Guia de Segurança do Oracle® VM Server for SPARC 3.5

Número do Item: E86376-01
Agosto de 2017

Número do Item: E86376-01

Acessibilidade da Documentação

Para obter informações sobre o compromisso da Oracle com a acessibilidade, visite o Web site do Programa de Acessibilidade da Oracle em `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Acceso ao Oracle Support

Os clientes da Oracle que adquiriram serviços de suporte têm acesso a suporte eletrônico por meio do My Oracle Support. Para obter informações, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` caso tenha deficiência de audição.

Conteúdo

Como usar esta documentação

- **Visão geral** - Fornece informações sobre o uso do software Oracle VM Server for SPARC 3.5 de maneira segura.
- **Público-alvo** – Administradores de sistemas que gerenciam a segurança em servidores SPARC virtualizados
- **Conhecimento necessário** – Os administradores de sistemas que gerenciam esses servidores devem ter um conhecimento prático de sistemas UNIX e do sistema operacional Oracle Solaris (SO Oracle Solaris)

Biblioteca de documentação do produto

A documentação e os recursos desse produto e dos produtos relacionados estão disponíveis em http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html.

Feedback

Forneça feedback sobre esta documentação em http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CAPÍTULO 1

Visão geral da segurança do Oracle VM Server for SPARC

Embora o número de recomendações de segurança deste documento possa dar uma impressão diferente, a instalação típica do Oracle VM Server for SPARC já oferece bastante proteção contra o uso não autorizado. Mesmo que uma exploração seja improvável, há uma pequena superfície de ataque e algum risco ainda existe. Da mesma que forma que você pode optar por usar um alarme contra roubo, além dos dispositivos de segurança padrão, como travas nas portas, para aumentar a segurança de sua casa, medidas adicionais de segurança da rede podem ajudar a reduzir a chance de ocorrerem problemas inesperados ou minimizar os danos potenciais.

Este capítulo aborda os seguintes tópicos de segurança do Oracle VM Server for SPARC:

Recursos de segurança usados pelo Oracle VM Server for SPARC

O software Oracle VM Server for SPARC é um produto de virtualização que permite que várias máquinas virtuais (VM) Oracle Solaris sejam executadas em um único sistema físico, cada uma com seu próprio SO Oracle Solaris 10 ou Oracle Solaris 11 instalado. Cada VM também é denominada *domínio lógico*. Os domínios são instâncias independentes e podem executar diferentes versões do SO Oracle Solaris e diferentes softwares de aplicativo. Por exemplo, os domínios podem ter diferentes revisões de pacote instaladas, diversos serviços ativados e contas do sistema com senhas distintas. Consulte *Oracle Solaris 10 Security Guidelines* e *Oracle Solaris 11 Security Guidelines* para obter informações sobre a segurança do Oracle Solaris.

O comando `ldm` chama o Logical Domains Manager e deve ser executado no domínio de controle para configurar domínios e recuperar informações de estado. A limitação do acesso ao domínio de controle e ao comando `ldm` é fundamental para a segurança dos domínios executados no sistema. Para limitar o acesso aos dados de configuração do domínio, use os recursos de segurança do Oracle VM Server for SPARC, como os direitos do Oracle Solaris para consoles e autorizações do `solaris.ldoms`. Consulte "Logical Domains Manager Profile Contents" in *Oracle VM Server for SPARC 3.5 Administration Guide*.

O software Oracle VM Server for SPARC usa os seguintes recursos de segurança:

- Os recursos de segurança disponíveis nos sistemas operacionais Oracle Solaris 10 e Oracle Solaris 11 também estão disponíveis nos domínios que executam o software Oracle VM Server for SPARC. Consulte *Oracle Solaris 10 Security Guidelines* e *Oracle Solaris 11 Security Guidelines*.
- Os recursos de segurança do SO Oracle Solaris podem ser aplicados ao software Oracle VM Server for SPARC. Para obter informações abrangentes sobre como garantir a segurança do Oracle VM Server for SPARC, consulte "Segurança em um ambiente virtualizado" [15] e "Defesa contra ataques" [17].
- Os sistemas operacionais Oracle Solaris 10 e Oracle Solaris 11 incluem correções de segurança que estão disponíveis para o seu sistema. Obtenha as correções do SO Oracle Solaris 10 como patches ou atualizações de segurança. Obtenha as correções do SO Oracle Solaris 11 como SRUs (Support Repository Updates).
- Para obter informações sobre como limitar o acesso aos comandos de administração e aos consoles de domínio do Oracle VM Server for SPARC, consulte o Chapter 2, "Oracle VM Server for SPARC Security" in *Oracle VM Server for SPARC 3.5 Administration Guide*.

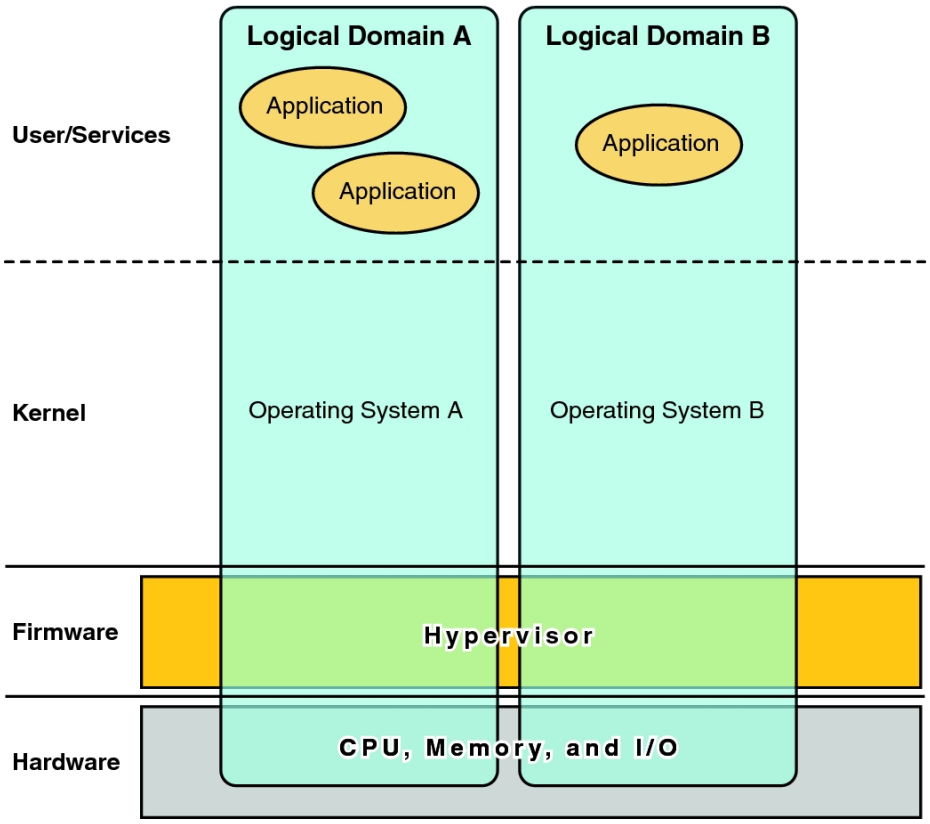
Visão geral do produto Oracle VM Server for SPARC

O Oracle VM Server for SPARC oferece recursos de virtualização de nível empresarial altamente eficientes para os servidores Oracle SPARC T-series, bem como para o servidor SPARC M5 e Servidores Fujitsu M10. Usando o software Oracle VM Server for SPARC, você pode criar vários servidores virtuais, denominados domínios lógicos, em um único sistema. Esse tipo de configuração permite que você utilize a escala de threads oferecida por esses servidores SPARC e pelo SO Oracle Solaris.

Um *domínio lógico* é uma máquina virtual que contém um agrupamento lógico separado de recursos. Um domínio lógico possui seu próprio sistema operacional e identidade em um único sistema de computadores. Cada domínio lógico pode ser criado, destruído, reconfigurado e reinicializado de forma independente, sem exigir a execução de um ciclo de energia do servidor. É possível executar diversos softwares de aplicativo em domínios lógicos diferentes e mantê-los independentes para fins de desempenho e segurança.

Para obter informações sobre como usar o software Oracle VM Server for SPARC, consulte o *Oracle VM Server for SPARC 3.5 Administration Guide* e o *Oracle VM Server for SPARC 3.5 Reference Manual*. Para obter informações sobre o hardware e o software necessários, consulte o *Oracle VM Server for SPARC 3.5 Installation Guide*.

FIGURA 1 Hypervisor com suporte para dois domínios lógicos



O software Oracle VM Server for SPARC usa os seguintes componentes para permitir a virtualização do sistema:

- **Hypervisor.** O hypervisor é uma pequena camada de firmware que fornece uma arquitetura de máquina virtualizada estável na qual um sistema operacional pode ser instalado. Os servidores Sun da Oracle que usam o hypervisor oferecem recursos de hardware para permitir o controle do hypervisor sobre as atividades do sistema operacional em um domínio lógico.

O número de domínios e os recursos de cada domínio suportados por determinado hypervisor SPARC dependem do servidor. O hypervisor pode alocar subconjuntos dos recursos de CPU, memória e E/S do servidor para determinado domínio lógico. Essa alocação permite que vários sistemas operacionais sejam suportados simultaneamente, cada um em seu próprio domínio lógico. Os recursos podem ser reorganizados entre domínios lógicos distintos com uma granularidade arbitrária. Por exemplo, as CPUs podem ser atribuídas a um domínio lógico com a granularidade de um thread de CPU.

O *processador de serviço* (SP), também conhecido como o *controlador do sistema* (SC), monitora e executa a máquina física. O Logical Domains Manager, e não o SP, gerencia os domínios lógicos.

- **Domínio de controle.** O Logical Domains Manager é executado neste domínio e permite que você crie e gerencie outros domínios lógicos, bem como aloque recursos virtuais para outros domínios. Só é possível ter um domínio de controle por servidor. O domínio de controle é o primeiro domínio criado quando o software Oracle VM Server for SPARC é instalado. O domínio de controle é denominado `primário`.
- **Domínio de serviço.** Um domínio de serviço fornece serviços de dispositivos virtuais a outros domínios, como um switch virtual, um VCC (virtual console concentrator) e um servidor de disco virtual. Qualquer domínio pode ser configurado como um domínio de serviço.
- **Domínio de E/S.** Um domínio de E/S tem acesso direto a dispositivos físicos de E/S, como uma placa de rede em um controlador PCIe (PCI EXPRESS). Um domínio de E/S pode possuir um complexo raiz PCIe, um slot PCIe ou um dispositivo PCIe integrado usando o recurso de E/S direta (DIO). Consulte "Creating an I/O Domain by Assigning PCIe Endpoint Devices" in *Oracle VM Server for SPARC 3.5 Administration Guide*.

  Um domínio de E/S pode compartilhar dispositivos físicos de E/S com outros domínios na forma de dispositivos virtuais quando também é usado como um domínio de serviço.
- **Domínio raiz.** Um domínio raiz tem um complexo raiz PCIe atribuído a ele. Esse domínio possui a malha PCIe desse complexo raiz e fornece todos os serviços relacionados a malha, como tratamento de erros. Um domínio raiz também é um domínio de E/S, uma vez que possui dispositivos físicos de E/S e tem acesso direto a eles.

  O número de domínios raiz que podem existir depende da arquitetura da plataforma. Por exemplo, se estiver usando um servidor SPARC T4-4 da Oracle, você poderá ter até quatro domínios raiz.
- **Domínio convidado.** Um domínio convidado é um domínio que não é de E/S e que consome serviços de dispositivos virtuais fornecidos por um ou mais domínios de serviço. Um domínio convidado não tem dispositivos físicos de E/S. Ele possui somente dispositivos de E/S virtuais, como discos virtuais e interfaces de rede virtual.

Em geral, um sistema Oracle VM Server for SPARC possui apenas um domínio de controle que fornece os serviços executados pelos domínios de E/S e de serviço. Para melhorar a

redundância e a utilização da plataforma, considere configurar mais de um domínio de E/S em seu sistema Oracle VM Server for SPARC.

Aplicação dos princípios gerais de segurança ao Oracle VM Server for SPARC

Você pode configurar os domínios convidados de diversas maneiras para oferecer diferentes níveis de isolamento desses domínios, compartilhamento de hardware e conectividade de domínio. Esses fatores contribuem para o nível de segurança da configuração geral do Oracle VM Server for SPARC. Para obter recomendações sobre como implantar o software Oracle VM Server for SPARC de maneira segura, consulte “Segurança em um ambiente virtualizado” [15] e “Defesa contra ataques” [17].

Você pode aplicar alguns dos seguintes princípios gerais de segurança:

- **Minimize a superfície de ataque.**
  - Minimize os erros de configuração não intencionais criando diretrizes operacionais que permitem avaliar regularmente a segurança do sistema. Consulte “Contramedida: Criação de diretrizes operacionais” [20].
  - Planeje cuidadosamente a arquitetura do ambiente virtual para aumentar o isolamento dos domínios. Consulte as contramedidas descritas para “Ameaça: Erros na arquitetura do ambiente virtual” [20].
  - Planeje cuidadosamente quais recursos devem ser atribuídos e se eles devem ser compartilhados. Consulte “Contramedida: Atribuição de recursos de hardware com cautela” [23] e “Contramedida: Atribuição de recursos compartilhados com cautela” [23].
  - Verifique se os domínios lógicos estão protegidos contra manipulação aplicando as contramedidas descritas para “Ameaça: Manipulação do ambiente de execução” [24] e “Contramedida: Proteção do sistema operacional do domínio convidado” [38].
    - “Contramedida: Proteção dos caminhos de acesso interativo” [25].
    - “Contramedida: Como minimizar o SO Oracle Solaris” [25].
    - “Contramedida: Proteção do SO Oracle Solaris” [25].
    - “Contramedida: Proteção do Logical Domains Manager” [32].
    - “Contramedida: Uso da separação de funções e do isolamento de aplicativos” [26] descreve a importância de atribuir funções aos diversos domínios e garantir que o domínio de controle execute um software que forneça a infraestrutura necessária para hospedar os domínios convidados. Você deve executar aplicativos que possam ser executados por outros sistemas nos domínios convidados designados para esse fim.

        - “Contramedida: Configuração de uma rede de gerenciamento dedicada” [26] descreve uma configuração de rede mais avançada que conecta os servidores com SPs a uma rede de gerenciamento dedicada a fim de proteger o SP do acesso à rede.
    - Exponha um domínio convidado à rede *somente* quando necessário. Você pode usar switches virtuais para limitar a conectividade de rede de um domínio convidado *somente* às redes apropriadas.
    - Siga as etapas para minimizar a superfície de ataque do Oracle Solaris 10 e do Oracle Solaris 11 conforme descrito em *Oracle Solaris 10 Security Guidelines* e *Oracle Solaris 11 Security Guidelines*.
    - Proteja o núcleo do hypervisor conforme descrito em “Contramedida: Validação de assinaturas de firmware e software” [29] e “Contramedida: Validação dos módulos de kernel” [30].
    - Proteja o domínio de controle contra ataques de negação de serviço. Consulte “Contramedida: Proteção do acesso do console” [31].
    - Certifique-se de que o Logical Domains Manager não possa ser executado por usuários não autorizados. Consulte “Ameaça: Uso não autorizado dos utilitários de configuração” [31].
    - Certifique-se de que o domínio de serviço não possa ser acessado por usuários ou processos não autorizados. Consulte “Ameaça: Manipulação de um domínio de serviço” [34].
    - Proteja os domínios de E/S ou os domínios de serviço contra ataques de negação de serviço. Consulte “Ameaça: Ataque de negação de serviço de um domínio de E/S ou de serviço” [36].
    - Certifique-se de que os domínios de E/S não possam ser acessados por usuários ou processos não autorizados. Consulte “Ameaça: Manipulação de um domínio de E/S” [37].
    - Desative os serviços desnecessários do gerenciador de domínios. O Logical Domains Manager fornece serviços de rede para acesso, monitoramento e migração de domínios. Consulte “Contramedida: Proteção do Logical Domains Manager” [32] e “Contramedida: Proteção do Oracle ILOM” [28].
    - **Forneça o privilégio mínimo para executar uma operação.**
        - Isole os sistemas em *classes de segurança*, que são grupos de sistemas convidados individuais que compartilham os mesmos privilégios e requisitos de segurança. Atribuindo somente domínios convidados de uma única classe de segurança a uma única plataforma de hardware, você criará uma barreira de isolamento, impedindo que os domínios penetrem em uma classe de segurança diferente. Consulte “Contramedida: Atribuição de convidados a plataformas de hardware com cautela” [20].
        - Use direitos para restringir a capacidade de gerenciar com o comando `ldm`. *Somente* os usuários que precisam administrar domínios devem ter essa capacidade. Atribua

uma função que use o perfil de direitos Gerenciamento de LDoms aos usuários que necessitam de acesso a todos os subcomandos `ldm`. Atribua uma função que use o perfil de direitos Revisão de LDoms aos usuários que necessitam somente de acesso aos subcomandos `ldm` list. Consulte "Using Rights Profiles and Roles" in *Oracle VM Server for SPARC 3.5 Administration Guide*.

- Use direitos para restringir o acesso ao console *somente* dos domínios que você, como administrador do Oracle VM Server for SPARC, administra. *Não* permita o acesso geral a todos os domínios. Consulte "Controlling Access to a Domain Console by Using Rights" in *Oracle VM Server for SPARC 3.5 Administration Guide*.

Segurança em um ambiente virtualizado

Para proteger de maneira eficaz o ambiente virtualizado do Oracle VM Server for SPARC, proteja o sistema operacional e cada serviço executado em cada domínio. Para reduzir os efeitos de uma violação bem-sucedida, separe os serviços implantando-os em domínios diferentes.

O ambiente Oracle VM Server for SPARC usa um hypervisor para virtualizar os recursos de CPU, memória e E/S de domínios lógicos. Cada domínio é um servidor virtualizado separado que deve ser protegido contra ataques potenciais.

Um ambiente virtualizado permite consolidar vários servidores em um só por meio do compartilhamento de recursos de hardware. No Oracle VM Server for SPARC, os recursos de CPU e memória são alocados exclusivamente para cada domínio, o que impede o abuso em decorrência do uso excessivo de CPU ou da superalocação de memória. Recursos de disco e rede são geralmente fornecidos por domínios de serviço para vários domínios convidados.

Ao avaliar a segurança, pressuponha *sempre* que o seu ambiente tem uma falha que poderá ser explorada por um invasor. Por exemplo, um invasor poderá explorar uma vulnerabilidade do hypervisor para sequestrar o sistema inteiro, incluindo seus domínios convidados. Portanto, *sempre* implante os sistemas para minimizar o risco de dano em caso de violação.

Ambiente de execução

O ambiente de execução inclui os seguintes componentes:

- **Hypervisor –** Firmware específico da plataforma que virtualiza o hardware e que depende em grande parte do suporte de hardware embutido na CPU.
- **Domínio de controle –** Um domínio especializado que configura o hypervisor e executa o Logical Domains Manager, que gerencia os domínios lógicos.

- **Domínio de E/S ou domínio raiz –** Um domínio que possui alguns ou todos os dispositivos de E/S disponíveis da plataforma e os compartilha com outros domínios.
- **Domínio de serviço –** Um domínio que oferece serviços a outros domínios. Um domínio de serviço pode permitir o acesso do console a outros domínios ou fornecer discos virtuais. Um domínio de serviço que permite o acesso de discos virtuais a outros domínios também é um domínio de E/S.

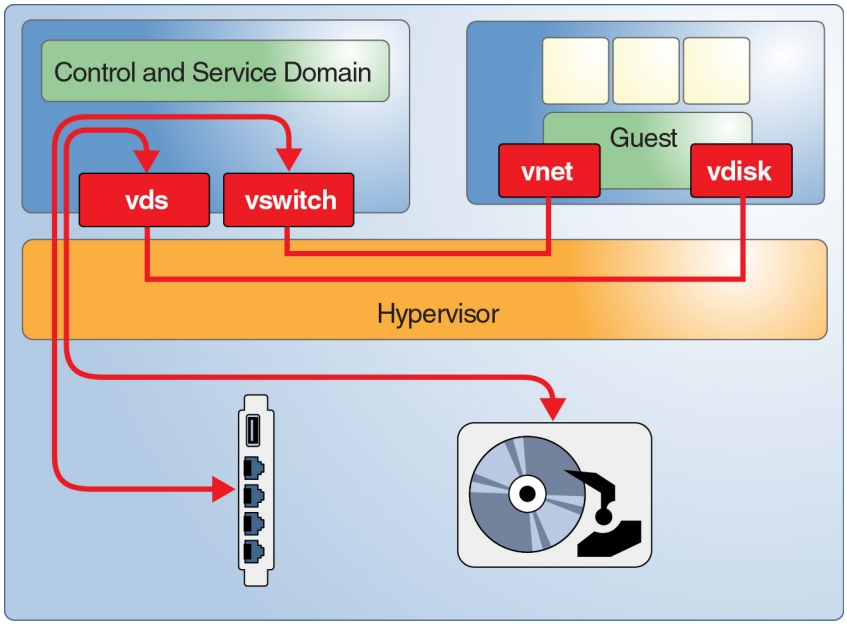
Para obter mais informações sobre esses componentes, consulte a Figura 1 e as descrições detalhadas dos componentes.

Você pode melhorar a utilização das configurações de E/S redundantes definindo um segundo domínio de E/S. Também pode usar um segundo domínio de E/S para isolar o hardware contra violações de segurança. Para obter informações sobre as opções de configuração, consulte o *Oracle VM Server for SPARC 3.5 Administration Guide*.

Proteção do ambiente de execução

O Oracle VM Server for SPARC possui vários alvos de ataque no ambiente de execução. A Figura 2 mostra uma configuração simples do Oracle VM Server for SPARC na qual o domínio de controle fornece serviços de rede e de disco para um domínio convidado. Esses serviços são implementados por meio de daemons e módulos de kernel que são executados no domínio de controle. O Logical Domains Manager atribui LDCs (Logical Domain Channels) a cada serviço e a um cliente para facilitar a comunicação ponto a ponto entre eles. Um invasor poderá explorar um erro em um componente para romper o isolamento dos domínios convidados. Por exemplo, ele poderá executar um código arbitrário no domínio de serviço ou interromper as operações normais da plataforma.

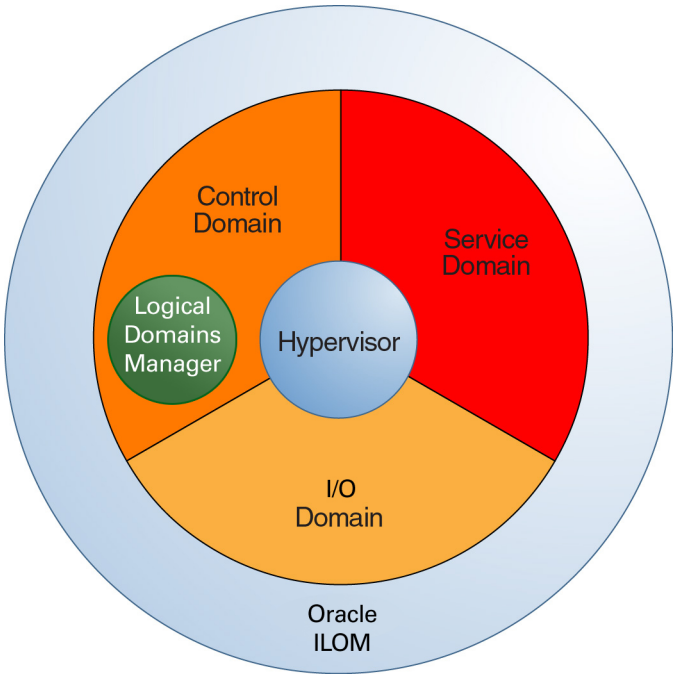
FIGURA 2 Exemplo de ambiente Oracle VM Server for SPARC



Defesa contra ataques

A figura a seguir mostra os componentes de virtualização que constituem o “ambiente de execução” do Oracle VM Server for SPARC. Esses componentes não estão estritamente separados. A configuração mais simples é combinar todas essas funções em um único domínio. O domínio de controle também pode funcionar como um domínio de E/S e um domínio de serviço para outros domínios.

FIGURA 3 Componentes do ambiente de execução



Suponha que um invasor tente romper o isolamento do sistema e, em seguida, manipular o hypervisor ou outro componente do ambiente de execução para acessar um domínio convidado. Você deve proteger cada domínio convidado como faria com qualquer servidor autônomo.

O restante deste capítulo apresenta as possibilidades de ameaças e as diversas medidas que você pode tomar para combatê-las. Cada um desses ataques tenta romper ou eliminar o isolamento dos diferentes domínios executados em uma única plataforma. As seções a seguir descrevem as ameaças a cada parte de um sistema Oracle VM Server for SPARC:

- “Ambiente operacional” [19]
- “Ambiente de execução” [24]
- “Oracle ILOM” [27]
- “Hypervisor” [29]
- “Domínio de controle” [30]
- “Logical Domains Manager” [31].
- “Domínio de E/S” [35]

- “Domínio de serviço” [33]
- “Domínios convidados” [38]

Ambiente operacional

O ambiente operacional inclui os sistemas físicos e seus componentes, arquitetos de datacenter, administradores e membros da organização de TI. Uma violação de segurança poderá ocorrer em qualquer parte desse ambiente.

A virtualização insere uma camada de software entre o hardware real e os domínios convidados que executam os serviços de produção, o que aumenta a complexidade. Como resultado, você deve planejar e configurar com cautela o sistema virtual e ficar atento a erros humanos. Além disso, cuidado com as tentativas de invasores de obter acesso ao ambiente operacional usando a “engenharia social”.

As seções a seguir descrevem as diferentes ameaças que podem ser encontradas no nível do ambiente operacional.

Ameaça: Configuração incorreta não intencional

A principal preocupação relacionada à segurança em um ambiente virtualizado é manter o isolamento do servidor por meio da separação dos segmentos de rede, da segregação do acesso administrativo e da implantação de servidores em classes de segurança, que são grupos de domínios com os mesmos privilégios e requisitos de segurança.

Configure com cautela os recursos virtuais para evitar alguns dos seguintes erros:

- Criação de canais de comunicação desnecessários entre os domínios convidados de produção e o ambiente de execução
- Criação de acesso desnecessário aos segmentos de rede
- Criação de conexões não intencionais entre classes de segurança distintas
- Migração não intencional de um domínio convidado para a classe de segurança errada
- Alocação de hardware insuficiente, o que poderá levar a uma sobrecarga inesperada de recursos
- Atribuição de discos ou dispositivos de E/S ao domínio errado

Contramedida: Criação de diretrizes operacionais

Antes de começar, defina com cautela as diretrizes operacionais do seu ambiente Oracle VM Server for SPARC. Essas diretrizes descrevem as seguintes tarefas a serem executadas e como executá-las:

- Gerenciar os patches de todos os componentes do ambiente
- Permitir a implantação de alterações de forma segura, rastreável e bem definida
- Verificar os arquivos de log em intervalos regulares
- Monitorar a integridade e a disponibilidade do ambiente

Executar regularmente verificações para garantir que essas diretrizes se mantenham atualizadas e adequadas e verificar se elas estão sendo seguidas nas operações diárias.

Além dessas diretrizes, você pode tomar várias medidas mais técnicas para reduzir o risco de ações não intencionais. Consulte “Logical Domains Manager” [31].

Ameaça: Erros na arquitetura do ambiente virtual

Ao mover um sistema físico para um ambiente virtualizado, normalmente você pode manter a configuração de armazenamento no estado em que se encontra reutilizando os LUNs originais. Entretanto, a configuração de rede deverá ser adaptada ao ambiente virtualizado, e a arquitetura resultante poderá ser consideravelmente diferente da usada no sistema físico.

Você deve considerar como manter o isolamento das classes de segurança distintas e as respectivas necessidades. Além disso, considere o hardware compartilhado da plataforma e os componentes compartilhados, como switches de rede e switches SAN.

Para aumentar a segurança do seu ambiente, certifique-se de manter o isolamento dos domínios convidados e das classes de segurança. Ao projetar a arquitetura, preveja os possíveis erros e ataques e implemente linhas de defesa. Um design adequado ajuda a limitar os problemas potenciais de segurança e, ao mesmo tempo, gerenciar a complexidade e o custo.

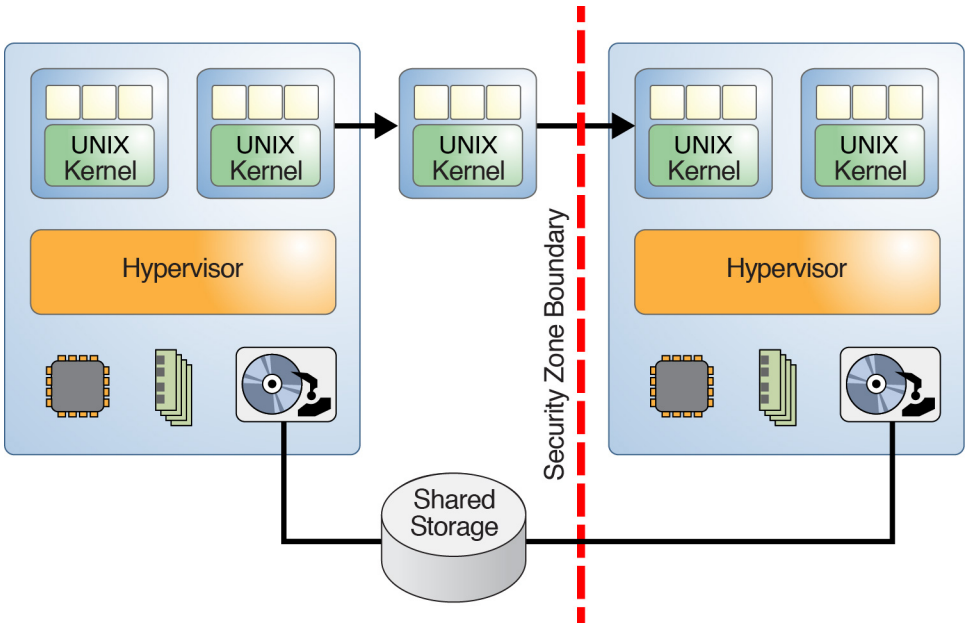
Contramedida: Atribuição de convidados a plataformas de hardware com cautela

Use classes de segurança, que são grupos de domínios com os mesmos privilégios e requisitos de segurança, para isolar os domínios individuais uns dos outros. A atribuição de domínios convidados da mesma classe de segurança a determinada plataforma de hardware impedirá que o ataque atinja outra classe de segurança, mesmo que o isolamento seja rompido.

Contramedida: Planejamento de uma migração de domínio do Oracle VM Server for SPARC

O recurso de migração dinâmica de domínio poderá ocasionar o rompimento do isolamento se um domínio convidado for migrado de forma inadvertida para uma plataforma atribuída a uma classe de segurança diferente, conforme mostrado na figura a seguir. Portanto, planeje com cautela a migração de domínios convidados a fim de impedir que ela ultrapasse os limites de uma classe de segurança.

FIGURA 4 Migração de domínios entre os limites de segurança



Para minimizar ou eliminar a vulnerabilidade de segurança imposta pela operação de migração, você deverá trocar e instalar manualmente os certificados de host gerados pelo comando `ldmd` fora de banda entre cada par de máquina de origem e de destino. Para obter informações sobre como configurar os certificados SSL, consulte “Configuring SSL Certificates for Migration” in *Oracle VM Server for SPARC 3.5 Administration Guide*.

Contramedida: Configuração correta de conexões virtuais

A perda de controle de todas as conexões de rede virtuais poderá fazer com que um domínio obtenha acesso indevido a um segmento de rede. Por exemplo, esse acesso poderá atravessar o firewall ou os limites de uma classe de segurança.

Para reduzir o risco de erros de implementação, planeje e documente com cautela todas as conexões virtuais e físicas em seu ambiente. Otimize o plano de conexão de domínios para que ele seja simples e gerenciável. Documente claramente o seu plano e verifique se a sua implementação está correta em relação a ele antes de passar para a produção. Mesmo depois que o ambiente virtual estiver em produção, verifique a implementação em relação ao plano em intervalos regulares.

Contramedida: Uso do recurso VLAN Tagging

Você pode usar o recurso VLAN Tagging para consolidar vários segmentos Ethernet em uma única rede física. Esse recurso também está disponível para switches virtuais. Para mitigar os riscos envolvidos nos erros de software na implementação de switches virtuais, configure um switch virtual por NIC e VLAN física. Para oferecer maior proteção contra erros no driver Ethernet, evite usar VLANs "tagged". Entretanto, a probabilidade de ocorrerem esses erros é baixa uma vez que essa vulnerabilidade de VLANs "tagged" é bastante conhecida. Os testes de invasão no servidor Oracle Sun SPARC T-series com o software Oracle VM Server for SPARC não mostraram essa vulnerabilidade.

Contramedida: Uso de appliances de segurança virtual

Os appliances de segurança, como filtros de pacote e firewalls, são instrumentos de isolamento e protegem o isolamento das classes de segurança. Como esses appliances estão sujeitos às mesmas ameaças que qualquer outro domínio convidado, o seu uso não garante total proteção contra uma violação do isolamento. Portanto, considere com cautela todos os aspectos de risco e segurança antes de decidir virtualizar esse serviço.

Ameaça: Efeitos colaterais do compartilhamento de recursos

O compartilhamento de recursos em um ambiente virtualizado poderá levar a ataques de negação de serviço (DoS), que sobrecarregam um recurso até que ele afete negativamente outro componente, como outro domínio.

Em um ambiente Oracle VM Server for SPARC, apenas alguns recursos podem ser afetados por um ataque de negação de serviço. Os recursos de CPU e memória são atribuídos exclusivamente a cada domínio convidado, o que impede a maioria dos ataques de negação de

serviço. Mesmo a atribuição exclusiva desses recursos poderá tornar um domínio convidado mais lento das seguintes maneiras:

- Sobrecarregando as áreas do cache compartilhadas entre strands e atribuídas a dois domínios convidados
- Sobrecarregando a largura de banda de memória

Diferentemente dos recursos de CPU e memória, os serviços de disco e rede são geralmente compartilhados entre domínios convidados. Esses serviços são fornecidos para os domínios convidados por um ou mais domínios de serviço. Considere com cautela como atribuir e distribuir esses recursos para os domínios convidados. Observe que toda configuração que permita o máximo desempenho e utilização de recursos simultaneamente minimiza o risco de efeitos colaterais.

Avaliação: Efeitos colaterais de recursos compartilhados

Um link de rede poderá se tornar saturado ou um disco poderá ficar sobrecarregado quer seja atribuído exclusivamente a um domínio ou compartilhado entre domínios. Esses ataques afetam a disponibilidade de um serviço enquanto estão ocorrendo. O alvo do ataque não é comprometido e nenhum dado é perdido. Você pode minimizar facilmente os efeitos dessa ameaça, mas lembre-se de que isso se limitará aos recursos de rede e disco no Oracle VM Server for SPARC.

Contramedida: Atribuição de recursos de hardware com cautela

Certifique-se de atribuir somente os recursos necessários de hardware aos domínios convidados. Lembre-se de cancelar a atribuição de um recurso não utilizado quando ele não for mais necessário; por exemplo, uma porta de rede ou uma unidade de DVD necessária somente durante uma instalação. Seguindo essa prática, você minimizará o número de possíveis pontos de entrada para um invasor.

Contramedida: Atribuição de recursos compartilhados com cautela

Os recursos de hardware compartilhados, como portas de rede física, são um possível alvo de ataques de negação de serviço. Para limitar o impacto desses ataques a um único grupo de domínios convidados, determine com cautela quais domínios convidados compartilham quais recursos de hardware.

Por exemplo, os domínios convidados que compartilham recursos de hardware poderiam ser agrupados com base nos mesmos requisitos de segurança ou disponibilidade. Além do agrupamento, você pode aplicar diferentes tipos de controles de recursos.

Você deve considerar como compartilhar os recursos de disco e rede. Você pode mitigar os problemas separando o acesso ao disco por meio de caminhos de acesso físico dedicados ou de serviços de disco virtual dedicados.

Resumo: Efeitos colaterais de recursos compartilhados

Todas as contramedidas descritas nesta seção exigem que você entenda os detalhes técnicos de sua implantação e suas implicações de segurança. Planeje com cautela, documente bem e mantenha sua arquitetura o mais simples possível. Você deve entender as implicações do hardware virtualizado a fim de se preparar para implantar o software Oracle VM Server for SPARC de maneira segura.

Os domínios lógicos são resistentes aos efeitos do compartilhamento de CPUs e memória, uma vez que pouco compartilhamento ocorre de fato. Contudo, é melhor aplicar controles de recursos, como o gerenciamento de recursos do Solaris, nos domínios convidados. O uso desses controles oferece proteção contra o comportamento inadequado dos aplicativos, tanto em um ambiente virtual como não virtualizado.

Ambiente de execução

A Figura 3 mostra os componentes do ambiente de execução. Cada componente fornece certos serviços que, em conjunto, formam a plataforma geral na qual os domínios convidados de produção devem ser executados. A configuração adequada dos componentes é extremamente importante para a integridade do sistema.

Todos os componentes do ambiente de execução são alvos potenciais para um invasor. Esta seção descreve as ameaças que podem afetar cada componente do ambiente de execução. Algumas ameaças e contramedidas podem se aplicar a mais de um componente.

Ameaça: Manipulação do ambiente de execução

Manipulando o ambiente de execução, você pode obter controle de diversas maneiras. Por exemplo, você pode instalar um firmware manipulado no Oracle ILOM para rastrear toda a E/S dos domínios convidados em um domínio de E/S. Esse tipo de ataque pode acessar e alterar a configuração do sistema. Um invasor que obtiver controle do domínio de controle do Oracle VM Server for SPARC poderá reconfigurar o sistema da maneira como quiser, e um invasor que obtiver controle de um domínio de E/S poderá fazer alterações no armazenado anexado, como discos de inicialização.

Avaliação: Manipulação do ambiente de execução

Um invasor que conseguir invadir o Oracle ILOM ou qualquer domínio do ambiente de execução poderá ler e manipular todos os dados disponíveis para esse domínio. Esse acesso poderá ser obtido através da rede ou por meio de um erro na pilha de virtualização. Esse tipo de ataque é difícil de ser realizado uma vez que, geralmente, o Oracle ILOM e os domínios não podem ser atacados diretamente.

As contramedidas para proteger contra a manipulação do ambiente de execução são práticas de segurança padrão e devem ser implementadas em qualquer sistema. Essas práticas oferecem uma camada adicional de proteção ao ambiente de execução que reduz ainda mais o risco de invasão e manipulação.

Contramedida: Proteção dos caminhos de acesso interativo

Certifique-se de criar *somente* as contas necessárias para os aplicativos executados no sistema.

Certifique-se de que as contas necessárias para administração estejam protegidas por meio da autenticação baseada em chaves ou de senhas fortes. Essas chaves ou senhas não devem ser compartilhadas entre diferentes domínios. Além disso, considere implementar a autenticação de dois fatores ou uma “regra de duas pessoas” para tomar certas ações.

Não use logins anônimos para contas, como `root`, a fim de garantir que você tenha total controle dos comandos executados no sistema e possa identificar os responsáveis por sua execução. Em vez disso, use direitos para conceder aos administradores acesso *somente* às funções que eles estão autorizados a executar. Certifique-se de que o acesso à rede administrativa use sempre criptografia, como SSH, e que a estação de trabalho do administrador seja tratada como um sistema de alta segurança.

Contramedida: Como minimizar o SO Oracle Solaris

Todo software instalado em um sistema poderá ser comprometido, portanto, instale *somente* o software necessário a fim de minimizar as chances de violação.

Contramedida: Proteção do SO Oracle Solaris

Além de instalar um SO Oracle Solaris minimizado, configure pacotes de software para proteger o software contra ataques. Primeiro, execute serviços de rede limitados para desativar todos os serviços de rede, exceto o SSH. Essa política é o comportamento padrão nos sistemas Oracle Solaris 11. Para obter informações sobre como proteger o SO Oracle Solaris, consulte *Oracle Solaris 10 Security Guidelines* e *Oracle Solaris 11 Security Guidelines*.

Contramedida: Uso da separação de funções e do isolamento de aplicativos

Por necessidade, os aplicativos de produção são conectados a outros sistemas e, como resultado, ficam mais expostos a ataques externos. *Não* implante aplicativos de produção em um domínio que faça parte do ambiente de execução. Em vez disso, implante-os *somente* em domínios convidados que não tenham outros privilégios.

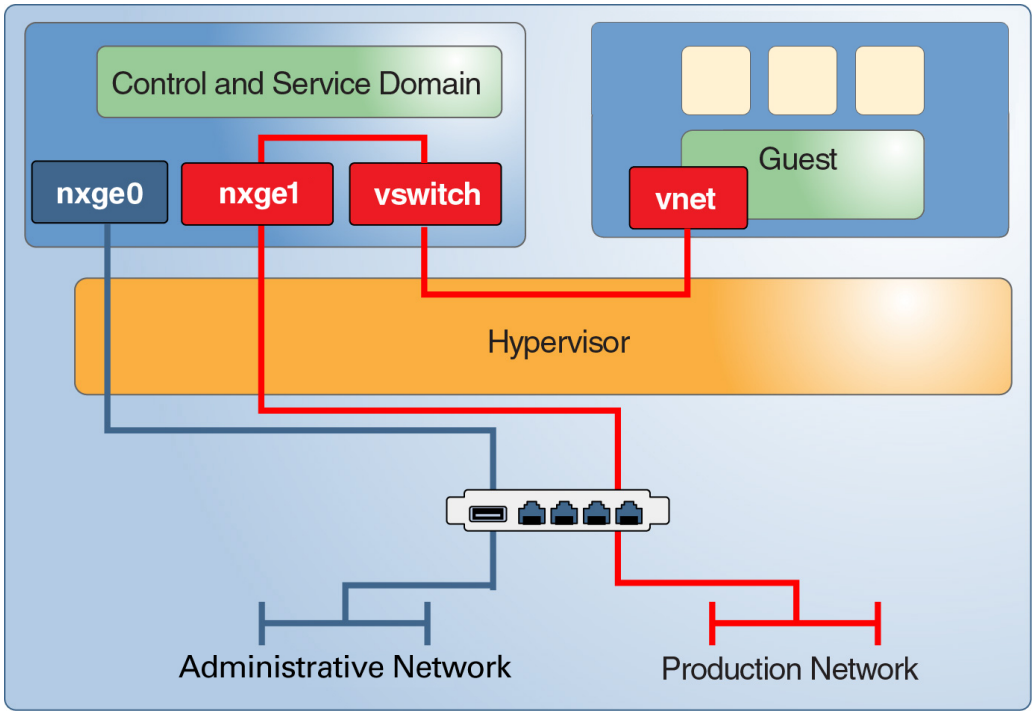
O ambiente de execução deve fornecer somente a infraestrutura necessária para esses domínios convidados. A separação do ambiente de execução dos aplicativos de produção permite implementar a granularidade nos privilégios de administração. O administrador de domínios convidados de produção não precisa ter acesso ao ambiente de execução, e o administrador do ambiente de execução não precisa ter acesso aos domínios convidados de produção. Se possível, atribua as diferentes funções do ambiente de execução, como o domínio de controle e o domínio de E/S, a domínios diferentes. Esse tipo de configuração reduz o dano que poderá ser causado se algum desses domínios for comprometido.

Também é possível estender a separação de funções ao ambiente de rede usado para estabelecer conexão com os diversos servidores.

Contramedida: Configuração de uma rede de gerenciamento dedicada

Conecte todos os servidores dotados de processadores de serviço (SPs) a uma rede de gerenciamento dedicada. Essa configuração também é recomendada para os domínios do ambiente de execução. Caso eles estejam conectados a uma rede, hospede esses domínios em sua própria rede dedicada. *Não* conecte os domínios do ambiente de execução diretamente às redes atribuídas aos domínios de produção. Embora você possa realizar todo o trabalho administrativo por meio da única conexão de console disponibilizada pelo processador de serviço Oracle ILOM, essa configuração dificulta muito a administração tornando-a impraticável. A separação das redes de produção e de administração oferece proteção contra interceptação e manipulação. Esse tipo de separação também elimina a possibilidade de um ataque no ambiente de execução a partir dos domínios convidados na rede compartilhada.

FIGURA 5 Rede de gerenciamento dedicada



Oracle ILOM

Todos os sistemas Oracle SPARC atuais incluem um controlador do sistema incorporado (Oracle ILOM), com os seguintes recursos:

- Gerencia os controles ambientais básicos, como a velocidade do ventilador e a energia do chassi
- Permite atualizações de firmware
- Fornece o console do sistema para o domínio de controle

Você pode acessar o Oracle ILOM por meio de uma conexão serial ou usar SSH, HTTP, HTTPS, SNMP ou IPMI para acessá-lo por meio de uma porta de rede. Os Servidores Fujitsu M10 usam o XSCF, em vez do Oracle ILOM para executar funções semelhantes.

Ameaça: Negação de serviço do sistema completo

Um invasor que obtiver controle do Oracle ILOM poderá comprometer o sistema de várias maneiras, incluindo:

- Desligando todos os convidados em execução
- Instalando um firmware manipulado para obter acesso a pelo menos um domínio convidado

Esses cenários se aplicam a qualquer sistema que tenha um dispositivo controlador como esse. Em um ambiente virtualizado, o dano poderá ser bem maior do que em um ambiente físico porque vários domínios hospedados no mesmo compartimento do sistema estão em risco.

Da mesma maneira, um invasor que obtiver controle do domínio de controle ou de um domínio de E/S poderá desativar facilmente todos os domínios convidados dependentes encerrando os serviços de E/S correspondentes.

Avaliação: Negação de serviço do sistema completo

Em geral, o Oracle ILOM é conectado a uma rede administrativa que deve estar bem protegida e isolada das redes de produção normais.

Da mesma forma, um invasor poderá violar um domínio de serviço na rede ou por meio de um erro na pilha de virtualização e, em seguida, bloquear a E/S dos convidados ou executar um desligamento do sistema. Embora o dano seja limitado porque não há perda nem comprometimento dos dados, ele poderá afetar um grande número de domínios convidados. Portanto, é importante garantir a proteção contra a possibilidade dessa ameaça para limitar o dano potencial.

Contramedida: Proteção do Oracle ILOM

Como o processador de serviço do sistema, o Oracle ILOM controla os recursos críticos, como a energia do chassi, as configurações de inicialização do Oracle VM Server for SPARC e o acesso do console ao domínio de controle. As seguintes medidas ajudam a proteger o Oracle ILOM:

- Colocar a porta de rede do Oracle ILOM em um segmento de rede diferente da rede administrativa, que é usada para os domínios do ambiente de execução.
- Desativar todos os serviços desnecessários para a operação, como HTTP, IPMI, SNMP, HTTPS e SSH.
- Configurar contas de administrador dedicadas e pessoais que concedam somente os direitos necessários. Para aumentar a responsabilidade das ações executadas pelos administradores, certifique-se de criar contas de administrador pessoais. Esse tipo de acesso é importante

principalmente para acesso do console, atualizações de firmware e gerenciamento das configurações de inicialização.

Hypervisor

O hypervisor é a camada de firmware que implementa e controla a virtualização do hardware real. Ele inclui os seguintes componentes:

- O hypervisor real, que é implementado no firmware e suportado pelas CPUs do sistema.
- Os módulos de kernel executados no domínio de controle para configurar o hypervisor.
- Os módulos de kernel e os daemons executados nos domínios de E/S e de serviço para fornecer E/S virtualizada, bem como os módulos de kernel que se comunicam por meio de LDCs (Logical Domain Channels).
- Os módulos de kernel e os drivers de dispositivo executados nos domínios convidados para acessar dispositivos de E/S virtualizados, bem como os módulos de kernel que se comunicam por meio de LDCs.

Ameaça: Rompimento do isolamento

Um invasor poderá sequestrar os domínios convidados ou o sistema inteiro invadindo o ambiente de execução isolado fornecido pelo hypervisor. Potencialmente, essa ameaça poderá causar o dano mais grave de todos em um sistema.

Avaliação: Rompimento do isolamento

Um design de sistema modular poderá melhorar o isolamento concedendo níveis diferentes de privilégios aos domínios convidados, ao hypervisor e ao domínio de controle. Cada módulo funcional é implementado em um módulo de kernel, driver de dispositivo ou daemon diferente e configurável. Essa modularidade exige APIs e protocolos de comunicação simples, reduzindo o risco geral de erro.

Mesmo que a exploração de um erro pareça improvável, o dano potencial poderá fazer com que o invasor controle todo o sistema.

Contramedida: Validação de assinaturas de firmware e software

Mesmo que você possa baixar o firmware do sistema e os patches do SO diretamente de um site da Oracle, esses patches podem ser manipulados. Antes de instalar o software, verifique as somas de verificação MD5 dos pacotes de software. As somas de verificação de todos os softwares disponíveis para download são publicadas pela Oracle.

Contramedida: Validação dos módulos de kernel

O Oracle VM Server for SPARC usa vários drivers e módulos de kernel para implementar o sistema de virtualização geral. Todos os módulos de kernel e a maioria dos binários distribuídos com o SO Oracle Solaris têm uma assinatura digital. Use o utilitário `elfsign` para verificar a assinatura digital de cada driver e módulo de kernel. Você pode usar o comando `pkg verify` do Oracle Solaris 11 para verificar a integridade do binário do Oracle Solaris. Consulte `https://blogs.oracle.com/cmt/entry/solaris_fingerprint_database_how_it`.

Primeiro, você deve verificar a integridade do utilitário `elfsign`. Use o recurso BART (Basic Audit and Reporting Tool) para automatizar o processo de verificação de assinaturas digitais. O artigo 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`) descreve como combinar o recurso BART e o Solaris Fingerprint Database para executar automaticamente verificações de integridade semelhantes. Embora o Fingerprint Database tenha sido descontinuado, os conceitos descritos nesse documento podem ser aplicados para uso do utilitário `elfsign` e do recurso BART de maneira semelhante.

É possível usar o recurso de boot verificado como uma contramedida para a validação dos módulos Kernel. Para configurar a validação automática de módulos Kernel durante a inicialização, define as políticas de boot verificado no Oracle ILOM. Consulte os documentos referentes à sua plataforma específica em `http://docs.oracle.com/en/hardware/`. Para validar módulos Kernel no domínio de controle, defina as políticas de boot verificado no Oracle ILOM. Para validar módulos Kernel em domínios convidados, use o Logical Domains Manager para definir as políticas de boot verificado.

Domínio de controle

O domínio de controle, que geralmente tem as funções de um domínio de E/S e de um domínio de serviço, deve ser mantido em segurança, uma vez que ele pode modificar a configuração do hypervisor, que controla todos os recursos de hardware conectados.

Ameaça: Negação de serviço do domínio de controle

O desligamento do domínio de controle poderá resultar em uma negação de serviço das ferramentas de configuração. Como o domínio de controle é necessário somente para alterações de configuração, os domínios convidados não serão afetados se acessarem seus recursos de rede e disco por meio de outros domínios de serviço.

Ameaça: Negação de serviço do domínio de controle

Um ataque ao domínio de controle por meio da rede equivale a um ataque a qualquer instância do SO Oracle Solaris protegida de forma adequada. O dano causado por um desligamento ou uma negação de serviço semelhante do domínio de controle é relativamente baixo. Entretanto, os domínios convidados serão afetados se o domínio de controle também funcionar como um domínio de serviço para esses domínios.

Contramedida: Proteção do acesso do console

Evite configurar o acesso da rede administrativa aos domínios do ambiente de execução. Esse cenário exige que você utilize o serviço de console do Oracle ILOM para que o domínio de controle execute todas as tarefas de administração. O acesso do console a todos os outros domínios ainda é possível por meio do serviço `vntsd` executado no domínio de controle.

Considere essa opção com cuidado. Embora ela reduza o risco de um ataque na rede administrativa, somente um administrador poderá acessar o console de cada vez.

Para obter informações sobre como configurar de maneira segura o `vntsd`, consulte "How to Enable the Virtual Network Terminal Server Daemon" in *Oracle VM Server for SPARC 3.5 Administration Guide*.

Logical Domains Manager

O Logical Domains Manager é executado no domínio de controle e é usado para configurar o hypervisor, bem como para criar e configurar todos os domínios e os respectivos recursos de hardware. Certifique-se de que o uso do Logical Domains Manager seja registrado e monitorado.

Ameaça: Uso não autorizado dos utilitários de configuração

Um invasor poderá assumir o controle do ID de usuário de um administrador ou um administrador de um grupo diferente poderá obter acesso não autorizado a outro sistema.

Avaliação: Uso não autorizado dos utilitários de configuração

Certifique-se de que o administrador não tenha acesso desnecessário a um sistema implementando um gerenciamento de identidades mantido de forma adequada. Além disso, implemente um controle de acesso estrito e preciso, bem como outras medidas, como a regra de duas pessoas.

Contramedida: Aplicação da regra de duas pessoas

Considere implementar uma regra de duas pessoas para o Logical Domains Manager e outras ferramentas administrativas usando direitos. Essa regra oferece proteção contra ataques de engenharia social, contas administrativas comprometidas e erros humanos.

Contramedida: Uso de direitos para o Logical Domains Manager

O uso de direitos para o comando `ldm` permite implementar um controle de acesso preciso e manter total rastreabilidade. Para obter informações sobre a configuração de direitos, consulte o *Oracle VM Server for SPARC 3.5 Administration Guide*. O uso de direitos ajuda a proteger contra erros humanos porque nem todos os recursos do comando `ldm` são disponibilizados para todos os administradores.

Contramedida: Proteção do Logical Domains Manager

Desative os serviços desnecessários do gerenciador de domínios. O Logical Domains Manager fornece serviços de rede para acesso, monitoramento e migração de domínios. A desativação dos serviços de rede reduz a superfície de ataque do Logical Domains Manager ao mínimo necessário para seu funcionamento normal. Esse cenário combate ataques de negação de serviço e outras tentativas de usar indevidamente esses serviços de rede.

Observação - Embora a desativação dos serviços do gerenciador de domínios ajude a minimizar a superfície de ataque, não é possível saber antecipadamente todos os efeitos colaterais dessa ação em uma configuração.

Desative os seguintes serviços de rede quando eles não estiverem sendo usados:

- Serviço de migração na porta TCP `8101`

  Para desativar esse serviço, consulte a descrição das propriedades `ldmd/incoming_migration_enabled` e `ldmd/outgoing_migration_enabled` na página man `ldmd`(1M).
- Suporte ao protocolo XMPP (Extensible Messaging and Presence Protocol) na porta TCP `6482`

  Para obter informações sobre como desativar esse serviço consulte "XML Transport" in *Oracle VM Server for SPARC 3.5 Developer's Guide*.

  Desativar o XMPP impede o funcionamento de algumas ferramentas de gerenciamento e recursos chave do Oracle VM Server for SPARC. Consulte "Interface XML do Oracle VM Server for SPARC" [41].
- SNMP (Simple Network Management Protocol) na porta UDP `161`

Determine se deseja usar o Oracle VM Server for SPARC MIB (Management Information Base) para examinar os domínios. Esse recurso exige que o serviço SNMP esteja ativado. Com base em sua escolha, siga um destes procedimentos:

- **Ative o serviço SNMP para usar o Oracle VM Server for SPARC MIB.** Instale o Oracle VM Server for SPARC MIB com segurança. Consulte "How to Install the Oracle VM Server for SPARC MIB Software Package" in *Oracle VM Server for SPARC 3.5 Management Information Base User's Guide* e o Chapter 3, "Managing Security" in *Oracle VM Server for SPARC 3.5 Management Information Base User's Guide*.
- **Desative o serviço SNMP.** Para obter informações sobre como desativar esse serviço, consulte "How to Remove the Oracle VM Server for SPARC MIB Software Package" in *Oracle VM Server for SPARC 3.5 Management Information Base User's Guide*.

- Serviço de descoberta no endereço multicast `239.129.9.27` e na porta `64535`

Observação - Observe que esse mecanismo de descoberta também é usado pelo daemon `ldmd` para detectar colisões durante a atribuição automática de endereços MAC. Se você desativar o serviço de descoberta, a detecção de colisões de endereços MAC não funcionará e, portanto, a alocação automática desses endereços não funcionará corretamente.

Você *não poderá* desativar esse serviço enquanto o daemon Logical Domains Manager, `ldmd`, estiver em execução. Em vez disso, use o recurso Filtro de IP do Oracle Solaris para bloquear o acesso a esse serviço, o que minimizará a superfície de ataque do Logical Domains Manager. O bloqueio do acesso impede o uso não autorizado do utilitário, o que combate efetivamente os ataques de negação de serviço e outras tentativas de usar indevidamente esses serviços de rede. Consulte o Chapter 20, "IP Filter in Oracle Solaris (Overview)" in *Oracle Solaris Administration: IP Services* e "Using IP Filter Rule Sets" in *Oracle Solaris Administration: IP Services*.

Consulte também "Contramedida: Proteção do Oracle ILOM" [28].

Domínio de serviço

Um domínio de serviço fornece alguns serviços virtuais aos domínios convidados no sistema. Esses serviços podem incluir um serviço de switch virtual, disco virtual ou console virtual.

A Figura 6 mostra um exemplo de domínio de serviço que oferece serviços de console. Em geral, o domínio de controle hospeda os serviços de console e, portanto, também é um domínio de serviço. Os domínios do ambiente de execução geralmente combinam as funções de um domínio de controle, de um domínio de E/S e de um domínio de serviço em um ou dois domínios.

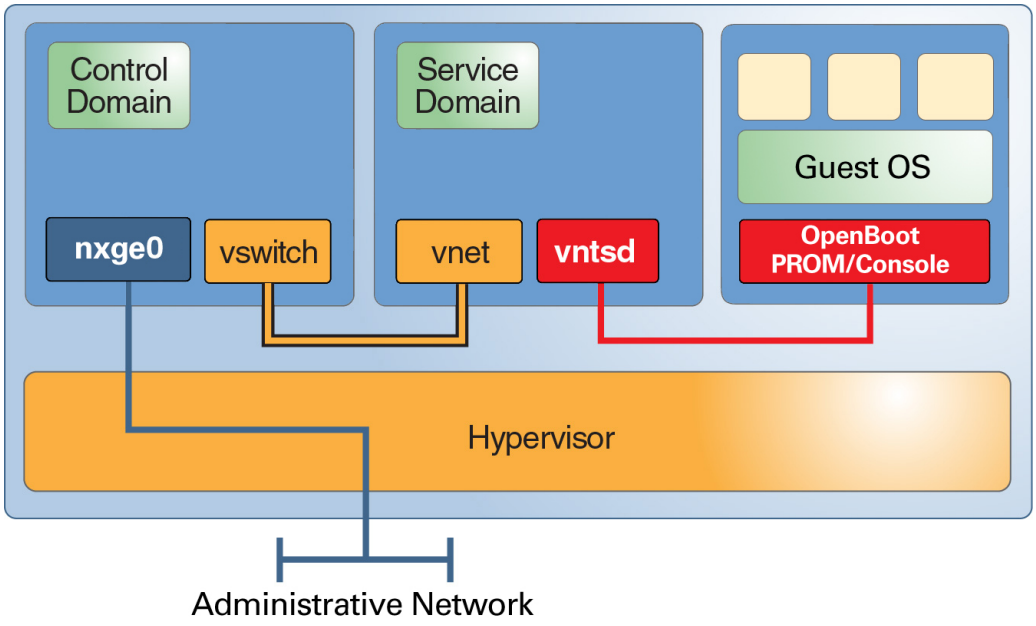
Ameaça: Manipulação de um domínio de serviço

Um invasor que obtiver controle de um domínio de serviço poderá manipular dados ou ter acesso a qualquer comunicação que ocorra por meio dos serviços oferecidos. Esse controle poderá incluir o acesso do console aos domínios convidados, o acesso a serviços de rede ou o acesso a serviços de disco.

Avaliação: Manipulação de um domínio de serviço

Embora as estratégias de ataque sejam as mesmas de um ataque no domínio de controle, o dano potencial é menor porque o invasor não pode modificar a configuração do sistema. O dano resultante poderá incluir o roubo ou a manipulação dos dados oferecidos pelo domínio de serviço, mas não a manipulação de quaisquer origens de dados. Dependendo do serviço, o invasor talvez precise trocar módulos de kernel.

FIGURA 6 Exemplo de domínio de serviço



Contramedida: Segregação granular de domínios de serviço

Se possível, faça com que cada domínio de serviço ofereça apenas *um* serviço aos seus respectivos clientes. Essa configuração garantirá que somente um serviço seja comprometido em caso de violação de um domínio de serviço. Entretanto, avalie a importância desse tipo de configuração em relação à complexidade adicional. Observe que a existência de domínios de E/S redundantes é altamente recomendável.

Contramedida: Isolamento de domínios de serviço e de domínios convidados

É possível isolar os domínios de serviço do Oracle Solaris 10 e do Oracle Solaris 11 dos domínios convidados. As soluções a seguir são mostradas na ordem preferencial de implementação:

- Certifique-se de que o domínio de serviço e o domínio convidado não compartilhem a mesma porta de rede. Além disso, não conecte uma interface de switch virtual ao domínio de serviço. Para os domínios de serviço do Oracle Solaris 11, não conecte VNICs às portas físicas usadas para switches virtuais.
- Caso deva usar a mesma porta de rede para os sistemas operacionais Oracle Solaris 10 e Oracle Solaris 11, coloque o tráfego do domínio de E/S em uma VLAN que não seja usada pelos domínios convidados.
- Se não for possível implementar nenhuma das soluções anteriores, não conecte o switch virtual ao sistema operacional Oracle Solaris 10 e aplique filtros de IP no sistema operacional Oracle Solaris 11.

Contramedida: Restrição do acesso a consoles virtuais

Certifique-se de que o acesso aos consoles virtuais individuais esteja limitado *somente* aos usuários que devem acessá-los. Essa configuração garantirá que nenhum administrador tenha acesso a todos os consoles, o que impede o acesso a consoles diferentes dos atribuídos a uma conta comprometida. Consulte “How to Create Default Services” in *Oracle VM Server for SPARC 3.5 Administration Guide*.

Domínio de E/S

Qualquer domínio que tenha acesso direto a dispositivos físicos de E/S, como portas de rede ou discos, é um domínio de E/S. Para obter informações sobre como configurar domínios de E/S, consulte o Chapter 6, “Configuring I/O Domains” in *Oracle VM Server for SPARC 3.5 Administration Guide*.

Um domínio de E/S também poderá ser um domínio de serviço caso forneça serviços de E/S a domínios convidados, o que permitirá o acesso dos domínios ao hardware.

Ameaça: Ataque de negação de serviço de um domínio de E/S ou de serviço

Um invasor que bloquear os serviços de E/S de um domínios de E/S fará com que todos os domínios convidados dependentes sejam igualmente bloqueados. Um ataque de negação de serviço bem-sucedido poderá ser alcançado por meio da sobrecarga da infraestrutura de disco ou da rede de back-end ou por meio da introdução de um erro no domínio. Ambos os ataques podem fazer com que o domínio pare ou dispare um alerta. Da mesma forma, um invasor que suspender os serviços de um domínio de serviço fará com que os domínios convidados que dependem desses serviços parem imediatamente. Se o domínio convidado parar, sua operação será retomada quando o serviço de E/S reiniciar.

Avaliação: Ataque de negação de serviço de um domínio de E/S ou de serviço

Normalmente os ataques de negação de serviço são executados na rede. Esses ataques podem ser bem-sucedidos porque as portas de rede estão abertas para comunicação e podem ficar saturadas com o tráfego da rede. Uma perda resultante de serviço bloqueará os domínios convidados dependentes. Um ataque semelhante nos recursos de disco poderá ocorrer por meio da infraestrutura de SAN ou de um ataque ao domínio de E/S. O único dano é uma interrupção temporária de todos os domínios convidados dependentes. Embora o impacto das tarefas de negação de serviço possa ser significativo, os dados não são comprometidos nem perdidos, e a configuração do sistema permanece intacta.

Contramedida: Configuração granular de domínios de E/S

A configuração de vários domínios de E/S reduz o impacto de uma falha ou comprometimento de um domínio. Você pode atribuir slots PCIe individuais a um domínio convidado para dotá-lo dos recursos de um domínio de E/S. Se ocorrer uma falha no domínio raiz que possui o barramento PCIe, esse barramento será redefinido, o que levará a uma falha subsequente do domínio atribuído ao slot individual. Esse recurso não elimina totalmente a necessidade de existirem dois domínios raiz, cada um com um barramento PCIe separado.

Contramedida: Configuração de hardware e domínios raiz redundantes

A alta disponibilidade também contribui para maior segurança, pois garante que os serviços suportem ataques de negação de serviço. O Oracle VM Server for SPARC implementa

metodologias de alta disponibilidade, como o uso de recursos de disco e rede redundantes em domínios de E/S redundantes. Essa opção de configuração permite atualizações dinâmicas dos domínios de E/S e oferece proteção contra o impacto de uma falha em um domínio de E/S devido a um ataque de negação de serviço bem-sucedido. Com o advento do SR-IOV, os domínios convidados podem ter acesso direto a dispositivos de E/S individuais. Entretanto, quando o SR-IOV não for uma opção, considere a criação de domínios de E/S redundantes. Consulte “Contramedida: Segregação granular de domínios de serviço” [35].

Ameaça: Manipulação de um domínio de E/S

Um domínio de E/S tem acesso direto a dispositivos de back-end, geralmente discos, os quais ele virtualiza e oferece aos domínios convidados. Um invasor bem-sucedido terá total acesso a esses dispositivos e poderá ler dados confidenciais ou manipular o software nos discos de inicialização dos domínios convidados.

Avaliação: Manipulação de um domínio de E/S

A probabilidade de um ataque em um domínio de E/S é a mesma de um ataque bem-sucedido em um domínio de serviço ou de controle. O domínio de E/S é um alvo atraente devido ao acesso potencial a um grande número de dispositivos de disco. Portanto, considere essa ameaça ao lidar com dados confidenciais em um domínio convidado executado em discos virtualizados.

Contramedida: Proteção de discos virtuais

Quando um domínio de E/S é comprometido, o invasor tem total aceso aos discos virtuais do domínio convidado.

Proteja o conteúdo dos discos virtuais da seguinte maneira:

- **Criptografando o conteúdo dos discos virtuais.** Nos sistemas Oracle Solaris 10, você poderá usar um aplicativo que criptografa seus próprios dados, como o `pgp`/`gpg` ou os tablespaces criptografados do Oracle 11g. Nos sistemas Oracle Solaris 11, você poderá usar conjuntos de dados criptografados pelo ZFS para permitir a criptografia transparente de todos os dados armazenados no sistema de arquivos.
- **Distribuindo os dados por vários discos virtuais em diferentes domínios de E/S.** Um domínio convidado poderá criar um volume distribuído (RAID 1/RAID 5) por vários discos virtuais obtidos de dois domínios de E/S. Se um desses domínios de E/S for comprometido, o invasor terá dificuldade de usar a parte dos dados disponível.

Domínios convidados

Embora os domínios convidados não façam parte do ambiente de execução, eles são o alvo mais provável de um ataque uma vez que estão conectados à rede. Um invasor que violar um sistema virtualizado poderá iniciar ataques no ambiente de execução.

Contramedida: Proteção do sistema operacional do domínio convidado

O sistema operacional do domínio convidado é geralmente a primeira linha de defesa contra qualquer ataque. Com exceção dos ataques que têm origem no datacenter, um invasor poderá invadir um domínio convidado que tenha conexões externas antes de tentar romper o isolamento desse domínio e capturar o ambiente completo. Portanto, é necessário proteger o sistema operacional do domínio convidado.

Para aumentar a proteção do sistema operacional, você poderá implantar seu aplicativo no Solaris Zones, o que introduzirá uma camada adicional de isolamento entre o serviço de rede do aplicativo e o sistema operacional do domínio convidado. Um ataque bem-sucedido ao serviço comprometerá apenas a zona, e não o sistema operacional subjacente, impedindo que o invasor expanda seu controle para além dos recursos alocados para a zona. Como resultado, será mais difícil romper o isolamento do convidado. Para obter informações sobre como proteger o sistema operacional convidado, consulte *Oracle Solaris 10 Security Guidelines* e *Oracle Solaris 11 Security Guidelines*.

♦ ♦ ♦ CAPÍTULO 2

Instalação e configuração seguras do Oracle VM Server for SPARC

Este capítulo descreve as considerações de segurança relacionadas à instalação e à comfiguração do software Oracle VM Server for SPARC.

Instalação

O software Oracle VM Server for SPARC é instalado automaticamente de forma segura como um pacote Oracle Solaris 11. Uma vez concluída a instalação, você deverá ter privilégios de administrador para configurar os domínios com os direitos e os recursos de autorização. Esses recursos não estão ativados por padrão.

Configuração pós-instalação

Execute as seguintes tarefas após instalar o software Oracle VM Server for SPARC para garantir um uso mais seguro:

- Configure o domínio de controle com os serviços virtuais de E/S necessários, como serviços de switch virtual, servidor de disco virtual e VCC (virtual console concentrator). Consulte o Chapter 3, “Setting Up Services and the Control Domain” in *Oracle VM Server for SPARC 3.5 Administration Guide*.
- Configure os domínios convidados. Consulte o Chapter 4, “Setting Up Guest Domains” in *Oracle VM Server for SPARC 3.5 Administration Guide*.

  Você pode usar um switch virtual para configurar os domínios convidados por meio de uma rede administrativa e de uma rede de produção. Nesse caso, um switch virtual será criado com o uso da interface da rede de produção como o dispositivo de rede de switch virtual. Consulte “Contramedida: Configuração de uma rede de gerenciamento dedicada” [26].

  A segurança de um domínio convidado torna-se comprometida quando quaisquer de seus discos virtuais são comprometidos. Portanto, certifique-se de que os discos virtuais

(armazenamentos de rede anexados, arquivos de imagem do disco armazenados localmente ou discos físicos) estejam armazenados em um local seguro.

O daemon `vntsd` está desativado por padrão. Quando esse daemon está ativado, todos os usuários que fizeram login no domínio de controle podem se conectar ao console de um domínio convidado. Para evitar esse tipo de acesso, verifique se o daemon `vntsd` está desativado ou use direitos para limitar o acesso de conectividade do console *somente* aos usuários autorizados.

- Por padrão, o processador de serviço (SP) é configurado de forma segura. Para obter informações sobre como usar o software Oracle Integrated Lights Out Management (Oracle ILOM) para gerenciar o SP, consulte a documentação referente à sua plataforma em `http://www.oracle.com/technetwork/documentation/sparc-tseries-servers-252697.html`.

♦ ♦ ♦ CAPÍTULO 3

Considerações de segurança para desenvolvedores

Este capítulo fornece informações para os desenvolvedores que produzem aplicativos para o software Oracle VM Server for SPARC.

Interface XML do Oracle VM Server for SPARC

Você pode criar programas externos que interagem com o software Oracle VM Server for SPARC por meio do mecanismo de comunicação XML (Extensible Markup Language). O XML usa o XMPP (Extensible Messaging and Presence Protocol). A interface XML é compatível apenas com o protocolo TLS (Transport Layer Security) versão 1.2.

Como um invasor pode tentar explorar esse protocolo de rede para acessar um sistema, considere desativar o XMPP. Para obter informações sobre como desativar o XMPP, consulte "XML Transport" in *Oracle VM Server for SPARC 3.5 Developer's Guide*. Para obter informações sobre os mecanismos de segurança usados pelo Logical Domains Manager, consulte "XMPP Server" in *Oracle VM Server for SPARC 3.5 Developer's Guide*.

Desativar o XMPP impede que o Oracle VM Manager ou o Ops Center gerencie o sistema e impede que você use alguns recursos chave do Oracle VM Server for SPARC como os seguintes comandos:

- `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`

♦ ♦ ♦ APÊNDICE A

Lista de verificação de implantação segura

Esta lista de verificação resume as etapas a serem tomadas para proteger o ambiente Oracle VM Server for SPARC. Os detalhes são fornecidos em outros documentos, incluindo:

- *Oracle VM Server for SPARC 3.5 Administration Guide*
- *Oracle Solaris 10 Security Guidelines*
- *Oracle Solaris 11 Security Guidelines*

Lista de verificação de segurança do Oracle VM Server for SPARC

- Execute as etapas de proteção do SO Oracle Solaris para seus domínios convidados da mesma maneira que em um ambiente não virtualizado.
- Use os perfis de direitos Gerenciamento de LDoms e Revisão de LDoms para delegar os privilégios apropriados aos usuários.
- Use direitos para restringir o acesso ao console de domínios que *somente* você, como administrador do Oracle VM Server for SPARC, deve acessar.
- Desative os serviços desnecessários do gerenciador de domínios.
- Implante somente domínios convidados da mesma classe de segurança em uma plataforma física.
- Verifique se não há conexões de rede entre a rede administrativa do ambiente de execução e os domínios convidados.
- Atribua somente os recursos necessários aos domínios convidados.