Server der Serien SPARC und Netra SPARC T5

Sicherheitshandbuch

Teilenr.: E40476-01
April 2013

Inhaltsverzeichnis

• • • Kapitel 1

Sicherheitsrichtlinien für Server der Serien SPARC und Netra SPARC T5

Dieses Dokument bietet allgemeine Sicherheitsrichtlinien für Server vom Typ SPARC T5-1B, T5-2, T5-4, T5-8 und Netra SPARC T5-1B. Mit diesem Handbuch soll die Sicherheit bei der Verwendung dieser Server in Kombination mit anderen Oracle-Hardwareprodukten wie Netzwerk-Switches und Netzwerkschnittstellenkarten gewährleistet werden.

Dieses Kapitel enthält die folgenden Abschnitte:

Sicherheitsgrundsätze

Es gibt vier Sicherheitsgrundsätze: Zugang, Authentifizierung, Autorisierung und Überwachung.

- **Zugang**

  Physische und virtuelle Steuerungsmechanismen schützen Ihre Hardware oder Daten vor unerlaubten Zugriffen.
  - Bei Hardware beziehen sich Zugangsbeschränkungen in der Regel auf *physische* Zugangsbeschränkungen.
  - Bei Software wird sowohl der physische als auch der virtuelle Zugang beschränkt.
  - Firmware kann nur über den Oracle-Aktualisierungsprozess geändert werden.
- **Authentifizierung**

  Alle Betriebssysteme für die einzelnen Plattformen verfügen über Funktionen, die eingerichtet werden können, um sicherzustellen, dass es sich bei einem Benutzer wirklich um diesen Benutzer handelt.

  Die Authentifizierung bietet unterschiedliche Sicherheitsgrade über Maßnahmen wie Ausweise und Passwörter.
- **Autorisierung**

Durch die Autorisierung können Mitarbeiter nur mit der Hardware und Software arbeiten, für die sie geschult wurden. Legen Sie Berechtigungen für das Lesen, Schreiben und Ausführen fest, um den Zugriff von Benutzern auf Befehle, Festplattenspeicher, Geräte und Anwendungen zu steuern.

- **Überwachung**

  Verwenden Sie Hardware- und Softwareüberwachungsfunktionen von Oracle zur Überwachung von Anmeldevorgängen und zur Wartung der Hardware.

  - Die Anmeldung von Benutzern kann anhand von Systemprotokollen überwacht werden. Besonders Systemadministrator- und Wartungskonten bieten Zugriff auf leistungsstarke Befehle und sollten anhand von Systemprotokollen sorgfältig überwacht werden. Protokolle werden generell über einen langen Zeitraum geführt. Aus diesem Grund ist es äußerst wichtig, Protokolldateien regelmäßig als veraltet einzustufen, sobald diese gemäß der Unternehmensrichtlinie des Kunden eine bestimmte Größe überschreiten.
  - Die Nachverfolgung der IT-Ressourcen von Kunden funktioniert generell über Seriennummern. Oracle-Teilenummern werden auf allen Karten, Modulen und Hauptplatinen elektronisch gespeichert und können zu Inventarerfassungszwecken verwendet werden.

Einrichten einer sicheren Umgebung

Beachten Sie die folgenden Hinweise vor und während der Installation und Konfiguration eines Servers und zugehöriger Geräte.

Hardwaresicherheit

Physische Hardware kann durch Einschränken des Zugangs zur Hardware und Aufbewahren der Seriennummern relativ einfach abgesichert werden.

- **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.
  - Schränken Sie den Zugang auf USB-Konsolen ein, die einen leistungsstärkeren Zugang als SSH-Verbindungen bieten. Geräte wie System-Controller, Steckdosenleisten (Power Distribution Units, PDUs) und Netzwerk-Switches weisen USB-Anschlüsse 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) oder CRUs (Customer Replaceable Units) in einem abschließbaren Schrank. Nur autorisiertes Personal sollte Zugang zu diesem Schrank haben.
- **Bewahren Sie Seriennummern auf**
  - Bewahren Sie alle Hardwareseriennummern auf.
  - Versehen Sie alle wichtigen Komponenten der Computerhardware, wie z. B. Ersatzteile, mit einer Sicherheitskennzeichnung. Verwenden Sie spezielle UV-Stifte oder geprägte Beschriftungen.
  - Bewahren Sie Hardwareaktivierungsschlüssel und Lizenzen an einem sicheren Ort auf, der im Systemnotfall für den Systemverwalter einfach zugänglich ist. Die ausgedruckten Dokumente sind möglicherweise Ihr einziger Eigentumsnachweis.

Softwaresicherheit

Hardwaresicherheit wird größtenteils durch Softwaremaßnahmen umgesetzt.

- Ändern Sie alle Standardpasswörter, wenn ein neues System installiert wird. Für die meisten Geräte werden allgemein bekannte Standardpasswörter wie **"changeme"** verwendet, bei denen die Gefahr besteht, dass Unbefugte Zugriff erhalten. Geräte wie Netzwerk-Switches können außerdem standardmäßig mehrere Benutzerkonten umfassen. Stellen Sie sicher, dass Sie die Passwörter für alle Konten geändert haben.
- Schränken Sie die Verwendung des `Root`-Superuser-Kontos ein. Stattdessen sollten nach Möglichkeit Oracle Integrated Lights Out Manager (Oracle ILOM)-Benutzerprofile wie z. B. `""Operator"` und `"Administrator"` verwendet werden.
- Trennen Sie den Serviceprozessor vom Gesamtnetzwerk, indem Sie ihn in ein dezidiertes Netzwerk integrieren.
- Informationen zum Aktivieren der Sicherheitsfunktionen Ihrer Software finden Sie in der produktbegleitenden Dokumentation.
- Ein Server kann mithilfe von "WAN Boot" oder "iSCSI Boot" sicher gebootet werden.
  - Lesen Sie für das Oracle Solaris 10-Release das Handbuch *Oracle Solaris Installation Guide: Network-Based Installations* für weitere Informationen.
  - Lesen Sie für das Oracle Solaris 11-Release das Handbuch *Installing Oracle Solaris 11 Systems* für weitere Informationen zu "WAN Boot" und das Handbuch *System Administration Guide: Basic Administration* für weitere Informationen zu "iSCSI Boot".

Das Dokument *Oracle Solaris Security Guidelines* enthält Informationen zu folgenden Themen:

- Schützen von Oracle Solaris
- Anwenden von Oracle Solaris-Sicherheitsfunktionen bei der Systemkonfiguration
- Sicheres Vorgehen beim Hinzufügen von Anwendungen und Benutzern zu einem System
- Schutz von netzwerkbasierten Anwendungen

Sie finden das Dokument *Oracle Solaris Security Guidelines* für die von Ihnen verwendete Version unter:

- http://www.oracle.com/goto/Solaris11/docs
- http://www.oracle.com/goto/Solaris10/docs

Firmwaresicherheit

Alle Unterkomponenten der Oracle System-Firmware können nur gemeinsam aktualisiert werden. Die Oracle System-Firmware verwendet einen kontrollierten Firmwareaktualisierungsprozess, um nicht autorisierte Firmwaremodifizierungen zu verhindern. Ausschließlich der Superuser oder ein authentifizierter Benutzer mit ordnungsgemäßer Autorisierung kann den Aktualisierungsprozess verwenden.

Oracle OpenBoot-Sicherheit

Der Zugriff auf die Oracle OpenBoot Firmware-Befehlszeilenschnittstelle kann unter Verwendung der OpenBoot Sicherheitsvariablen durch ein Passwort geschützt werden.

Informationen zum Festlegen der OpenBoot-Sicherheitsvariablen finden Sie im *OpenBoot 4.x-Befehlsreferenzhandbuch*.

- http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

Oracle ILOM-Firmware

Oracle Integrated Lights Out Manager (ILOM) ist eine Systemverwaltungs-Firmware, die auf dem Server, dem Servermodul, dem Modularsystem sowie anderer Oracle-Hardware vorinstalliert ist. Oracle ILOM ermöglicht die aktive Verwaltung und Überwachung der in Ihrem System installierten Komponenten. Die Art und Weise, auf die Sie Oracle ILOM verwenden, beeinflusst die Sicherheit Ihres Systems. Weitere Informationen zur Verwendung dieser Firmware 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), finden Sie in der Dokumentation zu Oracle ILOM:

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

Verwalten einer sicheren Umgebung

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

Hardwaresteuerung

Einige Oracle-Systeme lassen sich so einrichten, dass sie durch Softwarebefehle aktiviert bzw. deaktiviert werden können. Zusätzlich können die PDUs einiger Systemschränke per Remote-Zugriff über Softwarebefehle 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

Oracle-Seriennummern sind in die Firmware auf Optionskarten und Systemhauptplatinen eingebettet. Diese Seriennummern können über LAN-Verbindungen (Local Area Network) zu Inventarnachverfolgungszwecken gelesen werden.

Durch drahtlose RFID-Lesegeräte (Radio Frequency Identification) gestaltet sich die Ressourcenüberwachung noch einfacher. 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

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

Lokaler und Remote-Zugriff

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

- 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 unautorisierten Zugriffen schützt.
  - TACACS+ (Terminal Access Controller Access-Control System) ist ein Protokoll, das einem Remotezugriffsserver die Kommunikation mit einem authentifizierten Server erlaubt, um die Zugriffsberechtigung eines Benutzers für ein Netzwerk zu bestimmen.
- 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.
- Beschränken Sie die Remotekonfiguration 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.
- Frühere SNMP-Versionen bieten keinen ausreichenden Schutz, da sie Authentifizierungsdaten unverschlüsselt übertragen. Nur Version 3 von SNMP bietet sichere Übertragungen.
- Bei einigen Produkten ist PUBLIC serienmäßig 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. Wenn SNMP erforderlich ist, ändern Sie die SNMP-Standardcommunityzeichenfolge in eine sichere Communityzeichenfolge.
- Aktivieren Sie den Protokollierungsvorgang und senden Sie Protokolle 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.
- Melden Sie sich nach Verwendung des System-Controllers immer ab, wenn dieser eine Webbrowseroberfläche hat.

Datensicherheit

Halten Sie sich an folgende Richtlinien, um einen maximalen Datenschutz zu erreichen:

- Sichern Sie wichtige Daten auf externen Festplatten 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. Durch das Löschen von Dateien oder Neuformatieren des Laufwerks werden lediglich die Adresstabellen auf dem Laufwerk entfernt. Informationen können auch nach dem Löschen von Dateien oder Neuformatieren des Laufwerks wiederhergestellt werden. (Löschen Sie alle Daten auf der Festplatte unwiderruflich mithilfe von Tools zur vollständigen Bereinigung von Festplatten.)

Netzwerksicherheit

Halten Sie sich an folgende Richtlinien, um die bestmögliche Netzwerksicherheit zu erreichen:

- Die meisten Switches lassen das Definieren von VLANs (Virtual Local Area Networks) zu. Definieren Sie über Ihren Switch VLANs, damit sensible Systemcluster vom übrigen Netzwerk getrennt werden. Dadurch sinkt die Wahrscheinlichkeit, dass Benutzer auf diesen Clients und Servern Zugriff auf Daten erhalten.
- 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.
- 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.
- Pflegen Sie offline eine Switch-Konfigurationsdatei und beschränken Sie den Zugriff auf befugte Administratoren. Die Konfigurationsdatei sollte beschreibende Kommentare zu jeder Einstellung enthalten.
- 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.
- 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".
- Deaktivieren Sie nicht erforderliche Netzwerkdienste wie TCP Small Server oder HTTP. Aktivieren Sie erforderliche Netzwerkdienste und konfigurieren Sie sie sicher.
- Je nach Switch unterscheiden sich die Stufen der Portsicherheitsfunktionen. 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.