

# Horizon DaaS Platform 6.1

## Technical Notes

This document provides information on a variety of technical topics related to the Horizon DaaS Platform.

August 2014

**vmware**

## Revision History

Date	Version	Description
09/04/2014	1.0	Initial release
09/23/2014	1.1	Corrected TOC to include Appendices

© 2014 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# Contents

1 Backing Up and Restoring Databases	7
1.1 Back Up a Database	7
1.2 Restore a Database	7
2 Slony Reinitialization	9
3 Billing Summary Reports	10
3.1 Overview	10
3.2 Override Report Intervals	10
3.3 Description of Record Layout	10
4 Custom Branding	12
4.1 Introduction	12
4.2 Desktop Portal	12
4.3 Enterprise Center	12
5 Database Failover	14
5.1 Overview	14
5.2 Enable Write Operations on the Secondary Database	14
5.3 Promote the Secondary Appliance to Primary Appliance	15
6 Datacenters	16
6.1 Failover a Datacenter	16
6.2 Failback a Datacenter	17
6.3 Rename a Datacenter	20
6.3.1 Overview	20
6.3.2 Edit final_config.txt	20
6.3.3 Rerun bootstrap.sh	20
6.4 Decommission a Datacenter	21
6.4.1 Execute Initial Shutdown Steps	21
6.4.2 Perform Initial Tenant Maintenance	21
6.4.3 Promote the Primary Service Provider and Tenant to be the Primary Across Datacenters	21
6.4.4 Perform Initial Service Provider Maintenance on Remaining Datacenter	22
6.4.5 Clean Up Proxychains Configuration	22
6.4.6 Clean Up FDB	22
6.4.7 Re-initialize Slony on Affected Nodes	23
6.4.8 Bringing the System Up	23
6.4.9 Install New Root CA and Certificates on the Other Appliances	24
6.4.10 Final Tasks	24
7 DtRAM Performance Test Setup	25
7.1 Performance Testing	25
7.1.1 Overview	25
7.1.2 Previous Results	25
7.2 Troubleshooting and Diagnosis	27
7.2.1 Summary	27
7.2.2 dtRAM Configuration	27
7.2.3 dtRAM Operation	30

8 Gold Patterns	32
8.1 Creating a Linux Gold Pattern	32
8.1.1 Overview	32
8.1.2 Prepare the Linux Desktop	32
8.1.3 Install the Linux Python DaaS Agent	32
8.1.4 Remove and Purge the Linux Python DaaS Agent Package	33
8.2 Enable Post-Sysprep Commands	34
9 Monitoring	35
9.1 Introduction	35
9.1.1 Critical Nodes	35
9.1.2 Basic System Functions	36
9.2 Web Application Monitoring	36
9.2.1 Port Response	36
9.2.2 Monitoring CIM Classes	36
9.3 CIM Providers on Horizon DaaS Management Nodes	36
9.3.1 Operating Environment CIM Providers for Horizon DaaS Nodes	36
9.3.2 Application-Specific CIM Providers for Horizon DaaS Management Appliances	39
9.3.3 Description of Horizon DaaS CIM Providers	40
9.4 WBEM and CIM	46
9.4.1 Connecting to the WBEM/CIM Server of a Horizon DaaS Management Appliance	47
9.4.2 Using WBEM/CIM to Monitor ESX Hosts	48
10 Configure NetApp Storage	49
10.1 Summary	49
10.2 Hardware and Software Requirements	49
10.3 NFS Exports	49
10.4 Local Mount Point Structure	49
10.5 Permissions and Security	50
10.6 Add a New NetApp Service Account	50
11 RDS Configuration	51
11.1 Overview	51
11.2 Service Provider and Tenant Deployment Coordination	51
11.2.1 Profile Sizing Guide	52
11.2.2 Example: RDS Customer Provisioning	52
11.2.3 Recommended Reading	53
11.3 Configuring RDS on the Horizon DaaS Platform	54
11.3.1 Service Provider Creates a Session Based Desktop Model (RDS Virtual Server)	54
11.3.2 Service Provider Assigns Quota	54
11.3.3 Enterprise Center Administrator Creates Session Profiles	55
11.3.4 Enterprise Center Administrator Creates Session Pools	56
11.3.5 Browsing Session Pools	60
12 Remote Applications	61
12.1 Overview	61
12.2 System Requirements	61
12.2.1 Operating Systems	61
12.2.2 End Point Client	61
12.2.3 Protocols	62
12.2.4 Licenses	62
12.3 Enterprise Center Setup	62
12.3.1 Create a Pool and Associated Remote Applications	62
12.3.2 Map Users to the New Pool	63
12.4 Launch an Application in the Desktop Portal	63

12.5 Launch an Application in the View Client	65
12.6 Important Session Timeout Recommendations	66
12.6.1 RDS/Session Pools	66
12.6.2 Individual Desktop Pools	67
12.7 Switch session types	68
<b>13 Configure RSA</b>	<b>69</b>
13.1 Add Tenant Appliances to the RSA Authentication Manager	69
13.2 Enterprise Center Configuration	69
13.3 Generic Troubleshooting for "Access Denied"	70
13.4 Troubleshoot Problems with Files Required by the RSA APIs	71
13.5 Restore Tenant Appliance(s)	72
13.6 Deactivate RSA Authentication (Service Providers Only)	72
13.7 How an End User Logs in to the Horizon DaaS Portal	73
13.7.1 Invalid Token Codes	74
13.7.2 Establish an RSA SecurID PIN	74
13.8 Known Limitations of the RSA API	75
<b>14 Super Tenant</b>	<b>76</b>
14.1 Overview	76
14.2 Super Tenant Prerequisites	76
14.2.1 Networking Requirements	76
14.2.2 Tenant Active Directory and DNS Configuration	76
14.2.3 Tenant DHCP Configuration	77
14.2.4 Gold Pattern and DaaS Agent	77
14.2.5 Tenant Infrastructure Overview Diagram	78
14.3 Service Center	79
14.3.1 Create a Super Tenant	79
14.3.2 Enable an Existing Tenant as a Super Tenant	79
14.3.3 Add Networks for a Super Tenant	80
14.3.4 Disabling the Super Tenant Option	81
14.4 Enterprise Center	81
14.4.1 Create a Desktop/Session Pool	82
14.4.2 Browse Pool View	83
14.4.3 Desktop Pool Migration	83
14.4.4 RDS isolation	83
14.5 Billing	83
<b>Appendix A Connection Matrix</b>	<b>85</b>
<b>Appendix B Guest OS Support</b>	<b>91</b>

This page intentionally left blank

# 1 Backing Up and Restoring Databases

---

## 1.1 Back Up a Database

### Procedure

- ▶ Run the following command in the appliance:

```
/usr/local/desktop/scripts/backup_db.sh -P '<postgres_db_password>'
```

This command extracts a PostgreSQL database into an archive file, creating a backup file of the form `<hostname>.<timestamp>.tar.gz` in the `/usr/local/desktop/backup` folder.

### Optional Commands

`backup_db.sh` accepts the following optional command line arguments.

Argument	Description
<code>-P password</code>	Password for database user admin
<code>-V true</code>	Enable verbose mode
<code>-U username</code>	PostgreSQL username (default is postgres).

## 1.2 Restore a Database

The procedure below restores one database.

### Note the following:

- You must perform all restores on the primary appliance, and then re-initialize slony to populate the database to the secondary appliance.
- If you need to restore a tenant appliance, you might need to restore both the edb and fdb databases.

### Procedure

1. Run `sudo bash` and authenticate.
2. Stop `dtService` for both service provider appliances or for both tenant appliances:  

```
service dtService stop
```
3. Stop slony:  

```
service dtService stop  
killall slon
```

4. On the primary appliance, complete these steps.

a. Copy the backup file to a directory in /tmp (the file has the form *<hostname>.<timestamp>.tar.gz*):

```
mkdir /tmp/backup_working  
cp /usr/local/desktop/backup/<filename> /tmp/backup_working
```

b. Extract the backup file:

```
cd /tmp/backup_working  
tar zxvf <filename>
```

c. Move to the directory where the .bak file exists and perform the restore. For example:

```
cd /usr/local/desktop/backup  
env PGPASSWORD=<pswd> /usr/local/pgsql/bin/pg_restore -i -w -U admin -d <type>  
-v --clean <filename>
```

where:

- *<pswd>* is the postgres database password
- *<type>* is the file type, either edb or fdb
- *<filename>* is the name of the extracted backup file

5. On both appliances, re-initialize slony. For instructions, see [Slony Reinitialization](#).

## 2 Slony Reinitialization

---

On each appliance in an Organization run these commands as root.

### Procedure

1. Stop dtService on all nodes:

```
service dtService stop
```

2. Stop slon daemons (kill daemons on target nodes):

```
killall slon
```

3. Run this command on the target db (FDB or EDB):

```
drop schema _slony cascade;
```

**Note:** Drop the schema only for the affected database pair.

4. If you stopped dtService on the Primary service provider node for re-initialization of the FDB on the service provider appliances, then start the service again on the primary service provider node:

```
service dtService start
```

5. Start slon daemons as follows.

- For the service provider org, start the daemon for the FDB:

```
/usr/local/desktopone/scripts/start_slon_fdb.sh
```

- For the tenant org, start the daemons for both the FDB and the EDB:

```
/usr/local/desktopone/scripts/start_slon_fdb.sh
```

```
/usr/local/desktopone/scripts/start_slon_edb.sh
```

6. Access the dt-console on the primary service provider appliance using the credentials found under **dt-Console Access** on the **General Configuration** page of the Service Center

7. Invoke the UpgradeManagerImpl bean and activate methods below.

For FDB:

```
Invoke initSlonyForOrg(orgId,<blank>,"fabric")
```

For EDB:

```
Invoke initSlonyForDesktopManager(orgId, datacenterId, elementId)
```

When these methods have returned true, start the dtServices on the stopped appliances.

## 3 Billing Summary Reports

---

### 3.1 Overview

Horizon DaaS captures Quota information along with usage for each tenant. This data is sorted by Datacenter, and is intended to be used by the service provider for billing information.

All billing information retrieval must be done via REST APIs. The retrieval of billing information via scripts is not supported.

**Note:** By default the Billing Summary Report will contain information about disabled and enabled tenants, but there is a policy ('`billing.summary.skip.disabled.tenants`') that can alter this functionality to only collect information for enabled tenants. To activate this option, set the policy value to 'true'.

### 3.2 Override Report Intervals

By default, the platform captures billing summary information daily just after midnight (UTC) and purges previous summaries older than 180 days. To override these default intervals, follow the procedure below.

#### Procedure

1. In the Service Center, select **tenants ► policy**.
2. On the Policy Configuration page, set the following policies:
  - **billing.summary.collection.interval**  
The interval between billing collections in milliseconds (ms). The default is 86400000 ms (24 hours).
  - **billing.summary.purge.interval policies**  
The number of days to retain billing summary records in the database. The default is 180 days. Records older than the interval are purged from the database. Set to 0 to retain all billing history in the database.

### 3.3 Description of Record Layout

The table below describes the values returned in each column.

Column Name	Sample Value	Description
snapshot	201203220856	Date and Time of record (format: yyyyMMddhhmm)
org_id	1001	The unique ID of the Organization/Tenant

<b>org_name</b>	Tenant A	The name for the tenant identified by org_id
<b>datacenter_id</b>	5925d361-4c1c-490e-9616-c5041d067b8e	A unique ID that identifies the Datacenter location
<b>status</b>	enabled	The status of the tenant: <b>Enabled, Disabled, Error</b>
<b>type_id</b>	1cb3f348-f987-4834-a33c-742ef30d356b	Unique Id for given Type: <ul style="list-style-type: none"> <li>• <b>template</b> for Template quota</li> <li>• <b>desktop</b> if there are no quotas (all 0) and no <b>in_use_count</b> numbers. In this case, <b>quota</b> and <b>in_use_count</b> are set to -1 to indicate nothing was found for the tenant.</li> </ul>
<b>desktop_model_name</b>	Pro	This value is blank for a <b>Template.Quota</b>
<b>model_protocols</b>	31	If the type is <b>PROTOCOL</b> , this column indicates the bitmask value for that protocol. RDP = bit 0 RGS = bit 1 HDX = bit 2 VNC = bit 3 NX = bit 4 PCoIP = bit 5  For example, the bitmask <b>31</b> means RDP, RGS, HDX, VNC, and NX are available and the bitmask <b>1</b> means only RDP. If the type is <b>DESKTOPMODEL</b> , this column is ignored and contains 0.
<b>quota</b>	17	Error Value of -1
<b>in_use_count</b>	17	When Session Type= Number of sessions provisioned for; otherwise -1 indicates an error while the summary was being taken or that the system could not communicate with the tenant. The in_use_count can be higher than the quota only if the VMs exist on the hypervisor or are created outside the Horizon DaaS environment. This occurs only for Imported or Utility Desktop Model Quota mapped to the Imported, Recycle and Utility pools.
<b>date_updated</b>	2012-03-22 08:56:30.784	The last time this row was modified
<b>type</b>	PROTOCOL	Indicates the type of quota ( <b>DESKTOPMODEL, SESSION, PROTOCOL, TEMPLATE</b> )

## 4 Custom Branding

---

### 4.1 Introduction

If you have a custom branding scheme for Desktop Portal or Enterprise Center, you will need to check whether everything appears as expected after upgrading a tenant. There are a few areas to which you should pay particular attention due to VMware branding changes.

### 4.2 Desktop Portal

- Login page:

CSS selector: `#productNameInner`

You may need to adjust the margin-left property and/or decrease the font-size, for example :

`font-size: 14px;`

- Other pages:

You will likely need to make the same changes as for the login page. Additionally, you may need to adjust the background-position of the `#banner` selector:

`background-position: 0px 0px;`

### 4.3 Enterprise Center

- Login page:

CSS selector: `#productName`

There is a new element nested underneath with the ID `platformName`. Recommended changes:

- Make this the same color as `#productName`, if you have customized the text color
- Decrease the font sizes of both `#platformName` and `#productName`

- Other pages:

CSS selector: `#productName`

In addition to decreasing the font size, you may need to decrease the margin-left property, for example:

`margin-left: 110px;`

Alternatively, you can relatively position this element, for example:

```
position: relative;  
top: -5px;  
left: 100px;
```

CSS selector: `#topMenu`

You can also decrease or eliminate the `margin-left` property:

```
margin-left: 0;
```

CSS selector: `.loggedInUser`

You may need to decrease the `margin-top` property. Some custom brandings have this set to 25px, for instance. If the logged-in user display is shifted downwards or not visible, this margin may need to be decreased significantly, for example:

```
margin-top: -75px;
```

# 5 Database Failover

---

## 5.1 Overview

When the primary appliance fails, the secondary database is read-only. There are two procedures outlined below to address this situation:

- Enabling write operations on the secondary database
- Permanently promoting the secondary appliance to become the primary appliance

## 5.2 Enable Write Operations on the Secondary Database

The goal of this procedure is to switch the master database to the secondary appliance (tenant or service provider) in the event that the primary appliance is not available. The goal is to enable write operations so that the secondary appliance's database is the master datasource.

### Procedure

1. Stop the `dtService` on both the primary (if accessible) and the secondary appliance:  

```
sudo service dtService stop
```
2. Stop all slony daemons on both the primary (if accessible) and the secondary appliances:  

```
sudo killall slon
```
3. In the secondary appliance, connect to the `fdb` database and execute the following SQL command:  

```
fdb=# drop schema _slony cascade;
```
4. Repeat step 3 for the EDB if the appliance belongs to a tenant organization.
5. If the database on the primary appliance is still accessible, then backup the database, copy the database files and restore the database into the secondary appliance (for procedures, see [Backing Up and Restoring Databases](#)).
6. Open the file `/usr/local/desktopone/release/active/conf/fdb.properties` for edit and remove the IP address of the primary appliance.
7. Repeat step 6 for `/usr/local/desktopone/release/active/edb.properties` if the appliance belongs to a tenant organization.
8. Start `dtService` in the secondary appliance.

## 5.3 Promote the Secondary Appliance to Primary Appliance

To permanently promote the secondary appliance to be the primary appliance, you need to reinitialize slony as described in the [Slony Reinitialization](#) section of this document.

## 6 Datacenters

---

### 6.1 Failover a Datacenter

**Note:** The Service Center Portal may be unavailable for some steps during this process, make sure that you schedule the work at an appropriate time.

**Note:** Wait for all appliances to come online before beginning this procedure.

To failover a failed data center's primary node to a healthy data center's primary node, follow the procedure below.

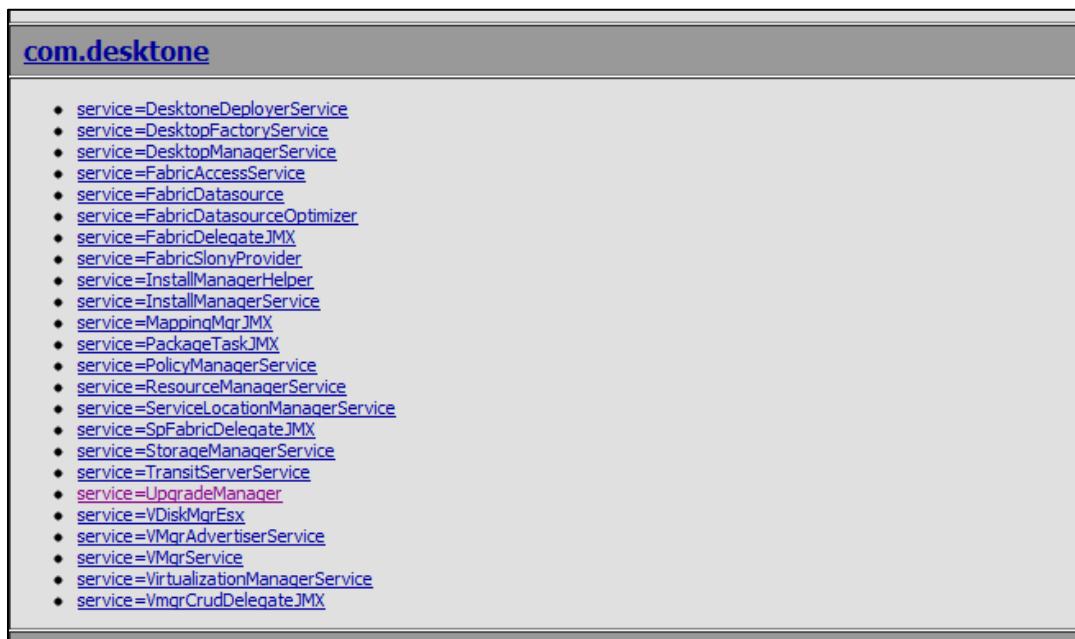
#### Procedure

1. Navigate to the dt-console of the service provider (<http://<Service Provider Appliance IP>/dt-console/>) and log in using the following credentials.

Username: jbossWSUser

Password: U6KqaP5E

2. Click the **service=UpgradeManager** link.



3. To failover the service provider's master database, invoke the **failoverDatacenter** method with the p1 set to 1000 (the org id of the service provider) and p2 set to the eth0 IP of the primary service provider appliance of the second datacenter.

Operation	Return Type	Description	Parameters
failoverDatacenter	boolean	failoverDatacenter	<p>p1 long (no description) 1000</p> <p>p2 java.lang.String (no description) 172.18.109.130</p> <p>Invoke</p>
upgradeAllOrmsSynchronously	boolean	upgradeAllOrmsSynchronously	[no parameters]

4. Restart the service provider appliances.
5. Find the org ids of each of the tenants that you want to failover by connecting to the service provider via ssh and executing the following:  

```
psql -U admin -d fdb -c 'select id, org_name from organization'
```
6. For each tenant, execute **failoverDatacenter** in the dt-console of the healthy service provider appliance as in step 3 with the appropriate org id and the eth1 IP (of the primary tenant appliance in the second datacenter).

**Note: To failover tenant datacenters, use the eth1 of the primary tenant appliance on the healthy datacenter and not eth0 as used for the service providers.**

Every execution of the failoverDatacenter should return true.

7. Restart dtService on the healthy datacenter's service provider appliances

## 6.2 Failback a Datacenter

**Note: The Service Center Portal may be unavailable for some steps during this process, make sure that you schedule the work at an appropriate time.**

To failback to a restored data center's primary node from a failover, follow the procedure below.

### Procedure

1. Stop the dtService on all appliances that belong to the organization, across all data centers:  

```
service dtService stop
```
2. Back up the fabric database from the current master node:  

```
/usr/local/deskstone/scripts/backupdb.sh -P '<database password>'
```

This creates a file called `<hostname>.<timestamp>.tar.gz` in the `/usr/local/deskstone/backup` folder.
3. SCP the backup file to the original master/primary node.
4. Extract the backup file:  

```
tar -zxvf <hostname>.<timestamp>.tar.gz
```
5. Restore the backup on this original master node.

**Note: do this once for each database type. This means you will do this twice for tenant appliances, the first time should be for the fdb, and the second time should be for the edb.**

```
env PGPASSWORD=<pswd> /usr/local/pgsql/bin/pg_restore -i -w -U admin -d <ft> -v --clean <fn>
```

where:

<pswd> = database password

<ft> = EDB or FDB (done for each for tenant appliances, or just once for service provider appliances)

<fn> = the path to the extracted file with respect to the <ft> parameter

6. Open a psql session to the fabric database on all service provider appliances:

```
psql -U admin fdb
```

7. Purge the \_slony schema for all databases (master and slave):

```
drop schema _slony cascade;
```

8. Exit from the psql session:

```
\q
```

9. If you are restoring service provider appliances, start the dtService on the original master database appliance (do not do this for tenant appliances):

```
service dtService start
```

10. Reinitialize the database cluster by performing the following steps.

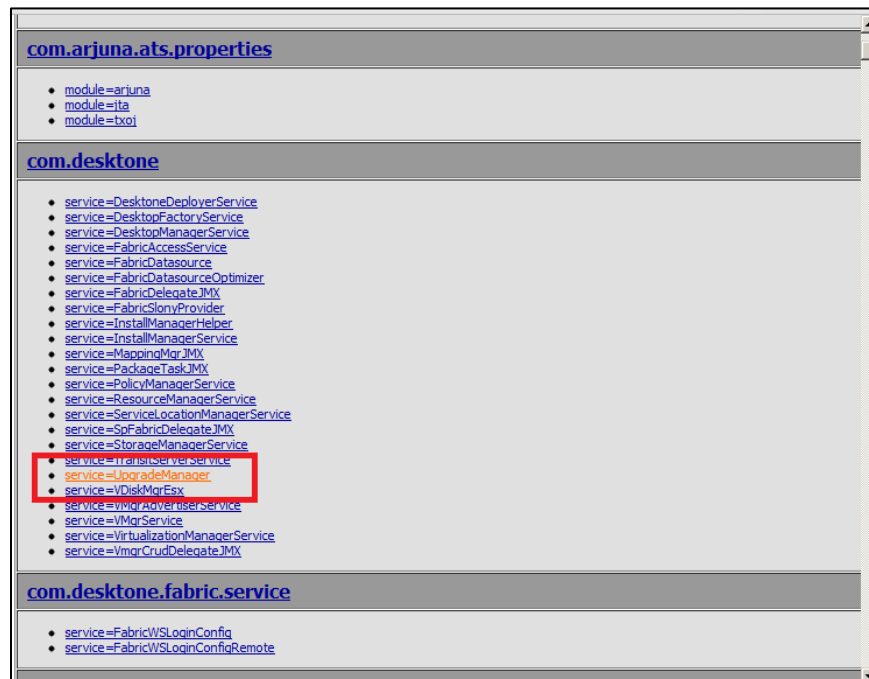
- a. Connect to the JMX console of the original master appliance with a web browser:

<https://<Service Provider Appliance IP>/dt-console>

Username: jmxUser

Password: U6KqaP5E

- b. Under com.desktone, click **service=UpgradeManager**



- c. Scroll to the **initSlonyForOrg** operation:

Operation	Return Type	Description	Parameters
<b>upgradeAllOrgs</b>	boolean	upgradeAllOrgs	[no parameters] Invoke
<b>upgradeOrgsSimultaneously</b>	java.lang.String	upgradeOrgsSimultaneously	p1 java.lang.String (no description) Invoke
<b>upgradeOrg</b>	boolean	upgradeOrg	p1 long (no description) Invoke
<b>upgradeAppliance</b>	boolean	upgradeAppliance	p1 java.lang.String (no description) p2 com.desktone.dataModel.ApplianceDTO (no description) p3 java.util.Set (no description) Invoke
<b>rollbackAppliance</b>	boolean	rollbackAppliance	p1 com.desktone.dataModel.ApplianceDTO (no description) Invoke
<b>initSlonyForOrg</b>	boolean	initSlonyForOrg	p1 long (no description) p2 java.lang.String (no description) p3 java.lang.String (no description) Invoke
<b>clearRunningSet</b>	boolean	clearRunningSet	[no parameters] Invoke
<b>main</b>	void	main	p1 [Ljava.lang.String; (no description) Invoke

- d. Enter the following parameter values:

p1: Enter the org ID, which is always **1000** for the service provider appliances.

p3: Enter **fabric** or **element**, depending on the database type you are reinitializing.

Operation	Return Type	Description	Parameters
<b>upgradeAllOrgs</b>	boolean	upgradeAllOrgs	[no parameters] Invoke
<b>upgradeOrgsSimultaneously</b>	java.lang.String	upgradeOrgsSimultaneously	p1 java.lang.String (no description) Invoke
<b>upgradeOrg</b>	boolean	upgradeOrg	p1 long (no description) Invoke
<b>upgradeAppliance</b>	boolean	upgradeAppliance	p1 java.lang.String (no description) p2 com.desktone.dataModel.ApplianceDTO (no description) p3 java.util.Set (no description) Invoke
<b>rollbackAppliance</b>	boolean	rollbackAppliance	p1 com.desktone.dataModel.ApplianceDTO (no description) Invoke
<b>initSlonyForOrg</b>	boolean	initSlonyForOrg	p1 long (no description) 1000 p2 java.lang.String (no description) p3 java.lang.String (no description) fabric Invoke
<b>clearRunningSet</b>	boolean	clearRunningSet	[no parameters] Invoke
<b>main</b>	void	main	p1 [Ljava.lang.String; (no description) Invoke

- e. Click **Invoke** to invoke the method. This will return “true” when successful.

11. Start **dtService** on all remaining appliances (including the master for a tenant restore):

```
service dtService start
```

## 6.3 Rename a Datacenter

### 6.3.1 Overview

When you bootstrap the primary service provider appliance, the bootstrap script (`bootstrap.sh`) prompts you to enter the name of the datacenter that hosts the service provider appliance.

If you subsequently add an additional datacenter, do not enter the name of the first datacenter when bootstrapping the primary service provider appliance for the new datacenter.

If you do inadvertently enter the wrong datacenter name, you will receive a FATAL message with a stack trace when the second stage of `bootstrap.sh` is run on the primary service provider appliance in the new datacenter. If this occurs, use the procedure described in this section to correct the datacenter name.

### 6.3.2 Edit `final_config.txt`

The bootstrap script saves the values you enter to a file named `final_config.txt` in the `/usr/local/desktop/scripts` directory. To correct a misnamed Datacenter, you need to edit `/usr/local/desktop/scripts/final_config.txt` on the new primary service provider appliance, using an editor such as `nano` or `vi`.

Here is an example of `final_config.txt`, with the **DataCenter Name** line highlighted:

```
DataCenter Name: JAPAN
Backbone VLAN ID: 3127
Hostname: bob-dc2-sp1
Eth1 IP: 169.254.215.8
Eth1 Netmask: 255.255.255.0
Backbone IP Block: 169.254.215.0/24
SP VLAN ID: 2109
Eth0 IP: 172.18.109.8
Eth0 Netmask: 255.255.255.0
Eth0 CIDR: 24
Gateway: 172.18.109.1
HA Transit Server IP: 169.254.215.9
Floating IP: 172.18.109.7
DataCenter UID: 60cb3d08-ddc5-4a5a-9102-d35a7fbf6f73
PSQL pass:
Nameserver: 172.18.109.2
DataCenter Master: False
Multi-DataCenter: True
NTP Server 1: ntp.ubuntu.com
Other Service Provider IP: 172.16.109.17
To change the name from JAPAN to India:
DataCenter Name: INDIA
```

### 6.3.3 Rerun `bootstrap.sh`

After updating the datacenter name and saving `final_config.txt`, rerun stage 2 of `bootstrap.sh` and continue with the rest of the installation.

## 6.4 Decommission a Datacenter

**Note:** All commands should be run with root credentials.

### 6.4.1 Execute Initial Shutdown Steps

#### Procedure

1. Take snapshots of all service provider and resource manager appliances.
2. Take snapshots of all tenant appliances for any Multi-DC system.
3. Shut down service provider, resource manager and tenant appliances in DC2 (target datacenter to be decommissioned).

### 6.4.2 Perform Initial Tenant Maintenance

Complete the following steps on the remaining datacenter for all affected tenants.

#### Procedure

1. Stop dtService on all tenant appliances:  

```
service dtService stop
```
1. Delete this file on all tenant appliances:  

```
/usr/local/desktonerelease/active/conf/proxy.conf
```
2. Terminate Slony Daemon Process on all tenant appliances:  

```
killall slon
```
3. Remove Slony Schema on all tenant appliances (both FDB and EDB):  

```
drop schema _slony cascade;
```
4. Remove DC2 IP addresses from this file, on the line starting "host=" :  

```
/usr/local/desktonerelease/active/conf/fdb.properties
```

### 6.4.3 Promote the Primary Service Provider and Tenant to be the Primary Across Datacenters

#### Procedure

1. Go to the psql prompt
2. Execute the following commands:
  - ```
update appliance set capabilities = 199 where name='<primarysp>'
```
  - ```
update appliance set capabilities = 240 where name='<primarytenant>'
```

## 6.4.4 Perform Initial Service Provider Maintenance on Remaining Datacenter

Perform the following steps on the remaining datacenter.

### Procedure

1. Stop dtService on all service provider appliances:  

```
service dtService stop
```
2. Stop dtService on all resource manager appliances:  

```
service dtService stop
```
3. Delete this file on all resource manager appliances if it exists:  

```
/usr/local/deskstone/release/active/conf/proxy.conf
```
4. Terminate Slony Daemon Process on all service provider appliances:  

```
killall slon
```
5. Remove Slony Schema on all service provider appliances (both FDB):  

```
drop schema _slony cascade;
```
6. Remove DC2 IP addresses from this file found on the service provider appliances, on the line starting "host=" :  

```
/usr/local/deskstone/release/active/conf/fdb.properties
```

## 6.4.5 Clean Up Proxychains Configuration

### Procedure

- Replace /etc/proxychains.conf with the clean version on all service provider, resource manager, and Multi-DC tenant appliances.

## 6.4.6 Clean Up FDB

All commands should be run on the primary node.

### Procedure

1. On the service provider appliance:  

```
select * from datacenter;
```
2. From the previous query results, select the ID associated with the datacenter to be decommissioned and run the following commands on service provider FDB:  

```
delete from billing_summary where datacenter_id='<prev_query_id>';  
delete from datacenter where id='<prev_query_id>;
```
3. Run the same query from step 2 on the tenant FDB that is being decommissioned.

## 6.4.7 Re-initialize Slony on Affected Nodes

### Procedure

1. Start slony daemons on service provider appliances:  
`/usr/local/desktop/scripts/start_slon_fdb.sh`
2. Start slony daemons on all affected tenant appliances:  
`/usr/local/desktop/scripts/start_slon_fdb.sh`  
`/usr/local/desktop/scripts/start_slon_edb.sh`
3. Restart memcached on service provider appliance:  
`service memcached restart`
4. Start dtService on Primary service provider node:  
`service dtService start`
5. Initialize FDB for service providers:  
`initSlonyForOrg(1000,<blank>,"fabric")`
6. Initialize FDB for all affected tenants:  
`initSlonyForOrg(orgId,<blank>,"fabric")`
7. Initialize EDB for all affected tenants:  
`initSlonyForOrg(orgId,remainingDCId,"element")`
8. Confirm slony table replication set is limited to 2 nodes on both tenant and service provider appliances (query should return 2 rows):  
`select * from _slony.sl_node;`

Slony should now be initialized correctly and the socks proxy configurations should be removed.

## 6.4.8 Bringing the System Up

### Procedure

1. Restart memcached on other service provider appliance (not primary):  
`service memcached restart`
2. Start dtService on other service provider appliance (not primary):  
`service dtService start`
3. Reboot the resource manager appliances:  
`reboot now`
4. Start dtService on tenant appliances:  
`service dtService start`
5. Confirm that customers can access their desktops on the affected tenant.
6. [optional] Attempt to expand a pool on the affected tenant.
7. Review Quota and Hypervisor Host Assignment on affected tenant.

## 6.4.9 Install New Root CA and Certificates on the Other Appliances

### Procedure

1. In the policy section of the service provider user interface, turn the hidden policy `appliance.ssl.validation.enable` to `false`, for both the service provider and tenants.
2. In the UpgradeManager section of dt-console execute the method (this will make the primary service provider the root CA):  
  
`installCA`
3. At the psql prompt of the service provider collect the appliance ID of the secondary service provider in this datacenter by using the query:  
  
`Select id from appliance where name='<secondary_sp_name>;`
4. In the InstallManagerService section of dt-console execute the `generateIntermediateCertificate` method for the secondary service provider appliance:  
  
`generateIntermediateCertificate('<appliance_id>')`
5. Repeat step 4 for the rest of the resource manager and tenant appliances in this datacenter
6. In the policy section of the service provider user interface, turn the hidden policy `appliance.ssl.validation.enable` to `true`, for both the service provider and tenants.
7. Restart `dtService` on all appliances in this datacenter.

## 6.4.10 Final Tasks

Once all systems appear to be functioning correctly:

- Delete the decommissioned datacenter's appliances.
- Delete the existing datacenter's appliance snapshots.

# 7 DtRAM Performance Test Setup

---

## 7.1 Performance Testing

### 7.1.1 Overview

This test is to test the performance of the dtRAM. It was found during testing that the real bottleneck is the Ethernet throughput. The throughput is directly related to the NIC capability and CPU. The other limiting factor is the number of states that the dtRAM sets up. For a normal connection through the dtRAM there are 2 states to establish a connection. The dtRAM is setup for 200,000 states.

### 7.1.2 Previous Results

#### 7.1.2.1 dtRAM ESX Setup

- 1 GB RAM
- 1 CPU
- e1000 NIC (Gb/s network)
- storage 8 GB configured

The memory was set to 1GB to have the install complete in a reasonable amount of time and to expedite power cycling of dtRAM. Less memory was used during testing.

#### 7.1.2.2 Results

- The test ran between 388 Mb/s – 425 Mb/s
- The end-point of the iperf server was on an external network
- The end-point of the iperf client was on an internal network.
- The worst case would be to have both on external networks.

#### **vSphere performance**

##### **Memory:**

During steady state 50 MB active was used.

Pfsense calculations are similar. Pfsense calculates 1 kbyte/per port and we use 2 ports per user.

**CPU:**

1.25 GHz (max) used during test.

**Storage:**

250 MB used

**Test Overview:**

Below is an explanation of all the pfctl commands used. The bold lines are the executed commands.

**Procedure**

1. Setup dtRAM with a tunnel between the dtRAM anchor and the RDP desktop. This is done with pf commands on the dtRAM. See "Setup tunnel on dtRAM" section.
2. Setup the simulated internal desktop. Iperf is set to server and port 3389 to mimic RDP. See "Internal Desktop" section.
3. Send traffic from the external desktop to the dtRAM tunnel. See "External Desktop" section.

**7.1.2.3 Set Up tunnel on dtRAM**

Below is an explanation of all the pfctl commands that we use. The bold lines are the executed commands.

These commands are performed on the dtRAM.

Initialize the anchors once on the dtRAM.

Setup a tunnel on the dtRAM using an anchor.

Once traffic is sent using the iperf commands below, the anchor should be flushed.

- **Initialization:**

```
/sbin/pfctl -s nat 2>/dev/null
```

This returns all the anchors. It is run the first time dtRAM is run.

The output needs to be parsed to retrieve the anchor.

- **Request of tunnel:**

\$ip = Windows VM IP

\$port = Remote desktop protocol (RDP 3389)

```
echo "rdr proto tcp -> $ip port $port" > tunnel.txt
```

\$anchor = name of anchor found in initialization call. Freetrial has 59 anchors.

An example would be "dtRAM.8001".

```
/sbin/pfctl -a $anchor -f - < tunnel.txt
```

- **Flush anchor:**

After several seconds of sending the RDP file to the user flush the port.

\$anchor - Anchor that you want to close. In the above example "dtRAM.8001"

```
/sbin/pfctl -a $anchor -F nat 2>&1
```

#### 7.1.2.4 Internal Desktop

This desktop would mimic a remotely connect desktop. Create a VM that uses Linux. Apt-get install iperf on this desktop.

To mimic RDP run the following command:

```
iperf -s -p 3389
```

#### 7.1.2.5 External Desktop

This desktop would mimic a desktop that connects to the dtRAM. Create a VM that uses Linux, and create this vm on an external network that is not part of the dtRAM network. Apt-get install iperf on this desktop.

```
iperf -c <ip address of dtRAM carp addresses> -p <port of anchor>
```

**Note: For the above anchor “dtram.8001”, this would be port 8001.**

Once the above command is executed traffic will be sent to the internal desktop. The throughput will be calculated and displayed by the iperf command.

## 7.2 Troubleshooting and Diagnosis

### 7.2.1 Summary

This section explains how to diagnose problems and make sure that the dtRAM is running properly after it is installed.

### 7.2.2 dtRAM Configuration

The commands in the following sections help to confirm that the dtRAM software is working properly and that the dtRAM machines are properly connected to the network.

#### 7.2.2.1 Location of dtRAMs

The virtual dtRAMs are on the IPv4 network:

```
qadtram71-us# ifconfig em1
em1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=19b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, TS04>
    ether 00:30:48:bd:ac:39
    inet 169.254.204.9 netmask 0xffffffff00 broadcast 169.254.204.255
    inet6 fdf8:c879:493e:1:230:48ff:febd:ac39 prefixlen 64 autoconf
```

```
qadtram72-us# ifconfig em1
em1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=19b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, TS04>
    ether 00:30:48:bf:d4:43
    inet 169.254.204.10 netmask 0xffffffff00 broadcast 169.254.204.255
    inet6 fdf8:c879:493e:1:230:48ff:febf:d443 prefixlen 64 autoconf
```

### 7.2.2.2 Check dtRAM Status

Make sure the dtRAM daemon is running on both dtRAM nodes:

```
qadtram71-us # ps ax|grep lighty-dtram
926 ?? I      8:06.32 /usr/local/sbin/lighttpd -f /var/etc/lighty-dtram.conf
qadtram72-us # ps ax|grep lighty-dtram
957 ?? I     11:56.12 /usr/local/sbin/lighttpd -f /var/etc/lighty-dtram.conf
```

### 7.2.2.3 Start and Stop Process

To stop the dtRAM process:

```
kill <process id found in command above>
```

To start the dtRAM process after stopping:

```
/usr/local/sbin/lighttpd -f /var/etc/lighty-dtram.conf
```

### 7.2.2.4 Verify CARP Master and Backup

At any given time, one dtRAM will be the MASTER and one will be the BACKUP. Check the carp0 interface to confirm this:

```
qadtram71-us # ifconfig vip1
carp0: flags=49<UP,LOOPBACK,RUNNING> metric 0 mtu 1500
inet 172.16.115.254 netmask 0xffffffff00
carp: MASTER vhid 1 advbase 1 advskew 0
qadtram72-us # ifconfig vip1
carp0: flags=49<UP,LOOPBACK,RUNNING> metric 0 mtu 1500
inet 172.16.115.254 netmask 0xffffffff00
carp: BACKUP vhid 1 advbase 1 advskew 0
```

### 7.2.2.5 Test External Connectivity to the dtRAM Using Telnet and Tcpdump

The master dtRAM will be listening on a range of ports that you specified when you installed the dtRAM software (for example, 8001-8010). You can find the defined port range in /tmp/rules.debug. To make sure the NAT address for the dtRAM is connected to the dtRAM, you can attempt to telnet to that address and make sure you're receiving the request on the master dtRAM:

First, on the master dtRAM, use tcpdump to listen to a range of ports that includes the range defined in /tmp/rules.debug. For example,

```
qadtram71-us# tcpdump -i em0 portrange 8001-8020
```

From another machine, such as the service provider appliance, attempt to telnet to the NAT address for the dtRAM and specify a port. For example:

```
desktone@us-sp:/usr/local/desktone$ telnet 67.110.143.140 8001
Trying 67.110.143.140...
telnet: Unable to connect to remote host: Connection refused
desktone@us-sp:/usr/local/desktone$ telnet 67.110.143.140 8010
Trying 67.110.143.140...
telnet: Unable to connect to remote host: Connection refused
desktone@us-sp:/usr/local/desktone$ telnet 67.110.143.140 8020
Trying 67.110.143.140...
```

Note that the last request (on port 8020) hangs, as the dtRAM is not accepting communication on this port.

The 'connection refused' messages in response to the telnet commands indicate that the dtRAM was listening on that port.

On the dtRAM (MASTER), the request is received, indicating that the NAT address is connected to the em0 interface on the master dtRAM:

```
qadtram71-us# tcpdump -i em0 portrange 8001-8020
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em0, link-type EN10MB (Ethernet), capture size 96 bytes
08:59:55.041960 IP 67.110.143.130.60506 > 172.16.115.254.8001: S 326757097:326757097(0)
win 5840
08:59:55.041968 IP 172.16.115.254.8001 > 67.110.143.130.60506: R 0:0(0) ack 326757098
win 0
09:00:01.709755 IP 67.110.143.130.60206 > 172.16.115.254.8010: S 421429074:421429074(0)
win 5840
09:00:01.709762 IP 172.16.115.254.8010 > 67.110.143.130.60206: R 0:0(0) ack 421429075
win 0
## Note that the last request (on port 8020), does not show up, as the dtRAM is not
accepting communication on this port.
```

### 7.2.2.6 Test Tenant Appliance Connectivity to the dtRAM

From one of the tenant appliances (must be in the IP address range specified during dtRAM installation), check that you can retrieve the WSDL (web services description language) file from the dtRAM. If you need to check the range, look for this line in /tmp/rules.debug, which specifies either a list of tenant appliance IP address or a CIDR range of tenant appliance IP addresses. For example:

```
elementNetworks="{172.16.115.0/24}"
```

In this example, the dtRAM will accept WSDL requests from tenant appliances in the CIDR range 172.16.115.0/24.

To find the IP address of the tenant appliance, perform the following steps.

#### Procedure

1. On the service provider appliance, select **tenant ► browse tenants**.
2. For each tenant appliance:
  - a. Click **Edit**.
  - b. Click the **Appliances** tab.
  - c. Click the **Details** link.
  - d. The IP address you need has Adapter Name eth0.

**Note that both of the tenant network addresses are in the specified CIDR range, 172.16.115.0/24.**

To check the WSDL from the tenant appliance, ssh to the tenant appliance from the service provider appliance, then use the curl command from the tenant appliance command line.

- dtRAM requires credentials from tenant appliance
- The dtRAM expects a username and password from the tenant appliance before it will give out the WSDL file. These credentials are embedded in the tenant appliance software, but if you are connecting directly using curl or wget, you will need to include them in your command line as shown below.

```
curl --user ramservice:eVxJ95a
http://172.16.115.254:8000/core/services/RAMService?WSDL
wget --user=ramservice --password=eVxJ95a
http://172.16.115.254:8000/core/services/RAMService?WSDL
```

```
root@eutb5:~# curl --user ramservice:eVxJ95a
http://172.16.115.254:8000/core/services/RAMService?WSDL
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions targetNamespace="http://www.desktone.com/RAMService"
```

```

.
.
.
</wsdl:service>
</wsdl:definitions>

```

If you do not get a WSDL file from a tenant appliance that is in the dtRAM's specified range, then the dtRAM is not working properly.

## 7.2.3 dtRAM Operation

Once you are sure that the dtRAM itself is working well, you can try it using the Service Center, Enterprise Center, and User Portal. For information about configuring dtRAM from the Service Center for a particular tenant, see the Horizon DaaS Platform 5.0 Blueprint.

After you have configured the dtRAM, you can map a pool or a virtual desktop to a user and then attempt to connect to that pool or desktop from outside the tenant network.

The following procedures confirm that the dtRAM actually works to connect an external user to a mapped virtual desktop.

### 7.2.3.1 Check for Proper dtRAM Operation

Follow these steps to verify that the dtRAM is operating properly.

#### Procedure

1. Login to the User Portal for the tenant whose dtRAM you want to test. You must log in from a machine that is outside the tenant network (not on the list of internal networks for that tenant). Do not check the box to automatically log in to your default desktop.

2. To monitor the lighttpd web service:

```
cd /var/log/
clog lighttpddttram.error.log
```

3. To monitor the dttram:

```
clog dttram.log
```

4. To monitor tunnel creation and flushing:

```
clog filter.log
```

5. To watch connections get assigned:

```
cd /var/db/
tail -f dttram.db
```

6. If you receive an RDP file on the User Portal machine, do not click Connect yet. First, on the master dtRAM, execute the following tcpdump command (using the port from the initial dtRAM connection):

```
qadtram71-us# tcpdump -i em0 port 3389 or port 8002
```

7. On the User Portal machine, click Connect on the RDP file.

8. On the master dtRAM, tcpdump output similar to the following indicates that the dtRAM is properly passing packets between the end-client device and the virtual desktop. In particular, the first highlighted IP address is the carp0 address of the dtRAM, including the port the dtRAM is using to establish that connection. The second highlighted IP address is the virtual desktop RDP connection.

```
qadtram71-us# tcpdump -i em0 port 3389 or port 8002
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em0, link-type EN10MB (Ethernet), capture size 96 bytes
```

```

10:51:41.936030 IP 67.110.143.130.57778 > 172.16.115.254.8002 : S
2719116191:2719116191(0) win 64512 <mss 1460,nop,nop,sackOK>
10:51:41.936075 IP 172.16.115.254.52244 > 172.16.115.102.rdp : S
2719116191:2719116191(0) win 64512 <mss 1460,nop,nop,sackOK>
10:51:41.936397 IP 172.16.115.102.rdp > 172.16.115.254.52244: S
3750291169:3750291169(0) ack 2719116192 win 64240 <mss 1460,nop,nop,sackOK>
10:51:41.936413 IP 172.16.115.254.8002 > 67.110.143.130.57778: S
3750291169:3750291169(0) ack 2719116192 win 64240 <mss 1460,nop,nop,sackOK>
10:51:41.938146 IP 67.110.143.130.57778 > 172.16.115.254.8002: . ack 1 win 64512
10:51:41.938157 IP 172.16.115.254.52244 > 172.16.115.102.rdp: . ack 1 win 64512
10:51:41.938645 IP 67.110.143.130.57778 > 172.16.115.254.8002: P 1:48(47) ack 1
win 64512
10:51:41.938651 IP 172.16.115.254.52244 > 172.16.115.102.rdp: P 1:48(47) ack 1 win
64512
10:51:42.050834 IP 172.16.115.102.rdp > 172.16.115.254.52244: P 1:12(11) ack 48
win 64193
10:51:42.050855 IP 172.16.115.254.8002 > 67.110.143.130.57778: P 1:12(11) ack 48
win 64193
10:51:42.054203 IP 67.110.143.130.57778 > 172.16.115.254.8002: P 48:476(428) ack
12 win 64501
10:51:42.054210 IP 172.16.115.254.52244 > 172.16.115.102.rdp: P 48:476(428) ack 12
win 64501

```

### 7.2.3.2 Configuration Files of Interest

Make any FreeBSD, firewall rules, or dtRAM configuration changes in this file:

/conf/config.xml

View dtRAM configurations in this file

/usr/local/dttram/config.xml

View firewall rules in this file:

/tmp/rules.debug

### 7.2.3.3 Making the Remote Connection

If you still cannot connect to the virtual desktop remotely from the User Portal, there might be a problem with the virtual desktop configuration.

### 7.2.3.4 Data Encryption Problem

If after clicking Connect on the RDP file, the connection fails reporting that there is a data encryption problem, there might be an issue with the certificate for terminal services on the VM. Complete the following steps on the VM.

#### Procedure

1. Run regedit and delete the certificate from:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\Parameters
2. Reboot the VM.
3. Try connecting to the pool or VM again through the dtRAM.

## 8 Gold Patterns

---

### 8.1 Creating a Linux Gold Pattern

#### 8.1.1 Overview

There are two tasks you must perform in order to create a Linux gold pattern:

- Prepare the Linux desktop
- Install the Linux Python DaaS Agent

**Note:** The following process has been tested with Ubuntu, although it may work with other distributions as well.

#### 8.1.2 Prepare the Linux Desktop

##### Procedure

1. Create a VM with Linux OS.
2. Install VMwareTools as described in the [VMware Knowledge Base](#).
3. Enable SSH on the desktop:
  - a. Execute command:  

```
sudo apt-get install openssh-server openssh-client
```
  - b. Check the configuration file `/etc/ssh/sshd_config`. The Port should be set for 22; if it is not, set it for 22 and re-start the SSH service.
4. Install and configure [NoMachine](#) version 3.x for NX.

#### 8.1.3 Install the Linux Python DaaS Agent

Before you begin the installation process, note the following:

- The Linux Python DaaS Agent debian package requires OpenSSL version 0.9.8 or higher. If OpenSSL is not installed, the Agent package will attempt to install it.
- The internal package name is **dt-python-linux-agent**
- The daemon service is **dtDaemon**, which has the following start/stop/status commands.
  - `sudo initctl start dtDaemon`

- `sudo initctl stop dtDaemon`
- `sudo initctl status dtDaemon`
- The installation directory is **/home/desktop/dtDaemon/** directory
- Default log directory is **/var/log/sealListener.log**

The steps below show examples of the commands to enter as well as the code returned by the system.

#### Procedure

1. Download latest Linux Python DaaS Agent from the VMware website.
2. Execute the installation command.

**Note: The installation process automatically creates 'desktop' user account and prompts you to create a password. This user is used for the customization process.**

```
sudo dpkg -i dt-python-linux-agent-6.1.0_i386.deb
```

```
desktop@AshLinux32 ~ $ sudo dpkg -i dt-python-linux-agent-6.1.0_i386.deb
Selecting previously unselected package dt-python-linux-agent.
(Reading database ... 169845 files and directories currently installed.)
Unpacking dt-python-linux-agent (from dt-python-linux-agent-6.1.0_i386.deb) ...
This is Pre Install script
Creating desktop user
useradd: user 'desktop' already exists
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Setting up dt-python-linux-agent (6.1.0) ...
This is Post Install script
Copying config Files.
Finished Copying config Files.
Starting daemon.
dtDaemon start/running, process 2813
Finished installation
```

## 8.1.4 Remove and Purge the Linux Python DaaS Agent Package

### 8.1.4.1 Remove the Package

#### Procedure

- Enter the following:

```
desktop@AshLinux32 ~ $ sudo dpkg -r dt-python-linux-agent
```

Example of output:

```
[sudo] password for desktop:
(Reading database ... 169853 files and directories currently installed.)
Removing dt-python-linux-agent ...
This is Pre Remove script
Stopping daemon...
dtDaemon stop/waiting
Deleting files from dtDaemon directory...
This is Post Remove script
Removing daemon configuration file..
Finished post installation script execution.
```

### 8.1.4.2 Purge the Package

#### Procedure

- Enter the following:

```
desktopone@AshLinux32 ~ $ sudo dpkg -P dt-python-linux-agent
```

Example of output:

```
(Reading database ... 169853 files and directories currently installed.)
Removing dt-python-linux-agent ...
This is Pre Remove script
Stopping daemon...
dtDaemon stop/waiting
Deleting files from dtDaemon directory...
This is Post Remove script
Removing daemon configuration file..
Finished post installation script execution.
Purging configuration files for dt-python-linux-agent ...
This is Post Remove script
Removing daemon configuration file..
rm: cannot remove `/etc/dtDaemon.conf': No such file or directory
rm: cannot remove `/etc/init/dtDaemon.conf': No such file or directory
Finished post installation script execution.
dpkg: warning: while removing dt-python-linux-agent, directory '/home/desktopone'
not empty so not removed.
```

## 8.2 Enable Post-Sysprep Commands

Perform these steps on the image before converting it to a gold pattern.

#### Procedure

1. Create a folder named **sysprep** under C:\ **driver**.
2. Create a batch file named **postprep-extra.bat** in the **sysprep** folder.
3. Add required commands in batch file and save it.
4. Convert the desktop to a gold pattern.

File path : c:\sysprep\postprep-extra.bat

Sysprep launches this batch file during specialize pass execution (before agent comes and joins the domain).

To set the post sysprep batch file in the template before converting to a gold pattern (executed before domain join), perform the following steps.

#### Procedure

1. Create a batch:  
c:\sysprep\postprep-extra.bat
2. Create the C:\Sysprep\.... folder structure:  
For Windows XP template: C:\Sysprep\i386\%\$OEM%\ postprep-extra.bat  
For Windows Vista /7: C:\Sysprep\ postprep-extra.bat
3. Save it with your commands.

Sysprep executes this batch file in post execution.

# 9 Monitoring

---

## 9.1 Introduction

This section describes basic monitoring of the Horizon DaaS environment. It also provides links to more detailed information about Horizon DaaS CIM providers and information about connectivity and ports.

The intent of this section is to provide information on the major items that should be monitored in the Horizon DaaS environment. At this time VMware does not have preference for the monitoring tool to be used, and the choice is left to the provider. Therefore the methods of implementation will depend upon the monitoring tool selected.

### 9.1.1 Critical Nodes

There are several nodes that are critical to proper functioning in a Horizon DaaS environment. In many cases the Horizon DaaS software is able to "self-heal". However, any impairment to these nodes should still be noted and potential action taken regardless of the Horizon DaaS software capability to "self-heal". Providing feedback on these occurrences is also important to improving the quality of the Horizon DaaS software. The nodes (whether iron or virtual) that should be actively monitored are listed below. Some of these are Horizon DaaS appliances and some are not. More details of the items that can be monitored are outlined later in this section.

Service provider nodes:

- Active Directory
- ESX hosts
- Load balancer
- NFS server
- Network routers
- Time server

Horizon DaaS nodes:

- Service Provider
- Tenant
- Resource Manager

## 9.1.2 Basic System Functions

For each of the nodes listed under "Critical Nodes", these basic functions should be monitored:

- File system space
- CPU usage
- Memory usage

The method of monitoring this information will vary depending upon the OS being monitored and the monitoring software itself. Please consult your monitoring software documentation for details.

## 9.2 Web Application Monitoring

Basic verification of a Horizon DaaS installation includes connecting to the following web pages (both through a load balancer, if applicable, and directly to each node):

- Desktop Portal
- Enterprise Center
- Service Center

### 9.2.1 Port Response

In addition to using ping, monitoring software can check response of specific ports - that is, if they respond to an "open socket" request. DNS and DHCP are exceptions which use UDP, and may require more intelligent monitoring.

### 9.2.2 Monitoring CIM Classes

Horizon DaaS management nodes run a variety of CIM classes that provide information about system operation. See CIM Providers on Horizon DaaS Management Nodes for more details.

## 9.3 CIM Providers on Horizon DaaS Management Nodes

This chapter describes the CIM providers that monitor a Horizon DaaS installation. Key properties for monitoring are **highlighted** in the descriptions below.

### 9.3.1 Operating Environment CIM Providers for Horizon DaaS Nodes

These CIM providers report on the operating environment for Horizon DaaS management nodes. They should be monitored on all Horizon DaaS nodes:

- Linux\_OperatingSystem
- Linux\_EthernetPort
- Linux\_ComputerSystem
- CIM\_FileSystem

### 9.3.1.1 Linux\_OperatingSystem

#### Description

There will only be a single instance of this class per appliance.

#### Properties

- **FreePhysicalMemory**: If this reaches 0 that is a critical fault and needs to be resolved immediately . (see the calculation below).
- **FreeVirtualMemory**: If this reaches 0 0 that is a critical fault and needs to be resolved immediately (see the calculation below).
- **HealthState**: Anything but a value of 5 indicates a problem.
- **OperationalStatus**: Anything but a value of 2 (OK) indicates a problem. However, an occasional value of 4 (stressed) may appear. If repeated samplings indicate a value other than 2, you should raise an alert.
- **TotalVirtualMemorySize**: The total amount of swap space available to the system.

#### Calculations

- **PercentSwapUsed**:  $(100 * \text{TotalVirtualMemorySize} - \text{FreeVirtualMemory}) / \text{TotalVirtualMemorySize}$ .
- It is useful to monitor for swap space usage. Once the system begins using swap space, performance will degrade. The free memory alert should be triggered prior to the system using swap space so the use of swap should be considered a serious problem.

#### Mitigation

Recommendation is to warn if PercentSwapUsed > 5% and alert if PercentSwapUsed > 20%.

If the memory used reaches high levels, you should check to see if there are any memory-intensive processes that need to be restarted using top and shift-M on the node in question:

```
$ top
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
6816	root	20	0	2069m	389m	13m	S	0.0	19.6	3:36.97	java
6634	root	20	0	755m	84m	9.8m	S	0.0	4.2	1:21.70	java
...											

If no single application appears to be the culprit, restart the node.

### 9.3.1.2 Linux\_EthernetPort

#### Description

There will typically be two instances of this class, one for the eth0 interface (tenant or service-provider network) and one for the eth1 (management backbone) interface.

#### Properties

- **EnabledState**: Anything but the value 2 is a problem.
- **Status**: Anything but OK is a problem.

## Mitigation

If the eth0 status is not OK, then use `ifconfig` to check that the interfaces are up and have an IP address. You should also be able to ping the IPv4 gateway for each node.

If the eth1 status is not OK, then try to connect to that appliance via `ssh` from the transit server. If this works, then the eth1 interface is OK.

### 9.3.1.3 Linux\_ComputerSystem

#### Description

There will only be a single instance of this class per appliance.

#### Properties

- **EnabledState**: Anything but a value of **2** indicates an issue.

#### Mitigation

If EnabledState is anything but **2**, attempt to ping the node, `ssh` to the node, and check the status of the `dtService` (`service dtService status`) on the node.

### 9.3.1.4 CIM\_FileSystem

#### Description

There are several subclasses of this. (You can also check the `CIM_LocalFileSystem` class if you don't want to view remote file systems.) The most important to focus on are all the `Linux_Ext4FileSystem` instances. In addition to the root file system, there may be others that are important to check that they are not in `ReadOnly` mode. Currently you should check these file systems:

- `/` (root)
- `/boot`
- `/data`
- `/tmp`
- `/usr/local`
- `/var`

Additionally on the resource manager nodes and the DB nodes there will be some number of `Linux_NFS` instances. These are remotely mounted file systems. You can choose to monitor these mounts via our appliances or an alternate mechanism based on the storage system.

#### Properties

- **EnabledState**: Any value other than **2** (enabled) on a remotely mounted NFS file system is cause for alarm. However, local file systems in management nodes may show up with an EnabledState of **3**.
- **ReadOnly**: This value should be `FALSE`. A value of `TRUE` is cause for alarm. If the `CIM_FileSystem` class does not respond for a particular file system, the file system may be read-only and you should restart the node. Contact Horizon DaaS support if the restart fails.
- **Status**: Any value other than `OK` is cause for alarm.

Go to the node and use `mount` to check that the file system is mounted. If the file system is mounted, try to create a file.

- **PercentageSpaceUsed**: Displays percent of available disk space that is used. Recommendation is to warn at 70% and then increase the alert priority in 10% increments (that is, 70, 80, 90).

## Mitigation

If any of the file systems report high usage, please contact Horizon DaaS support for corrective action.

## 9.3.2 Application-Specific CIM Providers for Horizon DaaS Management Appliances

Note: For non-Horizon DaaS-specific CIM provider classes, see [Operating Environment CIM Providers for Horizon DaaS Nodes](#).

### 9.3.2.1 Service Provider Appliances

The CIM providers for service provider appliances are as follows:

- Desktonet\_ApplicationServer
- Desktonet\_ApplicationServerStatistics
- Desktonet\_InstalledProduct
- Desktonet\_CommonDatabase
- Desktonet\_DatabaseService
- Desktonet\_DatabaseReplicationService
- Desktonet\_ActiveDirectoryStatus
- Desktonet\_HypervisorManagerStatus
- Desktonet\_NTPTService

### 9.3.2.2 Resource Manager Appliances

The CIM providers for Horizon DaaS resource manager nodes are as follows:

- Desktonet\_ApplicationServer
- Desktonet\_ApplicationServerStatistics
- Desktonet\_InstalledProduct
- Desktonet\_NTPTService

### 9.3.2.3 Tenant Appliances

The CIM providers for tenant appliances are as follows:

- Desktonet\_ApplicationServer
- Desktonet\_ApplicationServerStatistics
- Desktonet\_InstalledProduct
- Desktonet\_CommonDatabase
- Desktonet\_DatabaseService
- Desktonet\_DatabaseReplicationService
- Desktonet\_RemoteAccessManagerStatistics

- Deskstone\_ActiveDirectoryStatus
- Deskstone\_NTPTService

#### 9.3.2.4 Desktop Manager Appliances

- The CIM providers for Desktop Manager appliances are as follows:
- Deskstone\_ApplicationServer
- Deskstone\_ApplicationServerStatistics
- Deskstone\_InstalledProduct
- Deskstone\_CommonDatabase
- Deskstone\_DatabaseService
- Deskstone\_DatabaseReplicationService
- Deskstone\_NTPTService

### 9.3.3 Description of Horizon DaaS CIM Providers

#### 9.3.3.1 Deskstone\_CommonDatabase

##### Description

Describes the PostgreSQL server running on database nodes.

##### Properties

- InstanceID: Key to uniquely identify the instance of this class. Set to Deskstone\_hostName\_postgreSQL.
- HomeDirectory: Home directory of the PostgreSQL service.
- DataDirectory: Data directory of the PostgreSQL service.
- DatabaseVersion: Version number of the database.
- **MaxConnections**: Maximum number of connections that the PostgreSQL server can manage concurrently. The value is extracted from the PostgreSQL configuration file from the parameter "max\_connections".
- **Status**: Indicates the current status of the PostgreSQL server. OK indicates PostgreSQL is running. STOPPED indicates that the database is stopped. If the database is down (status STOPPED), any other data provided should be ignored.
- ListenAddress: The port and ip address on which postmaster process is listening for new connections.

##### Calculations

- **Percent maximum connections used**: You should total up the ActiveConnections used by each database instance on the server (see Deskstone\_DatabaseService provider) and divide by the MaxConnections from this class to determine the load on the database server. That is:  

$$100 * (\text{Sum}(\text{ActiveConnections}) / \text{MaxConnections})$$

##### Mitigation

If the database is stopped, check the database server:

```
$ service postgresql status
```

If PostgreSQL is not running, start the service, then run the status command again:

```
$ service postgresql start
$ service postgresql status
```

If the database will not start, examine the PostgreSQL logs and contact Horizon DaaS support.

The recommendation is to warn at 80%, critical at 90% of Percent maximum connections used.

If the percent maximum connections reaches the critical level, you should examine the database server to determine which cache node or nodes is consuming a large number of connections (5-10 connections is the normal range for a cache node):

```
$ netstat -an | grep 5432
```

### 9.3.3.2 Desktone\_DatabaseService

#### Description

Specifies the details of database instances running on DaaS appliances. In the Horizon DaaS Platform, appliances have one or more database instances running, as follows:

- Service provider appliances - FDB only
- Tenant appliances - both FDB and EDB
- Desktop manager appliances - EDB only

#### Properties

- Name: Unique identification of the service. Set to hostName\_DBInstanceName. For rollback purposes, upgrades will create a db name\_version instance. You do not need to monitor the database instances that have the version appended.
- **ActiveConnections**: Specifies the number of active connections to this database instance at the time of sampling/monitoring. See the calculation for Desktone\_CommonDatabase using this number totaled across all database instances on a server compared to the maximum connections permitted on a single database server.

### 9.3.3.3 Desktone\_DatabaseReplicationService

#### Description

Provides information about database instances that are replicated. This provider runs on all Fabric database servers. In the Horizon DaaS Platform, appliances have one or more database instances running, as follows:

- Service provider appliances - Fabric Database (FDB) only
- Tenant appliances - both Fabric Database (FDB) and Element Database (EDB)
- Desktop manager appliances - Element Database (EDB) only

#### Properties

- SystemCreationClassName: Name of the class used to create the database instance.
- SystemName: Name of the system on which the database instance is running. Set to host name in our case.
- CreationClassName: Name of the class used to create the database instance.
- Name: Unique identification of the service. Set to hostName\_databaseInstanceName.
- NodeID: Represents the UID of the node in the context of the replication system.

- **Role:** Indication of whether the database instance is master or slave instance.
- **SyncStatus:** Synchronization status applies to the slave instance only. This property does not have any significance in case of master instance. For a slave instance, the SyncStatus value will be the number of milliseconds since the last synchronization. For example, SyncStatus = 1200 means that the last successful sync was 1.2 seconds before. Warn if the SyncStatus is more than 40 seconds old. Critical if SyncStatus is more than 2 minutes old.
- **Status:** Indicates the current status of the replication service. OK indicates the replication service is running. STOPPED indicates that the replication service is stopped. The replication service should be running for all database instances in use.

### Mitigation

If replication is stopped (or if the SyncStatus is out of date), you should check that the replication daemon (slony) is running properly on the database server:

```
$ ps -ef | grep db.conf
root 1062      1  0 Sep17 ? 00:00:00 /usr/local/pgsql/bin/slony -f
/usr/local/desktopone/release/static/conf/slony_edb.conf
root 1121      1  0 Sep17 ? 00:00:00 /usr/local/pgsql/bin/slony -f
/usr/local/desktopone/release/static/conf/slony_fdb.conf
root 1443 1062  0 Sep17 ? 00:07:39 /usr/local/pgsql/bin/slony -f
/usr/local/desktopone/release/static/conf/slony_edb.conf
root 1446 1121  0 Sep17 ? 00:06:01 /usr/local/pgsql/bin/slony -f
/usr/local/desktopone/release/static/conf/slony_fdb.conf
```

There should be 2 processes for each database instance. If replication is not running properly for any of the instances, you can restart replication:

```
$ nohup /usr/local/pgsql/bin/slony -f
/usr/local/desktopone/release/static/conf/slony_fdb.conf >/dev/null 2>&1 &
$ nohup /usr/local/pgsql/bin/slony -f
/usr/local/desktopone/release/static/conf/slony_edb.conf >/dev/null 2>&1 &
```

### 9.3.3.4 Desktopone\_InstalledProduct

#### Description

Provides information about the Horizon DaaS software, including the version and build number.

#### Properties

- ProductIdentifyingNumber: Product identification. This property contains build information.
- ProductName: Product's commonly used name. Set to "Virtual-D."
- ProductVendor: Vendor's name: Desktopone.
- ProductVersion: Product version information
- SystemID: Host name where the product is installed.

### 9.3.3.5 Desktopone\_ApplicationServer

#### Description

Provides information about the application server used by the Horizon DaaS software.

#### Properties

- Name: Name by which the application server is identified. Set to "Jboss" for Element manager and Resource manager.

- **SoftwareElementID**: Identifier for software element to be used in conjunction with other keys to uniquely identify the element. Set to host name on which the application server is running.
- **Version**: Version of the application server.
- **SoftwareElementState**: This property defines the various states of software element's life cycle. For example: Running, Executable, Deployable etc. A SoftwareElementState of 3 indicates that the application server is running.

#### Mitigation

If the application server is not running, go to the node in question and check the status:

```
$ service dtService status
Deskton Service is running under PID 6761
```

If the Deskton Service is not running, start it (and watch the log file):

```
$ service dtService start
```

- **TargetOperatingSystem**: Specifies the node's operating system environment. Set to 36 (LINUX).

### 9.3.3.6 Deskton\_ApplicationServerStatistics

#### Description

There will be a single instance of this class for all of the application appliances (that is, this will not be present in DB appliances).

#### Properties

These properties report on operations of the JVM (Java virtual machine) used for the Horizon DaaS application.

- **InstanceID**: Key to uniquely identify the instance of this class. Set to DesktonHostName\_Jboss.
- **ThreadCount**: Total number of threads running during the monitoring sample.
- **ThreadGroupCount**: Total number of thread groups that exist during the sample time.
- **HeapSize**: Current size of heap memory
- **MaxHeapSize**: Maximum heap memory allowed on the application server.
- **Uptime**: The length of time the application server has been running in milliseconds.

#### Calculations

- **Heap size used**:  $100 * \text{HeapSize} / \text{MaxHeapSize}$ . Recommendation is to warn at 85% and then increase the alert priority in 5% increments (that is, 90, 95, 100).

#### Mitigation

At 85%, schedule a restart of the dtService. At 90% or higher, restart the dtService immediately:

```
$ service dtService restart
```

If the heap memory used increases to high levels often (more than once per week), you should analyze your environment in concert with Horizon DaaS support.

### 9.3.3.7 DesktoneremoteAccessManagerStatistics

#### Description

Reports on the status of the dtRAM service on a tenant node. Note that this CIM provider actually runs on a tenant node, not on the dtRAM itself.

#### Properties

- InstanceID: Key to uniquely identify the instance of this class. Set to DesktoneremoteAccessManager.
- **EnabledStatus**: Reports if the dtRAM is enabled or not on this node. Possible values are TRUE or FALSE.
- **AvailableStatus**: Reports the availability of dtRAM service is enabled. Possible value are TRUE or FALSE.

#### Mitigation

If the dtRAM is enabled, but the AvailableStatus is anything other than TRUE, you should check the dtramd status from the dtRAM machine:

```
dtRAM01# /usr/local/etc/rc.d/dtramd status
dtramd is running as pid 1369
If dtRAM is not running, restart it:
dtRAM01# /usr/local/etc/rc.d/dtramd restart
```

### 9.3.3.8 DesktonerActiveDirectoryStatus

#### Description

ActiveDirectoryStatus provider is derived from CIM\_LogicalElement, and it provides information and status of domain controllers which are added in Horizon DaaS Platform. This provider runs on service provider and tenant appliances.

#### Properties

- CSCreationClassName [key]: Name of the class used to create the database instance.
- SystemName [key]: Name of the system on which the provider instance is running. Set to host name in our case.
- CreationClassName [key]: Name of the class used to create the provider instance.
- DcAddress [key]: describes the unique domain controller address.
- DomainName: describes the domain name associated with domain controller.
- LdapUri: describes the LDAP Url of current domain controller
- **ResponseTime**: describes the response time in milliseconds for LDAP query from Horizon DaaS appliance. The administrator should monitor this property and alert as required if it is preferred domain controller. Example: 0-15 seconds response time is OK, 15-30 seconds is WARN, and >30 seconds is CRITICAL.
- LastUpdated: describes the last updated time for this controller
- **IsPreferred**: Indicates whether the domain controller is preferred domain controller or not in Horizon DaaS Platform
- **CommunicationStatus** [derived]: indicates the ability of the Horizon DaaS Platform to communicate with domain controller. 2 - OK, 4 - Lost Communication

- **OperationalStatus** [derived]: indicates the status of domain controller in Horizon DaaS Platform . 2- OK, 13 – Lost communication.
- **Status** [derived, **deprecated**]: indicates the current state of domain controller in Horizon DaaS Platform (OK, Lost Comm)

#### Mitigation

Make sure that preferred domain controllers are up and running, and verify the latency between appliance and domain controller if response time is high.

Check the required communication ports are open between domain controller and Horizon DaaS appliances.

### 9.3.3.9 Desktone\_HypervisorManagerStatus

#### Description

HypervisorManagerStatus provider is derived from CIM\_LogicalElement, and it provides information and status of Hypervisor Managers in Horizon DaaS Platform. The Hypervisor Manager is a Horizon DaaS entity which manages the hypervisor hosts. This provider runs on service provider appliances only.

#### Properties

- **CSCreationClassName** [key]: Name of the class used to create the database instance.
- **SystemName** [key]: Name of the system on which the provider instance is running. Set to host name in our case.
- **CreationClassName** [key]: Name of the class used to create the provider instance.
- **HostAddress** [key]: describes the hypervisor manager host address and version. It is an address of vCenter, ESX, or vCloud host.
- **Type**: describes the type of hypervisor manager whether it is vCenter/ESX/ vCloud and its product version. Ex: "ESX, 5.1.0"
- **CommunicationStatus** [derived]: indicates the ability of the Horizon DaaS Hypervisor Manager to communicate with Hypervisor Host. 2 – OK, 4 – Lost Communication
- **OperationalStatus** [derived]: indicates the current status of the Horizon DaaS Hypervisor Manager in Horizon DaaS Platform. 2- OK, 13 – Lost communication,
- **Status** [derived, **deprecated**]: indicates the current status of Horizon DaaS Hypervisor Manager in Horizon DaaS Platform (OK, Lost Comm)

#### Mitigation

- Make sure that discovered host is assigned to resource manager.
- Make sure that Hypervisor host is running and reachable from service provider appliance.
- Please verify if there any API compatibility errors in service provider or resource manager desktone logs.
- Check the required communication ports are open between Horizon DaaS appliances and hypervisor hosts.

### 9.3.3.10 Desktone\_NTPService

#### Description

NTPService provider is derived from CIM\_Service, and it provides information about NTP daemon which runs on Horizon DaaS appliance. It also reports time synchronization status. The NTPService provider is available on all Horizon DaaS appliances except dtRAM appliance.

#### Properties

- CSGlobalClassName [key, derived]: Name of the class used to create the database instance.
- SystemName [key, derived]: Name of the system on which the NTP daemon is running. Set to host name in our case.
- CreationClassName [key, derived]: Name of the class used to create the provider instance.
- name [key, derived]: describes the name of the service. It is "NTPD" in our case.
- **Started**[derived]: Started is a Boolean that indicates whether the NTP Service has been started (TRUE), or stopped (FALSE).
- ServerAddresses: describes the NTP server addresses configured in /etc/ntp.conf. It is a comma separated string of addresses.
- PrimarySource: describes the current NTP source in use for time synchronization.
- **SyncState**: indicates NTP synchronization status. TRUE, if NTP is in sync with time source, otherwise FALSE. The SyncState depends on jitter, condition of peer and reach status.
- **Jitter**: describes the jitter value in milliseconds of selected time source. If there is any problem to get the jitter or no primary source is selected by NTP, it returns 60000 milliseconds in order to alert. Providers marks SyncState property to FALSE if jitter is higher than 1000 milliseconds.
- **OperationalStatus**[derived]: indicates the current status of NTP daemon and time synchronization.  
  
OperationalStatus=2 (OK) -> NTP time is in sync(SyncState =TRUE) and all time sources configured are reachable.  
  
OperationalStatus=5 (Predictive Failure) indicates NTP time is in sync, but one or more configured time servers are not reachable or rejected.  
  
OperationalStatus=6 (ERROR) time source is not in sync or NTP service is down
- **StatusDescriptions** [derived]: describes the OperationalStatus in detail which helps administrator troubleshoot NTP time synchronization.

#### Mitigation

Make sure that NTP daemon is running. Troubleshoot NTP for time synchronization.

Make sure that there is connectivity between the service provider nodes and the ntp source.

## 9.4 WBEM and CIM

The Horizon DaaS management appliances allow monitoring via the standard WBEM (web-based enterprise management) CIM (common information model) interface. You can use any monitoring tool capable of understanding the CIM data model (for example, Tivoli).

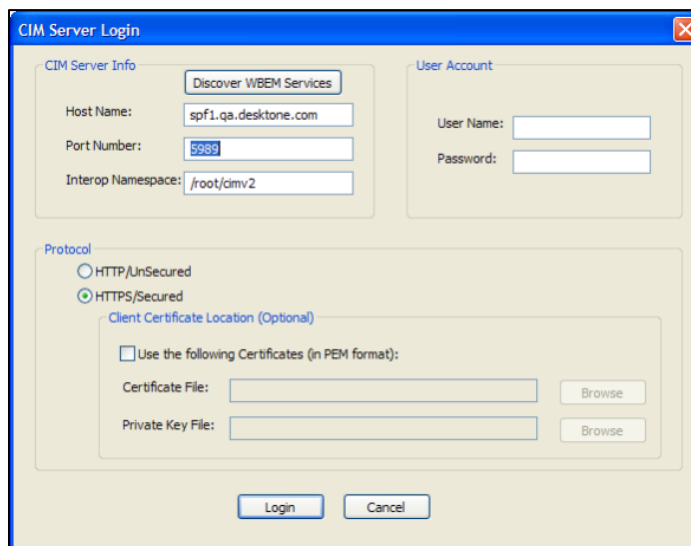
### 9.4.1 Connecting to the WBEM/CIM Server of a Horizon DaaS Management Appliance

To log in to the WBEM/CIM interface of one of the Horizon DaaS management appliances, you need the following information:

- Host name: The DNS name or IP address of the management appliance
- Port number: 5989
- Namespace: /root/cimv2

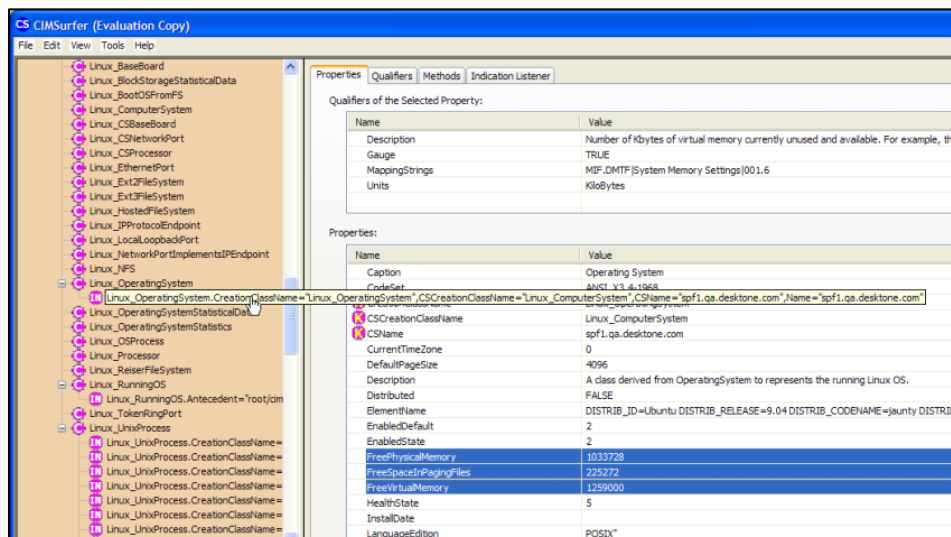
For example, CIMSURfer is a basic browser for CIM information. In practice, you would use a different tool, such as Tivoli, that automatically monitors a number of management appliances and provide alerts based on conditions in the CIM classes of interest. This example also accesses the CIM server without a certificate.

## CIM Server Login



The following figure shows the type of information available from the `Linux_OperatingSystem` class. Using the properties, you can determine the amount or percentage of free memory that is still available.

## CIM Classes

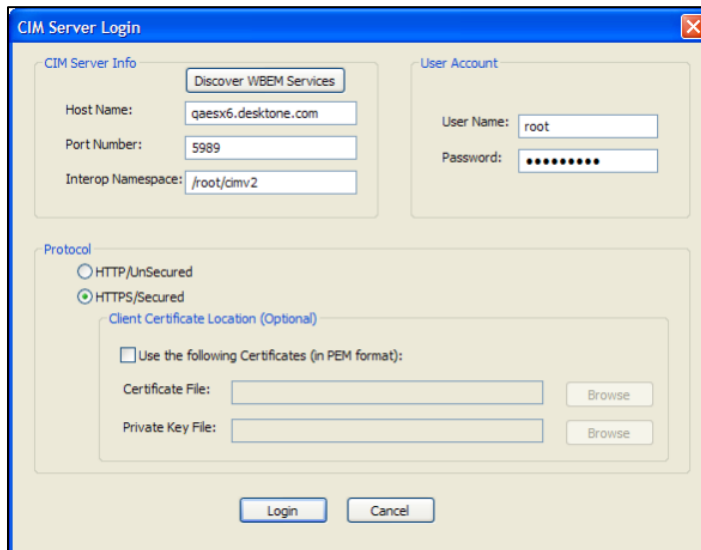


## 9.4.2 Using WBEM/CIM to Monitor ESX Hosts

Since the ESX hosts also expose a WBEM/CIM interface, you can also monitor the ESX hosts. Logging in to the ESX is the same as logging into a management appliance, except that user credentials are required.

The login credentials should be the same ones you use to access the host using the VI client:

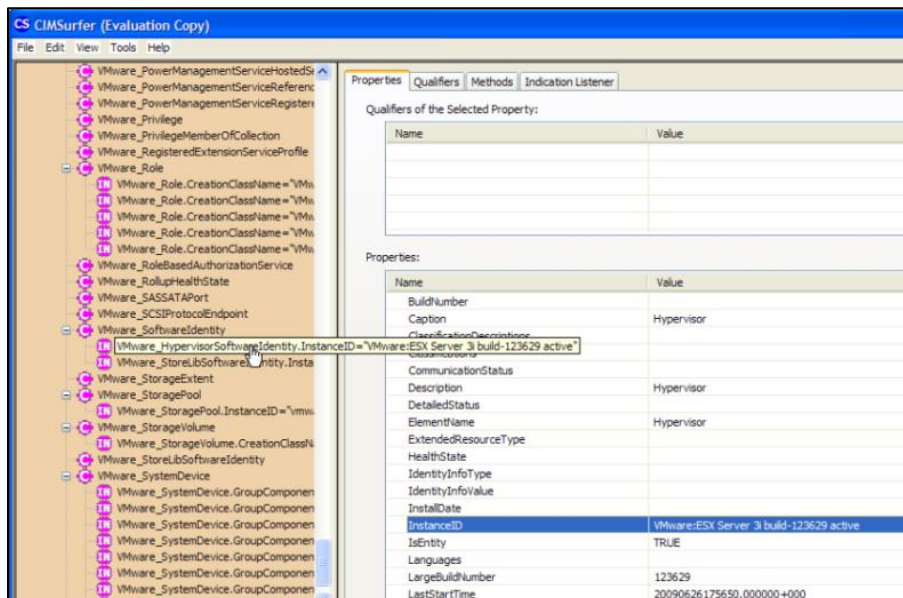
### Logging in to the ESX



The image shows a 'CIM Server Login' dialog box. It has two main sections: 'CIM Server Info' and 'User Account'. In the 'CIM Server Info' section, there is a 'Discover WBEM Services' button, and fields for 'Host Name' (qaesx5.desktone.com), 'Port Number' (5989), and 'Interop Namespace' (/root/cimv2). The 'User Account' section has fields for 'User Name' (root) and 'Password' (masked with dots). Below these is a 'Protocol' section with radio buttons for 'HTTP/UnSecured' and 'HTTPS/Secured' (which is selected). Under 'HTTPS/Secured', there is a 'Client Certificate Location (Optional)' section with a checkbox 'Use the following Certificates (in PEM format):' and fields for 'Certificate File' and 'Private Key File', each with a 'Browse' button. At the bottom are 'Login' and 'Cancel' buttons.

The following figure illustrates how the ESX hosts will expose different classes than the Horizon DaaS management appliances. We recommend that you consult VMware to determine which classes are important to monitor.

### Classes Exposed by ESX Host



The image shows a screenshot of the 'CS CIMSurfer (Evaluation Copy)' application. The left pane displays a tree view of CIM classes, with 'VMware\_HypervisorSoftwareIdentity' selected. The right pane shows the 'Properties' tab for the selected class, displaying a table of properties and their values. The properties include Name, BuildNumber, Caption, ClassificationDescription, CommunicationStatus, Description, DetailedStatus, ElementName, ExtendedResourceType, HealthState, IdentityInfoType, IdentityInfoValue, InstallDate, InstanceID, IsEntity, Languages, LargeBuildNumber, and LastStartTime.

Name	Value
BuildNumber	
Caption	Hypervisor
ClassificationDescription	
CommunicationStatus	
Description	Hypervisor
DetailedStatus	
ElementName	Hypervisor
ExtendedResourceType	
HealthState	
IdentityInfoType	
IdentityInfoValue	
InstallDate	
InstanceID	VMware-ESX Server 3 build-123629 active
IsEntity	TRUE
Languages	
LargeBuildNumber	123629
LastStartTime	20090626 17:56:50.000000+000

# 10 Configure NetApp Storage

---

## 10.1 Summary

This section describes the configuration for NetApp storage with the Horizon DaaS platform.

## 10.2 Hardware and Software Requirements

VMware recommends NetApp storage with FlexClone for the VM image storage to take advantage of deduplication. For the other storage volumes, generic NFS will suffice.

**NetApp hardware and software:**

- FAS3140C e/w 3 shelves of 1TB drives (42)
- PAM card
- NFS
- NearStore A-SIS
- FlexVol
- FlexScale

## 10.3 NFS Exports

See the Knowledge Base for mount points:

<https://cportal.desktone.com/display/KB/Desktone+Hunter+SP3+Datastore+Configuration>.

Also, VMware recommends NetApp storage with FlexClone for the VM image storage (/vol/vol\_tenanta and /vol/vol\_tenantb in this example) to take advantage of deduplication. For the other storage volumes, generic NFS will suffice.

## 10.4 Local Mount Point Structure

On the transit server node, create a directory structure identical to the NFS exports that you will be mounting. While this is not strictly required, it assists in solving mount related issues, and to remember what is mounted where. For example, for the exports defined above, create the following directory structure on the local management node:

```
/vol
|-- db
|-- vol_sp
|-- vol_tenanta
|-- vol_tenantb
|-- vol_dbbackup
`-- vol_upload
```

## 10.5 Permissions and Security

All mounted file systems should have the following export options set:

- Read-write access: Set for all hosts (you can choose to limit to specific hosts if desired, but you should check this as you add management nodes).
- Root access: Specify a range of host addresses which should have root access (using CIDR notation). This range must include all the management nodes.
- Security: Select Unix style security for the exports.

When you view the export options for the NFS exports, it should look like this:

```
Read-Write Access (All Hosts)
Root Access (10.155.0.0/24)
Security (sys)
```

## 10.6 Add a New NetApp Service Account

From your NetApp system, you need to add a new role, group, and user:

- Add a New Role

```
netapp2> useradmin role add desktone_role -c "Role for Deskstone API Support" -a
login-http-admin,api-license-list-info,api-system-get-info,api-system-get-
version,api-system-get-ontapi-version,api-nfs-status,api-nfs-exportfs-list-rules-
2,api-nfs-exportfs-modify-rule-2,api-clone-start,api-clone-stop,api-clone-list-
status,api-vfiler-list-info
Wed Nov 25 19:34:57 GMT [useradmin.added.deleted:info]: The role 'desktone_role'
has been added.
Role added.
```

- Add a New Group

```
netapp2> useradmin group add deskstone_group -c "Group for Deskstone" -r
desktone_role
Wed Nov 25 19:41:35 GMT [useradmin.added.deleted:info]: The group 'desktone_group'
has been added.
Group added.
```

- Add a New User

```
netapp2> useradmin user add deskstone -c "Service account for Deskstone" -n
"Deskstone SA" -g deskstone_group
New password:
Retype new password:
User added.
netapp2> Wed Nov 25 19:57:50 GMT [useradmin.added.deleted:info]: The user
'deskstone' has been added.
```

# 11 RDS Configuration

---

## 11.1 Overview

This section describes how to configure Remote Desktop Services (Microsoft RDSH) on the Horizon DaaS platform. Remote Desktop Services, using the Remote Desktop Protocol (RDP), enables users to connect to Microsoft Windows remotely using Remote Desktop Connection (RDC).

In the RDS session-based model, the service provider determines the type of RDS Session Hosts available to the tenant and the max number of concurrent sessions that can connect. The tenant IT administrator is responsible for the RDS image and provisioning the hosts.

In RDS, every user session in a shared pool is identical, supporting the same applications and settings installed on the RDS Host. The user cannot install applications or customize the environment. Users receive a session from an available host in the session pool when connecting to it. When the user disconnects or logs off, the session becomes available to someone else (disconnect is different from logoff – a disconnected session would first need to time out). Users will always be directed to the RDS host with the lightest current load. Lightest load refers to the host that has the fewest number of sessions.

This section is designed for service providers. It is advisable that each service provider develop a best practice/recommendations guide for their customers based on their specific offering.

## 11.2 Service Provider and Tenant Deployment Coordination

The high level dialogue and actions that occur between a service provider and tenant are as follows:

Step	Tenant	Service Provider
1	Tenant expresses the general requirements for their session based desktops: the types of users, applications that need to be installed on the image, and number of concurrent sessions for each profile.	Deployment services will scope out the necessary number and size of servers that can fulfill the tenant request.
2	Tenant confirms the recommended scope.	Deployment services will create the RDS Server models and assign tenant quota.
3	Tenant can take an RDS Server Template and customize it with required applications and settings.	
4	Tenant provisions a pool for each user profile.	

5	If performance needs to be fine-tuned, the tenant creates a new pool using a different session profile. (The session profile for an existing pool cannot be changed.)
---	---

## 11.2.1 Profile Sizing Guide

RDS session profile sizing is use case dependent. As a best practice, 15 RDS sessions per real CPU core is considered an upper limit. Pending configuration and experimentation, that limit can be raised slightly but must be tested at load prior to acceptance. The Enterprise Center comes with three default session profiles:

Session Profile	Description	vCPU	GB vRAM
Small	For Task Workers – with limited 1 or 2 non-graphical applications	.5	.5
Medium	For Knowledge Worker – with MS Office usage	1	1
Large	For Advanced Worker – Technical or advanced graphics	2	2

If you define additional session profiles in the Enterprise Center, the number of CPUs you specify is vCPU, not real CPU (vCPU is the CPU ratio defined when discovering the hypervisor). Also keep in mind that you want to consider at least 2 GB of vRAM for the O/S use itself.

For example, if you need to plan capacity for 100 Task Workers, you will require a total capacity allocation of 50 vCPU and 50+2 GB vRAM. It is likely that your allocation will need to take virtual resource utilization into account and force you to allocate slightly more in order to maximize the use of the real hardware.

As a best practice, a virtual server should be sized to hold approximately 20-40 users, in contrast to a large scale server with hundreds of sessions. While this means more Operating System storage allocation due to smaller servers, the benefits include (1) limited disruption when updating the pool images and (2) more containment of an out-of-control session (CPU/Memory). Consequently, VMware recommends that service providers standardize on the following server models and deploy physical hardware which can optimize to this sizing:

Virtual Server	vCPU / GB vRAM
RDS-Small	16 / 16
RDS-Medium	32 / 32
RDS- Large	64 / 64

## 11.2.2 Example: RDS Customer Provisioning

The following example provides context for the operations described in the help guide below. The example is fictional and service providers are expected to establish their own internal best practices on how to provision RDS server capacity.

A customer of a fictional service provider, AcmeITServices (AITS), is buying User Sessions and estimates they will need to provision 300 sessions for task workers and 500 sessions for knowledge workers. AITS' sales guidance recommends that task workers use the small session profile (.5 vCPU, .5GB vRAM) and that knowledge workers use a medium session profile (1 vCPU, 1GB vRAM). Based on the customer requirements, that means that the customer will need the following total virtual resources to satisfy their deployment:

Use Case	# of Sessions	vCPU / Session	vRAM / Session	vCPU Total	vRAM Total
Task Worker	300	0.5	0.5	150	150
Knowledge Worker	500	1	1	500	500
<b>Total:</b>	<b>800</b>			<b>650</b>	<b>650</b>

AITS' internal best practices for load balancing and bare metal utilization recommends provisioning medium RDS virtual servers with 32 vCPU to 32 GB vRAM or similar ratios scaled down/up, depending on the size of the pool. This sizing ratio of CPU to Memory has mostly to do with the bare metal hardware that AITS deploys – and may be different from one service provider to another.

Given these requirements, the following virtual servers fulfill the customer requirements:

Use Case	Server Type	Server vCPU	Server vRam	Required For CPU	Required For Ram	Required Servers	Total CPU	Total Ram
Task Workers	RDS-Small	16	16	10	10	10	160	160
Knowledge Worker	RDS-Med	32	32	16	16	16	512	512
<b>Total:</b>							<b>672</b>	<b>672</b>

- Server vCPU: The number of virtual CPUs based on the desktop model.
- Server vRAM: The amount of virtual RAM in gigabytes based on the desktop model.
- Required for CPU: The number of physical servers needed to fulfill the CPU requirements.
- Required for RAM: The number of physical servers needed to fulfill the memory requirements.
- Required Servers: Always the greater of Required for CPU and Required for RAM to ensure that enough CPU and RAM is available for the sessions.
- Total CPU: vCPU \* Required Servers
- Total RAM: vRAM \* Required Servers

In this configuration, the 300 task workers are spread over 10 servers, or 30 users per server. The knowledge workers are spread across 16 servers, or 31 users per server. A lower footprint configuration for the Knowledge Workers might be using 5 RDS-Large server (8cpuX64ram) and 1 RDS-Med server – primarily saving on storage of the O/S.

Note that due to the vCPU/RAM ratio, the knowledge workers will be deployed with a 3% undercapacity (650 required / 672 provisioned) – which is quite good.

Additional considerations for virtual server sizing are the number of different images that will be used with a specific RDS Session Profile. For planning purposes, consider each use case to be distinct if it is expected to use a different image. For example, another customer is looking for 900 user sessions that will be accessed by users from 3 different departments, 1 of which (approximately 400 sessions) will use a different image. In this second example, you should consider Knowledge Worker Subcase 1(500 Sessions) and Knowledge Worker Subcase 2 (400 sessions) as your basis for allocation.

**Note: The Tenant defines the session profile size**

When the Tenant Administrator is defining the RDS pool, they select the session profile size – either one of the defaults or they can define their own. It is up to the tenant to do the final tuning of sessions - and they may discover they can tweak the parameters up or down. Moving to different ratios than recommended may mean that the customer requires less or more capacity as well - which they would have to request from the service provider.

### 11.2.3 Recommended Reading

The document Remote Desktop Services Capacity Planning can be downloaded using the following URL:

<http://www.microsoft.com/en-us/download/details.aspx?id=17190>

## 11.3 Configuring RDS on the Horizon DaaS Platform

This section explains the following four steps required to configure RDS on the Horizon DaaS Platform:

1. The Service Center Admin creates a session-based desktop model (**configuration ► desktop models**).
2. The Service Center Admin, in addition to establishing desktop model quota for session-based desktops, assigns session quota and protocol quota for the tenant (**tenants ► browse tenants**).
3. The Enterprise Center Admin creates session profiles (**pool management ► session profiles**).
4. The Enterprise Center Admin creates session pools (**pool Management ► create session pool**).

### 11.3.1 Service Provider Creates a Session Based Desktop Model (RDS Virtual Server)

1. In the Service Center, select **configuration ► desktop models**.
2. Click the **Add desktop model** link and enter the following information:
  - Session Based: Choose **Yes** to provision remote desktop connections using Microsoft RDSH (Remote Desktop Services). Selecting **Yes** automatically sets the Desktop Type to dynamic. Dynamic desktops are assigned on an as-needed basis. An end user receives a session from an available desktop in the pool when connecting to it. When the user disconnects or logs off, the session becomes available to someone else.
  - Memory: The amount of memory allocated to each virtual desktop, specified in megabytes. For a session-based model (RDS) the memory the Administrator allocates to each desktop is typically higher because each desktop is supporting many sessions.
  - Number of CPUs: The number of virtual CPUs allocated to each virtual desktop.

For example:

The screenshot shows a web form titled "Desktop Models". At the top left, there is a link "+ Add desktop model". The form contains the following fields and values:

Field	Value
Name:	8GigRDS
Session Based	<input checked="" type="radio"/> No <input checked="" type="radio"/> Yes
Desktop Type:	Dynamic
Memory:	8192 MB
Number of CPUs	4

At the bottom of the form, there are two buttons: "Cancel" and "Add desktop model".

3. Click Add desktop model.

### 11.3.2 Service Provider Assigns Quota

The service provider next assigns quota to new desktop model:

1. In the Service Center, select **tenants ► browse tenants**. The **Edit Tenant** screen appears.
2. On the **Edit Tenant** screen, select the **Quotas** tab.
3. On the Quotas tab, specify the following quota:
  - Protocol Quota: This is the number of VMs (desktops) that can use a protocol. Unlimited means that an unlimited number of VMs can use the protocol. The value the Administrator enters cannot be smaller than the value in the In Use column. Note: when upgrading from Augusta 5.1

to Augusta 5.2, the system automatically computes a value for RDP VM Quota based on the number of RDP sessions in use and also pre-selects the Unlimited checkbox.

- Session Quota: This is the total number of RDS sessions that can exist across all VMs.

For example:

### Protocol Quota

Set the protocol quota to a number or unlimited. Unlimited allows unrestricted use of the selected protocol.

Protocol	Unlimited	VM Quota	In Use
RDP	<input checked="" type="checkbox"/>	94	11
RGS	<input type="checkbox"/>	93	2
HDX	<input type="checkbox"/>	94	2
VNC	<input type="checkbox"/>	93	2
NX	<input type="checkbox"/>	93	0
PCoIP	<input type="checkbox"/>	0	0

Update Back to List

### Gold Pattern Quota

Set the gold pattern quota as desired. This number represents the number of gold patterns plus reserved desktops.

Name	VM Quota	In Use
Gold Patterns	3	3

Update

### Session Quota

Set the quota for session based VM connections. This number represents the total number of sessions the tenant can use in session pools.

Name	Session Quota	In Use
Sessions	23	8

Update

### 11.3.3 Enterprise Center Administrator Creates Session Profiles

The Enterprise Center Administrator next creates a Session Profile. A Session Profile specifies the memory and CPUs dedicated to each user session. The profile determines the slice of a given session-based VM that each user will have.

1. In the Enterprise Center, select **Pool Management ► Session Profiles**. The Session Profiles screen appears.
2. Click the **Add Session Profile** link. The page expands to display the following fields:
  - Name: Choose a naming scheme for session profiles that indicates the level of resources allocated for each session, for example Small, Medium, and Large.
  - Memory (MB): The memory dedicated to each user session.
  - Number of CPUs: The fractional part of one or more CPUs dedicated to each user session, for example .5 or 1.85.

For example:

**Session Profiles**

Session profiles are used for creating session pools. Each profile specifies the are used simultaneously.

[+ Add Session Profile](#)

\* Name:

\* Memory (MB):

\* Number of CPUs:

Name	Memory (MB)	CPUs	Session Pools Using	Action
Small	512	0.5	6	<input type="button" value="Delete"/>
Medium	1024	1.0	0	<input type="button" value="Delete"/>
Large	2048	2.0	0	<input type="button" value="Delete"/>

Navigation menu (right): browse pools, create pool, browse session pools, create session pool, patterns, **session profiles**, tasks and events

- After entering the required information, click the **Add Session Profile** button.

### 11.3.4 Enterprise Center Administrator Creates Session Pools

The Enterprise Center Administrator next creates Session Pools. Session Pools are an efficient way of assigning desktop sessions to similar user types. Session pools are based on the same session profile and gold pattern and use the same specs and configurations.

In the Enterprise Center, select **Pool Management ► Create Session Pool**. The Create Session Pool screen appears (see illustration below).

The Enterprise Center Administrator completes the following four steps on the Create Session Pool screen:

- Pool Composition Input
- Set Session Count
- Configuration
- Confirm Pool

After entering the required values in each step, click Next to save the values and advance to the next step. Fields marked with a red asterisk (\*) require input.

#### 11.3.4.1 Create Session Pool ► Pool Composition Input

In this step, the Enterprise Center Administrator determines the characteristics of each session in a pool:

Data Center	Select the Data Center in which to create the pool.
Name	Enter a name for the pool.
Session Profile	A Session Profile specifies the memory and CPUs dedicated to each user in the pool. The profile determines the slice of a given session-based VM each user has. The service provider determines the available Session Profiles.
Gold Pattern	Select a gold pattern to base the pool on. The only gold patterns in the list are those using the Windows Server 2008 R2 operating system, as this is the only supported OS capable of running a Microsoft RDS host.

Protocols	<p>Select RDP, PCoIP, or both (protocols are described above). Note the following:</p> <ul style="list-style-type: none"> <li>• Session Hosts must have compatible protocols to be utilized across multiple Session Pools.</li> <li>• You can view but cannot change the protocol for an existing Session based pool.</li> <li>• If you do not currently have any PCoIP quota, the PCoIP checkbox does not appear.</li> </ul>
Network	<p>This field will be selectively shown when the network to pool option is enabled. This option must be enabled for the tenant by the service provider administrator. If the network to pool option is enabled, a drop down list of available networks will be shown. A single network can be selected indicating which network the pools created in the pool will be placed on.</p>
Customer ID	<p>This field will be selectively shown when the super tenant option is enabled. This option must be enabled for the tenant by the service provider administrator. The super tenant option is designed for an MSP to use a single tenant to manage multiple customers. For further information about the super tenant option please see inquire with your service provider administrator. The customer id field is a free form text field that allows an MSP to attach a customer code for billing and other tracking purposes.</p>


#### 11.3.4.2 Create Session Pool ► Set Session Count

The system displays the maximum number of sessions the pool can accommodate. This number is calculated based on the system resources required by each session, the available quota for the session-based desktop models used by other pools, and the remaining quota of sessions for all VMs.

Number of Sessions	<p>Enter a value no greater than the maximum displayed by the system. <b>Note: If maximum number of sessions displayed by the system is not large enough, select a different Session Profile that presents a smaller slice of the VM to each user and click Next. The system will recalculate the maximum number of sessions and display the new value.</b></p>
Show Session Hosts	<p>Click this link to display a table that indicates the VMs that will host the sessions in this pool and how many sessions will be hosted on each VM. Session hosts are a collection of VMs (possibly mixed footprint) that can be partially or completely dedicated to hosting one or more session pools. The system determines the appropriate number of VMs by considering the system resources each session requires, as specified by the Session Profile; and the footprint specified by the desktop model.</p>

For example:

**Step 2: Set Session Count**

 The pool can accommodate **24 sessions at most**.

This is based on your selected profile, session quota of 228 available sessions and quotas for session based desktop models.

Number of Sessions

[Show Session Hosts](#)

Sessions to Add to Existing Hosts

Additional sessions will be added to these existing hosts.

Name	Memory	CPUs	Sessions Reserved	Session Capacity	Capacity Used
nrds100	2048	2	4	4	100%
nrds101	2048	2	4	4	100%

New Hosts

Based on your input and available desktop model quotas, the following session hosts will be provisioned.

Desktop Model	Memory	CPUs	Sessions Reserved	Session Capacity	Capacity Used
RDS 1	2048	2	4	4	100%
RDS 1	2048	2	2	4	50%

#### 11.3.4.3 Create Session Pool ► Configuration

The configuration screen has three panels: Provisioning, Pool Configuration, and User Experience.

- Provisioning Panel: Use this panel to change the following desktop provisioning characteristics:

VM Name Composition Rule	A base name for the VMs in this pool. By default, the system provides a base name derived from the pool name. Desktops are named incrementally based on this name.
Computer OU	The VMs in a pool can optionally belong to an AD organizational unit that the Administrator specifies here. This defines a specific organizational unit for this pool. This organizational unit must exist before specifying it in this field.
Domain Join	Select No to prevent desktops from joining the specified domain (default=Yes). Enable only for Windows desktops that aren't joined to the domain via a run once script, etc.
Domain	Select the NETBIOS domain to which this pool of desktops should belong.
Assigned Groups	Enter the AD groups map the pool to automatically. For example, CN=MyCompanyUsers,OU=Groups. Enter cn or ou to see a list of valid groups. Groups can also be assigned easily to pools from the Mapping screen.

- Pool Configuration Panel: Use this panel to define policies to be applied to the pool.

Session Timeout for VM	Enter the session idle timeout interval in milliseconds. The default is one hour (3,600,000 ms).
Run Once Script (optional)	The location of a run once script that should run after sysprep completes. If there is more than one script, combine them into a parent file that calls the remaining scripts.

- Remote Applications panel: on the Remote Applications tab, for each application you want to make available, click Add New Applications and specify the following:
  - Name: The name displayed in Desktop Portal.
  - Application Path: The path to the executable on the gold pattern image.
  - Icon: (optional) An image associated with the application in the user portal. If you do not have View Agent version 6.1, this column will display a question mark icon or an icon from the existing URL if there is one. If not specified, a generic icon is displayed in the Desktop Portal; however, no icon is displayed in the Enterprise Center if not specified. If the icon is not reachable, the system displays a message to the user and a question mark is displayed in place of the icon. When you add an application, the icon may not be immediately available, even if it is available in other pools
  - Command Line Parameters: (optional) Any application parameters you wish to supply when the application is launched.

After specifying the Name, Application Path and any optional settings, click Add Application.

You can control access to a full session for pools with remote applications via the Allow full desktop checkbox. When the box is checked, users can choose whether to connect to individual applications or a full session. When the box is unchecked, users will only be able to connect to individual applications and not to a full session.

**Note: If you clear the Allow full desktop checkbox but have no applications added, the system will automatically re-check the box and change the setting back.**

- User Experience panel: Use this panel to choose any desired RDP redirection options (clipboard, drives, etc.). RDP redirection options specify which local devices on a rich client (for example, a laptop computer) get redirected to the desktop environment. Any device that gets redirected will show up as a device in the virtual desktop.

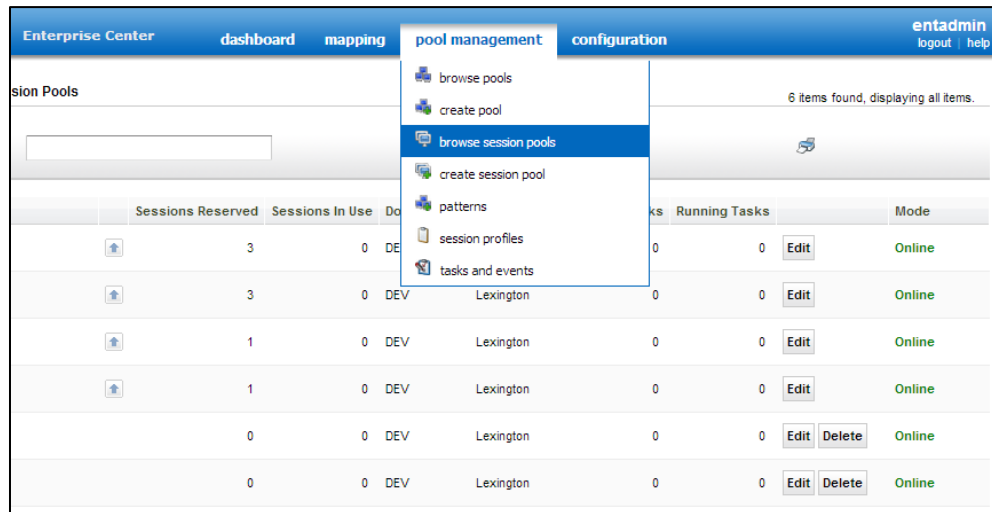
#### 11.3.4.4 Create Session Pool ► Confirm Pool

##### Procedure

1. Review the pool characteristics.
2. Click **Back** to change any of the information.
3. Click **Create** to create the session pool.

### 11.3.5 Browsing Session Pools

After creating a new Session Pool, to view the available session pools, select **pool management ► browse session pools**. For example:



Enterprise Center				dashboard	mapping	pool management	configuration	entadmin logout   help	
Session Pools						6 items found, displaying all items.			
	Sessions Reserved	Sessions In Use	Do	ks	Running Tasks	Mode			
	3	0	DEV	Lexington	0	0	Edit	Online	
	3	0	DEV	Lexington	0	0	Edit	Online	
	1	0	DEV	Lexington	0	0	Edit	Online	
	1	0	DEV	Lexington	0	0	Edit	Online	
	0	0	DEV	Lexington	0	0	Edit	Delete	Online
	0	0	DEV	Lexington	0	0	Edit	Delete	Online

- Editing a Session Pool: Select the Edit button for a pool to edit that pool's characteristics.
- Deleting a Session Pool. The Delete button is present only after the Administrator first edits the session pool to decrease the Session Count to zero.

# 12 Remote Applications

---

## 12.1 Overview

The Horizon DaaS Platform can be configured to allow end-users to access specific applications remotely from a web browser, rather than connecting to the entire desktop. Remote applications run either in a desktop or a terminal services session and retain the context of the user data folders, allowing users to access their data files and save to the remote desktop or session.

When end users log into the Desktop Portal, they see the desktops and applications they have been entitled to by the IT Administrator. File Explorer can be one of the applications exposed as a remote application, enabling a user to launch an application by clicking on a file in File Explorer.

This release adds endpoint client support for Android devices.

## 12.2 System Requirements

### 12.2.1 Operating Systems

- Windows 7: Enterprise and Ultimate (RDP only)
- Windows 8: Enterprise (RDP only)
- Windows 2008 Server R2 (RDP and PCoIP)
- Windows Server 2012 (RDP and PCoIP)

### 12.2.2 End Point Client

- The end point must support the Microsoft RDP protocol and its Remote App feature.
- Applications are available only via the Desktop Portal on Windows, or via the DaaS Mobile Client on iPad, iPhone, or Android.
- Windows clients:
  - Windows clients require Remote Desktop Connection 6.0 or higher. RDC 6.1 is included in Windows XP SP3, Windows 7, and Windows Server 2008.
  - Windows Server 2003 SP1 or SP2 clients, and Windows XP SP2 clients require RDC 6.0 to be installed separately, as those releases contain an earlier RDC version. You may download the installer package from [article 925876](#) in the Microsoft Knowledge Base.

### 12.2.3 Protocols

RDP and PCoIP are currently the only supported protocols for remote applications. Users can continue to access full desktop sessions using other protocols.

Note the following regarding use of the PCoIP protocol:

- To use remote applications with PCoIP, you need to have Horizon DaaS Agent version 6.1 or higher.
- Remote application connections via PCoIP are only supported for Session based pools..
- You cannot launch multiple items from the portal via PCoIP. If you attempt to do this, the View Client will close itself. To use multiple mapped items, go to the View Client.
- There are also a number of limitations when using PCoIP with RDS servers. For more information, see the View Client documentation.

### 12.2.4 Licenses

Remote application access is configured using existing components of the Horizon DaaS Platform and the Windows O/S in the template. As such, the standard Horizon DaaS Platform and application-specific software licensing requirements apply:

- Hypervisor license for the host (i.e. vSphere Enterprise)
- Windows Remote Desktop Services SAL – SPLA user license
- Horizon DaaS Concurrent User License for RDS / Apps

For Windows Server with RDS:

- Windows Server 2008 R2 or 2012 license – SPLA user license (depending on number of instances per host, might benefit from the Datacenter edition)
- Windows Server SAL – SPLA user license

## 12.3 Enterprise Center Setup

To enable remote applications for end users, the Enterprise Center Administrator must create a pool, associate remote applications with the pool, and then map users to the pool.

### 12.3.1 Create a Pool and Associated Remote Applications

A pool is a group of VMs based on the same gold pattern and configurations.

#### Procedure

1. Log in to the Enterprise Center.
2. Create a pool using one of the following methods:

#### Individual Desktop Based

- a. Select **Pool Management ► Create Pool ► Individual Desktop Based**
- b. To create a pool of desktops, select a desktop model to base this pool on. Desktop models are defined by your service provider. The desktop model specifies the desktop type, memory, and number of CPUs for each VM in the pool.
- c. Specify the other pool characteristics as appropriate.

- d. Click Customize Pool and select the **Remote Applications** tab.

#### Session Based

- a. Select **Pool Management ► Create Pool ► Session Based**
  - b. Complete the Pool Composition Input and Set Session Count panels as appropriate.
  - c. On the Configuration panel, select the **Remote Applications** tab
3. On the Remote Applications tab, for each application you want to make available, click **Add New Application** and specify the following:
    - a. Name: The name displayed in Desktop Portal.
    - b. Application Path: The path to the executable on the gold pattern image.
    - c. Icon: (optional) An image associated with the application in the user portal. If you do not have View Agent version 6.1, this column will display a question mark icon or an icon from the existing URL if there is one. If not specified, a generic icon is displayed in the Desktop Portal; however, no icon is displayed in the Enterprise Center if not specified. If the icon is not reachable, the system displays a message to the user and a question mark is displayed in place of the icon. When you add an application, the icon may not be immediately available, even if it is available in other pools.
    - d. Command Line Parameters: (optional) Any application parameters you wish to supply when the application is launched.
  4. Click **Add Application**.

To add additional applications, click **Add Application** and repeat the steps above.
  5. Allow full desktop: (optional) Give the user the option to launch the entire desktop.

**Note:** If you clear the **Allow full desktop** checkbox but have no applications added, the system will automatically re-check the box and change the setting back.

### 12.3.2 Map Users to the New Pool

As with any pool, the Administrator maps users as follows.

#### Procedure

1. In the Enterprise Center, select **Mapping**.
2. On the Mapping screen, click the plus ( + ) icon in the Add Mapping column for the user to map.
3. Enter the pool and click **OK**.

## 12.4 Launch an Application in the Desktop Portal

Note the following items regarding launching remote applications.

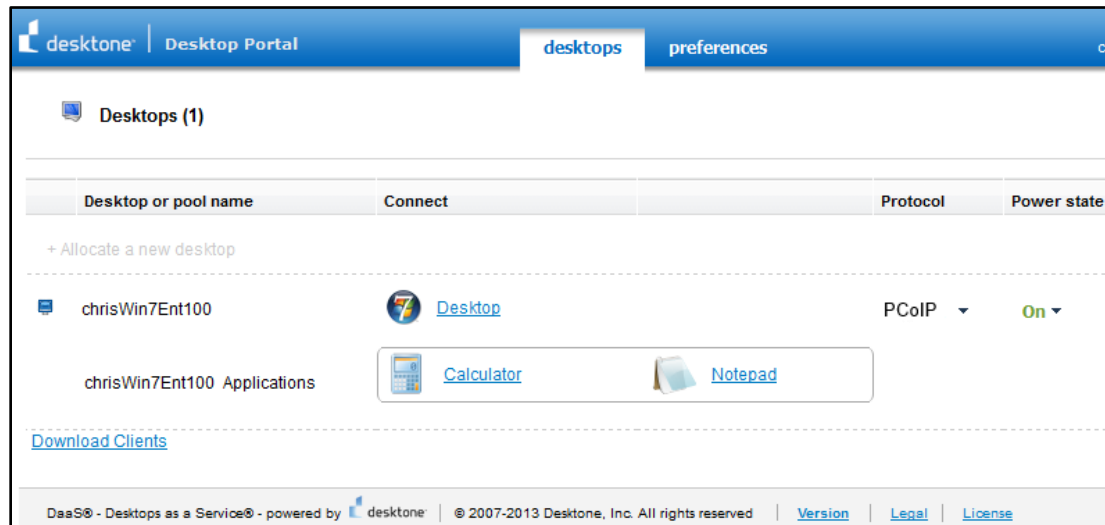
- Regarding use of the PCoIP protocol
  - To use remote applications with PCoIP, you need to have Horizon DaaS Agent 6.1.
  - Remote application connections via PCoIP are only supported for Session based pools.
  - You cannot launch multiple items from the portal via PCoIP. If you attempt to do this, the View Client will close itself. To use multiple mapped items, go to the View Client.

- There are also a number of limitations when with using PCoIP with RDS servers. For more information, see the View Client documentation.
- You cannot select the default protocol for RDS servers.
- The auto-launch function works for both RDS and VDI.
- The HTML Access (Blast) protocol does not support RDS remote applications.

To launch a remote application from the Desktop Portal using PCoIP, perform the following steps.

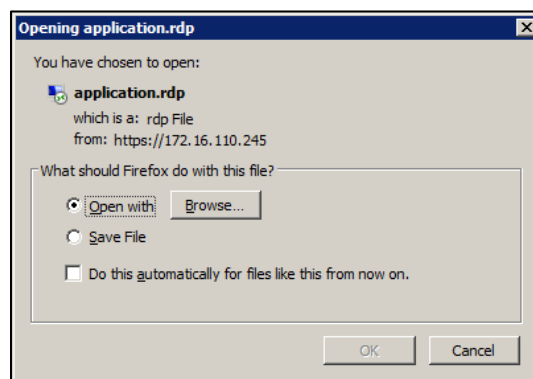
#### Procedure

1. Select the application name from the set of applications displayed beneath the Desktop link. For example:



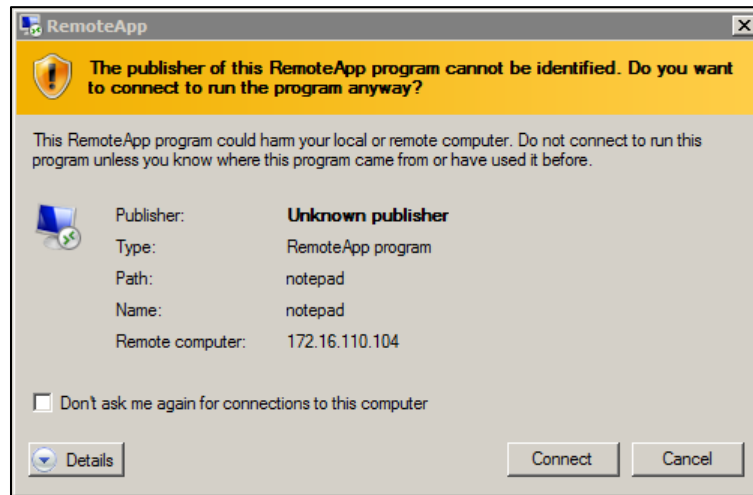
**Note:** A user cannot open both a desktop session and an application at the same time. If the user tries to launch an application while a desktop session is still running, the system presents the option to end the existing session.

2. The **Opening application.rdp** download dialog is displayed, for example:



3. Click **OK**.

4. Click **OK** on the next screen:



5. Click **Connect**. (If prompted, enter your username and password.) The RemoteApp session is opened with the application running, in this example, Notepad.

**Note:** Users should always close the application(s) they are using before disconnecting from the desktop session. Failure to do so could cause any documents they are working on to be locked against editing until the session eventually times out.

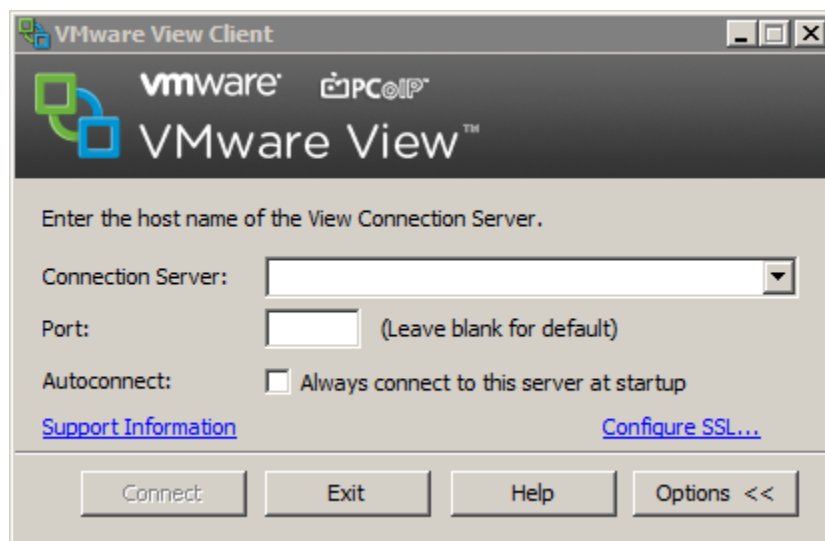
## 12.5 Launch an Application in the View Client

**Note:** Do not use the VMware Horizon View Client for Windows with Local Mode Option.

After installing the required software, you should be able to connect to a desktop using the View Client:

### Procedure

1. Launch the VMware Horizon View Client.
2. In the Connection Sever field, enter the IP address or DNS name of the Desktop Portal:



3. Click **Connect**.
4. Enter User Name and Password.

5. Click **Login**. The View Client displays the list of available remote applications.

**Note: The connection is established using the default display protocol. The default can be set in either the Horizon DaaS Desktop Portal or by the System Administrator in the Horizon DaaS Enterprise Center when creating pools.**

6. Select an application and click **Connect**.

**Note: Right-mouse click on an application to see the following additional desktop operations:**

- Connect: Connects to the desktop using the default display protocol.
- Display Protocol: Overrides the default display protocol.
- Logoff: Ends your desktop session. Any unsaved work will be lost.
- Reset Desktop: Restarts Windows OS.

## 12.6 Important Session Timeout Recommendations

### 12.6.1 RDS/Session Pools

Since every VM in a session pool (RDS pool) can be shared by multiple users, there are some important considerations regarding session timeouts. The administrator should strive for a balance between keeping as many sessions available for other users as possible while remote applications are used, and preventing forced logoff of users who are connected but idle.

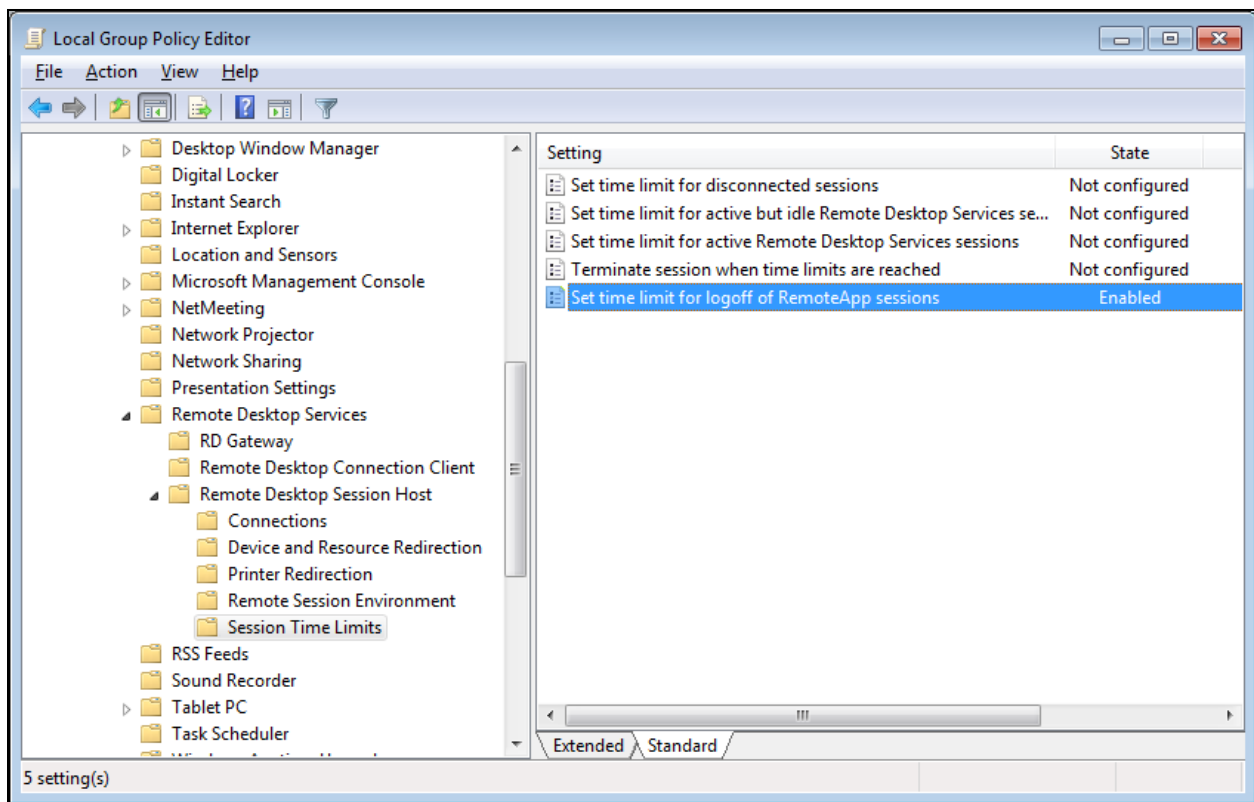
As stated by Microsoft, with remote applications, there is no clear way for a user to logoff, and when a session is disconnected – by the user clicking the “X” button, for instance – the session will remain in a disconnected state without being logged off. The session allocated to this user would remain unavailable to anyone else until a session timeout is reached.

The Horizon DaaS Platform has a single session timeout policy per pool (Edit Pool -> Pool Configuration-> Session Timeout for VM). This specifies the maximum time a user’s session can remain logged in and idle before it becomes logged off. To cause a disconnected remote application session to be logged off shortly after it is closed, the administrator can choose to set this to a low value – 5 minutes, for example – but a side effect would be that a full desktop session would also be logged off after 5 minutes of idle time.

To terminate an app session following a user disconnect - without requiring a change to the Horizon DaaS session timeout – a Windows Group Policy can be applied to VMs of an RDS Session Pool. This setting is called “Set time limit for logoff of RemoteApp sessions”. It can be found on the following Microsoft Technet article: <http://technet.microsoft.com/en-us/library/cc753112%28v=ws.10%29.aspx>

The path cited in the Technet article is incorrect. The correct path to the setting in the Group Policy Management Console is:

User Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits



Administrators are advised to configure this GPO and set the logoff delay to “Immediately”. In this way, a remote application session will be terminated following closure of a remote app, and the session will be returned to the pool of available sessions. Since this can be applied without adjusting the Horizon DaaS session timeout, an administrator can configure the idle time before a desktop or application session gets logged off independently of this GPO setting.

Note that even after setting the logoff delay to “Immediately”, there may still be a delay of a few seconds between a user closing a remote app and the platform receiving notification that the session has been closed.

## 12.6.2 Individual Desktop Pools

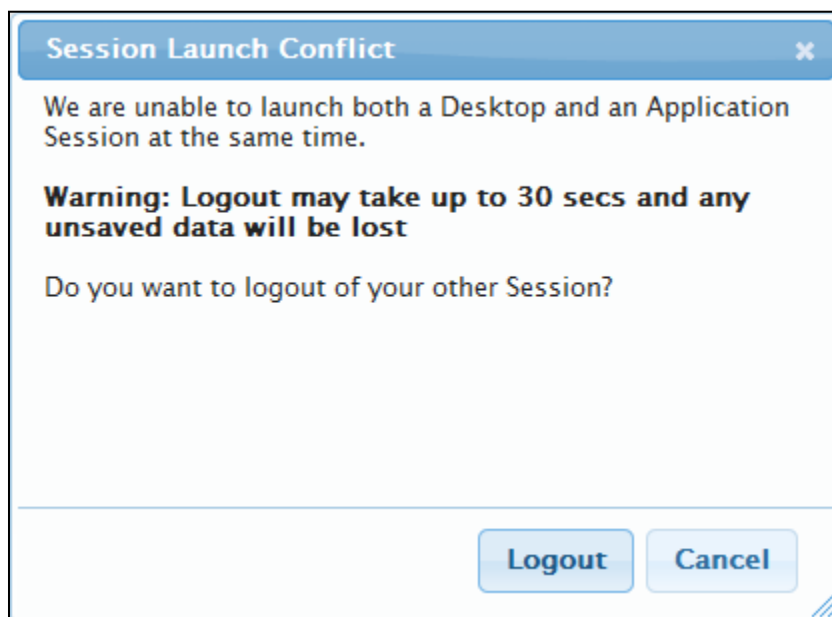
The Group Policy setting for Windows RDS VMs mentioned above is not available for individual Windows desktops. So the only means an administrator has to control the logoff of a remote application is through the Horizon DaaS Platform session timeout, which controls both desktop and remote application sessions.

Consequently, administrators are encouraged to consider the typical expected usage of any dynamic desktop pools when deciding how to configure the session timeout, as a disconnected remote app will cause a dynamic pool VM to remain allocated until the session timeout interval is reached. If only remote applications will be available on such pools, a low timeout (e.g. 30 minutes) may be acceptable. However, if a mixed use of desktops and applications is anticipated, a low timeout should be weighed against how quickly it is too early to completely logoff an idle user’s full desktop session.

The session timeout of a static pool will likely be of less concern as each user is assigned to a specific VM permanently in this model. So while a disconnected, but not yet logged off, remote application session will cause the VM to remain in allocated state, the allocation of that VM has no bearing on the availability of a session for any other user.

## 12.7 Switch session types

On a pool where both the full desktop and remote applications are exposed, end users are limited to an active session of only one session type simultaneously. Therefore, if a user has a desktop session running – whether that user is actively using it or is idle – and then attempts to launch an app on the same desktop or pool, the Desktop Portal presents a dialog box to prompt the user to log out of the current session before proceeding:



In the case of an individual desktop pool or VM, this will actually disconnect the user, rather than initiate a complete logout. This is to provide the user a chance to reconnect to the desktop session following their app session, in case the session timeout has not yet been reached following the usage of their app session. Also, this avoids the reboot upon logout from a dynamic pool VM, which would cause the given VM to initiate its reboot immediately and become unavailable until the reboot completes.

The same dialog would be presented if the user started a remote application first, and then attempted to switch to a desktop while the app is still running, or just a few seconds after the app is closed. Note, however, that it is not possible to reconnect to a remote application instance after it is closed. As discussed earlier, the app session will remain in a disconnected state until the session timeout is reached, and then terminated.

With session pools, the logout of the existing session will occur in response to the “Logout” prompt. Then, with either pool type, the user is free to connect using the desired session type once the dialog disappears.

# 13 Configure RSA

---

## 13.1 Add Tenant Appliances to the RSA Authentication Manager

All tenants must be visible to the Authentication Manager, and so must be added to the RSA Authentication Manager as Authentication Agents. It is also necessary that the RSA Authentication Manager be able to communicate over the front end IPs with the tenant appliances.

**Troubleshooting:** If the tenant appliance cannot ping the RSA Authentication Manager or the RSA Authentication Manager can't ping the tenant appliances, then the customer should consult their Network team and make sure the two Networks can see each other and communicate.

### Procedure

1. Log into the Primary RSA Authentication Manager.
2. Select **Access ► Authentication Agents ► Add New**.

If the RSA Authentication Manager cannot communicate over the front end IPs with the tenant appliances, you might not be able to add the tenant as an Authentication Agent.

**Note:** All tenant appliances must be listed as Authentication Agents, but their floating IPs do not need to be added. Additionally, if there is a NAT IP address different from the internal/local IP address, it must be added to the "Alternate IP Address" section listed in the Add New user interface on the RSA Authentication Manager.

## 13.2 Enterprise Center Configuration

**Note:** You must complete the steps in the preceding section, "Tenant Visibility to Authentication Manager," before proceeding with Enterprise Center Configuration.

To configure RSA authentication, the tenant Administrator completes the following steps in the Horizon DaaS Enterprise Center.

### Procedure

1. Log in to the Horizon DaaS Enterprise Center.
2. Select **Configuration ► Multi-Factor Authentication**. The RSA SecurID Authentication screen is displayed.
3. In the **File path** field, browse for the file `sdconf.rec` and then click **Upload**. Upon successful upload, a green check mark is displayed.

**Note:** The file `sdconf.rec` is generated by the RSA Authentication Manager by logging into the RSA Security Console and navigating to **Access ► Authentication Agents ► Generate Configuration Files**.

4. **RSA Authentication Status:** The displayed status initially is DISABLED. To validate that RSA authentication is functioning properly and change the status to ENABLED, complete the following steps:
  - a. Click **Enable** to display the Test Authentication dialog.
  - b. In the dialog, enter a valid username and RSA code.
  - c. Click **Test**. If the authentication is successful, RSA authentication is enabled for all subsequent user logins and the displayed status changes from DISABLED to ENABLED.

**Note: Once enabled, the service provider can temporarily override RSA authentication, allowing Enterprise Center Administrators to bypass the RSA authentication step when logging in to the Enterprise Center or User Portal. For example, if the Tenant Administrator can no longer authenticate on any appliance using their RSA Credentials, the Administrator should contact the service provider to temporarily deactivate RSA Authentication. To re-enable, click Enable.**

5. **Require Same Username Throughout Authentication:** (optional) When enabled, this feature locks the Domain Username field. This forces the user attempting to authenticate to have the same username credentials for both RSA and Domain Challenge. Otherwise, the username field is not locked on the Domain Challenge screen and the user may enter a different name.
6. **Only Prompt External connections for RSA Credentials:** (optional) If unchecked, all users, both inside and outside the network, must enter RSA credentials. If checked, users inside the network do not need to enter RSA credentials. The distinction between internal and external is configured by the service provider.

## 13.3 Generic Troubleshooting for "Access Denied"

The Horizon DaaS Enterprise Center does not have access to the RSA Authentication Manager error log. In order to view these failures, the Tenant Administrator must launch the RSA Authentication Monitor.

### Procedure

1. Log into the RSA Authentication Manager.
2. Select **Reporting ► Real-time Activity Monitor ► Authentication Activity Monitor**.
3. Click **Start** in the Activity Monitor.

Some common causes of 'Access Denied' include the following:

Cause	Description
Bad PIN	The user entered an invalid PIN value. PINs are unique to each SecurID token and might not be required for all SecurID Setups.
Bad Token Code	The user entered an expired or misspelled token code.
Bad Username	The user name is not recognized by the RSA Authentication Manager.
Node Secret File Mismatch (secured file)	There are three common reasons for mismatches: <ul style="list-style-type: none"><li>• The file is missing on the tenant/Agent but was not cleared on the Server.</li><li>• The file was flagged as cleared on the Server, but still exists on the Agent.</li><li>• The file is corrupted or does not match.</li></ul>
User Account Locked	The user attempted to authenticate X number of times and failed each time, where X is setup by the System Administrator on the RSA Authentication Manager.

Authentication Timeout	<p>Authentication took longer than 60 seconds for one of the following two reasons. In either case, the user should retry:</p> <ul style="list-style-type: none"> <li>• In instances of high latency, it is possible the authentication request timed out.</li> <li>• After initial configuration, dtService restart, and Agent Restart, the first login with RSA can time out because of the time the RSA API takes to initialize.</li> </ul>
Out of Sync Clock	RSA Authentication Manager time clock is more than 60 seconds out of sync with Agent Time clock. This can happen if both systems are not using the same NTP clock or if time drift is extreme.

## 13.4 Troubleshoot Problems with Files Required by the RSA APIs

The Horizon DaaS integration with the RSA APIs requires two files to be in place before start up can occur:

File	Description	Troubleshooting
rsa_api.properties	The dt-platform debian installs this file into /usr/local/desktop/release/active/template/conf. At the first authentication, it is automatically moved to the /usr/local/desktop/release/active/conf directory.	No troubleshooting should be necessary.
sdconf.rec	To generate, log into the RSA Security Console and select <b>Access ► Authentication Agents ► Generate Configuration Files</b> . The file must then be uploaded by the Tenant Administrator in the Horizon DaaS Enterprise Center.	<p>If sdconf.rec is no longer on the source appliance, there are two options:</p> <p>The Tenant Administrator can upload the file again in the Enterprise Center by selecting <b>Configuration ► Multi-Factor Authentication</b>.</p> <p>The service provider can copy the file from another tenant appliance to the directory /usr/local/desktop/release/active/template/conf on the source appliance.</p>

The RSA API creates two files on the first successful authentication and these are used for future authentications:

File	Description
securid (referred to as "Node Secret")	This file is used as a communication key between the RSA Authentication Manager and the RSA Agent. A mismatch between the local Node Secret status and the RSA Authentication Manager Node Secret status will result in Access Denied. At the tenant, the platform does not know if the Node Secret does not match. This file is created only after a successful authentication and only if the RSA Authentication Manager believes it has not issued the Node Secret file.
JASatus.1 (referred to as "Offline Files")	This file is used to keep track of the "state of the realm" for RSA Authentication Manager instances.

RSA support can direct the Tenant Administrator to remove these files by completing the following steps.

#### Procedure

1. Log into the Horizon DaaS Enterprise Center.
2. Select **Configuration ► Multi-Factor Authentication**
3. **securid:** Scroll down to “Clear Local Node Secret File” and click **Apply**. The local RSA Agent is restarted. (Note: This might result in a longer authentication for the first user if authentication failures occur while the Agent is being reinitialized.)
4. **JASStatus.1:** Scroll down to “Remove Offline RSA Files Across Tenant Appliances” and click **Apply**.

## 13.5 Restore Tenant Appliance(s)

After restoring a tenant appliance, the Tenant Administrator needs to validate the following.

#### Procedure

1. Validate that you can log into the Enterprise Center. If you cannot log in, the service provider needs to activate the override policy for the tenant to allow them to configure RSA for use.
2. RSA Node Secret file status: Restoring a tenant appliance automatically clears the node secret file. You also need to manually update the RSA Authentication Manager to reflect this fact for each tenant appliance restored:
  - a. Navigate to **Access ► Authentication Agents ► Manage Existing**.
  - b. Find the Agent (tenant) in question.
  - c. In the drop down menu for that entry, click the **Manage Node Secret** field.
  - d. Check the **Clear the Node Secret** option.
  - e. Click **Save**.
3. Update the sdconf.rec file: Complete steps 1 -3 in Enterprise Center Configuration on page 4.

## 13.6 Deactivate RSA Authentication (Service Providers Only)

If the Tenant Administrator can no longer authenticate on any appliance using their RSA Credentials, the service provider can deactivate RSA Authentication for that tenant by setting the following policy to true: `tenant.authentication.override`

Setting this policy to true bypasses the RSA Authentication challenge screen for all users of a given tenant. While set to true, any users of the Enterprise Center, User Portal, and View Client can log in by entering just their username and domain.

To deactivate RSA Authentication for a tenant, the service provider performs the following steps.

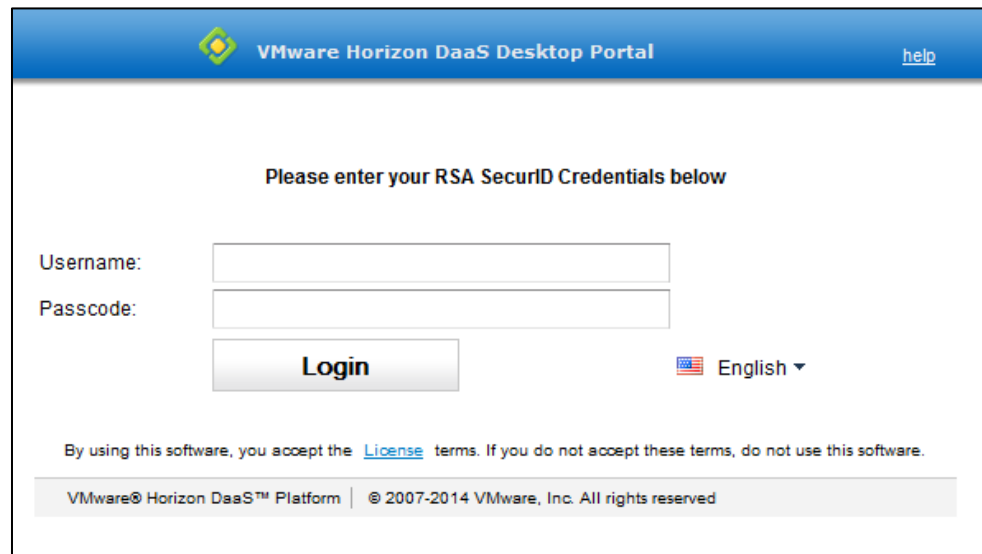
#### Procedure

1. Log into the Horizon DaaS Service Center.
2. Scroll down the page until you see the `tenant.authentication.override` policy.
3. Change the value of `tenant.authentication.override` to false.
4. Click **OK**.

The Tenant Administrator can re-activate RSA Authentication for a tenant in the Enterprise Center by selecting **Select Configuration ► Multi-Factor Authentication**.

## 13.7 How an End User Logs in to the Horizon DaaS Portal

Once the Tenant Administrator has enabled RSA authentication, users see the following login screen:



On this screen, users enter their RSA SecurID credentials:

- **Username:** This is the user's unique login name. The username might be locked and non-editable depending on how the System administrator has set up authentication.
- **Passcode:** This is the authentication code displayed by the RSA SecurID token. The token generates a new authentication code at fixed intervals (usually 60 seconds).

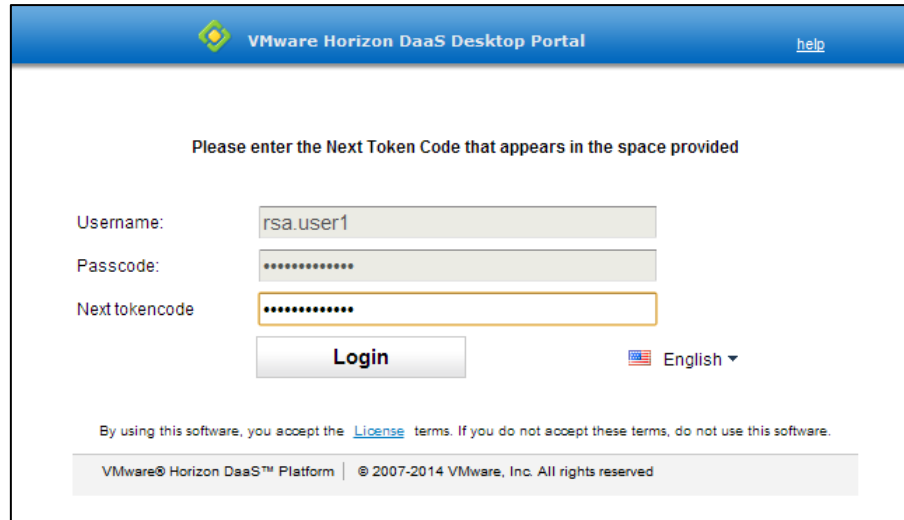
**Note:** If a user makes repeated failed authentication attempts, their RSA User account might become locked. In this instance, users should contact their System Administrator.

To be authenticated and allowed access to the Portal, the user needs to enter the authentication code being displayed in real time on the RSA SecurID token (if the user set up a PIN when logging in to the Desktop Portal the first time, then the user also enters the PIN). The user must enter the complete passcode within the timeout period. The amount of time remaining in the timeout period is indicated by the horizontal bars to the left of the authentication code display. When the last horizontal bar disappears, the timeout period expires, a new authentication code is displayed, and the timeout period restarts. Each token code is valid for a single authentication only and cannot be reused in subsequent logins.

### 13.7.1 Invalid Token Codes

If a user fails to enter the code correctly within the timeout period, the user must wait for the next code to appear.

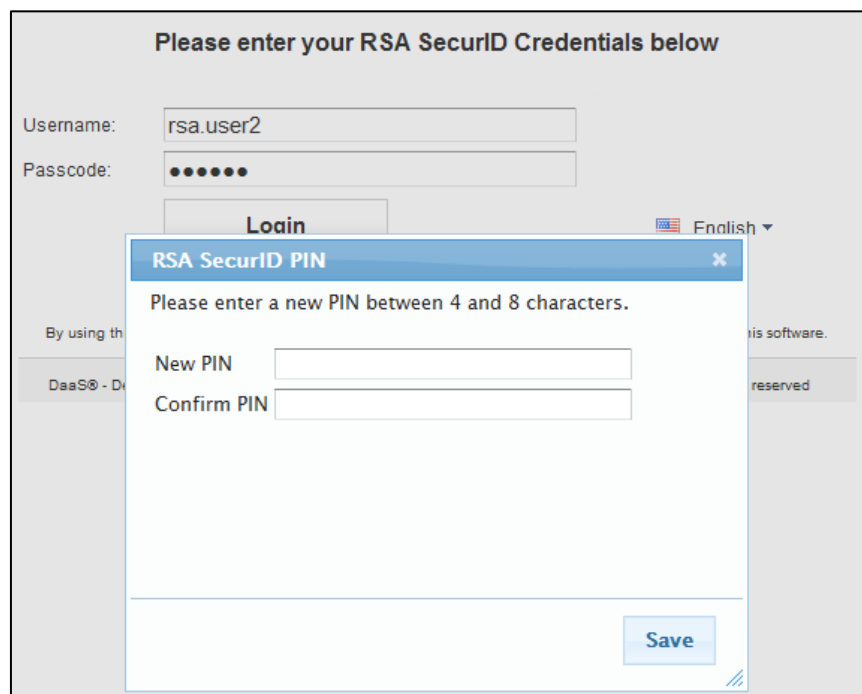
If the user makes three unsuccessful attempts, but on the fourth or fifth attempt correctly enters the code, the system prompts the user to enter the next code. For example:



**Note:** The WYSE P20 Thin Client allows only 8 characters when entering the next token code. These users should enter just the token code without the PIN in the Next Token Code field. Entering the PIN plus the token will exceed the character limit.

### 13.7.2 Establish an RSA SecurID PIN

If a company uses personal PINs, the first time a user logs in to the Portal, after entering the RSA passcode and clicking **Login**, the system displays the RSA SecurID PIN screen. For example:



Users either select their own PIN, or the New PIN field is pre-populated for them with a system generated PIN. The 4 – 8 character limit shown in the sample screen is an example only, the user's PIN character limit is established by the System Administrator.

When the user confirms the PIN and clicks Save, the system displays the standard login screen on which they enter their username, password, and domain. If a user refreshes the display before completing this final login step, the login is aborted and the user must begin the login process again by entering the username and RSA passcode on the initial screen. This prevents someone other than the user from logging in if the user happens to step away from their desk before entering the username, password, and domain.

## 13.8 Known Limitations of the RSA API

Some limitations exist around the RSA API. Most of these are a result of some caching that occurs once the API has started up.

- Changes to the RSA PIN policy will not take effect until the RSA Authentication Agent is restarted.
- Removing the securid file will not be detected until the RSA Authentication Agent is restarted.

**Note: The configuration page control which clears the local securid file also restarts the RSA Authentication Agent. This means that the only time this condition can occur is if someone manually removes the file from the tenant appliance.**

- Most Authentication and PIN change failures are generic in nature. They do not contain any information about why the authentication or PIN change failed.

# 14 Super Tenant

---

## 14.1 Overview

Horizon DaaS service providers and Managed service providers (MSPs) are increasingly targeting the SMB market. Creating a separate tenant for each customer will consume significantly more resources than might be necessary for customers who typically need no more than 20 desktops or sessions. MSPs prefer a shared tenant where they can provision each customer into its own pool, but maintain logical separation between the pools. This type of shared tenant will be referred to in this context as a Super Tenant.

It is assumed that the MSP will manage Enterprise Center, Active Directory, and user/group mappings to the pool on behalf of the individual customers. Some MSPs will also need to separate customers across hosts either for security reasons or for Microsoft licensing compliance.

**Note:** Please refer to the regular tenant install guide for further details.

## 14.2 Super Tenant Prerequisites

### 14.2.1 Networking Requirements

A Super Tenant must have a perimeter network (e.g. DMZ in Figure 2) where Horizon DaaS tenant appliances and other external facing components like the Horizon DaaS dtRAM are behind a firewall. The tenant administrator must create subnets for each customer to isolate. Each subnet must be labeled (typically with a customer id or name) to easily identify customers on hypervisors and the Horizon DaaS Platform. The administrator must configure these subnets so that traffic is allowed between the DMZ and customer subnets (e.g. N1C1 and N2C2 in diagram 2.5) and vice versa. The Administrator can use either DVS (Distributed Virtual Switch) or standard vSwitch networks within vCenter. It may be advantageous to use distributed virtual networking since the number of VLANs per datacenter is limited according network specifications (4096 VLANs or less).

### 14.2.2 Tenant Active Directory and DNS Configuration

The tenant administrator can use a single Active Directory to serve all customers by creating customer specific security groups. The domain controllers and DNS server must be in the DMZ network so that all customer assigned subnets can connect. Please check Microsoft recommended best practices for use of domain controllers across subnets.

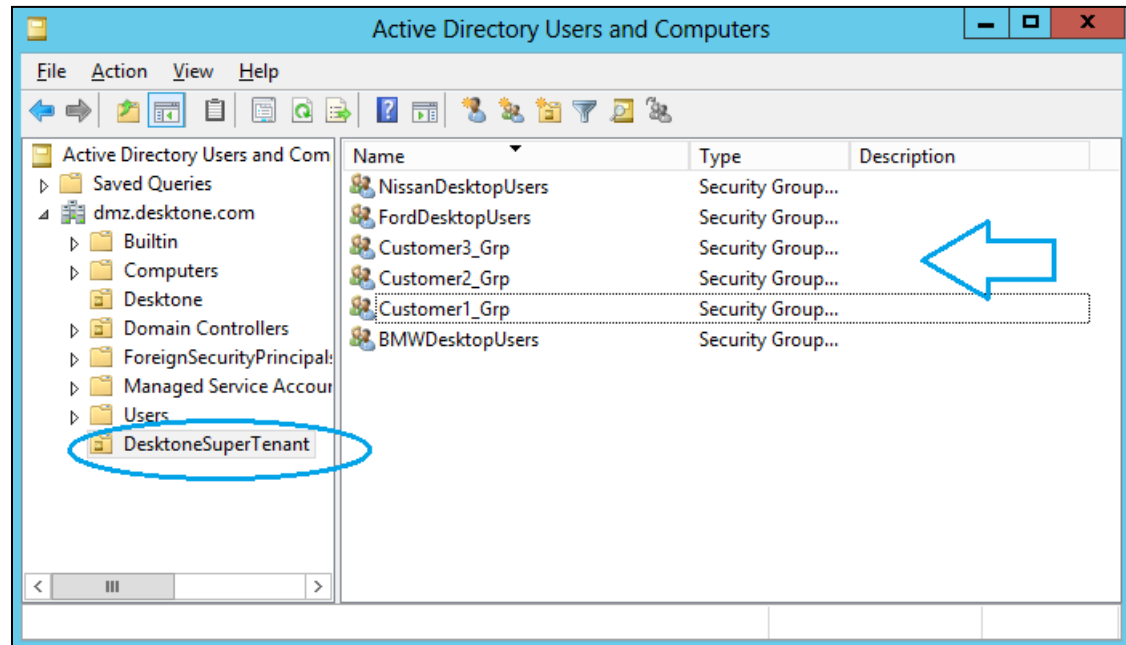
The administrator should create security groups for each customer to ease the user management and configuration in the Horizon DaaS Platform such as user mapping. Customers can be separated by creating Organizational Units with security groups under the OUs in Active Directory.

Example:

The figure below shows that the tenant administrator has created an OU named 'DesktonSuperTenant' in Active Directory, and created security groups for each customer such as Customer1\_Grp, FordDesktopUsers, etc.

The tenant administrator must then add each security group to the User Groups field on the Group Info tab of the Domain configuration.

### Sample Active Directory Structure



## 14.2.3 Tenant DHCP Configuration

The tenant administrator should configure DHCP considering the network topology of subnets. A single DHCP server can be used to serve all subnet desktop clients by utilizing BOOTP-relay agent capability of a network router, or having another computer that can function as a relay agent on each subnet.

Each DHCP scope should be verified to ensure the correct domain controller and DNS configuration for each network subnet.

Please refer to Microsoft recommendations and best practices to configure the DHCP server:

<http://technet.microsoft.com/en-us/library/cc771390.aspx>

## 14.2.4 Gold Pattern and DaaS Agent

### 14.2.4.1 Gold Pattern

The tenant admin should create a gold pattern and customize it per the customer's requirement. The admin can create individual gold patterns for each customer if required.

Important: Using a Windows client operating system image, such as Windows 7, in a Super Tenant may not be advisable due to Microsoft licensing restrictions. Specifically, the license associated with Windows 7 (also Windows XP and Window 8) requires that virtual instances run on isolated hardware per customer (e.g. Windows 7 instances for customer A and customer B cannot be on the same server or blade). A

popular approach due to the licensing restrictions is to use individual Windows Server instances skinned as Windows 7. This approach gives the end user a familiar desktop look and feel and also allows sharing of infrastructure with SPLA licensing. For further information please refer to Microsoft Windows licensing for virtualization at [microsoft.com](http://microsoft.com).

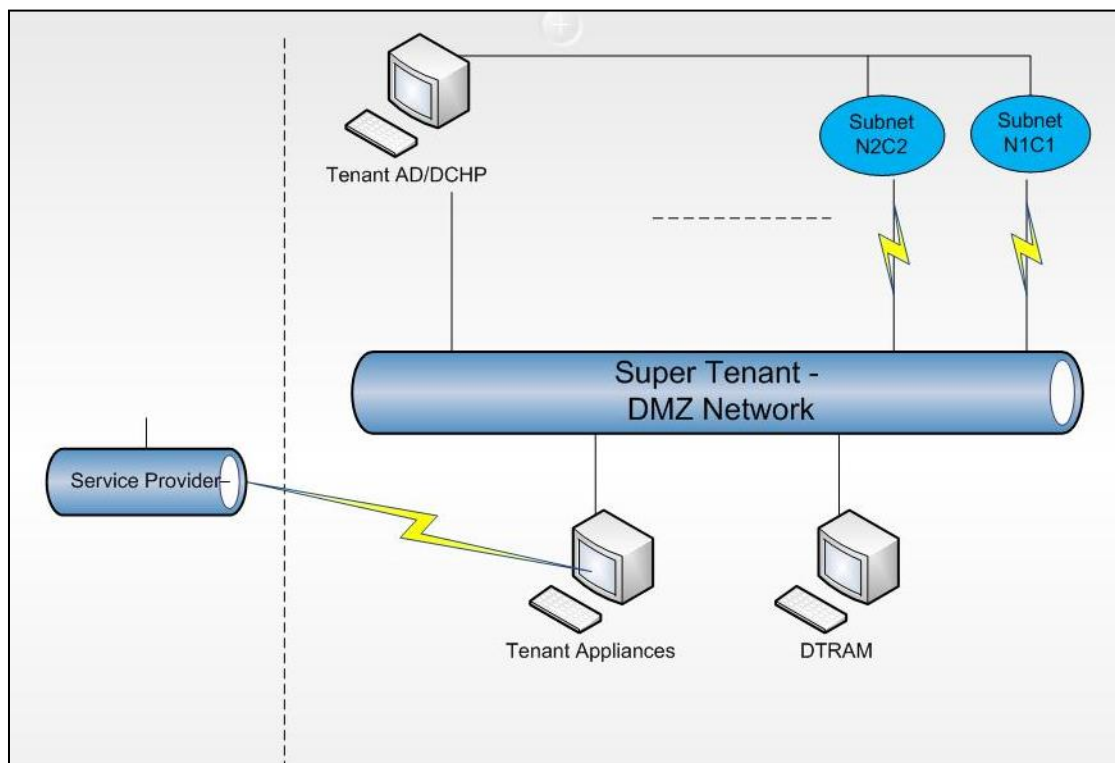
#### 14.2.4.2 DaaS Agent

The recommended way to deploy the DaaS Agent is to use tenant appliance auto discovery where a specific DHCP option code is used so that the DaaS Agent can automatically discover the IP addresses of the tenant appliances. This process is detailed in the Horizon DaaS Platform tenant installation guide. In our testing we've found that auto discovery does not always work on subnets other than the subnet where DHCP resides. As an alternative the standby address can be manually set in the MonitorAgent.ini file.

### 14.2.5 Tenant Infrastructure Overview Diagram

The figure below represents an overview of the Super Tenant network infrastructure. Horizon DaaS Platform communication between the tenant appliances and service provider appliances is done via backbone connectivity. This is standard for a non-Super Tenant as well. The Super Tenant has separate subnets (e.g. N1C1 and N2C2) for each customer. The subnet networks are isolated so that N1C1 network cannot access N2C2 network resources directly, but they can still connect to the DMZ network for communication with the tenant appliances and other tenant infrastructure components such as the domain controllers and DNS.

#### Tenant Infrastructure Overview



## 14.3 Service Center

This section describes the actions to be performed by the service provider admin in order to enable the Super Tenant.

### 14.3.1 Create a Super Tenant

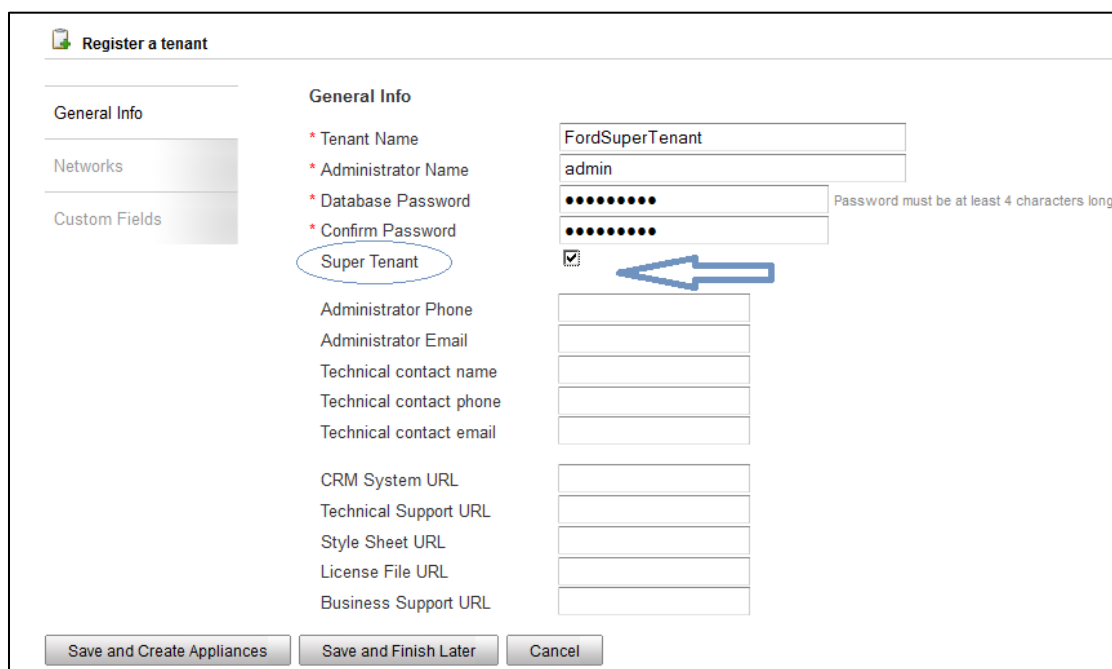
The service provider administrator should follow the steps below to enable Super Tenant capabilities at the time of tenant registration. Please make sure that you have prepared the required infrastructure for the Super Tenant as described above.

To enable the Super Tenant during initial registration, perform the steps below.

#### Procedure

1. Log in to the Service Center and click on the **Tenants** tab.
2. Click on the **Register a tenant** link and select the **Super Tenant** checkbox as shown in Figure 3.
3. Follow the normal tenant registration steps.

#### Enabling a Super Tenant during Registration



The screenshot shows the 'Register a tenant' form with a sidebar on the left containing 'General Info', 'Networks', and 'Custom Fields'. The 'General Info' section is active and contains the following fields: 'Tenant Name' (filled with 'FordSuperTenant'), 'Administrator Name' (filled with 'admin'), 'Database Password' (masked with dots), 'Confirm Password' (masked with dots), 'Super Tenant' (checkbox checked), 'Administrator Phone', 'Administrator Email', 'Technical contact name', 'Technical contact phone', 'Technical contact email', 'CRM System URL', 'Technical Support URL', 'Style Sheet URL', 'License File URL', and 'Business Support URL'. A blue arrow points to the 'Super Tenant' checkbox. At the bottom are three buttons: 'Save and Create Appliances', 'Save and Finish Later', and 'Cancel'.

### 14.3.2 Enable an Existing Tenant as a Super Tenant

A service provider administrator can also enable super tenant capabilities for an existing tenant. To enable the Super Tenant after initial registration, perform the steps below.

#### Procedure

1. Log in to the Service Center and click on the **Tenants** tab.
2. Click the **Edit** button for the tenant which you want to promote.

3. On the **General** tab, select the **Super Tenant** checkbox and click **Update** as shown in the figure below.

### Promoting an Existing Tenant to Super Tenant

Editing FordSuperTenant

General Custom Fields Quotas Remote Access Appliances Networks Entitlements Certificates

\* Tenant Name FordSuperTenant

\* Administrator Name admin

Super Tenant ☒

dtConsole Access [Show Info](#)

Administrator Phone

Administrator Email

Technical contact name

Technical contact phone

Technical contact email

CRM System URL

Technical Support URL

Style Sheet URL

License File URL

Business Support URL

[Update](#) [Back to List](#) [Delete Tenant](#) [Disable Tenant](#)

### 14.3.3 Add Networks for a Super Tenant


A service provider administrator must add networks to be used for Super Tenant customers in the Horizon DaaS Platform. To add networks, follow the procedure below.

#### Procedure

1. Log in to the Service Center and click on the **Tenants** tab.
2. Click the **Edit** button for the appropriate tenant.
3. Select the **Networks** tab and then click the **Add Network Component** link.
4. Enter the network details and click **Add Network Component** as shown in Figure 5.

**Note:** Fill in the **Network Label** field on the **Networks** tab with a user-friendly name associated with the tenant network. This field appears at pool creation time to allow you to associate a pool with a network.

## Adding Super Tenant Networks

 Editing AshSuperTenantFord

General Custom Fields Quotas Remote Access Appliances **Networks** Entitlements Certificates

Data Center: AshSuperTenantSP It is recommended that each VLAN not exceed 500 hosts. Add additional VLANs to aid in load balancing.

\* Network ID Type ☒ VLAN ☐ DVS

\* Network ID

\* Network Label

\* Gateway

\* DNS Server

\* Subnet Mask

Network ID	Network ID Type	Network Label	Gateway	DNS Server	Subnet Mask	Default	Action
112	VLAN	BMWNetwork	172.16.112.1	172.16.112.15	255.255.254.0	false	<input type="button" value="Delete"/>
115	VLAN	FordNetwork	172.16.110.1	172.16.110.17	255.255.255.0	false	<input type="button" value="Delete"/>
182	VLAN	VLAN182	172.16.182.1	172.16.182.15	255.255.255.0	false	<input type="button" value="Delete"/>
50	VLAN	VLAN50	172.16.50.1	172.16.50.17	255.255.255.0	false	<input type="button" value="Delete"/>
51	VLAN	SuperTenant51	172.16.51.1	172.16.50.17	255.255.255.0	true	<input type="button" value="Delete"/>

### 14.3.4 Disabling the Super Tenant Option

A service provider admin cannot disable the Super Tenant option for a tenant. This is by design.

## 14.4 Enterprise Center

This section describes the actions to be performed by the tenant admin in order to provide the customers of the Super Tenant with desktops or sessions. As a prerequisite to the steps detailed in this section, a gold pattern must be created to be used by the desktop and/or session pools. Since the gold pattern process is exactly the same as for a regular tenant, it is not described here. Please refer to the Enterprise Center help for further information on gold patterns.

## 14.4.1 Create a Desktop/Session Pool

The following section describes how to create a pool for a customer and assign the network. A pool is a group of VMs based on the same gold pattern and configurations.

### Procedure

1. Log in to the Enterprise Center.
2. Create a pool using one of the following methods:

#### Individual Desktop Based

- a. Select **Pool Management ► Create Pool ► Individual Desktop Based**
- b. To create a pool of desktops, select a desktop model to base this pool on. Desktop models are defined by your service provider. The desktop model specifies the desktop type, memory, and number of CPUs for each VM in the pool.
- c. Specify the Customer Id which is an identifier to differentiate customers which are managed under this Super Tenant.
- d. Select the Network assigned to this pool. The desktops will be configured to use this network.
- e. Specify the other pool characteristics as appropriate, and create the pool.

**Create New Pool**

Please fill in the Pool specifications below.

Data Center: BobSuperDC

\* Name: BMWPersPool

\* Desktop Model: Normal

\* Protocols: ☒ RDP ☐ PCoIP

Desktop Type: Static

\* Gold Pattern: BobSuperRDSP

Customer ID: BMW001

\* Network: BMW182

Based On: AudiDemoPool

Pool Size: 1 (9 Remaining)

Buttons: Clear, Review Pool, OR, Customize Pool

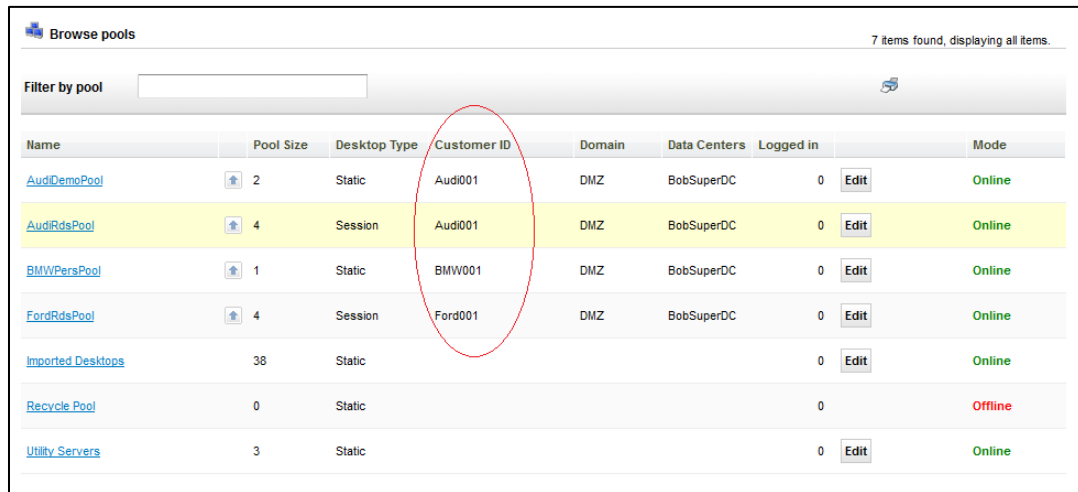
#### Session Based

- a. Select **Pool Management ► Create Pool ► Session Based**
- b. To create a session pool, enter the name for session pool and select a session profile, gold pattern for this pool.
- c. Specify the Customer Id which is an identifier to differentiate customers which are managed under this Super Tenant.
- d. Specify the Network assigned to this pool. The desktops will be configured to use this network.
- e. Specify the session count that pool should accommodate and verify the selected session host details.
- f. Specify the other pool characteristics as appropriate, and create the pool.

## 14.4.2 Browse Pool View

The Enterprise Center 'browse pool' tab displays a list of the pools along with other pool details. It also includes customer id. The Tenant administrator can export pool information to an Excel report by clicking the print icon on the browse pools page.

### Browse Pools



The screenshot shows the 'Browse pools' interface with a table of 7 items. The 'Customer ID' column is circled in red. The table has columns: Name, Pool Size, Desktop Type, Customer ID, Domain, Data Centers, Logged in, and Mode.

Name	Pool Size	Desktop Type	Customer ID	Domain	Data Centers	Logged in	Mode
<a href="#">AudiDemoPool</a>	2	Static	Audi001	DMZ	BobSuperDC	0	Online
<a href="#">AudiRdsPool</a>	4	Session	Audi001	DMZ	BobSuperDC	0	Online
<a href="#">BMWPersPool</a>	1	Static	BMW001	DMZ	BobSuperDC	0	Online
<a href="#">FordRdsPool</a>	4	Session	Ford001	DMZ	BobSuperDC	0	Online
<a href="#">Imported Desktops</a>	38	Static				0	Online
<a href="#">Recycle Pool</a>	0	Static				0	Offline
<a href="#">Utility Servers</a>	3	Static				0	Online

## 14.4.3 Desktop Pool Migration

The migration of desktops between pools is allowed only if the assigned network and other pool configuration matches.

## 14.4.4 RDS isolation

In a standard tenant, RDS servers can be shared between session pools that have the same session profile in order to optimally utilize the assigned resources. In a Super Tenant, RDS servers are isolated between individual customers for security reasons. In other words, any given RDS server is only ever used by a single customer.

## 14.5 Billing

The DtReportingManager now has an additional method 'SuperTenantBillingReports' and returns a collection of DtSuperTenantBillingReport records as described. Please refer to the Horizon DaaS Platform SDK for further information.

### DtReportingManager

Name	Description	Method	Relationship
SuperTenantBillingReports	Retrieves a list of super tenant billing reports based on the given DtBillingReportFilter	POST	association

### DtSuperTenantBillingReport

Collects billing data for super tenants by their customer ids.

## Links

There are no links in this object.

## Properties

Name	Description	Data Type
customerId	Sub-tenant customer ID pertaining to this record	String
desktopCount	List of desktop model to the in-use count of those desktop models by this customer in a super tenant. Count for each desktop model is wrapped within DtDesktopCountWrapper instances.	Collection of DtDesktopCountWrapper
organizationId	Organization ID of the super tenant	Long
sessionCount	Count of the number of sessions allocated to this customer	Long

## Sample Script output:

SUPER TENANT BILLING SUMMARY

ORG	CUSTOMER	TYPE	COUNT	DESKTOPMODELID
1001	Audi001	SESSION	4	
1001	Audi001	DESKTOP	2	1cb3f348-f987-4834-a33c-742ef30d356b
1001	Ford001	SESSION	4	
1001	BMW001	SESSION	0	
1001	BMW001	DESKTOP	1	1cb3f348-f987-4834-a33c-742ef30d356b

# Appendix A Connection Matrix

---

This appendix provides connection information for the Apex Horizon DaaS Platform release.

## Legend

Management Appliances		Other		Networks	
<u>Abbrev</u>	<u>Name</u>	<u>Abbrev</u>	<u>Name</u>	<u>Abbrev</u>	<u>Name</u>
SP	Service Provider	HYP	Hypervisor	T	Tenant Network
Resource Manager	Resource Manager	SS	Storage System	SP	Service Provider Network
T	Tenant	NFS	NFS Server	BB	Desktone Backbone Network
UP	Upload Server	VM	Virtual Desktop VM	I	Public Internet
RAM	dtRAM	EP	End Point Device		
		AD	Active Directory		
		MON	Monitoring System		
		RSA	RSA Authentication Manager		

<u>Source</u>	<u>Destination</u>	<u>Ports In Use</u>	<u>Networks</u>	<u>Description</u>	<u>Connectivity Type</u>
SP	SP	tcp/1098, tcp/1099, tcp/3873	BB, SP	Used for invoking remote APIs via Java RMI. Ports 1098 and 1099 are used for the naming service lookup and port 3873 is used for the actual remote method invocation. Authentication is done via username/password.	Local and Remote
SP	SP	tcp/11211	BB	Used for accessing memcached	Local Only
SP	SP	udp/694	SP	Periodic heartbeat between paired SP appliances (floating IP)	Local Only
SP	SP	tcp/5432	SP	Used to access the DB from the application, also replication	Local and Remote
SP	SP	tcp/22	BB, SP	Provides SSH and SCP capabilities to management appliances for purposes of installation and configuration. Authentication is done using a private/public ssh key registered to the appliance at installation time.	Local and Remote
SP	SP	tcp/20677	BB, SP	Used for proxying traffic between DCs	Local and Remote
SP	Resource Manager	tcp/8443	BB, SP	Used for invoking remote APIs via web services. Authentication is done via username/password and SSL certificate validation.	Local and Remote
SP	Resource Manager	tcp/22	BB	Provides SSH and SCP capabilities to management appliances for purposes of installation and configuration. Authentication is done using a private/public ssh key registered to the appliance at installation time.	Local Only
SP	T	tcp/1098, tcp/1099, tcp/3873	BB	Used for invoking remote APIs via Java RMI. Ports 1098 and 1099 are used for the naming service lookup and port 3873 is used for the actual remote method invocation. Authentication is done via username/password.	Local Only
SP	T	tcp/8443	BB	Used for invoking remote APIs via web services. Authentication is done via username/password and SSL certificate validation.	Local Only
SP	T	tcp/22	BB	Provides SSH and SCP capabilities to management appliances for purposes of installation and configuration. Authentication is done using a private/public ssh key registered to the appliance at installation time.	Local Only
SP	HYP	tcp/443	SP	Needed for access to the hypervisor management APIs. Authentication is done via username/password.	Local Only

SP	SS	tcp/22, tcp/80, tcp/443	SP	Used to invoke APIs on a storage system. The specific ports will vary depending on the type of storage system being used. Authentication is done via username/password.	Local Only
SP	NFS	tcp/2049	SP	Used to communicate with the NFS server. The SP mounts the NFS shares used to store the appliance template VM images for purposes of manufacturing and configuration. Authentication is done via network identity.	Local Only
SP	AD	tcp/389, tcp/636	SP	Used to authenticate users to the Service Center. The protocol choice of ldap or ldaps is decided by the SP administrator at the time of domain registration.	Local and Remote
Resource Manager	SP	tcp/8443	BB	Used for invoking remote APIs via web services. Authentication is done via username/password and SSL certificate validation.	Local Only
Resource Manager	SP	tcp/20677	BB	Used for proxying traffic between DCs	Local Only
Resource Manager	Resource Manager	tcp/11211	BB	Used for accessing memcached	Local Only
Resource Manager	T	tcp/8443	BB	Used for invoking remote APIs (state monitoring) via web services. Authentication is done via username/password.	Local Only
Resource Manager	HYP	tcp/443	SP	Needed for access to the hypervisor management APIs. Authentication is done via username/password.	Local Only
Resource Manager	SS	tcp/22, tcp/80, tcp/443	SP	Used to invoke APIs on a storage system. The specific ports will vary depending on the type of storage system being used. Authentication is done via username/password.	Local Only
Resource Manager	NFS	tcp/2049	SP	Used to communicate with the NFS server. The RMgr mounts the NFS shares used to store the tenant VM images for purposes of manufacturing and configuration. Authentication is done via network identity.	Local Only

T	SP	tcp/1098, tcp/1099, tcp/3873	BB	Used for invoking remote APIs via Java RMI. Ports 1098 and 1099 are used for the naming service lookup and port 3873 is used for the actual remote method invocation. Authentication is done via username/password.	Local Only
T	SP	tcp/8443	BB	Used for invoking remote APIs via web services. Authentication is done via username/password and SSL certificate validation.	Local Only
T	SP	tcp/20677	BB	Used for proxying traffic between DCs	Local Only
T	Resource Manager	tcp/1098, tcp/1099, tcp/3873	BB	Used for invoking remote APIs via Java RMI. Ports 1098 and 1099 are used for the naming service lookup and port 3873 is used for the actual remote method invocation.	Local Only
T	Resource Manager	tcp/8443	BB	Used for invoking remote APIs via web services. Authentication is done via username/password and SSL certificate validation.	Local Only
T	T	udp/694	BB	Periodic heartbeat between paired tenant appliances (floating IP)	Local Only
T	T	tcp/5432	BB	Used to access the DB from the application, also replication	Local Only
T	T	tcp/11211	BB	Used for accessing memcached	Local Only
T	VM	tcp/49152- 65535	T	Used for downstream communication between the DaaS Agent (on a Windows 7 and later virtual desktop) and the tenant appliance. A dynamically determined port in the range of 49152-65535 is determined at the time the agent logs on. Authentication is done via a session key exchange between the agent and tenant appliance.	Local Only
T	VM	tcp/1025-5000	T	Used for downstream communication between the DaaS Agent (on a Windows XP virtual desktop) and the tenant appliance. A dynamically determined port in the range of 1025-5000 is determined at the time the agent logs on. Authentication is done via a session key exchange between the agent and tenant appliance.	Local Only
T	VM	tcp/22	T	Required in the customization process for Linux virtual desktop provisioning (not required if not using Linux as a desktop O/S)	Local Only
T	VM	tcp/3389	T	Tenant appliance tests that the desktop is listening on port 3389 for RDP connections.	Local Only
T	VM	tcp/8443, tcp/443	T	For connection between the Horizon DaaS tenant appliance to the VMware View connection agent that runs in the desktop.	Local Only

T	AD	tcp/389, tcp/636	T	Used to authenticate users to the User Portal and the Enterprise Center. Additionally the configured user groups and their members are cached in the tenant fabric for performance purposes. The protocol choice of ldap or ldaps is decided by the SP administrator at the time of domain registration.	Local and Remote
T	RAM	tcp/8000	T	Used for invoking remote APIs on the dtRAM. This call happens only when a request to serve a desktop requires a tunnel. Note: port 8000 is the default port (configurable). Authentication is done via username/password.	Local Only
T	RSA	udp/5500	T	Used for communicating with the RSA Authentication Manager when SecurID is in use by the tenant. It is possible for the Authentication Manager to not be located in the same data center as the tenant appliances. An HA authentication manager used for failover could be located remotely as well.	Local and Remote
VM	T	tcp/8443, tcp/443	T	Used for upstream web services communication between the DaaS Agent and the tenant appliance. Authentication is done via username/password and SSL certificate validation.	Local Only
VM	T	udp/5678	T	Used for upstream communication between the DaaS Agent and the tenant appliance. Authentication is done via a session key exchange between the agent and tenant appliance.	Local Only
VM	KMS	tcp/1688	T	Access to the KMS server for purposes of licensing the version of Windows on the virtual desktop	Local Only
UP	NFS	tcp/2049	SP	Used for storing the desktop images uploaded from tenants to NAS. Authentication is done via network identity.	Local Only
MON	SP	tcp/5989	BB	Provides access to monitoring information via CIM-XML over https. This is available on all appliances and binds to all network interfaces. Best practice is to limit access on the backbone only. The interface is unauthenticated.	Local Only

MON	Resource Manager	tcp/5989	BB	Provides access to monitoring information via CIM-XML over https. This is available on all appliances and binds to all network interfaces. Best practice is to limit access on the backbone only. The interface is unauthenticated.	Local Only
MON	T	tcp/5989	BB	Provides access to monitoring information via CIM-XML over https. This is available on all appliances and binds to all network interfaces. Best practice is to limit access on the backbone only. The interface is unauthenticated.	Local Only
EP	VM	tcp/3389, udp/3389	T	Provides access to the virtual desktop via RDP	Local Only
EP	VM	tcp/1494	T	Provides access to the virtual desktop via HDX	Local Only
EP	VM	tcp/22	T	Provides access to the virtual desktop via NX	Local Only
EP	VM	tcp/4172, udp/4172, tcp/32111	T	Provides access to the virtual desktop via PCoIP	Local Only
EP	VM	tcp/22443	T	Provides access to the virtual desktop via HTML Access (Blast)	Local Only
EP	VM	tcp/42966	T	Provides access to the virtual desktop via RGS	Local Only
EP	VM	tcp/5900	T	Provides access to the virtual desktop via VNC	Local Only
EP	VM	tcp/80, tcp/443	T, I	Access to the web portals. If remote access is enabled the desktop portal needs to be made publicly available. Note that port 80 will redirect to 443.	Local (Remote w/dtRAM)
EP	RAM	tcp/8001-8050	I	Provides access to the virtual desktop via the dtRAM over the public Internet	Remote Only

## Appendix B Guest OS Support

SUPPORTED							
Operating System	Patch/ SP	32/64 Bit	VDI/ RDS	Additional Variants/Specs	Support added in 6.1	Remote Apps	Comments and Caveats
WinXP	SP3	32 only	VDI	Professional		NS	
Win7	Base/ SP1	Both	VDI	Professional/ Enterprise		Supported for RDP - Enterprise Only	Enterprise required for VDI Remote Apps over RDP
Win8.0		Both	VDI	Enterprise only		Supported for RDP - Enterprise Only	Enterprise required for VDI Remote Apps over RDP
Win8.1		Both	VDI	Professional/ Enterprise	X	Supported for RDP - Enterprise Only	Enterprise required for VDI Remote Apps over RDP
WinServer 2008r2	SP1	64 only	VDI/ RDS	Data Center Edition Only		Supported for VDI - RDP and RDSH -PCoIP	PCoIP on RDS supported in 6.1 only Win2008R2 Server supported for both VDI and RDSH
WinServer 2012		64 only	RDS	Standard (Tested), DataCenter (Supported/Not Tested)		Supported for RDSH - PCoIP	PCoIP on RDS supported in 6.1 only and requires 6.0.1 release of View Agent/VADC
WinServer 2012r2		64 only	RDS	Standard (Tested), DataCenter (Supported/Not Tested)	X	Supported for RDSH - PCoIP	PCoIP on RDS supported in 6.1 only and requires 6.0.1 release of View Agent/VADC

NOT SUPPORTED							
Operating System	Patch/ SP	32/64 Bit	VDI/ RDS	Additional Variants/Specs	Support added in 6.1	Remote Apps	Comments and Caveats
WinXP	SP3	64 only					Support no versions of XP other than SP3 - 32B
WinXP	SP2	Both					Support no versions of XP other than SP3 - 32B
Win2003 – Std/Enterprise	All	Both					
Win8.0		Both		Non-Enterprise			Only support Win8 Enterprise
WinServer 2008	Non R2	Both					Only support DataCenter, R2 version
Windows Vista	All	Both		Any variant			

Support for the following added in 6.1:

- Win81 for VDI desktops
- WinServer2012r2 for RDS hosts
- PCoIP support for RDS hosts and applications for Win2008r2, Win2012, and Win2012r2