Horizon DaaS 8.0.0 Service Center User Guide

VMware Horizon DaaS

vmware®

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

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

Contents

About the Service Center User Guide 1

The Service Center User Guide provides information on creating and maintaining Horizon DaaS tenants in the Service Center user interface.

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.

Getting Started

2

The Service Center is a web-based application that Service Provider Administrators use to manage their environments.

You can use the Service Center to:

- Manage data center resources, such as compute resources (servers), storage, and management appliances.

- Manage tenant contracts and define tenant models and quotas.

- Configure tenant appliances and networks.

- Create and assign additional roles and permissions among the Service provider administrators to securely distribute management tasks among larger organizations.

This chapter includes the following topics:

- Log Into the Service Center

- Set the Service Center Session Timeout

- DaaS Platform Infrastructure

Log Into the Service Center

You can log into the Service Center user interface.

Procedure

1   Find out the URL of your Service Center.

2   Navigate to that URL using your web browser.

3   Enter your username and password.

4   Select a domain.

5   Click the **Login** button.

Set the Service Center Session Timeout

You can override the default setting for the Service Center session timeout.

By default, you are logged out of the Service Center after 30 minutes of inactivity. To override this default timeout period, perform the steps below.

Procedure

1   Select **tenants > policy**.

The Policy Configuration page displays.

2   Select Service Provider from the Tenant Name drop-down list.

3   Change the default value for the admin.session.timeout policy.

The value must be greater than zero.

DaaS Platform Infrastructure

This topic provides an overview of the platform infrastructure.

Overview

The DaaS service grid forms the basic DaaS infrastructure, enabling the Administrator to add compute resources (servers) and storage to the platform and assign these compute resources and storage to tenants. The service grid is comprised of both appliances and hosts.

- A 'tenant' is a customer that consumes hosted virtual desktops from a Service Provider.

- An 'appliance' is a virtual machine (VM) combined with a functional unit of Horizon DaaS software in the Horizon DaaS Platform.

Data Centers

A data center is purely a container: it does not represent any piece of hardware or software, but it usually corresponds to a geographic data center managed by a service provider.

The data center logically groups the service provider's lower-level virtualization resources. A data center has associated with it one or more resource managers, and each resource manager has associated with it Desktop Managers and Hosts. The number of physical servers in the data center depends in large part on the size of the tenant installation and the number of tenants.

Adding a new data center is accomplished during the appliance bootstrap process; refer to the installation instructions for more details.

Management Appliances

Three DaaS management appliances control the DaaS platform:

- 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. The Service Provider Appliance is the first appliance installed in a data center and provides the foundation to install the remainder of the Horizon DaaS application.

- Resource Manager Appliance

  The Resource Manager abstracts the specifics about the desktop infrastructure from the tenant appliances and allows multiple Desktop Managers to communicate with their respective virtualization resources. A Resource Manager appliance integrates with the hypervisor and storage infrastructure in a given data center. A single Resource Manager appliance can be shared across multiple tenants.

- Tenant Appliance

  Provides the tenant with both end user and administrative access to their virtual desktops. End users access and manage their individual virtual desktops via the Desktop Portal. Administrators create and manage their virtual desktops via the Enterprise Center. The Tenant Appliance includes the Desktop Manager, a per-tenant resource that manages each tenants virtualization resources and communicates with a tenant's hosts (hypervisors). You associate the desktop manager with a resource manager and one or more host managers.

Hosts

- Management Host

  A physical machine that runs a hypervisor and hosts multiple DaaS management appliances.

- Virtual Desktop Host

  A physical machine that runs a hypervisor and hosts virtual desktops. A virtual desktop is a virtual machine that is running remotely (relative to the end user).

Networks

There are three distinct networks within the data center:

- The Backbone network is fully controlled by the service provider. This network is a link local non-routable subnet (169.254.0.0/16) that is logically separated from all tenant networks. The backbone network connects all DaaS management appliances. Tenant appliances connect to the service provider resource manager via the backbone network.

- The service provider network is a discrete network. The service provider VLAN is used to communicate with the service provider appliance. This network connects Virtual Desktop hosts to VM storage systems.

- The tenant network is fully controlled by the tenant, again as a discrete VLAN that is separate from the service provider and other tenant networks. The tenant network connects the tenant appliances to a tenant's virtual desktops. The tenant VLAN is not accessible to the service provider. (A tenant network is not a subnet of the service provider network; rather, it is a logical extension of the tenant network existing in the Service Provider data center.)

Common Tasks

3

This section provides instructions for a number of common tasks in the Service Center user interface.

Instructions for common tasks are found in the subjects linked below.

This chapter includes the following topics:

- Assign Resources to a New Tenant
- Add a New Compute Resource to an Existing Tenant
- Export or Print Data

Assign Resources to a New Tenant

After you have registered a new tenant, you can assign resources to it.

Procedure

1   Select the service grid menu.

2   Select the Desktop Managers panel on the left side of the screen.

3   Click on the link for the new tenant.

4   Select the Compute Resources tab.

5   Select Compute Resource(s) from the list of Available Compute Resources at the bottom of the page.

6   Select the Storage tab.

7   Assign the appropriate Storage Configuration to the tenant.

The Compute Resource must be assigned first so that the platform can assign the storage to the Compute Resource.

Add a New Compute Resource to an Existing Tenant

You can add a new compute resource to an existing tenant.

Procedure

1   Select the service grid menu.

2   Select the Desktop Managers panel on the left side of the screen.

3 Click on the link for the desired tenant.

4 Select the Compute Resources tab.

5 Add the additional Compute Resource from the list of Available Compute Resources.

Export or Print Data

You can export or print data from the Service Center user interface.

You can export some data to formats suitable for printing or further processing. The export function is available on pages that have a small printer icon in the upper right portion of the screen.

Procedure

1 Click the printer icon.

A new screen displays showing exportable data.

2 Click one of the export icons at the lower right corner of the page.

You can choose to export this information to CSV (comma-separated values), Excel, or PDF formats.

Tenants

4

The Tenants screen serves as the home page of the Service Center.

The Tenants screen shows a list of installed Tenants. From here an Admin can add (register) new Tenants and modify existing Tenant Policies and configuration. There is one row in the table for each tenant.

You can perform the following tasks on the Browse Tenants page:

- To edit tenant information, click the Edit button for the tenant to display the Edit Tenant screen. See Edit a Tenant for more information.

- To register a new tenant, click the **register a tenant** link or select **tenants > register a tenant**. See Register a Tenant for more information.

- To configure policy settings for a particular tenant, select **tenants > policy**. See Configure Policies for more information.

This chapter includes the following topics:

- Pre-Requisites for Adding a New Tenant

- Register a Tenant

- Edit a Tenant

- Configure Policies

Pre-Requisites for Adding a New Tenant

The following are tasks you must perform before you can add a new tenant.

Assign Tenant Hosts (ESX servers)

The management interface must be reachable from the Service Provider network and be defined in the Service Provider DNS. You must also configure an account on the hosts for access to APIs.

Create a Mount Point

On the NFS storage subsystem, create a mount point for the tenant to host their desktops. Configure NFS permissions to have at a minimum the tenant desktop host IP and the IPs of the Resource Manager appliances. It is recommended that for ease of use, allow the entire management appliance subnet and hosts subnet.

Configure Backhaul (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.

Define Tenant Network & VLAN

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 and VLAN to the tenant network. This VLAN must be assigned to a vSwitch in both of the Management ESX Hosts as well as all desktop hosts assigned to the tenant.

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 IP Addresses in the Tenant Network

Allocate up to seven IP addresses in the tenant network. Allocate two IP addresses for management appliances plus a third for the shared IP and another three if the tenant requests access via the dtRAM. If the tenant has backhaul to a DHCP server you may optionally need a seventh IP for a DHCP relay service.

Define or install Tenant Active Directory

The tenant must configure their Active Directory as defined in the installation guide. 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
```

A Tenant may opt to only allow two required users:

- Service Account - read only access for authentication

- Domain Join Account - domain join privilege to add VMs to AD

If accounts are restricted as defined above then set the tenant policy fabric.ad.validateSysPrepUserPrivs to false. See Configure Policies for more information.

Determine if the Tenant Requires a Certificate

If so, the customer must provide the service provider with the necessary certificate files in Apache SSL format. See Certificates for more information.

Register a Tenant

You can register a new tenant in the Service Center user interface.

Procedure

1   Click on the **register a tenant** link.

2   On the General Info tab, enter information as described below.

-   Enter the tenant name, administrator name, and database password.

-   Super Tenant - Select the check box to enable Super Tenant capabilities for the Tenant. Please make sure that you have prepared the required infrastructure for the Super Tenant beforehand. For more information, see the Super Tenant section in the Service Provider Manual.

-   Sync Gold Patterns - Select the check box to enable image sync for the Tenant. If you have multiple Desktop Managers registered to a Tenant within the same Data Center, this feature allows you to:

    -   Duplicate images across Desktop Managers without having to manually clone and import the images.

    -   Sync changes to images across Desktop Managers without having to make the changes on all copies.

        Note   When Sync Gold Patterns is enabled, the cloned images on additional Desktop Managers are not counted against template quota. If you then disable Sync Gold Patterns, those cloned images begin being counted against template quota, which may require you to increase the quota in order to avoid exceeding it.

-   The URLs are optional:

    -   The CRM system URL field allows the service provider to record the location of the CRM system for this tenant: this does not appear as a link anywhere.

    -   The technical support URL shows up as the Support link on the Enterprise Center.

    -   The style sheet URL allows you to customize the look of the tenant's Enterprise Center. See Add an External Style Sheet for more information.

    -   The license file URL should be a URL that points to a valid PDF file.

    -   The business support URL (if provided) will show up as the Business link on the Enterprise Center.

3   Click **Networks** on the left of the page to display the Networks tab.

4   On the Networks tab, enter the Network ID, Network ID Type, Network Label, Gateway, DNS Server, and Subnet Mask of the Data Center. You must enter this information in order to be able to add appliances and desktops.

5   Click **Custom Fields** on the left of the page to display the Custom Fields tab.

6   (Optional) Enter free-form information for custom field(s). This information becomes part of the tenant details.

7   Click **Save and Create Appliances**.

The new tenant appears in the tenants tab, along with a unique organization ID the system assigns to it.

8   Enter Name and IP Address for Primary and Secondary Appliances, enter schedule information, and click **Create Appliances**.

Note   Be sure that the time you enter under Schedule Install is in the future. If you enter a time in past, the system will accept it without an error, but the scheduled task will not be executed.

Tenant deployment may take some time after you have clicked **Create Appliances**, and you need to wait for the deployment to finish before you can assign one or more networks on the Desktop Managers Networks tab as described in the steps above.

9   After the appliance has been fully deployed, select **service grid > resources** and select **Desktop Managers** on the left of the page.

10 Select the desktop manager and click the Networks tab

Note   This is a different tab than the Networks tab mentioned in Step 3.

11 Assign one or more networks to the tenant in order to complete the tenant registration process.

Edit a Tenant

You can edit tenants listed on the Browse Tenants page.

When you click on the **Edit** button for a tenant, the Editing Tenant screen displays with several tabs for editing tenant information.

General

You can edit general tenant settings on the General tab.

The only required fields are the Tenant Name and Administrator Name. Enter this information and any of the non-required field data you want to maintain.

Super Tenant

Select the check box to enable Super Tenant capabilities for the Tenant. Please make sure that you have prepared the required infrastructure for the Super Tenant beforehand. For more information, see the Super Tenant section in the Service Provider Manual.

Sync Gold Patterns

Select the check box to enable image sync for the Tenant. If you have multiple Desktop Managers registered to a Tenant within the same Data Center, this feature allows you to:

■   Duplicate images across Desktop Managers without having to manually clone and import the images.

■   Sync changes to images across Desktop Managers without having to make the changes on all copies.

Local Admin Access

Click **Show Info** button to display credentials for local admin. Click **Reset Password** button to reset password.

Max Concurrent Refresh (last field displayed)

Maximum number of VMs that can be refreshed concurrently per pool by the tenant admin. This setting only affects RDS server pools and dynamic non-persistent pools. Recommendation is 5 or less, depending on infrastructure performance.

Delete Tenant button

Permanently deletes a disabled tenant. All data, including billing information, is permanently removed from the database. Do not delete a tenant until after the current billing cycle is completed. After you click the **Delete Tenant** button, a delete task for the tenant appears on the Reservations screen.

Disable Tenant button

Prepares the tenant for deletion and powers off all appliances for the tenant. You should keep a tenant disabled until the current billing cycle is completed. Disabled tenants are not visible on the Tenants screen or on the Resources screen. To see which Tenants have been disabled, uncheck **Show only active tenants** on the Tenants screen. To re-enable a disabled tenant, click the **Enable** button.

Custom Fields

You can add or edit custom fields on the Custom Fields tab.

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.

Quotas

On the Quotas tab, you can make settings for user licenses and desktop capacity.

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.

Desktop Capacity

The following values are displayed under Desktop Capacity.

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.

> **WARNING**   Before you enter a value, confirm that adequate compute resources are available.

Remote Access

The Remote Access tab shows a list of internal networks currently configured.

To add an internal network, click the link and enter the IP address range using classless inter-domain routing (CIDR) notation. You can add multiple internal network address ranges if necessary.

Appliances

You can add or edit appliances for a tenant on the Appliances tab.

Add Appliances

To add primary and secondary Desktop Managers, perform the following steps:

1   Click the **Add Appliances** link.

2   On the Tenant Install page, enter information as described below.

Section	Field	Description
Primary Appliance	Name	A user-friendly name indicative of the role of the appliance (for example <initials>-<dc#>-<dmgr#>).
	IP Address	The IP address of the primary appliance in an HA pair. This address must be within the range specified by the subnet mask.
Secondary Appliance	Name	A user-friendly name indicative of the role of the appliance (for example <initials>-<dc#>-<dmgr#>).
	IP Address	The IP address of the secondary appliance in an HA pair. This address must be within the range specified by the subnet mask.
Schedule Install	Start date	The scheduled date for the install of the primary and secondary appliances.
	Start Time	Enter time in format HH:MM 00:00-23:59 GMT - use 00:00 for "now".
		Note Be sure that the time you enter under Schedule Install is in the future. If you enter a time in past, the system will accept it without an error, but the scheduled task will not be executed.

3   Click **Create Appliances**.

4   Select **appliances > reservations** to check the status of provisioning the Desktop Managers.

5   When provisioning is complete, select **service grid > resources** and select **Desktop Managers**.

6   Add compute resources for each desktop manager and network(s) as described in Desktop Managers.

- Only compute resources not associated with any existing appliance or user desktop can be assigned to a newly provisioned desktop manager.

- The desktop manager should be associated with the tenant network that requires expansion.

7   If you have not yet created a Standard Capacity, create one now as described in Desktop Capacity and Model Definition.

8   Select **Tenants** and click the **Edit** button to edit the tenant

9   Select the Quotas tab.

10 Under Desktop Capacity, select the new desktop manager and a standard capacity not being used by another desktop manager in the tenant, and then set desired Capacity value.

11 Under Template Quota, set desired Template Quota value.

> **WARNING**   Before you enter a value, confirm that adequate compute resources are available.

12 Create a desktop template VM and deploy it on the compute resource defined above. Failure to do this will either not allow the DaaS Agent to setup correctly OR not allow the image to be created.

13 [Optional] Enable Sync Gold Patterns on the General tab. For more information, see General.

Edit Appliances

You can edit appliances if you need to correct errors made during the initial installation or to reflect subsequent changes in the underlying network infrastructure.

To edit an appliance:

1   Click the **Edit Appliances** link. The appliance configuration page displays.

2   Update values as described below.

Section	Field	Description
Primary Appliance	Name	A user-friendly name indicative of the role of the appliance (for example <initials>-<dc#>-<dmgr#>).
	IP Address	The IP address of the primary appliance in an HA pair. This address must be within the range specified by the subnet mask.
Secondary Appliance	Name	A user-friendly name indicative of the role of the appliance (for example <initials>-<dc#>-<dmgr#>).
	IP Address	The IP address of the secondary appliance in an HA pair. This address must be within the range specified by the subnet mask.
Schedule Update	Start date	The scheduled date for the update of the primary and secondary appliances.
	Start Time	Enter time in format HH:MM 00:00-23:59 GMT - use 00:00 for "now".

3   Click **Update** to make the changes. You can check the status of the update on the **appliances > reservations** screen.

Networks

You edit network information for a tenant on the Networks tab.

The Networks tab lists the current network configuration for the Tenant. To add a Network Configuration, click the **Add Network Configuration** button and populate the required information.

Depending on the type of network, the Network ID can be a VLAN ID, a VXLAN ID, or the case-sensitive distributed port group name if you are using a virtual distributed (DVS) switch via VMware vCenter. You may have multiple VLANs or VXLANs configured for a Tenant in a given data center, and also multiple DVS port groups. You cannot mix network types in a given data center. (e.g. a Tenant that is configured to use a VLAN may not use DVS and vice versa). The initial Network Type is configured during the Tenant Registration.

Note   When using DVS, the port group binding must be set to "Ephemeral - no binding"

Entitlements

You can add or edit entitlements for a tenant on the Entitlements tab.

The term entitlement refers to a file that enables a virtual desktop to use some third-party application (for example, a remote display protocol server or client program). The entitlement file may be a simple text file that contains a license, or it may be an executable file that runs when the application starts up.

To add an entitlement on the Entitlements tab:

1   Click the **Add New Entitlements** link.

2   Make settings as follows.

Setting/Field	Description
Control Action	Always Grant means that the file is copied every time the virtual desktop starts. Grant means that the file is copied just once.
Entitlement	Select an entitlement file by browsing the network. If the filename of the entitlement file and the file system path on the virtual desktop matches a service-wide entitlement, the tenant entitlement will override the service-wide entitlement the next time the virtual desktop reboots. Otherwise, the tenant entitlement is added to the set of service-wide entitlements that are part of the desktop model already
File System Location	When the virtual desktop starts up, the Entitlement file is written to the File System Location.
Invoke Action	None means that the entitlement file just needs to be present. Regsvr32 means that the entitlement file needs to be registered as an OLE control using Regsvr32.exe.
Reboot	If the virtual desktop needs to be rebooted to activate the entitlement, you need to check this box.
Select Desktop Model	(Tenant entitlements only) Select the desktop model to which to apply the entitlement.

3   Click the **Add Entitlement** button.

Maintenance

On the Maintenance tab, you can set up a maintenance notice that displays at the top of the Dashboard page in Enterprise Center.

Create a New Maintenance Notice

To create a new maintenance notice:

1   Type the text of the notice in the Notice Details text box using only alphanumeric characters. The notice can have a maximum of 4096 characters, and special characters such as the following are not supported: & ( ) % < >

2   Enter Start Date, Start Time, Expire Date, and Expire Time in the formats specified.

3   Click **Publish Notice**.

Edit a Maintenance Notice

To edit an existing maintenance notice:

1   Click the **Edit Notice** button at the bottom of the page.

2   Edit the text of the notice in the Notice Details text box using only alphanumeric characters. The notice can have a maximum of 4096 characters, and special characters such as the following are not supported: & ( ) % < >

3   Edit values for Start Date, Start Time, Expire Date, and Expire Time in the formats specified.

4   Click **Publish Notice**.

Certificates

You can upload custom SSL certificates on the Certificates tab.

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

■   If the tenant does not already have a certificate, you can generate it following the instructions under Generate Tenant Certificates below.

■   If it already has a certificate, proceed directly to Apply Tenant Certificates below.

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.

To generate a tenant certificate:

1   Collect the following information from 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   When the .key and .csr files have been created, zip them up and send them to the customer so they can request a cert from a certificate authority.

Apply Tenant Certificates

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).

To apply a tenant certificate:

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 follow 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 - Select the Click here 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.

Configure Policies

You can set policies for tenants on the Configure Policies tab.

You set policies on a per tenant basis. The Policy configuration screen displays the values of configuration parameters for Tenant appliances and Desktop Managers.

Click the **Show Description** button to show a brief description of each parameter. The default value appears in square brackets.

To change the value of a policy parameter:

1   Double-click the row of the parameter you want to change.

2   Enter the new value.

3   Click **OK** to make the change or **Cancel** to retain the current value.

The screen displays only the most common policies by default. To see the full list, including advanced policies, select the web page and type "dtpolicy".

Configure Policies for Agent Update Functionality

In order for the Agent Update functionality to work, you must specify the upgrade server URL in the agentupdate.updateserver.url policy.

The following policies also affect this functionality, and can be set as needed (default values are shown in brackets):

agentupdate.cachePath	File share location for downloading agent installers. Tenant Appliance will update this as needed.
agentupdate.cipherList	Cryptographic cipher suite to use with SSL when connecting to Update Server [ECDHE-RSA-AES256-GCM-SHA384]
agentupdate.enable	When enabled (set to true), Tenant Appliance will scan for agent updates on Update Server. Setting this to false will disable the scan for new agents and also disables the scan for hot patch files on the file share.

agentupdate.enablehotpatch	When enabled (set to true), Tenant Appliance will scan for hot patch files placed on the file share by Customer Admin. Setting this to false will disable the scan for hot patch files on the file share.
agentupdate.job.repeatInterval	Interval (in ms) between scans for new agents on Update Server. Defaults to 24 hours [86400000]
agentupdate.job.startDelay	Wait time (in ms) for agent update scan to start after Tenant Appliance startup. Defaults to 1 minute [60000]
agentupdate.sslProtocol	Cryptographic protocols to use with SSL when connecting to Update Server [TLS_V1_2]
element.agentupdate.max.concurrent.updates.per.pool	Max number of VMs to update at a time in each pool. This will also be the max number of failures in a pool after which an agent update task will give up and fail. Default is 30.

Service Grid

<div style="text-align: right; font-size: 3em; color: #ccc;">5</div>

You can manage resource managers, desktop managers, compute resources, and data centers in the Service Grid.

Service Grid features are described in the topics linked below.

This chapter includes the following topics:

- Resources
- Data Centers

Resources

You can manager esource managers, desktop managers, and compute resources on the Resources page.

Features on the Resources page are described in the topics linked below.

Resource Managers

A resource manager is a service provider resource that allows multiple desktop managers to communicate with their virtual physical infrastructure resources. A resource manager integrates with the hypervisor and storage infrastructure in a given data center. A single resource manager appliance can be shared across multiple tenants

The Resource Managers pane on the left side of the Resources page provides a tree view of the desktop managers and compute resources associated with each resource manager in the selected data center. A data center has associated with it a minimum of two resource managers, one each for the SP and tenants. Each tenant resource manager has associated with it desktop managers and compute resources:

- Expand the tree for the resource manager to show the defined desktop managers, vCenter, vCenter Data Center and compute resources for that resource manager.

- Click on a resource manager, desktop manager, vCenter or compute resource in the left pane to display tabs of information specific to that resource in the right pane.

Once you have a resource manager associated with a data center, when you click on the link for that resource manager in the Resource Managers panel, the Compute Resources, Desktop Managers, and Storage Systems tabs are displayed in the right panel.

General

You can make general settings for a resource manager on the General tab.

After clicking on the link for a resource manager in the left pane, the General tab updates to display the name, hostname, UUID, and Data Center for that resource manager.

Renaming a Resource Manager

VMware recommends that you always change the name of the resource manager from the default (IP address) to a more meaningful, friendly name.

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

2   On the General tab, double-click on the IP address of the resource manager (Name field). A text box opens in which you can change the name.

3   Change the name to the user friendly name, for example "Service Provider RMgr".

Compute Resources

You can manage compute resources for a resource manager on the Compute Resources tab.

The Compute Resources tab shows the status and type of each compute resource associated with this resource manager. You can also remove the association of a compute resource from a resource manager by clicking the **remove** button.

Reassigning a Compute Resource

A reassign option appears on the Compute Resources tab. This allows you to add or remove a compute resource that was previously assigned.

To reassign compute resources:

1   Select **service grid -> resources -> Resource Managers**.

2   Select the service provider resource manager.

3   Select the Compute Resources tab.

4   Click **Reassign** next to the Virtual Center and the Desktop Compute Resources dialog will open.

5   Select or deselect compute resources from the list of compute resources in the Desktop Compute Resources dialog.

> **Note**   You cannot deselect a compute resource with management appliances on it.

6   For each selected compute resource, change the over-allocation ratios if applicable. VMware recommends the following values:

   ▪   Memory Over allocation Ratio: 1.0

- Virtual to Physical CPU Ratio: 10.0

7   If this compute resource is to be shared between 2 or more tenants, check the **Share This Compute Resource** box. Note that this option must be selected at assignment time and cannot be changed later.

8   Click **Save**. If this compute resource is shared, the Partitioned Compute Resource dialog displays.

9   Set partition sizes for Memory and CPU, and click **Save**.

Desktop Managers

You can view desktop managers for a resource manager on the Desktop Managers tab.

The Desktop Managers tab shows the ID and status of each desktop manager associated with this resource manager. See Desktop Managers for more information about desktop managers.

Desktop Managers

You can manage desktop managers on the Desktop Managers page.

A desktop manager is a per-tenant resource that manages each tenant's virtualization resources and communicates with a tenant's compute resources (hypervisors). Each desktop manager needs to be associated with a resource manager and one or more host managers.

When you click on the Desktop Managers panel on the left side of the Resources screen, the right side of the Resources screen displays the General tab. The General tab lists the assigned Desktop Managers and unassigned Desktop Managers. You can assign an unassigned Desktop Manager from this tab as well as unassign one that is already assigned.

When you select the link for a specific Desktop Manager, the General tab shows the Name, Id, Tenant, and Resource Manager for that Desktop Manager, and the panel updates to display additional tabs: Compute Resources, Instances, Networks, and Datastores.

General

You can make general settings for desktop manager on the General tab.

Before selecting a Desktop Manager link, the General tab lists the assigned Desktop Managers and unassigned Desktop Managers. You can assign an unassigned Desktop Manager from this tab.

Renaming a Desktop Manager

VMware recommends that you always change the name of the desktop manager from the default (IP address) to a more meaningful, friendly name.

To rename a desktop manager:

1   In the Desktop Managers panel on the left side of the page, click on the IP address of desktop manager.

2   On the General tab, double-click on the IP address of the desktop manager (Name field). A text box opens in which you can change the name.

3   Change the name to the user friendly name, for example "DMgr1".

Compute Resources

You can manage compute resources for a desktop manager on the Compute Resources tab.

This tab shows the VMware vCenter controlled by this desktop manager. It is only possible to assign one vCenter to any given desktop manager.

Assign a Compute Resource to a Tenant

Once a VMware vCenter gets added as a desktop compute resource, it appears in the Available Compute Resources section of the Compute Resources tab.

To assign a compute resource to a tenant:

1   In the Available Compute Resources section, click **Assign** to assign the Virtual Center.

2   Pick your compute resource(s) from the list of compute resources in the Desktop Compute Resources dialog.

3   You will be presented with a capacity dialog for each compute resource you selected. Change the over-allocation ratios if applicable. VMware recommends the following values:

    ■   Memory Over allocation Ratio: 1.0

    ■   Virtual to Physical CPU Ratio: 10.0

4   If this compute resource is to be shared between 2 or more tenants, check the **Share This Compute Resource** box. Note that this option must be selected at assignment time and cannot be changed later.

5   If you wish to change the Usage setting for the compute resource, do so by selecting/deselecting the check boxes. For more information on this setting, see Working with Compute Resources

6   Click **Save**.

7   If this compute resource is shared, the Partitioned Compute Resource dialog displays

8   Set partition sizes for Memory and CPU, and click **Save**.

Reassigning a Compute Resource to a Tenant

After assigning the vCenter, a reassign option will appear. This will allow you to add or remove a compute resource that was previously assigned.

To reassign compute resources assigned to your tenant:

1   In the Assigned Compute Resources section, click **Reassign** next to the Virtual Center.

2   Select or deselect compute resources from the list of compute resources in the Desktop Compute Resources dialog.

3   You will be presented with a capacity dialog for each compute resource you selected. Change the over-allocation ratios if applicable. VMware recommends the following values:

    ■   Memory Over allocation Ratio: 1.0

- Virtual to Physical CPU Ratio: 10.0

4   If this compute resource is to be shared between 2 or more tenants, check the **Share This Compute Resource** box. Note that this option must be selected at assignment time and cannot be changed later.

5   If you wish to change the Usage setting for the compute resource, do so by selecting/deselecting the check boxes.

6   Click **Save**.

7   If this compute resource is shared, the Partitioned Compute Resource dialog displays.

8   Set partition sizes for Memory and CPU, and click **Save**.

Unassign a Compute Resource from a Tenant

After assigning the vCenter, an unassign option will appear. This will allow you to remove a vCenter that was previously assigned.

To unassign a vCenter:

1   Select the Compute Resources tab.

2   In the Assigned Compute Resources section, click **Unassign** next to the Virtual Center.

Once a vCenter is assigned, expanding the Desktop Managers tree will display the VMware vCenter. Clicking on items in the tree under the vCenter show information as described in Working with Compute Resources.

Instances

You can view instances for a desktop manager on the Instances tab.

The Desktop Manager Instances tab presents detailed information about the appliance or appliances that comprise this desktop manager.

Networks

You can manage networks for a desktop manager on the Networks tab.

The Networks tab is used for assigning networks to tenants. For more information, see Register a Tenant.

Datastores

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

Note   For Instant Clone images, if you do not set up any datastores for desktop storage, the system looks for datastores that are accessible, not read-only, and have multi-host access (non-local).

- If no such datastores are found, assignment creation fails.

- If such a datastore is found and used, VMs might not be placed on the same datastore as the template VM, which can also cause performance issues for users.

To set up datastores:

1   Click the appropriate text box (Desktop Primary Storage, Desktop Auxiliary Storage).

2   Enter a regular expression for the names of the datastores.

Note the following:

■   In order for a datastore to be added, that datastore must be present, using a consistent name, on all compute resources assigned to a given desktop manager.

■   If you set up multiple datastores for desktop storage, clones are put on the datastore that contains the image if it is 75% full or less. If that datastore is more than 75% full, then the clones are put on the datastore that has more space available.

■   The 75% threshold above is a default setting that can be changed using the datastore.max.usage.percent policy.

Compute Resources

You can manage compute resources on the Compute Resources panel of the Resources page.

The Compute Resources panel on the left side of the Resources screen provides information about the following resources associated with this data center:

■   A virtual desktop host can be a VMware vCenter that manages multiple hypervisors and hosts virtual desktops.

■   A management host can be a VMware vCenter that manages multiple hypervisors and hosts management appliances.

When you click on the Compute Resources panel, the right pane updates to display the General and Add Host Manager tabs. If you have any Partitioned Compute Resources, the Partitioned Compute Summary tab displays as well.

Before you select the link for a specific Compute Resource, the General tab provides general information about the supported Compute Resource types.

Selecting the VMware vCenter host manager link updates the right panel to display the General and Accounts tabs.

Add Host Manager

Since there is at most 1 management vCenter per data center, adding a vCenter host manager is only done at the time a data center is initially configured.

To add a VMware vCenter desktop host manager:

1   Enter the DNS name or IP address of the VMware vCenter host manager to add.

2   Supply credentials (username/password) for this host manager (should login as Administrator).

3   Choose a desktop resource manager to associate with this host manager.

4   Click the Add button.

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

5   Click Accept.

The system indicates it is discovering the host manager and calculating capacity.

6   Select your vCenter data center and click Save.

Note   If you only have one vCenter data center, you will not be prompted to select it.

Note   When you add a desktop host manager, you will not be prompted to set the Compute Resource capacity. This will be set later when the Compute Resource is assigned to a tenant desktop manager.

Working with Host Managers

You can manage host managers by selecting a host manager in the Compute Resources panel on the Resources page.

When you select a host manager, the General and Accounts tab display.

General

The General tab displays information for a host manager.

You can perform the following actions on the General tab:

■   Update Compute Resources - Picks up any compute resource changes in the vCenter data center. Any Compute Resources that have been added or removed will be updated.

■   Remove Host Manager - Removes a VMware vCenter host manager.

You can also expand the tree for the Management vCenter and see the vCenter data center that was selected for your Management appliances as well as the Compute Resources in that vCenter data center. Expanding the tree for the desktop host manager also displays the selected vCenter data center and compute resources.

Accounts

Note   You can add additional accounts so that if the first set of login credentials fails, the system will try the next set.

To add a user account:

1   Click the **Add User Account** link.

2   Enter username and password for the account.

3   Click the **Add User Account** button.

To delete a user account, click the **Delete** button next to it in the Existing Credentials list.

Working with Compute Resources

You can manage computes resources by expanding the tree on the Compute Resources panel of the Resources page.

When you expand the tree down to the compute resource level, the following tabs display: General, Tenants, and Datastore Config.

General

Selected items on the tab are described below.

- 'Compute resource role' field

  The compute resource role can be Active, Reserved, or Standby.

  Compute resources can host either virtual desktops or management appliance VMs. You can use the compute resource role to define how a compute resource is to be used. The compute resource role is only relevant for desktop compute resources. While a role can be set on a management compute resource, it has no effect on the use of that compute resource.

  From the Compute Resources panel under service grid -> resources, expand the Virtual Center tree down to the compute resource level. Select a compute resource, then select the role from the drop-down box.

  - Active - An active compute resource is a compute resource that is actively hosting virtual desktops.

  - Standby - A standby compute resource is a compute resource that can host desktops in the event that another compute resource fails. However, the compute resource recovery option is not available for Desktop Managers that are using vCenter compute resources. If compute resource recovery is needed for vCenter compute resources, it's recommended to use vCenter to migrate desktops from the failed compute resource to a new compute resource.

  - Reserved - A reserved compute resource is a compute resource that will not be used for provisioning desktops.

- 'Usage' field

  The Usage field shows the value(s) selected in the Usage setting (see Edit Compute Resource below).

- 'Edit Compute Resource' button

  Selecting the Edit Compute Resource button allows you to make the following settings.

  - Over-allocation ratios for the compute resource - VMware recommends the following values:

    - Memory Over allocation Ratio: 1.0

    - Virtual to Physical CPU Ratio: 10.0

  - Sharing of compute resource - If this host manager is to be shared between 2 or more tenants, check the "Share This Compute Resource" box. Note that this option must be selected at discovery time and cannot be changed after the compute resource has been assigned.

  - Usage - This setting indicates the usage(s) for the compute resource. You can select one or more of the following.

    - Service - Service Provider, Resource Manager and NSX Controllers

- Tenant - Tenants, Desktop Managers, Access Points

- Network - Edge Gateway Servers

Note This setting does not affect desktop deployment selection.

Tenants

The Tenants tab lists the tenants using this compute resource.

Datastore Config

This tab lists the datastores that are configured on this compute resource.

Data Centers

You can manage your data center on the Data Centers page.

You can view or edit basic information such as the name and description, and you can also add other management appliances such as resource managers using the Add Appliance button in the Edit Data Center dialog.

Add Appliances

Each Data Center has appliances. For example, during the initial installation, you create a High Availability (HA) Service Provider Appliance and a Tenant Resource Manager. To add appliances:

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

2   Click **Edit**. The system displays the Edit Data Center popup.

3   Verify the displayed information and click **Add Appliances**. The Appliance Install screen displays.

4   Enter information as described below.

Section	Field	Description
Appliance	Type	Select either Service Provider or Resource Manager from the drop-down.
		Note If you have already created the Server Provider HA pair, the only option shown will be Resource manager.
Primary Appliance	Name	A user-friendly name indicative of the role of the appliance (for example <initials>-<dc#>-<dmgr#>).
	IP Address	The IP address of the primary appliance in an HA pair. This address must be within the range specified by the subnet mask.
Secondary Appliance	Name	A user-friendly name indicative of the role of the appliance (for example <initials>-<dc#>-<dmgr#>).
	IP Address	The IP address of the secondary appliance in an HA pair. This address must be within the range specified by the subnet mask.
New reservation	Friendly Name	Name for the reservation.

Section	Field	Description
	Start date	The scheduled date for the install of the appliance(s).
	Start Time	Enter time in format HH:MM 00:00-23:59 GMT - use 00:00 for "now".

5   Click **Create Appliance**.

If you want to check the status of a reservation, select **appliances > reservations**.

Change the NTP Server

To change or add external NTP servers on a Service Provider, perform the following steps:

1   Edit the /etc/ntp.conf file.

2   Find the following line in the file:

```
#You do need to talk to an NTP server or two (or three).
```

3   On subsequent lines following this line, for each NTP server, add a unique line of the following form:

```
server name
```

- If you are changing the existing NTP server, replace the existing name.

- If you are adding another NTP server, add a new line that specifies the name of the additional NTP server.

4   Restart the NTP server using the following command:

```
sudo /etc/init.d/ntp restart
```

Appliances

6

You can manage appliances on the Appliances page.

The appliance screen lists all the appliances installed in the service grid: Service Provider appliances, Resource Manger appliances, and Tenant appliances.

Actions You Can Perform on Appliances

Click the Actions link to perform the following actions:

- Restart Services

- Reboot Appliance

- Restore Appliance

  The restore appliance option is provided to recreate an appliance. Efforts should first be made to resolve any issues with an existing appliance before using the restore option. Any custom changes made to the appliance would be lost when the appliance is recreated. When a primary SP or tenant appliance is restored, a database backup is taken before deleting the original appliance. That backup is then restored once the appliance is recreated. Replication is automatically reinitialized.

  Note the following:

  - If you have any old versions of appliances from previous builds, be sure to delete them before performing a restore.

  - After a restore, you need to manually reconfigure any custom branding you have in place.

- Download Logs

  Selecting the Download Logs link zips the following files:

  - desktone.log

  - slony and sys logs (where applicable)

  - netstat

  - system performance/top

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.

1   Configure the DHCP scope for the desktop subnet, starting at x.x.x.30.

2   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:

1   Select **control panel** → **administrative tools** and open the DHCP configuration client.

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

3   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.

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

5   Add IP addresses for tenant appliances.

This chapter includes the following topics:

- Appliance Templates

- Reservations

- Software Updates

- Maintenance

Appliance Templates

You can view and add appliance templates on the Appliance Templates page.

Appliance templates are listed along with the software version and data center for each.

Note   The version number for templates is not updated when you install a new patch.

- To filter the list by data center, select the data center from the drop-down list and click **Search**.

- To add a template, click the **Add Appliance Template** link and select the template from the list.

Reservations

You can view and manage reservations on the Reservations page.

It takes approximately 30-60 minutes for the system to create new tenant appliances when you add a Tenant or a new Data Center. During this time, you can check the status of a reservation on the Reservations screen. For HA, the reservation details will list two appliances.

Appliance Installation Failures: If the State column indicates that an appliance installation failed, click the **Reschedule** link in the Action column and attempt the installation again by rescheduling.

Note   Be sure that the time you enter when resceduling is in the future. If you enter a time in past, the system will accept it without an error, but the scheduled task will not be executed.

Software Updates

You can push software patches to appliances on the System Patches page.

Pushing out software patches to all appliances in one or more Data Centers is a two-step process:

1   Upload the patch.

2   Install the patch file on all appliances.

These actions are described in the sections below.

Upload a Patch File

When you upload the patch file, it is automatically replicated to all appliances:

1   Select **appliances → software updates**. The System Patches screen displays.

2   Click **Browse** to browse for the patch file.

3   Click **Upload**.

- The Service Center checks whether the file is the correct file type.

- It can take up to one minute for each appliance. You must wait until the patch file has been replicated to an appliance before installing the patch on that appliance.

Install a Patch File

Note   If you start the installation before the patch file has been replicated to all Service Provider appliances, you are warned that replication is not complete on specific appliances. However, you can begin installation on those appliances where replication is complete.

To install the patch:

1   Select **appliances → software updates** to display the System Patches screen. This screen lists the available patches. Each patch name is a link.

2   Click on the name of a patch. The screen redisplays to show those organizations which have appliances that have not been patched.

3   For each organization you need to patch:

a   Mark the checkbox for that organization.

b   Accept the Data Center default setting of All.

4   Click **Install**.

Maintenance

On the Maintenance page, you can perform the actions below.

Perform Failover Master

You can perform failover master on the Maintenance page.

Procedure

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

2   In the Fail Over section of the page, enter the following information.

- Organization id: Org ID of the appliance to which the failover will be done.

- Data Center name: Name of the Data Center where the appliance is located to which the failover will be done.

- DB instance name: Name of database instance for failover.

- Element ID: ID of the Desktop Manager to list New Master IP for failover . This option is visible when DB instance name is 'edb'.

- New master IP: eth0 IP of the appliance to which the failover will be done.

3   Click the **FailOverMaster** button.

4   Restart the service provider appliances.

Initialize Slony for a Desktop Manager or Organization

You can initialize slony on the Maintenance page in the Service Center user interface.

Procedure

1   Stop dtService on all nodes:

```
service dtService stop
```

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

```
killall slon
```

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

```
drop schema _slony cascade;
```

Note   Drop the schema only for the affected database pair.

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

```
service dtService start
```

5 Start slon daemons as follows.

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

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

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

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

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

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

7 In the Slony Operations section of the page, enter the following information.

- Organization id: Org ID of the appliance to which the init slony would be performed.

- DB instance name: Name of database instance for init slony.

- Element ID: ID of the Desktop Manager to list New Master IP for init slony operation. This option is visible when DB instance name is 'edb'.

8 Click **Init Slony**.

Configuration 7

You can access configuration options from the configuration menu in the Service Provider user interface.

There are four options in the configuration menu:

- general
- domains
- roles & permissions
- standard capacity (opens the Desktop Capacity & Model Definition page)

This chapter includes the following topics:

- General Configuration
- Domains
- Roles and Permissions
- Desktop Capacity and Model Definition

General Configuration

On the General Configuration page, you can make the settings described below.

- Branding: You can add a Style Sheet to customize the branding of the Service Center.

- Terms of Service: You can enter a Terms of Service URL here. If you have made a revision to these terms with the same URL, you can click the Force Reacceptance button, which updates the version of the terms causes the tenant administrator to be prompted again in the tenant UI upon next login.

- Product Name: You can enter a product name to display in the browser title bar for all of the web applications: the Service Center, the Enterprise Center, and the Desktop Portal.

- Other Configuration: Clicking this link opens the Editing Service Provider page.

- Current Role(s): The level of access that the Tenant has authorized for you: Super Admin or Read Only. The DaaS platform has a special local account to enable you to access to the Tenant's Enterprise Center. Using this account, you can assist the Tenant with initial configuration and problem solving without having an account in the Tenants AD. The user name for the account is "desktone". Obtain the password from the Tenant.

By default, the account is disabled upon creation of a new tenant. The Tenant can enable or disable the account from within the Enterprise Center at any time.

Add an External Style Sheet

You can change the look of the Service Center by overriding the default style sheet.

By default, the style sheet used for the Service Center is used for the Enterprise Center and the Desktop Portal. If a tenant administrator chooses, they can override the style sheet used for the Desktop Portal for their end users.

The default style sheet for the Service Center is located at the following URL:

```
https://<your.tenant.appliance>/service/css/normal.css
```

You can override some or all of the elements in the default style sheet by specifying your own in the System section of the Configuration tab. If you do override the default style sheet, you will need to add any new graphics to your web server as well.

For example, to change the background color of the top banner and the logo for the Service Center using a background image bannerBack.gif and a logo image logo.gif:

1   Create a style sheet with the following content:

```
body{

    background: url("../images/bannerBack.gif");

    background-repeat: repeat-x;
        font-family: arial, sans-serif;

}

#banner{

    background: url("../images/logo.gif");

    background-position: top left;
        background-repeat: no-repeat;

}
```

The #banner element changes the image for the Service Center. If you want to change the image for the User Portal, change the #banner_portal element in the style sheet.

2   Place the style sheet and the two images on a web server that is using the same certificate as your fabric web server. For example, if the style sheet is called NewStyle.css, you could copy it to admin/NewStyle.css on your style sheet web server.

Enter the following URL in the External style sheet URL field of the system configuration screen:

```
https://<your.web.server>/service/NewStyle.css
```

The new style sheet applies the new banner background and the logo

Edit Service Provider

The Editing Service Provider page contains four tabs: General, Custom Fields, Certificates, and Proxy Config.

General

The only required fields are the Tenant Name and Administrator Name. Enter this information and any of the non-required field data you want to maintain.

Custom Fields

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.

Certificates

To enable a custom certificate, you upload three certificate files in Apache format: SSL Certificate, SSL Key, and CA Certificate.

To apply a Service Provider certificate:

1   On the General Configuration page, click the **Other Configuration** link. The Editing Service Provider page displays.

2   Click the Certificates tab.

3   On the Certificates tab, browse for and select the follow 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.

4   Click **Submit** to upload the files.

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 uploaded. For more information on how to get a signed certificate, contact the certificate authority.

Note   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 Service Center'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.

Proxy Config

This tab is used to set up vCenter Direct Access.

Domains

You can manage domains on the Domains page.

To view information for a domain, click the domain in the list on the left of the page.

Register a Domain

You can register a domain on the Domains page.

Note To add auxiliary bind account(s) to a domain, you must first register the domain as described below, then edit it as described in Edit a Domain.

When you register a domain, this does not create the new domain, but rather registers an existing Active Directory domain with the system.

To register a domain:

1 Click the **Register a Domain** link.

2 Enter information on the Domain Bind tab as described below.

Field	Description
Name	Enter the NETBIOS name for this domain in upper case letters. For example, SALES.
Domain suffix	Enter the domain suffix. For example, sales.mycompany.net.
Protocol	AD protocol. For example, LDAP.
Port	Numerical port used for the AD protocol.
Domain Controller IPs	(Optional) By default, the system discovers domain controllers based on the Domain suffix. Optionally enter one or more IP addresses to override this default.
Context	Enter the AD context for this domain. For example, if the domain suffix is sales.mycompany.net, enter dc=sales,dc=mycompany,dc=net.
Domain Bind Account DN	Enter the distinguished name for the service account user for this domain. For example, CN=Administrator,CN=Users.
Password	Enter the password for the service account.
Password verify	Re-enter the password.

Any incorrect information is highlighted in red and a description of the error is displayed.

3 Click **Save**.

4 Click the Group Info tab and enter group(s) as desired.

The system gives you suggestions for auto-completing the group name after you type the first four characters.

Admin groups - Enter security groups for admin users. For example, cn=adminusers,ou=groups. Click Add Admin Group to add another group. There are several different types of admin users. If you are registering an enterprise domain, you need to add at least a Super Admin - Enterprise Admin. You can use the Add Admin Group link to add additional security groups with different privileges. See Roles and Permissions to customize the permissions available to a particular role.

5   Click **Save**.

The system redirects you to the login page.

Edit a Domain

You can edit a domain on the Domains page.

To edit a Domain:

1   Click the domain in the list on the left of the Domains page.

2   Click **Edit**.

3   To edit general information:

a   Edit information on the Domain Bind tab as described below.

Field	Description
Name	Enter the NETBIOS name for this domain in upper case letters. For example, SALES.
Domain suffix	Enter the domain suffix. For example, sales.mycompany.net.
Protocol	AD protocol. For example, LDAP.
Port	Numerical port used for the AD protocol.
Domain Controller IPs	(Optional) By default, the system discovers domain controllers based on the Domain suffix. Optionally enter one or more IP addresses to override this default.
Context	Enter the AD context for this domain. For example, if the domain suffix is sales.mycompany.net, enter dc=sales,dc=mycompany,dc=net.
Domain Bind Account DN	Enter the distinguished name for the service account user for this domain. For example, CN=Administrator,CN=Users.
Password	Enter the password for the service account.
Password verify	Re-enter the password.

Any incorrect information is highlighted in red and a description of the error is displayed.

b   Click **Save**.

4   To edit group information:

a   Click the Group Info tab and edit group(s) as desired.

The system gives you suggestions for auto-completing the group name after you type the first four characters.

Admin groups - Enter security groups for admin users. For example, cn=adminusers,ou=groups. Click Add Admin Group to add another group. There are several different types of admin users. If you are registering an enterprise domain, you need to add at least a Super Admin - Enterprise Admin. You can use the Add Admin Group link to add additional security groups with different privileges. See Roles and Permissions to customize the permissions available to a particular role.

b   Click **Save**.

5   To add or edit auxiliary bind account(s):

a   Click the Auxiliary Bind Accounts tab.

b   To add an account, enter the account DN, enter and re-enter the password, and then click the **Add Bind Account** link.

c   To edit an account, edit information in the fields as desired.

d   Click **Save**.

Roles and Permissions

You can add or remove permissions for roles on the Roles page.

Select one of the roles and edit the permissions as desired by double-clicking to turn the permission on or off.

Desktop Capacity and Model Definition

You can define standard capacities and desktop models on the Desktop Capacity & Model Definition page.

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

Define a New Standard Capacity

You can define a new standard capacity on the Desktop Capacity & Model Definition page.

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 information as described below.

▪   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. Supported values are from 256 MB to 8 GB, depending on the underlying NVIDIA GRID card.

  Note Before making this setting, review the following information:

  - A vGPU-based capacity can be mapped only to a GPU-capable desktop manager.

  - A GPU-capable desktop manager is dedicated to the GPU desktops. Non-GPU desktops should not be created.

  - You can have multiple GPU desktops with different vGPUs in the same compute/desktop manager. The limitation in this case is that GPU resources may be under-utilized.

  - GPU desktops require memory to be reserved. Hence memory over allocation is not possible in a GPU compute.

  - vMotion and DRS are not supported for GPU desktops.

- 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 a standard capacity on the Desktop Capacity & Model Definition page.

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**.

Note

If a standard capacity is disabled after having an assignment created for one of its desktop models, then the assignment will still remain active.

Create a Desktop Model

You can create a desktop model on the Desktop Capacity & Model Definition page.

Prerequisites

You must have at least one standard capacity defined before you can create a 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.

  Note the following:

    - A desktop Manager can be mapped to only one standard capacity.

    - Once capacity is consumed (even a single unit), a desktop manager cannot be mapped/reassigned to different standard capacity.

- 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**.

What to do next

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 a desktop model on the Desktop Capacity & Model Definition page.

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.

Downloading Reports on the Desktop Capacity and Model Definition Page

On the Desktop Capacity and Model Definition Page, you can download the Customer Usage Report and the Concurrent Users License Report.

- Customer Usage Report

    - To download the Customer Usage Report, click the **Download Usage Report** link under the Standard Capacities list on the left of the page.

    - The report downloads in .csv format.

    - The Usage Report shows data for overall capacity quantity.

■ Concurrent Users License Report

■ To download the Concurrent Users License Report, select the date range, VM type (or 'allDesktopsApps' for all VMs), and Organization ID (or 'all' for all orgs), and then click the **Download Report** button.

■ A zip file downloads containing the GeneralReport file in .csv format.

■ This file shows peak concurrent users, along with any errors, for selected orgs.

Helpdesk Console - Backend Control Panel (Beta Feature) 8

You can configure the Helpdesk Console using the Backend Control Panel on your service provider appliance. For more information on the Helpdesk Console, see the release notes and Tenant Administration guide.

Notice Regarding Beta Features and Support

HELPDESK CONSOLE IS PROVIDED "AS IS", WITHOUT SLA OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

If you encounter questions or issues using Helpdesk Console, you can send them to deployment@vmware.com. VMware is not committed to productization of any features or resolution of any issues of the Helpdesk Console.

Access the Backend Control Panel

To access the control panel:

1   Navigate to the following URL:

https://<SP appliance IP>/dt-haca-backend

2   Log in using your usual service provider credentials.

Settings on the Backend Control Panel

Check boxes control which Helpdesk Console tabs display for each tenant, as described below.

Check Box	Helpdesk Console Tab	Tab Description	Checked By Default?
CONSOLE	Virtual Machines	Provides console access to all desktops for assigned administrators (Super-Administrator and Support Administrators). This version of the tab displays for users with the Super-Administrator role.	Yes
CONSOLE_FOR_NON_ADMIN	Virtual Machines	Provides console access to standard users to their assigned VMs for self-servicing/remediation purposes.	Yes
HEALTH	Health	Allows an administrator to monitor overall health of desktops, desktop assignments, and application assignments. The health agent (an optional install on the desktops and images) reports on running services, running applications, and open network ports.	No
REMOTE_ASSIST	Remote Assistance	Allows a helpdesk operator or administrator to shadow an active user session.	Yes
REPORT	Usage Report	Displays usage trends and allows administrator to view user activity session reports.	No
HISTORY	History	Provides the access log for auditing purposes.	Yes
LAB	Lab	For VMware internal use; should not be enabled.	No