Horizon DaaS 8.0.0 Service Provider Administration

VMware Horizon DaaS

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Horizon DaaS Service Provider Administration

1

The Horizon DaaS Service Provider Administration manual provides information on how to administer the Horizon DaaS system.

Intended Audience

This document is intended for experienced IT system administrators who are familiar with virtual machine technology and datacenter operations.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Service Provider Installation

2

This section provides you with information on how to install and configure the service provider appliances using vCenter discovery of the management compute resources

Note USING LANGUAGE SETTINGS OTHER THAN "ENGLISH" FOR BROWSERS WHILE ACCESSING THE SERVICE CENTER CAN CAUSE THIS INSTALLATION TO FAIL. TO AVOID THIS, USE ENGLISH BROWSER SETTINGS WHEN ACCESSING THE SERVICE CENTER.

In this installation, you complete the following:

1. Install the first service provider appliance in the datacenter.

   A DaaS appliance is a virtual machine combined with a functional unit of software in the DaaS platform. The service provider appliance provides two types of access to the system: via the Service Center web based UI; as a transit point for enabling ssh access to all the management appliances in the data center.

2. Bootstrap the service provider appliance. Once bootstrapped, the Service Provider Appliance provides the foundation to install the remainder of the DaaS application.

3. Start the Service Center on the DaaS Management Appliance and configure the Service Provider environment. Create a second service provider appliance for high availability (HA).

The Service Center provides a web-based UI for managing data center resources (hosts, storage, and the DaaS management appliances). You also use the Service Center to manage tenant contracts, configure tenant appliances and networks, and create and assign roles and permissions.

This chapter includes the following topics:

Service Provider Prerequisites

Before you can perform the installation, you first need to complete the tasks listed below.

Contact your customer service representative for help with any of these prerequisites.

Procedure

1. Build the network infrastructure required to support multi-tenancy, typically accomplished with:

   - VLAN tagging for network separation at layer 2.
   - VRFs to isolate tenants and allow for a separate routing table per tenant.

   The configured VLANs must be the same across all management hosts. In vCenter, there is an additional option of using distributed virtual switches (DVS). By integrating either the VMware vSphere Distributed Switch or the Cisco Nexus 1000V with vCenter, separation can be accomplished using distributed switch port groups. The port group must be configured to use ephemeral port binding.

2. Allocate at least two ESXi hosts or at least one cluster for DaaS management appliances.

   Install a vCenter management server meeting the version requirements. All ESXi hosts should have the compute (RAM, CPU, local disk) required to meet expected Tenant Appliance density.

3. Provide an account to access the hypervisor manager API.

   On the vCenter, configure an account which can be used to manage the virtual resources via the vSphere API. This account must have appropriate privileges.

4. Assign one subnet to the service provider network. This subnet also needs to have access to the API of the hypervisors.

5. Assign service provider network.

   Assign a VLAN, a VXLAN, or a Distributed Virtual Port Group (DVPG) to the service provider network. This VLAN or DVPG must map to a virtual network assigned to all management hosts.

6. Assign a network to be used for DaaS platform management traffic.

   Assign one VLAN (non-routable subnet), one VXLAN, or one Distributed Virtual Port Group (DVPG) as the Link Local Network.

7. Allocate link-local addresses.

   For a typical data center, it is recommended that you use a /22 network (for example, 169.254.16.0/22). However, a demo environment or small data center can use a /24 network. You should not use anything smaller than /24.

A link-local address is an IP address used only for communications within a link (segment of a local network) or a point-to-point connection to which a host is connected. Routers do not forward packets with link-local addresses. The address block 169.254.1.0 through 169.254.254.255 is reserved for link-local addressing in Internet Protocol Version 4. You cannot choose addresses outside this range. Refer to Internet Engineering Task Force (IETF) RFC 3927 for more information.

8 Allocate storage for management appliances.

By default, the System will clone out management appliances on local disk (via a local datastore). This is considered a best practice.

9 DNS Configuration

There must be a DNS server available from the Service Provider (SP) network which can be used to resolve the name of the domain so that the Service Center can authenticate. Confirm all vSphere servers are defined in the DNS and that the hosts and storage systems are configured locally with the matching DNS name as well.

10 IP Address Allocation

Allocate five IP addresses in the SP network: two for the Service Provider appliances plus one for the shared floating IP and two for the Resource Manager appliances. If the Service Provider wants to access the Service Center using a hostname instead of an IP address, setup a DNS record to point to the floating IP address of the Service Provider appliance pair.

11 NTP Configuration

There must be at least one NTP server available from the SP network to allow for time synchronization.

12 Active Directory Configuration

There must be an Active Directory accessible on the SP network for authentication. Have available the information listed in the table below to configure the domain for the Service Provider. It is highly recommended that you confirm the values using an AD tool such as Microsoft Active Directory Explorer, which can be downloaded from the Microsoft web site.

Configuration	Example
NETBIOS	SP
Domain Suffix	sp.desktone.com
Protocol	LDAP
Port	389
Context	dc=sp,dc=desktone,dc=com
Primary DNS Server IP and name	172.16.109.2 (You only need to specify one Domain Name Server - the rest should be automatically identified)

Configuration	Example
Service Account Used to parse your AD structure through a standard LDAP query - may be read only	CN= Administrator,CN=Users (UserMustChangePassword = false, Password Never Expires) (Do not include the context in the service account name)
Service Account Password	ADPasswd
Super Admin (Service Center Access)	cn=serviceprovideradmin,ou=groups (do not include the context)
Admin Level1 (Optional)	cn=Admin-1,cn=admins,ou=groups

13 SSL Certificate

Provide an SSL Certificate in Apache2 format to install for a valid certificate. For more details, see Apply Service Provider Certificate Files to Service Provider Appliances.

Required Files

Make sure you have all the files listed in the table below before you begin the installation. Contact your support representative for the necessary files.

File Contents	File(s)
Appliance Template	ApplianceTemplate_8_0_0_20180316.ova
Debians	av-manager-8.1.0-2788-airBAT.deb cloud-connector-client_1.3.0.deb dt-aux-8_0_0.deb dt-keybox_2.85.01.5171022.deb dt-platform-8_0_0.deb wem-service-diagnose-1.0.153.deb xmp-8.1.0-1937-airBAT.deb
DaaS Agent	VMware-DaaS-Agent-8.0.0-8159435.msi
Unified Access Gateway	UAG 3.2.1: ■ euc-unified-access-gateway-3.2.1.0-7766089_OVF10.ova ■ euc-unified-access-gateway-fips-3.2.1.0-7766106_OVF10.ova UAG 3.2: ■ euc-unified-access-gateway-3.2.0.0-7395815_OVF10.ova ■ euc unified-access-gateway-fips-3.2.0.0-7395812_OVF10.ova
Horizon Agent	VMware-viewagent-7.3.2-7161471.exe [32-bit] VMware-viewagent-x86_64-7.3.2-7161471.exe [64-bit]
vIDM Connector	identity-manager-connector-2018.1.1.0-7986908_OVF10.ova
vIDM SVA	identity-manager-3.2.0.0-8016174_OVF10.ova

Bootstrap Primary Service Provider (SP1) Appliance

This section includes the procedures for bootstrapping the primary service provider appliance.

Prepare Storage Configuration on Both Management Hosts

On both management hosts, add the Service Provider datastore. Be sure to use the same name on each host.

Note The name you use in vSphere for the storage needs to be exactly the same on each host and will be entered into the platform later.

Deploy the DaaS OVA File

On a DaaS Management Host, using the vSphere client, deploy two copies of the DaaS OVA file. The first copy becomes the primary Service Provider (SP1) appliance upon completion of the bootstrap process. The second copy becomes the template for all subsequent DaaS management appliances.

Note The Appliance Template needs to be on the same cluster as the SP1 appliance.

Prerequisites

Make sure that you have downloaded the DaaS OVA file (Appliance Template) specified in this document. You need to locate the file on a Windows drive accessible by the vSphere client in order to deploy it from the vSphere client. vSphere cannot natively mount a Linux partition or connect to an NFS share.

Procedure

1 Start the vSphere client.

2 Select **File > Deploy OVF Template** to deploy the first copy of the ova file, which becomes the first service provider appliance. The vSphere client launches the Deploy OVF Template wizard. The wizard has six steps. After completing each section, click **Next**.

   a Source: Browse for the OVA file you downloaded.

   b OVF Template Details: Click **Next** to skip this step.

   c Name and Location: Rename the VM with the name of the Service Provider Appliance you defined in the Service Provider Installation Worksheet, for example “DatacenterName-sp1”.

   d Storage: Deploy the SP1 Appliance to local/shared storage on one of the two management hosts.

   e Disk Format: Click **Next** to skip this step.

f Network Mapping: The first column lists the two Source Networks. For each, select a Destination Network. The first network (VM Network) should point to the Service Provider Network. The second network (Dev Network) should point to the Link Local Backbone Network.

g Properties: Enter a new password for the template. Note: Make sure that you note the password for later use and that you use the same one for both copies of the file.

h Ready to Complete: Click **Finish**. A dialog indicates the status of the deployment.

3 3. Select **File > Deploy OVF Template** again to deploy the second copy of the OVA file, which becomes the template for all subsequent DaaS management appliances.

In the wizard, specify the source of the OVA file (the same as in Step 2a), a name that distinguishes the file as the DaaS management appliance template, the service provider local/NFS storage, and the destination network (as defined in the previous step). We recommend you preface the name of your data center to the beginning of the appliance template name, for example “DatacenterName-template”. The name of the template must be unique across all datacenters. Also make sure that the password you enter in the wizard is that same as the one you entered for the first copy of the file.

Run the Bootstrap Script to Configure Network on SP1 Appliance

Run the bootstrap script to configure the network on the Service Provider appliance.

Procedure

1 From the vSphere client, power on the SP1 appliance and open the console window.

2 Log in using User: desktone Password: password you entered in the previous section.

Note For greater security, you should specify a custom appliance password when prompted by the bootstrap script.

3 Begin the bootstrap process by executing the following command:

```
sudo /usr/local/desktone/scripts/bootstrap.sh
```

4 The bootstrap script prompts you to enter network information for the fields listed in the table below. The values shown are sample values only. After you finish entering the network information, the host reboots. It might take five minutes for the appliance to start after reboot. Because the node is not configured until the reboot completes, disregard any error messages displayed on the console.

5 After the host reboots, you can login via putty or any other ssh terminal you choose.

6 Enter information at the prompts as described below.

Field	Sample Value	Notes
Enter Data Center Name	CityOfFirstDC	
Enter IP for eth1 (backbone)	169.254.4.20	For the Backbone network (must be a link-local address)
Enter netmask CIDR format 0-32	22	For the Backbone network
Enter IP for eth0 (SP)	172.16.109.20	For the SP network
Enter netmask CIDR format 0-32	24	For the SP network
Enter gateway for eth0 (SP)	172.16.109.1	For the SP network
Enter hostname	SP1.DESKTONE.COM	Match the name used for the IP on the SP datacenter.
Enter nameserver	172.16.109.2	
Enter NTP servers (separate servers by commas.) If you press enter for the first NTP server, [ntp.ubuntu.com] will be configured.	172.16.3.1	Enter a value only if you have a time server.
Enter IP for floating address	172.16.109.26	
Enter psql password	dtPasswd	Must have at least eight characters and contain at least one each of upper case letter, lower case letter, number, and special character. This alters the psql passwords for admin, master, slave and slony user. The password is not displayed on the screen.
Enter appliance password	myPasswd	Must have at least eight characters and contain at least one each of upper case letter, lower case letter, number, and special character. The user-defined password for Service Provider appliances in this datacenter. Any Service Provider appliance accessible by ssh requires this custom password.
Enter cim user password		Enter password for cim-user account. Only this account will have access to CIM monitoring services.
Does this configuration look correct?	yes or no	The information echoed back includes two internal values, Data Center UID and VMGR UID, which you can ignore.

Copy the DaaS Software to the Service Provider Appliance

Perform the steps below to copy the software to your service provider appliance.

Procedure

1. Log into the SP1 appliance via putty (or equivalent), using the following credentials.

   - User: desktone
   - Password: the appliance password you set previously.

2. Copy the following files to the /data/tmp directory on the SP1 appliance. (Do not copy the files to /data/repo at this time.)

   - av-manager-8.1.0-2788-airBAT.deb
   - cloud-connector-client_1.3.0.deb
   - dt-aux-8_0_0.deb
   - dt-keybox_2.85.01.5171022.deb
   - dt-platform-8_0_0.deb
   - wem-service-diagnose-1.0.153.deb
   - xmp-8.1.0-1937-airBAT.deb

3. At the appliance command prompt, move the files into the /data/repo directory on the appliance by running the following for each debian file:

   ```
   sudo mv /data/tmp/<name of debian file> /data/repo
   ```

Run Bootstrap Script to Install the DaaS Software

You must run the bootstrap shell script a second time to install the DaaS software.

Procedure

1. Run the bootstrap shell script:

   ```
   sudo /usr/local/desktone/scripts/bootstrap.sh
   ```

   System reboots.

2. SSH into the system again and wait for the log file to appear and watch desktone.log file:

   ```
   tail  -f  /var/log/desktone/desktone.log
   ```

   The system is up when you see a message similar to this in the log:

   ```
   Appliance deployed flag set to started
   ```

3 Open a browser and log into https://172.16.109.xxx/service, or whatever IP you supplied for “IP for eth0 (SP)” above.

Note It might take five minutes for the appliance to start after reboot. Because the node is not configured until the reboot cycle completes, you can disregard any error messages displayed on the console.

Configure Service Center

This section includes procedures for setting up Service Center in your environment.

Start the Service Center

Start the Service Center by entering the URL or IP address in a browser. For example: https://<IP for eth0 (SP)>/service Replace <IP for eth0 (SP)> with the IP address that you specified previously.

Note You can safely ignore the warning about the website’s security certificate and proceed to the Service Center page.

Register the Service Provider Domain

The first time you access the DaaS Service Center, the Register a domain page displays so that you can provide Microsoft Active Directory domain information.

You enter the information on two tabs: Domain Bind and Group Info. This information is required to access Microsoft Active Directory and to authenticate users. Make sure you have the DN information available to register the domains.

Note You must enter all information on both tabs (Domain Bind and Group Info) without letting your browser session expire. If you need to enter the information on the second tab (Group Info) at a later date, make note of the URL of the first tab (Domain Bind) so that you can navigate back to the Register a Domain page

Procedure

1 On the Register a Domain page, Domain Bind tab, enter values for the fields listed in the table below.

Table 2-1.

Field	Sample Value
Name	SP
Domain Suffix	sp.desktone.com
Protocol	LDAP
Directory Server Name	MicrosoftAD (leave this default, you do not need to select a Directory Server Name)

Table 2-1. (continued)

Field	Sample Value
Port	389
Domain Controller IPs (DNS Server)	172.16.109.2
Context	dc=sp,dc=desktone,dc=com
Domain Bind Account DN	CN=Administrator,CN=Users (do not include the context)
Password	ADPasswd
Password Verify	ADPasswd

2 Click **Save**.

3 On the Register a Domain page, Group Info tab, start typing a value for Admin Groups. The system will offer suggestions for auto-complete. For example, cn=serviceadmins,ou=groups.

4 Click **Save**.

The Service Center login page displays.

5 Enter your username, password, and domain then click **Login**.

Discover the DaaS Management Server

When you log in, the Discover Management Server page is displayed. Use this page to discover the vCenter Server which holds the DaaS Management Appliance Template (.ova file) you imported. The template is used for creating DaaS management appliances.

Procedure

1 Enter values for the fields listed in the table below. Enter the IP address or FQDN of the vCenter Server that is hosting the SP1 appliance.

Field	Sample Value
IP Address/Hostname	mgVC1.domain.desktone.com
Username	root
Password	vCenterPasswd

2 Click **Discover Server**.

The system prompts you to accept the certificate for the vCenter.

3 Click **Accept**.

The system indicates it is discovering host and calculating capacity.

4 Select the Compute Resource(s) (ESXi hosts or Cluster) you have set assign for DaaS Appliances. These will be used to provision Appliances.

Note A minimum of 2 ESXi hosts is required for high availability (HA). A cluster is considered to be HA on its own.

For each selected Compute, a dialog appears. If the server is too small to accommodate the ratios, you may be prompted to re-configure them.

5 Make any desired changes to the ratios and/or the Usage setting. Usage options are as follows:

- Service – SP appliance
- Tenant – Tenant appliance(s)
- Network – setting not active

6 Click **Save** to save the values.

A VM list will be displayed containing all the VMs from the compute selected as part of step 5.

Note Only VMs from the "Service" cluster are shown for the Appliance Template.

7 Select the DaaS appliance template from this list.

Note This should NOT be the Service Provider appliance itself, but should be the Appliance .ova that was deployed earlier.

Results

Once the system has discovered the appliance template, the Browse Tenants screen is displayed.

(Optional) Rename Resource Manager

You can rename a resource manager by performing the steps below.

Procedure

1 In the Service Center, select **service grid > resources**.

2 In the Resource Managers panel on the left, click on the IP address of the resource manager.

3 On the General tab, in the Name field, double-click on the IP address of the resource manager.

A text box opens in which you can change the name.

4 Change the name to the user friendly name, for example “Service Provider RMGR” and click **OK**.

Create the Remaining Service Provider Appliances

Horizon DaaS requires that Service Provider management appliances be installed as High Availability (HA) pairs.

To ensure physical hardware high availability, HA DaaS Management appliance pairs are distributed across two physical DaaS Management Hosts. With vCenter, the appliances are automatically distributed to the management hosts you selected.

Create HA Service Provider (SP2) Appliance

Perform the steps below to create the second service provider (SP2) appliance.

Procedure

1 Select **service grid > data centers**.

2 Click the **Edit** button (at end of line for new data center).

The system displays the Edit Data Center popup.

3 Verify the displayed information and click **Add Appliances**.

The Appliance Install screen displays.

4 Select **Service Provider Appliance** from the Appliance Type drop-down and enter values for the fields listed in the table below.

Field	Sample Value	Notes
Name	SP2	Do not use fully qualified domain name.
IP Address	172.16.109.21	

5 Enter values for the New Reservation fields listed in the table below.

Field	Sample Value	Notes
Friendly Name	Create SP2	
Start Date		Select Today from the drop-down or enter the month, day, and year.
Start Time		Enter 00:00 to indicate now, or the actual time in UT format.

6 Click **Create Appliance**.

7 To check the status of a reservation, select **appliances > reservations**.

Apply Service Provider Certificate Files to Service Provider Appliances

The DaaS platform allows you to upload custom SSL certificates for each service provider appliance. To enable a custom certificate, you upload three certificate files in Apache format: SSL Certificate, SSL Key, and CA Certificate.

Note To upload the three certificate files, you navigate to the Certificates tab under configuration (this is a different Certificates tab than the one used for tenants).

Procedure

1. In Service Center, select **configuration > general**.
2. Select the **Click here** link.
3. Click the **Certificates** tab.
4. On the Certificates tab, browse for and select the following three files:
   - CA Certificate: The public certificate from a certificate authority that was used to sign the service provider certificate. This file will have a .pem or .crt extension.
   - SSL Certificate: The service provider’s public certificate, which was signed by the CA. This file has a .crt extension, which indicates that it is a certificate file.
   - SSL Key: The private key used to decrypt the service provider’s SSL certificate. This is needed in order to be able to respond to certificate requests. This file has a .key file extension.
5. Click **Submit** to upload the files.
6. Select the **Click here** link to install the certificate on the service provider appliances.

   Note the following:

   - To get the SSL Certificate file the service provider administrator should submit a certificate sign request to their certificate authority. Their certificate authority will provide the administrator with a certificate file (.crt) which can be provided to the DaaS service provider to be uploaded. For more information on how to get a signed certificate, contact the certificate authority.
   - If the IP address or URL for the Service Center does not resolve to the service provider CN in their certificate, the service provider administrator may wish to include in their certificate a Subject Alternative Name so that the desktop portal's URL accessed by web clients can be matched to the uploaded service provider certificate. For more details on how to add a Subject Alternative Name to the certificate, contact the certificate authority.

Add Tenant Resource Manager

Perform the steps below to create a tenant resource manager appliance.

Procedure

1 In the Service Center, select **service grid > data centers**. The Data Centers page appears.

   The page contains a table of the available data centers.

2 Find the line for your data center and click **Edit**.

   The Edit Data Center popup appears.

3 Click **Add Appliances**.

   The Appliance Install page appears.

4 In the Appliance Type drop-down, select **Resource Manager**.

   The page displays the data entry fields for the Primary and Secondary resource managers.

5 Enter values for the fields listed in the table below. The IPs belong in the Service Provider network (not the link-local network).

Field	Sample Value
Primary Name	RMGR1
Primary IP	172.16.109.22
Secondary Name	RMGR2
Secondary IP	172.16.109.23

6 Enter values for the New Reservation fields listed in the table below.

Field	Sample Value	Notes
Friendly Name	Create RSMGR	
Start Date		Select Today from the drop-down or enter the month, day, and year.
Start Time		Enter 00:00 to indicate now, or the actual time in UT format.

7 Click **Create Appliance**.

   To check the status of a reservation, select **appliances > reservations**.

8 Select **service grid > resources** to see the tenant resource manager once it is up and running.

(Optional) Give the Tenant Resource Manager a Friendly Name

You can give a tenant resource manager a friendly name by performing the steps below.

Procedure

1 In the Resource Managers panel on the left side of the page, click on the IP address of the new resource manager.

2 On the General tab, in the Name field, double-click on the IP address of the resource manager.

A text box opens in which you can change the name.

3 Change the name to the user friendly name, for example “Tenant RMGR” and click **OK**.

Define Standard Capacities and Desktop Models

This section describes how to define standard capacities and desktop models.

Select **configuration > Standard Capacity** to open the Desktop Capacity & Model Definition page. This page lists the currently defined Standard Capacities and Desktop Models.

- The definition of the standard capacity currently selected in the Standard Capacity list is shown under Capacity Definition.
- Desktop Models are listed by name, along with the number of capacity units each includes.
- Each standard capacity defined on the left side of the page can be used as a 'capacity unit' for creating new desktop models.

Define a New Standard Capacity

Perform the steps below to define a new standard capacity.

Procedure

1 Click "+" above the Standard Capacities list.

2 In the Capacity Definition dialog, enter a name for the new standard capacity.

3 Under Capacity Definition, enter the following information:

   - Enabled - Indicates whether the standard capacity is enabled.
   - vCPU - Number of virtual CPUs.
   - vRAM - Amount of virtual RAM in MB.
   - vGPU - Size of virtual GPU. Select a value from the drop-down list.
   - HD - Hard disk size in GB.
   - Display - Display name for the standard capacity.

4 Click **Add Desktop Capacity**.

Edit or Enable/Disable a Standard Capacity

You can edit, enable, or disable an existing standard capacity.

To edit or enable/disable a defined standard capacity, select it in the Standard Capacity list, make changes under Capacity Definition, and click **Add Desktop Capacity**.

Create a New Desktop Model

Perform the steps below to create a new desktop model.

Procedure

1. If there is more than one standard capacity defined, select the one you want to use in the Standard Capacity list on the left of the page.
2. Click "+" above the Desktop Models list.
3. In the Model Definition dialog, enter the following information:
   - Name - Name for the desktop model.
   - Standard Capacity - Number of capacity units per desktop. The capacity unit in use is defined in the currently selected Capacity Definition.
   - Session - Indicates whether the desktop model is session-based. Choose Yes to provision remote desktop connections using Microsoft RDS (Remote Desktop Services). In this model, the Service Provider determines the type of services available to the Tenant and every desktop is identical, supporting the same applications. The user cannot install applications or customize the environment.
   - Enabled - Indicates whether the desktop model is enabled.
4. Click **Save**.

   Note After adding a desktop model, you need to go to the Quotas tab of the Edit Tenant screen to enable and enter a value for Standard Capacity.

Edit or Enable/Disable a Desktop Model

You can edit, enable, or disable an existing desktop model.

To edit or enable/disable a desktop model, select it in the Desktop Model list, make changes in the Model Definition dialog, and click **Save**.

Note If you change a desktop model, the changes will apply only to new pools that use the desktop model. The changes will not apply to existing pools created using the desktop model.

Tenant Installation

3

Horizon DaaS allows you to manage your tenant desktops using VMware vCenter hypervisor management software. This section provides you with instructions for installing and configuring a Tenant appliance in a datacenter using vCenter after you have installed or upgraded and configured the Service Provider appliance and Resource Manager.

A Tenant Installation Worksheet is included at the end of this section to help you collect and organize all the information needed to complete the install. Please consider that the installation process explained in this section is dedicated to standing up a tenant in Horizon DaaS. However, a successful tenant launch also needs to take into consideration items such as VDA licensing and image requirements and preparation. Please contact VMware support for further guidance with developing your own tenant on-boarding processes.

Note USING LANGUAGE SETTINGS OTHER THAN "ENGLISH" FOR BROWSERS WHILE ACCESSING THE SERVICE CENTER CAN CAUSE THIS INSTALLATION TO FAIL. TO AVOID THIS, USE ENGLISH BROWSER SETTINGS WHEN ACCESSING THE SERVICE CENTER.

This chapter includes the following topics:

Tenant Installation Prerequisites

This section describes prerequisites for tenant installation.

Note The prerequisites are slightly different depending on whether the tenant will have VPN backhaul to the customer network for services or applications.

Discover and Assign vCenters

Perform the tasks below to configure an account in the vCenter for Horizon DaaS to manage the virtual resources via the vSphere API.

- Discover one or more vCenter servers for Tenant desktops.

- Assign one of these vCenters to the Tenant Desktop Manager via the Service Center Service Grid. There is a limit of 1 vCenter per Desktop Manager.

Note You can use the same vCenter for both your management appliances and tenant desktops or you can use separate vCenters for each.

Note The datastores configured on each vSphere ESXi or cluster within a vCenter Datacenter must be the same. Shared storage is required for desktop VMs. In order for this to work properly, datastores must be created and mapped to the same LUNs on all the desktop hosts for a particular tenant with the same datastore name (case sensitive).

Set Up Enterprise Network Connectivity

Connectivity in this context refers to VPN/MPLS.

If the tenant requires backhaul then configure VPN access (IPSEC Tunnel, MPLS Circuit) from the tenant network back to the customers network that houses, for example, their AD, DNS, and DHCP as well as any other applications required by the virtual desktop users.

Configure Tenant Network

Perform the tasks below to define the tenant network.

- If the tenant has backhaul, work with the tenant to identify an internal subnet that is not in use in their infrastructure to be used for the virtual desktops. Otherwise assign an appropriate subnet to the tenant network.
- Add VLAN(s), VXLAN(s), or a Distributed Virtual Port Group (DVPG) to the tenant. At least one of these must be the Tenant Network.
- Assign at least one of the added network(s) to the Desktop Manager via the Service Grid in the Service Center. These networks will be used to ensure desktop isolation and may be shared across multiple Desktop Managers.

Note DVPG must be configured to use ephemeral port binding.

Important:

Configure DNS

You must define or install a DNS server for the tenant.

There must be a DNS server available from the tenant network which can be used to resolve the name of the domain so that the tenant can authenticate.

Allocate Tenant IP Addresses

Allocate IP addresses as follows.

A minimum of 3 IP addresses should be allocated on the tenant network. Additional IPs will need to be allocated for scenarios where multiple Desktop Managers are required.

- Two IPs for the management appliances themselves
- One IP to be shared between the appliances
- (Optional) One IP if the tenant has backhaul to a DHCP server. This will be used for the DHCP relay service

Define or Install DHCP Service for the Tenant

Perform the tasks below to set up DHCP for the tenant.

- A DHCP helper/relay is required to deliver the DHCP requests over the VPN tunnel to the tenant network. This can be done directly on the switches to which the hosts are attached or if not possible, a small Linux appliance can be configured in the tenant to perform this function.
- Configure the DHCP scope for the desktop subnet, starting at x.x.x.30.
- Configure DHCP option code 74 (IRC Chat) to point to the two IPs allocated for the tenant appliances. For example, if you are using a Windows server to provide DHCP service:

  a Open the DHCP configuration client from **Control Panel > Administrative Tools**.

  b Right-click **Server Options** and select **Configure Options** from the pop-up menu

  c If you have defined limited address scopes, you can confine the options configuration to a particular scope. Click on the scope and right-click on **Scope Options** to configure the 074 option code for that scope only. Configuration is the same as for the whole DHCP server.

  d Scroll down to the 074 option for Internet Relay Chat (IRC) and check the box.

  e Add IP addresses for tenant appliances.

Configure Active Directory

Define or install tenant Active Directory as shown below and have the information ready to be used during the installation.

Table 3-1.

Field	Description
NETBIOS Name	Active Directory domain name
DNS Domain Name	Fully qualified Active Directory domain name
Protocol	LDAP
Bind Username	Domain administrator
Bind Password	Domain administrator password
Port	The default for this field is 389. You should not need to modify this field unless you are using a non-standard port.

Table 3-1. (continued)

Field	Description
Domain Controller IP	(Optional) Specify a single preferred domain controller IP address if you want AD traffic to hit a specific domain controller.
Context	This field is auto-populated based on the DNS Domain Name information provided earlier.

It is highly recommended that you confirm the values using an AD tool such as Active Directory Explorer, which can be downloaded from the Microsoft web site.

Apply SSL Certificate

If the tenant requires a certificate, you will need the necessary certificate files in Apache SSL format.

For more details, see Apply Tenant Certificates to Tenant Appliances.

Set Up File Shares

File shares are used to allow the import of Agent update software and AppStacks.

- File shares can be in the same domain as the Active Directory that is added to the system. They can also be part of a CIFS share.
- The system must have read permissions on your file shares.
- AppStacks which are already present in the file share are imported automatically when the file share is added. For more information, see the Administration Console help.

  Note Once you create a file share, you cannot remove it. If you entered the wrong file path, just edit the file share from the Administrator console and import it again.

For more information, see the Settings section of the Tenant Administration guide.

Tenant Installation Procedures

This section includes the tasks required for tenant installation.

Create Tenant Appliances

Perform the tasks below to create tenant appliances.

Procedure

1. In Service Center, select **tenants > register a tenant**.

   The Register a tenant page displays.

2 On the General Info tab, the only required fields are the Tenant Name, Administrator Name, and Database Password. Enter this information and any of the non-required field data that you want to maintain.

3 On the Networks tab, next to the data center drop-down, click **Add** and enter values for the fields listed in the table below (for both primary and secondary).

The default networking option is to use VLANs mapped to virtual networks on each of the vSphere hosts. When using vCenter there is an option of using distributed virtual switches (DVS). This is an install time decision and cannot be changed after the tenant has been installed.

Field	Sample Value	Notes
Network ID	115	VLAN ID, VXLAN ID, or DVPG Name
Network ID Type	VLAN	VLAN, VXLAN, or DVS
Network Label	My Network	Free Form Text Field
Gateway	172.16.115.1	
DNS Name	172.16.115.2	Directory Name server
Subnet mask	255.255.255.0	

4 On the Custom Fields tab, enter any site-specific information you want to maintain. These are free-form text fields with no data validation.

5 After entering your information on the General Info, Networks, and Custom Fields tabs, select **Save and Create Appliances**.

6 Enter values for the fields listed in the table below (primary and secondary).

Field	Sample Value	Notes
Primary Name	TenantNode1	User-friendly name
Primary IP		
Secondary Name	TenantNode2	User-friendly name
Secondary IP		
Floating IP Address		
Start Date/Time		

7 Wait for the system to spawn your tenant appliances (time will vary depending on infrastructure). To check the status of a reservation, select **appliances > reservations**.

8 Verify that the appliances were created.

Add Desktop Compute Resources

Perform the steps below to add desktop compute resources.

Note If you are using the same vCenter to host your management appliances and tenant desktops, you do not need to complete this section. This is because you have already discovered the vCenter when setting up your management appliances. Instead, continue to Assign Resources to Tenant below.

If you are using separate vCenters for management appliances and desktop hosts, you must complete this section to add a physical desktop host for the tenant desktops. This host will be used for:

- Importing your initial starter desktop.
- Hosting your assignments (pools).

Procedure

1 In Service Center, select **service grid > resources** to display the Resources screen.

The left side of the screen displays three panels: Resource Managers, Desktop Managers, and Compute Resources.

2 Select the Compute Resources panel. The page redisplays with the Add Host Manager tab next to the General tab.

3 Click the Add Host Manager tab and enter values for the fields listed in the table below.

Field	Sample Value
IP Address/Hostname	Enter the DNS name or IP address of the Desktop vCenter.
User name	Administrator
Password	vCenterPsswd
Resource Manager	Select the tenant resource manager from the drop-down

4 Click the **Add** button.

The system prompts you to accept the certificate for the vCenter.

5 Click **Accept**.

6 When prompted, accept the certificate.

Note The assignment of individual ESXi or Cluster resources within this vCenter Datacenter to a particular Desktop Manager will be made after this step.

Assign Resources to Tenant

Perform the steps below to add resources to the tenant.

Procedure

1. In Service Center, select **service grid > resources**.
2. Select the Desktop Managers pane.
3. Select the appropriate Desktop manager listed in the Desktop Managers panel by clicking on the name in the tree.

   Note You may need to click refresh if the expected Desktop Manager is not present.

4. Click on the Compute Resources tab, and click **Assign** on the vCenter you have setup for the Tenant Desktops
5. A list of both clusters and ESXi hosts will be displayed. Select one or more of the desired compute to be assigned to the Desktop Manager. Click **OK** when done.

   For each selected compute resource, a capacity popup will display.

6. Review the overallocation settings and click **Save** if satisfactory.

   Note If the server capacity is not enough to meet the current usage base on overallocation, you will need to increase overallocation or decrease the amount of VMs on the compute.

Assign Networks to Desktop Manager(s)

Perform the steps below to assign networks to your desktop manager(s).

Procedure

1. In Service Center, select **service grid > resources** to display the Resources screen and select the Desktop Managers tab

   On the tab, desktop managers are listed as <tenant name>_<desktop manager name>.

2. Click on the desktop manager and select the Networks tab.

   Note This tab will only be displayed once Compute Resources have been assigned and will only display networks that are available across all assigned compute resources. If you do not see a network that you expect, validate that the network is available and labelled correctly across all compute resources.

3. Click assign on at least one network.

   The assigned networks effect what VMs will be detected as belonging to the Desktop Manager.

Configure Datastores

The Datastores tab is used to specify datastores for your system to use.

Procedure

1 In the Service Center, select **service grid > resources** to display the Resources screen and select the Desktop Managers tab

  In the tab, the desktop managers are listed as <tenant name>_<desktop manager name>.

2 Select a desktop manager and then select the Datastores tab.

3 Double-click in the appropriate field (Desktop Primary Storage, Desktop Auxilliary Storage) .

4 Enter a regular expression for the name(s) of the datastore(s).

  Note In order for a datastore to be added, it must first be configured on a Compute Resource.

Configure User Licenses and Desktop Capacity

Perform the steps below to configure user licenses and desktop capacity.

Procedure

1 In Service Center, select **tenants > browse tenants**.

2 In the table, click **Edit** for the tenant which you wish to edit.

  The Editing Tenant page displays.

3 Select the Quotas tab.

4 Under User License, select one of the following two options and enter a value for it.

  - Concurrent - Maximum number of concurrent users permitted.
  - Named - Maximum number of named users permitted.

5 Under Desktop Capacity, edit values as described below.

  Note Not all values are editable.

  - Data Center - Select data center from drop-down list.
  - Std Capacity - Indicates maximum number of desktops. In Use value shows number currently in use.
  - Storage Capacity - Shows current storage capacity (not editable).
  - Implicit Desktop Storage - Shows implicit desktop storage (not editable).
  - Add-on Storage - (Optional) Enter value for add-on storage in GB.
  - Desktop Manager - Select desktop manager from drop-down list.
  - Template Quota - Enter/change value for template quota. In Use value shows number currently in use.

Set Up Desktop Connection Via Unified Access Gateway

Perform the steps below to set up the desktop connection.

Note the following:

- VMware Unified Access Gateway is the new name for VMware Access Point.
- You cannot deploy a Unified Access Gateway VM from a vSphere Windows client. You must deploy it from the vSphere web client.

Procedure

1 Download the latest version of the Unified Access Gateway OVA file.

2 Determine the IP addresses (DNS/Netmask/Gateway) for the required networks, as described below.

Configuration	Networks
3 NIC	Internet Any network with internet access Management - This can be your 169 network. Since this does not have its own DNS or Gateway, you can enter any numbers for DNS and set the netmask to 255.255.255.0 Backend - Network that the Tenant uses for desktops
2 NIC	Internet - Network the Tenant is on Management - This can be your 169 network. Since this does not have its own DNS or Gateway, you can enter any numbers for DNS and set the netmask to 255.255.255.0
1 NIC	Internet - Network that the Tenant is on

3 In the vSphere web client, follow the normal method for deploying a template. On the Properties page, enter information as shown below.

Field	Value
Root Password	Enter initial password for root user. Password must be at least eight characters long and must contain: ■ At least one upper case letter ■ At least one lower case letter ■ At least one number ■ At least one special character (!, @, #, etc.)
Admin Password	Enter password to be used for REST API Admin user
Locale	en_us
Settings JSON	Leave blank
View Destination URL	Leave blank
View Destination URL Thumbprints	Leave blank

Field	Value
View Proxy Pattern	Leave blank
DNS	Enter DNS of Internet network
Internet IP Address	Enter Internet Network IP address from the previous step
Management Network IP Address	If configuration is 3 NIC or 2 NIC, enter Management Network IP from the previous step. If configuration is 1 NIC, this item does not display.
Backend Network IP Address	If configuration is 3 NIC, enter Management Network IP from the previous step. If configuration is 1 NIC or 2 NIC, this item does not display.

4 Power on the VM and wait for the login screen to appear on the console.

5 On the tenant appliance, run the following command:

```
sudo /usr/local/desktone/scripts/apsetup.sh
```

6 Enter the requested information for the Unified Access Gateway appliance.

The response status returned will indicate whether the configuration was successful.

Response status	Result
200	Configuration successful
400	Invalid input
401	Password incorrect. Confirm that password matches admin password configured during OVA deployment
000	Network connection failure. Confirm that IP address matches management IP address configured during OVA deployment

7 Configure NAT and firewall rules to allow access to the Unified Access Gateway appliance through Internet network.

Note When using an edge gateway load balancer the NAT for ports 80 and 443 are not required. These ports are forwarded automatically.

Port	Usage
4172/tcp, 4172/udp	PCoIP desktop access protocol
8443/tcp	HTML desktop access protocol
443/tcp	Secure web portal access
80/tcp	Insecure web portal access (will be redirected to 443)

Enter the Tenant AD Information

Enter Active Directory information for the tenant in the Administration Console. For more information see the Tenant Administration guide.

Note If you do not use a domain admin account for the Service Account then you must set the tenant policy fabric.ad.validateSysPrepUserPrivs to false.

Apply Tenant Certificates to Tenant Appliances

Horizon DaaS allows you to upload custom SSL certificates for each tenant.

- If the tenant does not already have a certificate, you can generate it before applying it.
- If it already has a certificate, you can apply that certificate.

Generate Tenant Certificates

You can generate the tenant's CSR file (certificate signing request) either on the Service Provider appliance or the tenant nodes.

- If you are generating certificates on the Service Provider appliance, be sure to create in a tenant specific directory so files are not confused among tenants.
- Always name the file using the domain for which the cert is being generated.

Procedure

1 Collect the following information for the tenant:

   - Country Code
   - State and Locality
   - Full Legal Company Name
   - Organizational Unit

2 At the command line run the following command:

   ```
   openssl req –new –newkey rsa:2048 –nodes –keyout server.key –out server.csr
   ```

   where server is the domain you want to create a cert for - such as desktops.tenant.com

   The system generates two files: the Private-Key file for the decryption of your SSL Certificate, and a certificate signing request (CSR) file (used to apply for your SSL Certificate) with apache openssl.

3 When you are prompted for the Common Name (domain name), enter the fully qualified domain name for the site you are securing.

   If you are generating an Apache CSR for a Wildcard SSL Certificate your common name should start with an asterisk (such as *.example.com).

4. Once the .key and .csr files are created, zip them up and send them to the customer so they can request a cert from a certificate authority.
5. Copy the files to /usr/local/desktone/cert on the tenant node so they are backed up by the automated backup process.

Apply Tenant Certificates

Horizon DaaS allows you to upload custom SSL certificates for each tenant.

To enable a custom certificate, you upload three certificate files in Apache format: SSL Certificate, SSL Key, and CA Certificate. The tenant might provide you with all three files. Or, to ensure the files are generated properly, you can generate the public and private keys yourself, forward these keys to the tenant, and then the tenant can request the signed certificate from the signing authority.

Note To upload the three certificate files, you navigate to the Certificates tab under tenants (this is a different Certificates tab than the one used for service providers).

Procedure

1. In the Service Center, select **tenants > browse tenants**.
2. On the Tenants screen, click **Edit** for the tenant.
3. Click the Certificates tab.
4. On the Certificates tab browse for and select the following three files:
   - CA Certificate - The public certificate from a certificate authority that was used to sign the tenant certificate. This file will have a .pem or .crt extension.
   - SSL Certificate - The tenant’s public certificate, which was signed by the CA. This file has a .crt extension, which indicates that it is a certificate file.
   - SSL Key - The private key used to decrypt the tenant’s SSL certificate. This is needed in order to be able to respond to certificate requests. This file has a .key file extension.
5. Click **Submit** to upload the files.

   You can upload the files before or after installing appliances:

   - Before - The certificate is automatically installed on all the tenant appliances when you click the **Submit** button.
   - After - Click the link on the Certificates tab to install the certificate on the tenant appliances.

   Note If the IP address or URL for the tenant's desktop portal does not resolve to the tenants CN in their certificate, the tenant administrator may wish to include in their certificate a Subject Alternative Name so that the desktop portal's URL accessed by web clients can be matched to the uploaded tenant certificate. For more details on how to add a Subject Alternative Name to the certificate, contact the certificate authority.

To back up, copy the files to /usr/local/desktone/cert/temp on the primary Tenant appliance so they are backed up by the automated backup process.

Tenant Installation Worksheet

This topic lists the fields you will need to populate in the Service Center when installing a tenant. The fields are listed in the order they must be provided during the installation.

Field	Values	Sample Value / Notes
Tenant VLAN/VXLAN ID		115
Tenant Gateway		172.16.115.1
Tenant DNS Name		172.16.115.2 (AD server)
Tenant Subnet mask		255.255.255.0
Primary Tenant Appliance Name		TenantA-Node1
Primary Tenant Appliance IP Address		172.16.115.21
Secondary Tenant Appliance Name		TenantA-Node2
Secondary Tenant Appliance IP Address		172.16.115.22
Floating IP Address		172.16.115.20
Tenant Host/Server IP Address		DNS name or IP of host
Tenant Host/Server User name		HostMgtAcct
Tenant Host/Server Password		hostPsswd
Tenant Storage System Address		storage.sp.com
Tenant Storage System Username		rootAccessAct
Tenant Storage System Password		storagePsswd
Name of Tenant Directory to Mount		tenantAnfs
Tenant Remote Mount Point		/vol/tenanta

To configure the tenant Active Directory, you will also need to collect the following:

Field	Values	Sample Value / Notes
Active Directory (AD) Name		TENANT
Domain		tenant.com
AD Protocol		LDAP
AD Port		389
Nameserver		172.16.115.2
Context		dc=tenant,dc=com
Service Account		CN=Administrator,CN=Users
Password		TenantAPsswd
Admin Group		cn=enterprisecenteradmin,ou=groups

Field	Values	Sample Value / Notes
User Group		cn=portalusers,ou=groups
Admin User		Administrator
Password		AdminPsswd
Primary DNS		172.16.115.2

Unified Access Gateway Setup

4

This section describes the process for setting up Unified Access Gateway (formerly known as Access Point), which replaced Remote Access Manager (dtRAM) in DaaS deployments.

Unified Access Gateway is a VMware developed End-User Computing (EUC) appliance that acts as a specialized gateway (or reverse proxy) that manages access to enterprise EUC products deployed in a private or public cloud. It consolidates functionality that was previously implemented in various enterprise EUC products, and simplifies deployments for customers who use multiple EUC products within their environments.

The following are advantages of migrating to Unified Access Gateway:

- Customers who migrate to Unified Access Gateway can reduce their firewall open ports to 443, 4172 and 8443.
- Unified Access Gateway properly handles SSL certificates for HTML Access (Blast) so that a certificate will no longer be required on the virtual desktop.

Note For internal access not via Unified Access Gateway, desktops will still need to have SSL certificates.

Basic Functionality

The basic functionality of Unified Access Gateway is as follows.

- The client makes a connection to the reverse proxy, and when the response comes back, the client intercepts it.
- The connection can be established by either a browser or the Horizon client.
- Once a virtual desktop session is established, the PCoIP SG, Blast SG, or View Tunnel may be used for the virtual desktop traffic, depending on what protocol the user has selected. The tunnel is used for the RDP protocol as well as USB connections.

Unified Access Gateway used in a Horizon DaaS deployment has the following characteristics:

- There will be no authentication (at least for the first release). This responsibility will remain within the Tenant Appliance.

- All communication will be proxied through Unified Access Gateway if the end-user is accessing the solution from outside of the corporate network. This includes:
  - All View-specific protocol handling (XMLAPI, PCoIP, etc)
  - Any Tenant Appliance communication

Unified Access Gateway vs. dtRAM

The main differences between dtRAM and Unified Access Gateway are outlined in the table below.

dtRAM (no longer supported)	Unified Access Gateway
Tenant appliance sits in front of the dtRAM and controls its operations	Unified Access Gateway appliance sits in front of the tenant appliance so that the tenant does not know it exists. The tenant requires software changes to accommodate this new architectural shift.
Does not make use of a PSG (or BSG or Tunnel) gateway that is installed	Makes use of a PSG (or BSG or Tunnel) gateway that is installed
Needs to use a wide range of ports for PCoIP etc. from the client and requires customers to open all of these ports to allow access	All PCoIP traffic can come in on the standard port (4172). Other single ports are used for BSG and Tunnel.
BSD-based and uses "pf" to forward traffic	Linux appliance with built-in proxying capabilities
Supports HA clustering	HA clustering is possible if you choose to configure load balancers
Has security weaknesses because it can only validate traffic based on source IP address	Uses deep protocol inspection techniques to ensure that traffic from the client is properly validated before it is passed on to the virtual desktops

The following are some considerations regarding Unified Access Gateway performance.

- Capacity – Unified Access Gateway has been tested with as many as 2,000 concurrent sessions, but the number of sessions your system can handle depends on the amount of data being sent and received (for example, video content).
- Monitoring– Unified Access Gateway does not currently have an internal monitoring tool.
- Rebooting – Performing a reboot operation for Unified Access Gateway disconnects all active users. The user's desktop session remains active, but the user will need to reestablish the connection to regain access to the desktop. If Unified Access Gateways are deployed in a load balanced configuration with multiple Unified Access Gateways, then any active or new users will be able to immediately reconnect via the load balancer and the connection will be handled by another Unified Access Gateway while one is rebooting.
- High Availability / Failover – HA clustering is possible if you choose to configure load balancers (see example in Appendix A).

This chapter includes the following topics:

- Set Up Unified Access Gateway

- Example of Load Balancer Configuration

Set Up Unified Access Gateway

You can set up Unified Access Gateway for use in your environment.

For more information about Unified Access Gateway configuration, see VMware Unified Access Gateway documentation.

Note You cannot deploy a Unified Access Gateway VM from a vSphere Windows client. You must deploy it from the vSphere web client.

Note Default tenant appliance certificates should not be used for configuring Unified Access Gateway. Custom certificates for Tenant should be uploaded from the Service Center user interface and those certificates should be used for configuring Unified Access Gateway.

Procedure

1 Download the latest version of the Unified Access Gateway OVA file.

2 Determine the IP addresses (DNS/Netmask/Gateway) for the required networks, as described below.

Configuration	Networks
3 NIC (Recommended configuration)	Internet (NIC 1) - Any network with internet access Management (NIC 2) - This can be your 169 network. Since this does not have its own DNS or Gateway, you can enter any numbers for DNS and set the netmask to 255.255.255.0 Backend (NIC 3) - Network that the Tenant uses for desktops
2 NIC	Internet (NIC 1) - Network the Tenant is on Management (NIC 2) - This can be your 169 network. Since this does not have its own DNS or Gateway, you can enter any numbers for DNS and set the netmask to 255.255.255.0
1 NIC	Internet (NIC 1) - Network that the Tenant is on

Note If NIC 2 is present, then the administration server (port 9443) that provides the REST APIs will only listen on that NIC. This server is accessed by the "apsetup.sh" script used in Step 5 below. If NIC 2 is not present, then that administration server listens on all of the interfaces.

3. In the vSphere web client, follow the normal method for deploying a template. In the “Customize template” step, enter information as shown below.

   Note The fields below may not all appear, depending on your configuration, and may also appear in a different order than that shown below.

   Table 4-1.

Networking Properties	External IP Address	Physical IP address of NIC 1. Note: If user access is via a NAT address, do not enter that address here.
	DNS server addresses	IP of the DNS that the Unified Access Gateway will use to resolve Hostnames.
	Management network IP Address	If configuration is 3 NIC or 2 NIC, enter Management Network IP from the previous step.
	Backend network IP Address	If configuration is 3 NIC, enter Backend Network IP from the previous step.
Password Options	Password for the root user of this VM	Initial password for root user. This must be a valid Linux password.
	Password for the admin user, which enables REST API access	Password to be used for REST API Admin user. Password must be at least eight characters long and must contain: ■ At least one upper case letter ■ At least one lower case letter ■ At least one number ■ At least one special character (!, @, #, etc.)
System Properties	Locale to use for localized messages	en_us
	Syslog server URL	Leave blank
Horizon Properties	Horizon server URL	Leave blank
	Horizon server thumbprints	Leave blank

4. When you have finished the deployment process, power on the VM and wait for the login screen to appear on the console.

5. On the tenant appliance, run the following command:

```
sudo /usr/local/desktone/scripts/apsetup.sh
```

6 Enter yes or no to the initial two prompts, as described below.

Prompt	Value
Do you want to setup this access point for internal access . . . :	Default value is no. If you enter anything other than y or yes, it will default to no and the access point will be configured for external connections in the DMZ network. In most cases you will use the external configuration. Enter yes to make this an internal access point so that the PCoIP traffic goes directly to the desktops, bypassing the access point.
Do you want to allow Horizon Air Helpdesk Console access . . . :	Enter yes to allow the Helpdesk Console access though the access point, or no to not allow access. The Helpdesk Console is a console access tool that allows you to run health scans, provide remote assistance, and view history and audit information for each VM in your system. **Note** This is a beta feature and is not supported at this time. For more information about trying this tool, please contact your deployment representative.

The system now proceeds to the Unified Access Gateway Configuration prompts.

7 Enter the requested information for the Unified Access Gateway appliance:

Prompt	Value
Admin Password:	Password for the admin user of the Unified Access Gateway.
Management IP:	This is the same address you entered above for Management network IP Address.
External IP:	The IP address for NIC 1 or the NAT IP address of NIC 1.
External Hostname [xx.xx.xx.xx]:	[Default hostname in brackets]
External PCoIP Port [4172]:	Default PCoIP Port shown in brackets: [4172]
External HTML Access Port [8443]:	Default HTML Access Port in brackets: [8443]
External Tunnel Port [443]:	Default Tunnel Port in brackets: [443]

The response status returned will indicate whether the configuration was successful.

Response status	Result
200	Configuration successful
400	Invalid input
401	Password incorrect. Confirm that password matches admin password configured during OVA deployment.

8 If dtRAM was in use on this environment previously, set the element.allocator.ram.use policy to false and remove the associated NAT and firewall rules.

9. Configure NAT and firewall rules to allow access to the Unified Access Gateway appliance through Internet network.

   Note When you are using an edge gateway load balancer the NAT for ports 80 and 443 are not required. These ports are forwarded automatically.

Port	Usage
4172/tcp, 4172/udp	PCoIP desktop access protocol
8443/tcp	HTML desktop access protocol
443/tcp	Secure web portal access
80/tcp	Insecure web portal access (will be redirected to 443)

Example of Load Balancer Configuration

The following is an example of the process for configuring a load balancer. The settings you use will be different.

Procedure

1. Choose an external IP to use for NAT (for example, 1.2.3.4).
2. Choose three external ports per Unified Access Gateway for NAT (for example, [41721, 8443, 4431], [41722, 8444, 4432]).
3. Log in to the vCloud Director interface as an Organization Administrator.
4. Navigate to Edge Gateway Services:
   a. Click Administration in the top menu.
   b. Click Virtual Datacenters in the Administration pane to the left.
   c. Click the Virtual Datacenter name in the pane on the right.
   d. The pane on the right has a row of tabs along the top. Click the Edge Gateways tab.
   e. In the list of Edge Gateways, click one to select it.
   f. Right-click the Edge Gateway and click Edge Gateway Services.

5. Configure DNAT:

   a. On the Edge Gateway Services page, click the NAT tab.

   b. Configure as shown below.

Applied On	Type	Original IP	Original Port	Translated IP	Translated Port	Protocol
external	DNAT	1.2.3.4	41721	192.168.0.10	4172	TCP & UDP
external	DNAT	1.2.3.4	8443	192.168.0.10	8443	TCP
external	DNAT	1.2.3.4	4431	192.168.0.10	443	TCP
external	DNAT	1.2.3.4	41722	192.168.0.11	4172	TCP & UDP
external	DNAT	1.2.3.4	8444	192.168.0.11	8443	TCP
external	DNAT	1.2.3.4	4432	192.168.0.11	443	TCP

6. Configure Firewall:

   a. On the Edge Gateway Services page, click the Firewall tab.

   b. Configure as shown below.

Name	Source	Destination	Protocol	Action
ap1-pcoip	any:any	1.2.3.4:41721	TCP & UDP	Allow
ap1-blast	any:any	1.2.3.4:8443	TCP	Allow
ap1-tunnel	any:any	1.2.3.4:4431	TCP	Allow
ap2-pcoip	any:any	1.2.3.4:41722	TCP & UDP	Allow
ap2-blast	any:any	1.2.3.4:8444	TCP	Allow
ap2-tunnel	any:any	1.2.3.4:4432	TCP	Allow

7. Configure load balancer pool servers:

   a. On the Load Balancer tab, click Pool Servers and click Add.

   b. On the Name & Description tab, type a name and optionally a description for the pool server.

   c. Click **Next**.

   d. On the Configure Service tab:

      - Click Enable for HTTP and HTTPS services.
      - Select IP Hash for the balancing method for both services.
      - For default ports, enter the following:
        - HTTP - Port 80
        - HTTPS - Port 443

   e. Click **Next**.

f On the Configure Health-Check tab:

- For HTTP and HTTPS, enter Monitor Ports.
- For HTTPS, change Mode to TCP.
- In the URI for HTTP service field, enter /favicon.ico.

g Click **Next**.

h On the Manage Members tab, add each Unified Access Gateway as a member, described below.

1. Click **Add**.
2. In the Add Member dialog:
   - Enter the IP address of the Internet UAG interface, as defined when you deployed the OVA.
   - For both HTTP and HTTPS, enter 80 for Port and 443 for Monitor Port.
3. Click **OK**.

8 Configure load balancer virtual server:

a On the Load Balancer tab, click **Virtual Servers** and then click **Add**.

b Enter a name and description for the virtual server.

c Select an external network from the **Applied on** drop-down menu.

d Enter the external IP address of the virtual server.

e From the drop-down menu, select the pool you created earlier.

f In Services, select **Enable for HTTP and HTTPS**.

g For Persistence Method, enter No persistence for HTTP and HTTPS.

h Click **Enabled** to enable the virtual server.

i Click **OK**.

HTML Access (Blast) Setup

5

The Horizon Agent has a very small footprint (90Kb) and supports the full Horizon Client capabilities: PCoIP, RDP, HTTPS, SSL, SSO, USB Redirection, printer support, and session management.

HTML Access (Blast) enables access to a desktop via any HTML5 compliant web browser.

To use HTML Access:

- Each virtual desktop must be running the latest Horizon Agent.
- Each virtual desktop must be running the latest Horizon DaaS Agent.
- SSL certificate install automation must be configured as described in Automate SSL Installation.

Launching RDSH applications is supported in HTML Access 3.4 and higher.

This chapter includes the following topics:

Prepare Desktops to Support Protocol

Before installing the software required to connect to desktops, complete the following pre-installation steps.

Procedure

1 Uninstall all software components related to all other protocols.

 Note You must uninstall all software components related to all other protocols (e.g. HDX, RGS). If you do not uninstall these other protocol components, your template will be corrupted and you will no longer successfully boot into Windows. This warning does not apply to RDP; the presence of RDP components does not cause problems.

2 Update VMware Tools.

3 Make sure that port 443 is not being used by any other software.

4 Enable the Windows Firewall if not already enabled.

5 Make sure that the following ports are open to TCP and/or UDP traffic as indicated:

Port(s)	Source	Destination	TCP	UDP
4172	Unified Access Gateway	VM	x	x
443	Tenant Appliance	VM	x	
22443	Unified Access Gateway	VM	x	

What to do next

Install the DaaS Agent

Install the DaaS Agent

After you have completed the preparation steps, you can install the DaaS Agent.

Note The manual configuration required for older versions of the DaaS Agent is no longer necessary.

Procedure

1 Download the most recent DaaS Agent installer file from the Myvmware.com download site.

2 Run the installer on the template virtual machine.

What to do next

Installing the Horizon Agent

Installing the Horizon Agent

After you have installed the DaaS Agent, you can install the Horizon Agent.

There are three possible scenarios when installing the Horizon Agent:

- Install on Windows desktop
- Install on Windows server as Personal Desktop (Non-RDSH)

- Install on Windows server as RDSH Role

Note If you have not installed the most recent version of the Horizon Agent, this can cause problems with creating RDS pools. In this case, when you create a new RDS pool, the system can allow you to select HTML Access (Blast) as a protocol, but this selection will not be applied to the pool even though it appears to have been applied successfully.

Install the Horizon Agent on a Windows Desktop

You can install the Horizon Agent on a Windows desktop.

Procedure

1 Download the latest Horizon Agent from the Myvmware download site. Note that there are separate downloads for 32-bit and 64-bit operating systems.

2 Double-click the Horizon Agent installation file (file name is: VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe for the 64-bit installer).

3 Perform a custom installation with the following options:

   - Deselect VMware Horizon View Composer Agent.
   - Select vRealize Operations Desktop Agent.

4 Restart the virtual machine when prompted.

What to do next

For improved security regarding the use of the Horizon Agent, disable weak ciphers in SSL and TLS, which requires you to edit the Group Policy Object (GPO) of the Active Directory server. See the appropriate Horizon Agent documentation for information about disabling weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.

Install the Horizon Agent on Windows Server as Personal Desktop (Non-RDSH)

You can install the Horizon Agent on Windows Server as a personal desktop.

Procedure

1 Download the latest Horizon Agent from VMware's website (https://my.vmware.com). Note that there are separate downloads for 32-bit and 64-bit operating systems.

2 Double-click the Horizon Agent installation file (file name is: VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe for the 64-bit installer).

3 Select the option to install the Horizon Agent in desktop mode.

4 Perform a custom installation with the following options:

   - Deselect VMware Horizon View Composer Agent.
   - Select vRealize Operations Desktop Agent.

5 Restart the virtual machine when prompted.

What to do next

For improved security regarding the use of the Horizon Agent, disable weak ciphers in SSL and TLS, which requires you to edit the Group Policy Object (GPO) of the Active Directory server. See the appropriate Horizon Agent documentation for information about disabling weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.

Install the Horizon Agent on Windows Server as an RDSH Role

You can install the Horizon Agent on Windows Server as an RDSH role.

Note To install the Horizon Agent in this scenario, you MUST run the command line install and cannot use the default “double click” GUI.

Procedure

1 Add the Remote Desktop Services role.

   a Select **Start > Administrative Tools > Server Manager** to open the Server Manager.

   b Select **Roles** and then select **Add Roles** in the right pane.

   The Before You Begin page of the Add Roles Wizard window appears.

   c Click **Next**.

   The Select Server Roles page appears.

   d Select the check box for Remote Desktop Services and click **Next**.

   The Remote Desktop Services page appears.

   e Click **Next**.

   The Select Role Services page appears.

   f Select the check box for Remote Desktop Session Host and click **Next**.

   The Uninstall and Reinstall Applications for Compatibility page appears.

   g Click **Next**.

   The Specify Authentication Method for Remote Desktop Session Host page appears.

   h Select the appropriate Authentication Level, and then click **Next**.

   The Specify Licensing Mode page appears.

   i Specify the licensing mode, and then click **Next**

   The Select User Groups Allowed Access To This RD Session Host Server page appears.

   j Add your Users or User Groups, and then click **Next**.

   The Configure Client Experience page appears.

k Make desired settings, and then click **Next**.

The Confirm Installation Selections page appears.

l Confirm your selections. If something is incorrect, click **Previous** to return to the previous steps and change the settings. Click **Install**.

The Installation Progress page appears. The installation takes a few minutes to finish. The Installation Results page appears, and asks for restart.

m Click **Close**.

A dialog appears, asking for confirmation for restart.

n Click **Yes** to restart the server.

o When the server comes back, log in again.

The Resuming Configuration page appears. It takes a few seconds to resume configuration. The Installation Results page appears.

p Click **Close** to complete the installation.

The Server Manager window appears.

q Click **Roles** and confirm that the Remote Desktop Services role is installed.

2. Download the latest Horizon Agent from VMware’s website (https://my.vmware.com). Note that there are separate downloads for 32-bit and 64-bit operating systems.
3. Run the following on the command line as an administrator user: `VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"`
4. Perform a custom installation with the following options:
   - Select vRealize Operations Desktop Agent.
5. Restart the virtual machine when prompted.

What to do next

For improved security regarding the use of the Horizon Agent, disable weak ciphers in SSL and TLS, which requires you to edit the Group Policy Object (GPO) of the Active Directory server. See the appropriate Horizon Agent documentation for information about disabling weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.

Add the HTML Access (Blast) Group Policy Settings to the Local Computer Policy Environment

After you have finished installing the agents, you must add the required GPO settings.

Procedure

1. Download the View GPO Bundle .zip file from the VMware Horizon download site at: http://www.vmware.com/go/downloadview

   The file is named VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip, where x.x.x is the version and yyyyyyy is the build number. All ADM and ADMX files that provide group policy settings for View are available in this file.

2. Copy the file to your Active Directory server and unzip the file.

   The HTML Access GPOs are included in the Blast-enUS.adm ADM Template file.

3. On the Active Directory server, edit the GPO.

Option	Description
Windows Server 2008 or 2012	1 Select **Start > Administrative Tools > Group Policy Management**. 2 Expand your domain, right-click the GPO that you created for the group policy settings, and select **Edit**.
Windows Server 2003	1 Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. 2 Right-click the OU that contains your View desktops and select Properties. 3 On the Group Policy tab, click **Open** to open the Group Policy Management plug-in. 4 In the right pane, right-click the GPO that you created for the group policy settings and select **Edit**.

   The Group Policy Object Editor window appears.

4. In the Group Policy Object Editor, right-click Administrative Templates under Computer Configuration and then select Add/Remove Templates.

5. Click Add, browse to the Blast-enUS.adm file, and click Open.

6. Click Close to apply the policy settings in the ADM Template file to the GPO.

   The VMware Blast folder appears in the left pane under Administrative Templates > Classic Administrative Templates.

7. Configure the HTML Access group policy settings.

8. Make sure your policy settings are applied to the remote desktops.

9. Run the gpupdate.exe command on the desktops.

10. Restart the desktops.

Automating SSL Installation

The process described in this section is needed to facilitate internal access that is not via Unified Access Gateway. If you do not have users requiring this type of access, you do not need to perform this procedure.

Note the following:

- You must follow this process on the gold pattern before converting the VM as a gold pattern or reseal.
- You must repeat this process each time you open and re-seal a gold pattern.

You can install the certificate using post sysprep script execution in order to avoid sysprep issues and duplicate certificate problems. You can also use your own own standard practice as well (for example, Active Directory GPO and scripts). Please read the Horizon View feature pack documentation for SSL certificate requirements.

Perform the tasks below to configure post sysprep commands/scripts in the Horizon DaaS environment.

Import Certificate and Record Certificate Thumbprint

You begin the SSL automation process by importing the certificate and recording its thumbprint.

Procedure

1 Add the certificate snap-in to MMC by performing the steps below.

In order to add certificates to the Windows certificate store, you must first add the certificate snap-in to the Microsoft Management Console (MMC). Before you begin, verify that the MMC and certificate snap-in are available on the Windows guest operating system.

a On the desktop, click Start and type `mmc.exe`.

b In the MMC window, select **File > Add/Remove Snap-in**.

c In the Add or Remove Snap-ins window, select **Certificates** and click **Add**.

d In the Certificates snap-in window, select **Computer account**, click **Next**, select local computer, and click **Finish**.

e In the Add or Remove snap-in window, click **OK**.

2 Import a certificate for the HTML Access Agent into the Windows Certificate Store by performing the steps below.

To replace a default HTML Access Agent certificate with a CA-signed certificate, you must import the CA-signed certificate into the Windows local computer certificate store. Before you begin, verify that the HTML Access Agent is installed, the CA-signed certificate was copied to the desktop, and the certificate snap-in was added to MMC (see Step 1 above).

a In the MMC window, expand the Certificates (Local Computer) node and select the Personal folder.

b In the Actions pane, select **More Actions > All Tasks > Import**.

c In the Certificate Import wizard, click **Next** and browse to the location where the certificate is stored.

d Select the certificate file and click **Open**.

To display your certificate file type, you can select its file format from the File name drop-down menu.

e Type the password for the private key that is included in the certificate file.

f Select **Mark this key as exportable**.

g Select **Include all extendable properties**.

h Click **Next** and click **Finish**.

The new certificate appears in the Certificates (Local Computer) > Personal > Certificates folder.

i Verify that the new certificate contains a private key.

1 In the Certificates (Local Computer) > Personal > Certificates folder, double-click the new certificate.

2 In the General tab of the Certificate Information dialog box, verify that the following statement appears: You have a private key that corresponds to this certificate.

3 Import root and intermediate certificates for the HTML Access Agent

If the root certificate and intermediate certificates in the certificate chain are not imported with the SSL certificate that you imported for the HTML Access Agent, you must import these certificates into the Windows local computer certificate store.

a In the MMC console, expand the Certificates (Local Computer) node and go to the Trusted Root Certification Authorities > Certificates folder.

- If your root certificate is in this folder, and there are no intermediate certificates in your certificate chain, skip this procedure.
- If your root certificate is not in this folder, proceed to step b.

b Right-click the Trusted Root Certification Authorities > Certificates folder and click **All Tasks > Import**.

c In the Certificate Import wizard, click **Next** and browse to the location where the root CA certificate is stored.

d Select the root CA certificate file and click **Open**.

e Click Next, click **Next**, and click **Finish**.

   f. If your server certificate was signed by an intermediate CA, import all intermediate certificates in the certificate chain into the Windows local computer certificate store.

      1. Go to the Certificates (Local Computer) > Intermediate Certification Authorities > Certificates folder.
      2. Repeat steps c through f for each intermediate certificate that must be imported.

4. In the certificate MMC window, navigate to the Certificates (Local Computer) > Personal > Certificates folder.
5. Double-click the CA-signed certificate that you imported into the Windows certificate store.
6. In the Certificates dialog box, click the Details tab, scroll down, and select the Thumbprint icon.
7. Copy the selected thumbprint to a text file.

   For example:

   ```
   31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e
   ```

   Note When you copy the thumbprint, do not to include the leading space. If you inadvertently paste the leading space with the thumbprint into the registry key (in Step 7), the certificate might not be configured successfully. This problem can occur even though the leading space is not displayed in the registry value text box.

What to do next

Create Post Sysprep Script/Batch File on Gold Pattern Image and Copy Certificate

Create Post Sysprep Script/Batch File on Gold Pattern Image and Copy Certificate

After you have imported the certificate and recorded the thumbprint, you must create the post sysprep script/batch file and copy the certificate.

Windows 7 and Later

Use post build configuration script “SetupComplete.cmd “to import the SSL certificate and configure the VMware HTML Access registry.

http://technet.microsoft.com/en-us/library/dd744268%28v=ws.10%29.aspx

For example:

1. Copy the SSL certificate file under C: drive. For this example, the “C:\desktone_ca_cert” file.
2. Create a file SetupComplete.cmd under "%WINDIR%\Setup\Scripts\" folder. Create “Scripts” folder if it does not exist.

3 Add following commands in SetupComplete.cmd file. The thumbprint value is what you copied in Step 1.

Note If you have root certificate and intermediate certificates in the certificate chain, then you need to add appropriate CertUtil commands in batch file.

```
CertUtil -importPFX -f -p "<password>" "C:\desktone_ca_cert.pfx"

reg add "HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config" /f /v "SslHash" /t REG_SZ /d "31 2a 32
50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e"

del /F /Q "C:\desktone_ca_cert.pfx"

del /F /Q "%systemroot%\setup\scripts\SetupComplete.cmd"
```

4 Save the SetupComplete.cmd file. You can test the SetupComplete.cmd file on test machine.

Windows XP

- Follow the Desktone post sysprep command execution approach to import the SSL certificate and configure the VMware HTML Access registry.
- Install the Administration Tools Pack for Windows XP as the CertUtil tool is not available with the OS install.

  http://www.microsoft.com/en-us/download/details.aspx?id=16770

  For example:

  a Copy the SSL certificate file under C: drive. For this example, the C:\desktone_ca_cert.pfx file.

  b Create folder path C:\Sysprep\i386\OEM\

  c Now create postprep-extra.bat file under C:\Sysprep\i386\OEM\ and add the following commands in the batch file. The thumbprint value is the one you recorded above after importing the certificate.

  Note If you have root certificate and intermediate certificates in the certificate chain, then you need to add appropriate CertUtil commands in the vbatch file.

  ```
  CertUtil -importPFX -f -p "<password>" "C:\desktone_ca_cert.pfx"

  del /F /Q "C:\desktone_ca_cert.pfx.pfx"

  reg add "HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config" /f /v "SslHash" /t REG_SZ /d "31 2a
  32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e"
  ```

  d Save the postprep-extra.bat file. You do not need a command to delete the batch postprep-extra.bat file as sysprep deletes the C:\Sysprep folder after successful deployment.

You can test the SetupComplete.cmd file on the test machine.

What to do next

Convert Image to Gold Pattern or Reseal

Convert Image to Gold Pattern or Reseal

After you have created the post sysprep script/batch file and copied the certificate, you convert the image to a gold pattern or reseal.

Procedure

1. Convert the image as a gold pattern or reseal, and create a pool.
2. Verify the HTML Access connection for the certificate, or check certificates and HTML Access registry on desktops.

   Note If the HTML Access (Blast) service generates the self-signed certificate even after you set the valid CA certificate as described above, then you can troubleshoot this issue by looking at the logs located here: %ProgramData%\VMWare\Vmware Blast\Blast-worker.txt

Troubleshooting Connection Problems

There are several configuration/setup problems that can result in an inability to launch a HTML Access (Blast) connection successfully.

- Browser is not HTML5 compliant. Check that the browser version is one cited in the requirements.
- Pop-up blocker enabled. The browser's pop-up blocker could prevent opening the new window for a HTML Access connection. Make sure that the user disables the pop-up blocker for the Desktop Portal.
- Windows firewall disabled. Make sure that the Windows Firewall is installed and running on the user's desktop. A disabled Windows Firewall will result in errors reported in the HTML Access logs.
- Certificate errors. If you receive an error that indicates a missing or non-matching certificate, review the instructions above under Import Certificate and Record Certificate Thumbprint and confirm that you have performed the necessary steps.

  Note You must repeat this process each time you open and re-seal a gold pattern.

Known Limitations and Workarounds

Note the limitations and workarounds listed below.

- An SSL certificate warning will be displayed upon connecting to the desktop. This is because the SSL certificate process was not performed correctly on a tenant gold pattern. It is recommended to use Unified Access Gateway for such connections.
- Changing resolution to 2560x1920 ends the HTML Access session. This happens due to lack of vRAM allocation. For more information see the View documentation.
- If your client system uses a super high resolution monitor (such as 2560 x 1600), HTML Access fails to display the desktop.

  Workaround: Lower the resolution on your monitor and connect. The resolution on the client monitor must be less than 2560 x 1600 if the remote desktop resolution is 1920 x 1200.
- Sound playback quality is best on browsers that have Web Audio API support, such as Chrome, Safari, and Firefox 25. Browsers that do not have this support include Internet Explorer (up to and including Internet Explorer 11) and Firefox 24 and earlier.
- Black artifacts appear on the screen on ESXi 5.1 or 5.0 hosts. This is a known HTML Access issue when the desktop HW version is 9 (ESX 5.0/5.1) with 3D disabled and the Windows 7 basic theme is used. This is not an issue when Aero is turned on or when the VM uses HW version 10 (ESX 5.5).
- Horizon Agent session timeout may occur before the Desktop Portal session timeout, resulting in “Authentication error” connecting to the desktop via HTML Access. The workaround for this this is to log out of Desktop Portal and log in again.

Tenant Customization

6

This chapter includes the following topics:

- Custom Branding
- Super Tenant

Custom Branding

If you have a custom branding scheme for Desktop Portal, you will need to check whether everything appears as expected after upgrading a tenant.

The following are items to which you should pay particular attention due to VMware branding changes.

- 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;

Super Tenant

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 Administration Console, 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.

Super Tenant Prerequisites

This topic details prerequisites for super tenant configuration.

Networking Requirements

A Super Tenant must have a perimeter network (e.g. DMZ in figure above) where DaaS tenant appliances and other external facing components like Unified Access Gateway 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 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).

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 DaaS platform such as user mapping. Customers can be separated by creating Organizational Units with security groups under the OUs in Active Directory.

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

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.

Note 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.

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. In our testing we have 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.

Configuring a Super Tenant in Service Center

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

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.

1. Log in to Service Center and click on the Tenants tab.
2. Click on the Register a tenant link and select the **Super Tenant** check box.
3. Follow the normal tenant registration steps.
4. When the tenant appliances have been successfully created, log into Service Center and navigate to **tenants > policy**.
5. Select the tenant organization from the **Organization** dropdown menu.
6. Set the `fabric.pool.network.assignments` policy to `true`.

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.

1 Log into 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**.

Add Networks for a Super Tenant

A service provider administrator must add networks to be used for super tenant customers in the platform. To add networks, follow the procedure below.

1 Log into 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**.

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.

Disabling the Super Tenant Option

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

Billing

The DtReportingManager now has an additional method ‘SuperTenantBillingReports’ and returns a collection of DtSuperTenantBillingReport records as described. Please refer to the 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
```

7 System Maintenance

This chapter includes the following topics:

- Backing Up and Restoring Databases
- Reinitialize Slony
- Database Failover
- Monitoring

Backing Up and Restoring Databases

You can back up and restore databases.

Back Up a Database

To back up a database, run the following command in the appliance:

```
/usr/local/desktone/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/desktone/backup folder.

Optional Commands - backup_db.sh accepts the following optional command line arguments.

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

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.

To restore a database:

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/desktone/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/desktone/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, fdb, or avdb)
   - <filenname > is the name of the extracted backup file

5 On both appliances, re-initialize slony. For instructions, see Slony Reinitialization.

6 Reboot both appliances.

Reinitialize Slony

You can reinitialize slony.

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

Note When you reinitialize slony for the edb, you must reinitialize slony for the avdb as well.

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 (example shows fdb, but you can substitute edb or avdb):

   ```
   psql –Uadmin fdb –p 6432
   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/desktone/scripts/start_slon_fdb.sh
     ```

   - For the tenant org, start the daemons for all databases:

     ```
     /usr/local/desktone/scripts/start_slon_fdb.sh
     /usr/local/desktone/scripts/start_slon_edb.sh
     /usr/local/desktone/scripts/start_slon_avdb.sh
     ```

6. In the Service Center, select **appliances > maintenance**.

7. In the Slony Operations section of the page, use the **Organization id** drop-down menu to select the Org ID of the appliance to which the init slony will be performed.

   The **DB instance name** menu appears.

8. Use the **DB instance name** menu to select the name of the database instance (Fabric, Element, or Appvolumes) for init slony.

   If you selected Element or Appvolumes, the **Element ID** menu appears.

9. If you selected Element or Appvolumes above, use the **Element ID** drop-down menu to select the ID of the Desktop Manager to list as New Master IP for the init slony operation. If you selected Fabric above, skip this step.

10. Click **Init Slony**.

11 If you have performed a slony reinit on the avdb of a tenant appliance, then restart the wem-diagnose-service:

```
service diagnose restart
```

Note This is not required for an avdb slony reinit on a desktop manager only appliance.

Database Failover

When the primary appliance fails, you can perform a database failover.

When the primary appliance fails, the secondary database is read-only. When failover occurs, perform the following tasks:

- Enable write operations on the secondary database
- Permanently promote the secondary service provider appliance to become the primary
- Permanently promote the secondary tenant appliance to become the primary
- Restart the primary appliance

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) if the primary appliance is not available. The goal is to enable write operations so that the secondary appliance's database is the master datasource.

1 Stop the dtService, av-manager, and diagnose service on both the primary (if accessible) and the secondary appliance:

```
sudo service dtService stop
sudo service av–manager stop
sudo service diagnose stop
```

2 Stop all slony daemons on both the primary (if accessible) and the secondary appliances:

```
sudo killall slon
```

3 On the secondary appliance, connect to the fdb database and execute the following SQL command:

```
 drop schema _slony cascade;
```

4 Repeat step 3 for the EDB and AVDB 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 (see Backing Up and Restoring Databases).

6 Open the file /usr/local/desktone/release/active/conf/fdb.properties for edit and remove the IP address of the primary appliance.

7. Repeat step 6 for /usr/local/desktone/release/active/edb.properties if the appliance belongs to a tenant organization.

8. Repeat step 6 for /usr/local/desktone/release/active/avdb.properties if the appliance belongs to a tenant organization.

9. Set DB_HOST and DB_PASSWORD environment variables:

   ```
   export DB_HOST=IP_of_TA2_appliance
   export DB_PASSWORD=database_password
   ```

10. Execute av-setup script as sudo:

    ```
    sudo /usr/local/desktone/scripts/av-setup
    ```

11. Open the applications.properties file for editing:

    ```
    vi /usr/local/xmpms/diagnose/config/application.properties
    ```

12. In the applications.properties file, edit lines as follows:

    ```
    db.jdbc.url=jdbc:postgresql://<ip address>:5432/avdb?ssl=true
    db.fdb.jdbc.url=jdbc:postgresql://<ip address>:5432/fdb?ssl=true
    ```

13. Start dtService, av-manager, and diagnose service on the secondary appliance:

    ```
    service dtService start
    service av-manager start
    service diagnose start
    ```

Promote the Secondary Service Provider Appliance to Primary

To permanently promote the secondary service provider appliance to be the primary service provider appliance, perform the following steps.

In this example, the primary appliance is 'A', and the secondary appliance is 'B', and appliance A is accessible (database in this appliance is accessible).

1. Stop dtService on all the service provider appliances:

   ```
   service dtService stop
   ```

2. Log into all the service provider appliances.

3. Open the file /usr/local/desktone/release/active/conf/fdb.properties for edit and remove the IP address of the primary appliance that is in failed status.

4. Stop all slony daemons on all service provider appliances:

   ```
   killall slon
   ```

5 On the primary and secondary appliance, connect to the FDB database and execute the following SQL command:

```
drop schema _slony cascade;
```

6 Execute the following SQL commands in secondary appliance of datacenter (replace 'A' and 'B' with names of your appliances):

```
fdb=# update appliance set capabilities = (capabilities & 65343) where name='A';
fdb=# update appliance set capabilities = (capabilities | 192) where name='B';
```

7 Start dtService on the service provider appliances other than the failed appliance:

```
service dtService start
```

Confirm that the appliance is up and running before proceeding with the next step.

8 Stop dtService on all the service provider appliances except for the master service provider appliance (the secondary service provider appliance is the master):

```
service dtService stop
```

9 Start slon daemons in all of the service provider appliances:

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

10 Login to the Service Center of master service provider appliance (the secondary service provider appliance is the master) with your browser and perform the slony reinitialization operation:

a Navigate to **appliances > maintenance > Slony Operations**.

b In the Organization id drop-down list, select 1000.

c Click on the Init Slony button to reinitialize slony.

11 When the slony re-initialization is complete, execute the following command in the FDB of the secondary appliance in the datacenter:

```
SELECT a.set_id, a.set_comment, (SELECT last_value FROM _slony.sl_local_node_id) AS local_id,
CASE WHEN a.set_origin = (SELECT  last_value FROM _slony.sl_local_node_id)THEN TRUE ELSE FALSE
END AS master_node from _slony.sl_set a;
```

Output should appear as follows:

```
set_id | set_comment | local_id | master_node
--------+--------------------------+----------+-------------
1 | All tables and Sequences | 1 | t
(1 row)
```

12 Start dtService on all appliances except for the failed service provider appliance.

```
service dtService start
```

Promote the Secondary Tenant Appliance to Primary

To permanently promote the secondary tenant appliance to be the primary tenant appliance, perform the following steps.

In this example, the primary appliance is 'A', and the secondary appliance is 'B', and appliance A is accessible (database in this appliance is accessible).

1 Stop dtService on all tenant appliances in the organization:

```
service dtService stop
```

2 Log into all the tenant appliances in the organization.

3 Open the file /usr/local/desktone/release/active/conf/fdb.properties for edit and remove the IP address of the primary appliance that is in failed status.

4 Stop all slony daemons on all tenant appliances in the organization:

```
killall slon
```

5 If required, back up the database on the master appliance and restore it on the slave appliances.

6 In the master and slave appliances, connect to the FDB database and execute the following SQL command:

```
drop schema _slony cascade;
```

7 Execute the following SQL commands on the master service provider appliance (replace 'A' and 'B' with names of your appliances):

```
fdb=# update appliance set capabilities = (capabilities & 65343) where name='A';
fdb=# update appliance set capabilities = (capabilities | 192) where name='B';
```

8 Start slon daemons on all of the tenant appliances in organization:

```
/usr/local/desktone/scripts/start_slon_fdb.sh
/usr/local/desktone/scripts/start_slon_edb.sh
/usr/local/desktone/scripts/start_slon_avdb.sh
```

9 Login to the Service Center of the master service provider appliance with your browser and perform the slony reinitialization operation:

   a Navigate to **appliances > maintenance > Slony Operations**.

   b Select organization ID for the tenant from the Organization id drop-down list.

   c Select Fabric for the DB instance name label.

d Click on the Init Slony button to reinit slony.

10 When the slony re-initialization is complete, execute following command in the FDB of the secondary tenant appliance in the datacenter:

```
SELECT a.set_id, a.set_comment, (SELECT last_value FROM _slony.sl_local_node_id) AS local_id,
CASE WHEN a.set_origin = (SELECT  last_value FROM _slony.sl_local_node_id) THEN TRUE ELSE FALSE
END AS master_node from _slony.sl_set a;
```

Output should appear as follows (if the primary appliance was failed in the first datacenter):

```
set_id | set_comment | local_id | master_node
--------+--------------------------+----------+-------------
1 | All tables and Sequences | 1 | t
(1 row)
```

11 Start dtService on all the tenant appliances except for the tenant appliance that is in failed status.

```
 service dtService start
```

Restart the Primary Appliance

When you restart the primary appliance after failover, perform a slony reinitialization on both the EDB and AVDB.

Monitoring

This section describes basic monitoring of the DaaS environment. It also provides links to more detailed information about 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 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.

Critical Nodes

There are several nodes that are critical to proper functioning in a DaaS environment. In many cases the DaaS software is able to "self-heal". However, any impairment to these nodes should still be noted and potential action taken regardless of the DaaS software capability to "self-heal". Providing feedback on these occurrences is also important to improving the quality of the DaaS software. The nodes (whether iron or virtual) that should be actively monitored are listed below. Some of these are 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

DaaS nodes:

- Service Provider
- Tenant
- Resource Manager

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.

Web Application Monitoring

Basic verification of a DaaS installation includes connecting to the following web pages (both through a load balancer, if applicable, and directly to each node): Desktop Portal, Administration Console, and Service Center.

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

CIM Providers on DaaS Management Nodes

This section describes the CIM providers that monitor a DaaS installation.

Key properties for monitoring are highlighted in the descriptions linked below.

Operating Environment CIM Providers for DaaS Nodes

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

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 * (TotalSwapSpaceSize – FreeSpaceInPagingFiles) / TotalSwapSpaceSize
  - 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 problem, restart the node.

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.

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.

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_Ext4FleSystem 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 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 DaaS support for corrective action.

Application-Specific CIM Providers for DaaS Management Appliances

This topic lists the application-specific CIM providers for DaaS management appliances.

Note For non-DaaS-specific CIM provider classes, see Operating Environment CIM Providers for DaaS Nodes.

Table 7-1.

Appliance Type	CIM Providers
Service Provider	■ Desktone_ApplicationServer ■ Desktone_ApplicationServerStatistics ■ Desktone_InstalledProduct ■ Desktone_CommonDatabase ■ Desktone_DatabaseService ■ Desktone_DatabaseReplicationService ■ Desktone_ActiveDirectoryStatus ■ Desktone_HypervisorManagerStatus ■ Desktone_NTPService
Resource Manager	■ Desktone_ApplicationServer ■ Desktone_ApplicationServerStatistics ■ Desktone_InstalledProduct ■ Desktone_NTPService

Table 7-1. (continued)

Appliance Type	CIM Providers
Tenant	- Desktone_ApplicationServer - Desktone_ApplicationServerStatistics - Desktone_AppVolumeServiceStatistics - Desktone_InstalledProduct - Desktone_CommonDatabase - Desktone_DatabaseService - Desktone_DatabaseReplicationService - Desktone_RemoteAccessManagerStatistics - Desktone_ActiveDirectoryStatus - Desktone_NTPService - Desktone_XMPService
Desktop Manager	- Desktone_ApplicationServer - Desktone_ApplicationServerStatistics - Desktone_AppVolumeServiceStatistics - Desktone_InstalledProduct - Desktone_CommonDatabase - Desktone_DatabaseService - Desktone_DatabaseReplicationService - Desktone_NTPService

Desktone_ActiveDirectoryStatus

This topic describes the Desktone_ActiveDirectoryStatus CIM provider.

- Description

  ActiveDirectoryStatus provider is derived from CIM_LogicalElement, and it provides information and status of domain controllers which are added in 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 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 DaaS platform
  - CommunicationStatus [derived]: indicates the ability of the DaaS platform to communicate with domain controller. 2 – OK, 4 – Lost Communication
  - OperationalStatus [derived]: indicates the status of domain controller in DaaS platform . 2-OK, 13 – Lost communication.
  - Status [derived, deprecated]: indicates the current state of domain controller in 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 DaaS appliances.

  Note When the preferred domain controller is not active, it will not be included in the CIM response.

Desktone_ApplicationServer

This topic describes the Desktone_ApplicationServer CIM provider.

- Description

  Provides information about the application server used by the 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.
  - TargetOperatingSystem: Specifies the node's operating system environment. Set to 36 (LINUX).
- Mitigation

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

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

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

```
$ service dtService start
```

Desktone_ApplicationServerStatistics

This topic describes the Desktone_ApplicationServerStatistics CIM provider.

- 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 DaaS application.

  - InstanceID: Key to uniquely identify the instance of this class. Set to DesktonehostName_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*HeapSize/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 together with DaaS support.

Desktone_AppVolumeServiceStatistics

This topic describes the Desktone_AppVolumeServiceStatistics CIM provider.

- Description

Specifies the high level statistics of App Volume service.

- Properties
  - InstanceID: Key to uniquely identify the instance of this class.
  - Port: Port which service is running on.
  - Status: Overall status of the AV Server.
  - ADConnectCount: Total count of AD connection attempts.
  - ADConnectTimeMax: Maximum Time (in MS) taken to connect to AD host.
  - ADConnectTimeAvg: Average Time (in MS) taken to connect to AD host.
  - ADConnectFailureCount: Total count of AD connection failures.
  - ADNTLMAuthFailureCount: Total count of AD NTLM auth failures.
  - VCPingResponseTimeMax: Maximum ping response times (in MS) from vCenter.
  - VCPingResponseTimeAvg: Average ping response time (in MS) from vCenter.
  - VCPingResponseCount: Total count of vCenter ping attempts.
  - VCPingResponseFailureCount: Total count of vCenter ping failures.
  - VCGetVMDisksTimeMax: Maximum Time (in MS) taken to fetch the list of volumes from a given datastore path.
  - VCGetVMDisksTimeAvg: Average Time: (in MS) taken to fetch the list of volumes from a given datastore path.
  - VCGetVMDisksCount: Total count of attempts to fetch the list of volumes from a given datastore path.
  - VMGetVMDisksFailureCount: Total count of failures while fetching the list of volumes from a given datastore path.
  - VSphereConnectTimeMax: Maximum Time (in MS) taken to connect to vSphere server using RbVmomi::connect.
  - VSphereConnectTimeAvg: Average Time (in MS) taken to connect to vSphere server using RbVmomi::connect.
  - VSphereConnectCount: Total number of vSphere connection attempts.
  - VSphereConnectFailureCount: Total count of failures while attempting to connect to vSphere using RbVmomi::connect.
  - VSphereVolConversionFailureCount: Total count of failures while attempting to convert volume (vmdk) to VMFS thin format.
  - VSphereMoveDiskFailureCount: Total count of ‘Move Disk’ task failures.
  - VSphereCopyDiskFailureCount: Total count of ‘Copy Disk’ task failures.
  - VSphereDeleteDiskFailureCount: Total count of ‘Delete Disk’ task failures.

  - VSphereCreateDiskFailureCount: Total count of ‘Create Disk’ task failures.
  - VSphereExtendDiskFailureCount: Total count of ‘Extend Disk’ task failures.
  - VolUploadTimeMax: Maximum Time (in MS) taken to upload volume.
  - VolUploadTimeAvg: Average Time (in MS) taken to upload volume.
  - VolUploadCount: Total count of volume upload attempts.
  - VolUploadFailureCount: Total count of volume upload failures.
  - FSMountFailureCount: Total count of fileshare mount failures.
  - FSUnmountFailureCount: Total count of fileshare unmount failures.
  - RequestProcessingCount: Total count of requests processed.
  - RequestProcessingTimeMin: Minimum Request processing time (in MS).
  - RequestProcessingTimeMax: Maximum Request processing time (in MS).
  - RequestProcessingTimeAvg: Average Request processing time (in MS).
  - DBConnectionOpenTimeMin: Minimum time (in MS) for which the DB connection is held.
  - DBConnectionOpenTimeMax: Maximum time (in MS) for which the DB connection is held.
  - DBConnectionOpenTimeAvg: Average time (in MS) for which the DB connection is held.
  - DBConnectionsOpenCount: Average time (in MS) for which the DB connection is held.

Desktone_CommonDatabase

This topic describes the Desktone_CommonDatabase CIM provider.

- Description

  Describes the PostgreSQL server running on database nodes.

- Properties

  - InstanceID: Key to uniquely identify the instance of this class. Set to Desktone_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 Desktone_DatabaseService provider) and divide by the MaxConnections from this class to determine the load on the database server. That is: 100*(Sum(ActiveConnections)/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 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
  ```

Desktone_DatabaseReplicationService

This topic describes the Desktone_DatabaseReplicationService CIM provider.

- Description

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

  - Service provider appliances – Fabric Database (FDB) only

  - Tenant appliances - Fabric Database (FDB), Element Database (EDB), and App Volumes Database (AVDB)

  - Desktop manager appliances - Element Database (EDB) and App Volumes Database (AVDB)

- 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/slon -f /usr/local/desktone/release/
  static/conf/slon_edb.conf
  root 1121     1  0 Sep17 ? 00:00:00 /usr/local/pgsql/bin/slon -f /usr/local/desktone/release/
  static/conf/slon_fdb.conf
  root 1443  1062  0 Sep17 ? 00:07:39 /usr/local/pgsql/bin/slon -f /usr/local/desktone/release/
  static/conf/slon_edb.conf
  root 1446  1121  0 Sep17 ? 00:06:01 /usr/local/pgsql/bin/slon -f /usr/local/desktone/release/
  static/conf/slon_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/slon -f
  /usr/local/desktone/release/static/conf/slon_fdb.conf >/dev/null 2>&1 &
  $ nohup /usr/local/pgsql/bin/slon -f
  /usr/local/desktone/release/static/conf/slon_edb.conf >/dev/null 2>&1 &
  ```

Desktone_DatabaseService

This topic describes the Desktone_DatabaseService CIM provider.

- Description

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

  - Service Provider appliances – Fabric Database (FDB) only
  - Tenant appliances - Fabric Database (FDB), Element Database (EDB), and App Volumes Database (AVDB)
  - Desktop Manager appliances - Element Database (EDB) and App Volumes Database (AVDB)

- 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.

Desktone_HypervisorManagerStatus

This topic describes the Desktone_HypervisorManagerStatus CIM provider.

- Description

  HypervisorManagerStatus provider is derived from CIM_LogicalElement, and it provides information and status of Hypervisor Managers in DaaS platform. The Hypervisor Manager is a 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 or ESX host.
  - Type: describes the type of hypervisor manager whether it is vCenter/ESX and its product version. Ex: "ESX, 5.1.0"
  - CommunicationStatus [derived]: indicates the ability of the DaaS Hypervisor Manager to communicate with Hypervisor Host. 2 – OK, 4 – Lost Communication
  - OperationalStatus [derived]: indicates the current status of the DaaS Hypervisor Manager in DaaS platform. 2- OK, 13 – Lost communication,

  - Status [derived, deprecated]: indicates the current status of DaaS Hypervisor Manager in 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 DaaS appliances and hypervisor hosts.

Desktone_InstalledProduct

This topic describes the Desktone_InstalledProduct CIM provider.

- Description

  Provides information about the 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: Desktone.
  - ProductVersion: Product version information
  - SystemID: Host name where the product is installed.

Desktone_NTPService

This topic describes the Desktone_NTPService CIM provider.

- Description

  NTPService provider is derived from CIM_Service, and it provides information about NTP daemon which runs on DaaS appliance. It also reports time synchronization status.
- Properties
  - CSCreationClassName [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.

Desktone_XMPService

This topic describes the Desktone_XMPService CIM provider.

- Description

  Desktone_XMPService provides information about the XMP service.
- Properties
  - PrimaryStatus: 0 indicates XMP service status Unknown; 1 indicates XMP service status is OK.
- 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.

Description of DaaS CIM Providers

This section describes the DaaS CIM providers.

Descriptions of DaaS CIM providers are linked below.

WBEM and CIM

The DaaS management appliances allow monitoring via the standard WBEM (web-based enterprise management)/CIM (common information model) interface.

You can install the wbemcli client, which can be used with queries or with plugin scripts in conjunction with tools like Nagios for monitoring. You can also use any tool which supports WBEM/CIM management, such as open source clients like OpenPegasus browser client, CImNavigator, openPegasus CLI client, and MS CIM Studio. The DaaS platform, however, has only been tested with the wbemcli client tool for CIM data verification.

Note the following:

- For security purposes, the only account that has access to CIM monitoring services is cim-user. You set the password for this account during the bootstrap process. As a result, scripts and plugins must be updated to specify the cim-user credentials. For example:

  ```
  wbemcli -noverify -nl -v ei 'https://cim-user:Desktone!#$%@10.31.20.25:5989/root/
  cimv2:Desktone_InstalledProduct'
  ```

- Small Footprint CIM Broker (SFCB) uses the appliance certificate instead of a self-signed certificate, enabling the client to verify the certificate/server identity. As a result, queries to CIM providers can be made by specifying the platform public CA file or adding it as a trusted certificate on the client machine. This change is optional, but it is recommended that clients be updated. The Service Provider administrator can pull the public CA certificate (/usr/local/desktone/cert/rootCA.pem) from the SP appliance. The public CA certificate is common for all appliances. For example:

  ```
  wbemcli  --cacert /etc/daas-cim/client.pem -nl -v ei 'https://cim-user:Desktone!#$
  %@10.31.20.25:5989/root/cimv2:Desktone_InstalledProduct'
  ```

  Note The copied rootCA.pem is renamed client.pem in example above. This renaming is not necessary.

Connection Matrix

8

The connection matrix shows details for connections, including ports used and connectivity type.

Abbreviations used in the connection matrix are as follows.

Management Appliances	Networks	Other
SP - Service Provider	T - Tenant Network	HYP -Hypervisor
DM - Desktop Manager	SP - Service Provider Network	SS - Storage System
RM - Resource Manager	BB - Backbone Network	NFS - NFS Server
T - Tenant	I - Public Internet	VM - Virtual Desktop VM
UP - Upload Server		EP - End Point Device
UAG - Unified Access Gateway		AD - Active Directory
ES - Enrollment Server		MON - Monitoring System
		RSA - RSA Authentication Manager
		WP = Web Proxy

Source	Destination	Ports In Use	Networks	Description	Connectivity Type
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

Source	Destination	Ports In Use	Networks	Description	Connectivity Type
SP	RM	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	RM	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	SP	Used to authenticate users to the Service Center.	Local and Remote
SP	WP	tcp/443	I	Used for Cloud Monitoring Service (CMS). If an SP appliance cannot access internet directly, you can configure a proxy on the SP to access CMS services (in AWS). The proxy config is in the cloud_config table in the SP FDB.	Remote

Source	Destination	Ports In Use	Networks	Description	Connectivity Type
RM	SP	tcp/8443	BB	Used for invoking remote APIs via web services. Authentication is done via username/password and SSL certificate validation.	Local Only
RM	SP	tcp/20677	BB	Used for proxying traffic between DCs	Local Only
RM	RM	tcp/11211	BB	Used for accessing memcached	Local Only
RM	T	tcp/8443	BB	Used for invoking remote APIs (state monitoring) via web services. Authentication is done via username/ password.	Local Only
RM	HYP	tcp/443	SP	Needed for access to the hypervisor management APIs. Authentication is done via username/password.	Local Only
RM	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
RM	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	AD	AD servers: tcp/3268	T/SP	Global catalog port on AD servers for LDAP.	(Remote for T) and (Local or Remote for SP)
T/SP	AD	AD servers: tcp/88	T/SP	Kerberos (for new, more secure LDAP communication & password change functionality)	(Remote for T) and (Local or Remote for SP)
T	RM	tcp/6443	BB	Used for connection to Resource Manager proxy (on backbone network) to provide App Volumes with vCenter connectivity.	Local Only
T	T	tcp/4002	T	Handles connections from agents. When agents startup they connect to the message bus on this port on one of the Desktop Managers so that they can receive messages from them.	Local Only
T	T	tcp/4101	BB	Used for router clustering. JMS routers on HA pairs connect to each other on this port so that they can route messages between Desktop Managers and ensure messages reach the agent, regardless of which Desktop Manager the agent is connected to.	Local Only
T	T	tcp/6443	Localhost only	Listens on localhost only for requests to vCenter from App Volumes.	Local Only

Source	Destination	Ports In Use	Networks	Description	Connectivity Type
T	RM	tcp/6443	BB	Listens on backbone network only, to provide App Volumes on Tenant & Desktop Manager appliances with vCenter connectivity.	
T	T	tcp/4001	Localhost only	Listens on localhost only for messages from Desktop Managers.	Local Only
T	T	tcp/6443	Localhost only	Listens on localhost only for requests to vCenter from App Volumes.	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	RM	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	RM	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

Source	Destination	Ports In Use	Networks	Description	Connectivity Type
T	VM	tcp/ 1025-5000	T	Used for downstream communication between the DaaS Agent (on a Windows 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 DaaS tenant appliance to the VMware View connection agent that runs in the desktop.	Local Only
T	AD	tcp/389	T	Used to authenticate users to the User Portal. Additionally the configured user groups and their members are cached in the tenant fabric for performance purposes.	Local and Remote
T	RSA	udp/5500	T	Used for communicating with the RSA Authentication Manager when SecurID is in use by the tenant.	Local and Remote
T	UAG	tcp/443	T	Used for Blast	Remote
T	UAG	tcp/8443	T	Used for Blast	Remote
T	UAG	tcp/4172 udp/4172	T	Used for PCoIP	Remote
T	UAG	tcp/80	T	Redirects to 443	Remote
T	WP	tcp/443	I	Used for Cloud Monitoring Service (CMS).	Remote
VM	T	tcp/3443	T	Listen port for App Volumes Agents.	Local Only
VM	T	tcp/3443	T	Listen port for App Volumes Agents.	Local Only
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

Source	Destination	Ports In Use	Networks	Description	Connectivity Type
UP	NFS	tcp/2049	SP	Used for storing the desktop images uploaded from tenants to NAS. Authentication is done via network identity.	Local Only
ES	T	tcp/32111	T	Used for True SSO.	Remote 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	RM	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