Oracle® VM Server for SPARC 3.1 Security Guide

Part No: E38407
August 2013

ORACLE

130819@25097

Contents

Preface 5

1 Oracle VM Server for SPARC Security Overview 7
Security Features Used by Oracle VM Server for SPARC 7
Oracle VM Server for SPARC Product Overview 8
Applying General Security Principles to Oracle VM Server for SPARC 11
Security in a Virtualized Environment 13
Execution Environment 13
Securing the Execution Environment 14
Defending Against Attacks 14
Operational Environment 16
Execution Environment 20
ILOM 23
Hypervisor 24
Control Domain 26
Logical Domains Manager 26
Service Domain 29
I/O Domain 30
Guest Domains 32

2 Secure Installation and Configuration of Oracle VM Server for SPARC 33
Installation 33
Postinstallation Configuration 33

3 Security Considerations for Developers 35
Oracle VM Server for SPARC XML Interface 35

A Secure Deployment Checklist 37
Oracle VM Server for SPARC Security Checklist 37

Preface

Oracle VM Server for SPARC 3.1 Security Guide includes information about how to securely install, configure, and use the Oracle VM Server for SPARC 3.1 software.

Product Documentation Library

Late-breaking information and known issues for this product are included in the documentation library at `http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html`.

The following table shows the documentation that is available for the Oracle VM Server for SPARC 3.1 release. These documents are available in both HTML and PDF formats unless otherwise indicated.

TABLE P–1 Related Documentation

Application	Title
Oracle VM Server for SPARC 3.1 Software	*Oracle VM Server for SPARC 3.1 Administration Guide* *Oracle VM Server for SPARC 3.1 Security Guide* *Oracle VM Server for SPARC 3.1 Reference Manual* *Oracle VM Server for SPARC 3.1 Release Notes*
Oracle VM Server for SPARC 3.1 `drd`(1M) and `vntsd`(1M) man pages	Oracle Solaris OS Reference Manuals: ■ Oracle Solaris 10 Documentation (`http://www.oracle.com/technetwork/documentation/solaris-10-192992.html`) ■ Oracle Solaris 11.1 Documentation (`http://docs.oracle.com/cd/E26502_01`)
Oracle Solaris OS: Installation and Configuration	Oracle Solaris OS Installation and Configuration Guides: ■ Oracle Solaris 10 Documentation (`http://www.oracle.com/technetwork/documentation/solaris-10-192992.html`) ■ Oracle Solaris 11.1 Documentation (`http://docs.oracle.com/cd/E26502_01`)

TABLE P–1 Related Documentation *(Continued)*

Application	Title
Oracle VM Server for SPARC and Oracle Solaris OS Security	Oracle VM Server for SPARC White Paper and Oracle Solaris OS Security Guides: ■ *Secure Deployment of Oracle VM Server for SPARC* (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/secure-ovm-sparc-deployment-294062.pdf`) ■ *Oracle Solaris 10 Security Guidelines* ■ *Oracle Solaris 11 Security Guidelines*

You can find documentation that relates to your server or software or the Oracle Solaris OS at `http://www.oracle.com/technetwork/indexes/documentation/index.html`. Use the Search box to find the documents and the information that you need.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program web site at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Feedback

Provide feedback about this documentation at `http://www.oracle.com/goto/docfeedback`.

◆ ◆ ◆ CHAPTER 1

Oracle VM Server for SPARC Security Overview

Although the number of security recommendations in this document might give a different impression, the typical Oracle VM Server for SPARC installation is already well secured against unauthorized use. A small attack surface exists and some degree of risk remains, even if exploitation is unlikely. Just as you might choose to add a burglar alarm to the protection of your home to supplement standard deterrents like locks on your doors, additional network security measures can help reduce the chance of unanticipated problems occurring or minimize the potential damage.

This chapter covers the following Oracle VM Server for SPARC security topics:

- "Security Features Used by Oracle VM Server for SPARC" on page 7
- "Oracle VM Server for SPARC Product Overview" on page 8
- "Applying General Security Principles to Oracle VM Server for SPARC" on page 11
- "Security in a Virtualized Environment" on page 13
- "Defending Against Attacks" on page 14

Security Features Used by Oracle VM Server for SPARC

The Oracle VM Server for SPARC software is a virtualization product that permits multiple Oracle Solaris virtual machines (VMs) to run on one physical system, each with its own Oracle Solaris 10 or Oracle Solaris 11 OS installed. Each VM is also called a *logical domain*. Domains are independent instances and can run different versions of the Oracle Solaris OS as well as different application software. For example, domains might have different package revisions installed, different services enabled, and system accounts with different passwords. See *Oracle Solaris 10 Security Guidelines* and *Oracle Solaris 11 Security Guidelines* for information about Oracle Solaris security.

The `ldm` command invokes the Logical Domains Manager and must be run on the control domain to configure domains and to retrieve state information. Limiting access to the control domain and to the `ldm` command is critical for the security of the domains that run on the system. To limit access to domain configuration data, use the Oracle VM Server for SPARC

security features such as Oracle Solaris rights for consoles and `solaris.ldoms` authorizations. See "Logical Domains Manager Profile Contents" in *Oracle VM Server for SPARC 3.1 Administration Guide*.

The Oracle VM Server for SPARC software uses the following security features:

- The security features that are available in the Oracle Solaris 10 OS and the Oracle Solaris 11 OS are also available on domains that run the Oracle VM Server for SPARC software. See *Oracle Solaris 10 Security Guidelines* and *Oracle Solaris 11 Security Guidelines*.
- The Oracle Solaris OS security features can be applied to the Oracle VM Server for SPARC software. For comprehensive information about ensuring Oracle VM Server for SPARC security, see "Security in a Virtualized Environment" on page 13 and "Defending Against Attacks" on page 14.
- The Oracle Solaris 10 OS and the Oracle Solaris 11 OS include security fixes that are available for your system. Obtain Oracle Solaris 10 OS fixes as security patches or updates. Obtain Oracle Solaris 11 OS fixes as Support Repository Updates (SRUs).
- For information about how to limit access to the Oracle VM Server for SPARC administration commands and domain consoles, and to enable the Oracle VM Server for SPARC auditing feature, see Chapter 3, "Oracle VM Server for SPARC Security," in *Oracle VM Server for SPARC 3.1 Administration Guide*.

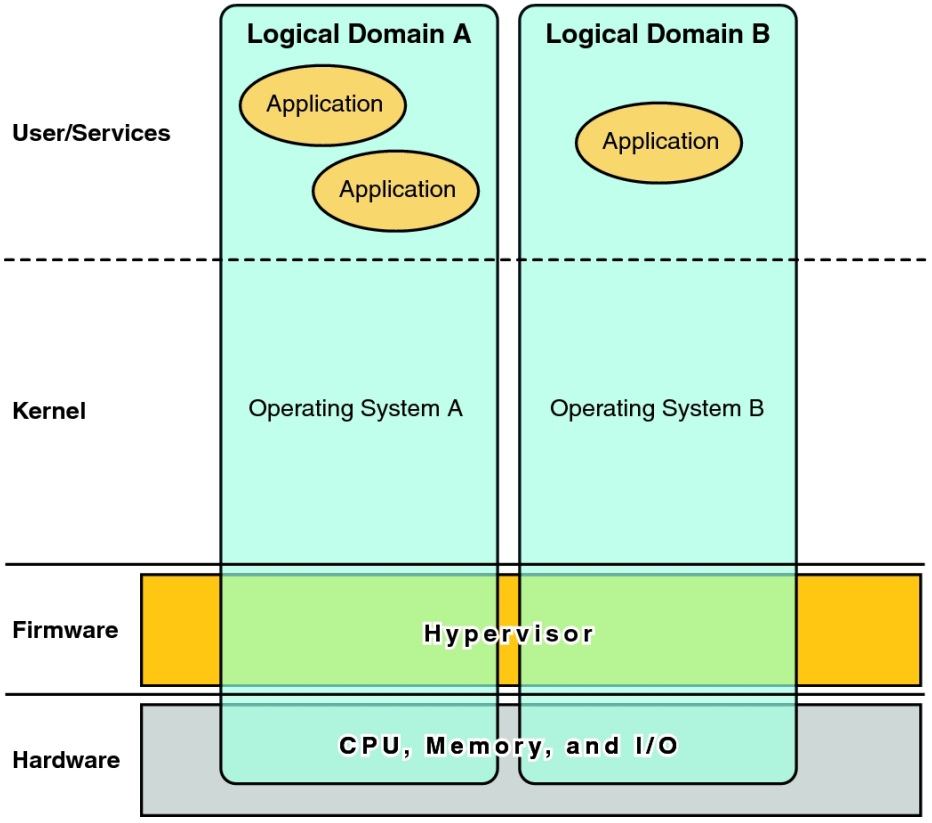
Oracle VM Server for SPARC Product Overview

Oracle VM Server for SPARC provides highly efficient, enterprise-class virtualization capabilities for Oracle's SPARC T-Series servers as well as the SPARC M5 server and Fujitsu M10 systems. Using the Oracle VM Server for SPARC software, you can create many virtual servers, called logical domains, on a single system. This kind of configuration enables you to take advantage of the massive thread scale offered by these SPARC servers and the Oracle Solaris OS.

A *logical domain* is a virtual machine that contains a discrete logical grouping of resources. A logical domain has its own operating system and identity within a single computer system. Each logical domain can be created, destroyed, reconfigured, and rebooted independently, without requiring you to perform a power cycle of the server. You can run a variety of application software in different logical domains and keep them independent for performance and security purposes.

For information about using the Oracle VM Server for SPARC software, see *Oracle VM Server for SPARC 3.1 Administration Guide* and *Oracle VM Server for SPARC 3.1 Reference Manual*. For information about the required hardware and software, see *Oracle VM Server for SPARC 3.1 Release Notes*.

FIGURE 1–1 Hypervisor Supporting Two Logical Domains



The Oracle VM Server for SPARC software uses the following components to provide system virtualization:

- **Hypervisor.** The hypervisor is a small firmware layer that provides a stable virtualized machine architecture to which an operating system can be installed. Oracle's Sun servers that use the hypervisor provide hardware features to support the hypervisor's control over the operating system activities on a logical domain.

  The number of domains and the capabilities of each domain that a specific SPARC hypervisor supports are server-dependent features. The hypervisor can allocate subsets of the server's CPU, memory, and I/O resources to a given logical domain. This allocation enables the support of multiple operating systems simultaneously, each within its own logical domain. Resources can be rearranged between separate logical domains with an arbitrary granularity. For example, CPUs are assignable to a logical domain with the granularity of a CPU thread.

The *service processor* (SP), also known as the *system controller* (SC), monitors and runs the physical machine. The Logical Domains Manager, and not the SP, manages the logical domains themselves.

- **Control domain.** The Logical Domains Manager runs in this domain and enables you to create and manage other logical domains and to allocate virtual resources to other domains. You can have only one control domain per server. The control domain is the first domain that is created when you install the Oracle VM Server for SPARC software. The control domain is named `primary`.
- **Service domain.** A service domain provides virtual device services to other domains such as a virtual switch, a virtual console concentrator, and a virtual disk server. Any domain can be configured as a service domain.
- **I/O domain.** An I/O domain has direct access to physical I/O devices such as a network card in a PCI EXPRESS (PCIe) controller. An I/O domain can own a PCIe root complex or it can own a PCIe slot or on-board PCIe device by using the direct I/O (DIO) feature. See "Creating an I/O Domain by Assigning PCIe Endpoint Devices" in *Oracle VM Server for SPARC 3.1 Administration Guide*.

  An I/O domain can share physical I/O devices with other domains in the form of virtual devices when the I/O domain is also used as a service domain.
- **Root domain.** A root domain has a PCIe root complex assigned to it. This domain owns the PCIe fabric of that root complex and provides all fabric-related services such as fabric error handling. A root domain is also an I/O domain, as it owns and has direct access to physical I/O devices.

  The number of root domains that you can have depends on your platform architecture. For example, if you are using a SPARC T4-4 server from Oracle, you can have up to four root domains.
- **Guest domain.** A guest domain is a non-I/O domain that consumes virtual device services that are provided by one or more service domains. A guest domain does not have any physical I/O devices. It has only virtual I/O devices such as virtual disks and virtual network interfaces.

Often, an Oracle VM Server for SPARC system has only a control domain that provides the services that are performed by I/O domains and service domains. To improve redundancy and platform serviceability, consider configuring more than one I/O domain on your Oracle VM Server for SPARC system.

Applying General Security Principles to Oracle VM Server for SPARC

You can configure guest domains in a variety of ways to provide varying levels of guest domain isolation, hardware sharing, and domain connectivity. These factors contribute to the security level of the overall Oracle VM Server for SPARC configuration. For recommendations about deploying the Oracle VM Server for SPARC software in a secure manner, see "Security in a Virtualized Environment" on page 13 and "Defending Against Attacks" on page 14.

You can apply some of the following general security principles:

- **Minimize the attack surface.**
  - Minimize unintentional configuration errors by creating operational guidelines that enable you to regularly evaluate the security of the system. See "Countermeasure: Creating Operational Guidelines" on page 16.
  - Carefully plan the architecture of the virtual environment to maximize the isolation of the domains. See the countermeasures described for "Threat: Errors in the Architecture of the Virtual Environment" on page 17.
  - Carefully plan which resources to assign and whether they are to be shared. See "Countermeasure: Carefully Assigning Hardware Resources" on page 19 and "Countermeasure: Carefully Assigning Shared Resources" on page 20.
  - Ensure that the logical domains are protected from manipulation by applying the countermeasures described for "Threat: Manipulation of the Execution Environment" on page 20 and "Countermeasure: Securing the Guest Domain OS" on page 32.
    - "Countermeasure: Securing Interactive Access Paths" on page 21.
    - "Countermeasure: Minimizing the Oracle Solaris OS" on page 21.
    - "Countermeasure: Hardening the Oracle Solaris OS" on page 21.
    - "Countermeasure: Hardening the Logical Domains Manager" on page 27.
    - "Countermeasure: Using Role Separation and Application Isolation" on page 21 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. You should run applications that can be run by other systems on guest domains that are designed for this purpose.
    - "Countermeasure: Configuring a Dedicated Management Network" on page 22 describes a more advanced network configuration that connects servers with SPs to a dedicated management network to shield the SP from network access.
  - Expose a guest domain to the network *only* when necessary. You can use virtual switches to limit a guest domain's network connectivity to *only* the appropriate networks.

- Follow the steps to minimize the attack surface for Oracle Solaris 10 and Oracle Solaris 11 as described in *Oracle Solaris 10 Security Guidelines* and *Oracle Solaris 11 Security Guidelines*.
- Protect the core of the hypervisor as described by "Countermeasure: Validating Firmware and Software Signatures" on page 25 and "Countermeasure: Validating Kernel Modules" on page 25.
- Protect the control domain against denial-of-service attacks. See "Countermeasure: Securing Console Access" on page 26.
- Ensure that the Logical Domains Manager cannot be run by unauthorized users. See "Threat: Unauthorized Use of Configuration Utilities" on page 26.
- Ensure that the service domain cannot be accessed by unauthorized users or processes. See "Threat: Manipulation of a Service Domain" on page 29.
- Protect an I/O domain or a service domain against denial-of-service attacks. See "Threat: Experiencing a Denial-of-Service of an I/O Domain or a Service Domain" on page 30.
- Ensure that an I/O domain cannot be accessed by unauthorized users or processes. See "Threat: Manipulation of an I/O Domain" on page 31.
- Disable unnecessary domain manager services. The Logical Domains Manager provides network services for domain access, monitoring, and migration. See "Countermeasure: Hardening the Logical Domains Manager" on page 27 and "Countermeasure: Securing the ILOM" on page 24.
- **Provide the least privilege to perform an operation.**
  - Isolate systems into *security classes*, which are groups of individual guest systems that share the same security requirements and privileges. By assigning only guest domains from a single security class to a single hardware platform, you create an isolation barrier, which prevents the domains from crossing into a different security class. See "Countermeasure: Carefully Assigning Guests to Hardware Platforms" on page 17.
  - Use rights to restrict the capability to manage domains with the `ldm` command. *Only* those users who must administer domains should be given this capability. Assign a role that uses the LDoms Management rights profile to users who require access to all of the `ldm` subcommands. Assign a role that uses the LDoms Review rights profile to users who only require access to the list-related `ldm` subcommands. See "Using Rights Profiles and Roles" in *Oracle VM Server for SPARC 3.1 Administration Guide*.
  - Use rights to restrict access to the console of *only* those domains that you, as the administrator of Oracle VM Server for SPARC, administer. Do *not* permit general access to all domains. See "Controlling Access to a Domain Console by Using Rights" in *Oracle VM Server for SPARC 3.1 Administration Guide*.
- **Monitor system activity.**

  Enable Oracle VM Server for SPARC auditing. See "Enabling and Using Auditing" in *Oracle VM Server for SPARC 3.1 Administration Guide*.

Security in a Virtualized Environment

To effectively secure your Oracle VM Server for SPARC virtualized environment, secure the operating system and each service that runs in each domain. To reduce the effects of a successful breach, separate services by deploying them to different domains.

The Oracle VM Server for SPARC environment uses a hypervisor to virtualize CPU, memory, and I/O resources for logical domains. Each domain is a discrete virtualized server that you must secure against potential attacks.

A virtualized environment enables you to consolidate several servers into one server by means of hardware resource sharing. In Oracle VM Server for SPARC, CPU and memory resources are allocated exclusively to each domain, which prevents abuse through excessive CPU usage or memory allocation. Disk and network resources are typically provided by service domains to many guest domains.

When evaluating security, *always* assume that your environment has a flaw that an attacker can exploit. For example, an attacker might exploit a weakness in the hypervisor to hijack the entire system, including its guest domains. So, *always* deploy systems to minimize the risk of damage in the case of a breach.

Execution Environment

The execution environment includes the following components:

- **Hypervisor –** Platform-specific firmware that virtualizes hardware and relies heavily on the hardware support that is built into the CPU.
- **Control domain –** A specialized domain that configures the hypervisor and runs the Logical Domains Manager, which manages the logical domains.
- **I/O domain or root domain –** A domain that owns some or all of the platform's available I/O devices and shares them with other domains.
- **Service domain –** A domain that offers services to other domains. A service domain might provide console access to other domains or provide virtual disks. A service domain that provides virtual disk access to other domains is also an I/O domain.

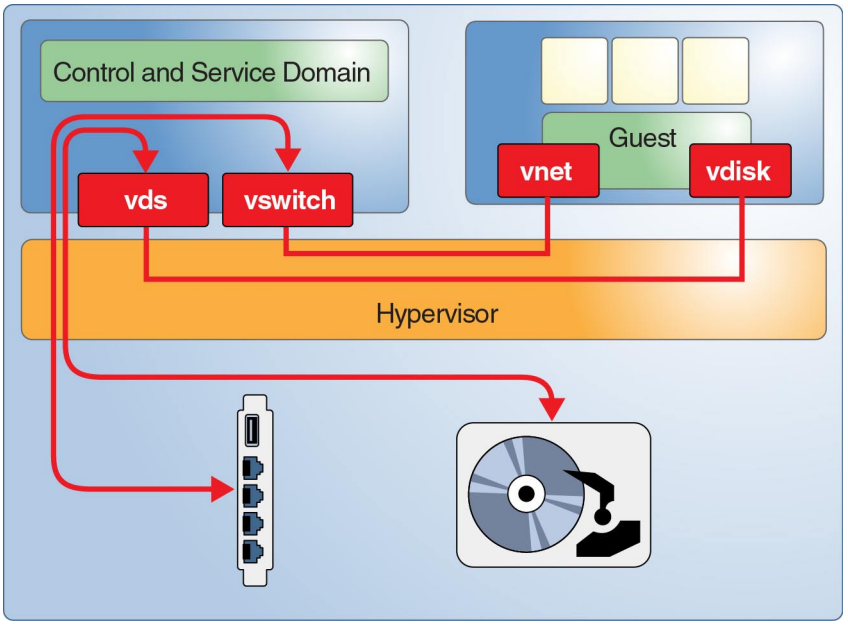
For more information about these components, see Figure 1–1 and the more detailed component descriptions.

You can improve serviceability for redundant I/O configurations by configuring a second I/O domain. You can also use a second I/O domain to isolate the hardware from security breaches. For information about configuration options, see *Oracle VM Server for SPARC 3.1 Administration Guide*.

Securing the Execution Environment

Oracle VM Server for SPARC has several attack targets in the execution environment. Figure 1–2 shows a simple Oracle VM Server for SPARC configuration where the control domain provides network and disk services to a guest domain. These services are implemented by means of daemons and kernel modules that run in the control domain. The Logical Domains Manager assigns Logical Domain Channels (LDCs) for each service and a client to facilitate a point-to-point communication between them. An attacker might exploit an error in any of the components to break the isolation of the guest domains. For example, an attacker might execute arbitrary code in the service domain or might disrupt normal operations on the platform.

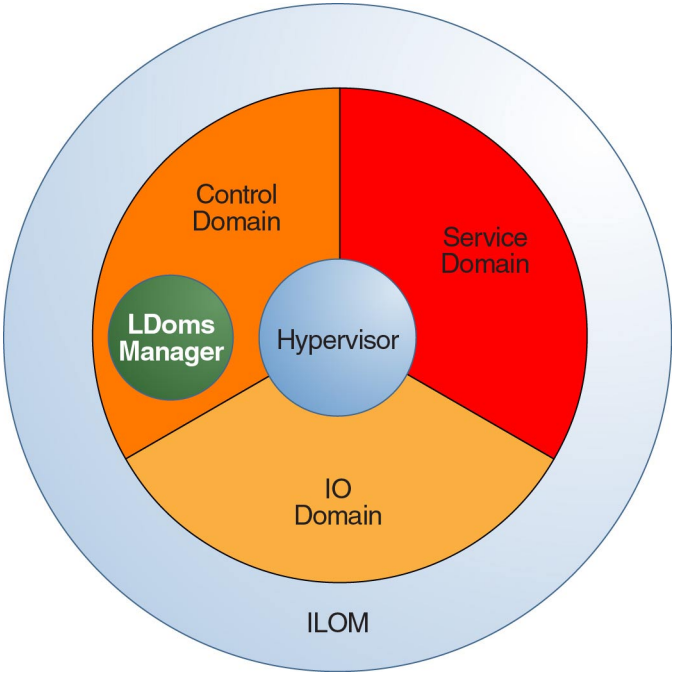
FIGURE 1–2 Sample of Oracle VM Server for SPARC Environment



Defending Against Attacks

The following figure shows the virtualization components that form the Oracle VM Server for SPARC "execution environment." These components are not strictly separated. The most simple configuration is to combine all of these functions in a single domain. The control domain might also act as an I/O domain and a service domain for other domains.

FIGURE 1–3 Components of the Execution Environment



Suppose an attacker attempts to break system isolation and then manipulate the hypervisor or another component of the execution environment to reach a guest domain. You must protect each guest domain as you would any stand-alone server.

The rest of this chapter presents threat possibilities and the various measures that you can take to counter them. Each of these attacks attempt to overcome or eliminate the isolation of the different domains that run on a single platform. The following sections describe the threats to each part of an Oracle VM Server for SPARC system:

- "Operational Environment" on page 16
- "Execution Environment" on page 20
- "ILOM" on page 23
- "Hypervisor" on page 24
- "Control Domain" on page 26
- "Logical Domains Manager" on page 26
- "I/O Domain" on page 30
- "Service Domain" on page 29
- "Guest Domains" on page 32

Operational Environment

The operational environment includes physical systems and their components, datacenter architects, administrators, and members of the IT organization. A security breach can occur at any point in the operational environment.

Virtualization places a layer of software between the actual hardware and the guest domains that run the production services, which increases complexity. As a result, you must carefully plan and configure the virtual system and beware of human error. Also, beware of attempts by attackers to gain access to the operational environment by using "social engineering."

The following sections describe the distinctive threats that you can counter at the operational environment level.

Threat: Unintentional Misconfiguration

The primary security concern for a virtualized environment is to sustain server isolation by separating network segments, segregating administrative access, and deploying servers to security classes, which are groups of domains that have the same security requirements and privileges.

Carefully configure virtual resources to avoid some of the following errors:

- Creating unnecessary communication channels between production guest domains and the execution environment
- Creating unnecessary access to network segments
- Creating unintentional connections between discrete security classes
- Unintentionally migrating a guest domain to the wrong security class
- Allocating insufficient hardware, which might lead to unexpected resource overloading
- Assigning disks or I/O devices to the wrong domain

Countermeasure: Creating Operational Guidelines

Before you begin, carefully define the operational guidelines for your Oracle VM Server for SPARC environment. These guidelines describe the following tasks to perform and how to perform them:

- Managing patches for all components of the environment
- Enabling the well-defined, traceable, and secure implementation of changes
- Checking log files at a regular interval
- Monitoring the integrity and availability of the environment

Regularly perform checks to ensure that these guidelines remain up to date and adequate, and to verify that these guidelines are being followed in everyday operations.

In addition to these guidelines, you can take several more technical measures to reduce the risk of unintentional actions. See "Logical Domains Manager" on page 26.

Threat: Errors in the Architecture of the Virtual Environment

When moving a physical system to a virtualized environment, you can usually keep the storage configuration as-is by reusing the original LUNs. However, the network configuration must be adapted to the virtualized environment and the resulting architecture might differ considerably from the architecture used on the physical system.

You must consider how to maintain the isolation of the discrete security classes and their needs. Also, consider the shared hardware of the platform and shared components such as network switches and SAN switches.

To maximize security for your environment, ensure that you maintain the isolation of guest domains and security classes. When you design the architecture, anticipate possible errors and attacks and implement lines of defense. A good design helps to confine potential security issues while managing complexity and cost.

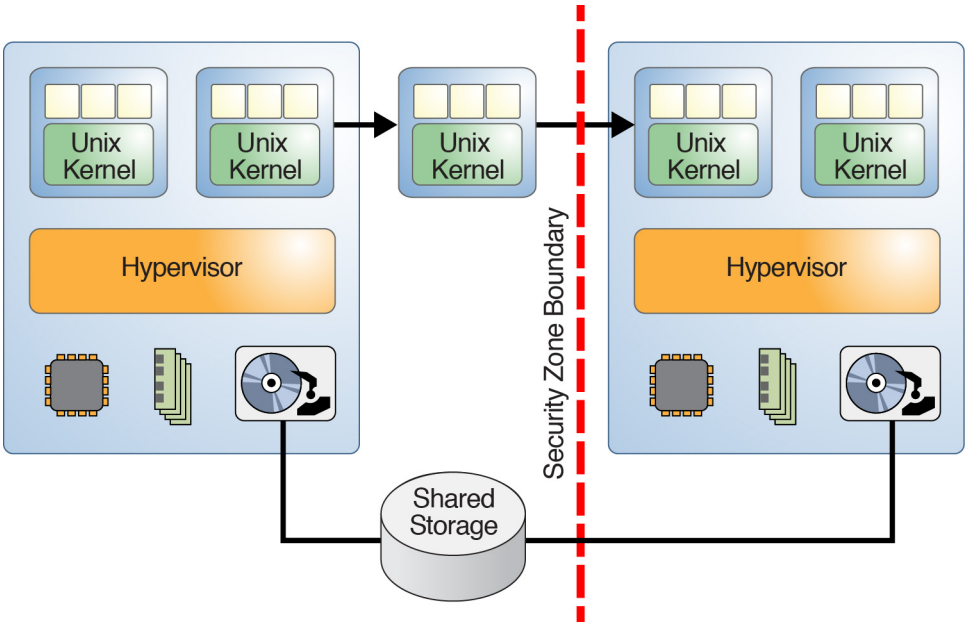
Countermeasure: Carefully Assigning Guests to Hardware Platforms

Use security classes, which are groups of domains that have the same security requirements and privileges, to isolate individual domains from each other. By assigning guest domains that are in the same security class to a certain hardware platform, even a breach of isolation prevents the attack from crossing into another security class.

Countermeasure: Planning an Oracle VM Server for SPARC Domain Migration

The live domain migration feature has the potential to break isolation if a guest domain is inadvertently migrated to a platform that is assigned to a different security class as shown in the following figure. So, carefully plan guest domain migration to ensure that a migration across security class boundaries is not permitted.

FIGURE 1–4 Domain Migration Across Security Boundaries



Countermeasure: Correctly Configuring Virtual Connections

Losing track of all of the virtual network connections might lead to a domain gaining erroneous access to a network segment. For example, such access might circumvent the firewall or a security class.

To reduce the risk of implementation errors, carefully plan and document all of the virtual and physical connections in your environment. Optimize the domain connection plan for simplicity and manageability. Clearly document your plan and verify the correctness of your implementation against your plan before going into production. Even after your virtual environment is in production, verify the implementation against the plan at regular intervals.

Countermeasure: Using VLAN Tagging

You can use VLAN tagging to consolidate several Ethernet segments onto a single physical network. This feature is also available for virtual switches. To mitigate the risks involved with software errors in the implementation of virtual switches, configure one virtual switch per physical NIC and VLAN. To further protect against errors in the Ethernet driver, refrain from using tagged VLANs. However, the probability for such errors is low as this tagged VLAN vulnerability is well known. Intrusion tests on Oracle's Sun SPARC T-Series platform with the Oracle VM Server for SPARC software have not shown this vulnerability.

Countermeasure: Using Virtual Security Appliances

Security appliances such as packet filters and firewalls are instruments of isolation and protect the isolation of security classes. These appliances are subject to the same threats as any other guest domain, so using them does not guarantee complete protection against an isolation breach. Therefore, carefully consider all aspects of risk and security before you decide to virtualize such a service.

Threat: Side Effects of Sharing Resources

Resource sharing in a virtualized environment might lead to denial-of-service (DoS) attacks, which overload a resource until it negatively affects another component such as another domain.

In a Oracle VM Server for SPARC environment, only some resources might be affected by a DoS attack. CPU and memory resources are assigned exclusively to each guest domain, which prevents most DoS attacks. Even the exclusive assignment of these resources might slow down a guest domain in the following ways:

- Thrashing the cache areas that are shared between strands and are assigned to two guest domains
- Overloading memory bandwidth

Unlike CPU and memory resources, disk and network services are usually shared between guest domains. These services are provided to the guest domains by one or more service domains. Carefully consider how to assign and distribute these resources to guest domains. Note that any configuration that permits maximum performance and resource utilization simultaneously minimizes the risk of side effects.

Evaluation: Side Effects Through Shared Resources

A network link can be saturated or a disk can be overloaded whether exclusively assigned to a domain or shared among domains. Such attacks affect the availability of a service for the duration of the attack. The target of the attack is not compromised and no data is lost. You can easily minimize the effects of this threat, but you should keep it in mind even though it is limited to network and disk resources on Oracle VM Server for SPARC.

Countermeasure: Carefully Assigning Hardware Resources

Ensure that you assign only required hardware resources to guest domains. Be sure to unassign an unused resource after the resource is no longer required, for example, a network port or DVD drive required only during an installation. By following this practice, you minimize the number of possible entry points for an attacker.

Countermeasure: Carefully Assigning Shared Resources

Shared hardware resources such as physical network ports, present a possible target for DoS attacks. To limit the impact of DoS attacks to a single group of guest domains, carefully determine which guest domains share which hardware resources.

For example, guest domains that share hardware resources could be grouped by the same availability or security requirements. Beyond grouping, you can apply different kinds of resource controls.

You must consider how to share disk and network resources. You can mitigate issues by separating disk access through dedicated physical access paths or through dedicated virtual disk services.

Summary: Side Effects Through Shared Resources

All the countermeasures described in this section require that you understand the technical details of your deployment and their security implications. Plan carefully, document well, and keep your architecture as simple as possible. Ensure that you understand the implications of virtualized hardware so that you can prepare to securely deploy the Oracle VM Server for SPARC software.

Logical domains are robust against the effects of sharing CPUs and memory, as little sharing actually occurs. Nevertheless, it is best to apply resource controls such as Solaris resource management within the guest domains. Using these controls protect against bad application behavior for either a virtual or a non-virtualized environment.

Execution Environment

Figure 1–3 shows the components of the execution environment. Each component provides certain services that together form the overall platform on which to run the production guest domains. Properly configuring the components is vitally important for the integrity of the system.

All of the execution environment components are potential targets for an attacker. This section describes the threats that might affect each component in the execution environment. Some threats and countermeasures might apply to more than one component.

Threat: Manipulation of the Execution Environment

By manipulating the execution environment, you can gain control in numerous ways. For example, you might install manipulated firmware in the ILOM to snoop on all guest domain I/O from within an I/O domain. Such an attack can access and change the system's configuration. An attacker that takes control of the Oracle VM Server for SPARC control domain can reconfigure the system in any way, and an attacker that takes control of an I/O domain can make changes to attached storage, such as to boot disks.

Evaluation: Manipulation of the Execution Environment

An attacker who successfully breaks in to either the ILOM or to any domain in the execution environment can read and manipulate all data that is available to that domain. This access might be gained over the network or by means of an error in the virtualization stack. Such an attack is difficult to perform as usually the ILOM and the domains cannot be attacked directly.

The countermeasures to protect against the manipulation of the execution environment are standard security practice and should be implemented on any system. Standard security practices present an additional layer of protection around the execution environment that further reduces the risk of intrusion and manipulation.

Countermeasure: Securing Interactive Access Paths

Ensure that you *only* create accounts that are required for the applications that run on the system.

Ensure that accounts that are required for administration are secured by using either key-based authentication or strong passwords. These keys or passwords should not be shared among different domains. Also, consider implementing two-factor authentication or a "two-person rule" for taking certain actions.

Do *not* use anonymous logins for accounts such as `root` to ensure that you have complete traceability and accountability of the commands run on the system. Instead, use rights to grant individual administrators access *only* to those functions that they are permitted to perform. Ensure that administrative network access always uses encryption such as SSH and that an administrator's workstation is treated as a high-security system.

Countermeasure: Minimizing the Oracle Solaris OS

Any software that is installed on a system can be compromised, so ensure that you install *only* the required software to minimize the breach window.

Countermeasure: Hardening the Oracle Solaris OS

In addition to installing a minimized Oracle Solaris OS, configure software packages to "harden" the software against attack. First, run limited network services to effectively disable all network services except for SSH. This policy is the default behavior on Oracle Solaris 11 systems. For information about how to secure the Oracle Solaris OS, see *Oracle Solaris 10 Security Guidelines* and *Oracle Solaris 11 Security Guidelines*.

Countermeasure: Using Role Separation and Application Isolation

By necessity, production applications are connected to other systems and as a result are more exposed to external attacks. Do *not* deploy production applications to a domain that is part of the execution environment. Instead, ensure that you deploy them *only* to guest domains that have no further privileges.

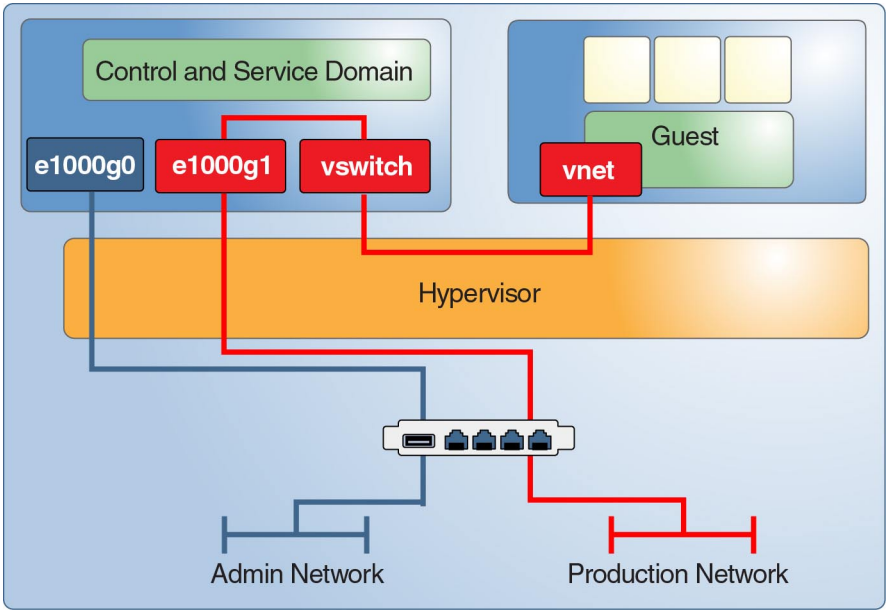
The execution environment should provide only the necessary infrastructure for these guest domains. Separating the execution environment from the production applications enables you to implement granularity in administration privileges. A production guest domain administrator does not require access to the execution environment and an execution environment administrator does not require access to the production guest domains. If possible, assign the different roles of the execution environment, such as the control domain and I/O domain, to different domains. This type of configuration reduces the amount of damage that can be done if any one of these domains is compromised.

You can also extend role separation to the network environment that is used to connect your different servers.

Countermeasure: Configuring a Dedicated Management Network

Connect all servers that are equipped with service processors (SPs) to a dedicated management network. This configuration is also recommended for the domains of the execution environment. If networked at all, host these domains on their own dedicated network. Do *not* connect the execution environment domains directly to those networks that are assigned to the production domains. While you can perform all administrative work through the single console connection that is made available by the ILOM SP, this configuration makes administration sufficiently cumbersome to be impracticable. By separating the production and administration networks, you protect against both eavesdropping and manipulation. This type of separation also eliminates the possibility of an attack on the execution environment from the guest domains over the shared network.

FIGURE 1–5 Dedicated Management Network



ILOM

All current Oracle SPARC systems include a built-in system controller (ILOM), which has the following capabilities:

- Manages basic environmental controls such as fan speed and chassis power
- Enables firmware upgrades
- Provides the system console for the control domain

You can access the ILOM through a serial connection or use SSH, HTTP, HTTPS, SNMP, or IPMI to access it through a network port. The Fujitsu M10 systems use XSCF instead of ILOM to perform similar functions.

Threat: Complete System Denial-of-Service

An attacker that gains control of the ILOM can compromise the system in many ways, including the following:

- Removing power from all running guests
- Installing manipulated firmware to gain access to at least one guest domain

These scenarios apply to any system that has such a controller device. In a virtualized environment, the damage can be that much greater than in a physical environment because many domains that are housed in the same system enclosure are at risk.

Likewise, an attacker that gains control over the control domain or an I/O domain can easily disable all dependent guest domains by shutting down the corresponding I/O services.

Evaluation: Complete System Denial-of-Service

While the ILOM is usually connected to an administrative network, you can also access the ILOM from the control domain by using IPMI with the BMC access module. As a result, both of these connection types should be well protected and isolated from normal production networks.

Likewise, an attacker can breach a service domain from the network or through an error in the virtualization stack, and then block guest I/O or perform a system shutdown. While the damage is limited as data is neither lost nor compromised, the damage can affect a large number of guest domains. So, ensure that you protect against the possibility of this threat to limit the potential damage.

Countermeasure: Securing the ILOM

As the system service processor, the ILOM controls critical features such as chassis power, Oracle VM Server for SPARC startup configurations, and console access to the control domain. The following measures enable you to secure the ILOM:

- Placing the ILOM's network port in a network segment that is separate from the administrative network, which is used for the domains in the execution environment.
- Disabling all services that are not required for operation, such as HTTP, IPMI, SNMP, HTTPS, and SSH.
- Configuring dedicated and personal administrator accounts that grant only the required rights. To maximize accountability of the actions taken by administrators, ensure that you create personal administrator accounts. This type of access is especially important for console access, firmware upgrades, and managing startup configurations.

Hypervisor

The hypervisor is the firmware layer that implements and controls the virtualization of real hardware. The hypervisor includes the following components:

- Actual hypervisor, which is implemented in firmware and supported by the systems' CPUs.
- Kernel modules that run in the control domain to configure the hypervisor.
- Kernel modules and daemons that run in I/O domains and service domains to provide virtualized I/O, as well as the kernel modules that communicate by means of Logical Domain Channels (LDCs).
- Kernel modules and device drivers that run in the guest domains to access virtualized I/O devices as well as the kernel modules that communicate by means of LDCs.

Threat: Breaking the Isolation

An attacker can hijack guest domains or the entire system by breaking out of the isolated runtime environment provided by the hypervisor. Potentially, this threat can cause the most severe damage to a system.

Evaluation: Breaking the Isolation

A modular system design can improve isolation by granting different levels of privileges to guest domains, the hypervisor, and the control domain. Each functional module is implemented in a separate and configurable kernel module, device driver, or daemon. This modularity requires clean APIs and simple communication protocols, reducing the overall risk for error.

Even if exploitation of an error seems unlikely, the potential damage can lead to the attacker controlling the entire system.

Countermeasure: Validating Firmware and Software Signatures

Even though you can download system firmware and OS patches directly from an Oracle web site, these patches can be manipulated. Before you install the software, ensure that you verify the MD5 checksums of the software packages. The checksums of all downloadable software is published by Oracle.

Countermeasure: Validating Kernel Modules

Oracle VM Server for SPARC uses several drivers and kernel modules to implement the overall virtualization system. All kernel modules and most binaries that are distributed with the Oracle Solaris OS carry a digital signature. Use the `elfsign` utility to check the digital signature for each kernel module and driver. You can use the Oracle Solaris 11 `pkg verify` command to check the integrity of Oracle Solaris binary. See `https://blogs.oracle.com/cmt/entry/solaris_fingerprint_database_how_it`.

First, you must establish the integrity of the `elfsign` utility. Use the basic audit and reporting tool (BART) to automate digital signature verification process. 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`) describes how to combine BART and the Solaris Fingerprint Database to automatically perform similar integrity checks. Although the fingerprint database has been discontinued, the concepts described in this document can be carried over to use `elfsign` and BART in a similar manner.

Control Domain

The control domain, which often has the roles of an I/O domain and a service domain, must be kept safe as it can modify the configuration of the hypervisor, which controls all attached hardware resources.

Threat: Control Domain Denial-of-Service

The shutdown of the control domain can result in a denial of service of the configuration tools. Because the control domain is required only for configuration changes, the guest domains are unaffected if they access their network and disk resources through other service domains.

Evaluation: Control Domain Denial-of-Service

Attacking the control domain over the network is equivalent to attacking any other properly protected Oracle Solaris OS instance. The damage of a shutdown or similar denial of service of the control domain is relatively low. However, guest domains are affected if the control domain also acts as a service domain for these guest domains.

Countermeasure: Securing Console Access

Avoid configuring administrative network access to the execution environment's domains. This scenario requires that you use the ILOM console service to the control domain to perform all administration tasks. Console access to all other domains is still possible by using the `vntsd` service running on the control domain.

Consider this option carefully. Although this option reduces the risk of being attacked over the administrative network, only one administrator can access the console at a time.

For information about securely configuring `vntsd`, see "How to Enable the Virtual Network Terminal Server Daemon" in *Oracle VM Server for SPARC 3.1 Administration Guide*.

Logical Domains Manager

The Logical Domains Manager runs in the control domain and is used to configure the hypervisor, and create and configure all domains and their hardware resources. Ensure that Logical Domains Manager use is logged and monitored.

Threat: Unauthorized Use of Configuration Utilities

An attacker might take control of an administrator's user ID or an administrator from a different group might gain unauthorized access to another system.

Evaluation: Unauthorized Use of Configuration Utilities

Ensure that an administrator does not have unnecessary access to a system by implementing well-maintained identity management. Also, implement strict, fine-grained access control and other measures such as the two-person rule.

Countermeasure: Applying the Two-Person Rule

Consider implementing a two-person rule for Logical Domains Manager and other administrative tools by using rights. See Enforcing the Two-Person Rule Via Role-Based Access Control in the Oracle Solaris 10 Operating System (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/twoperson-rule-solaris-277014.pdf`). This rule protects against social engineering attacks, compromised administrative accounts, and human error.

Countermeasure: Using Rights for the Logical Domains Manager

By using rights for the `ldm` command, you can implement fine-grained access control and maintain complete retraceability. For information about configuring rights, see *Oracle VM Server for SPARC 3.1 Administration Guide*. Using rights helps safeguard against human errors because not all features of the `ldm` command are available to all administrators.

Countermeasure: Hardening the Logical Domains Manager

Disable unnecessary domain manager services. The Logical Domains Manager provides network services for domain access, monitoring, and migration. Disabling network services reduces the attack surface of Logical Domains Manager to the minimum required to operate it normally. This scenario counters denial of service attacks and other attempts to misuse these network services.

Note – While disabling domain manager services help to minimize the attack surface, all of the side effects of doing so in any particular configuration cannot be known before hand.

Disable any of the following network services when they are not being used:

- Migration service on TCP port `8101`

  To disable this service, see the description of the `ldmd/incoming_migration_enabled` and `ldmd/outgoing_migration_enabled` properties in the `ldmd(1M)` man page.

- Extensible Messaging and Presence Protocol (XMPP) support on TCP port `6482`

  For information about how to disable this service, see "XML Transport" in *Oracle VM Server for SPARC 3.1 Administration Guide*.

Note that disabling XMPP prevents you from using some key Oracle VM Server for SPARC features such as domain migration, memory dynamic reconfiguration, and the `ldm init-system` command. Disabling XMPP also prevents Oracle VM Manager or Ops Center from managing the system.

- Simple Network Management Protocol (SNMP) on UDP port `161`

  Determine whether you want to use the Oracle VM Server for SPARC Management Information Base (MIB) to observe domains. This feature requires that the SNMP service is enabled. Based on your choice, do one of the following:

  - **Enable the SNMP service to use the Oracle VM Server for SPARC MIB.** Securely install the Oracle VM Server for SPARC MIB. See "How to Install the Oracle VM Server for SPARC MIB Software Package" in *Oracle VM Server for SPARC 3.1 Administration Guide* and "Managing Security" in *Oracle VM Server for SPARC 3.1 Administration Guide*.
  - **Disable the SNMP service.** For information about how to disable this service, see "How to Remove the Oracle VM Server for SPARC MIB Software Package" in *Oracle VM Server for SPARC 3.1 Administration Guide*.

- Discovery service on multicast address `239.129.9.27` and port `64535`

  Note – Note that this discovery mechanism is also used by the `ldmd` daemon to detect collisions when automatically assigning MAC addresses. If you disable the discovery service, MAC address collision detection will not work, and automatic MAC address allocation will therefore not work correctly.

  You *cannot* disable this service while the Logical Domains Manager daemon, `ldmd`, is running. Instead, use the IP Filter feature of Oracle Solaris to block access to this service, which minimizes the attack surface of the Logical Domains Manager. Blocking access prevents unauthorized use of the utility, which effectively counters denial-of-service attacks and other attempts to misuse these network services. See Chapter 20, "IP Filter in Oracle Solaris (Overview)," in *Oracle Solaris Administration: IP Services* and "Using IP Filter Rule Sets" in *Oracle Solaris Administration: IP Services*.

Also see "Countermeasure: Securing the ILOM" on page 24.

Countermeasure: Auditing the Logical Domains Manager

Protecting the Logical Domains Manager is vital to the security of the overall system. Any changes to the Oracle VM Server for SPARC configuration must be logged for tracing hostile actions. Scan the audit logs regularly and copy the logs to a separate system for secure archival. For more information, see Chapter 3, "Oracle VM Server for SPARC Security," in *Oracle VM Server for SPARC 3.1 Administration Guide*.

Service Domain

A service domain provides some virtual services to guest domains on the system. Services might include a virtual switch, virtual disk, or virtual console service.

Figure 1–6 shows an example service domain that offers console services. Often the control domain hosts the console services, and thus is also a service domain. The execution environment domains often combine the functions of a control domain, I/O domain, and service domain in one or two domains.

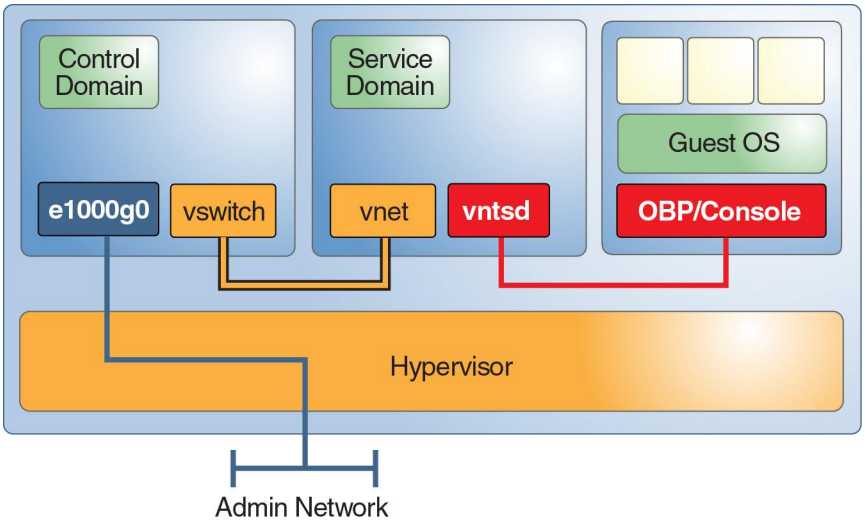
Threat: Manipulation of a Service Domain

An attacker who gains control of a service domain can manipulate data or listen to any communication that occurs through the offered services. This control might include console access to guest domains, access to network services, or access to disk services.

Evaluation: Manipulation of a Service Domain

While the attack strategies are the same as for an attack on the control domain, the possible damage is less because the attacker cannot modify the system configuration. The resulting damage might include the theft or manipulation of data that is being offered by the service domain but not manipulation of any data sources. Depending on the service, an attacker might be required to exchange kernel modules.

FIGURE 1–6 Service Domain Example



Countermeasure: Granularly Segregating Service Domains

If possible, have each service domain offer only *one* service to its clients. This configuration guarantees that only one service can be compromised if a service domain is breached. However, be sure to weigh the importance of this type of configuration against the additional complexity. Note that having redundant I/O domains is highly recommended.

Countermeasure: Isolating Service Domains and Guest Domains

You can isolate both Oracle Solaris 10 and Oracle Solaris 11 service domains from guest domains. The following solutions are shown in the preferred order of implementation:

- Ensure that the service domain and the guest domain do not share the same network port. Also, do not plumb any virtual switch interface on the service domain. For Oracle Solaris 11 service domains, do not plumb any VNICs on the physical ports that are used for virtual switches.
- If you must use the same network port for both the Oracle Solaris 10 OS and Oracle Solaris 11 OS, place the I/O domain traffic in a VLAN that is not used by guest domains.
- If you cannot implement either of the previous solutions, do not plumb the virtual switch in the Oracle Solaris 10 OS and apply IP filters in the Oracle Solaris 11 OS.

Countermeasure: Restricting Access to Virtual Consoles

Ensure that access to individual virtual consoles is limited to *only* those users that must access them. This configuration ensures that no single administrator has access to all consoles, which prevents access to consoles other than those assigned to a compromised account. See "How to Create Default Services" in *Oracle VM Server for SPARC 3.1 Administration Guide*.

I/O Domain

Any domain that has direct access to physical I/O devices such as network ports or disks is an I/O domain. For information about configuring I/O domains, see Chapter 6, "Setting Up I/O Domains," in *Oracle VM Server for SPARC 3.1 Administration Guide*.

An I/O domain also might be a service domain if it provides I/O services to guest domains, which gives the domains access to the hardware.

Threat: Experiencing a Denial-of-Service of an I/O Domain or a Service Domain

An attacker who blocks the I/O services of an I/O domain ensures that all dependent guest domains are equally blocked. A successful DoS attack might be achieved by overloading the back-end network or disk infrastructure or by injecting a fault into the domain. Either attack might force the domain to hang or panic. Likewise, an attacker who suspends a service domain's

services causes any guest domain that depends on these services to immediately hang. If the guest domain hangs, it will resume operation when the I/O service resumes.

Evaluation: Experiencing a Denial-of-Service of an I/O Domain or a Service Domain

DoS attacks are commonly made over the network. Such an attack can be successful because network ports are open for communication and can be overwhelmed by network traffic. A resulting loss of service blocks dependent guest domains. A similar attack on disk resources might be made by means of the SAN infrastructure or by attacking the I/O domain. The only damage is a temporary halt of all dependent guest domains. While the impact of DoS tasks might be substantial, data is neither compromised nor lost, and the system configuration remains intact.

Countermeasure: Granularly Configuring I/O Domains

Configuring multiple I/O domains reduces the impact of one domain failing or being compromised. You can assign individual PCIe slots to a guest domain to give it I/O domain capabilities. If the root domain that owns the PCIe bus crashes, that bus is reset, which leads to a subsequent crash of the domain that was assigned the individual slot. This feature does not fully eliminate the need for two root domains that each own a separate PCIe bus.

Countermeasure: Configuring Redundant Hardware and Root Domains

High availability also contributes to enhanced security because it ensures that services can withstand denial-of-service attacks. The Oracle VM Server for SPARC implements high availability methodologies such as using redundant disk and network resources in redundant I/O domains. This configuration option enables rolling upgrades of the I/O domains and protects against the impact of a failed I/O domain due to a successful DoS attack. With the advent of SR-IOV, guest domains can have direct access to individual I/O devices. However, when SR-IOV is not an option, consider creating redundant I/O domains. See "Countermeasure: Granularly Segregating Service Domains" on page 30.

Threat: Manipulation of an I/O Domain

An I/O domain has direct access to back-end devices, usually disks, which it virtualizes and then offers to guest domains. A successful attacker has full access to these devices and can read sensitive data or manipulate software on the boot disks of the guest domains.

Evaluation: Manipulation in an I/O Domain

An I/O domain attack is as likely as a successful attack on a service domain or the control domain. The I/O domain is an attractive target given the potential access to a large number of disk devices. Therefore, consider this threat when dealing with sensitive data in a guest domain that runs on virtualized disks.

Countermeasure: Protecting Virtual Disks

When an I/O domain is compromised, the attacker has full access to the guest domain's virtual disks.

Protect the contents of the virtual disks by doing the following:

- **Encrypting the contents of the virtual disks.** On Oracle Solaris 10 systems, you might use an application that can encrypt its own data, such as `pgp`/`gpg` or Oracle 11g encrypted tablespaces. On Oracle Solaris 11 systems, you might use ZFS encrypted datasets to provide transparent encryption of all data stored in the file system.
- **Distributing the data over several virtual disks across different I/O domains.** A guest domain might create a striped (RAID 1/RAID 5) volume that stripes over several virtual disks that are obtained from two I/O domains. If one of these I/O domains is compromised, the attacker would have difficulty making use of the portion of the data that is available.

Guest Domains

While guest domains are not part of the execution environment, they are the most likely target for an attack because they are connected to the network. An attacker who breaches a virtualized system can launch attacks on the execution environment.

Countermeasure: Securing the Guest Domain OS

The operating system on the guest domain is often the first line of defense against any attack. With the exception of attacks that originate within the datacenter, an attacker must break into a guest domain that has external connections before attempting to break guest domain isolation and capture the complete environment. Therefore, you must harden the guest domain's OS.

To further harden the OS, you can deploy your application in Solaris Zones, which place an additional layer of isolation between the application's network service and the operating system of the guest domain. A successful attack on the service compromises only the zone and not the underlying operating system, which prevents the attacker from expanding control beyond the resources that are allocated to the zone. As a result, eventually breaking guest isolation is more difficult. For more information about securing the guest OS, see *Oracle Solaris 10 Security Guidelines* and *Oracle Solaris 11 Security Guidelines*.

◆ ◆ ◆ CHAPTER 2

Secure Installation and Configuration of Oracle VM Server for SPARC

This chapter describes the security considerations that are related to installing and configuring the Oracle VM Server for SPARC software.

Installation

The Oracle VM Server for SPARC software is automatically installed securely as an Oracle Solaris 10 or an Oracle Solaris 11 package. After installation finishes, you must have administrator privileges to configure the domains with the rights, auditing, and authorization features. These features are not enabled by default.

Postinstallation Configuration

Perform the following tasks after you install the Oracle VM Server for SPARC software to maximize secure usage:

- Configure the control domain with the required virtual I/O services such as the virtual switch, virtual disk server, and virtual console concentrator services. See Chapter 4, "Setting Up Services and the Control Domain," in *Oracle VM Server for SPARC 3.1 Administration Guide*.
- Configure guest domains. See Chapter 5, "Setting Up Guest Domains," in *Oracle VM Server for SPARC 3.1 Administration Guide*.

  You can use a virtual switch to configure guest domains by means of an administrative network and a production network. In this case, a virtual switch is created by using the production network interface as the virtual switch network device. See "Countermeasure: Configuring a Dedicated Management Network" on page 22.

  The security of a guest domain becomes compromised when any of its virtual disks are compromised. So, ensure that virtual disks (network-attached storage, locally stored disk image files, or physical disks) are stored in a secure location.

The `vntsd` daemon is disabled by default. When this daemon is enabled, any user who is logged in to the control domain is permitted to connect to a guest domain's console. To prevent this type of access, ensure that the `vntsd` daemon is disabled, or use rights to limit console connectivity access *only* to sanctioned users.

- The service processor (SP) is configured securely by default. For information about using the Integrated Lights Out Management (ILOM) software to manage the SP, see the documentation for your platform at `http://www.oracle.com/technetwork/documentation/sparc-tseries-servers-252697.html`.

◆ ◆ ◆ CHAPTER 3

Security Considerations for Developers

This chapter provides information for developers who produce applications for the Oracle VM Server for SPARC software.

Oracle VM Server for SPARC XML Interface

You can create external programs that interact with the Oracle VM Server for SPARC software by means of the Extensible Markup Language (XML) communication mechanism. XML uses the Extensible Messaging and Presence Protocol (XMPP).

An attacker might attempt to exploit this network protocol to access a system, so consider disabling XMPP. For information about disabling XMPP, see "XML Transport" in *Oracle VM Server for SPARC 3.1 Administration Guide*. For information about the security mechanisms that Logical Domains Manager uses, see "XMPP Server" in *Oracle VM Server for SPARC 3.1 Administration Guide*.

Note that disabling XMPP prevents you from using some key Oracle VM Server for SPARC features such as domain migration, memory dynamic reconfiguration, and the `ldm init-system` command. Disabling XMPP also prevents Oracle VM Manager or Ops Center from managing the system.

◆ ◆ ◆ APPENDIX A

Secure Deployment Checklist

This checklist summarizes the steps that you can take to harden your Oracle VM Server for SPARC environment. The details are provided in other documents such as the following:

- *Oracle VM Server for SPARC 3.1 Administration Guide*
- *Oracle Solaris 10 Security Guidelines*
- *Oracle Solaris 11 Security Guidelines*

Oracle VM Server for SPARC Security Checklist

- ❒ Perform the Oracle Solaris OS hardening steps to your guest domains as you would in a non-virtualized environment.
- ❒ Use the LDoms Management and LDoms Review rights profiles to delegate the appropriate privileges to users.
- ❒ Use rights to restrict access to the console of domains that *only* you, as the administrator of Oracle VM Server for SPARC, must access.
- ❒ Enable the Oracle Solaris OS auditing feature for Oracle VM Server for SPARC.
- ❒ Disable unnecessary domain manager services.
- ❒ Only deploy guest domains of the same security class to one physical platform.
- ❒ Ensure that there are no network connections between the administration network of the execution environment and the guest domains.
- ❒ Only assign required resources to guest domains.