

Sun Virtual Desktop Infrastructure

VDI Demo (Featuring Microsoft Remote Desktop Services)
for Version 3.1

April 2011

ORACLE®

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

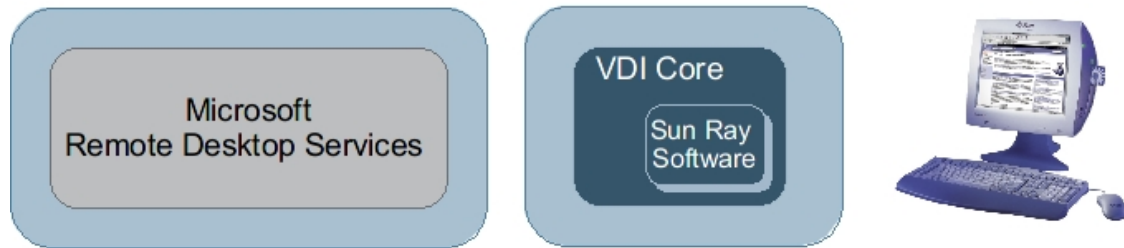
Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

VDI Demo (Featuring Microsoft Remote Desktop Services)


VDI Demo (Featuring Microsoft Remote Desktop Services)

The following information describes how to install and configure the VDI components (VDI Core and virtualization platform). You will need two separate hosts to be able to perform this install.



System Requirements

- 1 Windows Server 2008 or Windows Server 2003
Refer to [Windows Server 2008](#) or [Windows Server 2003](#) hardware requirements.
- 1 host for the VDI Core
At least one 2.0GHz x86 CPU
At least 4GB RAM
At least 32GB disk space

 The VDI Demos are not supported production environment configurations. For more information about supported production environment VDI configurations, please see the Supported Configurations page.

1. Install and Configure Microsoft Remote Desktop Services

Use the following information to install and configure Microsoft Remote Desktop Services (RDS) for your VDI Demo. It assumes you have referred to the Microsoft documentation for installing and configuring a Windows Server. For general information about how RDS works with VDI, see the [About Microsoft Remote Desktop Platforms](#) section.


How to Install Microsoft Remote Desktop Services

- To install the Remote Desktop Services role on Windows Server 2003 refer to <http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx>.
- To install the Remote Desktop Services role on Windows Server 2008 refer to <http://www.microsoft.com/windowsserver2008/en/us/rds-product-home.aspx>.


How to Prepare a Windows Server for VDI

After installing Microsoft Hyper-V or Microsoft Remote Desktop Services you must prepare your Windows server to communicate with the VDI Core. VDI does not require any agents to be installed on the Windows servers, instead the VDI Core communicates with Windows servers using Windows Remote Management (WinRM) over HTTPS (a secure protocol). For HTTPS, WinRM requires a server certificate to operate properly. This certificate is used for encryption of the communication channel. For more details, see "[Windows Remote Management](#)" or "[Configuration and Security](#)" in the Microsoft documentation.

Preparing the Windows server for communication with the VDI Core is a two-step process. First, you must generate the self-signed certificate using the Microsoft Internet Information Services (IIS) 6.0 Resource Kit Tools (Step 1, below). Then configure `winrm` to listen for HTTPS requests (Step 2, below).

 These steps are necessary for Remote Desktop Services (or Terminal Services) Windows servers so that critical information about the server can be displayed in the VDI Manager (including CPU usage, memory usage, and number of user sessions). The delivery of desktop sessions from RDS pools is still provided by a regular RDP connection. For information about how to configure the RDP settings per desktop pool, see the [How to Configure RDP Options Per Pool](#) page.

Before You Begin

 The following commands should be executed in Command shell, not Powershell.

Steps

1. Generate a self-signed certificate on the Windows server.
Use the `selfssl.exe` tool which is part of the IIS 6.0 Resource Kit and can be downloaded from the [Microsoft Support web site](#).

- a. Copy `selfssl.exe` to your Windows Server.
 - b. Create a self-signed certificate:

```
C:\Program Files\IIS Resources\SelfSSL\selfssl /T /V:<days>
```

There parameter `/V:` dictates the number of days the certificate will be valid. There is no maximum value.

- c. Run the `certutil` command, and make note of the Cert Hash of the new certificate:

```
certutil -store MY
```



If the Windows server and VDI server are not in time sync, you might not be able to connect VDI to the server as the certificate is not valid for the delta between both servers.

2. Configure Windows Remote Management for HTTPS.

The `winrm` tool is used to configure remote management settings on the server. You must specify the certificate hash to be used, and the authentication settings to allow the VDI Core to send requests.

- a. Install WS-Man (WinRM).



This step is for Windows Server 2003 only. Windows Server 2008 and Hyper-V Server 2008 come with WinRM pre-installed.

- b. Download the WS-MAN v1.1. installation file (`WindowsServer2003-KB936059-x86-ENU.exe`) from www.microsoft.com.
 - c. Proceed to the installation by running the installation file `WindowsServer2003-KB936059-x86-ENU.exe`.
 - d. Create a listener on the Windows Server.
In a command shell run:

```
winrm create winrm/config/listener?Address=IP:<HYPER_IP>+Transport=HTTPS
@{Hostname="<HOST>" ;CertificateThumbprint="<CERTHASH>" ;Port="443" }
```

- Replace <HYPER_IP> with the IP address of the Windows Server.
- Replace <HOST> with the Computer Name of the Windows Server.
- Replace <CERTHASH> with the Cert Hash value, with no spaces, noted from the self-signed certificate created with `selfssl`.

e. Open that port so that the Windows Server can receive requests from the VDI Core:

```
netsh firewall add portopening TCP 443 "Sun VDI Remote Management"
```

Port 443 is the port the VDI Core listens on by default.

f. Enable Basic authentication on the server by running the command:

```
winrm set winrm/config/service/auth @{Basic="true"}
```



If you use a port other than 443 for VDI communication with Hyper-V or RDS, you must remember to specify this port when adding the host in VDI Manager.

2. Install and Configure the VDI Core Software

How to Install and Configure the VDI Core Software (Demo)

Steps

1. As root user, unzip the VDI archive if you have not already done so, and run the installation (shown for x86).

```
# unzip vda_3.1_amd64.zip
# cd vda_3.1_amd64
# ./vda-install
```

After accepting the license agreement, the installation process begins, and all VDI components are installed. These components include:

```
Sun VDI 3.1 Installation
+ Installing Sun VDI Core...
+ Installing MySQL Database...
+ Installing Web Administration...
+ Installing Apache Tomcat...
+ Installing RDP Broker...
+ Installing Sun Ray Client...
+ Installing Java Runtime Environment...
+ Installing Sun Ray Server Software...
+ Installing Sun Ray Connector for Windows Operating Systems...
```

2. After successful installation reboot your machine.

```
# reboot
```

3. As root user, run the vda-config script, and choose the "0 **Evaluation Sun VDI Host**" configuration type:

```
# /opt/SUNWvda/sbin/vda-config
```

You will see the following configuration script:

```
Sun Ray Server Software Configuration
+ Providing configuration data...
+ Loading Sun Ray data store...
+ Populating Sun Ray data store...
+ Creating Sun Ray core services configuration...
+ Restarting Sun Ray data store daemon...
+ Configuring Sun Ray Server Software Web Administration...
+ Adding 10 user accounts for Sun Ray sessions...

Sun Ray Client Configuration
+ Setting Kiosk Mode Session Type to 'vda'...
+ Enabling Kiosk Mode Policy for All Card and Non-Card Users...
+ Enabling LAN Connections...
+ Configuring Sun Ray Connector for Windows Operating Systems...
+ Restarting Sun Ray Server Software...

MySQL Database Configuration
+ Creating MySQL group (vdadb)...
+ Creating MySQL user (vdadb)...
+ Setting up MySQL directory...
+ Setting up MySQL cluster directory...
+ Initializing database...
+ Starting Sun VDI database (MySQL)...
+ Setting user rights...
+ Creating database tables...
+ Configuring database connection...

Sun VDI Web Administration Configuration
+ Enabling Sun VDI web administration...
+ Restarting Sun VDI web administration...

RDP Broker Configuration
+ Starting RDP broker...

System Configuration
+ Restarting Common Agent Container service...
```

For more information about the settings of the default configuration, see the [VDI Defaults](#) page.

Once configuration is complete, go to <http://<server name>:1800> (or <http://localhost:1800> if remote administration has been disabled). Use root user credentials to log into the VDI Manager. You will be re-directed to https and the browser will ask you to accept the security certificate. After confirmation, you should get the login screen.

3. Set Up Desktop Providers and Pools

How to Create Desktop Providers (Microsoft Remote Desktop Services)

Desktop providers encapsulate the details of the underlying virtualization platform. At a minimum, you must configure one desktop provider before you can continue with the creation of pools. There is no limitation to the number of providers the system can manage, but note that there can be only one pool per desktop provider. At any time, you can configure additional providers.

Before You Begin

The Windows Server hosting Hyper-V must be prepared to communicate with the VDI Core before a desktop provider can be

created. Refer to the [How to Prepare a Windows Server for VDI](#) page for detailed information.

VDI Manager Steps

1. Sign into the VDI Manager.
 - a. Go to `http://<server name>:1800` (or `http://localhost:1800` if remote administration has been disabled), and use root user credentials. For a multi-host configuration, use one of the VDI Secondary hosts.
 - b. You will be re-directed to https and the browser will ask you to accept the security certificate. After confirmation, you should get the login screen.
2. Select the Desktop Providers category in the left sidebar.
3. Select New in the Microsoft Remote Desktop Providers overview.

The New Desktop Provider for Microsoft Remote Desktop wizard is displayed. It enables you to add either a Microsoft Remote Desktop (Terminal) Services host or several Microsoft Remote Desktop (Terminal) Services hosts that all participate in the same cluster.

 - a. Type the host name or IP address and the administrator credentials for the host.
 - b. When you are finished adding hosts, add more hosts or select the Select Existing Hosts option.
 - c. Click Finish.

The new desktop provider is displayed in the VDI Manager. You can now view the provider details, including CPU and memory utilization. You can add or remove additional Microsoft Remote Desktop Services hosts as needed, provided they all belong to the same cluster.

How to Create Desktop Pools

Sun VDI organizes desktops in pools. A pool is a collection (or container) of desktops. Typically you will create different pools for different types of users. For example, the engineering team at your company might have different desktop requirements than the marketing department.



Sun VirtualBox Desktop Providers Only

When changing pool settings from NAT networking to Host Networking + Windows RDP, existing desktops that are running must be stopped and restarted or else subsequent user requests for these desktops will fail. This issue occurs because existing, running desktops will be using NAT and will not have a public IP address. After the pools settings have been changed, subsequent requests for that desktop will attempt to access the desktop via the private (and inaccessible) NAT IP.



Microsoft Remote Desktop Providers Only

Only one pool can be created per Microsoft Remote Desktop provider.

VDI Manager Steps

1. Sign into the VDI Manager.
 - a. Go to `http://<server name>:1800` (or `http://localhost:1800` if remote administration has been disabled), and use root user credentials. For a multi-host configuration, use one of the VDI Secondary hosts.
 - b. You will be re-directed to https and the browser will ask you to accept the security certificate. After confirmation, you should get the login screen.
2. Select the Pools category in the left sidebar.
3. Click New in the All Pools overview.

A New Pool wizard is displayed.

 - a. For Sun VirtualBox and Microsoft Hyper-V desktop providers, choose one of the following pool types:
 - Dynamic pools are filled with cloned flexible desktops. If you choose the Dynamic Pool type, the desktops in the pool will be temporarily assigned to users. They will be recycled each time the user logs out. This pool type is considered dynamic because the user-desktop assignments are often changing.
 - Growing pools are filled with cloned personal desktops. If you choose the Growing Pool type, the desktops in the pool will be permanently assigned to users. Users can log in and out without losing their desktop settings. The desktops are not recycled.

- Manual pools are initially empty. They are filled manually by importing personal desktops. The Manual Pool type should be used if cloned desktop assignment is not an option.



For Microsoft Remote Desktop providers, pool types do not apply.

- Select a template.
If you have already imported a desktop from Sun VirtualBox or Microsoft Hyper-V, you can select it as a template to clone desktops from.
If no desktop has been imported yet, select None from the drop down menu. After a desktop has been imported, you can select it as a template from the pool's Cloning tab.
- If you chose a template in the previous step, select the pool size or enable automatic cloning.
You can modify your choice at any time in the pool's Cloning tab.
- Click Finish.
A new pool is displayed in the Pools overview.

4. Set Up a User Directory

How to Set Up a User Directory for a Demo

Now the desktops must be made available to users. Typically the user information is already stored in an Active Directory or LDAP server. Before you can assign users to desktops, you must configure the desired Active Directory/LDAP server and the VDI Core.



If you do not have a directory already installed, you may use [OpenDS](#) as explained in this [blog entry](#).



New Page!

If you would like more details about setting up Active Directory with Kerberos authentication, refer to the new [How to Set Up Active Directory and Kerberos for a Demo](#) page.

Steps

1. Select the Settings category in the left sidebar.
2. Then select the User Directory subcategory.
3. Click Add User Directory... to launch the User Directory wizard. Continue depending on your directory type.

- LDAP directory that supports Anonymous Authentication



Active Directory does not support Anonymous Authentication.

- Select LDAP Type, and click Next.
 - Select Anonymous Authentication.
 - Enter the hostname or IP address, and port number, of the LDAP server. 389 is the default port number used by most LDAP servers.
 - Enter the base DN of the LDAP server. Specifying a base DN is optional. It allows you to restrict the part of the LDAP directory used to search for the users. In most cases it is not necessary to provide the base DN.
For example: `cn=Users,dc=my,dc=company,dc=com`
 - Click Next to review your choices before completing the configuration.
- Active Directory or other type of LDAP directory that does not support Anonymous Authentication
 - Select LDAP Type, and click Next.
 - Select Simple Authentication.
 - Enter the hostname or IP address, and port number, of the LDAP server. 389 is the default port number used by most LDAP servers.
 - Enter the base DN of the LDAP server. Specifying a base DN is optional. It allows you to restrict the part of the LDAP directory used to search for the users. In most cases it is not necessary to provide the base

DN.

For example: `cn=Users,dc=my,dc=company,dc=com`

- e. Enter the user name. It must be the fully distinguished name (DN) of a user that has sufficient privileges to search the LDAP directory.

For example: `cn=super-user,cn=Users,dc=my,dc=company,dc=com`.

- f. Enter the password for the user.
- g. Click Next to review your choices before completing the configuration.

5. Add Users to Pools, and Assign Tokens to Users

How to Assign Users to Pools or Desktops

You can either assign a user to a specific desktop, or you can assign a user (or user group) to a desktop pool. If a user is assigned to a pool and requests a desktop, Sun VDI will automatically deliver any available desktop from the pool.

For Microsoft Remote Desktop providers, users cannot be directly assigned to desktops. Instead, users or groups are assigned to Remote Desktop Services pools.

VDI Manager Steps

1. Sign into the VDI Manager.
 - a. Go to `http://<server name>:1800` (or `http://localhost:1800` if remote administration has been disabled), and use root user credentials. For a multi-host configuration, use one of the VDI Secondary hosts.
 - b. You will be re-directed to https and the browser will ask you to accept the security certificate. After confirmation, you should get the login screen.
2. Select the Users category.
 - To assign a user or a group, select the Users and Groups subcategory in the left sidebar.
 - a. Search for users and groups in the user directory.
You can specify user name or user ID.
 - b. Select a user or group name, and then the Assignment tab in the corresponding profile.
 - c. Select Add in the either the user's Assigned Desktops or Assigned Pools table, or the group's Assigned Pools table.
 - To assign a custom group, select the custom group name in the left sidebar.
 - a. Select the Assignment tab in the custom group's profile.
 - b. Select Add in the custom group's Assigned Pools table.
3. In the pop-up window, choose the pool or desktop to be assigned, and click OK.

You can always see which pools and desktops are associated with a user by clicking the Summary tab of the user or group's profile.

How to Assign Tokens to Users

In a Sun Ray environment, users will take advantage of smart cards (tokens) to initiate a session on a Sun Ray thin client (DTU). With VDI 3.1, you can assign a token to a user. It is also possible to assign desktops directly to specific tokens. Once tokens have been created, they can be assigned to pools and desktops.

VDI Manager Steps

1. Sign into the VDI Manager.
 - a. Go to `http://<server name>:1800` (or `http://localhost:1800` if remote administration has been disabled), and use root user credentials. For a multi-host configuration, use one of the VDI Secondary hosts.
 - b. You will be re-directed to https and the browser will ask you to accept the security certificate. After confirmation, you should get the login screen.
2. Select the Users tab and Users and Groups entry in the left sidebar.

3. Search for a known user in the user directory.
4. Click on the user's name, and then select the Token tab in their profile.
5. Assign the token.
 - If you are assigning a new token, click New in the Tokens table. Then Enter the ID of the new token (e.g. Payflex.500d9b8900130200).
 - If you are assigning an existing token, select Add in the Tokens table. Then search for the desired token.



Token IDs can be copied directly from the SRSS Admin GUI (see the Tokens tab and display Currently Used Tokens).

CLI Steps

1. Open a terminal window and sign into the server with root credentials.
For a multi-host configuration, use one of the VDI Secondary hosts.

2. Assign a token.

- Assign a new token to a user.

```
# /opt/SUNWvda/sbin/vda token-create -p token-id=<token ID>,user=<user ID>
```

- Example – Creating a new token and assigning it to a user

```
# /opt/SUNWvda/sbin/vda token-create -p
token-id=Payflex.600a7c5600130200,user=jd123456
Token Payflex.600a7c5600130200 created
```

- Assign an existing token to a user.

```
# /opt/SUNWvda/sbin/vda token-create -p token-id=<token ID>,user=<user ID>
```

- Example – Assigning an existing token to a user

```
# /opt/SUNWvda/sbin/vda token-setprops -p user=jd123456
Payflex.600a7c5600130200
Token properties updated
```

6. Access a Virtual Desktop

The two easiest desktop access methods for a demo setup are Sun Ray and Remote Desktop Connection because they are already configured with VDI Core configuration. The following information will explain a quick way to get them up and running. If you would like to configure the advanced options for these software, or use Sun Secure Global Desktop Software (SGD) as your desktop access method, please refer to the main documentation set on the [Accessing Desktops](#) page.

How to Access Desktops with Sun Ray (Demo)

Sun Ray in VDI 3.1 supports [Sun Ray Desktop Unit \(DTU\)](#) and [Sun Desktop Access Clients](#) as virtual desktop access methods. The

steps below refer describe desktop access via a DTU. For detailed information about desktop access with Sun Ray, see the [Accessing Desktops](#) page.

Steps

If you have already directed your DTU to your VDI Core host, you will not need to do any extra configuration. Simply insert a user smartcard, and enter user credentials to access your desktop.

- Turn off authentication (optional).

This information is included to simplify a demo setup, but it is not a required step. If you decide to turn off authentication, no password will be required at the VDI desktop selector screen. If you required authentication for the guest operating system during virtual machine creation, the user must still authenticate themselves in the guest operating system.

Executed the following command on the VDI host:

```
/opt/SUNWvda/sbin/vda settings-setprops -p clientauthentication=Disabled
```



If you are already working from a DTU directed at a server other than your VDI Core host, you will need to redirect the DTU. Refer to the [How to Redirect a DTU Session](#) on the SRSS 4.2 information site for further details.

How to Access Desktops with Microsoft Remote Desktop Connection (Demo)

For detailed information about desktop access with Microsoft Remote Desktop Connection, see the [Accessing Desktops](#) page.

Steps

1. Open a Windows Remote Connection client either on Windows or Mac OSX.
2. Enter details for the VDI Core host and provide a user ID as the connection parameter.
3. Establish the connection to access your desktop.