Oracle® VM

Security Guide for Release 3.4

E64084-11
January 2022

Abstract

Document generated on: 2022-01-24 (revision: 7598)

Table of Contents

Preface

The Oracle VM Security Guide explains how to install, configure and use Oracle VM in a secure way.

Caution

Oracle VM environments can be built on both x86-64bit and SPARC hardware. Even though much of the content is generic and applicable to both architectures, you should keep in mind that this document focuses on the secure deployment of Oracle VM on x86 hardware platforms. Additional guidelines for the SPARC architecture can be found in the Oracle Technical Paper entitled *Secure Deployment of Oracle VM Server for SPARC*, which can be downloaded from the Oracle Technology Network: http://www.oracle.com/technetwork/articles/systems-hardware-architecture/secure-ovm-sparc-deployment-294062.pdf

Audience

This document is intended for system administrators who install, configure and manage the Oracle VM environment. We assume that you have a solid understanding of the product and are familiar with virtualization in general, Web technologies and the Oracle Linux operating system.

Documentation Accessibility

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

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.

Command Syntax

Oracle Linux command syntax appears in `monospace` font. The dollar character ($), number sign (#), or percent character (%) are Oracle Linux command prompts. Do not enter them as part of the command. The following command syntax conventions are used in this guide:

Convention	Description

backslash \	A backslash is the Oracle Linux command continuation character. It is used in command examples that are too long to fit on a single line. Enter the command as displayed (with a backslash) or enter it on a single line without a backslash:
	`dd if=/dev/rdsk/c0t1d0s6 of=/dev/rst0 bs=10b \`
	`count=10000`

braces { }	Braces indicate required items: `.DEFINE {macro1}`
brackets [ ]	Brackets indicate optional items: `cvtcrt termname [outfile]`
ellipses ...	Ellipses indicate an arbitrary number of similar items:

Convention	Description
	`CHKVAL fieldname value1 value2 ... valueN`
italics	Italic type indicates a variable. Substitute a value for the variable: `library_name`
vertical line |	A vertical line indicates a choice within braces or brackets: `FILE filesize [K|M]`
forward slash /	A forward slash is used as an escape character in the Oracle VM Manager Command Line Interface to escape the special characters ", ', ?, \, /, <, >: `create Tag name=MyTag description="HR/'s VMs"`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

Access to Oracle Support for Accessibility

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit https://www.oracle.com/corporate/accessibility/learning-support.html#support-tab.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Chapter 1 Oracle VM Security Overview

Table of Contents

This section gives an overview of the product and explains the general principles of application security.

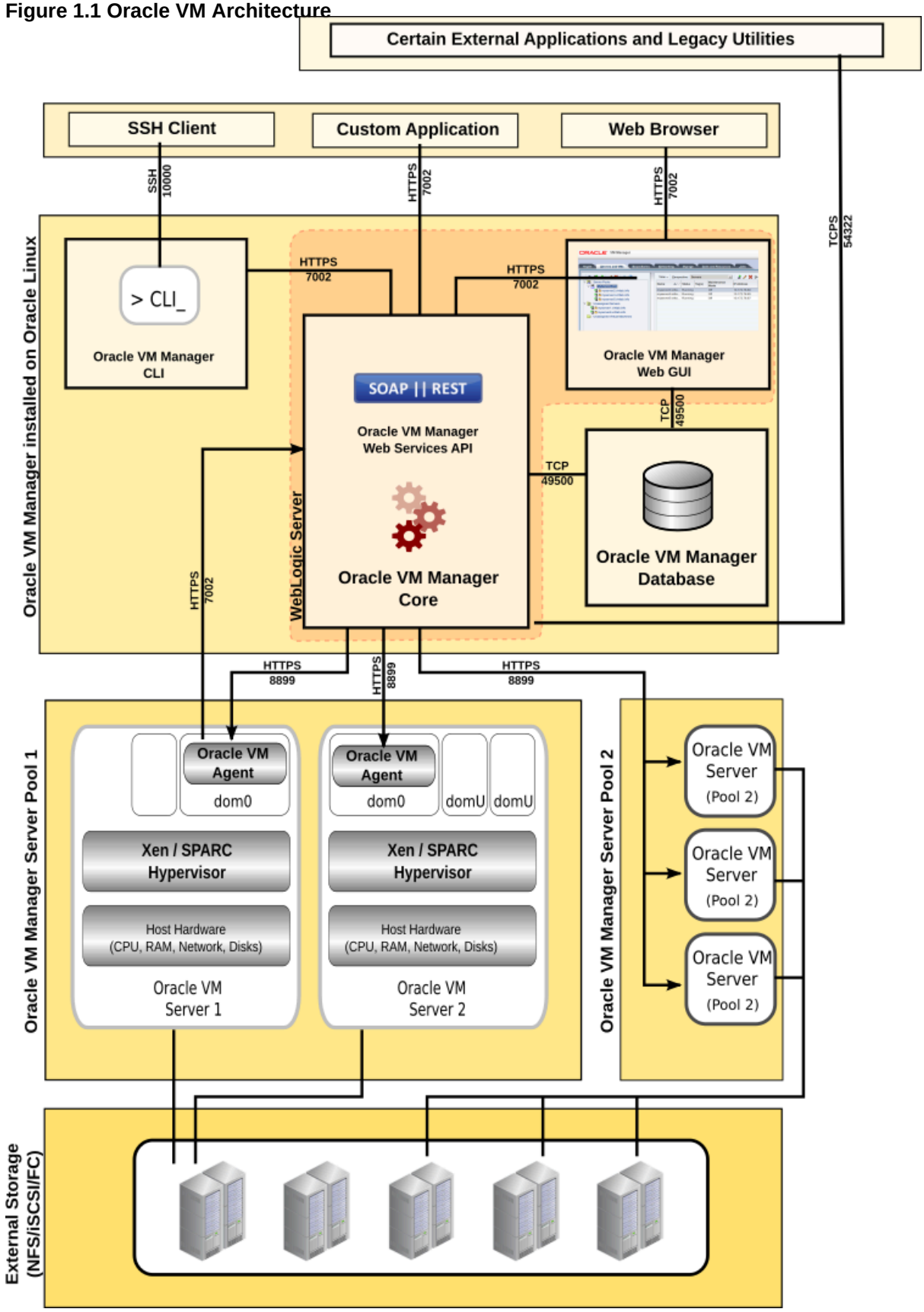
1.1 Oracle VM Overview

Oracle VM is a platform that provides a fully equipped environment with all the latest benefits of virtualization technology. Oracle VM enables you to deploy operating systems and application software within a supported virtualization environment.

1.1.1 What is the Oracle VM Architecture?

Oracle VM is a platform that provides a fully equipped environment with all the latest benefits of virtualization technology. Oracle VM enables you to deploy operating systems and application software within a supported virtualization environment. Oracle VM insulates users and administrators from the underlying virtualization technology and allows daily operations to be conducted using goal-oriented GUI interfaces. The components of Oracle VM are shown in Figure 1.1, “Oracle VM Architecture”.

Figure 1.1 Oracle VM Architecture



- **Client Applications:** Various user interfaces to Oracle VM Manager are provided, either via the graphical user interface (GUI) accessible using a web-browser; the command line interface (CLI) accessible using an SSH client; or external applications, such as Oracle Enterprise Manager, custom built applications or scripts that use the Web Services API (WS-API). All communications with Oracle VM Manager are secured using either a key or certificate based technology.

- **Oracle VM Manager:** Used to manage *Oracle VM Servers*, virtual machines, and resources. It is comprised of a number of subcomponents, including a web browser-based user interface; and a command line interface (CLI) allowing you to manage your infrastructure directly from the command line either via external scripts or by running manual command sequences. Each of these interfaces run as separate applications and interface with the Oracle VM Manager core application using the Web Services API.

  Oracle VM Manager is usually hosted on a standalone computer but it can also be run as a virtual machine in a carefully designed environment. However, support for running Oracle VM Manager on a virtual machine is limited and caveats apply. For more information, see the *Running Oracle VM Manager as a Virtual Machine* section of the Oracle VM Installation and Upgrade Guide.

  The Oracle VM Manager core application is an Oracle *WebLogic* application that runs on Oracle Linux. The user interface uses the Application Development Framework (ADF) application, providing a common look and feel, in line with other Oracle web-based applications. While the Oracle VM Manager core application and the Oracle VM Manager Web Interface are both WebLogic applications, they are separate applications, even though they share the same process space.

  While the Oracle VM Manager Web Interface and Oracle VM Manager Command Line Interface both use the Web Services API to interface with the Oracle VM Manager core application, the Oracle VM Manager Web Interface can query the Oracle VM Manager database directly for read-only operations. This design decision allows the Oracle VM Manager Web Interface to provide a wider range of filtering options and improves performance for some operations.

  Oracle VM Manager communicates with each Oracle VM Server via the Oracle VM Agent, using XML-RPC over HTTPS on port 8899. Actions on servers that are initiated within Oracle VM Manager are triggered using this method. The Oracle VM Agent on each Oracle VM Server is equally able to send notifications, statistics and event information back to Oracle VM Manager. Actions within Oracle VM Manager triggered by Oracle VM Agent are achieved using the Web Services API exposed by Oracle VM Manager and are secured using HTTPS.

  While Oracle VM Manager is a critical component for configuration actions within the Oracle VM infrastructure, the virtualized environment can continue to function properly even if Oracle VM Manager experiences downtime. This includes the ability to maintain *high availability* and to perform *live migration* of virtual machines running on an x86 platform. Note that live migration of virtual machines running on a SPARC platform, *does* require that the Oracle VM Manager is running to succeed, since the only supported method of performing a live migration on this platform is either through the Oracle VM Manager Web Interface or the Oracle VM Manager Command Line Interface.

- **Oracle VM Manager Database:** Used by the Oracle VM Manager core application to store and track configuration, status changes and events. Oracle VM Manager uses a MySQL Enterprise database that is bundled in the installer and which runs on the same host where Oracle VM Manager is installed. The database is configured for the exclusive use of Oracle VM Manager and must not be used by any other applications. The database is automatically backed up on a regular schedule, and facilities are provided to perform manual backups as well.

- **Oracle VM Server:** A managed virtualization environment providing a lightweight, secure, server platform which runs virtual machines, also known as domains. At least one Oracle VM Server is required, but several are needed to take advantage of clustering.

Oracle VM Server is installed on a bare metal computer, and contains the *Oracle VM Agent* to manage communication with Oracle VM Manager. *dom0* is an abbreviation for *domain zero*, the management or *control domain* with privileged access to the hardware and device drivers. *DomU* is an unprivileged *domain* with no direct access to the hardware or device drivers. A user-domain (domU) is started and managed on an Oracle VM Server by dom0.

On x86-based systems, Oracle VM Server is based upon an updated version of the underlying Xen *hypervisor* technology, and includes Oracle VM Agent. It also includes a Linux kernel with support for a broad array of devices and file systems. The Linux kernel is run as dom0 to manage one or more domU virtual machines, each of which could be Linux, Oracle Solaris, or Microsoft Windows™.

In contrast, Oracle VM Server for SPARC takes advantage of the hypervisor that is already included within the SPARC firmware, alongside the Oracle VM Agent for SPARC. The default Oracle Solaris operating system is usually promoted to act as the primary domain, which is equivalent to dom0 on x86 systems. Once the primary domain is in place, it can be used to create and manage further domains running different versions of the Oracle Solaris operating system.

Groups of Oracle VM Servers are usually clustered together to create server pools. This allows Oracle VM Manager to handle load balancing and failover for high-availability environments. Virtual machines run within a server pool and can be easily moved between the different servers that make up a server pool. Server pools also provide logical separation of servers and virtual machines. Server pools are required entities within the Oracle VM infrastructure, even if they consist of only one server.

Each Oracle VM Server maintains its own Berkeley Database, used to store local configuration and runtime information. This allows the Oracle VM Server to continue to function normally, even if Oracle VM Manager becomes unavailable for a period. Where Oracle VM Servers are clustered together, a separate cluster database, stored in the server pool file system, is shared between the servers. This allows the server pool to continue to provide clustering features, such as High Availability, even if Oracle VM Manager is unavailable.

- **External Shared Storage:** Provides storage for a variety of purposes and is required to enable high-availability options afforded through clustering. Storage discovery and management is achieved using the Oracle VM Manager, which then interacts with Oracle VM Servers via the storage connect framework to then interact with storage components. For morre information, see the *Understanding Storage* chapter of the Oracle VM Concepts Guide. Oracle VM provides support for a variety of external storage types including NFS, iSCSI and Fibre Channel.

1.1.2 Security Aspects of Oracle VM

The Oracle VM security architecture, by design, eliminates many security threats. The guidelines for secure deployment of virtualized solutions based on Oracle VM are largely based on network security. As these guidelines are generally applicable, they should always be reviewed for applicability in the context of each implementation and the security requirements and policies of the broader environment in which Oracle VM is deployed.

The following list describes the main aspects of the Oracle VM security architecture:

- Both Oracle VM Server and Oracle VM Manager provide an Oracle Linux environment that includes `iptables` or `firewalld` firewall with a default ruleset and policies.
- Oracle VM Server is a minimalist OS implementation derived from Oracle Linux and uses the Unbreakable Enterprise Kernel (UEK) Release 4 for enhanced performance and scale. By design, it has few moving parts and a minimum of network exposed services to reduce administrative effort, overhead, and attack surface.

- Oracle VM Manager 3.3.1 environments, and above, may only use the bundled MySQL database which is installed locally on the same host where Oracle VM Manager is installed. Access is restricted to localhost connections and is not remotely accessible. Furthermore, backup processes are automated to assist with recovery in the case of failure. The MySQL database may not be used for any other application outside of Oracle VM Manager.
- Default installations of Oracle VM Server or Oracle VM Manager do **not** provide physical security. They can be booted (using runlevel 1 or a rescue cd) and compromised by anyone with access to the physical console. Suitable physical security should be provided to prevent this type of exposure.
- TLS is used extensively to secure and authenticate communications between Oracle VM Manager and Oracle VM Servers; to secure and authenticate access to the Oracle VM Manager Web Services API; to secure all HTTPS communications and within the network component of a VM migration.
- The Oracle VM Servers' administrative connection to Oracle VM Manager uses HTTPS by default.
- Openssh along with public/private key authentication are fully supported on Oracle VM Server.
- 802.1q VLANS are fully supported for segregating VM and dom0 network traffic.

All components of the Oracle VM installation communicate with each other in a secure way. The following table shows, in detail, how each individual line of communication is set up securely:

Communication	**Description**
Browser to Oracle VM Manager GUI	When you log on to Oracle VM Manager, we strongly recommend that you use HTTPS and connect to TCP port 7002, since the user interface expects you to authenticate using a username and password, which must be protected. SSL encrypted communication is available as of version 3.1.1, and regular HTTP connectivity at TCP/7001 is disabled by default. However, it may be enabled via *Oracle WebLogic Server* for testing and demo purposes. In Oracle VM 3.3 and above, the SSL certificate that is used for communication encryption is generated by default within Oracle VM Manager and is signed by an internal CA (Certificate Authority) certificate within Oracle VM Manager. Tools are available to replace this certificate with one signed by a trusted third-party CA, if required, or alternately to obtain the internal CA certificate to add it to your own trusted CA certificates within your web-browser or application keystore. This CA certificate can be used to validate the SSL certificate presented when you connect to the HTTPS port for Oracle VM Manager. More information on the tools provided to manage these certificates is provided in *Oracle VM Administrator's Guide*. As of Oracle VM Release 3.4.5, TLS version 1.2 (TLSv1.2) is the default within Oracle VM Manager.
Oracle VM Manager GUI to Oracle VM Core	The Oracle VM Manager application uses the underlying Web-Services API to communicate with Oracle VM Core, running on the same server. The Web-Services API is exposed on the same HTTPS port as the Oracle VM Manager application, since it is served out of the same process space within Oracle WebLogic Server. All communication is secured using the same SSL certificate that is used to encrypt communications between the Oracle VM Manager GUI and a web-browser. Authentication of the Oracle VM Manager application to Oracle VM Core is achieved using the username and password of the user that authenticated against the user interface front-end. When the Oracle VM Manager application is started, it makes a connection to the Oracle VM Core Web-Services API to populate the GUI model and to

Communication	Description
	periodically poll for events to keep the GUI model up-to-date. Authentication of the Oracle VM Manager application to Oracle VM Core for this purpose is achieved using an SSL certificate. This certificate is generated during the installation of Oracle VM Manager. The certificate is signed and registered by the internal CA, which is used by Oracle VM Core to validate and authenticate connections from the Oracle VM Manager application. The public certificate for this certificate-key pair is stored in a Java truststore available to the Oracle VM Core. The private key for this certificate is stored within a secure Java keystore within the Oracle VM Manager application.
Web Services to Oracle VM Core	Oracle VM Core offers a web services API (WSAPI) that provides a REST endpoint exposed via HTTPS available on TCP port 7002. Communications are encrypted using the same SSL certificate that is used to encrypt communications between the Oracle VM Manager GUI and a web-browser. It is possible to register and sign a certificate to perform certificate based authentication with Oracle VM Core using the keytool management application described in Setting Up SSL in the *Oracle VM Administrator's Guide*, or programmatically using the methods provided by the WSAPI itself, as discussed in Certificate Management for Certificate-based Authentication Using REST in the *Oracle VM Web Services API Developer's Guide*. When creating a certificate to use for authentication purposes, it is highly advisable that the certificate key is generated with an adequate passphrase, and that the certificate and key are stored either in a passphrase protected keystore, or that they are stored in a protected area on the file system with access permissions limited to the user that intends to use them.
Client to CLI	The Oracle VM Manager Command Line Interface (CLI) is officially supported as of version 3.2.1. The client connects to the CLI, which runs on the Oracle VM Manager host, using SSH over port TCP/10000. A public key can be set up in the SSH server in order to allow CLI users to log on automatically without having to enter credentials each time. If this approach is used, it is recommended that a passphrase is still set for the private key and that an SSH Agent is used to handle the authentication of the key for repeated requests. The private key must be stored in a secure location on the file system with access permissions limited to the user that intends to use it. As of version 3.4.1, the CLI also supports the option to obscure sensitive information on screen as it is entered into the CLI. This facility is described in more detail in Masking Sensitive Data in the *Oracle VM Manager Command Line Interface User's Guide*. Users must ensure that this facility is used when entering sensitive data into the CLI, such as when sending passwords using the VM messaging channel.
CLI to Oracle VM Core	The Oracle VM Manager Command Line Interface (CLI) communicates with Oracle VM Core via the Web-Services API on TCP/7002 using HTTPS. Communications are encrypted using the same SSL certificate that is used to encrypt communications between the Oracle VM Manager GUI and a web-browser. Authentication of the CLI to Oracle VM Core is achieved using the username and password of the user that authenticated against the user interface front-end.
Oracle VM Agent to Oracle VM Core	The Oracle VM Agents running on the Oracle VM Servers use SSL/TLS encryption to communicate with Oracle VM Core via TCP/7002 (HTTPS) through the WSAPI. Authentication is achieved using an SSL certificate registered for the Oracle VM Agent when ownership is taken. The API access

Communication	Description
	is limited to the type of communications that the Agent has with Oracle VM Core, such as the notification of events and the provision of statistical information.
Oracle VM Core to Oracle VM Agent	Oracle VM Core, in turn, uses TCP/8899 to communicate with the Oracle VM Agents in the environment. The protocol is also HTTPS. Oracle VM Core initially authenticates itself to the Oracle VM Agent using a username and password combination during the process of taking ownership of the Oracle VM Server. Once the Oracle VM Core has been authenticated by the Oracle VM Agent, an additional SSL certificate is exchanged so that the Oracle VM Agent can perform future authentication of the Oracle VM Core using an SSL certificate-key pair, and *vice versa*.
VNC and Serial Console Access	Oracle VM Manager opens a secure SSL-encrypted connection to the VNC server that is created by the Xen hypervisor for each remote virtual machine running on an Oracle VM Server. These are accessed on the Oracle VM Server on TCP ports 6900 and up. Connections from client web-browsers take advantage of the noVNC console that is provided within the Oracle VM Manager web user interface. This connection uses the same TCP 7002 port as used to access the web user interface, and this is secured using the same SSL certificate. For serial console connections, Oracle VM Manager opens a secure SSL-encrypted connection to the serial terminal exported for each remote virtual machine running on an Oracle VM Server. These are accessed on the Oracle VM Server on TCP ports 10000 and up. Connections from client web-browsers take advantage of the jsTerm terminal emulator that is provided within the Oracle VM Manager web user interface. This connection uses the same TCP 7002 port as used to access the web user interface, and this is secured using the same SSL certificate.
Live Migration	Traffic related to live migration of virtual machines uses separate ports: TCP/8002 for non-encrypted and TCP/8003 for SSL-encrypted (TCPS) live migration. Secure live migration is a setting the user needs to switch on in the server pool properties as required. Based on this setting, Oracle VM Manager initiates SSL or non-SSL migration of the running virtual machine. For optimized security and performance, consider further network segregation by creating a separate network for live migration.
Oracle VM Agent Certificate	At installation, the Oracle VM Agent generates an SSL key and matching certificate. The properties are: • key algorithm: RSA. • private key size: 2048 bits. • certificate data management: according to X.509 standard. • location of the SSL key and certificate: `/etc/ovs-agent/cert`. By default, VNC traffic, virtual machine migration traffic and Oracle VM Agent communications are all secured using the same SSL key and certificate. The administrator can regenerate the key/certificate combination via the Oracle VM Server command line by means of this command: `ovs-agent-keygen`. It is technically possible to use separate SSL keys and certificates for Oracle VM Agent communications and for secure virtual machine migration. Note that

Communication	Description
	changing the SSL key and certificate combination on a server, requires that the server is released from ownership by Oracle VM Manager and that you will need to take ownership of the server again after the operation is completed. During the process where an Oracle VM Manager instance takes ownership of the Oracle VM Server, the public certificate used by the Oracle VM Agent is exchanged with Oracle VM Manager and it is signed and registered with the Oracle VM Manager instance using an internal CA certificate. A new key is generated and provided to the Oracle VM Agent. This key and the signed certificate is used to authenticate and secure subsequent communications with Oracle VM Manager.
Other traffic	In an Oracle VM environment, the Oracle VM Manager host is frequently used as the reference to provide time synchronization. In this case, an inbound connection from all Oracle VM Servers to UDP port 123 is required for NTP traffic. Oracle VM Servers in a clustered server pool use an OCFS2 pool file system and require a heartbeat network function to determine the status of each cluster member. The port used for this specific type of traffic is TCP/7777. Some external applications may continue to use the legacy API, which is available on TCP/54322 and is secured using SSL/TLS. This API is deprecated, and applications currently making use of it must be upgraded in the future. If you are not using any other applications outside of Oracle VM itself, to perform management within your environment, you should ensure that access to this port is disabled in your firewall rules.

Note

As of Oracle VM Release 3.4.5, all SSL/TLS encrypted communications use the TLSv1.2 protocol for messages that are sent and accepted. SSLv3 and TLSv1 are disabled by default within Oracle VM Manager for security reasons.

1.1.3 Security Considerations for Oracle VM

In this section, we explore some important security considerations that you must be aware of when using Oracle VM.

Limitation of Access To The Oracle VM Manager Host

It cannot be stressed enough that the Oracle VM Manager Core is a very powerful component within an Oracle VM deployment, providing control over many servers and virtual machines. With this in mind, access to this host should be severely restricted. User accounts should be limited to administrators who require access to manage a deployment. Furthermore, firewall rules should be hardened to limit access to networks where administrators may be located.

Users with access to utilities or tools that communicate with the Oracle VM Manager Core in any way, should be aware that the credentials that they use to authenticate, whether by username and password or by SSL certificate, are highly sensitive and that a compromise of this nature does not only threaten Oracle VM Manager itself, but also makes every server and virtual machine within the deployment vulnerable to attack.

Appropriate security practice with regard to identity and credential management should always be observed.

See Section 1.2, “General Oracle VM Security Principles” for more guidelines on system protection.

Encrypted Communication

Many communications with Oracle VM Manager over HTTPS are encrypted using an SSL certificate to protect the communication of sensitive information. By default, this certificate is signed by an internal CA certificate that is generated for the Oracle VM Manager instance during installation. Since most client applications, including user web browsers, will not have this CA certificate installed it is not possible for many client applications to validate the SSL certificate presented when accessing an Oracle VM Manager service over HTTPS. Some client applications may fail entirely if an SSL certificate cannot be validated, while other applications may simply issue a warning and allow users to proceed at their own risk. To minimize the likelihood of a man-in-the-middle attack, it is important that validation can actually take place. Therefore, it is appropriate to take one of the following courses of action:

- Install the CA certificate for the Oracle VM Manager instance into the trusted CA certificate store for all client applications that will have access to Oracle VM Manager.
- Change the SSL certificate used for HTTPS communications by Oracle VM Manager to use a certificate that is signed by a trusted third-party CA, for which all of your client applications already have the CA certificate installed.

These operations are discussed in detail in Setting Up SSL in the *Oracle VM Administrator's Guide*.

During initial Oracle VM Server discovery and key exchange, passwords are sent over the wire from the Oracle VM Manager to the Oracle VM Agent for authentication purposes. This communication is performed over SSL so should be secure. However, no certificate validation is performed against the Oracle VM Agent certificate at this point since the Oracle VM Agent certificate is unknown. Therefore, it is possible that this channel might be subject to a man-in-the-middle attack wherein a malicious entity impersonates the server so that the manager sends the password to this entity in an attempt to authenticate. Where possible the Oracle VM Manager system should be run within the same local area network as the Oracle VM Servers within your Oracle VM environment, and this network should have appropriate security controls to mitigate the risk that a malicious attacker is able to perform a man-in-the-middle attack. Additionally, it is worthwhile ensuring that the passwords for the Oracle VM Agent on each Oracle VM Server is unique. This means that in the unlikely event that a single server is compromised via a man-in-the-middle attack, access to all servers within the deployment is not immediately gained and the damage can be limited.

Certificate Based Authentication

It is a common misconception that use of certificate-based authentication automatically makes a system more secure than the use of passwords, but this is not necessarily true. Certificate-based authentication is susceptible to many of the same attacks as password authentication. In this section we will discuss some of the ways in which this system could be attacked so that the security level can be well understood. All protocols that are used conform to current best practices documented in the OSCS (Oracle Secure Coding Standard).

In general, certificate authentication is less susceptible to dictionary attacks as well as brute-force attacks over the secure communication channel. However, in order for an SSL certificate to be signed and registered by Oracle VM Manager, password-based authentication is still used within Oracle VM Manager. This is particularly relevant to the Oracle VM Agent, which must use password-based authentication to support initial discovery and take ownership requests, as well as to allow discovery by secondary (non-owning) managers. Equally, it cannot be assumed that every user is issued with an SSL certificate-key pair that can be configured for use within a web browser to authenticate requests to use the Oracle VM Manager Web Interface. As a result, the Oracle VM Manager Web Interface only supports password-based authentication. Therefore, there are still channels within Oracle VM that are open to dictionary and

brute-force attacks. These risks could be minimized by restricting access to systems using a strict firewall policy based on the requirements for different systems that need access to one another. It is important to understand that password exchanges are always encrypted using SSL/TLS, and are never exposed in clear text. Furthermore, stored passwords are always encrypted on the systems that hold them.

Where certificate-based authentication is used, if the private key used on either end of the communication is compromised, the attacker could use that private key and corresponding certificate to log into the other entity. On Oracle VM Manager, keys are encrypted and stored within a JKS keystore file which is protected by both a key password and a keystore password. These passwords are long, randomly generated passwords which are stored in the Oracle CSF (Credential Store Framework). The length and random nature of these passwords should preclude dictionary or brute-force attacks, but if the CSF is compromised then the keys could be retrieved. This mechanism conforms to the current security guidelines outlined by the OSCS.

In the case of Oracle VM Agent, the keys and certificates are stored in a non-encrypted PEM format. These files are readable only by the root user, but if the root user account is compromised, a user could then use this information to send bogus notification information to the manager. Likewise, a malicious user with root access could replace the Oracle VM Manager certificate information on the Oracle VM Agent with their own certificate to allow themselves to be authenticated for Oracle VM Agent commands. However, if they have already compromised the root account on the server this is probably a moot point since they already have unrestricted access to the system.

In the case where you choose to use certificate-based authentication within custom-built applications that make use of the WSAPI, you must ensure that appropriate actions are taken to protect keys from misuse. This includes setting a reasonable passphrase for your keys and ensuring that the keys are preferably stored in an encrypted format. A malicious user with access to a key that is registered for authentication against Oracle VM Manager has full access to the entire Oracle VM environment including all virtual machines, all storage, all servers and Oracle VM Manager itself.

When certificates are registered for authentication with Oracle VM Manager, the authorized certificate that allows authentication to the manager to take place is stored in the Oracle VM Manager database. This certificate only contains public key information, so it cannot be used in and of itself to log into Oracle VM Manager. However, a user who can modify the Oracle VM Manager database could replace this with a certificate of their own. For this attack vector to work, the certificate would need to be signed by a trusted CA (such as the Oracle VM Manager CA). Therefore, the risk can be mitigated by proper administration of the WebLogic trust store. To access the Oracle VM Manager CA private key to create such a certificate, the CSF would have to be compromised as well.

1.2 General Oracle VM Security Principles

The following principles are fundamental to using any application securely.

1.2.1 Keep Software Up-to-Date

One of the principles of good security practice is to keep all software versions and patches up-to-date. Throughout this document, we assume that you are installing the necessary security patches and package updates on the Oracle Linux host running *Oracle VM Manager*, as well as the *Oracle VM Servers* in your environment. It is recommended that you:

- Register your Oracle VM Manager host with the Unbreakable Linux Network (ULN). See Unbreakable Linux Network for information on using ULN.
- For x86-based Oracle VM Servers, set up a local YUM repository and retrieve the updates from the Oracle VM channel on ULN. See the *Getting Started with Oracle Linux Yum Server* article on OTN. As of

Oracle VM Release 3.3, you can upgrade SPARC-based servers using an IPS server update repository. See the *Oracle VM Manager User's Guide* for information on setting up these server update repositories.

- Create server update repositories for your Oracle VM Servers in Oracle VM Manager. See the *Oracle VM Manager User's Guide* for more information on creating server update repositories.

1.2.2 Restrict Network Access to Critical Services

Secure your network properly with firewalls. Software firewalls are part of the Oracle VM Manager and Oracle VM Server installations, but a best practice is to use an external firewall in addition. Keep all Oracle VM services on private network segments and allow public access only to and from services and systems that effectively require it. While firewalls are not infallible, they provide a high level of certainty that access to these systems is limited to a known network route, which can be monitored and further restricted, if necessary.

Should you decide to restrict access based on IP address, note that this often causes application client/server programs to fail for DHCP clients. In general, this is resolved by using static IP addresses or IP address reservation on the DHCP server. Note that with address reservation on the DHCP server, a connection may still fail if the IP lease expires while the DHCP server is unreachable. For Oracle VM in particular, static IP address assignment is highly recommended. In fact, the Oracle VM Manager host must maintain its IP address because the Oracle VM Servers under its control all record that IP address during server discovery. The IP is stored in the Oracle VM Agent database and used for communication with Oracle VM Manager. The same mechanism applies to the virtual IP address of a server pool, which must also be statically configured.

The network model of a given Oracle VM implementation depends on the hardware used, the scale of the environment, and the particular services deployed through its guest virtual machines. Various network configurations, security features of the network model, and guidelines for each networking type are described in more detail in the Security Features chapter; more specifically in Section 3.1, “Oracle VM Network Model”.

1.2.3 Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over-ambitious granting of responsibilities, roles, grants, etc., especially early on in an organization’s life cycle when people are few and work needs to be done quickly, often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

However, Oracle VM is a server virtualization solution, and is an administrator's tool in the first place. Access to Oracle VM Manager is controlled by the underlying WebLogic application server, and while it is possible to create multiple accounts to log in to Oracle VM Manager, the privileges for all administrator accounts are the same. Consequently, it is recommended to create administrator accounts only for those who need full access to Oracle VM configuration and resources, and to use a strong password on each account. Use passwords between 8 and 16 characters in length consisting of a combination of small letters, capital letters and numeric characters.

For users who need access to one or more virtual machines, but are not allowed to modify the Oracle VM configuration, an administrator may set up remote access on the virtual machines. For a Windows server, RDP can be used; for a Unix server you can use SSH for command line access, and VNC in case a graphical desktop environment is used. Connect the virtual machines to a network that is accessible from the trusted internal network.

If the specific implementation of Oracle VM is a large scale configuration that requires finer grained role based access control, an alternative is to manage the environment through Oracle Enterprise Manager Ops Center. In this configuration, access control is an integral part of Enterprise Manager Ops Center.

Oracle VM subscriptions include full, complete use of Oracle Enterprise Manager Cloud Control and Oracle Enterprise Manager OpsCenter. Customers who purchase Oracle VM subscriptions have an included license to use these products' virtualization and operating system management features as part of Oracle VM. The complete set of products (Oracle Enterprise Manager Cloud Control, Oracle Enterprise Manager OpsCenter, Oracle VM Manager and *Oracle VM Agent*) are regarded as one product suite.

1.2.4 Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice and regularly monitor audit records.

As an Oracle VM administrator you have access inside the Oracle VM Manager GUI to events and statistics. These are your first indicators of potential problems, including security risks. Particularly important errors to investigate are Oracle VM Server *disconnect* and *offline* events, as they indicate unexpected connectivity issues.

Oracle VM keeps a number of log files on different components in the environment. These log files are important for the manageability and supportability of Oracle VM. The following tables provide an overview of the log files that can assist you in troubleshooting and security auditing:

Oracle VM Manager Logs

Log Files	Location	Description
Oracle VM Manager installation or upgrade log	/tmp/install-yyyy-mm-dd-<id>.log - and/or - /tmp/upgrade-yyyy-mm-dd-<id>.log	All actions and operations that take place during an installation or upgrade procedure are saved to this file. Some log entries are simply informative, but a lot of debugging information is included.
Oracle VM Manager logs	/u01/app/oracle/ovm-manager-3/domains/ovm_domain/servers/AdminServer/logs/	The `access.log` file contains information about Oracle VM domain access and status. These logs actually come from the WebLogic server. The `AdminServer.log` file contains information similar to the events and statistics in Oracle VM Manager, but the logging is more detailed and more verbose.
CLI logs	/u01/app/oracle/ovm-manager-3/domains/ovm_domain/servers/AdminServer/logs/CLIAudit.log /u01/app/oracle/ovm-manager-3/domains/ovm_domain/servers/AdminServer/logs/CLI.log	In `CLIAudit.log`, located on the Oracle VM Manager host, the CLI maintains a full audit log of all executed commands. The `CLI.log` file contains CLI component entries.

Oracle VM Server Logs

Log Files	Location	Description
Oracle VM Agent log	/var/log/ovs-agent.log	The Oracle VM Agent log is essential for auditing of internal communications and connectivity of the physical servers in

Log Files	Location	Description
		your environment. From a security point of view, entries from authentication and connection failures with bad credentials, or an unusual number of access attempts could indicate unauthorized access attempts.
Oracle VM Agent notification log	/var/log/devmon.log	This file contains all details of what the Oracle VM Agent sends to Oracle VM Manager: all events from the server, including storage device events, network events etc.
Oracle VM console log	/var/log/ovm-consoled.log	This file logs all details for the Oracle VM console server that exports guest consoles.
Oracle VM Storage Connect plug-in log	/var/log/osc.log	This file logs all installation activities related to Oracle VM Storage Connect plug-in. It shows which plug-ins have been installed, which version is in use, and when exactly the installation has taken place.
Xen hypervisor logs	/var/log/xen/	The `xend.log` file contains detailed information about Xen-specific operations. It is particularly useful to track errors related to virtual machines, such as start or migration failures.

In the context of product security and auditability, the various log files show which operations have been performed by each Oracle VM Manager administrator account. Also, any unauthorized login attempt on Oracle VM Manager or SSH connection failure to an Oracle VM Server is reflected in the log files. Monitor the logs actively in order to detect security issues as early as possible.

1.2.5 Stay Up-to-Date on Latest Security Information

Oracle continually improves its software and documentation. Check the Oracle web site and relevant product and technology pages regularly. For example:

- Oracle Technology Network
- Oracle Virtualization Home
- Unbreakable Linux Network

1.3 Understanding your Oracle VM Environment

To better understand your security needs, ask yourself the following questions:

- **Which resources am I protecting?**

  The resources in an Oracle VM environment are the components previously listed: the Oracle VM Manager application and the Oracle Linux operating system it runs on, the Oracle VM Servers (domain 0 OS instances), and the guest virtual machines, including those that serve as templates. The last of these is the most straightforward to understand, and is similar to protecting the data and applications of non-

virtual systems, but is more complicated in a virtualized environment because a compromised guest puts not only its own contents at risk, but also exposes its neighbors and the infrastructure they use to the same risks. The network and storage resources upon which they depend must not be forgotten, as they also represent resources that must be protected, and are potential points of attack. Each of these has unique protection requirements that should be understood.

- **From whom am I protecting the resources?**

  The Oracle VM Server environment must be protected from physical intrusions, but most notably from network based attacks via any of the networks to which the systems are connected. If this is an Internet-facing environment, then resources must be protected from everyone on the Internet. If this is an intranet environment, it needs to be protected from unauthorized actions by employees or contractors. Since virtual machine environments are typically multi-user, multi-tenancy environments, the users should be protected from one another. Access to virtual machine assets, such as consoles, should only be provided to individuals responsible for operating them, just as with physical machines. System administrators should have access to only the resources needed to do their job, both to protect from errors or deliberate penetration on their parts, but also to protect against inadvertent compromise if their computers or login credentials are compromised. You might consider giving access to highly confidential data or strategic resources to only a few well trusted system administrators.

- **What will happen if the protections on strategic resources fail?**

  A failure in security protection can cause substantial damage, depending on which resource has been compromised. Understanding the security ramifications of each resource will help you protect it properly. A security failure with a guest virtual machine obviously compromises the data and applications residing in that guest, but also provides an intruder an attack vector that can be used to attack other guests and the Oracle VM Server, for example, by snooping their network traffic, mounting a denial of service attack, or spoofing their IP addresses. Compromising an Oracle VM Server would additionally permit an attacker to gain access to guests' virtual disks and consoles, or cause outages. A compromised Oracle VM Manager instance would permit an intruder to gain control of the server pool's resources, gain access to virtual disks and consoles, and attack all the servers and disks.

For all these reasons, the most secure environment will be based on the *defense in depth* principle, in which there are multiple layers of protection so that a failure in one area, such as a compromised password, does not place the entire environment at risk.

Chapter 2 Performing a Secure Oracle VM Installation

Table of Contents

This section provides an overview to planning an installation, and instructions for installing a secure system. It describes security-related deployment issues for each installed component; for example, MySQL database and Oracle WebLogic Server.

Oracle VM Manager automatically installs into a secure state. This section explains any security implications for choices made in the installation procedure, and how to enable any high security options, such as SSL. As the installation instructions suggest, the user should avoid installing or running components that are not needed in a specific deployment.

Security measures applied in a default installation include:

- Active software firewalls which only open standard required ports.

Note

If your firewall has been disabled prior to installation, you should enable the `iptables` or `firewalld` service after installation to allow the firewall rules to take effect.

- SSL encryption for all *Oracle VM Agent* communications.

Note

If you are upgrading from an Oracle VM version older than build 3.1.1.165, some Oracle VM Agent communications that were previously unencrypted are automatically reconfigured. From this build forward, SSL encryption is set by default for all Oracle VM Agent communications.

- HTTPS access to the Oracle VM Manager GUI.
- User credentials and authentication managed by Oracle WebLogic Server security realms:

  https://docs.oracle.com/middleware/1213/wls/SCOVR/realm_chap.htm#SCOVR186

- Small footprint JeOS-like operating system: Oracle Linux without unused packages in order to minimize attack surface.

2.1 Oracle VM Pre-Installation Tasks

This section describes any security configuration that must be applied before installation.

2.1.1 Preparing the Oracle VM Management Server

The Oracle VM management server must run one of the following operating systems:

- Oracle Linux (or Red Hat Enterprise Linux) 6 64-bit or later.
- Oracle Linux (or Red Hat Enterprise Linux) 7 64-bit or later.

It is recommended to leave all ports closed except the ones required by *Oracle VM Manager*. The required ports are:

- For inbound web browser connection: TCP/7002 (HTTPS, default).
- For inbound connection from Oracle VM Servers: TCP/7002 (HTTPS, default), UDP/123 (NTP).
- For outbound connection to Oracle VM Servers: TCP/8899 (Oracle VM Agent), TCP/6900-xxxx (VNC, 1 secure tunnel per virtual machine).
- For SSH access: TCP/22 (likely open by default).
- For CLI access using SSH: TCP/10000.

Note

The Oracle VM Manager Command Line Interface (CLI) is part of Oracle VM as of Release 3.2.

As part of the installation procedure, a script is included named `createOracle.sh`. You can run this script to perform a number of installation tasks in an automated way, including the standard firewall configuration.

For Oracle Linux (or Red Hat Enterprise Linux) 6, if the `iptables` package is installed, then the `iptables` rules are added during the installation. However, for Oracle Linux (or Red Hat Enterprise Linux) 7 and beyond, if the `firewalld` package is installed, then the `firewalld` rules are added.

Note that if `iptables` or `firewalld` has been disabled on the target host prior to the installation of Oracle VM Manager, the `createOracle.sh` script does not automatically re-enable the `iptables` or `firewalld` service. No rules are added if the firewall managements tools are *not* installed. Any rules added take effect when the service is enabled.

If firewall management tools are enabled, even if there are no rules defined, each packet is checked by the firewall management tools, which can have an impact on performance.

If you prefer or need to configure the firewall manually, follow these instructions.

For `iptables`, open the required ports in `iptables` as follows:

1. Log on to the Oracle VM management server as the `root` user.
2. At the command prompt, enter the appropriate command for each port to be opened; for example:

```
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 7002 -j ACCEPT
# iptables -A INPUT -m state --state NEW -m udp -p udp --dport 123 -j ACCEPT
# iptables -A INPUT -m state --state NEW -m udp -p udp --dport 10000 -j ACCEPT
```

3. Save the `iptables` configuration.

```
# service iptables save
```

This does not require `iptables` to be restarted as the commands open the ports while `iptables` is running. The save ensures they are opened on reboot/restart in future.

For `firewalld`, open the required ports in `firewalld` as follows:

1. Log on to the Oracle VM management server as the `root` user.
2. At the command prompt, enter the appropriate command (which persists over reboot) for each port to be opened; for example:

```
# firewall-cmd --permanent --zone=public --add-port=7200/tcp
# firewall-cmd --permanent --zone=public --add-port=123/udp
# firewall-cmd --permanent --zone=public --add-port=10000/tcp
# firewall-cmd --reload
```

2.1.2 The Oracle VM Firewall Rules

The diagram and table below illustrate the firewall rules and requirements for Oracle VM.

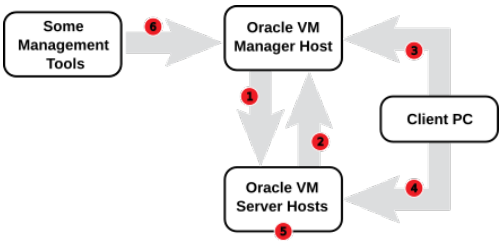


Table 2.1 Firewall Rules

No.	Component Relationship	Ports and Description	Optional
1	Oracle VM Manager to Oracle VM Server	• TCP/8899 - HTTPS connection to the Oracle VM Agent. • TCP/6900-xxxx - Secure VNC connections to connect to the VNC Console for virtual machines running on each Oracle VM Server. • TCP/10000-xxxx - Secure serial connections to connect to the Serial Console for virtual machines running on each Oracle VM Server.	No
2	Oracle VM Server to Oracle VM Manager	• TCP/7002 - HTTPS connection from Oracle VM Agent to the Oracle VM Core WSAPI. • UDP/123 - NTP requests to an NTP server running on the Oracle VM Manager host.	No
3	Client PC to Oracle VM Manager	• TCP/7002 - HTTPS connection from web browser to Oracle VM Manager web user interface, or WSAPI. • TCP/10000 - SSH connection from SSH client to Oracle VM Manager CLI. • TCP/22 - SSH connection to Oracle VM Manager host for administrative work.	No, although access to services should be limited to requirements
4	Client PC to Oracle VM Server	• TCP/22 - SSH connection to Dom0 on each Oracle VM Server for administrative work.	Yes
5	Oracle VM Server to Oracle VM Server	• TCP/7777 - OCFS2 heartbeat communication for clustered server pools.	No

No.	Component Relationship	Ports and Description	Optional
		• TCP/8002 - non-encrypted port to perform live virtual machine migrations. • TCP/8003 - Securely encrypted port to perform live virtual machine migrations.	
6	Some Management Tools to Oracle VM Manager	• TCP/7002 - Access to the Web Services API over HTTPS may be required by some other management tools outside of the immediate Oracle VM product suite. • TCP/54322 - A deprecated legacy API port is still available in this release to cater for any applications that may not have switched over to the Web Services API. This port should be disabled unless you are aware of an application that absolutely requires it. In this case, you should also notify the application vendor that the application must be updated to use the correct API before the next release. You can ensure that access to this port is not available by checking your firewall rules.	Yes

2.1.3 Preparing the Management Network

All physical servers in the Oracle VM environment are connected to the management network. Oracle VM Manager and the Oracle VM Servers communicate over the management network through the Oracle VM Agent, which runs on each server.

Strictly speaking, none of the physical servers need to be reachable externally, so it is recommended that the management network uses a private subnet. This private subnet may be reachable from within your corporate network or a portion of it. If the management network is not a private subnet, or if further security hardening is required, you can restrict access to the IP addresses of the Oracle VM Servers only. The goal is to protect the management network so that it is not exposed to users and machines that do not need to access the physical Oracle VM environment.

In addition to firewall configurations in your corporate network, the use of a VLAN may further shield the management network from unauthorized access. If management network access from outside the corporate network is required, consider enabling it through a VPN tunnel.

Note

For all firewall configurations in your corporate network you must reckon with the same port requirements as described above for `iptables` or `firewalld` on the Oracle VM management server.

Note

Depending on your server hardware and network resources you may want to further segregate network traffic by network role (management, storage, migration, virtual machines, heartbeat). The network model and its security implications are described in detail in Section 3.1, “Oracle VM Network Model”.

2.1.4 Installing Oracle VM Manager

This section describes how to install and configure *Oracle VM Manager* securely.

All applications and components required to run Oracle VM Manager are packaged in an installer ISO image. To install, burn the image onto a DVD-ROM and insert it into the host server, or mount the image onto the host server file system. The components involved in the Oracle VM Manager installation are:

Oracle VM Manager

The Oracle VM Manager web application is provided as an Oracle WebLogic Server domain and container.

Oracle WebLogic Server

Oracle VM Manager runs on top of Oracle WebLogic Server 12*c*, including Application Development Framework (ADF) Release 12*c*. See the Oracle WebLogic Server documentation for more information:

http://docs.oracle.com/middleware/1213/index.html

Oracle VM Manager has a simple domain topology that consists of a single Oracle WebLogic Server on which the Oracle VM Web Services API, Oracle VM Manager Web Interface, and Oracle VM Manager Online Help run.

MySQL Database

Oracle VM uses an Oracle MySQL Enterprise database as a back end repository.

Note

Oracle VM Manager includes a restricted-use license of these databases for use as the Oracle VM Manager Management Repository only.

The installation process in Oracle VM Release 3.4, allows you use of the bundled local MySQL database only.

Prior to installation of Oracle VM Manager for the first time, you should run the provided `createOracle.sh` script to properly setup the installation directory, file system permissions, users and groups and default firewall rules on the host where you are installing the product.

During installation, you set the users and passwords to use for the Oracle VM Manager database, Oracle WebLogic Server, and Oracle VM Manager during the installation. Choose clear user names and secure passwords. The password rules are:

- Must be 8-16 characters in length, but be aware that an 8 character password is still considered fairly weak and you should aim for 12 characters at a minimum.
- Contains at least 1 uppercase letter.
- Contains at least 1 lowercase letter.
- Contains at least 1 numeric value.

For more details, see Installing Oracle VM Manager in the *Oracle VM Installation and Upgrade Guide*.

For all security information related to the database, consult the following Oracle Technology Network (OTN) resources:

- MySQL home page: http://www.oracle.com/technetwork/database/mysql/index.html

- MySQL Security Guide: http://dev.mysql.com/doc/mysql-security-excerpt/8.0/en/index.html

Caution

Installing Oracle VM Manager as a guest on an Oracle VM Server in your managed environment is possible for testing and demo purposes, but not a recommended practice. Before you decide to create this setup, consider the following:

- The setup procedure is relatively complicated.
- The virtual machine running Oracle VM Manager could easily be shut down by accident.
- If the server pool goes offline, recovering the environment will be difficult or may fail.
- In addition to the risk of data loss or corruption, a race condition may occur because of the way the NTP service works: Oracle VM Manager is normally the NTP source for the entire environment, but as a virtual machine it is also a client of the NTP service.

2.1.5 Installing Oracle VM Server

This section describes how to install and configure *Oracle VM Server* securely.

Oracle VM Server runs a lightweight, optimized version of Oracle Linux. It is based upon an updated version of the Xen hypervisor technology and includes Oracle VM Agent. The installation of Oracle VM Server in itself is secure: it has no unused packages or applications and no services listening on any ports except for those required for the operation of the Oracle VM environment.

During the installation process you must provide passwords for the Oracle VM Agent and the `root` user account on the server. Be sure to choose secure passwords and share them only among administrators who need access to the Oracle VM Servers. Use the password rules described in Section 2.1.4, “Installing Oracle VM Manager”. Place the servers in a private network segment with restricted access, as described in Section 2.1.3, “Preparing the Management Network”.

2.1.6 Recommended Oracle VM Deployment Configurations

Proposing a number of recommended Oracle VM configurations is next to impossible, due to the nature of the product: server virtualization. Simply put, any server and any service or application a server makes available, can be virtualized. Consequently, the number of configurations possible is limited only by the capabilities of the physical hardware on which the virtual environment is deployed. An Oracle VM deployment can be a small-scale highly privileged setup with no external connectivity and access limited to only a few pairs of eyes; it could just as well be a battery of virtualized web servers hosting a variety of internet-facing services and applications; or it could be anything in between.

We try to categorize Oracle VM environments by their degree of access, and have documented a number of categories based on the network model. By itself, a privileged domain, or *dom0*, of a host Oracle VM Server is difficult to compromise because it has such a small footprint with very few moving parts and no obsolete packages. Exposure to attacks is highly influenced by the network configuration of both the physical and the virtual environment. In light of this, we identify the following categories according to their network security:

- No network connection.
- Isolated local network.

- Trusted internal network.
- Untrusted internal network.
- Internet-facing service.

Depending on the purpose of your particular Oracle VM configuration, the servers hosted, the services they offer, and who needs to access them, your environment will fall into one or several of these categories. The more users have access to the environment and the larger the network from where the environment can be accessed, the greater the exposure to attacks. What we recommend, is that you use the tightest restrictions possible for your environment, consistent with the purpose of the hosted servers, services and applications. In any case, you must make sure that administrative access to your Oracle VM environment is possible from a trusted network location only. Local system administration is the most secure way, but less practical. If system administration from a remote connection is required, enforce VPN and use encryption.

For detailed information about the categorization based on network connectivity, see Section 3.1, “Oracle VM Network Model”.

2.1.7 Oracle VM Post-Installation Configuration

The purpose of this section is to describe any security configuration changes that must be made after installation. However, the installers for Oracle VM components have been designed to minimize security risks by default, so potential issues are addressed automatically during the installation procedure. Some general security considerations are listed here:

- It is good practice to remove or disable components that are not needed in a given type of deployment. However, Oracle VM is based on a lightweight, optimized version of Oracle Linux: obsolete packages and components are simply not included in the installation media.
- Installation requires the creation and assignment of superusers and root passwords so that software can be installed and configured. As soon as the installation and configuration tasks have been completed, it is recommended that you create individual user accounts for each Oracle VM administrator. Consider disabling root access where possible.
- Weak or plain-text protocols, such as FTP or standard HTTP, must be disabled by default. For demo and testing purposes it would be acceptable to use them, but you must always be aware that this is insecure. Communications between Oracle VM components are properly secured by default. *Oracle VM Manager* and the *Oracle VM Servers* communicate via the Oracle VM Agents, and all agent communication is SSL-encrypted. Access to the Oracle VM Manager is configured to use HTTPS by default. By default, the SSL certificate, used to encrypt communications, is signed by an internal CA certificate that is generated for the Oracle VM Manager instance during installation. Since most client applications, including user web browsers, will not have this CA certificate installed it is not possible for many client applications to validate the SSL certificate presented when accessing an Oracle VM Manager service over HTTPS. Some client applications may fail entirely if an SSL certificate cannot be validated, while other applications may simply issue a warning and allow users to proceed at their own risk. To minimize the likelihood of a man-in-the-middle attack, it is important that validation can actually take place. Therefore, it is appropriate to take one of the following courses of action:
  - Install the CA certificate for the Oracle VM Manager instance into the trusted CA certificate store for all client applications that will have access to Oracle VM Manager.
  - Change the SSL certificate used for HTTPS communications by Oracle VM Manager to use a certificate that is signed by a trusted third-party CA, for which all of your client applications already have the CA certificate installed.

These operations are discussed in detail in the Oracle VM Administrator's Guide.

- Any files that may contain sensitive information should have restrictive file permissions by default. These files include audit logs, password files and configuration. Oracle VM is configured in such a way that no sensitive data, for example clear text passwords, can be disclosed in any logs or temporary files. File permissions are kept strict by default to prevent unauthorized access, and encryption is applied where required.

  Access to the physical servers is tightly restricted by default, which implies that the risk of information being compromised is very small. Therefore, sensitive data such as log files, password files and configuration data are generally well protected in an Oracle VM environment. After successful installation or upgrade of Oracle VM Manager, be sure to remove the log files from `/tmp`, as instructed by the installer.

2.1.7.1 Changing Oracle VM Agent SSL Certificates

Communications between Oracle VM Agents and Oracle VM Manager are SSL-encrypted using an RSA algorithm and 2048-bit private key. The relevant files are located in `/etc/ovs-agent/cert`:

- `certificate.pem`
- `key.pem`
- `request.pem`

Important

Any changes to the SSL certificates used by the Oracle VM Agent causes authentication failure for the Oracle VM Manager instance that currently has ownership of the server. To resolve this, after a change, you must release ownership of the server (this may include a requirement to remove a server from any server pool that it may belong to), and then rediscover the server and take ownership of it again as if it was a new server.

To replace the default self-signed certificate with your own trusted certificate, replace the certificate file and key files.

To generate a new certificate and key files, log on to an Oracle VM Server and execute the command `ovs-agent-keygen`. The command is used as follows:

```
# ovs-agent-keygen -h
Usage: ovs-agent-keygen [OPTION]
Generate SSL certificate and key files for Oracle VM Agent XMLRPC Server.
Options:
-f, --force      override existing files
-v, --version    show version number and exit
-h, --help       show this help message and exit
```

The generated files are placed in the directory mentioned above. If you use the "`-f`" option, the existing files are overwritten.

As of Oracle VM Release 3.3, the Oracle VM Agent password is only used for authentication during the initial discovery process. Thereafter, all subsequent authentication between the Oracle VM Manager and Oracle VM Agent is achieved using certificates. This approach improves security and helps to limit access to the Oracle VM Agent to the Oracle VM Manager instance that has ownership of the Oracle VM Server where the agent is running. Nonetheless, it is good practice to change the Oracle VM Agent password for

any server when ownership is released. A mechanism is in place to do this when you release ownership of a server within the Oracle VM Manager Web Interface and in the Oracle VM Manager Command Line Interface.

2.1.7.2 Enabling LDAP Authentication on Dom0

You can enable LDAP authentication on each *Oracle VM Server* instance to control and log access attempts on Dom0. Enabling LDAP authentication can enhance security for a critical asset (Dom0) for the same reasons that make centralized user control valuable in other contexts.

Note

Setting up LDAP authentication requires configuration settings that are specific to your business needs. It is beyond the scope of this documentation to provide detailed examples of the different methods to enable LDAP authentication. However, the following procedures provide basic steps to guide you through an initial configuration.

To enable LDAP authentication on Dom0, you can do either of the following:

- Follow the procedure in the Oracle Linux 6 Administration Guide to configure and install the `openldap-clients`, `sssd`, and `sssd-client` packages. You must use the `authconfig` command to enable LDAP authentication instead of running the Oracle Linux Authentication Configuration GUI.

  For more information, see *Enabling LDAP Authentication* at: http://docs.oracle.com/cd/E37670_01/E41138/html/ol_enblcli_ldap.html

- Configure LDAP authentication on Oracle VM Server as follows:

  1. Verify that the required packages are available and install them, if required.

     ```
     # rpm -qa | egrep -i 'nss-pam-ldap|pam_ldap'
     pam_ldap-185-11.el6.x86_64
     nss-pam-ldapd-0.7.5-20.el6_6.3.x86_64
     ```

  2. Copy the LDAP server SSL or TLS certificate to the following directory:

     `/etc/openldap/cacerts/openldap.pem`

  3. Set permissions on the certificate.

     ```
     # chmod 644 /etc/openldap/cacerts/openldap.pem
     ```

  4. Rehash the CA certificates.

     ```
     # cacertdir_rehash /etc/openldap/cacerts
     ```

  5. Enable LDAP authentication. Either use the `authconfig` command or start the interface for configuring system authentication.

     - ```
       # authconfig --enableldap --enableldapauth --ldapserver=ldap://hostname:389 \
        --ldapbasedn="dc=example,dc=com" --update
       ```

     - ```
       # authconfig-tui
       ```

The following are example configurations for LDAP authentication:

- `/etc/openldap/ldap.conf`

```
TLS_CACERTDIR /etc/openldap/cacerts
BASE dc=example,dc=com
URI ldap://hostname:389
```

- `/etc/pam_ldap.conf`

```
ssl start_tls
tls_cacertdir /etc/openldap/cacerts
base dc=example,dc=com
uri ldap://hostname:389
pam_password md5
```

- `/etc/nslcd.conf`

```
ssl start_tls
tls_cacertdir /etc/openldap/cacerts
base dc=example,dc=com
uri ldap://hostname:389
uid nslcd
gid ldap
```

2.1.7.3 Enabling FIPS for OpenSSL on Oracle VM Server

Consider enabling FIPS mode for OpenSSL to ensure that your OpenSSL is compliant with Federal Information Processing Standard (FIPS) Publication 140-2, which is a standard that establishes security requirements for cryptographic modules. This action can optionally be performed on each system that forms part of the infrastructure of your Oracle VM deployment. Further information on enabling FIPS mode for OpenSSL is provided in the *Oracle Linux 6 Security Guide* available at:

http://docs.oracle.com/cd/E37670_01/

In this section we outline the steps required to enable FIPS for OpenSSL on Oracle VM Server. It should be noted that there are some minor differences between Oracle VM Server and Oracle Linux 6 and therefore some of the steps to set up and configure FIPS mode for OpenSSL may differ from the instructions provided for Oracle Linux 6.

Note

The Oracle VM Server must have been registered with ULN. The `openssl-fips` package is available on the `ol6_x86_64_addons` channel.

To make an Oracle VM Server compliant with Federal Information Processing Standard (FIPS) Publication 140-2, perform the following steps:

1. First check that FIPS is not already enabled:

```
# cat /proc/sys/crypto/fips_enabled
0
```

2. Log in to ULN and enable the `ol6_x86_64_addons` channel for your system.

3. Install the `dracut-fips` package:

```
# yum install dracut-fips
```

This package must be installed so that the system checks the integrity of the kernel components at boot time.

4. Remove the existing `openssl` package and install the `openssl-fips-1.0.1*` package. You can use `yum shell` to perform these transactions as shown here:

```
# yum -y shell <<EOF
remove openssl
install openssl-fips-1.0.1*
run
EOF
```

You cannot use separate `yum remove` and `yum install` commands as `yum` itself depends on the OpenSSL library being available.

Alternatively, download the `openssl-fips-1.0.1*` package and use the `rpm` command instead:

```
# rpm -e --nodeps openssl
# rpm -ivh openssl-fips-1.0.1*.rpm
```

5. Identify the device UUID for your boot partition. There are a variety of ways to do this, the following shell command should return the UUID of the device being used for your boot partition:

```
# blkid `mount |grep \/boot|awk '{print $1}'`
```

Note that if you have partitioned the disk in such a way that `/boot` is not on its own partition, the above command will not return any output.

6. Edit `/etc/default/grub`:

a. If `/boot` or `/boot/efi` is located on a separate partition from `/` and you have obtained the UUID for the device where this partition is located, you must add the following line to ensure that when grub is updated FIPS is enabled automatically and that the system is able to identify the appropriate device to boot from:

```
GRUB_CMDLINE_LINUX_DEFAULT="splash=verbose verbose crashkernel=224M-:112M showopts fips=1 \
          boot=UUID=boot_UUID root=UUID=root_UUID"
```

Where *`boot_UUID`* and *`root_UUID`* are the UUIDs that you obtained in the previous step.

Caution

If `/boot` or `/boot/efi` exist on a separate partition from `/` and you do not specify a valid `boot=` entry, the system crashes because it cannot locate the kernel's `.hmac` file.

b. If `/boot` or `/boot/efi` is **not** located on a separate partition from `/`, then you do not need to specify the boot partition:

```
GRUB_CMDLINE_LINUX_DEFAULT="splash=verbose verbose crashkernel=224M-:112M showopts fips=1"
```

7. Rebuild the GRUB config to use the changes that you have made to `/etc/default/grub`:

a. On BIOS-based systems, issue the following command as root:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

b. On UEFI-based systems, issue the following command as root:

```
# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

8. Edit `/etc/sysconfig/prelink` and set `PRELINKING=no`.

Prelinking must be disabled to allow the system to verify the integrity of modules correctly.

9. Remove all existing prelinking from binaries and libraries:

```
# prelink -u -a
```

Caution

If you do not disable and remove all prelinking, users cannot log in and `/usr/sbin/sshd` does not start.

10. Recreate the `initramfs` file system:

```
# dracut -f
```

This can take some time to complete. You may run this with the `-v` or `--verbose` switch to monitor the process.

11. Remove the existing SSH host keys:

```
# rm /etc/ssh/ssh_host*
```

OpenSSH uses the FIPS-validated OpenSSL library modules to generate new, FIPS-approved keys when the system is next rebooted. (Under FIPS mode, `ssh-keygen` can create new RSA host keys in `/etc/ssh`, but not DSA keys, and it displays key fingerprints as SHA1 hashes instead of as MD5 hashes.)

12. Shut down and reboot the system into FIPS mode.

Note

While the system is rebooting, generate input events by pressing keys at random or by moving the mouse. You should create at least 256 such events to ensure that the system has sufficient entropy available for key generation.

13. When the system has rebooted, check that FIPS is enabled:

```
# cat /proc/sys/crypto/fips_enabled
1
```

14. To test that FIPS is functioning correctly, run the following OpenSSL command and check that an error is returned:

```
# openssl md5 /etc/hosts
Error setting digest md5
140297679636296:error:060A80A3:digital envelope routines:FIPS_DIGESTINIT:disabled for fips:fips_md.c:180:
```

The error is returned when you attempt to obtain an MD5 hash, because MD5 is not a FIPS approved Hash Standard.

Chapter 3 Oracle VM Security Features

Table of Contents

This chapter describes the main security mechanisms offered by Oracle VM. Its users are administrators, who rely on *Oracle VM Manager* and the CLI to configure and maintain the physical and virtual environment. The essential elements that define the level of security in Oracle VM, are:

- Installation into a default, secure state, as described in Chapter 2, *Performing a Secure Oracle VM Installation*.
- Strict control of administrative privileges.
- Network segregation and host isolation to prevent exposure of all but the required services.
- Separate end user access to virtual machines, and isolation of virtual machines from the underlying Oracle VM infrastructure.

Note

Oracle VM itself does not provide role based access control. If your environment requires it, use Oracle Enterprise Manager to manage your environment and all access to its physical and virtual resources.

3.1 Oracle VM Network Model

Use network configuration and access restrictions to expose to the outside world only what is needed.

From a network security point of view, remote host connectivity and access control are generally defined and scaled for these deployment categories:

- No network connection.
- Isolated local network.
- Trusted internal network.
- Untrusted internal network.
- Internet-facing service.

These categories are ordered from low to high exposure to network security risks, and they are also described below in more detail in that order.

3.1.1 No Network Connection

Some highly confidential applications cannot tolerate the possibility of any remote connection or exploit. Machines that require this level of security are usually kept in access restricted rooms and often built without network cards. This type of configuration is a recommended best practice for credential originating systems such as a root certificate authority where the compromise of the root keys would put all certificates and applications that were signed by that authority at risk.

Although some of Oracle VM's features such as High Availability and Master Failover are not available without a network, peer *Oracle VM Servers* and shared storage, the product can be configured for single-node service where VMs can provide these secure applications using a local text console, host networking and/or a shared disk to access them.

If host based network security and traffic restriction is needed between virtual machines on the same host, the ebtables application can provide Ethernet frame filtering across the Linux based bridges.

Guidelines for the no network connection model:

- Restrict physical access to the machines.
- Restrict login access to trusted administrators.
- Inspect removable media before connection and after disconnection, or ban them entirely from the secure area.
- Securely wipe or destroy replaced hard drives. Make sure that replacement hard drives are inspected or even wiped prior to installation.
- Implement ebtables rules if host-based network traffic control is needed between guests.

3.1.2 Isolated Local Network

An isolated local network consists of servers that are connected in an environment which has no connection to any other network. In this model, there is zero network connectivity to a larger internal network or the Internet. Since there is no potential for remote exploits from a large number of unknown sources, this environment provides well defined physical, network and security characteristics.

By definition, access to this configuration is limited to personnel with access to the trusted admin hosts (including Oracle Enterprise Manager or Oracle VM Manager) on the closed, local network. Threats consist of an accidental "convenience" connection being made to other networks or a trusted admin installing an unsigned package or application that may introduce a malware agent.

Guidelines for the isolated local network model:

- Set all default passwords for uniqueness and complexity. For using the High Availability and Virtual IP features where the master role may be moved to any node, ensure that the *Oracle VM Agent* password on each one is complex, but identical across the server pool.
- Limit physical Oracle VM Server(dom0) and Oracle VM Manager access to essential personnel.
- Avoid installing untrusted 3rd party software.
- If clustering with NFS shared storage, or exporting OCFS2 repositories for backup, make sure the storage network is also restricted to the cluster subnet, especially since the documented export with `no_root_squash` represents a potential exposure.

3.1.3 Trusted Internal Network

A Trusted Internal Network is a well maintained, trusted and probably small internal network where network traffic is unrestricted to and from the cluster subnet. While this configuration provides advantages of access to a company's infrastructure, services and storage, it also introduces a few threats. Most of these are not malicious, and normal internal safeguards such as an Intrusion Detection Systems, anti-virus software and active network monitoring typically address rogue employees or bot infestations that may attempt to disrupt the network. Human error via network and new admin mistakes are the most common causes of cluster service outages.

Guidelines for the trusted internal network model:

- Implement all the guidelines for isolated local networks.
- Disable ssh root logins. Admins should log in as themselves (using their global uid) with user privileges. Set up sudo to allow specific admin commands per user or root, if needed. See Section 3.2, “Administrator Privileges in Oracle VM” for details.
- If shared storage is mounted from outside the server pool subnet, restrict the export to the Oracle VM Server dom0 and VM IP addresses. Do not make NFS shares and LUNs on Fibre Channel or SAN storage globally accessible.
- Establish appropriate network firewalls as discussed below.

A default Oracle Linux install has the iptables or firewalld firewall enabled. However, a best practice for network filtering is to use an additional external firewall device. This permits separation of control (network administrator control of network access, use of globally administered and audited rules), and relieves the Oracle VM dom0 of the potentially high CPU load that can be created by implementing packet filter rules. In order to use Oracle VM Manager on a system with iptables or firewalld enabled you can either open the ports used by Oracle VM Manager, or open all ports by disabling iptables or firewalld. The latter is not advised in the absence of an external firewall devices because it removes network protection.

Be sure to open the necessary ports on the different firewalls that may be installed between different parts of your network. Additional information including a listing of required ports and a diagram showing how components connect to each other can also be found in Section 2.1, “Oracle VM Pre-Installation Tasks”.

Ensure that your external firewall device filters or blocks ICMP Timestamp requests from arbitrary hosts. It is possible to send ICMP Timestamp (Type 13) requests to obtain system information or perform various attacks.

If there is no external firewall device, for example, when using iptables, ensure that the iptables service is running on each node and that at least the default policy and ruleset are present in the file `/etc/sysconfig/iptables`:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [1:148]
-A INPUT -p tcp -m state --state NEW -m tcp --dport 10000 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 123 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 7002 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A INPUT -p icmp --icmp-type timestamp-request -j DROP
-A INPUT -p icmp --icmp-type timestamp-reply -j DROP
COMMIT
```

3.1.4 Untrusted Internal Network

An untrusted internal network has the characteristics of being loosely maintained, unmonitored, readily compromised from the outside or from ongoing and uncorrected malware infested workstations on the inside.

In this model, the dom0 admin control and VMs have been partitioned into separate VLANs where traffic flow is controlled by a 3 zone router/firewall. The firewall policy is to allow the admin network to make outbound connections to anywhere, but blocks inbound connections from the untrusted internal network. Firewall policies to the VM network would depend on the application but should only expose service ports to the internal network that are needed. A signature driven Intrusion Detection System is an option on the VM network to monitor for traffic patterns that indicate an attack is underway.

This model views any traffic from the internal network as potentially hostile. Additional hardening of this network can be done by implementing hardware-based or software-based firewalls and policies on the admin and dom0 hosts that block inbound traffic. The dom0 firewall rules can also be enhanced to reject peer dom0 traffic on all ports except OCFS2 (7777), Oracle VM Agent (8899), and the Xen administration ports (8002 and 8003).

Guidelines for the untrusted internal network model:

- Implement all the guidelines for trusted internal networks.
- Disable ssh root logins. Admins should log in as themselves (using their global uid) with user privileges. Set up sudo to allow specific admin commands per user or root, if needed. See Section 3.2, “Administrator Privileges in Oracle VM” for details.
- If using iptables, add failed connection logging to the existing iptables firewall just prior to the last REJECT line:

```
-A RH-Firewall-1-INPUT -m limit --limit 15/minute -j LOG --log-prefix "FW Drop:"
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
```

- Set up a remote syslog server to track all user logins and firewall connection failures.
- Disable the VNC connections on each Oracle VM Server dom0. Port-forward VNC connections via ssh and vncviewer rather than Oracle VM Manager:

```
#-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5900:5950 -j ACCEPT
ssh -L 5900:vmserverhost:5900 vmserverhost
```

- Disable port 8888 and IPP ports on Oracle VM Manager:

```
#-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
#-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
#-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8888 -j ACCEPT
```

Note

This will leave secure ports 22, 7002 and 10000 for admin command line access and Oracle VM Manager connections.

- Define a trusted admin network or host and limit Oracle VM Manager and Oracle VM Server ssh connections to that network or host. To implement this in iptables, comment out the existing ssh rule in the default `/etc/sysconfig/iptables` configuration file. Replace it with the information applicable to your trusted network or single admin host; for example the 192.168.0.0/24 network or the host with IP address 192.168.0.67:

```
#-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -p tcp -s 192.168.0.0/24 --dport 22 -j ACCEPT
-- or --
-A RH-Firewall-1-INPUT -p tcp -s 192.168.0.67 --dport 22 -j ACCEPT
```

Note

Connections that fail will fall through and be logged by the logging rule provided in the third bullet. When using iptables, all the rules in /etc/sysconfig/iptables can also be changed to restrict access to selected networks or hosts.

3.1.5 Internet Facing Services

The most challenging model for securing a network connected host is placing VM based services directly on the Internet. In this case, great care must be taken to insure that the environment won't be compromised through a wide variety of penetration techniques and exploits from a large, diverse and aggressive set of threats.

Even on an untrusted internal network without intrusion detection, internal users are known quantities and typically aware that they are being monitored, so they generally do not tend to be abusive or even overly curious. In contrast, the Internet provides virtual anonymity for malicious individuals, criminal gangs and hostile, well equipped governments. With an anonymous cloak, probing and attacking high profile network segments with automated tools that run 24/7 is a standard procedure. On perimeter firewalls, aggressive penetration attempts on the ssh, mysql, oracle, netbios and smtp service ports can typically be measured in "attacks per second".

There are a variety of topologies to provide zone isolation that can help to repel attacks and mitigate the effects of a successful intrusion event. The following describes some basic approaches.

Guidelines for network models involving Internet facing services:

- Implement all the guidelines for untrusted internal networks.
- All Internet facing hosts and VMs reside on an isolated network stub called a DMZ (for demilitarized zone). Connections into and out of the network are managed and monitored by a stateful firewall that enforces well defined rules and policies. If possible, an individual DMZ VLAN per VM is optimal for guest VM isolation.
- Never place Oracle VM Manager or any other mission critical administration tool on the Internet. Use a VPN to access these hosts on secure internal admin networks. This in particular applies to networked storage: these hosts should not be on the Internet-facing network.
- Place each dom0 (Oracle VM Server) that is hosting Internet-exposed VMs in an administrative DMZ. This zone cannot initiate connections to the internal network or the Internet, but is reachable from an administrator VLAN. The dom0 itself should not the reachable from the Internet or the internal network.
- Use selinux on Internet-exposed Linux VM guests whenever possible.

3.2 Administrator Privileges in Oracle VM

Each administrator should have an individual user account in order to access Oracle VM Servers and Oracle VM Manager.

Note

You can create unique user accounts for Oracle VM Manager with the Administrator Tool (ovm_admin). For more information, see Oracle VM Manager Administrator Tool (ovm_admin) in the *Oracle VM Administrator's Guide*.

The Oracle VM dom0 is a highly privileged environment. For maximum security, administrative access to it must be strictly controlled, limited to authorized individuals, and logged. It must be stressed that the recommended method for most Oracle VM management is through the graphical user interfaces provided by Oracle VM Manager, the Oracle VM Manager Command Line Interface, or Oracle Enterprise Manager Ops Center, rather than logging onto individual servers, except in specific situations where command line access to Oracle VM Servers is needed or recommended by Oracle Support Services.

That said, customers may choose to deploy "normal" Linux administrative controls and remain supported. A specific valid example includes modifying `/etc/ssh/sshd_config` and `/etc/sudoers` to prevent SSH root login and requiring administrators to login as themselves and use sudo to gain privileged access. Another valid example is modifying `/etc/login.defs` to control password length and expiration policies. Adding device drivers or rpms would be examples of changes that could harm supportability and proper function, and should only be done in consultation with Oracle VM Support. Customers are encouraged to carefully review their access and security controls for suitability in the Oracle VM environment.

End users of virtual machines in the Oracle VM environment should not be granted administrative rights. They should rather access their virtual machines directly via SSH, RDP or VNC. For large scale environments, instead apply role based access control via Oracle Enterprise Manager, as explained in Section 3.4, “User Access to Virtual Machines”.

3.3 Storage Configuration

The storage providers in an Oracle VM environment must also be configured in a way that exposes them only to the servers and virtual machines that make use of them. Access to the management functionality of each storage provider must be restricted to the administrators in charge of storage configuration.

First of all, connect the storage servers to a private network that is accessible from the Oracle VM Manager and Oracle VM Servers. The storage providers need not be reachable from outside the Oracle VM environment. This network can be the management network or, preferably, a separate storage network. Locking down the storage servers to the individual IP addresses of the Oracle VM servers (including the Manager) in the storage subnet, is the most restrictive and most secure way to provide access to storage. As a minimum, expose the storage only to the storage subnet.

In Oracle VM we distinguish between file servers and SANs. For both categories the recommendations above apply, because most non-local storage is both managed and provisioned over the network, meaning based on IP addresses. The exception is directly attached storage, such as Fibre Channel or InfiniBand: to prevent unauthorized access you must make sure that only the Host Bus Adapters (HBAs) of the required servers are physically connected to the Fibre Channel or InfiniBand switch. NFS-based file servers and iSCSI-based SAN servers can be restricted to a subset of IP addresses via configuration.

The management of the Oracle VM storage servers may be different depending on the Oracle VM Storage Connect plug-in used for interaction with the storage provider. If you are using generic NFS or iSCSI providers with the corresponding generic Oracle VM Storage Connect plug-in, then configuration occurs almost entirely on the storage host. If you are using a custom third-party Oracle VM Storage Connect plug-in, then you can perform a much larger portion of the storage configuration from within Oracle VM Manager. Regardless of whether you use generic or non-generic iSCSI storage, make sure that your targets, initiators and access groups are configured in the most restrictive way possible.

For information about how to configure access to your storage providers, consult the following topics in the Oracle VM documentation:

- Overall storage management: refer to Storage Tab in the *Oracle VM Manager User's Guide*.
- Storage access configuration through access groups: refer to Access Groups Perspective in the Oracle VM Manager User's Guide.

- Access group and storage initiator management on Oracle VM Servers: refer to Storage Initiators Perspective in the Oracle VM Manager User's Guide.

For a technical overview of Oracle VM Storage Connect, see the Oracle VM Storage Connect technical paper at:

http://www.oracle.com/us/technologies/virtualization/ovm3-storage-connect-459309.pdf.

For specific details about the configuration of your storage hardware, consult the hardware manufacturer's documentation.

3.4 User Access to Virtual Machines

By itself, the Oracle VM Manager GUI is an administrator tool. The administrator accounts have full access to all the functionality and all resources managed through Oracle VM Manager. Therefore it is highly recommended that only a few accounts be handed out to the people who are responsible for configuration and day-to-day management of the environment. Administrators must also have access to the guest operating systems of the virtual machines, and for that they use the VM console from within the Oracle VM Manager GUI. However, not every user with virtual machine access needs to be an Oracle VM administrator. This would violate the security principle of least privilege. (See Section 1.2.3, “Follow the Principle of Least Privilege”.) Depending on your particular deployment of Oracle VM, you may want to grant virtual machine access in a different way.

We distinguish between three methods of virtual machine access control:

- Oracle VM Manager console.
- Direct remote connectivity.
- Role-based access control with Oracle Enterprise Manager.

VM Console Access

An Oracle VM administrator can always access the guest operating system of a virtual machine via the console in Oracle VM Manager. This is the standard method to connect to a virtual machine hosted in an Oracle VM environment. If your virtual machines are servers hosting applications and services, for example, then it is likely that they are configured and maintained by system administrators. In this type of setup, end users interact with the service or application running on the server, but never log on to the virtual machine itself.

For this model it makes sense that only one or a handful of system administrators can access the virtual machine via the Oracle VM Manager console. From a security standpoint, a small number of administrator accounts is very manageable, while the Oracle VM resources remain hidden and protected from all other users.

Direct VM Access

If certain users need administrative access to virtual machines, but are not administrators of the Oracle VM environment, we recommend that you *do not* create additional administrator accounts for Oracle VM Manager. Instead, an Oracle VM administrator should set up the virtual machine and configure remote connectivity so that the virtual machine user can establish a connection without having to go through Oracle VM Manager. To establish direct VM access, follow the same principles and procedures as with a physical server:

1. Install and configure the appropriate operating system on the VM. Install any mandatory additional software as well.

2. Create the necessary user accounts and set the required privileges.

3. Connect the VM to a network that is accessible to the VM user(s), but make sure that the management network and other networks essential for your Oracle VM environment remain protected. Assign a static IP address to the VM to facilitate remote connectivity. Never use a public IP address for administrative access; instead, use a private IP address in the internal network and force users to set up a VPN connection to the internal network first.

4. Configure remote connectivity on the VM. For a Windows server, RDP can be used; for a Unix server you can use SSH for command line access, and VNC in case a graphical desktop environment is used.

5. Provide login credentials, VM IP address (or DNS name) and remote access port number to the users who require remote access.

Caution

Always apply the principle of least privilege: strictly enable only the functionality that users require.

Role Based Access

Large-scale deployments of Oracle VM have different requirements when it comes to user management and access control. A combination of the two access methods described above becomes unmanageable as the number of virtual machines increases, and different categories of users need different levels of access to groups of virtualized resources. If your environment is that large and complex, you need facilities such as role-based access control and directory service integration. Oracle VM Manager cannot provide this functionality, but if you need it, you can integrate your Oracle VM environment with Oracle Enterprise Manager.

The integration with Oracle Enterprise Manager adds a number of significant management features to Oracle VM, such as:

- Role-based access control: user groups and permission profiles.
- LDAP/directory service integration.
- resource assignment and ownership management.
- Separation, isolation and protection of resource groups (VMs, networks, storage, etc.).
- Profiles and deployment plans to create multiple VMs at once and to provision operating systems and software applications.

For a quick overview of role based access control with Oracle Enterprise Manager, see this post on Oracle's Virtualization Blog: https://blogs.oracle.com/virtualization/entry/crash_course_role_based_access.

For detailed information about integrating Oracle VM with Oracle Enterprise Manager, see the Oracle Enterprise Manager documentation at: http://www.oracle.com/technetwork/oem/grid-control/documentation/oem-091904.html

3.5 Virtual Machine Security Considerations

In many ways, virtual servers have security requirements identical to those of physical servers. The same applies to the applications and services they host. Virtualization provides security benefits: each virtual machine has a private security context, potentially with separate authentication and authorization rules, and with separate process, name and file system spaces. Deploying applications onto separate virtual

machines provides better security control compared to running multiple applications on the same host operating system: penetrating one virtual machine's OS doesn't necessarily compromise workload and data residing in other virtual machines. Nonetheless, some practices should be kept in mind to prevent virtualization from introducing security vulnerabilities.

One aspect is physical security. Virtual infrastructure is not as 'visible' as physical infrastructure: there is no sticky label on a virtual machine to indicate its purpose and security classification. If a data center identifies servers with extremely high security requirements, and physically isolates them in a locked room or cage to prevent tampering or theft of data, then the physical machines hosting their virtualized workloads should be isolated in a similar way. Even without secured areas, many institutions keep workloads of different security classes on different servers. Those same isolation rules apply for virtual machines. Care should be taken to ensure that the protected virtual machines are not migrated to a server in a less secure location. In the context of Oracle VM, this implies maintaining separate server pools, each with their own group of servers.

These rules of isolation should also be applied to networking: there are no color coded network cables to help staff identify and isolate different routes, segments and types network traffic to and from virtual machines or between them. There are no visual indicators that help ensure that application, management, and backup traffic are kept separate. Rather than plug network cables into different physical interfaces and switches, the Oracle VM administrator must ensure that the virtual network interfaces are connected to separate virtual networks. Specifically, use VLANs to isolate virtual machines from one another, and assign virtual networks for virtual machine traffic to different physical interfaces from those used for management, storage or backup. These can all be controlled from the Oracle VM Manager user interface. Ensure that secure live migration is selected to guarantee that virtual machine memory data is not sent across the wire unencrypted.

Additional care must be given to virtual machine disk images. In most cases the virtual disks are made available over the network for migration and failover purposes. In many cases they are files, which could easily be copied and stolen if the security of network storage is compromised. Therefore it is essential to lock down the NAS or SAN environments and prevent unauthorized access. An intruder with root access to a workstation on the storage network could mount storage assets and copy or alter their contents. Use a separate network for transmission between the storage servers and the Oracle VM hosts to ensure its traffic is not made public and subject to being snooped. Make sure that unauthorized individuals are not permitted to log into the Oracle VM Servers, as that would give them access to the guests' virtual disk images, and potentially much more.

All of these steps require controlling access to the Oracle VM Manager and Oracle VM Server domain 0 instances. Network access to these hosts should be on a private network, and the user accounts able to log into any of the servers in the Oracle VM environment should be rigorously controlled, and limited to the smallest possible number of individuals.