Oracle® VM Server for SPARC 3.3 – Sicherheitshandbuch

Teilenr.: E64651
Oktober 2015

Teilenr.: E64651

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** – Umfasst Informationen zur sicheren Verwendung der Oracle VM Server for SPARC 3.3-Software.
- **Zielgruppe** – Systemadministratoren, die die Sicherheit auf virtualisierten SPARC-Servern verwalten
- **Erforderliche Vorkenntnisse** – Systemadministratoren bei diesen Servern benötigen grundlegende Kenntnisse der UNIX®-Systeme und des Oracle Solaris-Betriebssystems (Oracle Solaris-BS)

Produktdokumentationsbibliothek

Dokumentation und Ressourcen für dieses Produkt und verwandte Produkte sind verfügbar unter `http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html`.

Feedback

Unter `http://www.oracle.com/goto/docfeedback` können Sie uns Feedback zu dieser Dokumentation geben.

♦ ♦ ♦ KAPITEL 1

Oracle VM Server for SPARC - Überblick über die Sicherheit

Auch wenn die Anzahl von Sicherheitsempfehlungen in diesem Dokument einen anderen Eindruck vermitteln könnte, ist die Standardinstallation von Oracle VM Server for SPARC bereits sicher vor nicht autorisierter Verwendung geschützt. Eine kleine Angriffsfläche und ein bestimmtes Sicherheitsrisiko bleiben jedoch immer, selbst wenn ein Missbrauch unwahrscheinlich ist. Genauso wie Sie eine Alarmanlage zum Schutz Ihrer Wohnung neben den üblichen Abschreckungen wie Schlössern an den Türen einbauen, können zusätzliche Netzwerksicherheitsmaßnahmen die Gefahr unerwarteter Probleme verringern oder potenzielle Schäden minimieren.

In diesem Kapitel werden die folgenden Oracle VM Server for SPARC-Sicherheitsthemen abgedeckt:

Von Oracle VM Server for SPARC verwendete Sicherheitsfunktionen

Die Oracle VM Server for SPARC-Software ist ein Virtualisierungsprodukt, bei dem mehrere Oracle Solaris Virtual Machines (VMs) auf nur einem physischen System ausgeführt werden können, wobei für jede ein eigenes Oracle Solaris 10- oder Oracle Solaris 11-BS installiert ist. Jede VM wird auch als *logische Domain* bezeichnet. Domains sind unabhängige Instanzen. Sie können unterschiedliche Versionen von Oracle Solaris-BS sowie unterschiedliche Anwendungssoftware ausführen. Beispiel: Für Domains können unterschiedliche Paketrevisionen installiert und unterschiedliche Services aktiviert sein; sie können auch Systemkonten mit unterschiedlichen Kennwörtern haben. In *Oracle Solaris 10 Security Guidelines* und *Oracle Solaris 11 Security Guidelines* finden Sie weitere Informationen zur Oracle Solaris-Sicherheit.

Der Befehl `ldm` ruft Logische Domains Manager auf und muss in der Kontrolldomain ausgeführt werden, um Domains zu konfigurieren und Statusinformationen abzurufen. Die Begrenzung des Zugriffs auf die Kontrolldomain und auf den Befehl `ldm` ist für die Sicherheit der Domains, die auf dem System ausgeführt werden, von wesentlicher Bedeutung. Um den Zugriff auf die Domainkonfigurationsdaten zu begrenzen, verwenden Sie die Oracle VM Server for SPARC-Sicherheitsfunktionen, wie Oracle Solaris-Rechte für Konsole und `solaris.ldoms`-Autorisierungen. Weitere Informationen finden Sie in „Logical Domains Manager Profile Contents“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

Die Oracle VM Server for SPARC-Software verwendet die folgenden Sicherheitsfunktionen:

- Die Sicherheitsfunktionen, die im Oracle Solaris 10-BS und Oracle Solaris 11-BS verfügbar sind, sind auch in Domains verfügbar, auf denen die Oracle VM Server for SPARC-Software ausgeführt wird. Weitere Informationen finden Sie in *Oracle Solaris 10 Security Guidelines* und *Oracle Solaris 11 Security Guidelines* .
- Die Oracle Solaris-BS-Sicherheitsfunktionen können für die Oracle VM Server for SPARC-Software angewendet werden. Umfassende Informationen zur Gewährleistung der Oracle VM Server for SPARC-Sicherheit finden Sie in „Sicherheit in einer virtualisierten Umgebung“ [15] und „Verteidigung vor Angriffen“ [17].
- Das Oracle Solaris 10-BS und das Oracle Solaris 11-BS umfassen Sicherheitsfixes, die für Ihr System verfügbar sind. Rufen Sie die Oracle Solaris 10-BS-Fixes als Sicherheitspatches oder -updates ab. Rufen Sie die Oracle Solaris 11-BS-Fixes als Support Repository Updates (SRUs) ab.
- Informationen zur Begrenzung des Zugriffs auf die Oracle VM Server for SPARC-Administrationsbefehle und Domainkonsolen finden Sie in Kapitel 2, „Oracle VM Server for SPARC Security“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

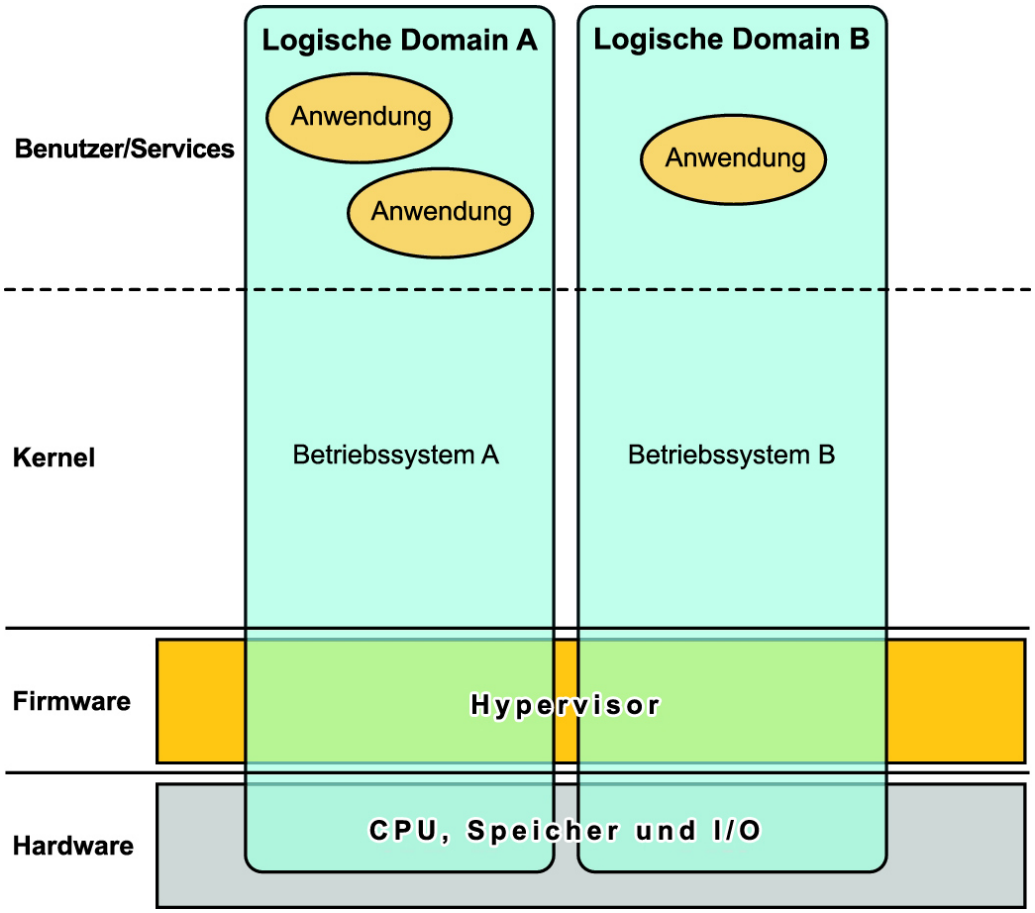
Oracle VM Server for SPARC–Produktüberblick

Oracle VM Server for SPARC stellt hocheffiziente Virtualisierungsfunktionen für Unternehmen bei Oracle SPARC T-Series-Servern sowie den SPARC M5-Servern und Fujitsu M10-Server bereit. Mit der Oracle VM Server for SPARC-Software können Sie viele virtuelle Server, die als logische Domains bezeichnet werden, auf einem einzelnen System erstellen. Mit dieser Art von Konfiguration können Sie das umfangreiche Threadspektrum nutzen, das diese SPARC-Server und das Oracle Solaris-BS bieten.

Eine *logische Domain* ist eine Virtual Machine, die eine diskrete logische Gruppierung von Ressourcen enthält. Eine logische Domain hat ihr eigenes Betriebssystem und ihre eigene Identität in einem einzelnen Computersystem. Jede logische Domain kann unabhängig erstellt, gelöscht, neu konfiguriert und neu gestartet werden, ohne dass Sie den Server aus- und wieder einschalten müssen. Sie können ein breites Spektrum an Anwendungssoftware in verschiedenen logischen Domains ausführen und diese aus Performance- und Sicherheitsgründen unabhängig voneinander halten.

Informationen zur Verwendung der Oracle VM Server for SPARC-Software finden Sie in *Oracle VM Server for SPARC 3.3 Administration Guide* und *Oracle VM Server for SPARC 3.3 Reference Manual* . Informationen zu der erforderlichen Hardware und Software finden Sie in *Oracle VM Server for SPARC 3.3 Installation Guide* .

ABBILDUNG 1-1 Hypervisor, der zwei logische Domains unterstützt



Die Oracle VM Server for SPARC-Software verwendet die folgenden Komponenten, um Systemvirtualisierung bereitzustellen:

- **Hypervisor.** Der Hypervisor ist eine kleine Firmwareschicht, die eine stabile virtualisierte Rechnerarchitektur bereitstellt, in der ein Betriebssystem installiert werden kann. Die Sun-Server von Oracle, die den Hypervisor verwenden, stellen Hardwarefunktionen bereit, mit

denen die Kontrolle des Hypervisors über die Betriebssystemaktivitäten in einer logischen Domain unterstützt werden.

Die Anzahl von Domains und die Funktionen jeder Domain, die ein spezifischer SPARC-Hypervisor unterstützt, sind serverabhängige Funktionen. Der Hypervisor kann Teilmengen der CPU, des Speichers und der I/O-Ressourcen des Servers einer bestimmten logischen Domain zuordnen. Diese Zuordnung ermöglicht die Unterstützung von mehreren Betriebssystemen gleichzeitig, jedes in seiner eigenen logischen Domain. Ressourcen können zwischen logischen Domains mit einer beliebigen Granularität neu angeordnet werden. Beispiel: CPUs können einer logischen Domain mit der Granularität eines CPU-Threads zugewiesen werden.

Der *Serviceprozessor* (SP), auch als *Systemcontroller* (SC) bezeichnet, überwacht und führt den physischen Rechner aus. Der Logische Domains Manager, und nicht der SP, verwaltet die logischen Domains selbst.

- **Kontrolldomain.** Der Logische Domains Manager wird in dieser Domain ausgeführt; mit ihm können Sie andere logische Domains erstellen und den anderen Domains virtuelle Ressourcen zuordnen. Es kann nur eine Kontrolldomain pro Server vorhanden sein. Die Kontrolldomain ist die erste Domain, die erstellt wird, wenn Sie die Oracle VM Server for SPARC-Software installieren. Die Kontrolldomain wird als `primär` bezeichnet.
- **Servicedomain.** Eine Servicedomain stellt virtuelle Geräteservices für andere Domains bereit, wie virtuellen Switch, virtuellen Konsolenkonzentrator und virtuellen Datenträgerserver Jede Domain kann als Servicedomain konfiguriert werden,
- **I/O-Domain.** Eine I/O-Domain hat direkten Zugriff auf physische I/O-Geräte wie eine Netzkarte in einem PCI EXPRESS-(PCIe-)Controller. Eine I/O-Domain kann Eigentümer eines PCIe-Root-Komplexes, eines PCIe-Slots oder eines On-Board-PCIe-Geräts sein, wenn das Direct-I/O-(DIO-)Feature verwendet wird. Weitere Informationen finden Sie in „Creating an I/O Domain by Assigning PCIe Endpoint Devices“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

  Eine I/O-Domain kann physische I/O-Geräte mit anderen Domains in Form von virtuellen Geräten gemeinsam verwenden, wenn die I/O-Domain auch als Servicedomain verwendet wird.
- **Root-Domain.** Einer Root-Domain ist ein PCIe-Root-Komplex zugewiesen. Diese Domain ist Eigentümer des PCIe-Fabrics dieses Root-Komplexes und stellt alle fabric-bezogenen Services bereit, wie Fabric-Fehlerbehandlung. Eine Root-Domain ist auch eine I/O-Domain, weil sie Eigentümer der physischen I/O-Geräte ist und direkten Zugriff auf diese I/O-Geräte hat.

  Die mögliche Anzahl von Root-Domains hängt von Ihrer Plattformarchitektur ab. Beispiel: Wenn Sie einen SPARC T4-4-Server von Oracle verwenden, sind bis zu vier Root-Domains möglich.
- **Gastdomain.** Eine Gastdomain ist eine Nicht-I/O-Domain, die virtuelle Geräteservices konsumiert, die von mindestens einer Servicedomain bereitgestellt werden Eine Gastdomain enthält keine physischen I/O-Geräte. Sie enthält nur virtuelle I/O-Geräte, wie virtuelle Datenträger und virtuelle Netzwerkschnittstellen.

Häufig enthält ein Oracle VM Server for SPARC-System nur eine Kontrolldomain, die die Services bereitstellt, die von I/O-Domains und Servicedomains ausgeführt werden. Um die Redundanz und Plattformwartbarkeit zu verbessern, sollten Sie mehr als eine I/O-Domain in Ihrem Oracle VM Server for SPARC-System konfigurieren.

Anwenden allgemeiner Sicherheitsrichtlinien für Oracle VM Server for SPARC

Sie können Gastdomains auf unterschiedliche Weise konfigurieren, um verschiedene Ebenen der Isolierung der Gastdomain, gemeinsame Verwendung von Hardware und Domainkonnektivität zu erreichen. Diese Faktoren tragen zur Sicherheitsebene der Gesamtkonfiguration von Oracle VM Server for SPARC bei. Empfehlungen zum sicheren Deployment der Oracle VM Server for SPARC-Software finden Sie in „Sicherheit in einer virtualisierten Umgebung“ [15] und „Verteidigung vor Angriffen“ [17].

Sie können einige der folgenden allgemeinen Sicherheitsgrundlagen anwenden:

- **Minimieren der Angriffsfläche.**
  - Minimieren Sie versehentliche Konfigurationsfehler, indem Sie Betriebsrichtlinien erstellen, mit denen Sie die Sicherheit des Systems regelmäßig bewerten können. Weitere Informationen finden Sie in „Gegenmaßnahme: Erstellen von Betriebsrichtlinien“ [20].
  - Planen Sie die Architektur der virtuellen Umgebung sorgfältig, um die Domains bestmöglich zu isolieren. Hierzu wird auf die Gegenmaßnahmen für „Bedrohung: Fehler in der Architektur der virtuellen Umgebung“ [20] verwiesen.
  - Planen Sie sorgfältig, welche Ressourcen zugewiesen werden sollen und ob sie freigegeben werden sollen. Weitere Informationen finden Sie in „Gegenmaßnahme: Sorgfältige Zuweisung von Hardwareressourcen“ [23] und „Gegenmaßnahme: Sorgfältige Zuweisung von gemeinsam verwendeten Ressourcen“ [23].
  - Stellen Sie sicher, dass die logischen Domains vor Manipulation geschützt werden, indem Sie die Gegenmaßnahmen ergreifen, die für „Bedrohung: Manipulation der Ausführungsumgebung“ [24] und „Gegenmaßnahme: Sichern des Betriebssystems der Gastdomain“ [38] beschrieben werden.
    - „Gegenmaßnahme: Sichern interaktiver Zugriffspfade“ [25].
    - „Gegenmaßnahme: Minimieren von Oracle Solaris-BS“ [25].
    - „Gegenmaßnahme: Schützen von Oracle Solaris-BS“ [25].
    - „Gegenmaßnahme: Schützen von Logische Domains Manager“ [32].
    - „Gegenmaßnahme: Rollentrennung und Isolierung von Anwendungen“ [26] describes the importance of assigning functionality roles to the various domains and ensuring that the control domain runs software that provides the infrastructure that is required to host guest domains. Sie müssen Anwendungen, die von anderen Systemen ausgeführt werden können, auf Gastdomains ausführen, die dazu ausgelegt sind.

    - „Gegenmaßnahme: Konfigurieren eines dedizierten Verwaltungsnetzwerks“ [26] describes a more advanced network configuration that connects servers with SPs to a dedicated management network to shield the SP from network access.
- Machen Sie eine Gastdomain für das Netzwerk *nur* verfügbar, wenn dies erforderlich ist. Mit virtuellen Switches können Sie die Netzwerkkonnektivität einer Gastdomain *nur* auf die entsprechenden Netzwerke begrenzen.
- Führen Sie die Schritte zur Minimierung der Angriffsfläche für Oracle Solaris 10 und Oracle Solaris 11 wie in *Oracle Solaris 10 Security Guidelines* und *Oracle Solaris 11 Security Guidelines* beschrieben aus.
- Schützen Sie den Kern des Hypervisors wie in „Gegenmaßnahme: Validieren von Firmware- und Softwaresignaturen“ [29] und „Gegenmaßnahme: Validieren von Kernel-Modulen“ [30] beschrieben.
- Schützen Sie die Kontrolldomain vor Denial-of-Service-Angriffen. Weitere Informationen finden Sie in „Gegenmaßnahme: Sichern des Konsolenzugriffs“ [31].
- Stellen Sie sicher, dass der Logische Domains Manager nicht von nicht autorisierten Benutzern ausgeführt werden kann. Weitere Informationen finden Sie in „Bedrohung: Nicht autorisierte Verwendung von Konfigurationsdienstprogrammen“ [31].
- Stellen Sie sicher, dass nicht autorisierte Benutzer oder Prozesse nicht auf die Servicedomain zugreifen können. Weitere Informationen finden Sie in „Bedrohung: Manipulation einer Servicedomain“ [34].
- Schützen Sie eine I/O-Domain oder eine Servicedomain vor Denial-of-Service-Angriffen. Weitere Informationen finden Sie in „Bedrohung: Denial-of-Service bei einer I/O-Domain oder Servicedomain“ [36].
- Stellen Sie sicher, dass nicht autorisierte Benutzer oder Prozesse nicht auf eine I/O-Domain zugreifen können. Weitere Informationen finden Sie in „Bedrohung; Manipulation einer I/O-Domain“ [37].
- Deaktivieren Sie nicht benötigte Domain Manager-Services. Der Logische Domains Manager stellt Netzwerkservices für Zugriff, Überwachung und Migration von Domains bereit. Weitere Informationen finden Sie in „Gegenmaßnahme: Schützen von Logische Domains Manager“ [32] and „Gegenmaßnahme: Sichern des ILOM“ [28].
- **Niedrigste Berechtigung zur Ausführung eines Vorgangs erteilen.**
    - Isolieren Sie Systeme in *Sicherheitsklassen*, bei denen es sich um Gruppen von individuellen Gastsystemen handelt, für die die dieselben Sicherheitsanforderungen und Berechtigungen gelten. Indem Sie einer einzelnen Hardwareplattform nur Gastdomains aus einer einzelnen Sicherheitsklasse zuweisen, schaffen Sie eine Isolationsbarriere, die den Übergang von Domains in eine andere Sicherheitsklasse verhindert. Weitere Informationen finden Sie in „Gegenmaßnahme: Sorgfältige Zuweisung von Gastdomains für Hardwareplattformen“ [20].
    - Mit entsprechenden Rechten beschränken Sie die Möglichkeit zur Verwaltung von Domains mit dem Befehl `ldm`. *Nur* den Benutzern, die Domains verwalten müssen, sollte diese Möglichkeit gegeben werden. Weisen Sie Benutzern, die Zugriff auf alle `ldm`-Unterbefehle benötigen, eine Rolle zu, die das LDoms Management-Rechteprofil verwendet. Weisen Sie Benutzern, die nur Zugriff auf die

listenbezogenen `ldm`-Unterbefehle benötigen, eine Rolle zu, die das LDoms Review-Rechteprofil verwendet. Weitere Informationen finden Sie in „Using Rights Profiles and Roles“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

- Mit Berechtigungen begrenzen Sie den Zugriff auf die Konsole *nur* der Domains, die Sie, als Administrator von Oracle VM Server for SPARC, verwalten. Lassen Sie *keinen* allgemeinen Zugriff auf alle Domains zu. Weitere Informationen finden Sie in „Controlling Access to a Domain Console by Using Rights“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

Sicherheit in einer virtualisierten Umgebung

Um Ihre virtualisierte Oracle VM Server for SPARC-Umgebung wirksam zu schützen, sichern Sie das Betriebssystem und jeden Service, der in jeder Domain ausgeführt wird. Um die Auswirkungen einer erfolgreichen Sicherheitsverletzung zu reduzieren, trennen Sie Services, indem Sie sie in unterschiedlichen Domains bereitstellen.

Die Oracle VM Server for SPARC-Umgebung verwendet einen Hypervisor zur Virtualisierung von CPU-, Speicher- und I/O-Ressourcen für logische Domains. Jede Domain stellt einen diskreten virtualisierten Server dar, den Sie vor potenziellen Angriffen schützen müssen.

Mit einer virtualisierten Umgebung können Sie mehrere Server zu einem Server konsolidieren, indem Hardwareressourcen gemeinsam verwendet werden. In Oracle VM Server for SPARC werden CPU- und Speicherressourcen jeder Domain exklusiv zugeordnet, was einen Missbrauch durch übermäßige CPU-Auslastung oder Speicherzuordnung verhindert. Datenträger- und Netzwerkressourcen werden im Allgemeinen mehreren Gastdomains von Servicedomains bereitgestellt.

Bei der Bewertung der Sicherheit gehen Sie *immer* davon aus, dass Ihre Umgebung einen Schwachpunkt enthält, den ein Angreifer nutzen kann. Beispiel: Ein Angreifer könnte einen Schwachpunkt im Hypervisor nutzen, um die Kontrolle über das ganze System zu übernehmen, einschließlich seiner Gastdomains. Stellen Sie deshalb Systeme *immer* so bereit, dass das das Schadensrisiko bei einer Sicherheitsverletzung minimiert wird.

Ausführungsumgebung

Die Ausführungsumgebung umfasst folgende Komponenten:

- **Hypervisor –** Plattformspezifische Firmware, die Hardware virtualisiert und stark auf die Hardwareunterstützung baut, die in der CPU integriert ist.
- **Kontrolldomain –** Eine besondere Domain, die den Hypervisor konfiguriert und den Logische Domains Manager ausführt, der die logischen Domains verwaltet.
- **I/O-Domain oder Root-Domain –** Eine Domain, der einige oder alle auf der Plattform verfügbaren I/O-Geräte gehören, und die diese mit anderen Domains gemeinsam verwendet.

- **Servicedomain –** Eine Domain, die anderen Domains Services bereitstellt. Eine Domain kann anderen Domains Konsolenzugriff erteilen oder virtuelle Datenträger bereitstellen. Eine Servicedomain, die anderen Domains Zugriff auf virtuelle Datenträger erteilt, ist auch eine I/O-Domain.

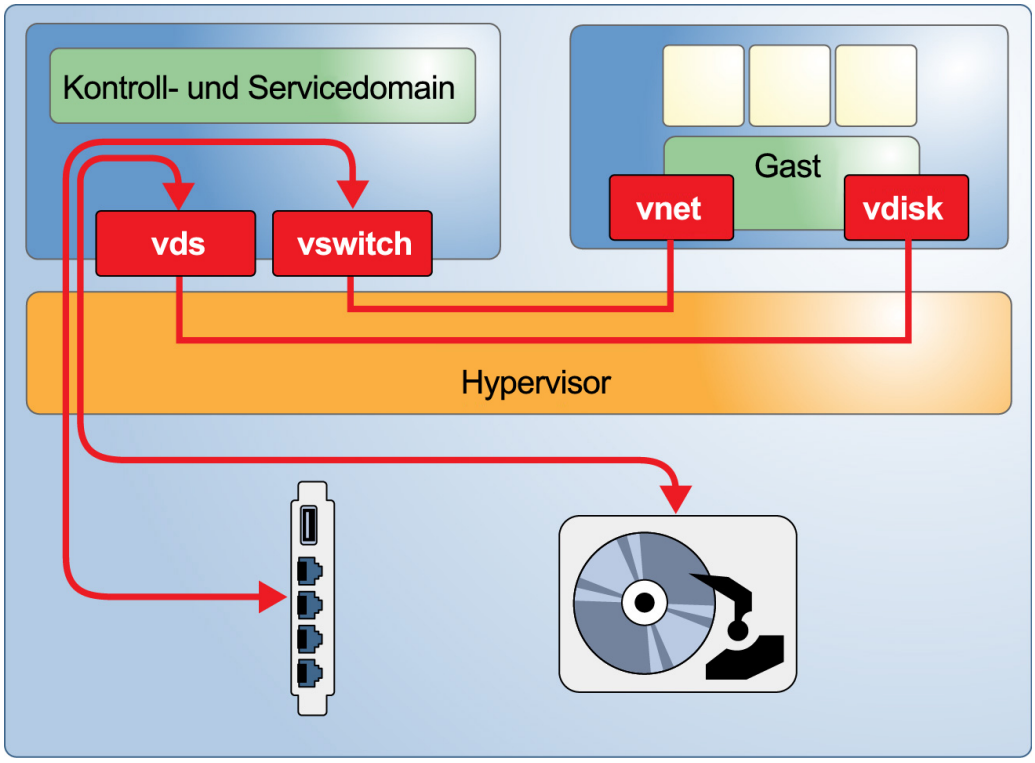
Weitere Informationen zu diesen Komponenten finden Sie in Abbildung 1-1, „Hypervisor, der zwei logische Domains unterstützt“ und den detaillierteren Komponentenbeschreibungen.

Sie können die Wartbarkeit von redundanten I/O-Konfigurationen verbessern, indem Sie eine zweite I/O-Domain konfigurieren. Sie können eine zweite I/O-Domain auch verwenden, um die Hardware vor Sicherheitsverletzungen zu bewahren. Weitere Informationen zu Konfigurationsoptionen finden Sie in *Oracle VM Server for SPARC 3.3 Administration Guide* .

Sichern der Ausführungsumgebung

Oracle VM Server for SPARC bietet verschiedene Angriffsziele in der Ausführungsumgebung. Abbildung 1-2, „Beispiel der Oracle VM Server for SPARC-Umgebung“ zeigt eine einfache Oracle VM Server for SPARC-Konfiguration, bei der die Kontrolldomain einer Gastdomain Netzwerk- und Datenträgerservices bereitstellt. Diese Services werden mit Daemons und Kernel-Modulen implementiert, die in der Kontrolldomain ausgeführt werden. Der Logische Domains Manager weist Logical Domain Channels (LDCs) für jeden Service und einen Client zu, um eine Punkt-zu-Punkt-Kommunikation zwischen diesen zu vereinfachen. Ein Angreifer könnte einen Fehler in einer der Komponenten nutzen, um die Isolation der Gastdomains zu durchbrechen. Beispiel: Ein Angreifer könnte beliebigen Code in der Servicedomain ausführen oder könnte normale Vorgänge auf der Plattform unterbrechen.

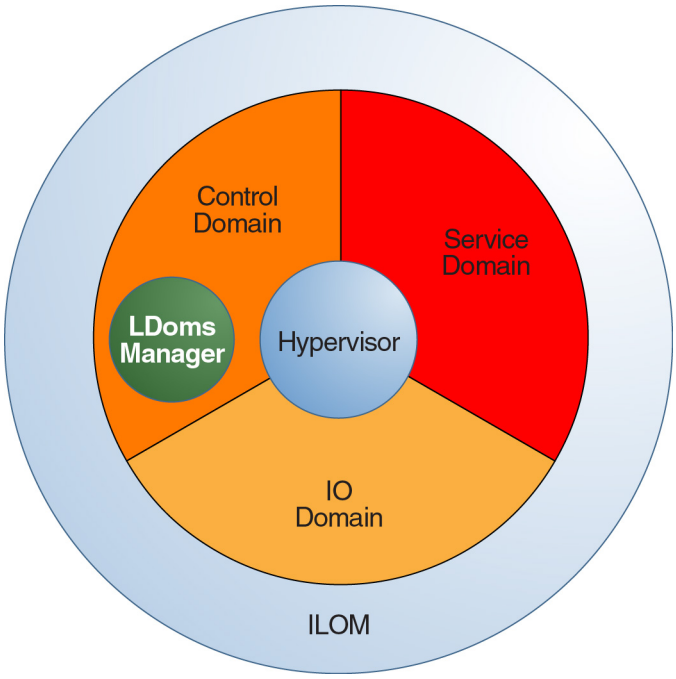
ABBILDUNG 1-2 Beispiel der Oracle VM Server for SPARC-Umgebung



Verteidigung vor Angriffen

In der folgenden Abbildung werden die Virtualisierungskomponenten dargestellt, aus denen die "Ausführungsumgebung" von Oracle VM Server for SPARC besteht. Diese Komponenten sind nicht streng getrennt. Bei der einfachsten Konfiguration werden diese Funktionen alle in einer einzelnen Domain zusammengefasst. Die Kontrolldomain kann auch als I/O-Domain und Servicedomain für die anderen Domains fungieren.

ABBILDUNG 1-3 Komponenten der Ausführungsumgebung



Angenommen, ein Angreifer versucht, die Systemisolation zu durchbrechen und danach den Hypervisor oder eine andere Komponente der Ausführungsumgebung zu manipulieren, um auf eine Gastdomain zuzugreifen. Sie müssen jede Gastdomain schützen wie jeden Standalone-Server.

Im weiteren Verlauf dieses Kapitels werden die Bedrohungsmöglichkeiten und die verschiedenen Gegenmaßnahmen beschrieben. Bei jedem dieser Angriffe wird versucht, die Isolation der verschiedenen Domains zu überwinden oder zu eliminieren, die auf einer einzelnen Plattform ausgeführt werden. In den folgenden Abschnitten werden die Bedrohungen für jeden Teil eines Oracle VM Server for SPARC-Systems beschrieben:

- „Betriebsumgebung“ [19]
- „Ausführungsumgebung“ [24]
- „ILOM“ [27]
- „Hypervisor“ [29]
- „Kontrolldomain“ [30]
- „Logische Domains Manager“ [31]
- „I/O-Domain“ [35]

- „Servicedomain“ [33]
- „Gastdomains“ [37]

Betriebsumgebung

Die Betriebsumgebung umfasst physische Systeme und deren Komponenten, Data Center-Architekten, Administratoren und Mitglieder der IT-Organisation. Eine Sicherheitsverletzung kann an jeder Stelle in der Betriebsumgebung auftreten.

Bei der Virtualisierung wird eine Softwareschicht zwischen der eigentlichen Hardware und den Gastdomains eingefügt, die die Production-Services ausführen, was die Komplexität erhöht. Deshalb müssen Sie das virtuelle System sorgfältig planen und konfigurieren und dabei die Möglichkeit menschlicher Fehler beachten. Außerdem müssen Sie sich dessen bewusst sein, dass Angreifer versuchen können, mit "Social Engineering" auf die Betriebsumgebung zuzugreifen.

In den folgenden Abschnitten werden die wichtigsten Bedrohungen beschrieben, denen Sie auf Betriebsumgebungsebene begegnen können.

Bedrohung: Unabsichtliche Fehlkonfiguration

Der wichtigste Sicherheitsaspekt bei einer virtuellen Umgebung besteht in der Aufrechterhaltung der Serverisolierung durch Trennung der Netzwerksegmente, Abgrenzung des administrativen Zugriffs und Deployment von Servern in Sicherheitsklassen, bei denen es sich um Gruppen von Domains handelt, die dieselben Sicherheitsanforderungen und Berechtigungen haben.

Konfigurieren Sie virtuelle Ressourcen sorgfältig, um folgende Fehler zu vermeiden:

- Erstellen unnötiger Kommunikationskanäle zwischen Production-Gastdomains und der Ausführungsumgebung
- Erstellen unnötiger Zugriffsmöglichkeiten auf Netzwerksegmente
- Erstellen unbeabsichtigter Verbindungen zwischen einzelnen Sicherheitsklassen
- Versehentliche Migration einer Gastdomain in die falsche Sicherheitsklasse
- Zuordnung nicht ausreichender Hardware, was zu unerwarteter Überlastung von Ressourcen führen kann
- Zuordnung von Datenträgern oder I/O-Geräten an die falsche Domain

Gegenmaßnahme: Erstellen von Betriebsrichtlinien

Als erstes definieren Sie die Betriebsrichtlinien für Ihre Oracle VM Server for SPARC-Umgebung sorgfältig. In diesen Richtlinien werden die folgenden Aufgaben beschrieben, die ausgeführt werden müssen und wie sie ausgeführt werden:

- Verwaltung von Patches für alle Komponenten der Umgebung
- Aktivierung der richtig definierten, nachvollziehbaren und sicheren Implementierung von Änderungen
- Prüfung von Logdateien in regelmäßigen Abständen
- Überwachung der Integrität und Verfügbarkeit der Umgebung

Führen Sie regelmäßig Kontrollen durch, um sicherzustellen, dass diese Richtlinien immer auf dem neuesten Stand und zutreffend sind, und um sicherzustellen, dass diese Richtlinien im täglichen Betrieb eingehalten werden.

Neben diesen Richtlinien können Sie verschiedene eher technische Maßnahmen ergreifen, um die Gefahr von versehentlichen Aktionen zu verringern. Weitere Informationen finden Sie in „Logische Domains Manager“ [31].

Bedrohung: Fehler in der Architektur der virtuellen Umgebung

Wenn Sie ein physisches System in eine virtuelle Umgebung verschieben, können Sie die Speicherkonfiguration im Allgemeinen unverändert belassen, indem Sie die ursprünglichen LUNs wieder verwenden. Die Netzwerkumgebung muss jedoch an die virtuelle Umgebung angepasst werden, und die sich daraus ergebende Architektur kann sich stark von der Architektur in dem physischen System unterscheiden.

Sie müssen überlegen, wie die Isolation der einzelnen Sicherheitsklassen und deren Anforderungen aufrechterhalten werden. Außerdem müssen Sie die gemeinsam verwendete Hardware der Plattform und der gemeinsam verwendeten Komponenten berücksichtigen, wie Netzwerkswitches und SAN-Switches.

Um die Sicherheit für Ihre Umgebung zu maximieren, muss die Isolation der Gastdomains und Sicherheitsklassen unbedingt aufrechterhalten werden. Beim Entwurf der Architektur rechnen Sie mit möglichen Fehlern und Angriffen und implementieren Sie eine Verteidigungslinie. Ein gutes Design begrenzt potenzielle Sicherheitsprobleme bei gleichzeitigem Komplexitäts- und Kostenmanagement.

Gegenmaßnahme: Sorgfältige Zuweisung von Gastdomains für Hardwareplattformen

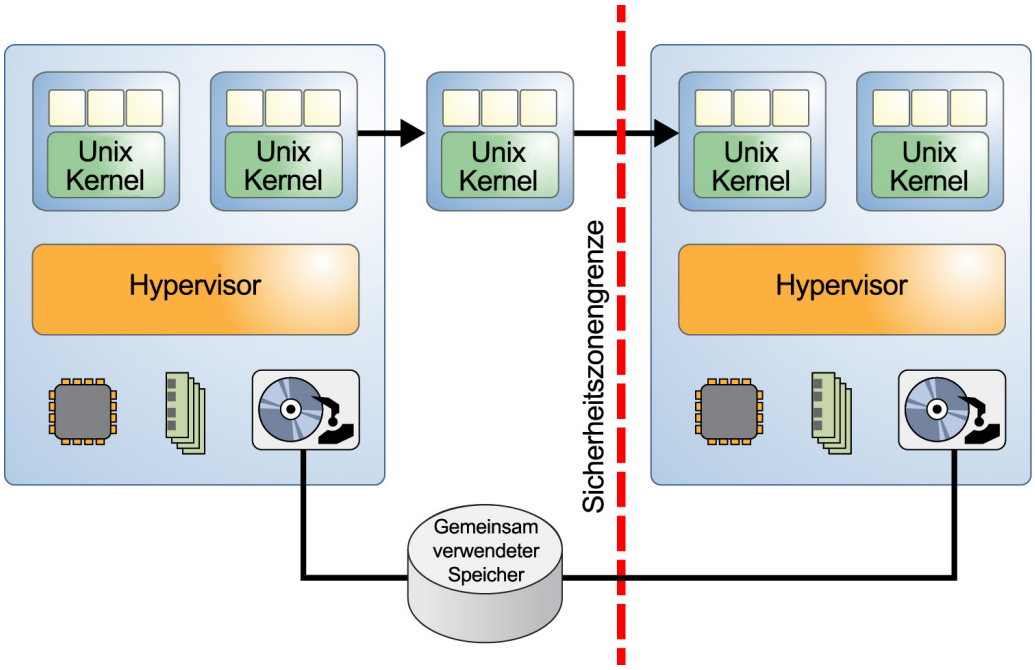
Verwenden Sie Sicherheitsklassen, d.h. Domaingruppen mit denselben Sicherheitsanforderungen und Berechtigungen, um einzelne Domains voneinander zu isolieren. Wenn Sie Gastdomains in derselben Sicherheitsklasse einer bestimmten Hardwareplattform

zuweisen, verhindert selbst eine Verletzung der Isolation, dass ein Angriff auf eine andere Sicherheitsklasse übergreift.

Gegenmaßnahme: Planen einer Oracle VM Server for SPARC-Domainmigration

Das Feature der Livedomainmigration hat das Potenzial, die Isolation zu durchbrechen, wenn eine Gastdomain versehentlich zu einer Plattform migriert wird, die einer anderen Sicherheitsklasse zugewiesen ist, wie in der folgenden Abbildung dargestellt. Deshalb planen Sie die Migration einer Gastdomain sorgfältig, um sicherzustellen, dass eine Migration über Grenzen der Sicherheitsklasse hinaus nicht zulässig ist.

ABBILDUNG 1-4 Domainmigration über Sicherheitsgrenzen hinweg



Um das Sicherheitsrisiko zu minimieren oder zu reduzieren, das der Migrationsvorgang birgt, müssen Sie `ldmd`-generierte Hostzertifikate Out-of-band zwischen jedem Quell- und Zielrechnerpaar austauschen und installieren. Informationen zur Einrichtung der SSL-Zertifikate finden Sie in „Configuring SSL Certificates for Migration“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

Gegenmaßnahme: Korrekte Konfiguration der virtuellen Verbindungen

Wenn der Überblick über alle virtuellen Netzwerkverbindungen verloren geht, kann eine Domain fälschlicherweise Zugriff auf ein Netzwerksegment erhalten. Beispiel: Ein derartiger Zugriff könnte die Firewall oder eine Sicherheitsklasse umgehen.

Um die Gefahr von Implementierungsfehlern zu verringern, planen und dokumentieren Sie alle virtuellen und physischen Verbindungen in Ihrer Umgebung sorgfältig. Optimieren Sie den Domainverbindungsplan im Hinblick auf Einfachheit und Verwaltbarkeit. Dokumentieren Sie Ihren Plan klar, und vergleichen Sie anhand des Plans, ob die Implementierung korrekt ist, bevor Sie den Production-Betrieb aufnehmen. Selbst nachdem die virtuelle Umgebung in Betrieb ist, prüfen Sie die Implementierung in regelmäßigen Abständen anhand des Plans.

Gegenmaßnahme: Verwenden von VLAN-Tagging

Mit VLAN-Tagging können Sie verschiedene Ethernet-Segmente in einem einzelnen physischen Netzwerk konsolidieren. Dieses Feature ist auch für virtuelle Switches verfügbar. Um die Risiken von Softwarefehlern bei der Implementierung von virtuellen Switches zu mindern, konfigurieren Sie einen virtuellen Switch pro physischer NIC und pro VLAN. Als weiteren Schutz vor Fehlern im Ethernet-Treiber vermeiden Sie die Verwendung von markierten VLANs. Die Wahrscheinlichkeit derartiger Fehler ist jedoch gering, weil diese Sicherheitslücke wegen markierter VLANs bekannt ist. Angriffserkennungstest in der Sun SPARC T-Series-Plattform von Oracle mit der Oracle VM Server for SPARC-Software haben diese Sicherheitslücke nicht aufgezeigt.

Gegenmaßnahme: Verwenden von virtuellen Sicherheits-Appliances

Sicherheits-Appliances wie Paketfilter und Firewalls sind Isolationsinstrumente und schützen die Isolation von Sicherheitsklassen. Diese Appliances unterliegen denselben Bedrohungen wie jede andere Gastdomain, deren Verwendung garantiert also keinen vollständigen Schutz vor einer Verletzung der Isolation. Beachten Sie deshalb alle Risiko- und Sicherheitsfaktoren, bevor Sie sich für die Virtualisierung eines derartigen Service entscheiden.

Bedrohung: Nebenwirkungen der gemeinsamen Verwendung von Ressourcen

Die gemeinsame Verwendung von Ressourcen in einer virtualisierten Umgebung kann zu Denial-of-Service-(DoS-)Angriffen führen, die eine Ressource überlasten, bis sich dies negativ auf andere Komponenten auswirkt, wie eine andere Domain.

In einer Oracle VM Server for SPARC-Umgebung sind möglicherweise nur einige Ressourcen von einem DoS-Angriff betroffen. CPU- und Speicherressourcen werden jeder Gastdomain

exklusiv zugewiesen, was die meisten DoS-Angriffe verhindert. Selbst die exklusive Zuweisung dieser Ressourcen kann die Gastdomain auf folgende Weise verlangsamen:

- Überlastung der Cachebereiche, die zwischen Hardwarethreads gemeinsam verwendet werden und zwei Gastdomains zugewiesen sind.
- Überlastung der Speicherbandbreite

Im Gegensatz zu CPU- und Speicherressourcen werden Datenträger- und Netzwerkservices im Allgemeinen zwischen Gastdomains gemeinsam verwendet. Diese Services werden den Gastdomains von mindestens einer Servicedomain bereitgestellt. Erwägen Sie sorgfältig, wie Sie diese Ressourcen Gastdomains zuweisen und zwischen diesen verteilen. Jede Konfiguration, die maximale Performance und Ressourcenauslastung zulässt, minimiert gleichzeitig das Risiko von Nebenwirkungen.

Bewertung: Nebenwirkungen durch gemeinsam verwendete Ressourcen

Ein Netzwerklink kann gesättigt oder ein Datenträger kann überlastet werden, unabhängig davon, ob er einer Domain exklusiv zugewiesen ist oder zwischen Domains gemeinsam verwendet wird. Diese Angriffe wirken sich auf die Verfügbarkeit eines Service während der Dauer des Angriffs aus. Das Ziel des Angriffs ist nicht gefährdet und es gehen keine Daten verloren. Sie können die Auswirkungen dieser Bedrohung einfach minimieren, sollten sich ihrer jedoch bewusst sein, selbst wenn sie auf Netzwerk- und Datenträgerressourcen in Oracle VM Server for SPARC begrenzt ist.

Gegenmaßnahme: Sorgfältige Zuweisung von Hardwareressourcen

Stellen Sie sicher, dass Sie Gastdomains nur erforderliche Hardwareressourcen zuweisen. Heben Sie die Zuweisung einer nicht verwendeten Ressource auf, wenn diese nicht mehr benötigt wird; Beispiel: Ein Netzwerkport oder DVD-Laufwerk, das nur während einer Installation benötigt wird. Mit dieser Vorgehensweise minimieren Sie die Anzahl von möglichen Einstiegspunkten für einen Angreifer.

Gegenmaßnahme: Sorgfältige Zuweisung von gemeinsam verwendeten Ressourcen

Gemeinsam verwendete Hardwareressourcen, wie physische Netzwerkports, bieten ein mögliches Ziel für DoS-Angriffe. Um die Auswirkungen von DoS-Angriffen auf eine einzelne Gruppe von Gastdomains zu begrenzen, legen Sie sorgfältig fest, welche Gastdomains welche Hardwareressourcen gemeinsam verwenden.

Beispiel: Gastdomains, die Hardwareressourcen gemeinsam verwenden, könnten nach denselben Verfügbarkeits- oder Sicherheitsanforderungen gruppiert werden. Über die Gruppierung hinaus können Sie verschiedene Arten von Ressourcenkontrollen anwenden.

Beachten Sie, wie Datenträger- und Netzwerkressourcen gemeinsam verwendet werden. Sie können Probleme vermindern, indem Sie den Datenträgerzugriff über dedizierte physische Zugriffspfade oder über dedizierte virtuelle Datenträgerservices trennen.

Überblick: Nebenwirkungen durch gemeinsam verwendete Ressourcen

Alle in diesem Abschnitt beschriebenen Gegenmaßnahmen setzen voraus, dass Sie die technischen Details Ihres Deployments und dessen Auswirkungen auf die Sicherheit verstehen. Planen Sie sorgfältig, dokumentieren Sie gut, und halten Sie Ihre Architektur so einfach wie möglich. Sie müssen sich der Auswirkungen der virtualisierten Hardware bewusst sein, damit Sie ein sicheres Deployment der Oracle VM Server for SPARC-Software vorbereiten können.

Logische Domains halten den Auswirkungen der gemeinsamen Verwendung von CPUs und Speicher stand, da die tatsächliche gemeinsame Verwendung gering ist. Dennoch sollten immer Ressourcenkontrollen wie Solaris-Ressourcenmanagement innerhalb der Gastdomains angewendet werden. Diese Kontrollen bieten einen Schutz vor fehlerhaftem Anwendungsverhalten bei einer virtuellen oder nicht virtualisierten Umgebung,

Ausführungsumgebung

Abbildung 1-3, „Komponenten der Ausführungsumgebung“ stellt die Komponenten der Ausführungsumgebung dar. Jede Komponente enthält bestimmte Services, die gemeinsam die Gesamtplattform bilden, auf der die Production-Gastdomains ausgeführt werden. Die ordnungsgemäße Konfiguration der Komponenten ist von wesentlicher Bedeutung für die Integrität des Systems.

Alle Komponenten der Ausführungsumgebung sind potenzielle Ziele für Angreifer. In diesem Abschnitt werden die Bedrohungen aufgeführt, die jede Komponente in der Ausführungsumgebung betreffen könnten. Einige Bedrohungen und Gegenmaßnahmen könnten für mehr als eine Komponente zutreffen.

Bedrohung: Manipulation der Ausführungsumgebung

Durch Manipulation der Ausführungsumgebung können Sie auf verschiedene Weise Kontrolle über die Umgebung erhalten. Beispiel: Sie könnten manipulierte Firmware in der ILOM installieren, um die gesamte I/O der Gastdomain innerhalb einer I/O-Domain zu überwachen. Ein solcher Angriff kann auf die Konfiguration des Systems zugreifen und diese ändern. Ein Angreifer, der die Kontrolle über die Oracle VM Server for SPARC-Kontrolldomain übernimmt, kann das System beliebig neu konfigurieren; ein Angreifer, der die Kontrolle über eine I/O-Domain übernimmt, kann Änderungen an dem zugeordneten Speicher, wie beispielsweise Bootdatenträgern, übernehmen.

Bewertung: Manipulation der Ausführungsumgebung

Ein Angreifer, der erfolgreich in den ILOM oder eine Domain in der Ausführungsumgebung eindringt, kann alle Daten lesen und manipulieren, die in dieser Domain verfügbar sind. Dieser Zugriff kann über das Netzwerk oder über einen Fehler im Virtualisierungsstack erfolgen. Ein solcher Angriff ist schwierig durchzuführen, weil der ILOM und die Domains im Allgemeinen nicht direkt angegriffen werden können.

Die Gegenmaßnahmen zum Schutz vor Manipulation der Ausführungsumgebung sind Standardsicherheitsmaßnahmen, die in jedem System implementiert sein sollten. Standardsicherheitsmaßnahmen bieten eine zusätzliche Schutzschicht um die Ausführungsumgebung, die das Risiko von Eindringen und Manipulation weiter verringern.

Gegenmaßnahme: Sichern interaktiver Zugriffspfade

Stellen Sie sicher, dass Sie *nur* Konten erstellen, die für die Anwendungen erforderlich sind, die auf dem System ausgeführt werden.

Stellen Sie sicher, dass Konten, die zur Administration erforderlich sind, entweder durch schlüsselbasierte Authentifizierung oder sichere Kennwörter gesichert werden. Diese Schlüssel oder Kennwörter dürfen nicht von verschiedenen Domains gemeinsam verwendet werden. Außerdem sollten Sie die Implementierung einer zweistufigen Authentifizierung oder eine "Vier-Augen-Regel" zur Ausführung bestimmter Aktionen in Erwägung ziehen.

Verwenden Sie *keine* anonymen Anmeldungen für Konten wie `root`, um sicherzustellen, dass Sie die volle Rückverfolgbarkeit und Verantwortung für die auf dem System ausgeführten Befehle haben. Verwenden Sie stattdessen Rechte, mit denen Sie einzelnen Administratoren *nur* Zugriff auf die Funktionen erteilen, zu deren Ausführung diese berechtigt sind. Stellen Sie sicher, dass der Netzwerkzugriff zu Administrationszwecken immer eine Verschlüsselung wie SSH verwendet, und dass die Workstation des Administrators als Hochsicherheitssystem behandelt wird.

Gegenmaßnahme: Minimieren von Oracle Solaris-BS

Jede auf einem System installierte Software kann gefährdet werden; installieren Sie deshalb *nur* die erforderliche Software, um das Fenster für Sicherheitsverletzungen zu minimieren.

Gegenmaßnahme: Schützen von Oracle Solaris-BS

Neben der Installation eines minimierten Oracle Solaris-BS konfigurieren Sie Softwarepakete so, dass die Software vor Angriffen geschützt ist. Als erstes führen Sie begrenzte Netzwerkservices aus, um alle Netzwerkservices mit Ausnahme von SSH zu deaktivieren.

Diese Richtlinie ist das Standardverhalten auf Oracle Solaris 11-Systemen. Weitere Informationen zur Sicherung des Oracle Solaris-BS finden Sie in *Oracle Solaris 10 Security Guidelines* und *Oracle Solaris 11 Security Guidelines* .

Gegenmaßnahme: Rollentrennung und Isolierung von Anwendungen

Production-Anwendungen sind notwendigerweise mit anderen Systemen verbunden und somit eher externen Angriffen ausgesetzt. Stellen Sie *keine* Production-Anwendungen in einer Domain bereit, die Bestandteil der Ausführungsumgebung ist. Stellen Sie diese stattdessen *nur* für Gastdomains bereit, die keine weiteren Berechtigungen haben.

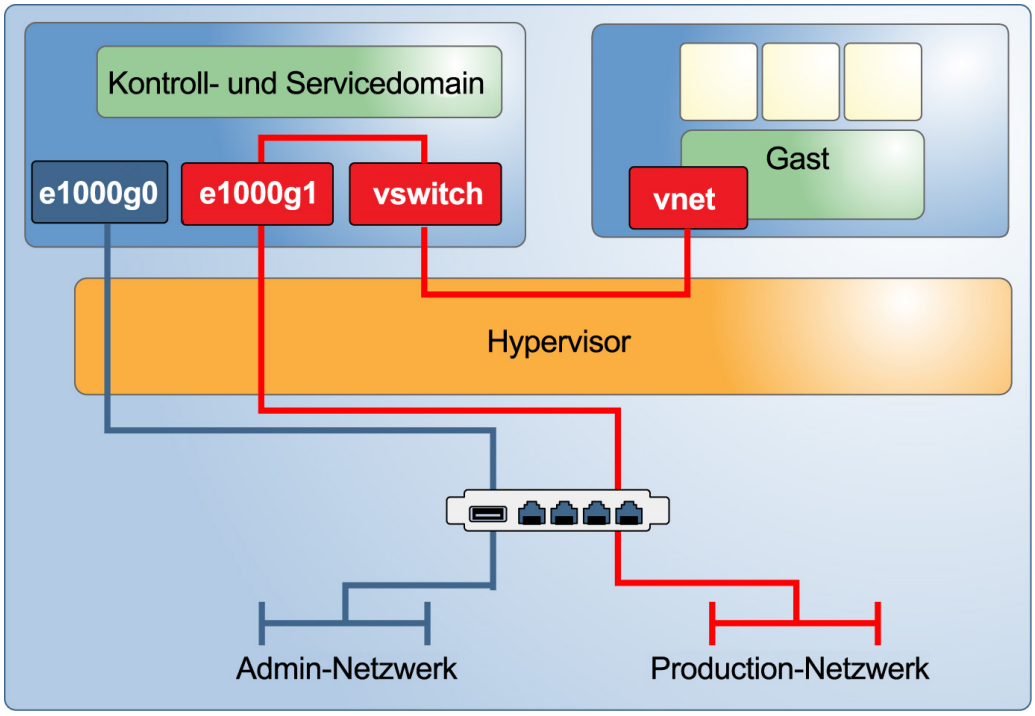
Die Ausführungsumgebung soll nur die erforderliche Infrastruktur für diese Gastdomains bereitstellen. Durch die Trennung der Ausführungsumgebung von den Production-Anwendungen können Sie Granularität in Administrationsberechtigungen implementieren. Der Administrator einer Production-Gastdomain benötigt keinen Zugriff auf die Ausführungsumgebung und der Administrator einer Ausführungsumgebung benötigt keinen Zugriff auf die Production-Gastdomains. Wenn möglich weisen Sie die verschiedenen Rollen der Ausführungsumgebung, wie der Kontroll- und I/O-Domain, unterschiedlichen Domains zu. Durch diese Art der Konfiguration wird der Schaden begrenzt, der entstehen kann, wenn eine dieser Domains gefährdet wird.

Sie können die Rollentrennung auch auf die Netzwerkumgebung erweitern, mit der die Verbindung zu verschiedenen Servern hergestellt wird.

Gegenmaßnahme: Konfigurieren eines dedizierten Verwaltungsnetzwerks

Verbinden Sie alle Server, die mit Serviceprozessoren (SPs) ausgestattet sind, mit einem dedizierten Verwaltungsnetzwerk. Diese Konfiguration wird auch für die Domains der Ausführungsumgebung empfohlen. Wenn sie überhaupt über ein Netzwerk verbunden sind, hosten Sie diese Domains in ihrem eigenen dedizierten Netzwerk. Verbinden Sie die Domains der Ausführungsumgebung *nicht* direkt mit Netzwerken, die Production-Domains zugewiesen sind. Sie können zwar alle administrativen Aufgaben über die einzelne Konsolverbindung ausführen, die von dem ILOM-SP zur Verfügung gestellt wird, diese Konfiguration macht jedoch die Verwaltung so mühsam, dass sie nicht praktikabel ist. Durch Trennung der Production- und Administrationsnetzwerke schützen Sie das System vor Lauschangriffen und Manipulation. Diese Art der Trennung verhindert auch Angriffe von Gastdomains auf die Ausführungsumgebung über das gemeinsame Netzwerk.

ABBILDUNG 1-5 Dediziertes Verwaltungsnetzwerk



ILOM

Alle aktuellen Oracle SPARC-Systeme umfassen einen integrierten Systemcontroller (ILOM), der folgende Funktionen hat:

- Verwaltung grundlegender Umgebungsüberwachungselemente, wie Lüftergeschwindigkeit und Stromversorgung des Gehäuses.
- Aktivierung von Firmwareupgrades
- Bereitstellung der Systemkonsole für die Kontrolldomain

Sie können auf den ILOM über eine serielle Verbindung zugreifen oder können SSH, HTTP, HTTPS, SNMP oder IPMI für den Zugriff über einen Netzwerkport verwenden. Die Fujitsu M10-Server verwenden XSCF anstelle von ILOM zur Ausführung ähnlicher Funktionen.

Bedrohung: Vollständiges Denial-of-Service des Systems

Ein Angreifer, der Kontrolle über den ILOM erhält, kann das System auf unterschiedliche Weise gefährden, einschließlich:

- Unterbrechung der Stromzufuhr für alle ausgeführten Gastdomains
- Installieren von manipulierter Firmware, um Zugriff auf mindestens eine Gastdomain zu erhalten

Diese Szenarios gelten für jedes System, das ein derartiges Controllergerät enthält. In einer virtualisierten Umgebung kann der Schaden wesentlich größer sein als in einer physischen Umgebung, weil viele Domains, die sich in demselben Systemgehäuse befinden, in Gefahr sind.

Gleichermaßen kann ein Angreifer, der Kontrolle über die Kontrolldomain oder eine I/O-Domain erhält, jederzeit alle abhängigen Gastdomains deaktivieren, indem er die entsprechenden I/O-Services herunterfährt.

Bewertung: Vollständiges Denial-of-Service des Systems

Während der ILOM im Allgemeinen mit einem administrativen Netzwerk verbunden ist, können Sie auch aus der Kontrolldomain auf den ILOM zugreifen, indem Sie IPMI mit dem BMC-Zugriffsmodul verwenden. Deshalb müssen diese beiden Verbindungstypen gut geschützt und von den normalen Production-Netzwerken isoliert werden.

Gleichermaßen kann ein Angreifer eine Servicedomain aus dem Netzwerk oder über einen Fehler in dem Virtualisierungsstack verletzen und dann die Gast-I/O blockieren oder ein System herunterfahren. Der Schaden ist zwar begrenzt, weil Daten weder verloren gehen noch gefährdet werden, kann sich jedoch auf eine große Anzahl von Gastdomains auswirken. Deshalb müssen Sie sich vor der Wahrscheinlichkeit dieser Bedrohung schützen, um einen potenziellen Schaden zu begrenzen.

Gegenmaßnahme: Sichern des ILOM

Als Systemserviceprozessor kontrolliert der ILOM kritische Funktionen wie Stromversorgung des Gehäuses, Konfigurationen für das Hochfahren von Oracle VM Server for SPARC und Konsolenzugriff auf die Kontrolldomain. Mit folgenden Maßnahmen können Sie den ILOM sichern:

- Setzen Sie den Netzwerkport des ILOM in ein Netzwerksegment, das von dem administrativen Netzwerk getrennt ist, das für die Domains in der Ausführungsumgebung verwendet wird.
- Für den Vorgang ist die Deaktivierung aller Services nicht erforderlich, wie HTTP, IPMI, SNMP, HTTPS und SSH.
- Konfigurieren dedizierter und persönlicher Administratorkonten, die nur die erforderlichen Rechte erteilen. Um die Verantwortung für die von Administratoren ausgeführten Aktionen

zu maximieren, müssen Sie persönliche Administratorkonten erstellen. Dieser Zugriffstyp ist besonders für Konsolenzugriff, Firmwareupgrades und Verwaltung von Startup-Konfigurationen wichtig.

Hypervisor

Der Hypervisor ist die Firmwareschicht, die die Virtualisierung der eigentlichen Hardware implementiert und kontrolliert. Der Hypervisor umfasst folgende Komponenten:

- Eigentlicher Hypervisor, der in Firmware implementiert ist und von den CPUs des Systems unterstützt wird.
- Firmwaremodule, die in der Kontrolldomain zur Konfiguration des Hypervisors ausgeführt werden.
- Kernel-Module und Daemons, die in I/O-Domains und Servicedomains ausgeführt werden, um virtualisierte I/O zu ermöglichen, sowie die Kernel-Module, die über Logical Domain Channels (LDCs) kommunizieren.
- Kernel-Module und Gerätetreiber, die in den Gastdomains ausgeführt werden, um auf virtualisierte I/O-Geräte zuzugreifen, sowie die Kernel-Module, die über LDCs kommunizieren.

Bedrohung: Durchbrechen der Isolation

Ein Angreifer kann die Kontrolle über Gastdomains oder das ganze System übernehmen, indem die isolierte Laufzeitumgebung durchbrochen wird, die vom Hypervisor bereitgestellt wird. Potenziell kann diese Bedrohung dem System den größten Schaden zufügen.

Bewertung: Durchbrechen der Isolation

Ein modularer Systementwurf kann die Isolation verbessern, indem Gastdomains, dem Hypervisor und der Kontrolldomain verschiedene Berechtigungsebenen erteilt werden. Jedes funktionale Modul wird in einem separaten und konfigurierbaren Kernel-Modul, Gerätetreiber oder Daemon implementiert. Diese Modularität erfordert saubere APIs und einfache Kommunikationsprotokolle, um das Gesamtfehlerrisiko zu verringern.

Selbst wenn der Missbrauch eines Fehlers unwahrscheinlich erscheint, kann ein potenzieller Schaden dem Angreifer die Möglichkeit geben, das ganze System zu kontrollieren.

Gegenmaßnahme: Validieren von Firmware- und Softwaresignaturen

Obwohl Sie die Systemfirmware und BS-Patches direkt von einer Oracle-Website herunterladen können, können diese Patches manipuliert sein. Bevor Sie die Software installieren, müssen

Sie die MD5-Prüfsummen der Softwarepakete prüfen. Die Prüfsummen aller herunterladbarer Softwarepakete werden von Oracle veröffentlicht.

Gegenmaßnahme: Validieren von Kernel-Modulen

Oracle VM Server for SPARC verwendet verschiedene Treiber und Kernel-Module zur Implementierung des gesamten Virtualisierungssystems. Alle Kernel-Module und die meisten Binärdateien, die mit dem Oracle Solaris-BS verteilt werden, haben eine digitale Signatur. Mit dem `elfsign`-Dienstprogramm prüfen Sie die digitale Signatur für jedes Kernel-Modul und jeden Treiber. Mit dem Oracle Solaris 11 `pkg verify`-Befehl können Sie die Integrität der Oracle Solaris-Binärdatei prüfen. Siehe auch `https://blogs.oracle.com/cmt/entry/solaris_fingerprint_database_how_it`

Als erstes müssen Sie die Integrität des `elfsign`-Dienstprogramms festlegen. Mit dem Basis-Audit- und Reporting-Tool (BART) können Sie die Prüfung der digitalen Signatur automatisieren. In Integrating BART and the Solaris Fingerprint Database in the Solaris 10 Operating System (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-005-bart-solaris-fp-db-276999.pdf`) wird beschrieben, wie Sie BART und die Solaris Fingerprint-Datenbank kombinieren, um ähnliche Integritätsprüfungen automatisch durchzuführen. Auch wenn die Fingerprint-Datenbank nicht mehr fortgeführt wird, können die in diesem Dokument beschriebenen Grundlagen noch zur Verwendung von `elfsign` und BART auf ähnliche Weise übernommen werden.

Kontrolldomain

Die Kontrolldomain, die häufig die Rolle einer I/O-Domain und einer Servicedomain hat, muss gesichert werden, da sie die Konfiguration des Hypervisors ändern kann, der alle zugeordneten Hardwareressourcen kontrolliert.

Bedrohung: Denial-of-Service bei der Kontrolldomain

Das Herunterfahren der Kontrolldomain kann zu einem Denial-of-Service der Konfigurationstools führen. Weil die Kontrolldomain nur für Konfigurationsänderungen benötigt wird, sind die Gastdomains nicht betroffen, wenn sie über andere Servicedomains auf ihre Netzwerk- und Datenträgerressourcen zugreifen.

Bewertung: Denial-of-Service bei der Kontrolldomain

Wenn die Kontrolldomain über das Netzwerk angegriffen wird, ist dies gleichbedeutend mit dem Angriff auf eine andere ordnungsgemäß geschützte Oracle Solaris-BS-Instanz. Der

Schaden durch das Herunterfahren oder ähnliches Denial-of-Service der Kontrolldomain ist relativ gering. Gastdomains sind jedoch betroffen, wenn die Kontrolldomain auch als Servicedomain für diese Gastdomains fungiert.

Gegenmaßnahme: Sichern des Konsolenzugriffs

Vermeiden Sie die Konfiguration des Zugriffs des administrativen Netzwerks auf die Domains der Ausführungsumgebung. Bei diesem Szenario müssen Sie den ILOM-Konsolenservice für die Kontrolldomain verwenden, um alle Administrationsaufgaben auszuführen. Der Konsolenzugriff zu allen anderen Domains ist weiter mit dem `vntsd`-Service möglich, der in der Kontrolldomain ausgeführt wird.

Überdenken Sie die Verwendung dieser Option sorgfältig. Auch wenn diese Option das Risiko eines Angriffs über das administrative Netzwerk reduziert, kann immer nur ein Administrator gleichzeitig auf die Konsole zugreifen.

Weitere Informationen zur sicheren Konfiguration von `vntsd` finden Sie in „How to Enable the Virtual Network Terminal Server Daemon“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

Logische Domains Manager

Der Logische Domains Manager wird in der Kontrolldomain ausgeführt und wird zur Konfiguration des Hypervisors verwendet; außerdem werden mit ihm alle Domains und deren Hardwareressourcen erstellt und konfiguriert. Stellen Sie sicher, dass Logische Domains Manager protokolliert und überwacht wird.

Bedrohung: Nicht autorisierte Verwendung von Konfigurationsdienstprogrammen

Ein Angreifer kann Kontrolle über die Benutzer-ID eines Administrators übernehmen oder ein Administrator aus einer anderen Gruppe kann nicht autorisierten Zugriff auf ein anderes System erhalten.

Bewertung: Nicht autorisierte Verwendung von Konfigurationsdienstprogrammen

Stellen Sie sicher, dass ein Administrator keinen nicht erforderlichen Zugriff auf ein System erhält, indem Sie durchdachtes Identitätsmanagement implementieren. Implementieren Sie außerdem eine strikte, feingranulierte Zugriffskontrolle und andere Maßnahmen, wie die Vier-Augen-Regel.

Gegenmaßnahme: Anwenden der Vier-Augen-Regel

Sie sollten die Implementierung einer Vier-Augen-Regel für Logische Domains Manager und andere administrative Tools durch Verwendung von Rechten in Erwägung ziehen. Enforcing a Two Man Rule Using Solaris 10 RBAC (`https://blogs.oracle.com/gbrunett/entry/enforcing_a_two_man_rule`). Diese Regel schützt vor Social Engineering-Angriffen, gefährdeten administrativen Konten und menschlichen Fehlern.

Gegenmaßnahme: Verwenden von Rechten für Logische Domains Manager

Durch Verwendung von Rechten für den `ldm`-Befehl können Sie feingranulierte Zugriffskontrolle implementieren und vollständige Rückverfolgung aufrechterhalten. Weitere Informationen zur Konfiguration von Rechten finden Sie in *Oracle VM Server for SPARC 3.3 Administration Guide* . Die Verwendung von Rechten schützt vor menschlichen Fehlern, weil nicht alle Funktionen des Befehls `ldm` für alle Administratoren verfügbar sind.

Gegenmaßnahme: Schützen von Logische Domains Manager

Deaktivieren Sie nicht benötigte Domain Manager-Services. Der Logische Domains Manager stellt Netzwerkservices für Zugriff, Überwachung und Migration von Domains bereit. Die Deaktivierung von Netzwerkservices reduziert die Angriffsfläche von Logische Domains Manager auf das Mindestmaß, das für den normalen Betrieb erforderlich ist. Dieses Szenario kontert Denial-of-Service-Angriffe und andere Versuche, diese Netzwerkservices zu missbrauchen.

Anmerkung - Durch Deaktivierung der Domainmanagerservices können Sie zwar die Angriffsfläche minimieren, es können jedoch nicht alle Nebenwirkungen dieser Aktion auf eine bestimmte Konfiguration vorhergesagt werden.

Deaktivieren Sie folgende Netzwerkservices, wenn sie nicht verwendet werden:

- Migrationsservice an TCP-Port `8101`

  Zur Deaktivierung dieses Service wird auf die Beschreibung der `ldmd/incoming_migration_enabled`- und `ldmd/outgoing_migration_enabled`-Eigenschaften in der Manpage `ldmd`(1M) verwiesen.
- Unterstützung von Extensible Messaging and Presence Protocol (XMPP) an TCP-Port `6482`

  Weitere Informationen zur Deaktivierung dieses Service finden Sie in „XML Transport“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

  Die Deaktivierung von XMPP verhindert die Ausführung einiger Verwaltungstools und Schlüsselfunktionen von Oracle VM Server for SPARC. Weitere Informationen finden Sie in „Oracle VM Server for SPARC-XML-Oberfläche“ [41].
- Simple Network Management Protocol (SNMP) an UDP-Port `161`

Prüfen Sie, ob Sie die Oracle VM Server for SPARC Management Information Base (MIB) zur Beobachtung von Domains verwenden möchten. Diese Funktion erfordert, dass der SNMP-Service aktiviert ist. Je nach Auswahl gehen Sie folgendermaßen vor:

- **Aktivieren Sie den SNMP-Service, um die Oracle VM Server for SPARC MIB zu verwenden.** Nehmen Sie eine sichere Installation der Oracle VM Server for SPARC MIB vor. Weitere Informationen finden Sie in „How to Install the Oracle VM Server for SPARC MIB Software Package“ in *Oracle VM Server for SPARC 3.3 Administration Guide* und „Managing Security“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .
- **Deaktivieren Sie den SNMP-Service.** Weitere Informationen zur Deaktivierung dieses Service finden Sie in „How to Remove the Oracle VM Server for SPARC MIB Software Package“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

- Discovery-Service an Multicast-Adresse `239.129.9.27` und Port `64535`

Anmerkung - Dieses Discovery-Verfahren wird auch von dem `ldmd`-Daemon zur Ermittlung von Konflikten bei der automatischen Zuweisung von MAC-Adressen verwendet. Wenn Sie den Discovery-Service deaktivieren, funktioniert die Erkennung von MAC-Adresskonflikten nicht. Somit funktioniert auch die automatische MAC-Adresszuordnung nicht ordnungsgemäß.

Sie können diesen Service *nicht* deaktivieren, während der Logische Domains Manager Daemon, `ldmd`, ausgeführt wird. Verwenden Sie stattdessen die IP-Filterfunktion von Oracle Solaris, um den Zugriff auf diesen Service zu blockieren, wodurch die Angriffsfläche von Logische Domains Manager minimiert wird. Durch die Blockierung des Zugriffs wird die nicht autorisierte Verwendung des Dienstprogramms verhindert, wodurch Denial-of-Service-Angriffe und andere Versuche zum Missbrauch dieser Netzwerkzugriffe gekontert werden. Weitere Informationen finden Sie in Kapitel 20, „IP Filter in Oracle Solaris (Overview)“ in *Oracle Solaris Administration: IP Services* und „Using IP Filter Rule Sets“ in *Oracle Solaris Administration: IP Services* .

Weitere Informationen finden Sie auch in „Gegenmaßnahme: Sichern des ILOM“ [28].

Servicedomain

Eine Servicedomain stellt Gastdomains in dem System einige virtuelle Services zur Verfügung. Services können einen virtuellen Switch, virtuellen Datenträger oder virtuellen Konsolenservice umfassen.

Abbildung 1-6, „Servicedomain - Beispiel“ enthält ein Beispiel für eine Servicedomain, die Konsolenservices bereitstellt. Häufig hostet die Kontrolldomain die Konsolenservices und ist somit auch eine Servicedomain. Die Domains der Ausführungsumgebung kombinieren häufig

die Funktionen einer Kontrolldomain, I/O-Domain und Servicedomain in einer oder zwei Domains.

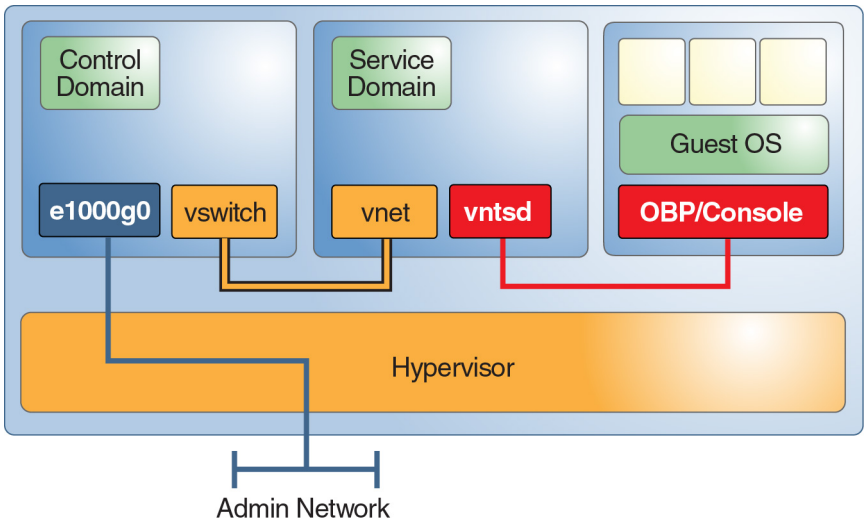
Bedrohung: Manipulation einer Servicedomain

Ein Angreifer, der Kontrolle über eine Servicedomain erhält, kann Daten manipulieren oder eine Kommunikation abhören, die über die angebotenen Services erfolgt. Diese Kontrolle kann den Konsolenzugriff auf Gastdomains, den Zugriff auf Netzwerkservices oder den Zugriff auf Datenträgerservices umfassen.

Bewertung: Manipulation einer Servicedomain

Während die Angriffsstrategien dieselben sind wie bei einem Angriff auf die Kontrolldomain ist der mögliche Schaden geringer, weil der Angreifer die Systemkonfiguration nicht ändern kann. Der auftretende Schaden könnte den Diebstahl oder die Manipulation von Daten umfassen, die von der Servicedomain bereitgestellt werden, jedoch nicht die Manipulation von Datenquellen. Je nach Service könnte ein Angreifer gezwungen sein, Kernel-Module auszutauschen.

ABBILDUNG 1-6 Servicedomain - Beispiel



Gegenmaßnahme: Granulares Trennen von Servicedomains

Wenn möglich sollte jede Servicedomain ihren Clients nur *einen* Service anbieten. Diese Konfiguration garantiert, dass nur ein Service gefährdet werden kann, wenn die Sicherheit einer Servicedomain verletzt wird. Sie müssen jedoch die Wichtigkeit dieses Konfigurationstyps gegen zusätzliche Komplexität abwägen. Die Verwendung von redundanten I/O-Domains wird unbedingt empfohlen.

Gegenmaßnahme: Isolieren von Servicedomains und Gastdomains

Sie können sowohl Oracle Solaris 10- als auch Oracle Solaris 11-Servicedomains von Gastdomains isolieren. Die folgenden Lösungen werden in der bevorzugten Reihenfolge der Implementierung dargestellt.

- Stellen Sie sicher, dass Servicedomain und Gastdomain nicht denselben Netzwerkport gemeinsam verwenden. Außerdem schließen Sie keine virtuelle Switchoberfläche an der Servicedomain an. Schließen Sie bei Oracle Solaris 11-Servicedomains keine VNICs an den physischen Ports an, die für virtuelle Switches verwendet werden.
- Wenn Sie denselben Netzwerkport für das Oracle Solaris 10-BS und das Oracle Solaris 11-BS verwenden müssen, wickeln Sie den Datenverkehr der I/O-Domain in einem VLAN ab, das nicht von Gastdomains verwendet wird.
- Wenn Sie keine der vorherigen Lösungen implementieren können, schließen Sie keinen virtuellen Switch im Oracle Solaris 10-BS an, und wenden Sie IP-Filter im Oracle Solaris 11-BS an.

Gegenmaßnahme: Einschränken des Zugriffs auf virtuelle Konsolen

Stellen Sie sicher, dass der Zugriff auf virtuelle Konsolen *nur* auf die Benutzer begrenzt ist, die auf diese zugreifen müssen. Diese Konfiguration gewährleistet, dass ein einzelner Administrator nicht Zugriff auf alle Konsolen hat, was den Zugriff auf andere Konsolen als die Konsolen verhindert, die einem gefährdeten Konto zugewiesen sind. Weitere Informationen finden Sie in „How to Create Default Services“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

I/O-Domain

Jede Domain, die direkten Zugriff auf physische I/O-Geräte hat, wie Netzwerkports oder Datenträger, ist eine I/O-Domain. Weitere Informationen zur Konfiguration von I/O-Domains finden Sie in Kapitel 5, „Configuring I/O Domains“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

Eine I/O-Domain könnte auch eine Servicedomain sein, wenn sie Gastdomains I/O-Services bereitstellt, was den Domains Zugriff auf die Hardware gibt.

Bedrohung: Denial-of-Service bei einer I/O-Domain oder Servicedomain

Ein Angreifer, der die I/O-Services einer I/O-Domain blockiert, blockiert dadurch auch alle abhängigen Gastdomains. Ein erfolgreicher DoS-Angriff kann erreicht werden, indem das Backend-Netzwerk oder die Datenträgerinfrastruktur überlastet oder ein Fehler in die Domain eingeschleust wird. Beide Angriffe können die Domain blockieren oder zu einer Alarmmeldung führen. Ebenso verursacht ein Angreifer, der die Services einer Servicedomain unterbricht, eine sofortige Blockierung jeder Gastdomain, die von diesen Services abhängt. Eine blockierte Gastdomain nimmt den Betrieb wieder auf, wenn der I/O-Service wieder aufgenommen wird.

Bewertung: Denial-of-Service bei einer I/O-Domain oder Servicedomain

DoS-Angriffe erfolgen im Allgemeinen über das Netzwerk. Ein solcher Angriff kann erfolgreich sein, weil Netzwerkports für Kommunikation offen sind und von Netzwerkdatenverkehr überflutet werden können. Eine sich daraus ergebende Serviceunterbrechung blockiert abhängige Gastdomains. Ein ähnlicher Angriff auf Datenträgerressourcen kann über die SAN-Infrastruktur oder durch Angriff der I/O-Domain erfolgen. Der einzige Schaden ist eine temporäre Unterbrechung aller abhängigen Gastdomains. Während die Auswirkungen von DoS-Aufgaben beträchtlich sein können, werden weder Daten gefährdet noch gehen Daten verloren, und die Systemkonfiguration bleibt intakt.

Gegenmaßnahme: Granulares Konfigurieren von I/O-Domains

Durch die Konfiguration von mehreren I/O-Domains werden die Auswirkungen eines Fehlers oder einer Gefährdung einer Domain verringert. Sie können einer Gastdomain individuelle PCIe-Slots zuweisen, damit sie I/O-Domainfunktionen erhält. Wenn die Root-Domain abstürzt, die Eigentümer des PCIe-Busses ist, wird dieser Bus zurückgesetzt, was zu einem nachfolgenden Crash der Domain führt, die dem jeweiligen Slot zugeordnet war. Trotz dieser Funktion sind weiterhin zwei Root-Domains erforderlich, die jeweils Eigentümer eines separaten PCIe-Busses sind.

Gegenmaßnahme: Konfigurieren redundanter Hardware- und Root-Domains.

Hohe Verfügbarkeit trägt auch zu erweiterter Sicherheit bei, weil sie gewährleistet, dass Services Denial-of-Service-Angriffen widerstehen können. Oracle VM Server for SPARC implementiert Hochverfügbarkeitsmethodologien wie die Verwendung redundanter Datenträger- und Netzwerkressourcen in redundanten I/O-Domains. Diese Konfigurationsoption ermöglicht rollende Upgrades der I/O-Domains und schützt vor den Auswirkungen einer fehlerhaften I/O-Domain aufgrund eines erfolgreichen DoS-Angriffs. Seit der Verfügbarkeit von SR-IOV können Gastdomains direkt auf einzelne I/O-Geräte zugreifen. Wenn SR-IOV jedoch keine Option ist, sollten Sie redundante I/O-Domains

erstellen. Weitere Informationen finden Sie in „Gegenmaßnahme: Granulares Trennen von Servicedomains“ [35].

Bedrohung; Manipulation einer I/O-Domain

Eine I/O-Domain hat direkten Zugriff auf Backend-Geräte, im Allgemeinen Datenträger, die sie virtualisiert und dann Gastdomains anbietet. Ein Angreifer hat vollen Zugriff auf diese Geräte und kann vertrauliche Daten lesen oder Software auf den Boot-Datenträgern der Gastdomains manipulieren.

Bewertung: Manipulation in einer I/O-Domain

Ein Angriff auf die I/O-Domain ist so wahrscheinlich wie ein erfolgreicher Angriff auf eine Servicedomain oder die Kontrolldomain. Die I/O-Domain ist aufgrund des potenziellen Zugriffs auf eine große Anzahl von Datenträgergeräten ein attraktives Ziel. Deshalb sollten Sie diese Bedrohung berücksichtigen, wenn Sie es mit vertraulichen Daten in einer Gastdomain zu tun haben, die auf virtualisierten Datenträgern ausgeführt wird.

Gegenmaßnahme: Schützen von virtuellen Datenträgern

Wenn eine I/O-Domain gefährdet ist, hat der Angreifer vollen Zugriff auf die virtuellen Datenträger der Gastdomain.

Schützen Sie den Inhalt der virtuellen Datenträger wie folgt:

- **Verschlüsseln des Inhalts der virtuellen Datenträger.** Bei Oracle Solaris 10-Systemen können Sie eine Anwendung verwenden, die ihre eigenen Daten verschlüsseln kann, wie `pgp`/`gpg` oder verschlüsselte Oracle 11g Tablespaces. Bei Oracle Solaris 11-Systemen können Sie verschlüsselte ZFS-Datasets für eine transparente Verschlüsselung aller im Dateisystem gespeicherten Daten verwenden.
- **Verteilen von Daten auf mehrere virtuelle Datenträger über verschiedene I/O-Domains hinweg.** Eine Gastdomain könnte einen Stripeset-Datenträger (RAID 1/RAID 5) erstellen, der durch Striping über mehrere virtuelle Datenträger verteilt wird, die aus zwei I/O-Domains abgerufen werden. Wenn eine dieser I/O-Domains gefährdet ist, hätte der Angreifer Schwierigkeiten, den verfügbaren Datenteil zu nutzen.

Gastdomains

Gastdomains sind zwar nicht Bestandteil der Ausführungsumgebung, sind jedoch das wahrscheinlichste Ziel eines Angriffs, weil sie mit dem Netzwerk verbunden sind. Ein Angreifer, der die Sicherheit eines virtualisierten Systems verletzt, kann Angriffe auf die Ausführungsumgebung starten.

Gegenmaßnahme: Sichern des Betriebssystems der Gastdomain

Das Betriebssystem in der Gastdomain ist häufig die erste Verteidigungslinie vor Angriffen. Mit Ausnahme von Angriffen, die innerhalb des Data Centers ausgelöst werden, muss ein Angreifer in eine Gastdomain eindringen, die externe Verbindungen hat, bevor er versucht, die Isolation einer Gastdomain zu durchbrechen und die gesamte Umgebung zu übernehmen. Deshalb müssen Sie das BS der Gastdomain schützen.

Um das Betriebssystem weiter zu schützen, können Sie Ihre Anwendung in Solaris-Zones bereitstellen, die eine zusätzliche Isolierungsschicht zwischen dem Netzwerkservice der Anwendung und dem Betriebssystem der Gastdomain einfügen. Ein erfolgreicher Angriff auf den Service gefährdet nur die Zone und nicht das zugrundeliegende Betriebssystem; dadurch wird verhindert, dass der Angreifer die Kontrolle über die Ressourcen hinaus erweitert, die der Zone zugewiesen sind. Auf diese Weise wird es schwieriger, die Isolation der Gastdomain zu durchbrechen. Weitere Informationen zur Sicherung des Gast-BS finden Sie in *Oracle Solaris 10 Security Guidelines* and *Oracle Solaris 11 Security Guidelines* .

♦ ♦ ♦ KAPITEL 2

Sichere Installation und Konfiguration von Oracle VM Server for SPARC

In diesem Kapitel werden die Sicherheitsüberlegungen im Zusammenhang mit der Installation und Konfiguration der Oracle VM Server for SPARC-Software beschrieben.

Installation

Die Oracle VM Server for SPARC-Software wird automatisch sicher als ein Oracle Solaris 11-Paket installiert. Nach Abschluss der Installation müssen Sie Administratorberechtigungen zur Konfiguration der Domains mit den Rechte- und Autorisierungsfunktionen haben. Diese Funktionen werden nicht automatisch aktiviert.

Konfiguration nach Abschluss der Installation

Führen Sie die folgenden Aufgaben nach der Installation der Oracle VM Server for SPARC-Software aus, um die sichere Verwendung zu maximieren:

- Konfigurieren Sie die Kontrolldomain mit den erforderlichen virtuellen I/O-Servern wie virtuellem Switch, virtuellem Datenträger und virtuellen Konsolenkonzentratorservices. Weitere Informationen finden Sie in Kapitel 3, „Setting Up Services and the Control Domain“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .
- Konfigurieren Sie Gastdomains. Weitere Informationen finden Sie in Kapitel 4, „Setting Up Guest Domains“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

  Mit einem virtuellen Switch können Sie Gastdomains über ein administratives Netzwerk und ein Production-Netzwerk konfigurieren. In diesem Fall wird ein virtueller Switch mit der Production-Netzwerkschnittstelle als virtuelles Switch-Netzwerkgerät erstellt. Weitere Informationen finden Sie unter „Gegenmaßnahme: Konfigurieren eines dedizierten Verwaltungsnetzwerks“ [26].

  Die Sicherheit einer Gastdomain wird gefährdet, wenn einer der virtuellen Datenträger gefährdet ist, Deshalb müssen Sie sicherstellen, dass virtuelle Datenträger (dem Netzwerk zugeordneter Speicher, lokal gespeicherte Datenträgerimagedateien oder physische Datenträger) an einem sicheren Ort gespeichert werden.

Der `vntsd`-Daemon ist standardmäßig deaktiviert. Wenn dieser Daemon aktiviert ist, kann sich jeder Benutzer, der bei der Kontrolldomain angemeldet ist, bei der Konsole einer Gastdomain anmelden. Um diese Art von Zugriff zu vermeiden, müssen Sie sicherstellen, dass der `vntsd`-Daemon deaktiviert ist oder müssen den Konsolenkonnektivitätszugriff *nur* auf berechtigte Benutzer begrenzen.

- Der Serviceprozessor (SP) ist standardmäßig sicher konfiguriert. Informationen zur Verwendung der Integrated Lights Out Management-(ILOM-)Software zur Verwaltung des SP finden Sie in der Dokumentation für Ihre Plattform unter `http://www.oracle.com/technetwork/documentation/sparc-tseries-servers-252697.html`.

♦ ♦ ♦ KAPITEL 3

Sicherheitsinformationen für Entwickler

Dieses Kapitel enthält Informationen für Entwickler, die Anwendungen für die Oracle VM Server for SPARC-Software erzeugen.

Oracle VM Server for SPARC-XML-Oberfläche

Sie können externe Programm erstellen, die mit der Oracle VM Server for SPARC-Software über das Extensible Markup Language-(XML-)Kommunikationsverfahren kommunizieren. XML verwendet das Extensible Messaging and Presence Protocol (XMPP).

Ein Angreifer könnte versuchen, dieses Netzwerkprotokoll für den Zugriff auf ein System zu nutzen, deshalb sollten Sie die Deaktivierung von XMPP in Erwägung ziehen. Informationen zur Deaktivierung von XMPP finden Sie in „XML Transport“ in *Oracle VM Server for SPARC 3.3 Administration Guide* . Weitere Informationen über die Sicherheitsverfahren, die Logische Domains Manager verwendet, finden Sie in „XMPP Server“ in *Oracle VM Server for SPARC 3.3 Administration Guide* .

Die Deaktivierung von XMPP verhindert die Verwaltung des Systems durch Oracle VM Manager oder Ops Center und die Nutzung von einigen Schlüsselfunktionen von Oracle VM Server for SPARC, darunter auch die folgenden Befehle:

- `ldm migrate-domain`
- `ldm init-system`
- `ldm remove-core -g`
- `ldm add-memory`
- `ldm set-memory`
- `ldm remove-memory`
- `ldm grow-socket`
- `ldm shrink-socket`
- `ldm set-socket`
- `ldm list-socket`

♦ ♦ ♦ ANHANG A

Checkliste für eine sichere Bereitstellung

In dieser Checkliste werden die Schritte zusammengefasst, mit denen Sie Ihre Oracle VM Server for SPARC-Umgebung schützen können. Die Einzelheiten werden in anderen Dokumenten beschrieben, wie:

- *Oracle VM Server for SPARC 3.3 Administration Guide*
- *Oracle Solaris 10 Security Guidelines*
- *Oracle Solaris 11 Security Guidelines*

Oracle VM Server for SPARC-Sicherheitscheckliste

- Führen Sie die Schritte zum Schützen von Oracle Solaris-BS für Ihre Gastdomains genauso aus wie in einer nicht-virtualisierten Umgebung.
- Mit den LDoms Management und LDoms Review-Rechteprofilen delegieren Sie die entsprechenden Berechtigungen für die Benutzer.
- Mit Berechtigungen begrenzen Sie den Zugriff auf die Konsole von Domains, auf die *nur* Sie, als Administrator von Oracle VM Server for SPARC, zugreifen müssen.
- Deaktivieren Sie nicht benötigte Domain Manager-Services.
- Stellen Sie nur Gastdomains derselben Sicherheitsklasse auf einer physischen Plattform bereit.
- Stellen Sie sicher, dass zwischen dem Administrationsnetzwerk der Ausführungsumgebung und den Gastdomains keine Netzwerkverbindungen vorhanden sind.
- Weisen Sie Gastdomains nur die erforderlichen Ressourcen zu.