System Assistant, ein auf einem vorinstallierten USB-Flashlaufwerk integriertes Serversetuptools.

Sicherheitsgrundsätze

Zu den Sicherheitsgrundsätzen zählen Zugang, Authentifizierung, Autorisierung und Überwachung.

• **Zugang**

Dieser Grundsatz bezieht sich auf den physischen Zugang zu Hardware bzw. den physischen oder virtuellen Zugang zu Software.

- Schützen Sie Ihre Hardware und Ihre Daten durch physische und virtuelle Steuerungsmechanismen vor unerlaubten Zugriffen.
- Informationen zum Aktivieren der Sicherheitsfunktionen Ihrer Software finden Sie in der produktbegleitenden Dokumentation.
- Installieren Sie Server und zugehörige Komponenten in einem Raum, der abgeschlossen werden kann und zu dem nicht jeder Zutritt hat.
- Wenn sich Geräte in einem Rack mit Türverriegelung befinden, halten Sie die Tür geschlossen, wenn Sie keine Wartungsarbeiten an Komponenten im Rack vornehmen müssen.
- Schränken Sie den Zugang zu Steckern oder Ports ein, die einen leistungsstärkeren Zugang als SSH-Verbindungen bieten. Geräte wie System-Controller, Steckdosenleisten (Power Distribution Units, PDUs) und Netzwerk-Switches weisen Steckerplätze und Ports auf.
- Schränken Sie den Zugang zu Hot-Swapping- oder Hot-Plugging-Geräten ein, da diese leicht entfernt werden können.
- Lagern Sie nicht verwendete FRUs (Field Replaceable Units) und CRUs (Customer Replaceable Units) in einem abschließbaren Schrank. Nur autorisiertes Personal sollte Zugang zu diesem Schrank haben.

• **Authentifizierung**

Dieser Grundsatz bezieht sich auf den Vorgang, bei dem festgestellt wird, ob es sich bei einem Benutzer von Hardware oder Software wirklich um diesen Benutzer handelt.

- Richten Sie Funktionen zur Authentifizierung wie ein Passwortsystem in den Betriebssystemen Ihrer Plattform ein, sodass festgestellt werden kann, ob es sich bei einem Benutzer wirklich um diesen Benutzer handelt.
- Stellen Sie sicher, dass Ihr Personal beim Betreten des Computerraums Mitarbeiterausweise trägt.
- Setzen Sie bei Benutzerkonten Zugriffskontrolllisten sinnvoll ein, und legen Sie Zeitüberschreitungen für Sitzungen sowie Berechtigungsstufen für Benutzer fest.

- **Autorisierung**

Dieser Grundsatz bezieht sich auf Beschränkungen bei der Verwendung von Hardware und Software durch Mitarbeiter.

- Ermöglichen Sie Mitarbeitern, nur mit der Hardware und Software zu arbeiten, die sie beherrschen.
- Legen Sie Berechtigungen für das Lesen, Schreiben und Ausführen fest, um den Zugriff von Benutzern auf Befehle, Festplattenspeicher, Geräte und Anwendungen zu steuern.

- **Überwachung**

Dieser Grundsatz bezieht sich auf die Hardware- und Softwarefunktionen zur Überwachung von Anmeldevorgängen und Wartung der Hardware.

- Überwachen Sie die Anmeldung von Benutzern anhand von Systemprotokollen. Kontrollieren Sie insbesondere Systemadministrator- und Servicekonten, da vor allem diese Konten Zugriff auf mächtige Befehle gewähren.
- Bewahren Sie alle Hardwareseriennummern auf. Verwenden Sie zur Überwachung von Systemressourcen die Komponentenseriennummer. Oracle-Teilenummern sind auf Karten, Modulen und Hauptplatinen elektronisch gespeichert.
- Versehen Sie für die Komponentenerkennung und -überwachung alle wichtigen Hardwarekomponenten wie FRUs mit einer Sicherheitskennung. Verwenden Sie spezielle UV-Stifte oder geprägte Beschriftungen.

Verwenden von Tools zur Konfiguration und Verwaltung von Servern

Orientieren Sie sich an folgenden Sicherheitsrichtlinien bei der Anwendung von Software- und Firmwaretools zur Konfiguration und Verwaltung Ihres Servers.

- „Oracle System Assistant“ [9]
- „Oracle ILOM“ [10]
- „Oracle Hardware Management Pack“ [11]

Oracle System Assistant

Oracle System Assistant ist ein vorinstalliertes Tool, mit dem Sie Serverhardware vor Ort oder per Remote-Zugriff konfigurieren und aktualisieren sowie unterstützte Betriebssysteme installieren können. Informationen zur Verwendung von Oracle System Assistant erhalten Sie im *Sun Server X3-2 Administration Guide* unter:

<http://www.oracle.com/pls/topic/lookup?ctx=SunServerX3-2>

Im Folgenden werden die mit Oracle System Assistant verbundenen Sicherheitsprobleme erläutert.

- **Oracle System Assistant umfasst eine bootfähige Root-Umgebung**

Die Oracle System Assistant-Anwendung wird auf einem vorinstallierten, internen USB-Flashlaufwerk ausgeführt. Sie setzt auf einer bootfähigen Linux-Root-Umgebung auf. Oracle System Assistant bietet außerdem die Möglichkeit, auf die zugrunde liegende Root-Shell zuzugreifen. Benutzer, die physischen Zugriff auf das System oder KVM-Remote-Zugriff (Keyboard, Video, Mouse, Storage) auf das System über Oracle ILOM haben, können Oracle System Assistant und die Root-Shell aufrufen.

Mithilfe einer Root-Umgebung können Sie Systemkonfiguration und -richtlinien ändern sowie auf Daten auf anderen Festplatten zugreifen. Eine Beschränkung des physischen Zugangs zum Server

sowie eine überlegte Zuweisung von Administratoren- und Konsolenberechtigungen für Oracle ILOM-Benutzer sind zu empfehlen.

- **Oracle System Assistant hängt ein für das Betriebssystem zugängliches USB-Speichergerät ein**

Oracle System Assistant ist nicht nur eine bootfähige Umgebung, sondern auch ein USB-Speichergerät (Flashlaufwerk). Das Hostbetriebssystem kann nach der Installation darauf zugreifen. Bei Wartungs- und Neukonfigurationsarbeiten erleichtert dies den Zugriff auf Tools und Treiber. Das USB-Speichergerät von Oracle System Assistant ist weder lese- noch schreibgeschützt und daher anfällig für Viren.

Es ist empfehlenswert, dass Sie für das Oracle System Assistant-Speichergerät dieselben Schutzmaßnahmen wie für Festplatten anwenden, einschließlich regelmäßiger Virenskans und Integritätsprüfungen.

- **Oracle System Assistant kann deaktiviert werden**

Oracle System Assistant unterstützt Sie beim Serversetup, beim Aktualisieren und Konfigurieren von Firmware sowie beim Installieren des Hostbetriebssystems. Wenn die obigen Auswirkungen auf die Sicherheit nicht akzeptabel oder Sie Oracle System Assistant nicht benötigen, können Sie das Tool deaktivieren. Durch die Deaktivierung von Oracle System Assistant kann das Hostbetriebssystem nicht mehr auf das USB-Speichergerät zugreifen. Außerdem kann Oracle System Assistant nicht gestartet werden.

Sie können Oracle System Assistant entweder im Tool selbst oder im BIOS deaktivieren. Wenn Oracle System Assistant deaktiviert ist, kann es nur durch das BIOS-Setupdienstprogramm erneut aktiviert werden. Ein passwortgeschütztes BIOS-Setup ist zu empfehlen, damit nur autorisierte Benutzer Oracle System Assistant erneut aktivieren können. Informationen zum Deaktivieren und erneuten Aktivieren von Oracle System Assistant finden Sie im *Sun Server X3-2 Administration Guide*.

Oracle ILOM

Sie können Systemkomponenten mit der Verwaltungsfirmware von Oracle ILOM (Oracle Integrated Lights Out Manager) selbst sichern, verwalten und überwachen. Sie ist auf dem Sun Server X3-2, anderen x86-basierten Oracle-Servern und auf einigen SPARC-basierten Oracle-Servern vorinstalliert.

Trennen Sie den Serviceprozessor (SP) vom Gesamtnetzwerk, indem Sie ihn in ein dediziertes internes Netzwerk integrieren. Oracle ILOM bietet Systemadministratoren Funktionen zur Serversteuerung und -überwachung. Je nach Autorisierungsebene der Administratoren können diese Funktionen unter anderem das Abschalten des Servers, Erstellen neuer Benutzerkonten und das Laden von Remote-Speichermedien umfassen. Um eine möglichst zuverlässige und sichere Umgebung für Oracle ILOM beizubehalten, muss der dedizierte Netzwerkverwaltungsanschluss oder Sideband-Verwaltungsanschluss am Server immer mit einem internen, vertrauenswürdigen Netzwerk oder einem dedizierten, sicheren Verwaltungs-/Privatnetzwerk verbunden sein.

Beschränken Sie die Verwendung des standardmäßigen Administratorkontos (**root**) auf die erste Oracle ILOM-Anmeldung. Dieses standardmäßige Administratorkonto wird nur zur Unterstützung bei der ersten Serverinstallation bereitgestellt. Deshalb müssen Sie das standardmäßige Administratorpasswort **changeme** während des Anfangssetups des Systems ändern, um einen bestmöglichen Schutz der Umgebung zu gewährleisten. Zusätzlich zur Änderung des Kennworts für das standardmäßige Administratorkonto sollte für jeden neuen Oracle ILOM-Benutzer ein neues Benutzerkonto mit eindeutigem Passwort und zugewiesenen Autorisierungsebenen eingerichtet werden.

In der Oracle ILOM-Dokumentation erhalten Sie Informationen zum Einrichten von Passwörtern, Verwalten von Benutzern und Anwenden von Sicherheitsfunktionen einschließlich SSH-, SSL-

und RADIUS-Authentifizierung (Secure Shell, Secure Socket, Remote Authentication Dial in User Service). Auf Oracle ILOM abgestimmte Sicherheitsrichtlinien finden Sie in der Oracle ILOM 3.1 Documentation Library im *Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide*. Die Dokumentation zu Oracle ILOM 3.1 finden Sie unter folgendem Link:

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

Oracle Hardware Management Pack

Oracle Hardware Management Pack ist für Ihren Server, zahlreiche andere x86-basierte Server sowie für einige SPARC-Server verfügbar. Oracle Hardware Management Pack besteht aus zwei Komponenten, d. h. aus einem SNMP-Überwachungsagenten sowie einer Familie von betriebssystemübergreifenden CLI-Tools (Command-Line Interface) für die Serververwaltung.

In Verbindung mit den SNMP-Plug-ins von Hardware Management Agent können Sie SNMP zur Überwachung von Oracle-Servern und -Servermodulen in Ihrem Rechenzentrum einsetzen, ohne dass Sie sich mit zwei Verwaltungspunkten (Host und Oracle ILOM) verbinden müssen. Durch diese Funktion kann eine einzelne IP-Adresse (IP-Adresse des Hosts) zur Überwachung von mehreren Servern und Servermodulen verwendet werden. Die SNMP-Plug-ins werden auf dem Hostbetriebssystem der Oracle-Server ausgeführt.

Zur Konfiguration von Oracle-Servern können Sie Oracle Server CLI Tools verwenden. Die CLI-Tools sind kompatibel mit Oracle Solaris, Oracle Linux, Oracle VM, weiteren Linux-Distributionen und Microsoft Windows-Betriebssystemen.

Weitere Informationen zu diesen Funktionen erhalten Sie in der Dokumentation zu Oracle Hardware Management Pack. Auf Oracle Hardware Management Pack abgestimmte Sicherheitsrichtlinien finden Sie in der Oracle Hardware Management Pack Documentation Library im *Oracle Hardware Management Pack (HMP) Security Guide*. Die Dokumentation zu Oracle Hardware Management Pack finden Sie unter folgendem Link:

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

Einrichten einer sicheren Umgebung

Installieren und konfigurieren Sie den Server und die zugehörigen Komponenten wie folgt:

- „Oracle-Richtlinien für Betriebssysteme“ [11]
- „Netzwerkports und -Switches“ [12]
- „VLAN“ [12]
- „InfiniBand“ [13]
- „Physische Hardwaresicherheit“ [13]
- „Softwaresicherheit“ [13]

Oracle-Richtlinien für Betriebssysteme

In der Oracle-Dokumentation zu Betriebssystemen (BS) erhalten Sie Informationen zu folgenden Themen:

- Anwenden von Sicherheitsfunktionen bei der Systemkonfiguration
- Sicheres Vorgehen beim Hinzufügen von Anwendungen und Benutzern zu einem System
- Schutz von netzwerkbasierenden Anwendungen

Die Sicherheitsbestimmungen für unterstützte Oracle-Betriebssysteme sind Teil der Documentation Library für das Betriebssystem. Sie finden die Sicherheitsbestimmungen für das jeweilige Oracle-Betriebssystem in der entsprechenden Documentation Library:

- **Oracle Solaris 10 1/13** - <http://www.oracle.com/goto/Solaris10/docs>
- **Oracle Solaris 11.1** - <http://www.oracle.com/goto/Solaris11/docs>
- **Oracle Linux** - <http://www.oracle.com/technetwork/documentation/ol-1861776.html>
- **Oracle VM** - <http://www.oracle.com/technetwork/documentation/vm-096300.html>

Informationen zu Betriebssystemen von anderen Anbietern, wie Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Windows und VMware ESXi, finden Sie in der entsprechenden Dokumentation.

Netzwerkports und -Switches

Je nach Switch unterscheiden sich die Stufen der Portsicherheitsfunktionen. In der Dokumentation zum Switch finden Sie Informationen zur Vorgehensweise bei folgenden Aufgaben:

- Verwenden Sie Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen für den lokalen und den Remote-Zugriff auf den Switch.
- Ändern Sie die Passwörter für Netzwerk-Switches, die standardmäßig mehrere Benutzerkonten und -passwörter umfassen können.
- Out-of-Band-Verwaltung von Switches (getrennt vom Datenverkehr). Wenn dies nicht möglich ist, weisen Sie eine separate VLAN-Nummer (Virtual Local Area Network) für die In-Band-Verwaltung zu.
- Verwenden Sie die Portspiegelungsfunktion des jeweiligen Netzwerk-Switch für den Zugriff auf das Angriffserkennungssystem.
- Pflegen Sie offline eine Switch-Konfigurationsdatei und beschränken Sie den Zugriff auf befugte Administratoren. Die Konfigurationsdatei sollte beschreibende Kommentare zu jeder Einstellung enthalten.
- Richten Sie einen Portschutz zur Beschränkung des Zugriffs anhand von MAC-Adressen ein. Deaktivieren Sie das automatische Trunking bei allen Ports.
- Verwenden Sie die folgenden Portsicherheitsfunktionen, sofern bei Ihrem Switch vorhanden:
 - Durch **MAC-Locking** wird eine MAC-Adresse (Media Access Control) eines oder mehrerer Geräte mit einem physischen Port auf einem Switch verbunden. Wenn Sie einen Switch-Port einer bestimmten MAC-Adresse zuweisen, können Superuser keine Backdoors in Ihr Netzwerk mit Rogue-Zugriffspunkten einbauen.
 - **MAC-Lockout** bewirkt, dass eine bestimmte MAC-Adresse keine Verbindung zu einem Switch mehr aufbauen kann.
 - Die Angaben zu den direkten Portverbindungen jedes Switch werden durch **MAC-Learning** beim Festlegen von Sicherheitseinstellungen durch den Netzwerk-Switch auf Basis aktueller Verbindungen verwendet.

VLAN

Beachten Sie beim Einrichten eines VLAN, dass dafür die Bandbreite in einem Netzwerk genutzt wird und zusätzliche Sicherheitsmaßnahmen erforderlich sind.

- Definieren Sie VLANs, damit sensible Systemcluster vom übrigen Netzwerk getrennt werden. Dadurch sinkt die Wahrscheinlichkeit, dass Benutzer auf diesen Clients und Servern Zugriff auf Daten erhalten.

- Weisen Sie Trunk-Ports eine eindeutige, systemeigene VLAN-Nummer zu.
- Beschränken Sie die Zahl der VLANs, die über einen Trunk transportiert werden können, auf das absolut notwendige Minimum.
- Deaktivieren Sie VTP (VLAN Trunking Protocol). Wenn dies nicht möglich ist, legen Sie für VTP die Verwaltungsdomäne, Passwort und Pruning fest. Versetzen Sie dann VTP in den Modus „transparent“.

InfiniBand

Schützen Sie InfiniBand-Hosts. Eine InfiniBand-Struktur ist nur so sicher wie der Infiniband-Host mit dem geringsten Schutz.

- Beachten Sie, dass eine Partitionierung keinen Schutz für die InfiniBand-Struktur bietet. Sie bewirkt lediglich eine Isolierung des InfiniBand-Datenverkehrs zwischen virtuellen Maschinen auf einem Host.
- Entscheiden Sie sich nach Möglichkeit für eine statische VLAN-Konfiguration.
- Deaktivieren Sie nicht verwendete Switch-Ports und weisen Sie ihnen eine nicht verwendete VLAN-Nummer zu.

Physische Hardwaresicherheit

Physische Hardware kann auf relativ einfache Weise gesichert werden: durch Zugangseinschränkungen und Aufbewahrung von Seriennummern.

- **Schränken Sie den Zugang ein**
 - Installieren Sie Server und zugehörige Komponenten in einem Raum, der abgeschlossen werden kann und zu dem nicht jeder Zutritt hat.
 - Wenn sich Geräte in einem Rack mit Türverriegelung befinden, halten Sie die Tür geschlossen, wenn Sie keine Wartungsarbeiten an Komponenten im Rack vornehmen müssen. Schließen Sie die Tür nach Wartung der Geräte ab.
 - Schränken Sie den Zugang zu USB-Verbindungen ein, die einen leistungsstärkeren Zugang als SSH-Verbindungen bieten. Geräte wie Systemcontroller, Steckdosenleisten (Power Distribution Units, PDUs) und Netzwerkswitches können USB-Anschlüsse aufweisen.
 - Schränken Sie den Zugang zu Hot-Swapping- oder Hot-Plugging-Geräten ein, da diese leicht entfernt werden können.
 - Lagern Sie nicht verwendete FRUs (Field Replaceable Units) oder CRUs (Customer Replaceable Units) in einem abschließbaren Schrank. Nur autorisiertes Personal sollte Zugang zu diesem Schrank haben.
- **Bewahren Sie Seriennummern auf**
 - Versehen Sie alle wichtigen Hardwarekomponenten wie FRUs mit einer Sicherheitskennung. Verwenden Sie spezielle UV-Stifte oder geprägte Beschriftungen.
 - Bewahren Sie alle Hardwareseriennummern auf.
 - Bewahren Sie Hardwareaktivierungsschlüssel und Lizenzen an einem sicheren Ort auf, der im Systemnotfall für den Systemverwalter einfach zugänglich ist. Die ausgedruckten Dokumente sind möglicherweise Ihr einziger Eigentumsnachweis.

Softwaresicherheit

Hardwaresicherheit wird meistens mithilfe von Softwaremaßnahmen umgesetzt.

- Ändern Sie alle Standardpasswörter, wenn Sie ein neues System installieren. Für die meisten Geräte werden allgemein bekannte Standardpasswörter wie **changeme** verwendet, bei denen die Gefahr besteht, dass Unbefugte Zugriff erhalten.
- Ändern Sie die Passwörter für Netzwerk-Switches, die standardmäßig mehrere Benutzerkonten und -passwörter umfassen können.
- Beschränken Sie die Verwendung des standardmäßigen Administratorkontos (**root**) auf einen einzigen Administratorbenutzer. Erstellen Sie für jeden neuen Benutzer ein neues Oracle ILOM-Konto. Stellen Sie sicher, dass jedem Oracle ILOM-Benutzerkonto ein eindeutiges Passwort und angemessene Autorisierungsberechtigungen (Operator, Administrator usw.) zugewiesen werden.
- Trennen Sie den Serviceprozessor vom Gesamtnetzwerk, indem Sie ihn in ein dediziertes Netzwerk integrieren.
- Schützen Sie den Zugang zu USB-Verbindungen. Geräte wie Systemcontroller, Steckdosenleisten (Power Distribution Units, PDUs) und Netzwerkswitches weisen USB-Anschlüsse auf, die einen leistungsstärkeren Zugang als SSH-Verbindungen bieten.
- Informationen zum Aktivieren der Sicherheitsfunktionen Ihrer Software finden Sie in der produktbegleitenden Dokumentation.
- Richten Sie einen Portschutz zur Beschränkung des Zugriffs anhand von MAC-Adressen ein. Deaktivieren Sie das automatische Trunking bei allen Ports.

Verwalten einer sicheren Umgebung

Steuern Sie nach abgeschlossener Erstinstallation und -konfiguration Hardware- und Überwachungssystemressourcen mithilfe von Oracle-Hardware- und Softwaresicherheitsfunktionen.

- „Energiesteuerung der Hardware“ [14]
- „Ressourcenüberwachung“ [14]
- „Software- und Firmware-Aktualisierungen“ [15]
- „Netzwerkzugriff“ [15]
- „Datenschutz und Sicherheit“ [16]
- „Protokollverwaltung“ [16]

Energiesteuerung der Hardware

Mithilfe von Software können Sie einige Oracle-Systeme ein- und ausschalten. Die PDUs einiger Systemschränke können per Remote-Zugriff aktiviert oder deaktiviert werden. Normalerweise wird die Autorisierung für diese Befehle während der Systemkonfiguration eingerichtet, die auf Systemadministratoren und Servicepersonal beschränkt ist. Weitere Informationen erhalten Sie in der Dokumentation zum System oder Systemschrank.

Ressourcenüberwachung

Überwachen Sie Hardwarebestände mithilfe von Seriennummern. Bei Oracle-Produkten sind Firmwareseriennummern in Optionskarten und Systemhauptplatinen implementiert. Diese Seriennummern sind über eine LAN-Verbindung einsehbar.

Die Ressourcenüberwachung gestaltet sich noch einfacher, wenn Sie drahtlose RFID-Lesegeräte (Radio Frequency Identification) verwenden. Weitere Informationen dazu finden Sie im Oracle-Whitepaper *How to Track Your Oracle Sun System Assets by Using RFID* unter:

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

Software- und Firmware-Aktualisierungen

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

- Prüfen Sie in regelmäßigen Abständen, ob Updates verfügbar sind.
- Installieren Sie immer die neueste Software- oder Firmwareversion.
- Installieren Sie alle erforderlichen Sicherheitspatches für Ihre Software.
- Beachten Sie, dass zu Komponenten wie Netzwerk-Switches auch Firmware gehört, die aktualisiert werden muss.

Netzwerkzugriff

Halten Sie sich an folgende Richtlinien, um einen sicheren lokalen und Remote-Zugriff auf Ihre Systeme zu gewährleisten:

- Beschränken Sie die Remote-Konfiguration auf bestimmte IP-Adressen, indem Sie SSH statt Telnet verwenden. Da bei Telnet die Übertragung von Benutzernamen und Passwörtern in Klartext erfolgt, können Anmeldedaten theoretisch von allen Personen im LAN-Segment eingesehen werden. Legen Sie ein sicheres Passwort für SSH fest.
- Verwenden Sie die Version 3 des SNMP (Simple Network Management Protocol), um eine sichere Übertragung zu gewährleisten. Frühere SNMP-Versionen bieten keinen ausreichenden Schutz, da sie Authentifizierungsdaten unverschlüsselt übertragen.
- Wenn SNMP erforderlich ist, ändern Sie die SNMP-Standardcommunityzeichenfolge in eine sichere Communityzeichenfolge. Bei einigen Produkten ist PUBLIC als SNMP-Standardcommunityzeichenfolge festgelegt. Angreifer können sich durch Abfragen einer Community ein sehr gutes Bild vom Netzwerk machen und MIB-Werte (Management Information Base) verändern.
- Melden Sie sich nach Verwendung des System-Controllers immer ab, wenn dieser eine Webbrowseroberfläche hat.
- Deaktivieren Sie nicht erforderliche Netzwerkservices wie TCP (Transmission Control Protocol) oder HTTP (Hypertext Transfer Protocol). Aktivieren Sie erforderliche Netzwerkservices und konfigurieren Sie sie sicher.
- Wenden Sie bei Verwendung von LDAP für den Zugriff auf das System die LDAP-Sicherheitsmaßnahmen an. Lesen Sie den *Oracle ILOM Security Guide* unter: <http://www.oracle.com/goto/ILOM/docs>
- Erstellen Sie ein Banner, das den nicht autorisierten Zugriff ausdrücklich untersagt.
- Setzen Sie Zugriffskontrolllisten sinnvoll ein.
- Legen Sie Zeitüberschreitungen für Sitzungen sowie Berechtigungsstufen fest.
- Verwenden Sie Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen für den lokalen und den Remote-Zugriff auf einen Switch.
- Verwenden Sie nach Möglichkeit die RADIUS- und TACACS+-Sicherheitsprotokolle:
 - RADIUS (Remote Authentication Dial In User Service) ist ein Client-/Serverprotokoll, das Netzwerke vor unautorisiertem Zugriff schützt.
 - TACACS+ (Terminal Access Controller Access-Control System) ist ein Protokoll, das einem Remote-Zugriffsserver die Kommunikation mit einem authentifizierten Server erlaubt, um die Zugriffsberechtigung eines Benutzers für ein Netzwerk zu bestimmen.
- Verwenden Sie die Portspiegelungsfunktion des jeweiligen Switches für den Zugriff auf das Angriffserkennungssystem.
- Richten Sie einen Portschutz zur Beschränkung des Zugriffs anhand von MAC-Adressen ein. Deaktivieren Sie das automatische Trunking bei allen Ports.

Datenschutz und Sicherheit

Halten Sie sich an folgende Richtlinien, um maximalen Datenschutz und höchste Sicherheit zu erreichen:

- Sichern Sie wichtige Daten auf externen Festplatten oder USB-Speichermedien. Speichern Sie die gesicherten Daten an einem zweiten Ort erneut ab, der sicher ist und sich nicht in der Nähe des ersten Speicherorts befindet.
- Schützen Sie vertrauliche Daten auf Festplatten mithilfe von Verschlüsselungssoftware.
- Zerstören Sie nicht mehr verwendete Festplatten, oder löschen Sie sämtliche der darauf enthaltenen Daten. Daten können auch dann wiederhergestellt werden, wenn sie gelöscht wurden oder die Festplatte neu formatiert wurde. Durch das Löschen oder Neuformatieren wird nur die Adresstabelle auf der Festplatte entfernt. Löschen Sie alle Daten auf der Festplatte unwiderruflich mithilfe von Tools zur vollständigen Bereinigung von Festplatten.

Protokollverwaltung

Überprüfen und verwalten Sie Ihre Protokolldateien in regelmäßigen Abständen. Diese Vorgehensweise trägt zum Schutz dieser Dateien bei.

- Aktivieren Sie den Protokollierungsvorgang und senden Sie Systemprotokolle an einen dezidierten, sicheren Protokollhost.
- Konfigurieren Sie die Protokollierung mithilfe von NTP (Network Time Protocol) und Zeitstempeln, damit die Zeitangaben korrekt sind.
- Prüfen Sie die Protokolle auf Vorfälle, und archivieren Sie sie gemäß den Sicherheitsrichtlinien.
- Wenn der Umfang der Protokolle eine vertretbare Größe überschritten hat, entfernen Sie Protokolldateien in regelmäßigen Abständen. Bewahren Sie eine Kopie der entfernten Dateien für künftige Verwendungszwecke oder statistische Analysen auf.