

Horizon DaaS Platform 6.1 Tenant Installation - vCenter

This guide provides information that is specific to installing and configuring a Tenant appliance in a datacenter using **vCenter** after installing or upgrading and configuring the Service Provider appliance and Resource Manager.

Error! No text of specified style in document.



Revision History

Date	Version	Description
09/04/2013	1.0	Initial release
10/06/2014	1.1	First revision
10/20/2014	1.2	Second revision

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

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

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

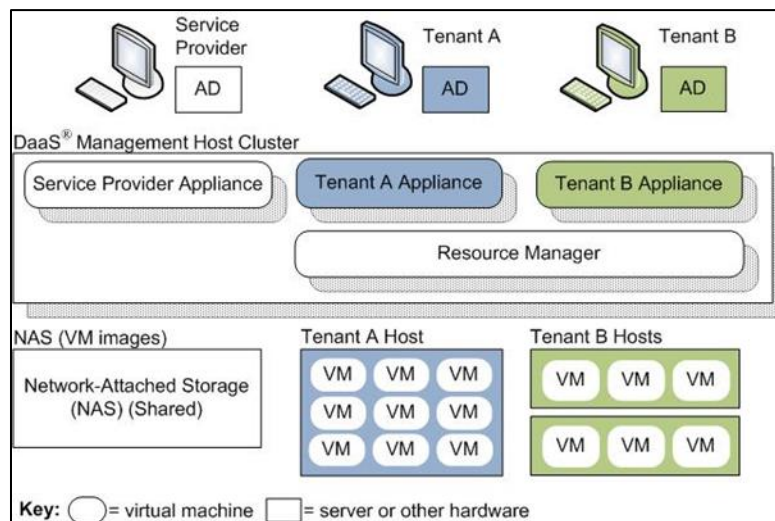
Contents

1 Overview	1
2 Tenant Installation Prerequisites	2
2.1 Discovery and Assignment	2
2.2 Enterprise Network Connectivity	2
2.3 Tenant Network Configuration	2
2.4 DNS Configuration	3
2.5 Allocate Tenant IP Addresses	3
2.6 Define or install DHCP service for the tenant.	3
2.7 Active Directory Configuration	3
2.8 Tenant Remote Access	4
2.9 SSL Certificate	4
2.10 (Optional) Install NetApp Virtual Storage Console for vSphere	5
3 Tenant Installation	6
3.1 Create Tenant Appliances	6
3.2 Add Desktop Compute Resources	7
3.3 (Optional) Configuring the Netapp Virtual Storage Console	8
3.4 Assign Resources to Tenant	8
3.5 Assign Networks to Desktop Manager(s)	9
3.6 Assign Desktop Model Quotas	9
3.7 Assign Protocol Quotas	9
3.8 Set up dtRAM	10
3.9 Enter the Tenant's AD Information	10
3.10 Apply Tenant Certificates to Tenant Appliances	11
3.10.1 Generate Tenant Certificates	11
3.10.2 Apply Tenant Certificates	11
3.11 Extending a Tenant Across Datacenters	12
3.11.1 Adding a Network Component	12
3.11.2 Adding Appliances	13
Appendix A Create a Virtual HA dtRAM	14
A.1 dtRAM Overview	14
A.2 Prerequisites	15
A.3 Obtain Network Information and Network Addresses	15
A.4 Create VMs using vSphere VI Client	16
A.5 Set Network Security Settings	17
A.6 Set Net.ReversePathFwdCheck and Net.ReversePathFwdCheckPromisc	18
A.7 Install dtRAM - Backup	19
A.8 Enable Web Configuration - Slave	19
A.9 Install dtRAM - Master	20
A.10 Setup dtRAM Console	22
A.11 Check the carp Interface	22
A.12 Final Configuration Steps	23
A.13 Verify the dtRAM Daemon is Running	23
A.14 Testing the dtRAM	23
A.15 Enabling dtRAM Policy	24
A.16 Adding a dtRAM Configuration	24

Appendix B Create a Windows 7 Gold Template	25
Appendix C Tenant Installation Worksheet	27

1 Overview

The DaaS platform software allows you to manage your tenant desktops using VMware vCenter hypervisor management software. This guide provides you with information that is specific to 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 document to help you collect and organize all the information needed to complete the install. Please consider that the installation process explained in this document is dedicated to standing up a tenant in the DaaS platform. 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.

2 Tenant Installation Prerequisites

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

The supported combinations for managing your tenant desktops with vCenter are the following:

Table 2–1 vCenter used as Hypervisor Manager

	ESXi 5.0	ESXi 5.1	ESXi 5.5
vCenter v 5.1	Supported	Supported	Supported

2.1 Discovery and Assignment

Configure an account in the vCenter for the DaaS platform 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. . If you are using the same vCenter, all the hosts required for management appliances and tenant desktops must be in the same vCenter DataCenter.

Important: 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).

2.2 Enterprise Network Connectivity

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.

2.3 Tenant Network Configuration

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 a single or multiple VLANs or a single Distributed Virtual Port Group (DVPG) to the tenant. At least one of these VLANs or DVPG 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.

Important: DVPG must be configured to use ephemeral port binding.

2.4 DNS Configuration

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.

2.5 Allocate Tenant IP Addresses

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

- 2 IPs for the Management Appliances themselves
- 1 IP to be shared between the Appliances
- 3 IPs for Remote Access via a dtRAM appliance
- (Optional) 1 IP if the tenant has backhaul to a DHCP server. This will be used for the DHCP relay service

2.6 Define or install DHCP service 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

2.7 Active Directory Configuration

Define or install tenant Active Directory. The tenant must configure their Active Directory as shown below and have the information ready to be used during the installation. It is highly recommended that you confirm the values using an AD tool such as AD Explorer:

<http://technet.microsoft.com/en-us/sysinternals/bb963907>

Table 2–2 Network Information for DaaS Management Host

Configuration	Example
NETBIOS	TENANT
Domain Suffix	ad.tenant.local
Protocol	ldaps
Port	636
Context	dc=ad,dc=tenant,dc=local
Primary DNS Server IP and name	172.16.109.2 You only need to specify one Directory Server - the rest should be automatically identified
Service Account	CN= Administrator,CN=Users (UserMustChangePassword = false, Password Never Expires) Do not include the context in the name. The Service Account is used to parse your AD structure through a standard LDAP query. This account may be read only.
Service Account Password	ADPasswd
Domain Join Account Name	Dtjoindomain (name only) The Domain Join Account is used to automatically join provisioned desktops to your domain. This account need only have domain join privileges.
Domain Join Account Password	Password
Super Admin (Enterprise Center Access)	cn=dtEnterpriseAdmins,ou=groups (do not include the context)
Admin Level1 (Optional)	cn=Admin-1,ou=groups
User Groups	cn=Users,ou=groups (do not include the context)

2.8 Tenant Remote Access

If the customer requires virtual HA dtRAM, complete the instructions listed in Creating a Virtual HA dtRAM in Appendix A. If the tenant has backhaul and is using dtRAM for access from the public internet, be sure to add the list of internal customer IP addresses which should bypass the dtRAM.

2.9 SSL Certificate

If the tenant requires a certificate, the customer must provide the service provider with the necessary certificate files in Apache SSL format. For more details, see [Apply Tenant Certificates to Tenant Appliances](#).

2.10 (Optional) Install NetApp Virtual Storage Console for vSphere

The NetApp Virtual Storage Console (VSC) for vSphere **must be installed on the same machine** as the vCenter server. When registering the VSC plug-in with vCenter, use the vCenter administrator account credentials, which will also be used to discover the desktop hypervisor in section 3 of this document.

Supported versions of VSC are 4.1-P1 and 4.2.1.

For further information please refer to the NetApp VSC installation and configuration guide.

3 Tenant Installation

Overview

To install the tenant, you complete the following tasks:

1. Create tenant appliances.
2. Add desktop host(s).
3. Assign tenant appliances to resource managers.
4. Assign quota.
5. Add dtRAM and configure internal networks.
6. (Optional) Enter the Tenant's Active Directory information.

3.1 Create Tenant Appliances

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 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 Table 3-1 (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.

Table 3–1 Data Centers

Field	Sample Value	Notes
Network ID	115	VLAN ID or DVPG Name
Network ID Type	VLAN	VLAN 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	

- On the Custom Fields tab, enter any site-specific information you want to maintain. These are free-form text fields with no data validation; the content is entirely up to you.
- After entering your information on the General Info, Networks, and Custom Fields tabs, select Save and Create Appliances.
- On the Tenant Install page, enter values for the fields listed in Table 3-2 (primary and secondary).

Table 3–2 Schedule Tenant Creation

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		

- Wait for the system to spawn your tenant appliances (time will vary depending on infrastructure). If you want to check the status of a reservation, select appliances ► reservations.
- Verify that the appliances were created.

3.2 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 pools
- 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.
 - Select the Compute Resources panel.

The page redisplay with the Add Host Manager tab next to the General tab.

- Click the Add Host Manager tab and enter values for the fields listed in Table 3-3.

Table 3–3 HA Server

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

- Click the Add button.

If you have multiple vCenter Datacenters configured, select the one that will be used for the desktop hosts. If you have only one vCenter Datacenter, you will not be prompted to select it.

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

3.3 (Optional) Configuring the Netapp Virtual Storage Console

If you are **not using** the Netapp Virtual Storage Console (VSC) for storage then skip this section and proceed to the next section. There is no need to define storage when managing with vCenter in the DaaS platform as this is already configured through the vCenter client.

If you are using the Netapp VSC plugin for storage perform the following steps:

- Service Center, select Service Grid ► Resources.
- Select the “Service Provider RMGR” in the pane on the left, then Storage Systems in the pane on the right.
- On the Storage Systems tab, select the Add Storage System link.
- Enter values for the fields listed in Table 3-4.

Important: When adding a storage system (controller) to the DaaS platform, the Address field must match how the storage system was discovered in the VSC on vCenter. If the storage system was discovered as an IP address you must enter the IP address in the Address field. If it was discovered as a FQDN, then you must enter the complete domain name in the Address field.

Table 3–4 Storage System

Field	Sample Value
Address	storage.desktone.com or 172.16.10.21
Username	root
Password	storagePswd

- Click the Add Storage System button.

The system adds the name of the storage system to the Storage Systems tab.

3.4 Assign Resources to Tenant

- In Service Center, select Service Grid ► Resources.
- Select the Desktop Managers pane.
- 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.
6. For each selected compute resource, a capacity popup will be displayed. 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.

3.5 Assign Networks to Desktop Manager(s)

1. In Service Center, select Service Grid ► Resources to display the Resources screen and select the Desktop Managers tab
2. In the tab, you will find the desktop managers listed as <tenant name>_<desktop manager name>. Click on the Desktop Manager in question 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 don't 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 1 network. The assigned networks affect what VMs will be detected as belonging to the Desktop Manager.

3.6 Assign Desktop Model Quotas

1. In Service Center, select Tenants ► Browse Tenants.
2. In the table, click Edit for the tenant which you wish to alter, the Editing Tenant page displays.
3. Select the Quotas tab. This panel displays all of the controlling Quotas which regulate what a Tenant is allowed to use at provisioning and desktop connection time. Included are the Protocol Quotas, Gold Pattern Quotas, RDS Session Quotas, and Desktop Model Quotas.

Desktop Model Quotas are assigned by Desktop Manager and will be calculated based on assigned compute and its associated population density (# of VMs).

4. Select the Datacenter & Desktop Manager from the drop downs which you wish to assign Quota to. Add the amount desired to the VM Quota Column. Click Update and a status window will appear after Quota assignment.

Note: You must enter a number that is at least as large as the In Use amount.

3.7 Assign Protocol Quotas

1. In Service Center, select Tenants ► Browse Tenants.
2. In the table, click Edit for the tenant for which you are applying the tenant model.

The Editing Tenant page appears.

3. Select the Quotas tab.

The Quotas tab displays a table listing all the protocol quotas available.

4. If there are more than 1 datacenter for this Tenant, select the Data Center from the drop down that you wish to assign Quota to.
5. Under the Protocol Quota section, enter a value in the Quota column or select the unlimited checkbox. This Quota will be applied across the Tenant in a given Datacenter.
6. Click Update and a status window will appear after Quota assignment.

3.8 Set up dtRAM

If the tenant has opted to use a dtRAM to connect to their desktops, the Service Provider needs to install and configure dtRAM as explained in [Appendix A](#).

3.9 Enter the Tenant's AD Information

Omit this step if the tenant will be entering their own AD information.

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.

1. In the Enterprise Center, enter values for the fields listed in Table 3-5.

Table 3–5 Tenant Active Directory

Field	Sample Value
Name	TENANT
Domain	ad.tenant.com
Protocol	ldaps
Port	636
Nameserver	172.16.109.2
Context	dc=ad,dc=tenant,dc=com
Service Account	CN=Administrator,CN=Users
Password	TenantAPsswd
Admin Group	cn=enterprisecenteradmin,ou=groups
User Group	cn=portalusers,ou=groups
Admin User	Administrator
Password	AdminPsswd
Primary DNS	172.16.109.2

2. After entering this information, click Register.

The DaaS Enterprise Center login screen is displayed for the tenant.

3.10 Apply Tenant Certificates to Tenant Appliances

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

- If the tenant does not already have a certificate, you may generate it following the instructions in section 3.10.1 below.
- If it already has a certificate, proceed directly to section 3.10.2

3.10.1 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 generating on the Service Provider appliance, please 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

```
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

This will generate 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/desktopone/cert on the tenant node so they are backed up by the automated backup process.

3.10.2 Apply Tenant Certificates

The DaaS platform 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.

Backing Up: Copy the files to /usr/local/desktopone/cert/temp on the primary Tenant appliance so they are backed up by the automated backup process.

Upgrading: If you are upgrading to the latest release of the DaaS platform, your existing certificates are not automatically imported. Make sure you have a backup copy of the three files so that you can upload them again.

3.11 Extending a Tenant Across Datacenters

Note: You must have already created another Datacenter before you can extend a tenant to that Datacenter. See Appendix A of the Service Provider Installation document for instructions on creating a second datacenter.

3.11.1 Adding a Network Component

1. In Service Center, go to the Tenants page and click the **Edit** button for the Tenant to be extended.
2. On the Networks tab, select the required datacenter in the Data Center dropdown.
3. Click the **Add Network Component** link.
4. Enter values for the fields listed in Table 3-6.

Note: The extended tenant must be placed on a different network than the tenant in the first datacenter.

Table 3–6 Network Component

Field	Sample Value	Notes
Network ID Type	VLAN	VLAN or DVS
Network ID	118	VLAN ID or DVPG Name
Network Label	My Network	Free Form Text Field
Gateway	172.16.118.1	
Subnet mask	255.255.255.0	
DNS Name	172.16.115.2	Directory Name server (Usually the same as the DC1 tenant)

- After entering your information, select **Add Network Component**.

3.11.2 Adding Appliances

- On the Appliances tab, select the **Add Appliances** link.
- Select the required datacenter in the Data Center dropdown.
- Enter values for the fields listed in Table 3-7.

Table 3–7 Tenant Install

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

- Wait for the system to spawn your tenant appliances (time will vary depending on infrastructure). If you want to check the status of a reservation, select appliances ► reservations.
- Verify that the appliances were created.
- Return to [Add Desktop Compute Resources](#) above and follow the steps to complete the extended tenant setup.

Appendix A Create a Virtual HA dtRAM

DaaS supports a virtual dtRAM, a DaaS remote access manager hosted on two VMs. This appendix contains the following sections, which explain how to create a virtual HA dtRAM:

- Overview
- Prerequisites
- Obtain Network Information and Network Addresses
- Create VMs using vSphere VI Client
- Set Network
- Set Net.ReversePathFwdCheck and Net.ReversePathFwdCheckPromisc
- Install dtRAM - Backup
- Install dtRAM - MasterSetup dtRAM Console
- Check the carp Interface
- Verify the dtRAM Daemon is Running
- Enabling dtRAM Policy
- Adding a dtRAM Configuration

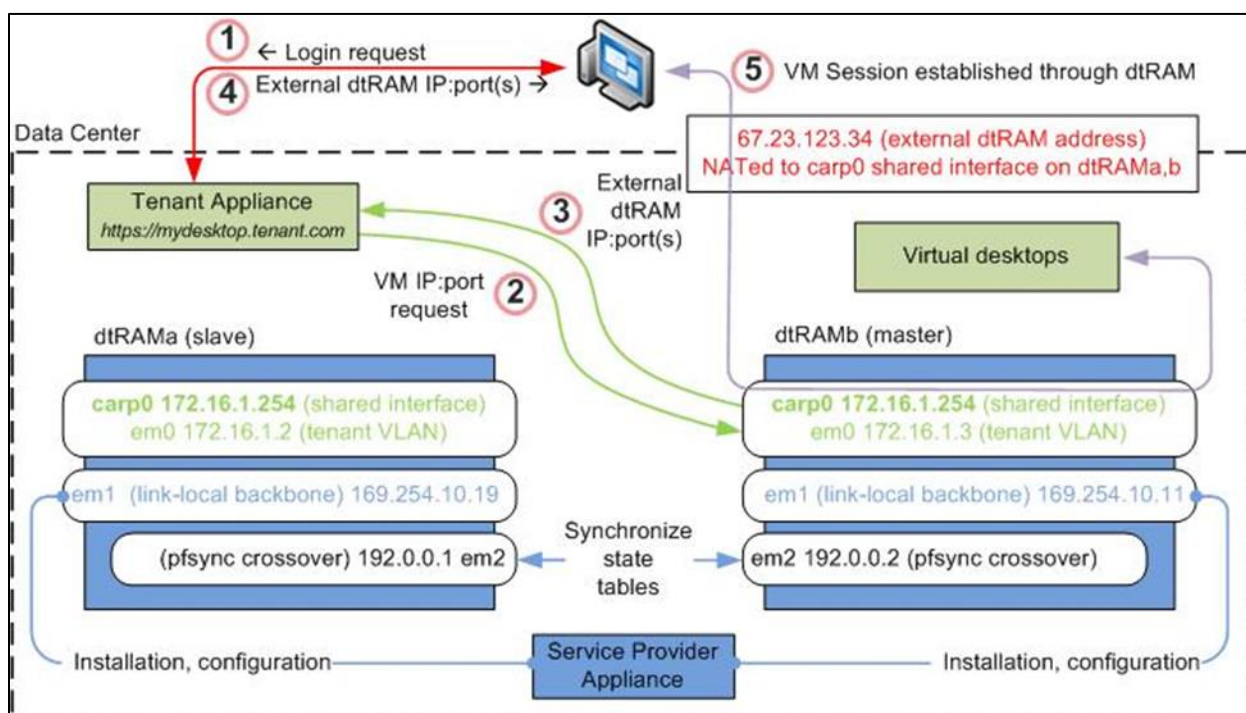
A.1 dtRAM Overview

The DaaS remote access manager (dtRAM) allows end users outside a tenant's internal network to access their virtual desktops. The dtRAM is software that runs on two physical or virtual servers to allow hitless failover high-availability.

Note that all virtual desktop sessions run through the dtRAM while the sessions are active, so remote access bandwidth is limited by the capacity of the dtRAM.

Figure 1 shows the interfaces and data flow between an HA dtRAM, the Tenant Appliances, and the router that NATs an external IP address to the shared (carp0) address of the dtRAM. (Note that, on a FreeBSD machine, the network interfaces are named after the device used. For example: em0, em1.) This diagram also illustrates the two stages of the dtRAM process: setting up the virtual desktop connection; and maintaining that connection after it has been established.

Figure 1: HA dtRAM Interfaces and Data Flow



A.2 Prerequisites

The following are the prerequisites for the dtRAM install.

- Three additional IP addresses in the tenant subnet (one for each dtRAM plus a “floating” address).
- Setup external NATs for access to the portal and to the floating dtRAM IP address.
- Open the firewall rules for ports 80 and 443 for the portal.
- For the dtRAM, you typically open ports 8001 – 8050. For multiple ports you can open other port ranges, for example 9001 – 9050.
- Setup an external DNS record for the portal and for the dtRAM.
- The .ova file for the dtRam has been uploaded to one of the datastores on the hypervisor.

A.3 Obtain Network Information and Network Addresses

To set up an HA dtRAM, you need to obtain the IP addresses shown in Table 3-6 and Table 3-7. You also need the following network information:

Table 3–8 Network Information for Creating Virtual HA dtRAM

Node	Tenant IP (an IP in the tenant network – em0)	Link local backbone IP (em1)	Crossover (em2)
Tenant-dtram1		169.254. .	192.168.1.
Tenant-dtram2		169.254. .	192.168.1.
dtRAM-carp			

- Bit count for shared network (for example, 24 for a /24 CIDR-notation network)
- Gateway for shared network
- DNS server (or "none")

Table 3–9 Common IP Addresses for HA dtRAM

Address	Description
External Address	You need an external IP address that is NATed to the shared internal dtRAM address (carp0). If the Tenant is using an FQDN for the dtRAM, the Tenant must be able to resolve the FQDN to the external IP address, not the shared internal dtRAM address.
Carp0 address	This is the shared address on the tenant VLAN that is used to access both VMs in the HA pair.

You need a set of the IP addresses listed in for each VM in an HA pair. The customary interface is indicated in parentheses.

Table 3–10 Individual IP Addresses for HA dtRAM

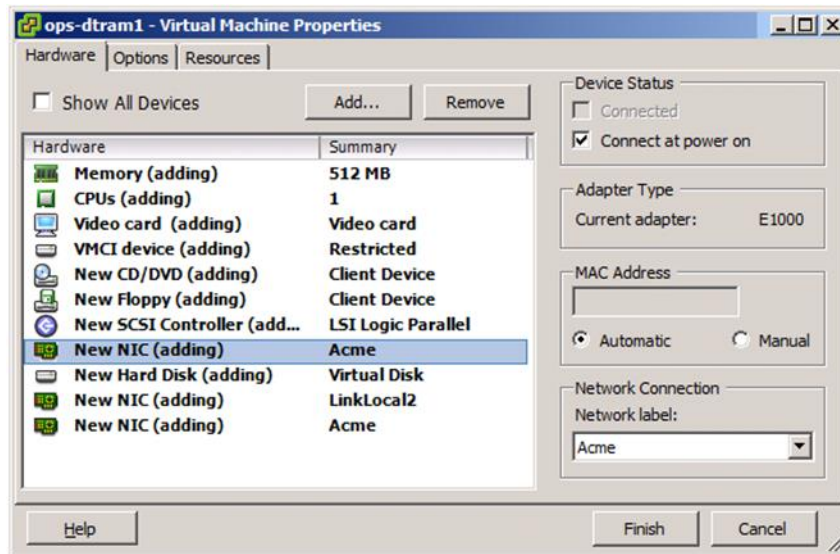
Address	Description
Tenant VLAN IP address (em0)	This IP address is used to connect via the external IP address and the carp0 address.
Management VLAN IP address (em1)	This IP address is used for communications from the Service Provider appliance.
Crossover IP address (em2)	This IP address is used to maintain state-table synchronization between the two VMs in an HA pair. This interface is solely for communication between these two VMs and is typically an address in the 192.168.0.0/16 space.

A.4 Create VMs using vSphere VI Client

Use vSphere VI client to create two new VMs for an HA dtRAM:

- 512 MB memory
- Disk: 8.00 GB
- OS: 32-bit FreeBSD
- 3 NICs NOTE: - You must use E1000 NICs, the VMXNET will not work.

The following figure presents an example of what the dtRAM will look like. The Tenant network in this example is Acme.



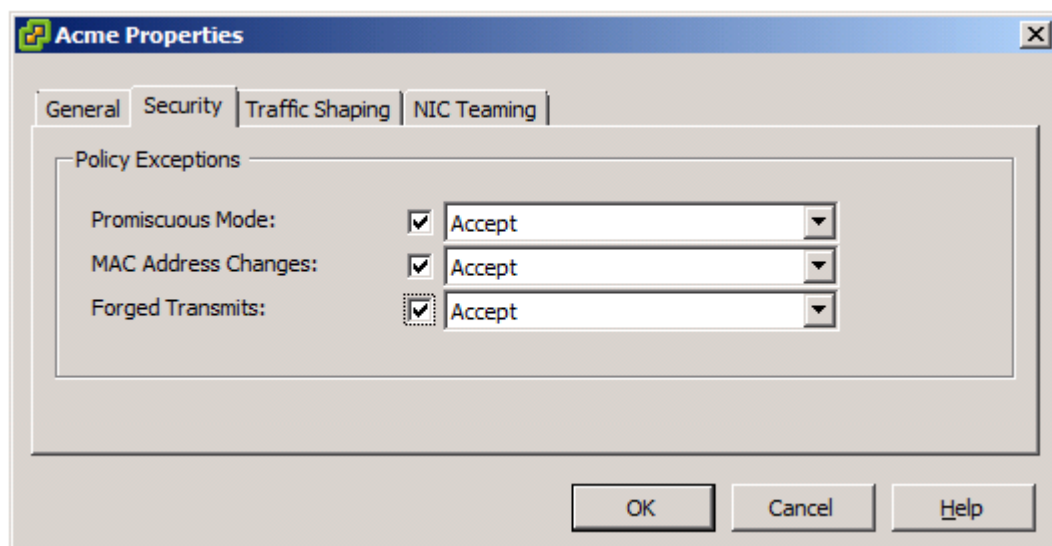
A.5 Set Network Security Settings

Note: This procedure in this section is not required when using the Cisco Nexus 1000v DVS. It is required when using the VMware DVS or standard vSwitch.

This setting applies for vSphere hosts. Make sure the network that carp0/em0 is connected to is set per the below security configuration settings for the tenant VLAN in the in the vSwitch. To check the network mode, perform the following steps.

Procedure

1. Select the vSphere hosting your dtRAMs.
2. Select the network that the carp interface and em0 are on.
3. In the Edit Settings dialog, select the Security tab.
4. Make sure all of the options are enabled



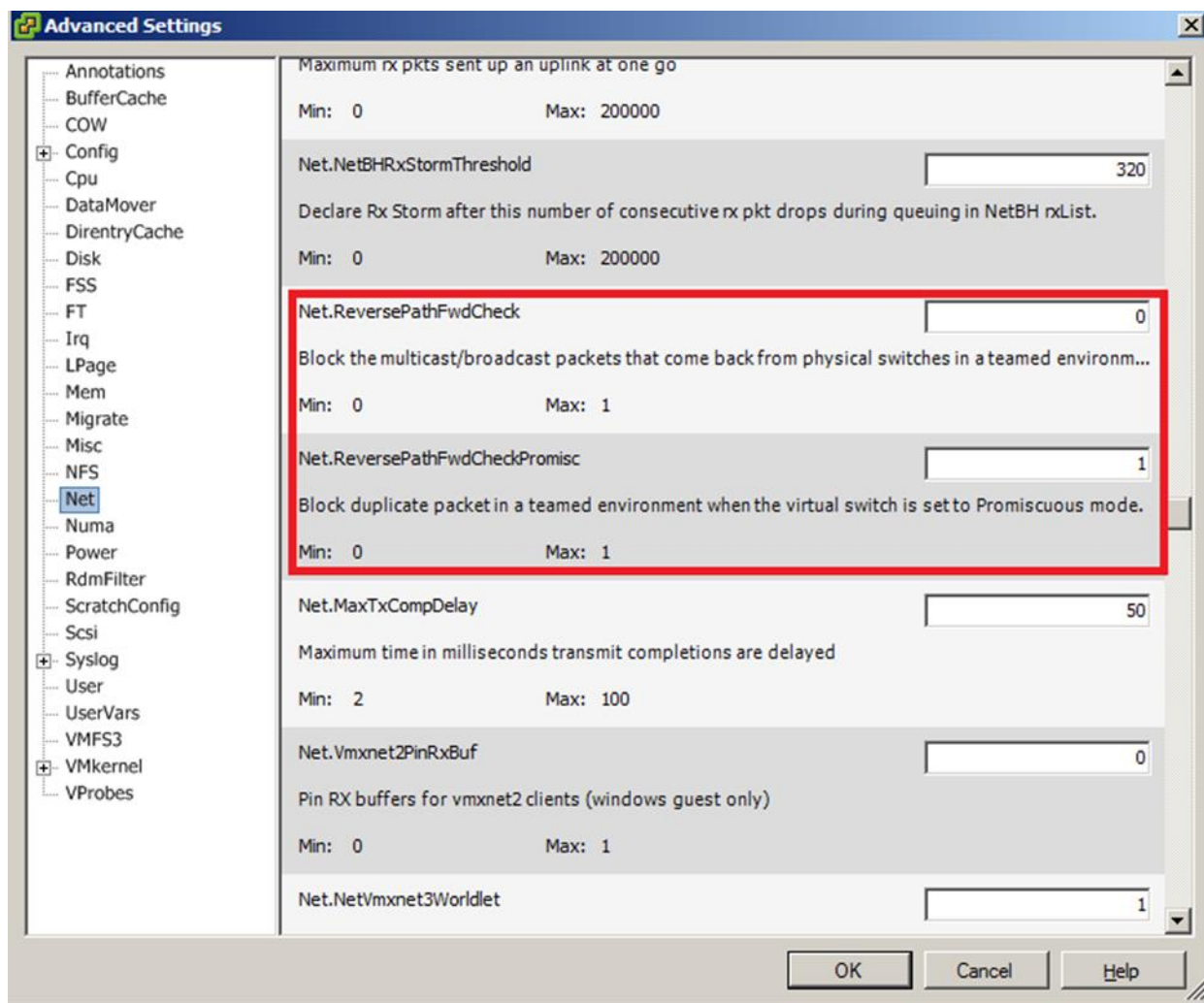
A.6 Set Net.ReversePathFwdCheck and Net.ReversePathFwdCheckPromisc

Note: This procedure in this section is not required when using the Cisco Nexus 1000v DVS. It is required when using the VMware DVS or standard vSwitch.

If the vSphere hosting your dtRAM VMs has multiple physical NICs tied to a vSwitch, you need to disable this setting. Otherwise, the packets destined for carp0/em0 in an HA dtRAM cannot reach their destinations. To change these settings, perform the following steps.

Procedure

1. Select the vSphere hosting your dtRAM.
2. On the Configuration tab, select Net in the Advanced Settings (Software) panel.
3. Enter the value 0 for the Net.ReversePathFwdCheck setting.
4. Enter the value 1 for the Net.ReversePathFwdCheckPromisc setting.



Important: After setting Net.ReversePathFwdCheck and Net.ReversePathFwdCheckPromisc as well as the Network Security Settings you need to reboot the vSphere host.

A.7 Install dtRAM - Backup

Procedure

1. You will first be prompted for which interfaces will be used for what (INTERNAL,MANAGEMENT,CROSSOVER) Enter these values in this order:
 - em0
 - em1
 - em2
2. Enter "y" to proceed.
3. You will now be prompted to enter the "INTERNAL IPv4 address". This is the Tenant IP address for the dtRAM.
4. Now enter the netmask in CIDR form for the Tenant IP.
5. Now enter the gateway address in the Tenant network.
6. Enter "none" as DNS is not required for the dtRAM.
7. You will now be prompted for the "EXTERNAL IP" address. There are two options:
 - a. FQDN (Fully Qualified Domain Name) of the dtRAM. The Tenant must be able to resolve the FQDN to the external IP address, not the shared internal dtRAM address.
 - b. Public IP address which has been setup to NAT to the carp0 address of the dtRAMs.
8. Enter "N" for Slave.
9. Next you are prompted for the type of IP address that will be used for the management network. Enter "4".
10. Now enter the Management IP address that will be assigned to this dtRAM (Link Local).
11. Enter the netmask of the Management network (Link Local).
12. Next you are prompted for the "CROSSOVER IPv4 address". Enter the CROSSOVER IP which is going to be applied to this dtRAM.
13. Enter the netmask of the network for the CROSSOVER network.
14. Next you are prompted to enter the "target IP address". This is the CROSSOVER IP address of the Master dtRAM.
15. The dtRAM will now complete the installation, and configuration.

A.8 Enable Web Configuration - Slave

Procedure

- ▶ On slave dtRAM, select menu item 11 - Restart webConfigurator.

A.9 Install dtRAM - Master

Procedure

1. You will first be prompted for which interfaces will be used for what (INTERNAL,MANAGEMENT,CROSSOVER) Enter these values in this order:
 - em0
 - em1
 - em2
2. Enter "y" to proceed.
3. You will now be prompted to enter the "INTERNAL IPv4 address". This is the Tenant IP address for the dtRAM.
4. Enter the netmask in CIDR form for the Tenant IP.
5. Enter the gateway address in the Tenant network.
6. Enter "none" as DNS is not required for the dtRAM.
7. You will now be prompted for the "EXTERNAL IP" address:
 - a. FQDN (Fully Qualified Domain Name) of the dtRAM. The Tenant must be able to resolve the FQDN to the external IP address, not the shared internal dtRAM address.
 - b. Public IP address which has been setup to NAT to the carp0 address of the dtRAMs.
8. Enter "Y" for Master.
9. You are now prompted for the "Shared IP address". Enter the CARP/Floating address here.
10. You are prompted for the VHID for this Shared CARP IP address. You can accept the default value of 1, which indicates you are using a single pair of dtRAMs on a single VLAN.
11. Next you are prompted for the type of IP address that will be used for the management network. Enter "4".
12. Now enter the Management IP address that will be assigned to this dtRAM (Link Local).
13. Enter the netmask of the Management network (Link Local).
14. Next you are prompted for the "CROSSOVER IPv4 address". Enter the CROSSOVER IP which is going to be applied to this dtRAM.
15. Enter the netmask of the network for the CROSSOVER network.
16. Next you are prompted to enter the "target IP address". This is the CROSSOVER IP address of the Slave dtRAM.
17. Enter the password "desktone" and press enter.
18. You are now prompted for the "Element IP address range". This should be a list of the 2 tenant appliance IPs separated by a comma. For example : 172.22.4.20,172.22.4.21
19. Now enter the range of ports to be used by the dtRAM. This range should match what has been configured in the firewall for open ports.
20. Press enter to accept port 8000 for the dtRAM to listen on.
21. The master dtRAM will now complete the install, and perform its configuration.

Sample dtRAM Installation Transcript

```
Enter the new INTERNAL IPv4 address.
> 172.16.110.26
Subnet masks are entered as bit counts (as in CIDR notation)
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8
Enter the new INTERNAL IPv4 subnet bit count
> 24
The INTERNAL IPv4 address has been set to 172.16.110.26
Please enter a gateway IP address for INTERNAL. It must be in the 172.16.110.26/24
subnet.
> 172.16.110.1
Please enter a DNS server to use for hostname resolution.
Enter 'none' if you do not have a local DNS server.
> none
Using 8.8.8.8 (Google public DNS) since no DNS server was chosen.
We need An EXTERNAL IP address.
This is the public IP address that is accessible to all.
This could be a DNS name or NAT'ed IP address.
Enter EXTERNAL address.
> 172.16.110.27
Will this system be the MASTER unit of a High-Availability pair?
Enter Y for Yes (Master), N for No (Slave).
[Y]> Y
Enter the Shared IP address for CARP network.
This is the common IP set on both the RAM1 and RAM2 for carp0
> 172.16.110.27
Enter the VHID for this Shared CARP IP address.
This ID must be unique for each CARP IP on a network.
[1]>
What type of IP address will be used on the MANAGEMENT interface?
Enter '4' for IPv4, and '6' for IPv6.
> 4
Enter the new MANAGEMENT IPv4 address.
> 172.16.110.78
Subnet masks are entered as bit counts (as in CIDR notation) in .
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8
Enter the new MANAGEMENT IPv4 subnet bit count
> 24
The MANAGEMENT IPv4 address has been set to 172.16.110.78
Enter the new CROSSOVER IPv4 address.
> 192.168.110.26
Subnet masks are entered as bit counts (as in CIDR notation) in .
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8
Enter the new CROSSOVER IPv4 subnet bit count
> 24
The CROSSOVER IPv4 address has been set to 192.168.110.26
Please enter the target IP address for synchronization.
This is typically the CROSSOVER IP address of the SLAVE unit.
> 192.168.110.25
Please enter the password for the SLAVE unit.
This is needed for configuration synchronization.
>
```

```

The following will capture the Element IP addresses in a tenant Network. RAM servers
are configured per a Tenant.
We can either specify a range or Individual Element IP's with comma separated values.
Enter the Element IP address range. (Example: 172.16.101.0/24 OR
172.16.101.1,172.16.101.3)
> 172.16.110.0/24
How many port ranges will be used for the Remote Desktop Protocol? [Enter a value of
1.]
> 1
Please enter port range.
Range can be given using a Lower Integer # - Higher Integer #
Example: 8001 - 8255
> 8001-8100
Enter the listen PORT number
[8000]>
Configuring dtRAM XML and restarting dtRAMd...
Configuring dtRAM XML and restarting dtRAMd...Updating system configuration...Reloading
and reconfiguring system, please wait...

```

A.10 Setup dtRAM Console

Once you install the dtRAM, the dtRAM Console is available:

```

**Welcome to DaaS® Fabric Edge Appliance 2.0.2-RELEASE (amd64) on deskstone **

```

```

MANAGEMENT (lan)      -> em1      -> 169.254.107.23
INTERNAL (wan)         -> em0      -> 172.16.112.23
CROSSOVER (opt1)      -> em2      -> 168.254.80.23

0) Logout (SSH only)      8) Shell
1) Assign Interfaces      9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults 12) Developer Shell
5) Reboot system          13) Upgrade from console
6) Halt system            14) Disable Secure Shell (sshd)
7) Ping host

17) Enter the Element IP address range & Configure DTRAM
18) Please enter port range & Configure DTRAM
19) Enter the listen PORT number & Configure DTRAM
20) Set all interface IP addresses & Configure DTRAM
21) Force a filter sync.
22) Restart webService.
23) Configure port list to be natted
30) VMWare Tools Menu.

```

For example, you can use the Console to:

- Enable/Disable SSH: Use menu item 14 to toggle SSH.
- Install VMware Tools: Run menu item 30 and then select 2 to activate VMware Tools.

A.11 Check the carp Interface

Once both dtRAM VMs are installed, you should be able to check the carp interface. One should be MASTER, one should be BACKUP:

```
[2.0.2-RELEASE][root@desktone.local]/root(1): ifconfig vip1
vip1: flags=49<UP,LOOPBACK,RUNNING> metric 0 mtu 1500
      inet 172.16.112.22 netmask 0xffffffff00
      carp: MASTER vhid 1 advbase 1 advskew 0

[2.0.2-RELEASE][root@desktone.local]/root(4): ifconfig vip1
vip1: flags=49<UP,LOOPBACK,RUNNING> metric 0 mtu 1500
      inet 172.16.112.22 netmask 0xffffffff00
      carp: BACKUP vhid 1 advbase 1 advskew 100
```

A.12 Final Configuration Steps

When you have finished checking the carp interface, perform the following steps.

Procedure

1. Configure the slave dtRAM.
2. Configure the primary dtRAM.
3. Reboot the slave dtRAM to confirm that the configurator is not running.

A.13 Verify the dtRAM Daemon is Running

To verify that the dtRAM daemon is running from the shell, select 8 to get a shell prompt and then use the `ps` command. For example:

```
ps ax|grep dttram
12073  ??  S   0:15.92 /usr/local/sbin/lighttpd -f /var/etc/lighty-dtram.conf
```

To kill the process and restart lighttpd with the correct conf file:

```
> kill 12073
> /usr/local/sbin/lighttpd -f /var/etc/lighty-dtram.conf
> ps ax | grep lighty-dtram
46822  ??  S   0:00.01 /usr/local/sbin/lighttpd -f /var/etc/lighty-dtram.conf
```

A.14 Testing the dtRAM

Once you have configured your dtRAM and external NAT you should confirm TCP and UDP connectivity to your dtRAM from the outside world. To test TCP connectivity, on the master dtRAM appliance, start a `tcpdump`.

```
tcpdump -i em0 portrange <port begin - port end>
```

Then from an external computer, try to telnet to a port in your dtRAM port range.

```
telnet <externalIP> 8025
```

The correct result will be connection refused on the client side and you should see the traffic on the dtRAM side. (Confirm the destination IP for the captured traffic is the dtRAM ip.)

You will need to repeat this test for UDP traffic as well as PCoIP uses both TCP and UDP. To generate UDP traffic from your client you will need a UDP test tool such as UDP Test Tool from SimpleComTools.com.

A.15 Enabling dtRAM Policy

To enable the dtRAM for a particular tenant, you need to set a tenant policy. From the Service Center:

1. Select **tenants ► policy**.

The Policy Configuration page displays.

2. From the Tenant Name dropdown, select the tenant for whom you want to enable the dtRAM.
3. Locate the following policy in the first column:
`element allocator.ram.use`
4. Before the dtRAM is enabled, the second column contains false. Double click the value in the second column.

You can now edit the value in the field.

5. Enter true.
6. Click **OK**.

A.16 Adding a dtRAM Configuration

Once you have enabled the dtRAM, you specify the dtRAM service location so that the management node can contact the dtRAM when a remote user attempts to login. From the Service Center:

1. Select **Tenants ► Browse tenants**.
2. Click **Edit** for the tenant you want to manage.
The Editing Tenant screen appears.
3. Select the **Remote Access** tab.
4. Click the **Add Remote Access Manager config** link (Note: this link is not visible if you have not enabled dtRAM).
5. Enter the IP address (Carp0 address) of the dtRAM on the tenant network. If you have more than one data center, use the drop-down box to select the correct data center for this dtRAM.
6. Click **Add RAM Config**.

If the dtRAM was successfully added to the configuration, you see the dtRAM listed in the dtRAM section at the bottom of the page.

Note: If the tenant connects to their VMs “locally” via a VPN in addition to externally via the dtRAM, then you must also enter the internal networks from which they connect. Failing to do so prevents internal users from connecting to their VM.

Appendix B Create a Windows 7 Gold Template

Before defining a VM as your gold template you need to create your template. We strongly recommend against using a P2V (physical-to-virtual) conversion tool. Instead a new OS install should be customized to VDI best practices.

There are numerous online publications on Windows 7 VDI best practices, such as

<http://www.vmware.com/files/pdf/VMware-View-OptimizationGuideWindows7-EN.pdf>

The following steps must be part of the VM preparation

1. Install VMWare tools and verify NIC settings:
 - a. From vCenter UI, right click the VM
 - b. Select Guest ► Install/Upgrade VMWare tools
 - c. Select Edit Settings ► Network Adapter
 - d. Confirm adapter type is VMXNET3
2. Enable Administrator account & confirm RDP access:
 - a. Right click Computer and select Manage.
 - b. Select Local Users and Groups.
 - c. Select Users.
 - d. Right click the Administrator user and select Properties.
 - e. On the General tab, uncheck account is disabled.
 - f. On the Member Of tab, confirm Administrator is a member of “Remote Desktop Users”
 - g. Set Administrator Password
3. Install DaaS Agent by copying `DaaSAgent_6.1.1.msi` onto your VM and running the install.

The DaaS Agent must be configured to point at the tenant appliances. This can be done 1 of 2 ways:

- DaaS Agent Discovery: The tenant appliance addresses can be automatically discovered by the DaaS Agent via DHCP by utilizing option code 74. The configuration of this option is described in section 2.7.
- Update of DaaS Agent configuration file: The tenant appliance addresses can be manually updated in the DaaS Agent configuration file. Open the file `C:\Program Files (x86)\DaaS`

Agent\service\MonitorAgent.ini with a text editor like notepad (note: on 32-bit systems the path will be exclude the "(x86)"). Remove the semi-colon on the line containing the parameter "standby_address" and provide a comma separated list of the tenant appliance IP addresses. A restart of the DaaS Agent Windows service is required after making this change.

4. Install the PCoIP protocol
 - a. Install VMWare View Agent
 - b. Install VMWare View Agent Connect
 - c. After install – verify VMware View Agent Direct Connection Plug-in appears in list of installed programs
 - d. Apply PCoIP GPO (.adm file) and configure protocol settings as appropriate
5. Join VM to domain and add the appropriate domain groups to "Remote Desktop Users" group.
6. Set power options for the VM to HIGH Performance:
 - a. Select Control Panel ► System and Security ► Power Options
 - b. Select High Performance
7. Confirm Windows firewall is disabled, or at least the necessary ports are configured.
8. Confirm Windows Updates are current.
9. Optional: Log in as Administrator and remove all other accounts on the VM.
10. (Optional if users connect through other browsers): Confirm Remote settings are not using NLA – NLA may interfere with IE users trying to connect to their desktops:
 - a. Right click Computer and select Properties.
 - b. Select Remote Settings.
 - c. Select "Allow connections from computers running any version of Remote Desktop"
11. Optional: Disable Ctrl-Alt-Del Secure logon. Some protocols (and users) struggle with entering CTRL-ALT-DEL to log into their VM. To disable this:
 - a. Run "netplwiz"
 - b. Select Advanced Tab
 - c. Uncheck "Require Users to press CTRL-ALT-DEL"
12. Install the appropriate protocol drivers if you choose additional protocols beyond RDP.

Once your VM is configured as you wish with the appropriate software you can begin the conversion process – note:

- VM must exist on the same host, storage and VLAN mapped to the tenant.
- Confirm the VM has been imported into the Enterprise Center and appears in Imported Desktops.

Appendix C Tenant Installation Worksheet

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

Table 3–11 Tenant Installation Fields in Service Center

Field	Values	Sample Value / Notes
Tenant VLAN 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

Optionally, if you are configuring the Tenant Active Directory, you will also need to collect the following:

Table 3–12 Tenant Installation Fields in Service Center

Field	Values	Sample Value / Notes
Active Directory (AD) Name		TENANT
Domain		tenant.com
AD Protocol		ldaps
AD Port		636
Nameserver		172.16.115.2
Context		dc=tenant,dc=com
Service Account		CN=Administrator,CN=Users
Password		TenantAPswd
Admin Group		cn=enterprisecenteradmin,ou=groups
User Group		cn=portalusers,ou=groups
Admin User		Administrator
Password		AdminPswd
Primary DNS		172.16.115.2