Table of Contents

Preface ................................................................................................................................. v
1. Overview .......................................................................................................................... 1
  1.1. General Security Considerations and Features ....................................................... 1
  1.2. Taxonomy .................................................................................................................. 2
2. Security Model ............................................................................................................... 5
  2.1. Desktop Access Layer ............................................................................................... 5
    2.1.1. Sun Ray Clients .................................................................................................. 5
    2.1.2. RDP Clients and the Oracle VDI RDP Broker .................................................. 7
    2.1.3. Web Services Clients ....................................................................................... 8
    2.1.4. Oracle Secure Global Desktop (SGD) ............................................................ 8
  2.2. Management Layer ................................................................................................... 9
    2.2.1. Common Agent Container ................................................................................ 9
    2.2.2. Oracle VDI Service ......................................................................................... 9
    2.2.3. Oracle VDI Center Agent ............................................................................... 10
    2.2.4. Oracle VDI Manager ....................................................................................... 10
    2.2.5. Oracle VDI Command-Line Tools .................................................................. 10
    2.2.6. Oracle VDI Database ...................................................................................... 10
    2.2.7. User Directory ................................................................................................ 11
  2.3. Virtualization Layer ............................................................................................... 12
    2.3.1. Desktop Provider Security ............................................................................... 12
    2.3.2. Desktop Security ............................................................................................. 13
    2.3.3. RDP Security .................................................................................................. 14
    2.3.4. Storage Security ............................................................................................. 14
3. Installation and Configuration Guidelines ................................................................. 17
  3.1. Installation Overview ............................................................................................... 17
  3.2. Oracle VDI Installation ........................................................................................... 19
  3.3. Component Installation .......................................................................................... 19
  3.4. Oracle VDI Configuration ....................................................................................... 19
    3.4.1. Oracle VDI Settings for Sun Ray Software .................................................... 19
    3.4.2. Default Oracle VDI Settings ......................................................................... 20
    3.4.3. Oracle VDI Host Configuration ..................................................................... 20
    3.4.4. Desktop Selector Configuration Recommendations ................................... 20
    3.4.5. Additional Configuration Recommendations ............................................... 21
    3.4.6. Configuration Summary ................................................................................ 21
Preface

The Oracle Virtual Desktop Infrastructure Security Guide is a supplemental guide to the security aspects of Oracle Virtual Desktop Infrastructure (VDI).

Audience

This document addresses the security concerns of Oracle VDI system administrators. It is assumed that readers are familiar with web and virtualization technologies and Windows system administration. Some previous exposure to UNIX operating systems, such as Oracle Solaris and Oracle Linux, is also helpful.

Document Organization

This document consists of a brief overview, a somewhat more detailed discussion of security issues based on the Oracle VDI taxonomy, and guidelines for installation and configuration:

- Chapter 1, Overview
- Chapter 2, Security Model
- Chapter 3, Installation and Configuration Guidelines

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.

Related Documents

The documentation for this product and related products is available at:


Conventions

The following text conventions are used in this document:

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

**Document Revision**

Document generated on: 2012-06-21 (revision: 1096)
Chapter 1. Overview

Table of Contents

1.1. General Security Considerations and Features ........................................................................... 1
1.2. Taxonomy .................................................................................................................................... 2

Oracle Virtual Desktop Infrastructure (Oracle VDI) is an integrated, end-to-end provisioning and delivery
service designed for the efficient management and control of virtualized desktops. Oracle VDI virtual
desktops are meant to be hosted in a secure data center.

Based largely on the integration of Sun Ray Software with other key software products, including the
Oracle VirtualBox hypervisor and MySQL database, Oracle VDI is designed to provide access to hosted
virtual desktops from a wide range of devices. It also enables customers to use hypervisor products from
other vendors, such as VMware vCenter and Microsoft Hyper-V.

This document discusses the security aspects of an Oracle VDI implementation.

1.1. General Security Considerations and Features

Oracle VDI draws on its own architecture as well as on security features of Sun Ray Software, Oracle
Secure Global Desktop (SGD), Oracle VM VirtualBox, Microsoft Remote Desktop Protocol (RDP), and
Java technologies such as Java Management Extensions (JMX). It offers users the ability to access the
same virtual desktop from a wide range of devices, located virtually anywhere. At the same time, Oracle
VDI enables data, storage, and applications to be moved from individual desktops to data centers, which
are easier and less costly to manage as well as less difficult to secure.

Access Control

Oracle VDI uses role-based access control to restrict system access according to the least privilege
principle. Each host has a root user who can assign administrative privileges to users according to
their roles as administrators, operators, and monitors for specific levels of administrative functionality,
such as managing pools of virtual machines or configuring companies. The vda CLI requires password
authentication for non-root users.

Users are typically assigned virtual desktops from pools of virtual machines configured to serve particular
job functions. Ordinary users are not usually assigned administrative roles, although they may administer
their own virtual desktops under some circumstances (see About Oracle VDI Role-Based Administration).
For access to client functionality, these users are authenticated against a corporate User Directory, which
is also the source of authentication for the desktop host.

Client authentication can be disabled to allow for special requirements (see How to Disable Client
Authentication in Sun Ray Software 5.3 Administration Guide).

Common Sense Practices

To further strengthen an Oracle VDI implementation, administrators may want to separate administrative
functions from user traffic by keeping them on separate networks. In some cases, it is advantageous to
use additional, separate networks for virtualization and for storage traffic as well. Network configuration is
discussed in How to Configure a Dedicated iSCSI Network and Planning a Sun Ray Network Environment
in Sun Ray Software 5.3 Administration Guide.
Security in general can also be enhanced by common-sense practices, such as:

- Establishing a thorough security policy and making sure it is enforced.

- Implementing firewalls to block unauthorized access to virtual desktops and administrative controls, and reviewing and updating their access rules on a regular basis (see Firewalls Ports and Protocols).

- Leaving client authentication enabled unless disabling it is strictly required for technical reasons.

- Disabling any unnecessary services that may be enabled by default.

- Making regular sweeps for possible vulnerabilities at the network, server, and storage levels.

For instance, a recent NASA study revealed serious deficiencies in at least six servers that had been considered secure. Site administrators and security officials may not find this surprising, but it should serve as a reminder that even the best security policy is meaningless without enforcement.

A Word About Viruses

Traditionally, Windows PCs have been widely targeted for viruses, malware, and various types of attacks. Other operating systems and form factors are also becoming increasingly subject to unwanted attention. Virtual PC desktops are subject to the same vulnerabilities as physical PC machines, and they require similar precautions, with a few key differences. For instance, scheduled virus scans of individual virtual desktops may slow down performance, so it is preferable to perform virus scanning on storage instead. It is always a good idea to perform routine virus checking of desktop pools as well, to keep possible infections from spreading. Also, viruses can be introduced, intentionally or not, via USB devices, so administrators should give careful consideration to the advantages and disadvantages of allowing USB device access.

The following references may also be useful:

- Virus Scanning on Sun Storage 7000 Unified Storage System With Trend Micro InterScan Web Security Suite

- Using Sophos Anti-Virus for Virus Scanning on the Sun ZFS Storage Appliance

- Virus Scan in the Sun ZFS Storage 7000 System Administration Guide

1.2. Taxonomy

Oracle VDI consists of four main elements, or layers, which are described in more detail in System Overview of Oracle Virtual Desktop Infrastructure.
Desktop Access

Oracle VDI provides many ways to access virtual desktops so that a user can work on the same virtual desktop from nearly anywhere, such as from:

- Sun Ray Clients
- Instances of the Oracle Virtual Desktop Client (OVDC) running on a wide range of devices, including nearly any desktop or laptop computer or an Apple iPad
- Remote Desktop Protocol (RDP) clients

Oracle Secure Global Desktop (SGD), for example, includes an RDP client that it uses to connect to Oracle VDI desktops.

Because Oracle VDI hosts these desktops in a relatively secure environment, some of the common risks associated with client devices, such as loss of confidential data, are mitigated.

Management

Oracle VDI manages every aspect of virtual desktop life cycles: creation, configuration, assignment to users, and recycling. To control, configure, and monitor its operation, Oracle VDI provides a command-line interface and the Oracle VDI Manager, a web-based management tool.

Virtualization

Oracle VDI can use any of several popular hypervisors to handle virtualization functionality. The Oracle VirtualBox hypervisor, which is well integrated into the Oracle VDI architecture, can be used to provision UNIX and Linux desktops as well as Windows desktops. Oracle VDI also supports Microsoft Hyper-V and
VMware vCenter, which provision only Windows desktops. In addition, Oracle VDI supports the use of Remote Desktop Services (RDS) hosts for session-based virtualization.

For security enhancement practices and precautions for non-Oracle products, see the manufacturers' product documentation.

**Storage**

To store instances of virtual machines, templates, snapshots, and other items associated with virtualization, Oracle VDI supports:

- Sun ZFS
- iSCSI Storage
- Network File System (NFS)
- Local Storage
Chapter 2. Security Model

Table of Contents

2.1. Desktop Access Layer ................................................................. 5
   2.1.1. Sun Ray Clients ................................................................. 5
   2.1.2. RDP Clients and the Oracle VDI RDP Broker ................................. 7
   2.1.3. Web Services Clients ......................................................... 8
   2.1.4. Oracle Secure Global Desktop (SGD) ...................................... 8
2.2. Management Layer ................................................................. 9
   2.2.1. Common Agent Container .................................................... 9
   2.2.2. Oracle VDI Service ............................................................. 9
   2.2.3. Oracle VDI Center Agent .................................................... 10
   2.2.4. Oracle VDI Manager ............................................................ 10
   2.2.5. Oracle VDI Command-Line Tools ........................................ 10
   2.2.6. Oracle VDI Database ......................................................... 10
   2.2.7. User Directory ................................................................. 11
2.3. Virtualization Layer ............................................................... 12
   2.3.1. Desktop Provider Security ................................................... 12
   2.3.2. Desktop Security .............................................................. 13
   2.3.3. RDP Security ................................................................. 14
   2.3.4. Storage Security .............................................................. 14

This chapter describes the main elements, or layers, of Oracle VDI with particular attention to security. For a more detailed description of other aspects of the Oracle VDI architecture, see System Overview of Oracle Virtual Desktop Infrastructure.

2.1. Desktop Access Layer

This section describes security properties of the methods used to access Oracle VDI desktops. For further details on aspects of desktop access that are not directly related to security, see Desktop Access.

2.1.1. Sun Ray Clients

Oracle VDI embeds and configures Sun Ray Software, including the Sun Ray Windows connector, to enable the use of Sun Ray Clients and the Oracle Virtual Desktop Connector for access to virtual desktops. Oracle VDI does not increase Sun Ray connection security requirements beyond the Sun Ray Software defaults.

2.1.1.1. Client Connection

Sun Ray Clients use the Oracle Appliance Link Protocol (ALP) to connect to a Sun Ray server running on an Oracle VDI host. ALP provides some limited security features, which can be administered at the Sun Ray server level. For example, ALP can encrypt keystroke and display traffic between the Sun Ray Client and the Sun Ray server, but it does not encrypt USB device traffic. For information on enabling and disabling USB devices, see How to Enable or Disable USB Services in the Sun Ray Software 5.3 Administration Guide.

After the Client is authenticated and connected to the Sun Ray Server via ALP, the Sun Ray Windows connector provides access to the virtual desktop via RDP. The RDP connection can and should occur entirely within the data center.
Sun Ray Clients can be located anywhere. If they are located outside the corporate network, their built-in VPN capabilities make it more difficult for network traffic to be intercepted. For more information, see VPN Support in the Sun Ray Software 5.3 Administration Guide.

The OVDC does not have built-in VPN capabilities. Use of OVDC in a configuration that requires VPN for remote access requires that VPN client software be installed on the host operating system (OS).

2.1.1.2. Kiosk Mode

Sun Ray Software kiosk mode bypasses traditional UNIX user authentication, typically to provide controlled access to a Windows session hosted on a Remote Desktop Services Host without requiring extra login steps for users. Oracle VDI uses kiosk mode to provide access to virtual desktops from traditional Sun Ray Clients, with or without smart cards, and from Oracle Virtual Desktop Clients clients.

The Oracle VDI kiosk session runs under an anonymous UNIX account. It authenticates users against the configured User Directory rather than the local UNIX passwd name service, presenting the user with an Oracle VDI login screen instead of a Sun Ray login screen.

Once authenticated to Oracle VDI, users can access their assigned virtual desktops. User credentials are retained in memory for the duration of the kiosk session so that credentials can be passed between processes, when needed, via UNIX pipes; however, credentials are never stored in a database, on a disk, or in any other persistent fashion.

If client-side authentication is disabled in Oracle VDI, no authentication is performed on the Oracle VDI host, and login is deferred to the virtual desktop.

Kiosk mode and sessions are described more fully in Kiosk Mode in the Sun Ray Software 5.3 Administration Guide.

2.1.1.3. Desktop Selector

Before gaining access to any desktop, each user normally goes through some kind of authentication mechanism. Oracle VDI comes with its own login dialog, which enforces a simple username/password authentication against a configured User Directory. Upon successful authentication, the user is presented with a desktop selection dialog, or Desktop Selector. The Desktop Selector displays a list of the desired desktops on the Sun Ray Client or OVDC. The desktop selection step can be skipped if the user is not assigned multiple desktops.

You can fine-tune and modify the behavior of the Desktop Selector two ways: by using the Oracle VDI command-line interface to modify global configuration settings or by using the Sun Ray Administration tool (Admin GUI) to modify arguments and parameters for the Oracle VDI kiosk session. Several of these settings also affect system security, as described below.

You can switch Oracle VDI authentication off completely, for instance, to support some other authentication mechanism or to hide the Oracle VDI login dialog/Desktop Selector. In such a scenario, it is highly recommended that you make sure authentication is enforced on the desktop operating system (OS) itself. For example, the desktop should be configured to bring up its own standard login screen before allowing access to any sensitive data.

When the Desktop Selector is used and authentication is enabled, desktops are typically configured for single sign-on (auto login). In this scenario, after successfully passing the initial Oracle VDI login screen, the user can access all assigned desktops without having to pass through any other login screens that might otherwise be presented by the desktop OS.

Oracle VDI automatically forwards any initially entered username/password information to the selected desktop. This is convenient for the user, but it also implies a potential security risk. If the user leaves the
Sun Ray session open without logging out explicitly, a different user could sit down at the Sun Ray Client and access all of the previous user's desktops without passing any kind of authentication. To minimize this risk:

- Instruct users either to log out explicitly before leaving a Sun Ray Client or to bring up the Oracle VDI screen lock (see Section 2.1.1.4, “Screen Locks”).

- Configure a reasonably short session idle timeout interval, so that a user who does not select a desktop within a given amount of time is automatically logged out by the system (see How to Change the Admin GUI Timeout in the Sun Ray Software 5.3 Administration Guide).

### 2.1.1.4. Screen Locks

Most desktop operating systems provide their own screen locking mechanism, which automatically locks the screen after a certain period of inactivity. Automatic screen locking, however, may give Oracle VDI users a false feeling of security. For instance, it is easy to use the Sun Ray Windows connector menu to disconnect from a desktop that displays a locked screen while remaining logged in the Oracle VDI system and able access assigned desktops. To avoid this possibility, you can enforce a logout always policy, so that the user is logged out of Oracle VDI completely when any displayed desktop is disconnected (see Desktop Selector Configuration).

The drawback of this policy is that it prevents users from switching between multiple desktops without having to re-enter a username/password pair. You can disable this default logout behavior in order to improve user experience but should consider the security implications before doing so.

Oracle VDI also provides its own built-in screen locking mechanism (see How to Enable Desktop Screen Locking on Sun Ray Clients), which is disabled by default. Once you switch it on explicitly, the screen locks whenever a Sun Ray session is disconnected, such as when a user removes a smart card. The user must then re-enter a password to access the selected/displayed desktop.

### 2.1.1.5. Smart Cards

Oracle VDI supports smart cards, which associate a Sun Ray session with a user by means of a token (see Tokens in the Sun Ray Software 5.3 Administration Guide). It is possible to restrict the system access to registered tokens, and tokens can be registered for specific users. The login screen implementation takes this information into account and presents the username in the login dialog. The username is read-only by default, so that when a smart card is inserted, a user cannot assume a different identity by changing the username on the login dialog. The default behavior is recommended.

### 2.1.2. RDP Clients and the Oracle VDI RDP Broker

The Oracle VDI RDP Broker is bundled with Oracle VDI to provide access to RDP-based Oracle VDI desktops for generic RDP clients (see About the Oracle VDI RDP Broker). It first submits client requests and user credentials to the Oracle VDI Service for authentication, after which the Oracle VDI Service locates and starts the requested desktop. It then redirects the RDP client to connect directly either to the desktop host or to the Oracle VDI RDP Proxy service.

The Oracle VDI RDP Broker communicates over secure RDP connections.

The Oracle VDI RDP Broker supports Standard RDP Security at the Client-Compatible Encryption Level. This means that it uses bidirectional RC4 encryption with a key-size of up to 128 bits (see Encryption Levels). It cannot use FIPS-compliant encryption.

RDP clients cannot use Enhanced RDP Security (TLS/SSL or CredSSP/NLA) when accessing the Oracle VDI RDP Broker.
2.1.2.1. Oracle VRDP

The Oracle VirtualBox Remote Display Protocol (VRDP) is a backward-compatible extension to RDP that supports the use of any standard RDP client to control remote virtual desktops. When an RDP client accesses Oracle VirtualBox desktops through VRDP, the client remains connected to the Oracle VDI RDP Proxy service, which is part of the Oracle VDI RDP Broker. The Oracle VDI RDP Proxy then relays RDP messages to the Oracle VDI desktop based on routing information contained in the routing token.

The routing token is sent to the RDP Proxy unencrypted. RDP connection security for connections through the Oracle VDI RDP Proxy is negotiated directly between the client and the virtual machine. Oracle VirtualBox supports Standard RDP Security at the Client-Compatible Encryption Level.

Although enhanced RDP security (TLS/SSL) is supported for direct access to VirtualBox VRDP, it cannot be used for connections through the Oracle VDI RDP Proxy.

2.1.2.2. Microsoft RDP

When an RDP client accesses Windows desktops through Microsoft RDP, the Oracle VDI RDP Broker redirects it to the Remote Desktop Services (RDS) server farm or to the individual desktop, which requires direct access from the client PC to the desktop host.

RDP connection security for these connections is negotiated directly between the client and the desktop host. The exact combination of RDP encryption and security options for connections depends on the configuration of the virtual machine or RDS server and client capabilities.

2.1.3. Web Services Clients

The Oracle VDI web service API enables the creation of custom clients. It uses the same web server as the Oracle VDI Manager and shares the same certificates.

The web service API also enables queries of desktop access information for a given Oracle VDI user and control of that user's desktop. Any such user must be registered in the User Directory and must present authentication credentials in order for a client to connect to the web service API. Web service API connections use secure HTTPS connections. Web services clients must be set up to accept the server certificates, which by default are self-signed.

To access the desktops managed through the web services API, web services clients require direct RDP access to the desktop host.

2.1.4. Oracle Secure Global Desktop (SGD)

SGD provides access to Oracle VDI desktops from the SGD webtop. Access methods have evolved over time, and are described in the following paragraphs. All use the Adaptive Internet Protocol (AIP) for access from the client PC to SGD and are described in Desktop Access Using Oracle Secure Global Desktop. See SGD documentation for more information about AIP security and configuration.

SGD 4.6 includes a Virtual Server Broker that acts as an Oracle VDI client. If Oracle VDI and SGD are installed on the same host, the Virtual Server Broker can establish a connection from the SGD RDP client to the user's Oracle VDI desktop.

SGD 4.7 also includes an add-on Virtual Server Broker, which uses the web services API. With SGD 4.7, SGD and Oracle VDI do not need to be co-located.

The web service security properties described in Section 2.1.3, “Web Services Clients” apply between the SGD server and the Oracle VDI and desktop hosts.
You may choose to set up a SGD Windows Object to access Oracle VDI through the Oracle VDI RDP Broker. In this case, the RDP client security properties described in Section 2.1.2, “RDP Clients and the Oracle VDI RDP Broker” apply between the SGD server and the Oracle VDI and desktop hosts.

SGD supports the encryption levels listed under Section 2.1.2, “RDP Clients and the Oracle VDI RDP Broker”. SGD does not support:

- Federal Information Processing Standards (FIPS) encryption level
- Transport Layer Security (TLS) for server authentication
- Terminal Server communication encryption

2.2. Management Layer

This section describes the functions of the elements used to manage Oracle VDI desktops.

2.2.1. Common Agent Container

The Common Agent Container, usually called Cacao, is a Java Management Extensions (JMX) management object container that provides JMX-compliant, secure access through one or more communication protocols. Management services that provide JMX interfaces can be realized as Cacao modules and executed within an instance of the Cacao daemon. Initial Cacao setup creates a self-signed Certificate Authority (CA) certificate for each configured instance. Communication is secured by certificates derived from this CA certificate.

Several Oracle VDI services are implemented as Cacao modules. These modules share a single Cacao daemon instance, named $vda$, which restricts access from local command-line tools to privileged users and allows remote access only from well-known peers whose CA or service certificate is registered in its trust keystore. Clients access the modules via secure SSL connections.

All Cacao modules log important events and access decisions, as well as more detailed information that is useful for troubleshooting, into a common, per-instance log file. (See Checking Oracle VDI Services and Logs for information about this file and how to configure logging.) By default, every user of the Oracle VDI host can read the Cacao log file.

2.2.2. Oracle VDI Service

The main Oracle VDI Service module is a Cacao module that manages virtualization and storage hosts to provide the services needed by Oracle VDI clients. It accesses the Oracle VDI database to store configuration data and runtime state shared by the entire Oracle VDI Center, or cluster of hosts running Oracle VDI (see Installing Oracle VDI and Configuring Oracle VDI Centers). The Oracle VDI Service also performs the administrative action requests it receives through the Oracle VDI web-based and command-line administration interfaces.

The Oracle VDI Service accepts requests only from local clients and administrative components. Every request requires appropriate authentication and authorization.

Client requests require user credentials that are authenticated against the configured User Directory, unless client authentication is disabled. Local components that can submit client requests include the Web Service API implementation hosted by the Oracle VDI web server and the $vda-client$ command-line interface. These components use a private interface based on local sockets to connect to the Oracle VDI Service.

Administrative requests require user authentication against the Oracle VDI host's passwd name service and authorization through assigned administrator roles. The local superuser (root) on each Oracle VDI host
automatically has all authorizations through the primary administrator role and can issue administrative requests through the `vda` CLI (see the `vda(1)` man page) without further authentication.

The Oracle VDI Service stores keys or passwords for virtualization and storage hosts securely in the Oracle VDI database. Credentials for access to the Oracle VDI database are stored in local files on the Oracle VDI host with restrictive access permissions. Oracle VDI administrators should protect privileged accounts on these hosts, as well as backups of host configuration data, against unauthorized access.

### 2.2.3. Oracle VDI Center Agent

The Oracle VDI Center Agent is a Cacao module that resides in the same Cacao agent instance as the Oracle VDI Service. The Oracle VDI Center Agent accepts administrative requests from privileged clients on the local host and internal requests from peer agents on other hosts in the Oracle VDI Center.

Communication between Oracle VDI Center Agents on different hosts also uses secure SSL connections. When a new host joins the Oracle VDI Center, it exchanges public certificates with the existing members. To ensure that this exchange takes place with the correct host, the configuration process presents a certificate fingerprint of the host being contacted for user verification.

The Oracle VDI Center Agent monitors and performs administrative actions on all local Oracle VDI Services but does not interact directly with virtualization or desktop hosts, storages, or the Oracle VDI database.

### 2.2.4. Oracle VDI Manager

The Oracle VDI Manager is the user interface for Oracle VDI administration. It is implemented by a non-privileged web server process. The same web server also provides the Oracle Oracle VDI web service API.

Connections to the Oracle VDI Manager use the HTTPS protocol. The Oracle VDI Manager offers an HTTP interface for initial contact, but that immediately redirects the web browser to the secure HTTPS port.

By default, the Oracle VDI Manager web server uses a self-signed certificate, so that users are required to accept a security exception when contacting the Oracle VDI Manager.

The Oracle VDI Manager requires the administrator to log in using a local user account on the Oracle VDI host. The login credentials are used to authenticate requests to the Oracle VDI Service.

### 2.2.5. Oracle VDI Command-Line Tools

The `vda` and `vda-backup` command-line tools issue requests to the VDA service, which applies role-based authorizations to each request. Both tools require password authentication for all non-root users. Other Oracle VDI command-line tools generally require local root privileges.

### 2.2.6. Oracle VDI Database

Oracle VDI stores most of its operation and configuration data in a MySQL database shared by all hosts. Oracle VDI automatically sets up and configures an embedded MySQL Server database. Administrators have the option of setting up and configuring a remote MySQL database to suit their own requirements.

Note

Administrators who choose to use a remote database are responsible for configuring appropriate security. Those who do not have full control may have to negotiate security with one or more database administrators. See
Oracle VDI uses a special database user account to access Oracle VDI data. Unless you use a remote database and specifies an existing account or a password, Oracle VDI generates a secure, random password for this account. Long, randomly generated passwords are generally more secure than shorter ones that are easier to remember or that may have been used before. Oracle VDI stores credentials for database access in a local file with restrictive privileges.

Oracle VDI also uses an account with administrative privileges in the database for certain database configuration tasks. This account is not used in normal operation. Unless you use an existing database account (remote database only) or to specify a password during configuration, Oracle VDI generates a secure, random password for this account, too. Oracle VDI stores credentials for database reconfiguration in a local file with restrictive privileges.

When an embedded MySQL Server database is configured for high availability, Oracle VDI uses another predefined account for database replication.

Oracle VDI uses secure SSL connections to access the embedded Oracle VDI MySQL Server database, using a short-lived (“throwaway”) CA to generate server and client certificates for securing database access. This facilitates replacing the whole set (CA cert, client cert, server cert), rather than individual certificates, for instance, if there is reason to believe that any of the involved keys has been compromised.

If you are using a remote database, it is your responsibility to set up SSL on the database server and provide the required certificates to Oracle VDI at configuration time.

### 2.2.7. User Directory

Oracle VDI uses an existing User Directory for user identification and authentication, associating desktops with users from the directory according to policies or direct assignments. Oracle VDI supports Active Directory (AD) or LDAP directories and five levels, or types, of authentication to use with these directories:

- **LDAP Anonymous Authentication**
  
  Anonymous authentication is useful for quick integration with an LDAP server but is not recommended for production environments. The connection from Oracle VDI to the User Directory is not authenticated at all. Anonymous read access is required on the directory.

- **LDAP Simple Authentication**
  
  Simple authentication is the recommended choice for production platforms that integrate with LDAP directories other than Active Directory. The connection from Oracle VDI to the User Directory is authenticated by the credentials (user DN/password) of an administrator.

- **LDAP Secure Authentication**
  
  With secure authentication, the connection from Oracle VDI to the User Directory is authenticated by the credentials (user DN/password) of an administrator and secured by SSL.

- **Kerberos Authentication**
  
  Kerberos Authentication is the typical choice for integration with Microsoft Active Directory. The connection from Oracle VDI to the User Directory is authenticated by the Kerberos protocol, using the credentials (username/password) of an administrator.

- **Public Key Authentication**
Public key authentication is recommended for integration with Microsoft Active Directory when the domain controller requires LDAP signing (see How to Enable LDAP Signing in Windows Server 2008). The connection to the User Directory is authenticated by a client certificate and secured by SSL.

Both Active Directory and LDAP also provide encryption so that user credentials are not submitted as plain text. See About User Directory Integration for more information about user directories in Oracle VDI.

2.3. Virtualization Layer

The following sections describe the security model used for desktops and desktop providers.

For more information about secure configuration of any virtualization or session platform not supplied by Oracle, please refer to the documentation provided by the vendor.

2.3.1. Desktop Provider Security

Oracle VDI categorizes desktop providers according to the virtualization platform they use or the type of session they support.

2.3.1.1. Hypervisor-based Desktop Providers

In the case of hypervisor-based desktop providers, the virtualization platform provides virtualization services and security mechanisms, and the desktop provider manages the virtualization services.

Oracle VDI manages hypervisors through the following interfaces:

• The Oracle VM VirtualBox desktop provider uses the Oracle VM VirtualBox web services API.
• The Microsoft Hyper-V desktop provider uses the Windows Remote Management (WinRM) interface.
• The VMware vCenter desktop provider uses the VMware Infrastructure SDK web services API.

Communication to and from these interfaces takes place over secure HTTPS connections (see Firewalls Between Oracle VDI and Desktop Providers).

Each desktop provider is configured with the username and password of a sufficiently privileged account of the hypervisor management interface. These credentials are stored securely in the Oracle VDI database.

2.3.1.2. Session-based Desktop Providers

Session-based desktop providers offer access to desktops hosted on remote computers or on the Oracle VDI host itself.

Kiosk Session Provider

Under Sun Ray Software, a given kiosk session normally runs as its own Sun Ray session, initiated by the X display manager (dtlogin/gdm), which operates with root privileges. The kiosk framework performs some of the session setup and teardown steps with root privileges and has hooks that allow customers to add session setup and teardown scripts, which also require root privileges.

Under Oracle VDI, kiosk sessions run within the already-started Oracle VDI kiosk session type, and the kiosk session runs without privileges. If a kiosk session type is designed to require root privileges, for instance, for custom setup and/or teardown code, it will not work, or at least will not work as intended.

Administrators should examine desktops and custom-designed kiosk sessions for possible vulnerabilities, such as users' ability to escape from the restricted session environment. For example, a UNIX terminal on
a custom kiosk session could give users access to a command-line interface of the underlying operating system.

It is also advisable to identify and fix application exploits, wherever possible, to prevent unauthorized access, especially to the underlying operating system. At one time, for example, the Netscape Navigator print function allowed users to modify the `lp` print command used by the browser so that a user could replace the `lp` command with any application or script on the system and run it by clicking Print.

For further information on kiosk sessions in general and developing customized kiosk sessions to further enhance security, see:

- *Kiosk Mode* in the *Sun Ray Software 5.3 Administration Guide*
- *Sun Ray Kiosk Desktop Providers*
- *Configuring Desktop Providers and Virtualization Platforms*

**RDS**

The Microsoft RDS desktop provider can be set up, optionally, to provide additional status information for monitoring through the Windows Remote Management (WinRM) interface. Communication to this interface takes place over secure HTTPS connections.

**Generic Session Provider**

In addition to the kiosk and RDS session providers, there is a generic session provider that can be used to access any RDP server, such as a standalone PC running a suitable version of Windows, as an Oracle VDI desktop.

**2.3.2. Desktop Security**

Most desktop providers offer access to full desktops as supported by the operating system of an individual virtual machine or a remote host. The security features and configuration of these desktops depend on the desktop host operating system and access method as well as on which desktop provider and desktop pool type is used. See *Preparing Desktops*.

Oracle VDI administrators should take the same precautions with these desktops as they would with any physical PC, securing them with respect to the remote access method as well as normal practices, such as providing anti-virus software.

**Desktop Templates**

The easiest way to create new virtual desktops is to clone them from a template. Templates make it easy and convenient to roll out new versions of OS, application software, and security updates to all derived desktops (see *About Templates and Revisions*). However, anyone administering pools of virtual machines should pay close attention to the secure installation and configuration of desktop templates, since any problems in the template are replicated in its clones.

Oracle VDI desktops that cannot be updated through a new template revision need to be updated individually, through manual or automated update mechanisms provided by the software vendor or vendors.

**Pools**

Flexible desktop pools can provide enhanced protection against malware or user error, depending on their recycling policy. When a used desktop is deleted and subsequently replaced by a fresh instance, the
newly cloned desktop is in the state provided by the template, which should be clean and well-defined. Any malware or misconfiguration issues that may have affected a prior instance are discarded when the virtual desktop is deleted.

### 2.3.3. RDP Security

Oracle VDI uses RDP for connections to virtual desktops. Administrators can specify levels of access control, authentication, connection, and session security with configuration policies on the Oracle VDI host. Some specific security properties of the connection can be controlled through RDP client settings and capabilities. Details vary depending on the desktop platform and access method.

#### RDP Connections

RDP connections are encrypted by default. The encryption mechanism depends on the configuration of the desktop host and the capabilities of the RDP client (see Section 2.1.2, “RDP Clients and the Oracle VDI RDP Broker”).

The Sun Ray Windows connector, which acts as the RDP client for Oracle Virtual Desktop Client (OVDC) and Sun Ray client connections, provides options to control security choices and requirements. For information about enhanced network security options for the Sun Ray Windows connector, see Network Security in the Sun Ray Software 5.3 Administration Guide.

RDP options can be configured separately for each pool. Most advanced security options, such as those to control peer verification for SSL connections, can also be configured globally through Oracle VDI kiosk session arguments.

Before users are granted access to desktop pools that use RDP, they are authenticated by the host, using the RDP authentication mechanisms specified with the Oracle VDI host configuration policies. RDP connections use a well-known port on the virtual machine (see Firewalls Between Clients and Oracle VDI).

#### VRDP Connections

The Oracle VM VirtualBox desktop provider can treat connecting to the host console and authenticating to the desktop operating system as separate steps, which do not need to occur at the same time. Since VRDP is a special case of RDP, VRDP connections are encrypted by default. Oracle VDI configures the virtual machine to require a secure, one-time password for RDP connections, made available only to authenticated Oracle Oracle VDI clients. If the guest OS supports this feature, then when the desktop becomes available for login, Oracle VDI cooperates with the Oracle VM Virtual Box guest extensions to provide automatic login to the desktop for the authenticated Oracle VDI user. This scenario does not apply, however, if Oracle VDI client authentication is disabled.

### 2.3.4. Storage Security

Oracle VDI uses storage systems to maintain desktop and template images, both for personal (static) and flexible (dynamic) desktops. These images can be managed and operated upon by Oracle VDI and/or the hypervisor. As the administrator, you can choose which desktop provider to use.

Oracle VDI manages the storage for the Oracle VM Virtual Box and Microsoft Hyper-V desktop providers and ZFS storage pools on Sun Unified Storage Systems or Oracle Solaris hosts. It uses Secure Shell (SSH) for management access to storage hosts. Management access requires a sufficiently privileged account on the storage host credentials for which are stored securely in the Oracle VDI database. Hypervisors access the desktop image data through a common account.

When Oracle VDI manages storage, it does not encrypt iSCSI used for data traffic connections by default. This is a good strategy for optimizing performance with large amounts of data, but it assumes that access
to the storage data network is sufficiently secured. An isolated network within the data center, with physical access controls, for instance, would supply sufficient security in this case. Oracle VDI administrators should ensure that the storage data network is in fact secured, whether by this method or by another.

Customers who use the VMware vCenter desktop provider should refer to VMware documentation for information about how to configure storage securely. When vCenter is used, Oracle VDI directs the use of storage, but does not interface with storage directly.

For all other desktop providers, and for local storage, Network File System (NFS) storage, and unmanaged iSCSI storage scenarios, storage is managed independently of Oracle VDI. For any of these cases, refer to the documentation for the specific storage product and operating system for information about secure configuration.
Chapter 3. Installation and Configuration Guidelines

Table of Contents

3.1. Installation Overview ................................................................. 17
3.2. Oracle VDI Installation ............................................................. 19
3.3. Component Installation ............................................................ 19
3.4. Oracle VDI Configuration ......................................................... 19
  3.4.1. Oracle VDI Settings for Sun Ray Software ......................... 19
  3.4.2. Default Oracle VDI Settings .............................................. 20
  3.4.3. Oracle VDI Host Configuration ........................................ 20
  3.4.4. Desktop Selector Configuration Recommendations ............ 20
  3.4.5. Additional Configuration Recommendations ..................... 21
  3.4.6. Configuration Summary .................................................. 21

When considering how best to secure an Oracle VDI implementation, first examine the current or planned installations of related software products, such as Sun Ray Software, VirtualBox, and, if it will be used, SGD. Specific security guidelines for these products are discussed in the following documents:

- Sun Ray Software Administration Guide
- VirtualBox Installation Guide
- VirtualBox Security Guide
- SGD Installation Guide
- SGD Security Guide

3.1. Installation Overview

The Oracle VDI installation process itself can be fairly straightforward if proper attention is paid to pre-installation considerations such as:

- What operating system platform to use
- What hypervisor to use as a virtualization server
- Network architecture
- Firewalls
- Storage
- MySQL database model
  - Embedded (default)
  - Remote (specify SSL keys and certificates for database access)

The following table summarizes the most important pre-installation choices.

Table 3.1. Pre-installation Topics

<table>
<thead>
<tr>
<th>Topic</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choosing the right operating system platform</td>
<td>Oracle VDI runs on Oracle Solaris and Oracle Linux. For ease of administration, it may make sense to use</td>
</tr>
</tbody>
</table>
### Installation Overview

<table>
<thead>
<tr>
<th>Topic</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>the operating system that IT staff find more familiar; however, please consider the following points:</td>
<td></td>
</tr>
<tr>
<td>• Oracle VDI does not support Oracle Solaris Trusted Extensions.</td>
<td></td>
</tr>
<tr>
<td>• Oracle VDI can be configured to use smart cards for authentication, but only on Oracle Solaris. PC/SC lite is not yet available on Linux platforms.</td>
<td></td>
</tr>
<tr>
<td>• Oracle VDI has its own Role-Based Access Control (RBAC) scheme, unrelated to Oracle Solaris RBAC. To set up RBAC, see About Oracle VDI Role-Based Administration.</td>
<td></td>
</tr>
<tr>
<td>• Oracle VDI does not support Security Enhanced (SE) Linux. Administrators who run Oracle VDI on Oracle Linux should disable the SE Linux mandatory access control function.</td>
<td></td>
</tr>
<tr>
<td>In permissive mode, rules are not enforced, but incidents that violate rules are logged, and the logs may become flooded, so this mode is not recommended.</td>
<td></td>
</tr>
<tr>
<td>Choosing a virtualization platform (hypervisor)</td>
<td>Oracle VDI includes Oracle VirtualBox, which uses VRDP as the default virtualization platform. VirtualBox:</td>
</tr>
<tr>
<td>VirtualBox:</td>
<td></td>
</tr>
<tr>
<td>• Enables Oracle Solaris and Oracle Linux as well as Windows desktops</td>
<td></td>
</tr>
<tr>
<td>• Connects to desktops at the hypervisor level, which eliminates the need to open the operating system itself</td>
<td></td>
</tr>
<tr>
<td>• Allows the use of multiple virtualization choices in parallel</td>
<td></td>
</tr>
<tr>
<td>Some customers already have VMware vCenter or Microsoft Hyper-V implementations in place, perhaps with customized security precautions configured. Oracle VDI supports the use of these products when customers find it appropriate; however, Oracle cannot be responsible for any security vulnerabilities incurred through the use of these hypervisors.</td>
<td></td>
</tr>
<tr>
<td>Choosing an external database model</td>
<td>Oracle VDI includes MySQL database software, but administrators can choose to use a different MySQL database, whether to utilize an existing database installation, to use a MySQL cluster as a database, or to get full control over security configuration of the database.</td>
</tr>
</tbody>
</table>
### 3.2. Oracle VDI Installation

The Oracle VDI installation script automates nearly every aspect of installation of Oracle VDI and its components. If installation is completed without a host being configured, no new services are enabled. Mere installation should not impact host security.

### 3.3. Component Installation

The Oracle VDI installer sets up VirtualBox and configures the VBox Webservice API.

### 3.4. Oracle VDI Configuration

Regular configuration procedures are documented in the Oracle VDI Administration Guide (see Installing Oracle VDI and Configuring Oracle VDI Centers). Security concerns and recommendations are listed in the following sections.

#### 3.4.1. Oracle VDI Settings for Sun Ray Software

The default Oracle VDI configuration of Sun Ray Software includes the following settings:

- The Sun Ray data store (admin) password is set to the password entered during Oracle VDI configuration. If no password is specified, a secure auto-generated password is used by default.
- Sun Ray Software is prepared for use in a failover group, with a secure, auto-generated Sun Ray group signature. As further hosts are added to the Oracle VDI Center, they are added to the Sun Ray Software failover and replication group.
- The Sun Ray Administration Tool (Admin GUI) is enabled and set up for remote HTTPS access. Administrator authentication is set up to use system authentication.
- The system root account is added to the list of authorized Sun Ray administrators.
- The fixed Sun Ray administrator admin account is removed.
- Kiosk mode is configured with the Oracle VDI vda kiosk session type.
• Kiosk mode is set up with the number of kiosk user accounts on each host specified during Oracle VDI configuration.

• Sun Ray access policy is set up to use kiosk mode with all kinds of tokens and to allow access using the Oracle Virtual Desktop Client.

• Session access is allowed for any client connecting via (routed) LAN.

### 3.4.2. Default Oracle VDI Settings

After standard Oracle VDI configuration:

• Oracle VDI and Sun Ray Software services are running and accepting connections.

• ALP encryption is set to default (off).

• Oracle VDI and Sun Ray Software Manager user interfaces are running.

### 3.4.3. Oracle VDI Host Configuration

Please keep the following considerations in mind when configuring a primary host:

• Administrator Password

  If you accept the default for this setting, a random, automatically generated password is used. Typically, such a password is more secure than a password specified by a human operator. You do not need to know this password for normal Oracle VDI operation. Unless you have special requirements, it is recommended that you accept the automatically generated default.

  If you later need direct access to the Oracle VDI database or to the Sun Ray Software data store, Oracle VDI provides methods to retrieve this password.

• User ID Range Start

  This setting defines the lowest number in a range of user IDs. The size of the range is determined by the Maximum Number of Sessions on This Host parameter. If you grow your installation, you may need to expand this range later.

  Do not assign an ID in this range for any actual user. During initial configuration, this is verified and the range moved to higher numbers, if necessary, but this cannot easily be enforced for the future, if you use a central naming service, such as LDAP or NIS for your user accounts.

  Specify this range so that it cannot collide with the range of user IDs you allocate for regular users, preferably by specifying a significantly higher number here.

  When configuring secondary hosts, pay particular attention to the verification of the primary host's SSL certificate as described in Configuring Oracle VDI on a Secondary Host. Once you accept the authenticity of the primary host, by entering the root password, that host gains access to the full Oracle VDI installation with all internal credentials.

### 3.4.4. Desktop Selector Configuration Recommendations

To further strengthen Desktop Selector, take the following measures:

• Enable the Oracle VDI screen lock (see How to Enable Desktop Screen Locking on Sun Ray Clients).

• Keep Oracle VDI authentication enabled (default), unless there is a strong reason to disable it.
# /opt/SUNWvda/sbin/vda settings-setprops -p clientscreenlock=Enabled

If authentication is disabled at the Oracle VDI level, then authentication must be enforced on the desktop OS.

# /opt/SUNWvda/sbin/vda settings-setprops -p clientauthentication=Enabled

• Configure the session idle timeout to a reasonably low value (the default is 180 seconds, i.e., three minutes).

VDA kiosk session arguments: -t (timeout in seconds)

• Keep the desktop logout always policy enabled (default).

# /opt/SUNWvda/sbin/vda settings-setprops -p client.logout.always=Enabled

• If smart cards/tokens are used, they should be registered explicitly for the desired users, whether through the Sun Ray administration tool or through Oracle VDI administration.

## 3.4.5. Additional Configuration Recommendations

To strengthen the standard configuration, take the following measures:

• Use the Sun Ray Software utcrypto CLI or the Sun Ray Web Admin tool to enable ALP encryption and server authentication (see Admin GUI Tools and Commands in the Sun Ray Software 5.3 Administration Guide).

• Synchronize primary and secondary hosts.

  • Oracle VDI configures the primary host as an NTP (Network Time Protocol) server. If the secondary hosts have different time settings, they can get out of sync with the primary. To prevent this condition, set up NTP on all Oracle VDI hosts (see Time Synchronization).

• Use MD5 Fingerprint to authenticate secondary hosts.

• Configure administrators and their roles.

  • In Sun Ray Software, use the utadminuser command to configure users (see the utadminuser(1M) man page).

  • In Oracle VDI, use the RBAC feature to assign roles (see About Oracle VDI Role-Based Administration).

• Disable the Oracle VDI RDP Broker service, if it is not needed.

• Use the Sun Ray Software utdevadm CLI to enable or disable device services as needed (see the utdevadm(1M) man page and How to Enable or Disable USB Services in the Sun Ray Software 5.3 Administration Guide).

## 3.4.6. Configuration Summary

After initial Oracle VDI configuration completes, the host is in the following state:

• Oracle VDI and Sun Ray Software services are running and accepting connections.

• Oracle VDI and Sun Ray Software Manager user interfaces are running. The local root user can log into each management UI with full privileges.
Configuration Summary

- Oracle VDI desktops are not configured and are not offered to connecting users.
- ALP encryption is set to the default (off).

The following settings have been applied to the Sun Ray services on the host:

- The Admin GUI is enabled and set up for remote HTTPS access.
- The system root account is added to the list of authorized Sun Ray administrators (see *Administrative Name and Password* in the *Sun Ray Software 5.3 Administration Guide*). The fixed Sun Ray administrator `admin` account is removed.
- The Sun Ray data store (`admin`) password is set to the password entered during Oracle VDI configuration. A secure auto-generated password is used by default.
- Sun Ray Software is prepared for use in a failover group, with a secure, auto-generated Sun Ray group signature. As further hosts are added to the Oracle VDI Center, they are added to the Sun Ray Software failover and replication group.
- Sun Ray access policy is set up to use kiosk mode for all kinds of access and to allow access using the Oracle Virtual Desktop Client with all kinds of tokens.
- Kiosk mode is configured with the Oracle Virtual Desktop Infrastructure `vda` kiosk session type.
- Kiosk mode is set up with the number of kiosk user accounts on each host specified during Oracle VDI configuration.
- Session access is allowed for any client connecting over a routed LAN.