# Oracle® VM

## Security Guide for Release 3

E35334-05
March 2014

# Oracle® VM: Security Guide for Release 3

## Abstract

Document generated on: 2014-03-06 (revision: 3777)

# Table of Contents

# Preface

## Table of Contents

The Oracle VM Security Guide is part of the Oracle VM product documentation. It provides valuable information about 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 White 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

# 1 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.

# 2 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.

# 3 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:<br>`dd if=/dev/rdsk/c0t1d0s6 of=/dev/rst0 bs=10b \` |

| Convention | Description |
|---|---|
| | `count=10000` |
| braces { } | Braces indicate required items:<br>`.DEFINE {macro1}` |
| brackets [ ] | Brackets indicate optional items:<br>`cvtcrt termname [outfile]` |
| ellipses ... | Ellipses indicate an arbitrary number of similar items:<br>`CHKVAL fieldname value1 value2 ... valueN` |
| *italics* | Italic type indicates a variable. Substitute a value for the variable:<br>*`library_name`* |
| vertical line \| | A vertical line indicates a choice within braces or brackets:<br>`FILE filesize [K\|M]` |
| forward slash / | A forward slash is used as an escape character in the Oracle VM Command Line Interface to escape the special characters `"`, `'`, `?`, `\`, `/`, `<`, `>`:<br>`create Tag name=MyTag description="HR/'s VMs"` |

# 4 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. |

# 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.

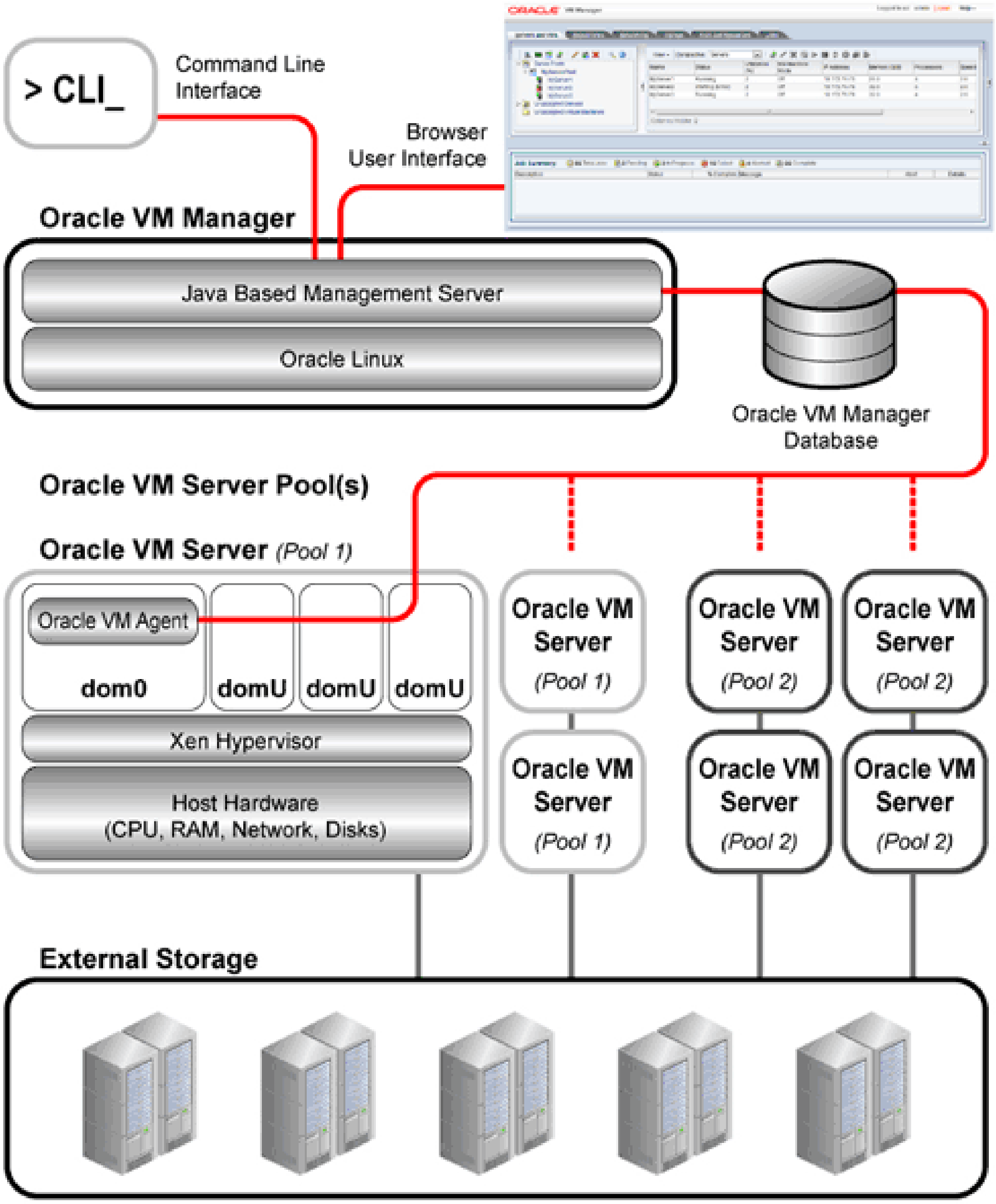
## 1.1 Oracle VM Overview

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 Description of Oracle VM Components

The components of Oracle VM are shown in Figure 1.1, “Oracle VM Architecture”.

**Figure 1.1 Oracle VM Architecture**


> CLI_
Command Line Interface
Browser User Interface
Oracle VM Manager
Java Based Management Server
Oracle Linux
Oracle VM Manager Database
Oracle VM Server Pool(s)
Oracle VM Server (Pool 1)
Oracle VM Agent
dom0
domU
domU
domU
Xen Hypervisor
Host Hardware (CPU, RAM, Network, Disks)
Oracle VM Server (Pool 1)
Oracle VM Server (Pool 1)
Oracle VM Server (Pool 2)
Oracle VM Server (Pool 2)
Oracle VM Server (Pool 2)
Oracle VM Server (Pool 2)
External Storage

**Caution**

The entire configuration of your Oracle VM environment, both physical and virtual, is maintained in the Oracle VM Manager database. As of Oracle VM Release 3.2, the underlying database for demo and testing environments is a MySQL database, whereas prior releases use an Oracle XE database. Both configurations are covered in this Oracle VM Security Guide.

- **Oracle VM Manager**: Provides the command line interface (CLI), as well as the graphical user interface (GUI). The Oracle VM CLI allows you to perform nearly the same management actions as the UI from an SSH connection. The GUI is an Application Development Framework (ADF) web application you use simply through your browser to manage *Oracle VM Servers*, virtual machines, and resources. Use *Oracle VM Manager* to:

  - Configure and manage Oracle VM Servers
  - Configure and manage networks
  - Configure and manage storage
  - Configure and manage resources such as virtual machine images, virtual machine templates, assemblies, and installation media
  - Create virtual machines from installation media, a virtual machine template, an assembly, or a virtual machine image
  - Manage virtual machines, including powering on and off, deleting, and live migrating
  - Import virtual machines created with Oracle VM or another solution for server virtualization

  The Oracle VM Manager GUI is an Oracle WebLogic Server application running on Oracle Linux. This can be a standalone computer, or part of a virtual machine running on an instance of Oracle VM Server. However, it is recommended that Oracle VM Manager be run on a standalone computer. This guarantees dedicated resources to Oracle VM Manager, and offers the flexibility to isolate its network traffic from the true guest virtual machine networks, to prevent snooping of any unencrypted contents or denial of service.

- **Oracle VM Server**: A managed virtualization environment providing a lightweight, secure server platform which runs virtual machines. At least one Oracle VM Server is required, but several are needed to take advantage of clustering. 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, file systems, and software RAID volume management. 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.

- **External Storage**: Oracle Storage Connect plugins provide access to storage. The plugins are distributed as RPM packages and deployed on the Oracle VM Servers. They are divided in two major categories: storage array plugins for any block based storage, and file system plugins for any network file system based storage. For both categories, generic plugins are included. They offer standard functionality to discover, register and use NFS storage, iSCSI or Fibre Channel SANs, and local storage. Interactive management operations, such as creating and modifying LUNs or configuring access groups on the storage hardware, are only offered by vendor-specific plugins.

For more background information about Oracle's virtualization technology, architecture, concepts and deployment of Oracle VM, see the *Oracle VM User's Guide*.

## 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 an iptables 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 2 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.
- The Oracle VM Manager XE or MySQL database is restricted to localhost connections and is not remotely accessible via port 1521. The XE or MySQL database is intended for test and development environments. Production Oracle VM environments must use Oracle Database - Standard (SE) or Enterprise (EE) Edition.
- 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.
- SSL is used for the network component of a VM migration.
- The Oracle VM Servers' administrative connection to Oracle VM Manager uses HTTPS by default as of Oracle VM version 3.1.1 errata 1.
- 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. 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.<br>By default, two-way SSL encryption is enabled via the built-in `DemoIdentity.jks` and `DemoTrust.jks`. It is recommended that you replace the keystores with your own version. Since Oracle VM Manager is a web interface running on top of an Oracle WebLogic Server, details and instructions about security, encryption and keystores can be found in the Oracle WebLogic Server documentation. In the documentation library, go to the Security section and open the document entitled Securing *Oracle WebLogic Server*. The current version at the time of writing is Oracle Fusion Middleware Securing Oracle WebLogic Server 12c Release 1. Relevant information and instructions can be found in these chapters:<br>• Configuring Identity and Trust<br>• Configuring SSL<br>• Configuring Security for a WebLogic Domain |
| Oracle VM Manager GUI to Oracle VM Core | Only local communication, meaning communication between an Oracle VM Manager GUI and Oracle VM Core running on the same server, is allowed over TCP/54321 without SSL encryption. In all other situations SSL encryption is enabled and port 54322 (TCPS) is used instead. |
| Web Services to Oracle VM Core | As of version 3.2.1, Oracle VM offers a web services API (WSAPI) exposed over both SOAP and REST. Local communication with Oracle VM Core occurs |

| Communication | Description |
|---|---|
|  | through TCP/54321; all non-local communication must be SSL-encrypted and uses TCPS/54322. |
| Client to CLI | The Oracle VM 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. |
| CLI to Oracle VM Core | The Oracle VM Command Line Interface (CLI), when running on the same host, communicates locally with Oracle VM Core through TCP/54321; all non-local communication must be SSL-encrypted and uses TCPS/54322.<br>Note that the direct connection between CLI and Oracle VM Core will be phased out of the product. At that point, the CLI will connect to the Oracle VM Web Services API, as described below. |
| CLI to web services | Direct connection between CLI and Oracle VM Core will be phased out of the product. At that point, the CLI will connect to the Oracle VM Web Services API. For that communication, it is recommended that HTTPS be used over TCP/7002. Regular HTTP is possible via TCP/7001 but should be avoided for purposes other than demonstration and testing. |
| Oracle VM Agent to Oracle VM Core | The Oracle VM Agents running on the Oracle VM Servers use SSL encryption. They communicate with Oracle VM Core via TCP/7002 (HTTPS). |
| 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 Agent to Oracle VM Agent | Communication between Oracle VM Agents is SSL-encrypted (HTTPS) and uses TCP/8899. |
| VNC proxy | The VNC proxy on the Oracle VM Manager host, used for connections to virtual machine consoles, listens on TCP/15901. Traffic is SSL-encrypted (TCPS). |
| VNC Server | The VNC server opens 1 tunnel for each remote virtual machine connection on the Oracle VM Servers. For SSL-encrypted connections, TCP ports 6900 and up (TCPS) are used. TCP ports 5900 and up can be used for unencrypted local connections. |
| 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 the SSL key and matching certificate. The properties are:<br>• key algorithm: RSA<br>• private key size: 1024 bits<br>• certificate data management: according to X.509 standard<br>• location of the SSL key and certificate: `/etc/ovs-agent/cert` |

| Communication | Description |
|---|---|
| | 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. |
| Other traffic | In an Oracle VM environment, the Oracle VM Manager host is used as the reference for time synchronization. Consequently, UDP port 123 is used for NTP traffic.<br>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. |

## 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 *Yum Repository Setup* 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 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 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 12c 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. We see the complete set of products (Oracle Enterprise Manager 12c Cloud Control, Oracle Enterprise Manager OpsCenter, Oracle VM Manager and *Oracle VM Agent*) as one product suite. Oracle Enterprise Manager 12c has complete Role Based Access Control, LDAP/Directory Services integration, a complete cloud self service end-user portal and cloud administrator portal. All these features are part of the Oracle VM portfolio without additional license cost. For more information about this integration of cloud components, see http://blogs.oracle.com/virtualization/entry/crash_course_role_based_access.

## 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<br>- and/or -<br>/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/machine1/base_adf_domain/servers/AdminServer/logs/ | The `access.log` and `base_adf_domain.log` files contain detailed information about Oracle VM domain access and status. These logs actually come from the WebLogic server.<br>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.<br>The `AdminServer-diagnostic.log` file collects entries related to the Oracle VM Manager user interface and Oracle WebLogic Server. |
| CLI logs | /u01/app/oracle/ovm-manager-3/machine1/base_adf_domain/servers/AdminServer/logs/CLIAudit.log<br>/u01/app/oracle/ovm-manager-3/machine1/base_adf_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.<br>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 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, |

| Log Files | Location | Description |
|---|---|---|
| | | including storage device events, network events etc. |
| Oracle VM console log | /var/log/ovm-consoled.log | [need info] |
| Storage Connect log | /var/log/osc.log | This file logs all installation activities related to Oracle Storage Connect plugins. It shows which plugins 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, Oracle database and WebLogic Server.

Oracle VM 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 components that are not needed in a specific deployment.

Security measures applied in a default installation include:

- active software firewalls (iptables) which only open standard required ports
- SSL encryption for all *Oracle VM Agent* communications, i.e. between agents but also to and from *Oracle VM Manager*

> **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 will be reconfigured automatically. 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
- Small footprint JeOS-like operating system: Oracle Linux without unused packages in order to mimimize 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 5 Update 5 64-bit or later
- Oracle Linux 6 64-bit or later

A default Oracle Linux installation has the firewall enabled (`iptables on`). 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, preferred), TCP/7001 (HTTP)
- for access to virtual machine consoles: TCP/15901 (secure VNC proxy)
- for inbound connection from Oracle VM Servers: TCP/7002 (HTTPS, default), TCP/7001 (HTTP), UDP/123 (NTP)
- for optional remote API access: TCP/54322 (Secure TCP over SSL, recommended), TCP/54321 (standard)
- for outbound connection to Oracle VM Servers: TCP/8899 (Oracle VM Agent), TCP/5900-xxxx (VNC, 1 secure tunnel per VM)
- for inter-server communication in clustered server pools: TCP/7777 (default OCFS2 port on storage network)
- for SSH access: TCP/22 (likely open by default)
- for CLI access using SSH: TCP/10000

**Note**

The Oracle VM Command Line Interface (CLI) is part of Oracle VM as of version 3.2.1.

**Note**

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

**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:

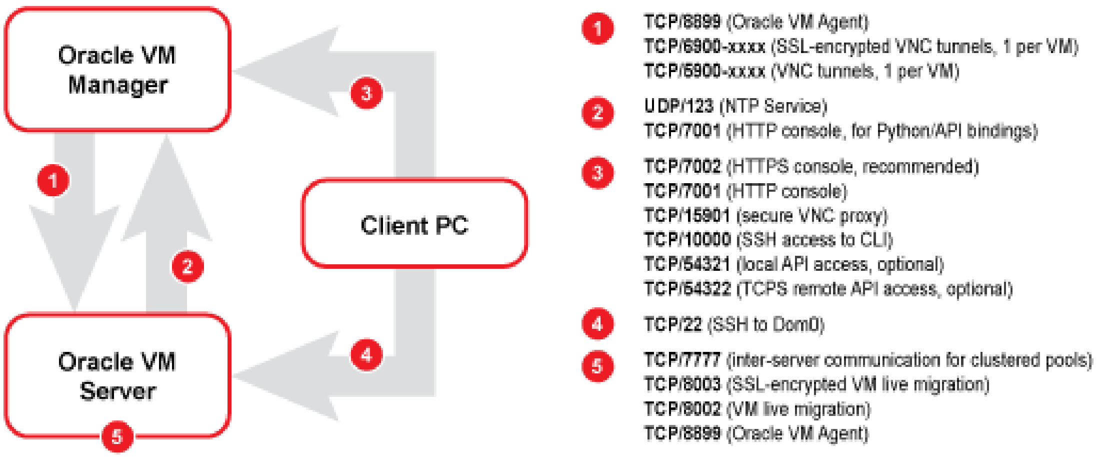
```
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 7001 -j ACCEPT
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 7002 -j ACCEPT
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 15901 -j ACCEPT
# iptables -A INPUT -m state --state NEW -m udp -p udp --dport 123 -j ACCEPT
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 54321 -j ACCEPT
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 54322 -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.

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



1 TCP/8899 (Oracle VM Agent)
TCP/6900-xxxx (SSL-encrypted VNC tunnels, 1 per VM)
TCP/5900-xxxx (VNC tunnels, 1 per VM)

2 UDP/123 (NTP Service)
TCP/7001 (HTTP console, for Python/API bindings)

3 TCP/7002 (HTTPS console, recommended)
TCP/7001 (HTTP console)
TCP/15901 (secure VNC proxy)
TCP/10000 (SSH access to CLI)
TCP/54321 (local API access, optional)
TCP/54322 (TCPS remote API access, optional)

4 TCP/22 (SSH to Dom0)

5 TCP/7777 (inter-server communication for clustered pools)
TCP/8003 (SSL-encrypted VM live migration)
TCP/8002 (VM live migration)
TCP/8899 (Oracle VM Agent)

## 2.1.2 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` 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”.

## 2.2 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 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 11*g*, including Application Development Framework (ADF) Release 11*g* Consult the Oracle WebLogic 11*g* documentation for more information.

Use of Oracle WebLogic Server with Oracle VM Manager is restricted to the servlet functionality without clustering for the Oracle VM management server.

## Oracle Database

Oracle VM uses an Oracle database as a backend repository. Depending on the version of Oracle VM and the type of installation you choose, the database may differ. These are the typical configurations:

- Oracle VM 3.1 *demo* installation with Oracle XE database backend
- Oracle VM 3.1 *production* installation with Oracle Database Standard Edition (Oracle SE) or Enterprise Edition (Oracle EE) database backend
- Oracle VM 3.2 *simple* installation with MySQL database backend
- Oracle VM 3.2 *custom* installation with Oracle Database Standard Edition (Oracle SE) or Enterprise Edition (Oracle EE) database backend

**Note**

*Only in non-production Oracle VM 3.1 environments* the Oracle XE database may be used as Oracle VM Manager repository. Oracle XE is intended for testing and demo purposes. It is not a supported product, and Oracle Support Services cannot provide bug fixes or patches.

**Note**

If you are deploying Oracle VM Manager in a production environment, you may use either MySQL database as part of the Oracle VM 3.2 *simple* installation, or Oracle Database Standard or Enterprise Edition, which you must install separately to Oracle VM. Oracle VM Manager includes a restricted-use license of these databases for use as the Oracle VM Manager Management Repository only.

When running the installer script from the Oracle VM Manager DVD or ISO image, you can choose between a quick installation to get started in the shortest possible time, and an advanced installation that offers more configuration options. In Oracle VM 3.1 these installation types are called *demo* and *production*; in Oracle VM 3.2 they are called *simple* and *custom*. The most flexible and preferred installation type of Oracle VM Manager is *production* or *custom*.

The production installation in Oracle VM 3.1, and the custom installation in Oracle VM 3.2, allow you to connect to an existing local or remote Oracle SE/EE database. You set the users and passwords to use for the Oracle Database, 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:

- 8-16 characters in length
- 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:

- Oracle Database Security and Compliance: http://www.oracle.com/technetwork/database/security/index.html
- Oracle Database Documentation home page: http://www.oracle.com/technetwork/database/enterprise-edition/documentation/index.html. Open the documentation library of your database version and select the topic *Security*.
- MySQL home page: http://www.oracle.com/technetwork/database/mysql/index.html
- MySQL Security Guide: http://dev.mysql.com/doc/mysql-security-excerpt/5.5/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.

## 2.3 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 2.2, “Installing Oracle VM Manager”. Place the servers in a private network segment with restricted access, as described in Section 2.1.2, “Preparing the Management Network”.

## 2.4 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 little 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”.

## 2.5 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 mimimize 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. To add a trusted CA certificate, follow the detailed instructions in Section 2.5.1, “Adding a Trusted CA Certificate and Keystore for SSL Encryption”. Additional instructions for the configuration of certificates are also included in this section.

- 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.

## 2.5.1 Adding a Trusted CA Certificate and Keystore for SSL Encryption

To create a secure production environment you need to obtain and install a trusted certificate from a Certificate Authority (CA). Oracle VM Manager runs on Oracle WebLogic Server, and Oracle WebLogic provides the interface for updating the digital certificate and keystore. To add a trusted CA certificate and keystore, see the procedure set out in the Oracle WebLogic documentation:

http://docs.oracle.com/cd/E17904_01/apirefs.1111/e13952/taskhelp/security/ConfigureKeystoresAndSSL.html

Two variables are mentioned in this procedure that you need to know when installing the certificate. The values for these variables in Oracle VM Manager are:

```
$JAVA_HOME\jre\lib\security   /u01/app/oracle/java/jre/lib/security
$WL_HOME\server\lib           /u01/app/oracle/Middleware/wlserver_10.3/server/lib
```

> **Note**
>
> Oracle VM has SSL enabled by default, and installs with a self-signed CA certificate. If you connect to Oracle VM Manager over HTTPS at TCP port 7002, you will receive a warning because your browser cannot verify the identity of Oracle VM Manager and considers the connection untrusted. It is recommended that you obtain a certificate from an official Certificate Authority, as described in this section and in the Oracle WebLogic documentation.

To access the Oracle WebLogic Server console, enter:

- https://*hostname*:7002/console -or-
- http://*hostname*:7001/console (HTTP is disabled by default in Release 3.2.1)

Log in with the user *weblogic* and the password you set during the Oracle VM Manager installation.

## 2.5.2 Securing Oracle VM Agent Communications with a Certificate

Communications between Oracle VM Agents and Oracle VM Manager are SSL-encrypted using an RSA algorithm and 1024-bit private key. The relevant files are located in `/etc/ovs-agent/cert`:

- `certificate.pem`

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

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

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 3.3.1, the Oracle VM Agent password is only used for authentication during the intial discovery process. Thereafter, all 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.

If you are using a version of Oracle VM prior to 3.3.1, you may wish to change the Oracle VM Agent password on occassion. The Oracle VM Manager user interface provides an option to batch change the Oracle VM Agent password for all of the servers within a server pool. You can find out more about this option within the *Oracle VM User's Guide* for your particular version of Oracle VM. This option is no longer available in version 3.3.1, due to the change of authentication mechanism.

## 2.5.3 Changing Certificate Settings for VNC and Live Migration

In a default Oracle VM installation, VNC and Live Migration traffic are secured with the same certificate as the one used for Oracle VM Agent communications. If required by your security policy, you can use a different certificate by specifying the appropriate location in the configuration file `/etc/xen/xend-config.sxp`. More specifically, you must look up the section below in the configuration file and change the location parameters of the certificate and key files:

```
# SSL key and certificate to use for the ssl relocation interface, if
#   xend-relocation-ssl-server is set.
(xend-relocation-server-ssl-key-file /etc/ovs-agent/cert/key.pem)
(xend-relocation-server-ssl-cert-file /etc/ovs-agent/cert/certificate.pem)
```

If the self-signed certificate expires, you may need to update the certificate keystore. This can be achieved by performing the following steps.

**To update the certificate keystore for the VNC RAS Proxy:**

1. Enter the following commands on the Oracle VM Manager host to create the keystore:

   ```
   # cd /u01/app/oracle/ovm-manager-3/bin
   # ./secureOvmmTcpGenKeyStore.sh
   ```

   You are prompted to enter the following information:

   ```
   Generate OVMM TCP over SSL key store by following steps:
   Enter keystore password: password
   ```

```
Re-enter new password: password
What is your first and last name?
  [Unknown]:  name
What is the name of your organizational unit?
  [Unknown]:  unit
What is the name of your organization?
  [Unknown]:  organization
What is the name of your City or Locality?
  [Unknown]:  City
What is the name of your State or Province?
  [Unknown]:  State
What is the two-letter country code for this unit?
  [Unknown]:  country_code
Is CN=name, OU=unit, O=organization, L=City, ST=State, C=country_code correct?
  [no]:  yes

Enter key password for <ovmm>
        (RETURN if same as keystore password): password
Re-enter new password: password
```

2. Use the keystore to enable the TCPS service using the `secureOvmmTcp.sh` script, which is in the same directory as the keystore script above. On the Oracle VM Manager host, enter:

   ```
   # ./secureOvmmTcp.sh
   ```

   You are prompted to enter the following information:

   ```
   Enabling OVMM TCP over SSL service

   Please enter the OVM manager user name: username
   Please enter the OVM manager user password: password
   Please enter the password for TCPS key store : password
              The keystore password created
                                                                      in the previous script
   The job of enabling OVMM TCPS service is committed, please restart OVMM to take effect.
   ```

3. Restart the local Oracle VM Manager instance:

   ```
   # /sbin/service ovmm stop
   # /sbin/service ovmm start
   ```

## 2.5.4 Enabling LDAP Authentication on Dom0

In environments with an existing LDAP authentication infrastructure, it may be preferable to enable LDAP authentication on each *Oracle VM Server* instance, to control and log access attempts on Dom0. This can enhance security for a critical asset (Dom0) for the same reasons that make centralized user control valuable in other contexts.

The packages required to the LDAP client are not included on the Oracle VM ServerISO. Therefore, it is necessary to download and install the packages manually. This section describes the steps required to do this.

Add the public or internal Yum repositories at the Oracle Linux 5u7 level. The most direct way to do this is to follow the instructions at http://public-yum.oracle.com/ for Oracle Linux 5:

```
# cd /etc/yum.repos.d
# wget http://public-yum.oracle.com/public-yum-el5.repo
```

Install the required packages to enable LDAP authentication, as well as any dependencies:

```
# yum install openldap-clients
# yum install nss_ldap
```

The installation prompts you to determine whether you wish to proceed, to which you should respond by returning the 'y' character to the prompt. The required dependencies are also listed and downloaded. If you intend to copy the package files and install them manually on your server instances, take note of the listed dependencies and ensure that these are also made available on each server where you intend to install the LDAP client.

Once installation is complete, copy the server SSL/TLS certificate to `/etc/openldap/cacerts/openldap.pem`. Make sure the certificate has the right permissions:

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

Rehash the CA certificates:

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

Enable LDAP authentication using the `authconfig` command:

```
# authconfig-tui
```

Ensure that LDAP is configured correctly to access your LDAP server. Configuration is specific to your own environment and requirements and falls outside of the scope of this document, however the following example configurations may serve to assist you:

- /etc/openldap/ldap.conf:

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

- /etc/ldap.conf:

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

## 2.5.5 Setting Up Virtual Machine Access

Oracle VM Manager uses a secure tunnel to protect virtual machine console data traffic across the network. Oracle VM Manager does not make a direct connection but rather uses a VNC proxy and SSL-encrypted tunneling. The virtual machine console is accessed via a client instance of a VNC viewer. The preferred location to install a VNC viewer is on the Oracle VM Manager host server.

Oracle recommends that you install the latest TightVNC package from http://oss.oracle.com/oraclevm/manager/RPMS/

Install TightVNC with this command:

```
# rpm -ivh tightvnc-java-version.noarch.rpm
```

Any firewall between Oracle VM Manager and the client accessing a virtual machine needs TCP port 15901 to be open for access to the secure VNC proxy. Any firewall between Oracle VM Manager and the Oracle VM Servers needs TCP ports 6900 and above to be open; one port for each virtual machine. For example, if you have 50 virtual machines, you should allow traffic over TCP ports 6900-6949.

> **Note**
>
> For non-encrypted local VNC connections to virtual machines, TCP ports 5900 and above can be used. SSL encryption is preferred from a security standpoint.

For more details about the installation and use of VNC, see Installing and Configuring Virtual Machine Console Utilities in the Oracle VM Installation and Upgrade Guide.

# 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 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 `root_no_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 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 enabled you can either open the ports used by Oracle VM Manager, or open all ports by disabling iptables. The latter is not advised in the absence of an external firewall devices because it removes network protection.

The web browser connection to Oracle VM Manager requires ports 7001, 7002 and 15901. Oracle VM Serversconnect to Oracle VM Manager using ports 7001, 7002, and optionally 54321 and 54322 for remote API access.

Oracle VM Manager, in turn, connects to the Oracle VM Servers through port 8899 for Oracle VM Agent communication, and port 5900 and up for secure VNC tunneling to virtual machines (one port per VM). Be sure to open the necessary ports on the different firewalls that may be installed between different parts of your network. Additional information and a diagram can also be found in Section 2.1, “Oracle VM Pre-Installation Tasks”.

When using iptables, ensure that the 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 [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -p tcp -m state --state NEW -m tcp --dport 21 -j DROP
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j DROP
-A INPUT -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-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 ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2049 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5900:5950 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8002 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8003 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8899 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 7777 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
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 Intrustion 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 or iptables 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.
- 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, 443 and 4433 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, 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. 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. For Oracle VM Manager, you can create and manage accounts through the WebLogic Server Administration Console. For instructions, see the Oracle Fusion Middleware documentation and navigate to WebLogic Server Administration, or go straight to this Administration Console Online Help page: Manage Users and Groups.

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 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 Storage Connect plugin used for interaction with the storage provider. If you are using generic NFS or iSCSI providers with the corresponding generic Oracle Storage Connect plugin, then configuration occurs almost entirely on the storage host. If you are using a custom third-party Oracle Storage Connect plugin, 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 Managing Storage in the *Oracle VM User's Guide*.
- Storage access configuration through access groups: refer to the *Oracle VM User's Guide*.
- Access group and storage initiator management on Oracle VM Servers: refer to the *Oracle VM User's Guide*.

For a technical overview of Oracle Storage Connect, see the Storage Connect white paper: 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 12c

**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 priniciples 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 funcionality 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, consult the Oracle Enterprise Manager documentation:

- Oracle Enterprise Manager Ops Center Administration Guide 12c Release 1: User and Role Management

- Oracle Enterprise Manager Ops Center Feature Reference Guide 12c Release 1: Oracle VM
- Oracle Enterprise Manager Cloud Administration Guide 12c Release 2: Part II - Infrastructure as a Service

## 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 datacenter 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 controled 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.