Oracle® Server X5-2L - Sicherheitshandbuch

Teilenr.: E58229-01
Oktober 2014

Teilenr.: E58229-01

Inhalt

Basissicherheit

Dieses Dokument enthält allgemeine Sicherheitsrichtlinien, mit denen Sie Ihren Oracle-Server, Servernetzwerkschnittstellen und verbundene Netzwerk-Switches schützen können.

Wenden Sie sich wegen zusätzlicher Sicherheitsanforderungen bei Ihrem System und Ihrer spezifischen Umgebung an den IT-Sicherheitsbeauftragten.

Es gibt einige Sicherheitsgrundlagen, die Sie bei der Verwendung der gesamten Hardware und Software beachten müssen. In diesem Abschnitt werden die vier grundlegenden Sicherheitsprinzipien abgedeckt:

Zugang

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

- Schützen Sie Ihre Hardware und Ihre Daten durch physische und virtuelle Steuerungsmechanismen vor unerlaubten Zugriffen.
- 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 auf Hardware oder Software erhalten.
- 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 Zugriff auf USB-Ports und -Konsolen ein. Geräte wie Systemcontroller, Stromverteilungseinheiten (Power Distribution Units, PDUs) und Netzwerk-Switches

weisen USB-Anschlüsse auf, die einen direkten Zugang zum System bieten können. Der physische Zugriff ist eine sicherere Methode, auf Komponenten zuzugreifen, da sie dabei keinen netzwerkbasierten Angriffen ausgesetzt ist.

- Begrenzen Sie die Möglichkeit, das System über das Netzwerk neu zu starten.
- 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

Bei der Authentifizierung wird ein Benutzer identifiziert, im Allgemeinen über vertrauliche Informationen, wie Benutzername und Kennwort. Durch die Authentifizierung wird sichergestellt, dass es sich bei Benutzern von Hardware oder Software wirklich um diese 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 Timeouts für Sitzungen sowie Berechtigungsstufen für Benutzer fest.

Autorisierung

Durch die Autorisierung können Administratoren kontrollieren, welche Aufgaben oder Berechtigungen ein Benutzer ausführen oder verwenden kann, Mitarbeiter können nur die Aufgaben ausführen und Berechtigungen verwenden, die ihnen zugewiesen wurden. Die Autorisierung bezieht sich auf Beschränkungen bei der Verwendung von Hardware und Software durch Mitarbeiter.

- Erlauben Sie Mitarbeitern, nur mit der Hardware und Software zu arbeiten, für deren Verwendung sie geschult und qualifiziert sind.
- Legen Sie Berechtigungen für das Lesen, Schreiben und Ausführen fest, um den Zugriff von Benutzern auf Befehle, Festplattenspeicher, Geräte und Anwendungen zu steuern.

Ressourcenerfassung und Auditing

Ressourcenerfassung und Auditing beziehen sich auf die Verwaltung einer Aufzeichnung von Benutzeraktivitäten im System. Oracle-Server verfügen über Software- und Hardwarefunktionen, mit denen Administratoren Anmeldeaktivitäten überwachen und Hardwarebestände verwalten können.

- Überwachen Sie die Anmeldung von Benutzern anhand von Systemprotokollen. Überwachen Sie insbesondere Systemadministrator- und Servicekonten, weil diese Konten Zugriff auf Befehle haben, die bei falscher Verwendung das System beschädigen oder zu Datenverlust führen können. Zugriff und Befehle müssen über Systemprotokolle sorgfältig überwacht werden.
- Schreiben Sie die Seriennummern der gesamten Hardware auf. Überwachen Sie die Systemkomponenten anhand ihrer Seriennummern. Oracle-Teilenummern werden auf Karten, Modulen und Hauptplatinen elektronisch gespeichert und können zu Inventarerfassungszwecken verwendet werden.
- Versehen Sie für die Komponentenerkennung und -überwachung alle wichtigen Hardwarekomponenten wie FRUs und CRUs mit einer Sicherheitskennung. Verwenden Sie spezielle UV-Stifte oder geprägte Beschriftungen.
- Verwahren Sie Hardwareaktivierungsschlüssel und Lizenzen an einem sicheren Ort, der für Systemadministratoren – insbesondere bei Systemnotfällen – leicht zugänglich ist. Die ausgedruckten Dokumente sind möglicherweise Ihr einziger Eigentumsnachweis.

Sichere Verwendung von Serverkonfigurations- und Managementools

Orientieren Sie sich bei der Anwendung von Software- und Firmwaretools zur Konfiguration und Verwaltung Ihres Servers an den Sicherheitsrichtlinien in diesen Abschnitten:

- „Oracle System Assistant“ [11]
- „Oracle ILOM“ [12]
- „Sicherheit von Oracle Hardware Management Pack“ [14]

Wenden Sie sich wegen zusätzlicher Sicherheitsanforderungen bei Ihrem System und Ihrer spezifischen Umgebung an den IT-Sicherheitsbeauftragten.

Oracle System Assistant

Oracle System Assistant ist ein vorinstalliertes Tool, mit dem Sie Serverhardware konfigurieren und aktualisieren sowie unterstützte Betriebssysteme installieren können. Informationen zur Anwendung von Oracle System Assistant erhalten Sie im *Oracle X5 Series Servers Administration Guide* unter:

`http://www.oracle.com/goto/x86AdminDiag/docs`

Im folgenden Abschnitt werden Sicherheitsfragen für Oracle System Assistant beschrieben.

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

  Die Oracle System Assistant-Anwendung wird auf einem vorinstallierten, internen USB-Flashlaufwerk ausgeführt. Oracle System Assistant 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 KVMS-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. Um die Sicherheit zu erhöhen, schützen Sie den physischen Zugang zu dem Server und weisen Administrator- und Konsolenberechtigungen für Oracle ILOM-Benutzer sparsam zu.

Die Oracle System Assistant-Shell soll Benutzern mit entsprechenden Berechtigungen die Verwendung von CLI-Tools des Oracle Hardware Management Packs zur Systemverwaltung ermöglichen. Die Shell soll keine Netzwerkservices bereitstellen. Netzwerkservices sind standardmäßig deaktiviert, um den höchsten Sicherheitsgrad zu gewährleisten. Sie sollten nicht aktiviert werden.

- **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.

  Im Hinblick auf höhere Sicherheit wenden Sie für das Oracle System Assistant-Speichergerät dieselben Methoden an, die Sie für den Schutz von Datenträgern verwenden, einschließlich Virenscans und Integritätsprüfung.

- **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 sind oder Sie Oracle System Assistant nicht benötigen, können Sie das Tool deaktivieren. Nachdem Sie Oracle System Assistant deaktiviert haben, ist das USB-Speichergerät für das Hostbetriebssystem nicht mehr zugänglich, und Benutzer können nicht in Oracle System Assistant booten.

  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-Setupdienstprogramm ist zu empfehlen, damit nur autorisierte Benutzer Oracle System Assistant erneut aktivieren können.

- **Hierzu wird auf die Oracle System Assistant-Dokumentation verwiesen.**

  Informationen zu Oracle System Assistant-Features und -Funktionen finden Sie im *Oracle X5 Series Servers Administration Guide* unter:

  `http://www.oracle.com/goto/x86AdminDiag/docs`

Oracle ILOM

Sie können Systemkomponenten mit der Verwaltungsfirmware von Oracle ILOM (Oracle Integrated Lights Out Manager) selbst sichern, verwalten und überwachen. Sie ist in x86-basierten Oracle-Servern und auf einigen SPARC-basierten Oracle-Servern vorinstalliert. Je nach Autorisierungsebene, die den Systemadministratoren erteilt wurde, können diese Funktionen die Möglichkeit umfassen, den Server auszuschalten, Benutzerkonten zu erstellen, Remote-Speichergeräte zu mounten usw.

- **Verwenden Sie ein sicheres, internes vertrauenswürdiges Netzwerk.**

  Unabhängig davon, ob Sie eine physische Verwaltungsverbindung zu Oracle ILOM über den lokalen seriellen Port, den dedizierten Netzwerkverwaltungsport oder den Standarddatennetzwerk-Port herstellen, muss dieser physische Port auf dem Server oder dem Chassis Monitoring Module (CMM) immer mit einem internen vertrauenswürdigen Netzwerk oder einem dedizierten sicheren Verwaltungsnetzwerk verbunden sein.

  Verbinden Sie den Oracle ILOM-Serviceprozessor (SP) nie mit einem öffentlichen Netzwerk, wie dem Internet. Führen Sie den Oracle ILOM SP-Verwaltungsdatenverkehr auf einem separaten Verwaltungsnetzwerk, auf das nur Administratoren Zugriffsberechtigungen haben.

- **Begrenzen Sie die Verwendung des Standardadministratorkontos.**

  Begrenzen Sie die Verwendung des Standardadministratorkontos (`root`) auf die anfängliche Oracle ILOM-Anmeldung. Dieses Standardadministratorkonto wird nur für die anfängliche Serverinstallation bereitgestellt. Ändern Sie deshalb das Standardadministratorpasswort (`changeme`) während des Anfangssetups des Systems, um einen bestmöglichen Schutz der Umgebung zu gewährleisten. Wenn Benutzer Zugriff auf das Standardadministratorkonto erhalten, können sie uneingeschränkt auf alle Oracle ILOM-Funktionen zugreifen. Richten Sie zusätzlich neue Benutzerkonten mit eindeutigen Passwörtern ein, und weisen Sie Autorisierungsebenen (Benutzerrollen) für jeden neuen Oracle ILOM-Benutzer ein.

- **Erwägen Sie die Risiken sorgfältig, wenn Sie den seriellen Port mit einem Terminalserver verbinden.**

  Terminalgeräte bieten nicht immer die entsprechenden Ebenen der Benutzerauthentifizierung oder -autorisierung, die erforderlich sind, um das System vor böswilligen Angriffen zu schützen. Um Ihr System vor unerwünschten Netzwerkangriffen zu schützen, stellen Sie keine serielle Verbindung (serieller Port) zu Oracle ILOM über irgendein Netzwerkumleitungsgerät her, wie einen Terminalserver, es sei denn, der Server verfügt über ausreichend Zugriffskontrollen.

  Außerdem werden bestimmte Oracle ILOM-Funktionen, wie Kennwortrücksetzung und das Preboot-Menü, nur über den physischen seriellen Port verfügbar gemacht. Wenn der serielle Port über einen nicht authentifizierten Terminalserver mit einem Netzwerk verbunden wird, ist kein physischer Zugriff mehr erforderlich, und die Sicherheit für diese Funktionen wird verringert.

- **Der Zugriff auf das Preboot-Menü erfordert physischen Zugang zu dem Server.**

  Das Oracle ILOM Preboot-Menü ist ein leistungsfähiges Dienstprogramm, mit dem Oracle ILOM auf Standardwerte zurückgesetzt und Firmware geflasht werden kann, wenn Oracle ILOM nicht mehr reagieren sollte. Nachdem Oracle ILOM zurückgesetzt wurde, muss ein Benutzer entweder eine Taste auf dem Server drücken (Standard) oder ein Passwort eingeben. Die Oracle ILOM Physical Presence-Eigenschaft kontrolliert dieses Verhalten (`check_physical_presence= true`). Für maximale Sicherheit beim Zugriff auf das Preboot-Menü ändern Sie die Standardeinstellung (`true`) nicht, sodass der Zugriff auf das Preboot-Menü immer den physischen Zugang zu dem Server erfordert.

- **Hierzu wird auf die Oracle ILOM-Dokumentation verwiesen.**

Lesen Sie die Oracle ILOM-Dokumentation für weitere Informationen zur Einrichtung von Passwörtern, Verwaltung von Benutzern und Anwendung von sicherheitsbezogenen Funktionen. Auf Oracle ILOM abgestimmte Sicherheitsrichtlinien finden Sie in der Oracle ILOM Documentation Library in *Oracle ILOM Security Guide*. Die Dokumentation zu Oracle ILOM finden Sie unter folgendem Link:

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

Sicherheit von Oracle Hardware Management Pack

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

- **Verwenden von SNMP-Plug-ins des Hardware Management Agents.**

  SNMP ist ein Standardprotokoll, das zur Systemüberwachung oder -verwaltung verwendet wird. In Verbindung mit den SNMP-Plug-ins von Hardware Management Agent können Sie SNMP zur Überwachung von Oracle-Servern in Ihrem Rechenzentrum einsetzen, ohne dass Sie sich mit zwei Verwaltungspunkten (Host und Oracle ILOM) verbinden müssen. Durch diese Funktion kann eine einzige IP-Adresse (IP-Adresse des Hosts) zur Überwachung von mehreren Servern verwendet werden.

  Die SNMP-Plug-ins werden auf dem Hostbetriebssystem der Oracle-Server ausgeführt. Das SNMP-Plug-in-Modul erweitert den nativen SNMP-Agent im Hostbetriebssystem um zusätzliche Oracle MIB-Funktionen. Oracle Hardware Management Pack selbst enthält keinen SNMP-Agent. Bei Linux wird dem net-snmp Agent ein Modul hinzugefügt. Bei Oracle Solaris wird dem Oracle Solaris Management Agent ein Modul hinzugefügt Bei Microsoft Windows wird der native SNMP-Service durch das Plug-in erweitert. Alle SNMP-bezogenen Sicherheitseinstellungen für das SNMP-Plug-in von Oracle Hardware Management Pack werden durch die Einstellungen des nativen SNMP-Agents oder -Service und nicht durch das Plug-in bestimmt.

  SNMPv1 und SNMPv2c bieten keine Verschlüsselung und führen die Authentifizierung anhand von Communityzeichenfolgen durch. SNMPv3 ist die sicherere Version. Sie wird empfohlen, weil sie einen sicheren Kanal durch Verschlüsselung bereitstellt und individuelle Benutzernamen und Passwörter verwendet.

- **Hierzu wird auf die Oracle Hardware Management Pack-Dokumentation verwiesen.**

  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

Planen einer sicheren Umgebung

Sicherheitsrichtlinien sollten bereits vor Eintreffen des Systems festgelegt worden sein. Danach müssen die Sicherheitsrichtlinien regelmäßig geprüft und angepasst werden, damit sie den Sicherheitsanforderungen Ihres Unternehmens entsprechen.

Verwenden Sie die Informationen in diesen Abschnitten vor und während der Installation und Konfiguration eines Servers und der zugehörigen Geräte:

Wenden Sie sich wegen zusätzlicher Sicherheitsanforderungen bei Ihrem System und Ihrer spezifischen Umgebung an den IT-Sicherheitsbeauftragten.

Passwortschutz

Passwörter sind ein wichtiger Aspekt der Sicherheit, da schlecht ausgewählte Passwörter dazu führen können, dass Unberechtigte Zugriff auf Unternehmensressourcen erlangen. Die Umsetzung von Best Practices bei der Passwortverwaltung führt dazu, dass Benutzer bei der Erstellung und beim Schutz ihrer Passwörter eine Reihe von Richtlinien einhalten. Typische Bestandteile einer Passwortrichtlinie müssen Folgendes definieren:

- Passwortlänge und -sicherheit
- Passwortdauer
- Allgemeine Vorgehensweise bei Passwörtern

Setzen Sie die folgenden gängigen Vorgehensweisen zur Erstellung komplexer Passwörter durch:

- Erstellen Sie keine Passwörter, die den Benutzernamen, den Mitarbeiternamen oder den Familiennamen enthalten.
- Wählen Sie keine Passwörter, die sich einfach erraten lassen.
- Erstellen Sie keine Passwörter, die eine aufeinander folgende Zeichenfolge von Zahlen wie 12345 enthalten.

- 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 keine alten Passwörter wiederverwenden.

Ändern Sie Passwörter regelmäßig. Auf diese Weise werden bösartige Aktivitäten verhindert und wird sichergestellt, dass die Passwörter den aktuellen Passwortrichtlinien entsprechen.

Sicherheitsrichtlinien 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 netzwerkbasierten Anwendungen

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

Betriebssystem	Link
Oracle Solaris-BS	www.oracle.com/technetwork/documentation/solaris-11-192991.html
Oracle Linux-BS	http://www.oracle.com/technetwork/documentation/ol-1-1861776.html
Oracle VM	http://www.oracle.com/technetwork/documentation/vm-096300.html

Informationen zu Betriebssystemen anderer Hersteller, wie Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Microsoft Windows und VMware ESXi, finden Sie in der Dokumentation des jeweiligen Herstellers.

Netzwerk-Switches und -ports

Bei Netzwerk-Switches 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 alle Passwörter für Netzwerk-Switches, die standardmäßig mehrere Benutzerkonten und -passwörter umfassen können.
- Nehmen Sie eine Out-of-Band-Verwaltung von Switches vor (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 autorisierte 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) von mindestens einem Gerät 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-Sicherheit

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

- Trennen Sie vertrauliche Cluster der Systeme vom restlichen Netzwerk ab, wenn Sie VLANs verwenden. 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 Verwaltungsdomain, Passwort und Pruning fest. Versetzen Sie dann VTP in den Modus "Transparent".
- Entscheiden Sie sich nach Möglichkeit für statische VLAN-Konfigurationen.

- Deaktivieren Sie nicht verwendete Switch-Ports, und weisen Sie ihnen eine nicht verwendete VLAN-Nummer zu.

InfiniBand-Sicherheit

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.

Verwalten einer sicheren Umgebung

Steuern Sie nach abgeschlossener Erstinstallation und Setup die Hardware- und Softwaresystemressourcen mithilfe von Oracle Hardware- und Softwaresicherheitsfunktionen.

Verwenden Sie die Informationen in diesen Abschnitten, um eine sichere Umgebung zu verwalten:

Wenden Sie sich wegen zusätzlicher Sicherheitsanforderungen bei Ihrem System und Ihrer spezifischen Umgebung an den IT-Sicherheitsbeauftragten.

Energiesteuerung

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. Ein Oracle Whitepaper mit dem Titel *How to Track Your Oracle Sun System Assets by Using RFID* finden Sie unter:

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

Software- und Firmwareaktualisierungen

Durch die neuen Softwarereleases und -patches wird die Sicherheit noch verbessert. Eine effektive proaktive Patchverwaltung ist ein wichtiger Teil der Systemsicherheit. Für optimale Sicherheit updaten Sie Ihr System immer mit dem neuesten Softwarerelease und allen erforderlichen Sicherheitspatches.

- Prüfen Sie regelmäßig auf Softwareupdates und Sicherheitspatches.
- 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 oder Patches benötigen kann.

Softwareupdates und Sicherheitspatches finden Sie auf der Website My Oracle Support unter:

http://support.oracle.com

Netzwerksicherheit

Nachdem die Netzwerke nach den neuesten Sicherheitsstandards konfiguriert wurden, sind regelmäßige Prüfung und Wartung erforderlich.

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. Bei SNMPv3 werden die Verschlüsselung zum Erreichen eines sicheren Kanals sowie individuelle Benutzernamen und Passwörter verwendet.
- Wenn SNMPv1 oder SNMPv2 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 Systemcontrollers immer ab, wenn dieser eine Browseroberfläche verwendet.
- Deaktivieren Sie nicht erforderliche Netzwerkservices wie TCP (Transmission Control Protocol) oder HTTP (Hypertext Transfer Protocol). Aktivieren Sie erforderliche Netzwerkservices, und konfigurieren Sie diese sicher.
- Erstellen Sie eine Bannermeldung, die bei der Anmeldung angezeigt wird und darauf hinweist, dass nicht autorisierter Zugriff untersagt ist. Sie können Benutzer über wichtige Richtlinien oder Regeln informieren. Das Banner kann dazu verwendet werden, Benutzer vor speziellen Zugriffsbeschränkungen für ein bestimmtes System zu warnen oder sie an Passwortrichtlinien und eine korrekte Handhabung zu erinnern.
- Verwenden Sie falls erforderlich Zugriffskontrolllisten, um Einschränkungen durchzusetzen.
- Legen Sie Timeouts für Sitzungen sowie Berechtigungsstufen fest.
- Verwenden Sie Authentifizierungs-, Autorisierungs- und Ressourcenerfassungsfunktionen für den lokalen und den Remote-Zugriff auf einen Switch.
- Verwenden Sie diese Services in sehr stark abgesicherten Umgebungen, da sie durch Zertifikate und andere sichere Verschlüsselungsmethoden zum Schutz des Kanals geschützt sind:
  - Active Directory
  - LDAP/SSL (Lightweight Directory Access Protocol/Secure Socket Layer)
- Verwenden Sie diese Services für private, sichere Netzwerke, in denen sich keine verdächtigen, böswilligen Benutzer befinden:
  - RADIUS (Remote Authentication Dial In User Service)
  - TACACS+ (Terminal Access Controller Access-Control System)
- Verwenden Sie die Portspiegelungsfunktion des jeweiligen Switch 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.

Weitere Informationen zur Netzwerksicherheit finden Sie im *Oracle ILOM - Sicherheitshandbuch*, das Bestandteil der Oracle ILOM Documentation Library ist. Die Dokumentation zu Oracle ILOM finden Sie unter folgendem Link:

`http://www.oracle.com/goto/ILOM/docs`

Datenschutz und Sicherheit

Halten Sie sich an folgende Richtlinien, um maximalen Datenschutz und maximale Datensicherheit zu gewährleisten:

- Sichern Sie wichtige Daten auf externen Datenträgern oder USB-Sticks. 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 eines Laufwerks.
- Festplatten werden häufig zum Speichern sensibler Informationen verwendet. Um die unautorisierte Offenlegung dieser Informationen zu verhindern, müssen Festplatten komplett bereinigt werden, bevor sie wiederverwendet, außer Betrieb genommen oder entsorgt werden.
  - Verwenden Sie Tools zum Bereinigen von Datenträgern, wie den Oracle Solaris-Befehl `format(1M)`, um alle Daten vollständig von der Festplatte zu löschen. Alternativ dazu können Sie physische Entmagnetisierungswerkzeuge verwenden, sofern angemessen und verfügbar.
  - In einigen Fällen sind die Daten auf den Festplatten so sensibel, dass die Festplatte physisch zerstört werden muss, indem sie pulverisiert oder eingeäschert wird.
  - Es wird dringend empfohlen, dass Organisationen sich auf ihre Datenschutzrichtlinien beziehen, um die am ehesten geeignete Methode zum Bereinigen von Festplatten zu bestimmen.

Achtung - Einige Daten auf modernen Festplatten, insbesondere SSDs (Solid State Drives), können möglicherweise nicht von Software zum Bereinigen von Datenträgern gelöscht werden. Dies liegt an der Art, wie sie den Datenzugriff verwalten.

Protokollverwaltung

Prüfen und verwalten Sie Ihre Protokolldateien in regelmäßigen Abständen. Folgende Vorgehensweisen tragen zum Schutz dieser Dateien bei:

- Aktivieren Sie den Protokollierungsvorgang, und senden Sie Systemprotokolle an einen dedizierten, sicheren Protokollhost.
- Konfigurieren Sie die Protokollierung mithilfe von NTP (Network Time Protocol) und Zeitstempeln, damit die Zeitangaben korrekt sind.
- Führen Sie regelmäßig festgelegte Scans von Netzwerkgeräteprotokollen auf ungewöhnliche Netzwerkaktivitäten oder -zugriffe durch.
- 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.