Oracle® VM Server for SPARC 3.0 Security Guide

Part No: E29666
November 2012

ORACLE

130524@25097

Contents

Preface

The *Oracle VM Server for SPARC 3.0 Security Guide* includes information about how to securely install, configure, and use the Oracle VM Server for SPARC 3.0 software.

Related Documentation

The following table shows the documentation that is available for and related to the Oracle VM Server for SPARC 3.0 release.

TABLE P–1 Related Documentation

Application	Title
Oracle VM Server for SPARC 3.0 Software	*Oracle VM Server for SPARC 3.0 Administration Guide* *Oracle VM Server for SPARC 3.0 Security Guide* *Oracle VM Server for SPARC 3.0 Reference Manual* *Oracle VM Server for SPARC 3.0 Release Notes*
Oracle VM Server for SPARC 3.0 `drd`(1M) and `vntsd`(1M) man pages	Oracle Solaris OS Reference Manuals: ■ Oracle Solaris 10 Documentation ■ Oracle Solaris 11 Documentation
Oracle Solaris OS: Installation and Configuration	Oracle Solaris OS Installation and Configuration Guides: ■ Oracle Solaris 10 Documentation ■ Oracle Solaris 11 Documentation
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, 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.

You can access the Oracle VM Server for SPARC discussion forum at `http://forums.oracle.com/forums/forum.jspa?forumID=1047`.

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.

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–2 Typographic Conventions

Typeface	Description	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows UNIX system prompts and superuser prompts for shells that are included in the Oracle Solaris OS. In command examples, the shell prompt indicates whether the command should be executed by a regular user or a user with privileges.

TABLE P–3 Shell Prompts

Shell	Prompt
Bash shell, Korn shell, and Bourne shell	`$`
Bash shell, Korn shell, and Bourne shell for superuser	`#`
C shell	`machine_name%`
C shell for superuser	`machine_name#`

◆ ◆ ◆ CHAPTER 1

Oracle VM Server for SPARC Security Overview

This chapter describes the following security features that are used by the Oracle VM Server for SPARC software:

Security Features Used by Oracle VM Server for SPARC

The Oracle VM Server for SPARC software is a virtualization product that permits more than one Oracle Solaris virtual machine (VM) 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 must be run on the control domain to configure the logical domain 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 the role-based access control (RBAC) feature of Oracle Solaris for consoles and `solaris.ldoms` authorizations. See "Logical Domains Manager Profile Contents" in *Oracle VM Server for SPARC 3.0 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 *Secure Deployment of Oracle VM Server for SPARC*.
- 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).
- 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 3.0 Administration Guide*.

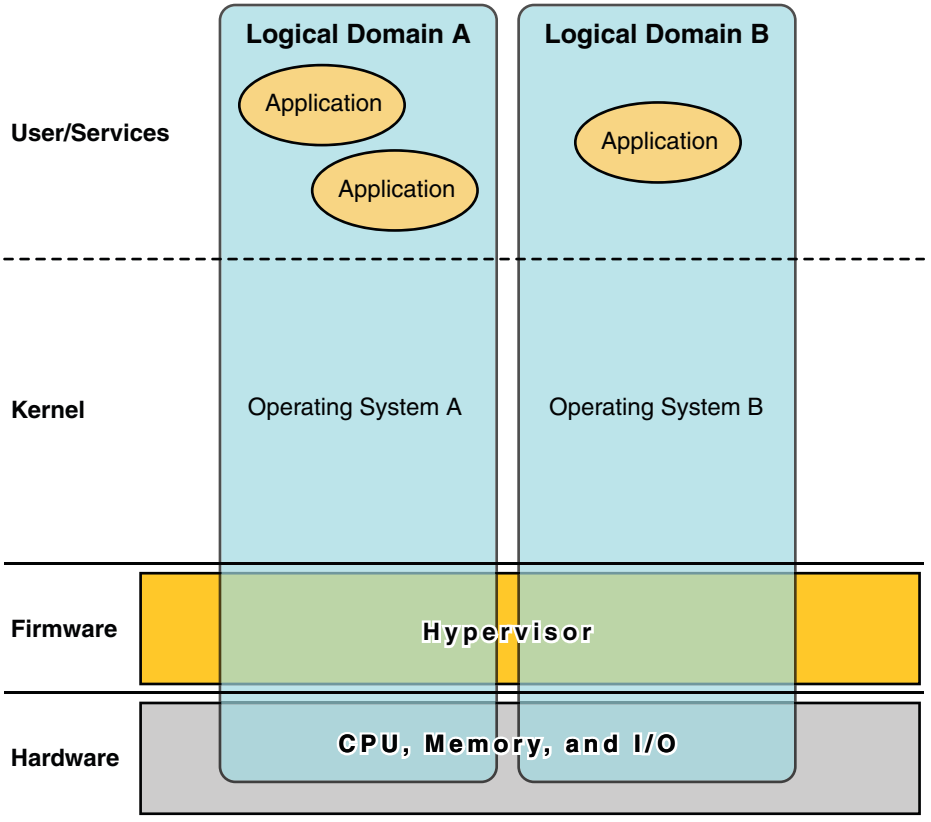
Oracle VM Server for SPARC Product Overview

Oracle VM Server for SPARC provides highly efficient, enterprise-class virtualization capabilities for Oracle's SPARC T-Series servers. Using the Oracle VM Server for SPARC software, you can create up to 128 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 SPARC T-Series 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 3.0 Administration Guide* and *Oracle VM Server for SPARC 3.0 Reference Manual*. For information about the required hardware and software, see *Oracle VM Server for SPARC 3.0 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, but it does not manage the logical domains. The Logical Domains Manager manages the logical domains.

- **Control domain.** The Logical Domains Manager runs in this domain so that you can 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 "Assigning PCIe Endpoint Devices" in *Oracle VM Server for SPARC 3.0 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 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 Sun SPARC Enterprise T5440 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 only has 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, to which you can apply some of the following general security principles:

- **Minimize the attack surface.**
  - Minimize the unintentional configuration errors by creating operational guidelines that enable you to regularly evaluate the security of the system. See "Counter Measure #1: Operational Guidelines" in *Secure Deployment of Oracle VM Server for SPARC*.
  - Carefully plan the architecture of the virtual environment to maximize the isolation of the domains. See the counter measures described for "Threat #2: Errors in the Architecture of the Virtual Environment" in *Secure Deployment of Oracle VM Server for SPARC*.
  - Carefully plan which resources to assign and whether they are to be shared. See "Counter Measure #7: Carefully Assigning Hardware Resources" and "Counter Measure #8: Careful Assignment of Shared Resources" in *Secure Deployment of Oracle VM Server for SPARC*.
  - Ensure that the logical domains are protected from manipulation by applying the counter measures described for "Threat #4: Manipulation of the Execution Environment" and "Counter Measure #28: Securing the Guest OS" in *Secure Deployment of Oracle VM Server for SPARC*.
  - 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 "Counter Measure #15: Validating Firmware and Software Signatures" and "Counter Measure #16: Validating Kernel Modules" in *Secure Deployment of Oracle VM Server for SPARC*.
  - Protect the control domain against denial-of-service attacks. See "Counter Measure #17: Console Access" in *Secure Deployment of Oracle VM Server for SPARC*.
  - Ensure that the Logical Domains Manager cannot be run by unauthorized users. See "Threat #8: Unauthorized Use of Configuration Utilities" in *Secure Deployment of Oracle VM Server for SPARC*.
  - Ensure that the service domain cannot be accessed by unauthorized users or processes. See "Threat #9: Manipulation of a Service Domain" in *Secure Deployment of Oracle VM Server for SPARC*.

- Protect an I/O domain or a service domain against denial-of-service attacks. See "Threat #10: Denial-of-Service of IO Domain or Service Domain" in *Secure Deployment of Oracle VM Server for SPARC*.
- Ensure that an I/O domain cannot be accessed by unauthorized users or processes. See "Threat #11: Manipulation of an IO Domain" in *Secure Deployment of Oracle VM Server for SPARC*.
- Disable unnecessary domain manager services. The Logical Domains Manager provides network services for domain access, monitoring, and migration. 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`

    To disable this service, see "XML Transport" in *Oracle VM Server for SPARC 3.0 Administration Guide*.
  - 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 3.0 Administration Guide* and "Managing Security" in *Oracle VM Server for SPARC 3.0 Administration Guide*.
    - **Disable the SNMP service.** To disable this service, see "How to Remove the Oracle VM Server for SPARC MIB Software Package" in *Oracle VM Server for SPARC 3.0 Administration Guide*.
  - Discovery service on multicast address `239.129.9.27` and port `64535`

    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 "Counter Measure #14: Securing the ILOM" and "Counter Measure #20: Hardening LDoms Manager" in *Secure Deployment of Oracle VM Server for SPARC*.

- **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 only assigning guest domains from a single security class to a single hardware platform, you create an isolation breach, which prevents the domains from crossing into a different security class. See "Counter Measure #2: Carefully Assigning Guests to Hardware Platforms" in *Secure Deployment of Oracle VM Server for SPARC*.
  - Use RBAC 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 3.0 Administration Guide*.
  - Use RBAC to restrict access to the console of *only* those domains that you, as the administrator of Oracle VM Server for SPARC, must access. Do *not* permit general access to all domains. See "Using Rights Profiles and Roles" in *Oracle VM Server for SPARC 3.0 Administration Guide*.
- **Monitor system activity.**

  Enable Oracle VM Server for SPARC auditing. See "Enabling and Using Auditing" in *Oracle VM Server for SPARC 3.0 Administration Guide*.

For recommendations about deploying the Oracle VM Server for SPARC software in a secure manner, see "Recommended Deployment Options" in *Secure Deployment of Oracle VM Server for SPARC*.

◆ ◆ ◆ CHAPTER 2

Secure Installation and Configuration of Oracle VM Server for SPARC

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

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 completes, you must have administrator privileges to configure the domains with the role-based access control (RBAC), 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 3.0 Administration Guide*.
- Configure guest domains. See Chapter 5, "Setting Up Guest Domains," in *Oracle VM Server for SPARC 3.0 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 "Counter Measure #13: Dedicated Management Network" in *Secure Deployment of Oracle VM Server for SPARC*.

  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 RBAC 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

Oracle VM Server for SPARC Security Features

This chapter provides an overview of security features that are used by the Oracle VM Server for SPARC software.

For information about authentication, access control, and auditing, see Chapter 3, "Oracle VM Server for SPARC Security," in *Oracle VM Server for SPARC 3.0 Administration Guide*.

Security Model

The Oracle VM Server for SPARC software builds on the security model and features that are built into the Oracle Solaris OS. For information about Oracle Solaris OS security guidelines, see *Oracle Solaris 11 Security Guidelines* and *Oracle Solaris 10 Security Guidelines*.

Configuring and Using Authentication

Like a bare-metal Oracle Solaris installation, any user who has an account can log in to a logical domain, even the control domain. The Oracle VM Server for SPARC software does not create any user accounts. See "Installing the Logical Domains Manager" in *Oracle VM Server for SPARC 3.0 Administration Guide*. For information about how to secure Oracle Solaris users, see "Securing Users" in *Oracle Solaris 11 Security Guidelines*.

To use the Logical Domains Manager to perform domain management activities on the control domain, a user must be granted special privileges to read and write configuration data. See "Logical Domains Manager Profile Contents" in *Oracle VM Server for SPARC 3.0 Administration Guide* and "Using Rights Profiles and Roles" in *Oracle VM Server for SPARC 3.0 Administration Guide*.

Configuring and Using RBAC

You can manage authorizations and rights profiles and assign roles to user accounts by using the role-based access control (RBAC) feature of the Oracle Solaris OS. For information about RBAC, see Chapter 9, "Using Role-Based Access Control (Tasks)," in *System Administration Guide: Security Services*.

Installing the Logical Domains Manager adds the necessary authorizations and rights profiles to the local files. See "Using Rights Profiles and Roles" in *Oracle VM Server for SPARC 3.0 Administration Guide*.

To configure users, authorizations, rights profiles, and roles in a naming service, see *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Configuring and Using Auditing

You should administer and audit an Oracle Solaris instance in a guest domain the same as you would an Oracle Solaris OS running on a bare-metal system. You can customize the Oracle Solaris OS auditing feature to audit only those functions and system services that are important for your environment. For Oracle VM Server for SPARC, ensure that the virtualization software class is audited. You can perform other auditing-related tasks. See "Using the Audit Service" in *Oracle Solaris 11 Security Guidelines* and "How to Audit Significant Events in Addition to Login/Logout" in *Oracle Solaris 11 Security Guidelines*.

The Logical Domains Manager creates audit events and passes them to the Oracle Solaris audit subsystem for storage and later examination. The history is kept in a log of what was done, when it was done, by whom, and what was affected. Note that you *cannot* view audit information for all of the domains in a system from its control domain.

So for each domain in the system, you can enable and disable the auditing feature based on the version of the Oracle Solaris OS that runs on your system, as follows:

- **Oracle Solaris 10 OS.** Use the `bsmconv` and `bsmunconv` commands. See the `bsmconv(1M)` and `bsmunconv(1M)` man pages, and the Oracle Solaris 10 version of *System Administration Guide: Security Services*.
- **Oracle Solaris 11 OS.** Use the `audit` command. See the `audit(1M)` man page and the Oracle Solaris 11 version of *System Administration Guide: Security Services*.

For more information, see "Enabling and Using Auditing" in *Oracle VM Server for SPARC 3.0 Administration Guide*.

Configuring and Using Other Security Features

Oracle VM Server for SPARC secures the usage of specific virtualization features. If enabled, the `vntsd` daemon is configured in the most secure configuration by default. It only accepts connections from the control domain and *not* over the network. You can configure a less secure option to permit network connections, if needed. See the description of the `vntsd/listen_addr` property in the `vntsd(1M)` man page.

Take care when configuring `vntsd` to accept network connections. It is best to permit only connections from the control domain or to disable `vntsd` for optimal security. See "Applying General Security Principles to Oracle VM Server for SPARC" on page 13.

The Oracle VM Server for SPARC domain migration feature uses security measures. The Logical Domains Manager on the source machine accepts the request to migrate a domain and establishes a secure network connection with the Logical Domains Manager that runs on the target machine. The migration occurs after this connection has been established. These secure connections are created by using authentication and encryption features. See "Security for Migration Operations" in *Oracle VM Server for SPARC 3.0 Administration Guide*.

In particular, the domain migration operation uses the Secure Sockets Layer (SSL), by default, to encrypt all traffic sent and received across the network. You can improve migration performance by assigning cryptographic units to the control domains of systems that support them.

When domain migration is not needed, you can disable the migration feature to prevent the `ldmd` process from listening on the migration port.

If you use domain migration, ensure that the `ldmd` daemon is configured to require password authentication during the migration. This is the default behavior.

◆ ◆ ◆ CHAPTER 4

Security Considerations for Developers

This chapter provides information that is helpful to 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 interface with the Oracle VM Server for SPARC software by means of the Extensible Markup Language (XML) communication mechanism, which uses the Extensible Messaging and Presence Protocol (XMPP).

Attackers might attempt to exploit this network protocol to access a system, so you might consider disabling XMPP. For information about disabling XMPP, see "XML Transport" in *Oracle VM Server for SPARC 3.0 Administration Guide*. For information about the security mechanisms that Logical Domains Manager uses, see "XMPP Server" in *Oracle VM Server for SPARC 3.0 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.

◆ ◆ ◆ 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 3.0 Administration Guide*
- *Oracle Solaris 10 Security Guidelines*
- *Oracle Solaris 11 Security Guidelines*
- *Secure Deployment of Oracle VM Server for SPARC*

Oracle VM Server for SPARC Security Checklist

- ❒ Perform the Oracle Solaris 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 role-based access control (RBAC) to restrict access to the console of *only* those domains that 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 systems of the same security class on one physical platform.
- ❒ Ensure that there are no network connections between the administration of the execution environment and the guest domains.
- ❒ Only assign required resources to guest systems.