

Horizon DaaS Platform 6.1 Blueprint

This document provides an overview of the data center infrastructure requirements of the Horizon DaaS Platform. The view presented here is from the service provider (SP) perspective: that is, data center infrastructure primarily refers to the organization of resources within the SP site. Topics such as tenant user storage requirements are not addressed in detail in this document.

August 2014

vmware

Revision History

Date	Version	Description
08/04/2014	DRAFT 1	Created new doc for 6.1; updated software version numbers; initial markup for direct ESX changes
09/01/2014	DRAFT 2	Edited and added details in dtRAM and Agent Compatibility sections under Platform Overview; updated information on appliance memory, HW reqs, host sizing, and CPU speed under Compute Resources; Removed refs to NAS in Figures 2-1, 2-2, 4-1, 4-2, 4-4; added placeholders for new Security section
09/04/2014	1.0	Accepted changes re: end of direct ESX support in following sections; Terms, Compute Resource Software Requirements (removed whole section), 4.1.1 Distributed Virtual Networking, Storage, Appendix A NetApp New security section: added content for 10.1 Platform Security, 10.1.2 DaaS Agent Services, 10.1.1 Appliance Services; deleted placeholders for 10.1.3 Security Between DaaS Agent and Desktop Manager, 10.2 Hypervisor Security, 10.2.1 Partitioned Hosts, 10.2.2 Transparent Page Sharing (TPS)
10/03/2014	DRAFT 3	Updated VSC and ONTAP versions in Appendix
10/06/2014	1.1	

© 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 Introduction	7
1.1 Intended Audience	7
1.2 Organization of this Document	7
1.3 Terms	8
2 Platform Overview	9
2.1 Key Components of the Horizon DaaS Platform	9
2.2 Horizon DaaS Management Appliances	11
2.2.1 Management Appliance High Availability	11
2.3 Utility and Maintenance Servers	13
2.3.1 Horizon DaaS Remote Access Manager (dtRAM)	13
2.3.2 Network Services	14
2.4 Agent Compatibility	14
3 Compute Resources	15
3.1 Hardware Requirements for Horizon DaaS Management Hosts	15
3.1.1 Horizon DaaS Appliance Sizing Requirements	15
3.1.2 Sizing a Management Host for a Specific Number of Tenants	16
3.2 Hardware Requirements for Virtual Desktop Hosts	16
3.2.1 Sizing a Desktop Host for a Specific Number of Desktops	16
3.2.2 Host Sizing Calculations	17
3.2.3 CPU Speed Considerations	17
4 Network Resources	18
4.1 Virtual LANs in the Horizon DaaS Platform	19
4.1.1 Distributed Virtual Networking	19
4.2 Layer 2 segregation using VLANs	20
4.3 Layer 3 segregation using VRFs	20
4.4 Networking Resources	21
4.4.1 Switches	21
4.4.2 Routers	21
4.4.3 Load Balancing	21
4.4.4 Gateways	21
4.4.5 Cross Data Center HA	21
4.5 Managing External IPs and global DNS entries	22
4.6 Wiring the Data Center	23
5 Storage Resources	25
5.1 Storage Options	25
5.1.1 SAN Storage	25
5.1.2 NFS Storage	25
5.2 Tenant Data Storage	27
6 Networking between Data Centers	28
6.1 Traffic between Data Centers	28
7 Sample Deployment	30
7.1 Horizon DaaS Management Appliances Required for Tenant A	31
7.2 Horizon DaaS Management Appliances Required for Tenant B	31
7.3 Desktop Host Requirements for Tenant A and Tenant B	31

7.4 Additional Data Centers and Tenant C	32
7.5 Storage: Three Tenants in Two Data Centers	32
8 Planning a Production Environment	33
9 Data Protection	34
9.1 Horizon DaaS Appliance Backup	34
9.2 Desktop Backup	34
9.3 User Data Backup / Replication	34
10 Security	35
10.1 Platform Security	35
10.1.1 Appliance Services	35
10.1.2 DaaS Agent Services	35
11 Role Separation and Administration	37
11.1 Service Center	37
11.2 Enterprise Center	37
11.3 Desktop Portal	37
Appendix A NetApp	39
A.1 Best Practices	40
A.2 Configuring Your vFiler	41
A.3 Desktop DR Deployment Strategies	42
Appendix B Cisco Virtualized Multi-Tenant Data Center (VMDC)	43
B.1 VMDC 2.2 Solution Components	44
B.2 Suggested components for trial and POC environments	45
Platform Install Checklist – Install Using vCenter	46
Service Provider Installation Worksheet	47
Tenant 1 – Installation Worksheet	49
Tenant 2 – Installation Worksheet	51
Figure 2-1 Relationship between Horizon DaaS Management Hosts and Horizon DaaS Appliances (Multi-Tenant)	10
Figure 2-2 Horizon DaaS Logical View (One Tenant)	10
Figure 4-1 Horizon DaaS Logical View (Additional Tenant)	19
Figure 4-2 Layer 2 Segregation Using VLANs	20
Figure 4-3 External Port based NAT	22
Figure 4-4 Sample Data Center Wiring Diagram	23
Figure 4-5 Sample ESX Network configuration for both tenant and management host.	24
Figure 5-1 Horizon DaaS Storage Architecture for NFS based configurations	26
Figure 6-1 Multiple Data Centers	28
Figure 7-1 Sample Network used in this Document	30
Figure 8-1 Sample Data Center Wiring Diagram	33
Table 1-1 Common Terms	8
Table 3-1 Horizon DaaS Appliance Sizing Requirements	15
Table 3-2 Sample Hardware Requirements for each Horizon DaaS management host	16
Table 3-3 Minimum Hardware Requirements for Virtual Desktop Host	17
Table 7-1 : Sample Appliance Estimate (Single Tenant)	31
Table 7-2 : Sample Appliance Estimate (Two Tenants)	31

Table 7-3 Additional Data Center Appliance Estimates	32
Table 7-4 Sample Storage Estimate (Two Data Centers)	32

This page intentionally left blank

1 Introduction

This document provides an overview of the data center infrastructure requirements of the Horizon DaaS Platform. The view presented here is from the service provider (SP) perspective: that is, data center infrastructure primarily refers to the organization of resources within the SP site. Topics such as tenant user storage requirements are not addressed in detail in this document.

The examples in this document are hypothetical and are presented to introduce the methods of estimation only. The equipment needed in any installation is specific to a data center, tenants, and network. For example, the typical storage requirements for a tenant are difficult to generalize since virtual machine (VM) image sizes can vary from as low as 8 or 10 GB in a student environment to more than 50 GB in a business environment.

Estimates in this document are based on past experience and cannot accurately reflect every environment. VMware strongly recommends performing an analysis to determine the requirements of your specific environment. Contact VMware Technical Support for assistance with this analysis.

1.1 Intended Audience

This document assumes that you are familiar with:

- Basic networking concepts such as layer 2 separation
- Microsoft Active Directory
- Virtualization software, such as from VMware vSphere
- Storage concepts such as I/O, protocols like NFS and iSCSI, and replication
- Linux and Windows operating systems
- Data center operations

1.2 Organization of this Document

Platform Overview introduces the individual components of a Horizon DaaS installation, describing each appliance's function and its place in the system.

Compute Resources describes how to size the servers needed to host the Horizon DaaS Platform.

Network Resources describes the build-out of more tenants within a data center. The emphasis in this section is on the core networking in the Horizon DaaS environment between the SP and tenants, particularly on maintaining clear and secure separation between tenants.

Storage Resources focuses on the storage resource requirements for a data center.

Networking between Data Centers demonstrates the basic architecture of a multiple data center SP that includes multiple tenants across multiple geographic locations.

Role Separation and Administration describes the three browser-based graphical user interface portals provided by the Horizon DaaS Platform: the Service Center (for SPs), Enterprise Center (for Tenant Administrators), and the Desktop Portal (for end-users).

1.3 Terms

Table 1-1 lists some common terms that are specific to the Horizon DaaS Platform. Other terms are defined as necessary within the text.

Table 1-1 Common Terms

Term	Definition
Appliance	An appliance is a virtual machine (VM) combined with a functional unit of software in the Horizon DaaS Platform. The term node is used interchangeably with appliance.
Data Center	Data center is a label used to logically group lower-level virtualization resources. Data center corresponds to a physical location managed by an SP.
Hypervisor	A hypervisor allows multiple operating systems to run concurrently on a host computer (hardware virtualization).
Hypervisor Manager	A hypervisor manager refers to the management layer that communicates directly with the hypervisor. vCenter is an external hypervisor management layer that aggregates multiple hypervisors.
Tenant	A customer that is consuming hosted virtual desktops from a Service Provider.
Virtual Desktop	A virtual desktop is a virtual machine that is running remotely (relative to the end user) usually on a virtual desktop host. The virtual desktop has input devices (keyboard and mouse) and a display device (monitor) to view the desktop display.
Virtual Machine Pool	<p>A pool is a named and managed collection of virtual desktops. There are two types of pools, static and dynamic. A typical data center will have a mix of static and dynamic pools.</p> <ul style="list-style-type: none">• A static pool consists of virtual desktops that are assigned to individuals. The first time a persistent user logs in, they are allocated an available VM from the pool. After that time, that VM is now assigned to that user and not available to other users. The number of VMs in the pool should equal the number of users assigned to the pool if all users have 1:1 mappings.• A dynamic pool consists of virtual desktops that are assigned on an as-needed basis. An end user receives any appropriate virtual desktop from the pool. The state of the virtual desktop in a dynamic pool can be recycled to a predefined state between sessions. The non-persistent pool defines the number of users that can be connected concurrently. Therefore, the number of users assigned to the pool can exceed the number of VMs in the pool.

2 Platform Overview

Your DaaS environment can be broken down into four key elements, compute, storage, network, and the Horizon DaaS Platform. Through our patented assembly of these resources managed by the Horizon DaaS Platform, your DaaS solution can scale to hundreds of thousands of virtual desktops across hundreds of tenants in multiple data centers around the globe.

2.1 Key Components of the Horizon DaaS Platform

Horizon DaaS Management Hosts – an HA pair of physical machines that run a hypervisor and host multiple Horizon DaaS management virtual appliances for the service provider and tenants.

Virtual Desktop Hosts - physical machines that run a hypervisor and host tenant desktop VMs. The Horizon DaaS Platform allows for sharing of a Virtual Desktop Host between multiple tenants; however, Microsoft licensing for desktop operating systems prohibits this configuration. If tenants are running a Linux OS or using Windows Server (for which there is SPLA licensing available) then sharing of the Virtual Desktop Host across tenants is permitted.

Storage System- A dedicated storage system supporting block or file based storage access for persistence of the virtual machine's virtual disk.

Networking– The network must support VLAN tagging or alternatively distributed virtual networking (also referred to as DVS) can be used in conjunction with VMware vCenter. A unique network should be defined for the management network (containing the hosts and storage systems), the Service Provider network (literally, an extension of the Service Providers network into the VMware datacenter), the Horizon DaaS management network (referred to as the backbone link local network), and 1 or more isolated networks for each tenant.

Horizon DaaS Appliances – Virtual servers that live on the Horizon DaaS Management Hosts and support the Horizon DaaS solution.

Figure 2–1 Relationship between Horizon DaaS Management Hosts and Horizon DaaS Appliances (Multi-Tenant)

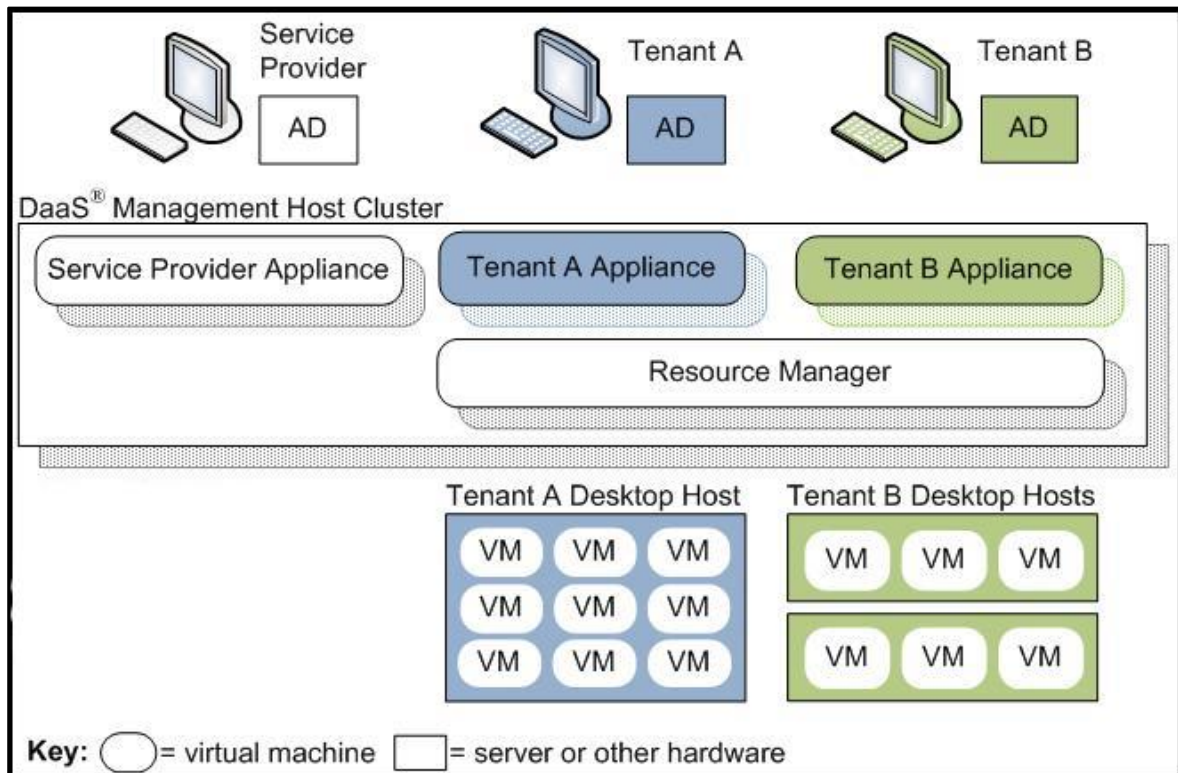
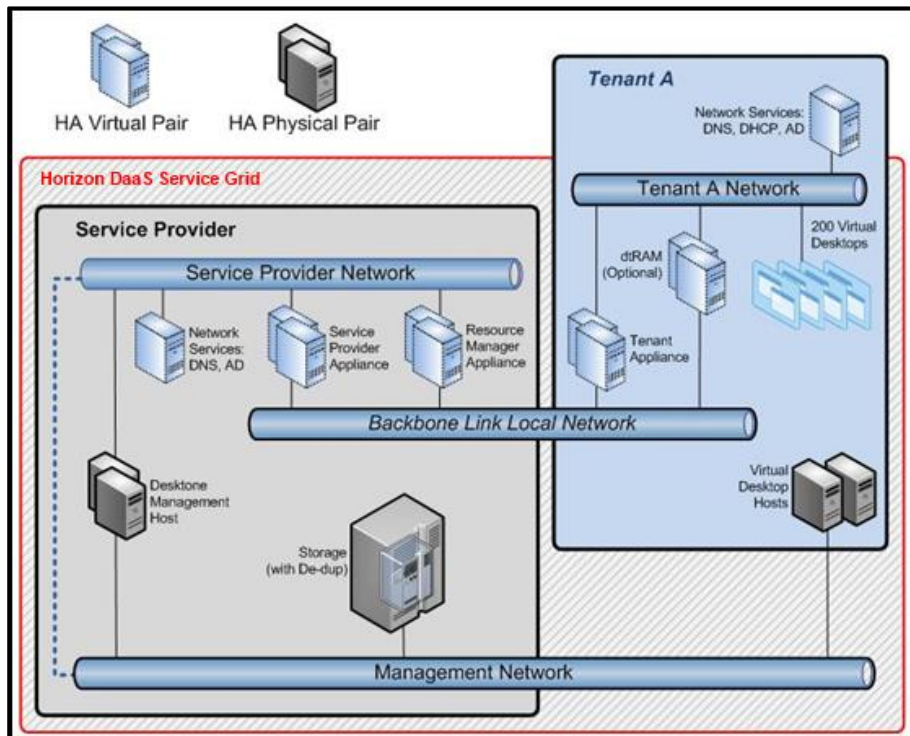


Figure 2–2 Horizon DaaS Logical View (One Tenant)



2.2 Horizon DaaS Management Appliances

The following Horizon DaaS Management Appliances are virtual machines that are used to control and run the Horizon DaaS Platform:

- **Service Provider Appliance** – Provides two types of access to the system: (a) via the Service Center web based UI; (b) 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, once bootstrapped, provides the foundation to install the remainder of the Horizon DaaS Platform.
- **Resource Manager Appliance** – A Resource Manager appliance integrates with the physical and virtual infrastructure in a given data center. A single Resource Manager appliance can be shared across multiple tenants. The Resource Manager abstracts all specifics of the infrastructure from the tenant appliances.
- **Tenant Appliance** – Provides the tenant with both end user and administrative access to their virtual desktops. End users can access and manage their individual virtual desktops via the Desktop Portal. Administrators have the ability to create and manage their virtual desktops via the Enterprise Center.
- **Desktop Manager Appliances** – A desktop manager appliance is a tenant appliance that does not include the components providing brokering and user access (end user or admin). Desktop manager appliances serve 2 key purposes:
 - **Desktop capacity scale out:** The initial tenant appliance is designed to provide capacity of up to 5,000 desktops per data center. When an individual tenant needs to scale beyond 5,000 desktops in a particular data center, additional desktop manager appliances can be added to provide this capacity. Additional desktop manager appliance pairs can support up to another 5,000 desktops each.
 - **Compute resource optimization:** A desktop manager is designed to treat the individually assigned compute equally. If there is a requirement for a specialized desktop workload, that workload can be optimized by creating a new desktop manager pair with only the compute for that workload assigned to it. A few examples of specialized workloads consist of delivering standard VDI, VDI with GPU, and RDS. In these cases the compute for these workloads would be separate and distinct from each other.

All management appliances are connected to the Backbone and either the SP network (Service Provider Appliance and Resource Manager Appliance) or the Tenants own network as shown in Figure 2-2 above. Horizon DaaS requires that all management appliances be installed as HA pairs. To ensure physical hardware high availability, all Horizon DaaS Management appliance pairs are automatically distributed across separate physical Horizon DaaS Management Hosts.

The Horizon DaaS Management Appliances allow monitoring via the standard CIM (common information model) WBEM (web-based enterprise management) interface. You can use any monitoring tool capable of understanding the CIM data model (for example, Tivoli). Information related to the types of CIM classes and recommended thresholds are available in the Horizon DaaS Platform Monitoring technote in the Partner Portal.

2.2.1 Management Appliance High Availability

High availability of management appliances is inherently built-in to the platform itself. How high availability is accomplished varies depending on the appliance type. In all cases management appliances are deployed in pairs to protect against the failure of any single appliance. Appliances are placed on separate physical management servers to protect against hardware failure. In some cases, paired appliances could end up on the same host. This would normally happen when vCenter clustering is used with DRS. DRS could vMotion an appliance to a host where the appliance pair already exists. It is possible to ensure that DRS doesn't move a VM, but it has been a conscious decision to let DRS appropriately balance the environment and determine where a VM should run. If a host were to fail that has both paired appliances the appliances would automatically and immediately be started on another host in the cluster resulting in

very minimal downtime. There are several technologies used to enable high availability that require different handling when an appliance goes down. They are:

- Database Replication: All management appliances that contain a database utilize a master/slave replication scheme. That means at any point in time there is only a single master database for a pair of appliances. The master database is the only database that can be written to. The master database will always be on the appliance that is marked as primary in the appliances screen in the service center. If an appliance that is not the primary appliance (i.e. is running a slave database instance) goes down there is no effect to the environment. If an appliance that is the primary appliance and therefore contains the master database instance of a database cluster goes down there are 2 courses of action depending on the type of appliance:
 - 1) Manual Failover: In general it's not desired to promote a slave instance in a database cluster to be the new master if it's not required. When failover occurs, the old master database has been evicted from the cluster. When the failed appliance comes back online, the database cluster must be reinitialized so that the new instance can be added. This requires a small amount of downtime. In many cases it's not required to automatically promote a slave instance in the database cluster to be the new master. This is possible because critical activities can still be accomplished without writing to the database. So, the approach here is to not automatically fail a master database instance but rather wait for the master to come back online. If the primary appliance has truly failed, a manual promotion of a slave instance should be performed.
 - 2) Automatic Failover: There are cases where it's not possible for the system to perform critical functions when the primary appliance has gone down. In these cases automatic action is taken to promote a slave instance to be the new master of the database cluster which evicts the old master instance from the cluster. There is care taken when doing this though. If a primary appliance were to reboot or go down for a short period of time it would not be desirable to evict it from the database cluster because manual cluster reinitialization would be required which implies downtime. So a grace period is allowed before action is taken. By default, this grace period is 5 minutes and can be alternately configured.
- Floating IP Address: For any appliances that have services accessed by a user (end user or admin), a floating IP address is used to ensure all traffic is routed to an active appliance. This includes SP and tenant appliances. When creating SP and tenant appliances, individual static IP addresses are requested as well as a 3rd shared address called a floating IP address. The appliance pair will share a floating IP address. The floating IP address is designed to move between the pair of appliances and always be bound to an appliance that is online. The technology used to handle failover of the floating IP address exchanges heartbeats between the paired appliances and when an appliance that was the owner of the floating IP address goes down it will be moved to the active appliance thus taking ownership of any traffic destined for the floating IP address. This process is near instantaneous as the heartbeats occur at a very frequent intervals and an arp request is sent to the switch ensuring network routing tables are immediately updated. In order to ensure consistent user access, any DNS resolution should be configured to point at the floating IP address and not an individual appliance address.

In general all appliances are considered disposable except for the database. It is highly recommended to backup the databases on all primary appliances on a nightly basis. Please see the technote regarding database backup for further information on how to configure backup. Scripts are provided in order to do proper database backup and restore. It is not required to backup the appliances themselves as they can very easily be recreated by using the appliance restore feature available in the Service Center. In fact appliance restore is almost always faster than manually restoring a VM from backup. Please refer to the online help on appliance restore in the Service Center. There are specific limitations to understand especially when restoring a pair of appliances at the same time. Given the approaches to HA as described above, the HA characteristics of the individual management appliances are as follows:

- Service Provider Appliances: SP appliances contain a replicated database and employ a manual failover approach. In a multi-DC install the primary appliance in the primary DC has the master DB instance and all other appliances run a slave instance. This even includes the primary SP appliance in a secondary DC. So, for example, in a 2 DC install there would be 2 pairs of appliances deployed (1 pair per DC) but 1 master DB instance and 3 slave instances.

- **Resource Manager Appliance:** Resource Manager appliances are completely stateless and therefore there are no special HA considerations for these appliances.
- **Tenant Appliances:** Tenant appliances contain 2 databases that make up separate database clusters. Inside a tenant appliance are 2 core services, referred to as the Access Manager and the Desktop Manager. Each of the core services manages a separate database cluster and employs a different approach to replication. The Access Manager employs a manual failover approach. This approach is taken because users can still establish connections to the desktops and applications even when the master database instance is down. Operations such as provisioning are not available when the primary tenant appliance is down. It's possible to manually promote a secondary tenant appliance if provisioning or other Access Manager operations are required. In a multi-DC tenant install there is only a single Access Manager master database just as there was for the SP appliances. The Desktop Manager service is used to manage the desktops themselves and employs an automatic failover approach because it must write to the database in order to perform basic operations such as desktop allocation. Automatic failover occurs as it has been described above.
- **Desktop Manager Appliances:** Desktop manager appliances run the Desktop Manager service as described previously in the Tenant Appliances section.

2.3 Utility and Maintenance Servers

In addition to core Horizon DaaS management systems, there are a number of auxiliary systems needed for full functionality. These are:

- Horizon DaaS Remote Access Manager (dtRAM)
- Network servers

2.3.1 Horizon DaaS Remote Access Manager (dtRAM)

The Horizon DaaS remote access manager (dtRAM) allows end users outside a tenant's internal network to access their virtual desktops without requiring VPN software. The dtRAM is a virtual appliance (.ova file) that runs on two virtual servers to allow instant failover high-availability. Once a virtual desktop session is established, all the traffic between the end client and the virtual desktop passes through the dtRAM.

The dtRAM requires no additional client software on the virtual desktop's device other than a supported web browser and the appropriate remote display protocol client software (for example, RDP) that is often provided as part of an OS installation. Appropriately configured thin clients can also access virtual desktops via the dtRAM as well.

The capacity of the dtRAM is governed by its usable bandwidth. The scalability of an individual pair of dtRAM virtual appliances can vary significantly based on the actual bandwidth being driven by the active session workloads. For example, if most active users are knowledge workers and using productivity applications such as Microsoft Word or PowerPoint an individual pair of dtRAM virtual appliances could scale to several thousand sessions. On the other hand if there are many active users watching a training video it could drive significantly more bandwidth and limit the number of sessions a pair of dtRAM virtual appliances can serve. If a tenant requires more than a single pair of dtRAM virtual appliances, you might need to load balance multiple dtRAMs for that tenant. You might choose to deploy the dtRAMs on either the Horizon DaaS Management Host or optionally on a new set of servers dedicated to hosting dtRAMs. If you choose to deploy dtRAMs on the management host, bandwidth to the host should be monitored closely to ensure an appropriate amount of bandwidth is available for normal appliance communication.

2.3.2 Network Services

DNS, DHCP, NTP and Active Directory are necessary components as part of a Horizon DaaS installation. There are two ways to implement these services. They can be implemented locally within the data center in the Tenant Network, or the Tenant Network can be extended via a site to site connection (VPN or MPLS) to the Tenant's own data center.

The site to site connection back to the customer's network works well for DNS, DHCP, and Active Directory as long as:

- The latency back to the customer's network is less than 200ms.
- The customer's data center has the bandwidth required for this connectivity.

If the site to site connection is being used for only the AD, DNS, and DHCP traffic, then there will be minimal bandwidth requirements (1Mbps or less). If the customer is using the site to site connection back to their network for other applications, then it is necessary to determine the bandwidth requirements of those applications. For example, if users will be accessing network file shares frequently using the CIFS protocol, then the latency needs to be kept to a minimum as CIFS has very poor performance once there is any latency or packet loss.

If the bandwidth requirements are too high, or the latency is not within a reasonable range, then it is possible to have a local copy of the AD running in the data center as a replicated AD.

2.4 Agent Compatibility

It is recommended that the View Agent, DaaS Agent, and View Agent Direct Connect (VADC) components be updated in all gold patterns and virtual desktops with each new release of the Horizon DaaS Platform. The DaaS Agent is backwards compatible to one minor version of the Horizon DaaS Platform. However, to take advantage of new functionality in the Horizon DaaS Platform, the DaaS Agent would need to be upgraded. For example, DaaS Agent v6.0.x can be used with Horizon DaaS Platform v6.1 (but some new features may not be available). Please refer to the product support notices section of the release notes for each Horizon DaaS Platform release for specifics on the functionality that affects these components.

3 Compute Resources

Compute resources refers to the physical servers necessary to support the Horizon DaaS Platform and the software required on those hosts. Horizon DaaS Management Appliances and desktop virtual machines cannot reside on the same physical server. Separate servers must be used for the following:

- Horizon DaaS Management Host (service provider)
- Virtual Desktop Host (tenant)

Although both types of hosts support virtualized servers or desktops, the optimization of each of these hosts is slightly different. As such the process for sizing each server is defined separately below.

3.1 Hardware Requirements for Horizon DaaS Management Hosts

The Management hosts are a pair of physical machines that contain the Horizon DaaS Management Appliances (both service provide and tenant appliances). Several sample profiles are defined below; once a server is full you can simply add additional Management hosts to the platform.

3.1.1 Horizon DaaS Appliance Sizing Requirements

The following are the prescribed sizing requirements for Horizon DaaS appliances.

Table 3–1 Horizon DaaS Appliance Sizing Requirements

Appliance	Template (Memory/Disk Space)	Sizing
Service Provider Appliance	Standard (3GB/20GB)	1 pair / dc
Resource Manager Appliance	Standard (3GB/20GB)	1 pair / dc / 20,000 VMs
Tenant Appliance	Standard (3GB/20GB)	1 pair / dc / tenant / 5,000 users
dtRAM Appliance	FreeBSD (512MB/8GB)	1 pair / dc / tenant

The smallest environment begins with two management hosts, each with one service provider appliance, one resource manager and one tenant appliance. From there, additional tenants are added to the datacenter by adding an additional tenant appliance to each management host. The size of the management host is generally referred to by the number of tenants it can support.

3.1.2 Sizing a Management Host for a Specific Number of Tenants

There are three variables to consider when determining the hardware configuration for a Horizon DaaS Management Host:

- CPU – Each core supports 10 tenants. For example, four cores are required to support 40 tenants.
- Memory – Each tenant requires 3.5 GB of RAM on each Horizon DaaS management host (3 GB for each of the tenant appliances and 0.5 GB for each of the dtRAM appliances). For example, 125 GB of RAM on each host is required to support 35 tenants.
- Storage – Each Tenant requires 56 GB of storage, 28 GB allocated to each Horizon DaaS management host (20 GB for each of the tenant appliances and 8 GB for each of the dtRAM appliances). For example, a pair of management hosts that can scale to 50 tenants requires 1400 GB (1.4 TB) of storage each (2.8 TB total).¹

Table 3-2 defines the server hardware used for two sample Horizon DaaS Management hosts.

Table 3–2 Sample Hardware Requirements for each Horizon DaaS management host

Component	Trial Environment	Production Recommendation
CPU	1 CPU	1 CPU
CPU Architecture	4 Cores	8 Cores
Minimum RAM	48 GB	128 GB
Data disk configuration ¹	560 GB	1.4 TB of Storage
Supported Tenants	15	35

3.2 Hardware Requirements for Virtual Desktop Hosts

Virtual desktop hosts are sized based on the number of CPU cores and amount of memory installed in the server. All tenant virtual desktops reside on shared storage. As such, Desktop Hosts only require a pair of small disks for the hypervisor O/S installation.

3.2.1 Sizing a Desktop Host for a Specific Number of Desktops

The guidelines for sizing the Memory and CPU for a desktop host are:

- CPU – VMware recommends allocating about 300 MHz CPU for a stand 1vCPU desktop. Based on the total speed of the CPU you can determine the virtual to physical ratio. For example, a 3.0 GHz CPU core will support 10 standard desktops, or a 10:1 virtual to physical ratio. Virtual to physical CPU ratios will vary based on use case and type of processor. Please refer to [CPU Speed Considerations](#) below for further information.
- Memory – VMware recommends setting a 30% over commit ratio for memory; that is 32GB of physical memory yields approximately 40GB of virtual memory allocated for desktops. Memory over commit ratios can vary based on the workload on a host. The more similar the workload the higher the memory over commit ratio can be. For example, if a host has all Windows 7 SP1 VMs then page sharing will be optimal and therefore the memory over commit can be high.

¹ If you are using external storage that has deduplication for the Horizon DaaS appliances, the storage capacity requirements would be less.

3.2.2 Host Sizing Calculations

Two formulas are helpful when sizing your hosts. There are four variables for each formula, you can solve for any of the four variables, so long as you know three. The variables are the number of VMs on the host, the amount of memory or CPU cores assigned to each virtual desktop, the amount of physical memory or CPU cores installed in the host, and the over commit ratios for either the memory or CPU cores.

Memory:

$$[\text{Number of VMs}] \times [\text{Virtual memory per VM}] \leq [\text{Physical memory}] \times [\text{Memory over commit ratio}]$$

CPU:

$$[\text{Number of VMs}] \times [\text{Virtual CPUs per VM}] \leq [\text{Number of physical cores}] \times [\text{CPU over commit ratio}]$$

Table 3-3 defines the server hardware used for the sample Virtual Desktop hosts. The table assumes a virtual desktop that consists of 2 GB of RAM and one virtual CPU. This example uses a 10 x CPU over commit ratio and a 1.5 x memory over commit ratio.

Table 3–3 Minimum Hardware Requirements for Virtual Desktop Host

Number of Desktops	Cores Required	RAM Required (GB)
20	2	32
40	4	64
60	6	96
80	8	128
120	12	192

3.2.3 CPU Speed Considerations

As the diversity of server processors continues to expand, a simple core ratio is not appropriate in most situations – particularly in the case of very fast or very slow processors. It has become standard practice to use MHz based sizing. To size desktops to a server using MHz based sizing simply multiply the clock speed of the processor by the number of cores then divide by a per user allocation. VMware recommends allocating 300 MHz per virtual CPU.

As with host sizing equations above, the equation has four variables, you can solve for any of the four variables, so long as you know three.

$$[\text{Number of VMs}] \times [\text{MHz allocated per desktop}] \leq [\text{Number of physical cores}] \times [\text{CPU clock speed}]$$

Example – how many desktops can I host with a single 1.9Ghz six core CPU?

$$\text{Number of VMs} = 6 \times 1900 / 250 = \sim 45$$

4 Network Resources

Note: IPv6 connectivity is required for all appliance installations over the Link Local Backbone network.

There are two key components to the network to assure tenant separation when assembling the Horizon DaaS Platform, VLAN tagging and VRF support. In the Horizon DaaS environment, a tenant network is not a subnet within the SP network; each tenant network is a logical extension of the tenant network existing in the SP data center.

Figure 4-1 shows the distinct networks within the data center:

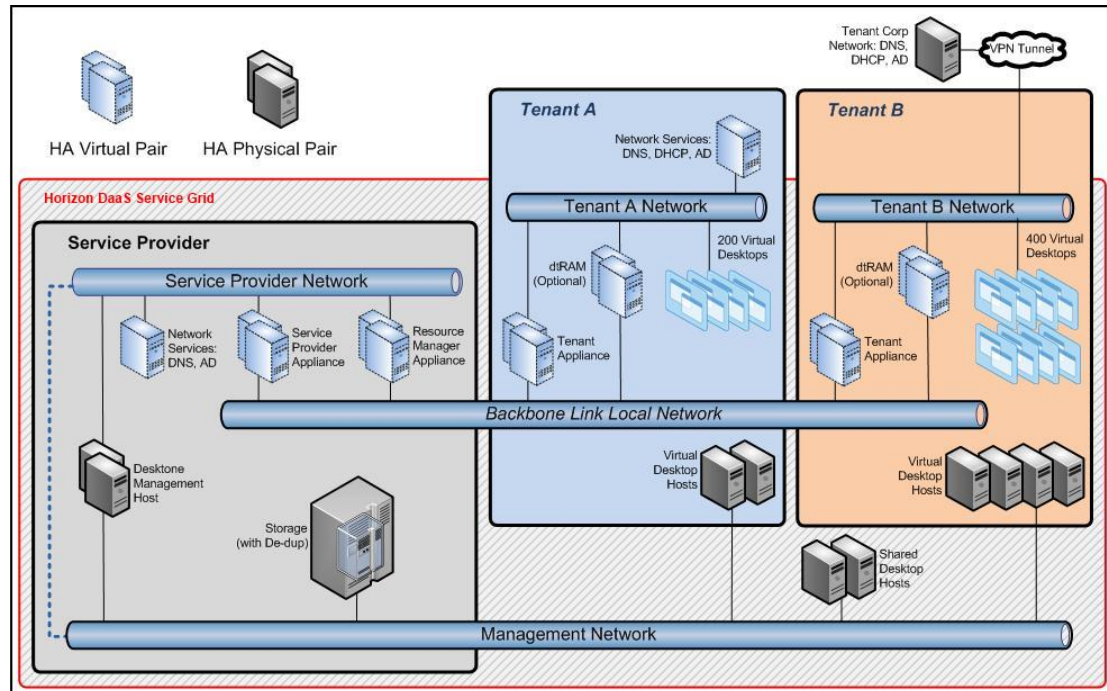
- The Link Local Backbone network is fully controlled by the SP. This network is a link local non-routable subnet (169.254.0.0/16) that is logically separated from all tenant networks. The backbone network connects all Horizon DaaS Management Appliances. For example, the Tenant A Appliance connects to the SP Resource Manager via the link local backbone network.
- The Management Network is used to segregate all the physical hosts and storage systems.
- The SP network is an extension of the Service Provider's network into the data center. The Service Center is accessed through the Service Provider appliances on the Service Provider network. The SP VLAN must have access to the management VLAN for access to Virtual Desktop hosts and the storage systems.
- The Tenant networks are fully controlled by the tenants, again as a discrete VLAN that is separate from the SP 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 SP.

Figure 4-1 emphasizes the clean separation of SP and tenant networks. The area labeled Horizon DaaS service grid provides the core of the Horizon DaaS Platform. The portion of the diagram directly connected to a Tenant network represents the components of the system that are duplicated for multiple tenants.

Note the following network architecture:

- The Tenant networks are not a subnet of the SP network. It is a logical extension of the Tenant A or Tenant B network existing in the SP data center.
- High availability indicates redundant pairs to ensure failover integrity. Most of the computing components are pairs of virtual machines (shown in light blue).
- The number of physical servers in a tenant network largely depends on the size and number of virtual desktops the tenant is hosting.

Figure 4–1 Horizon DaaS Logical View (Additional Tenant)



4.1 Virtual LANs in the Horizon DaaS Platform

A VLAN is an emulation of a standard LAN that allows data transfer to take place without the traditional physical restraints placed on a network. An understanding of the use of VLANs is important to planning and implementing the Horizon DaaS Platform due to their role in ensuring separation of tenants and SP, optimizing the performance of data and management information flows, and in increasing the scalability of the Horizon DaaS Platform.

4.1.1 Distributed Virtual Networking

, An alternate network configuration option is available by using distributed virtual networking as opposed to using the local vSwitch with VLANs. Distributed virtual networking allows the network configuration to be done in a software appliance based controller rather than in the physical hardware device (i.e. the router). There are two distributed virtual networking options available with the Horizon DaaS Platform. They are VMware vSphere Distributed Switch (VDS) and Cisco Nexus 1000V. Please refer to the product documentation for further information.

4.2 Layer 2 segregation using VLANs

VLANs provide segregation of traffic at layer 2 to prevent two tenants from seeing each other's traffic while still sharing the same physical network path. However, in order to reach the end-user, this traffic must pass through a router. Without additional segregation at layer 3, customers would be able to route to each other, or could have a non-resolvable conflict of IP addresses.

Figure 4-2 Layer 2 Segregation Using VLANs

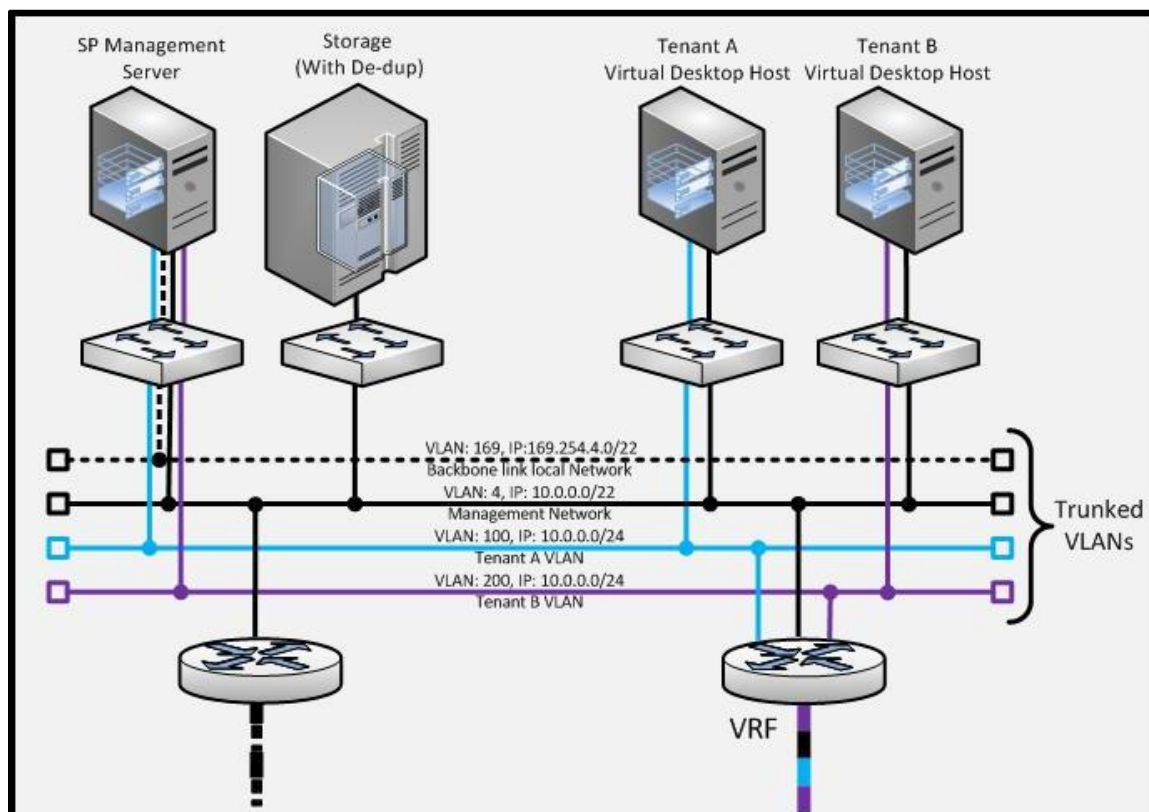


Figure 4-2 illustrates layer 2 segregation with two tenants. In a typical environment, a multilayer switch is required. Note that while four physical switches and two routers are shown in Figure 4-2, only one of each might be needed; virtual switches and routers can be used. The VLANs are trunked. In addition, each of the Virtual Desktop Hosts and the Horizon DaaS management host support multiple virtual machines.

4.3 Layer 3 segregation using VRFs

Virtual Routing and Forwarding (VRF) allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.

VLANs in a Horizon DaaS installation are aggregated into VRFs. Once aggregated into a VRF, segregation is handled at layer 3 and the VLAN IDs are effectively discarded. This means that VLANs require uniqueness only under one VRF, and the same VLAN IDs can be reused under multiple VRFs within a single data center.

4.4 Networking Resources

Switches, routers, load balancers and gateways play a role in any Horizon DaaS installation. This section lists the characteristics required of each of these components. Horizon DaaS is hardware agnostic, only requiring that equipment supports the characteristics listed in this document.

For example, any layer 3 network devices – including firewalls or routers – installed between the customer site and the customer’s virtual desktops at the SP’s data center must meet one of the following requirements, in order of preference:

- Support multiple independent routing tables (VRFs)
- Be dedicated to the customer and support out-of-band management
- Be dedicated to the customer and managed in-band from the customer’s network

Not meeting at least one of these requirements can result in IP address conflicts between the SP and the tenant.

4.4.1 Switches

Switches must support trunking of VLANs. Here are some guidelines regarding the connectivity requirements for the switches:

- Connectivity between the desktops hosts and the storage should be a 10 GB Ethernet network. For additional bandwidth, you could aggregate the two links to achieve 20 GB.
- Connectivity for tenant/protocol traffic can be 1 GB connections.

4.4.2 Routers

Tenant networks are VLAN tagged; for uniformity of management, SP networks are also VLAN tagged. Routers must support VRFs. If there will be customers with VPN access back into their corporate network for access to network services like DNS/AD/DHCP, or for access to other applications, then the router must have the ability to tie that VPN tunnel to the VRF for a tenant.

4.4.3 Load Balancing

Load balancing is only required in front of the tenant appliances for a tenant with 25,000 or more desktops in a single data center. Load balancing is required in front of the dtRAM appliances for a tenant with 5,000 or more concurrent external desktop connections in a single data center.

4.4.4 Gateways

Gateways must support VRFs.

4.4.5 Cross Data Center HA

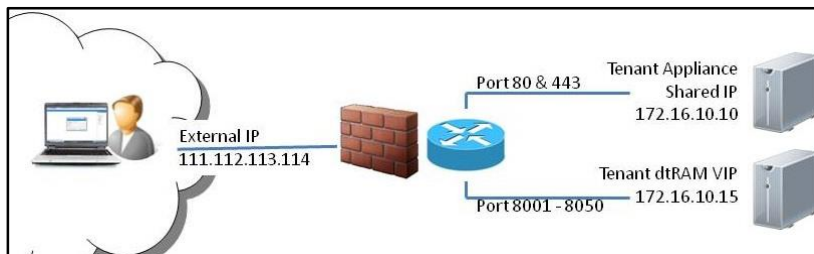
If you configure a tenant in two data centers, there should be a plan for failover to a backup data center in the event of a failure of one data center. The simplest solution is to redirect users to the backup data center by changing the DNS record for the portals. There are more advanced solutions available, such as configuring the F5 BIG-IP Global Traffic Manager to perform the failover automatically. The requirements for HA have to be determined before choosing the best solution.

4.5 Managing External IPs and global DNS entries

In order for a customer to access their cloud hosted desktops from anywhere, the service provider must allocate external IP addresses to each tenant. The edge router must be able to direct traffic destined for the tenant portals to the tenant appliance shared IP and dtRAM enabled desktop connections to the dtRAM VIP. This can most easily be accomplished by using two external IPs per tenant – the first is NAT'ed to the Tenant Appliance shared IP, and the second is NAT'ed to the dtRAM. Depending on the desired DNS name, a global DNS entry should be created for the portal IP on the Service Provider's DNS (such as tenant.SvcProsDesktops.com) or in the tenant's global DNS (such as desktops.tenant.com). The domain where the name is hosted matters because this also defines who is responsible for supplying the SSL certificates for the tenant.

Many routers support port based NATing. If your router is capable of redirecting traffic based on the incoming port, you can condense the number of external IPs needed to one per tenant. In such a configuration, configure traffic destined for port 80 or 443 to redirect to the Tenant Appliance Shared IP and dtRAM ports (typically 8001-8050) to redirect to the dtRAM VIP.

Figure 4–3 External Port based NAT



4.6 Wiring the Data Center

Figure 4-4 represents a sample data center wiring diagram. For clarity, only a sample of connections is represented to demonstrate connectivity from, for example, the desktop hosts to the top of rack switch, to the core switch then to the NAS storage.

Figure 4-4 Sample Data Center Wiring Diagram

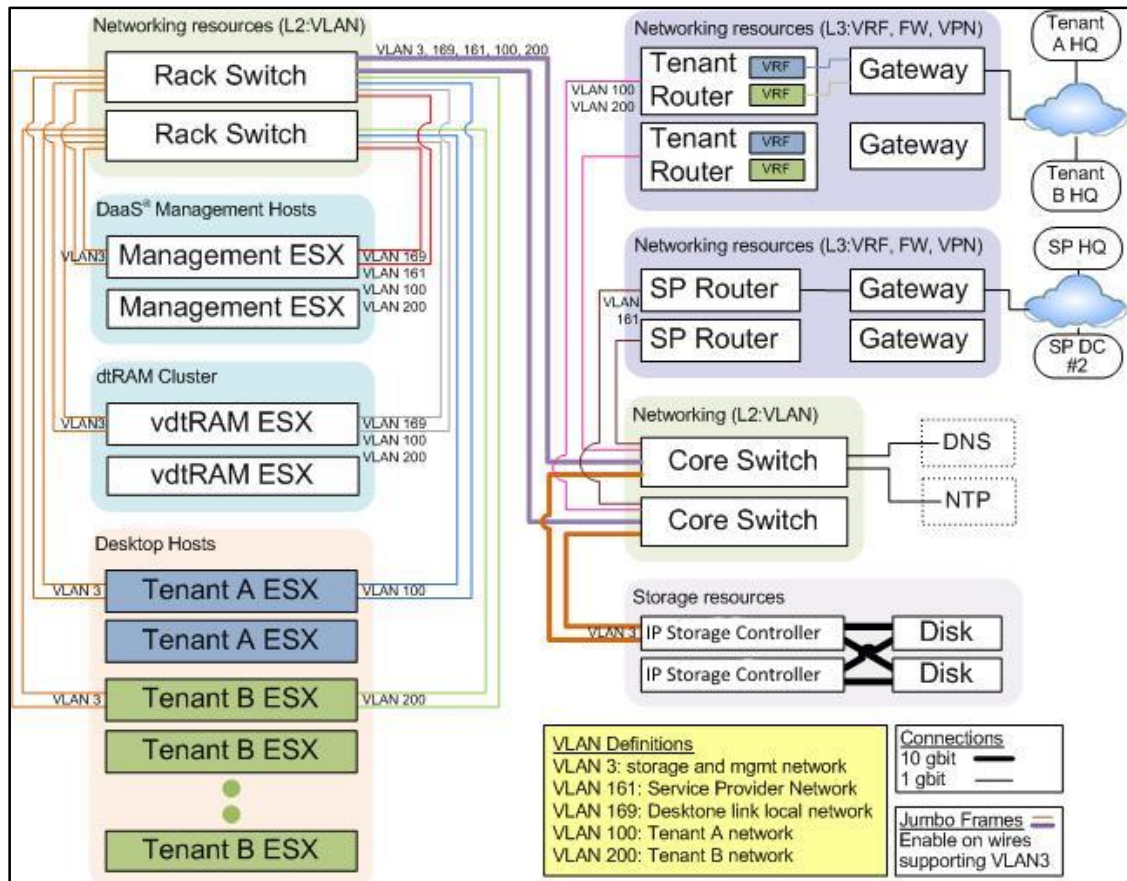


Figure 4-5 demonstrates an example of how to configure networking on an ESXi host for use with the Horizon DaaS Platform. Your management hosts will need to have the default tenant VLANs available since the tenant appliances reside there. Your desktop hosts need to have only the specific tenant VLAN that is assigned to that host. These need to be configured manually on the ESXi hosts before you add the host to the Horizon DaaS Platform.

Figure 4–5 Sample ESX Network configuration for both tenant and management host.



5 Storage Resources

Storage and storage planning are critical parts of any virtualization environment. There are two types of storage you must plan for, local storage on the host and networked storage. All hosts (both the Horizon DaaS management hosts and the Virtual Desktop Hosts) require local storage or SAN storage for the installation of the hypervisor; this is typically accomplished with a relatively small pair of RAID 1 disks installed in the host or a boot LUN from the SAN. Horizon DaaS management hosts require additional local storage or shared storage for all of the Horizon DaaS Management Appliances. For a Horizon DaaS management host, as described in Table 3-2, one could install four additional 600 GB high-speed SAS drives in a RAID 5 configuration to support the management appliances for 50 tenants. Alternatively, a 1.4 TB datastore could be used on each management host.

Horizon DaaS uses shared storage to store the virtual desktops. The shared storage options available depend on how the hypervisors are being discovered by the Horizon DaaS Platform. More information regarding the storage options follow.

5.1 Storage Options

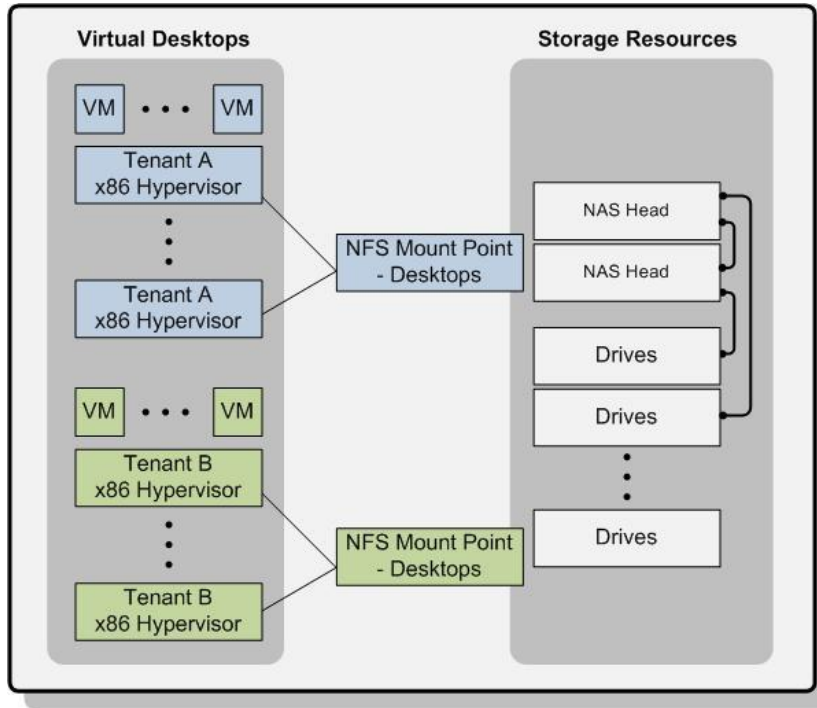
5.1.1 SAN Storage

Fibre channel and iSCSI storage can be used because local storage is not an option for storing desktop VMs. All storage configuration changes are made outside of the Horizon DaaS Platform. Typically this would be done using the vSphere client connected to vCenter. One or more LUNs must be mapped to all ESXi hosts assigned to a Desktop Manager. The datastore(s) associated to the LUN(s) must be created on all hosts for that Desktop Manager and have the same exact name (case sensitive). The Horizon DaaS Platform will clone desktop VMs to the same datastore that the gold pattern resides on using the native vCenter cloning API. Please refer to VMware documentation for further information regarding the use of shared storage across ESXi hosts.

5.1.2 NFS Storage

NFS is an option when using vCenter. The NFS share where the desktops are stored is mounted to each of the tenant's Virtual Desktop Hosts in a given data center as an NFS datastore. Because the virtual desktops are on shared storage, it is possible to move a virtual desktop from one tenant host to another. Make sure your NFS datastore has sufficient I/O capacity. For planning purposes, assume an average of 12- 20 IOPs per virtual desktop for standard knowledge worker workloads. Figure 5-1 presents an overview of the Horizon DaaS storage architecture.

Figure 5–1 Horizon DaaS Storage Architecture for NFS based configurations



Notable characteristics of this architecture are:

- NFS shares presented and mounted on corresponding host servers
- Isolation is accomplished by presentation of NFS shares to specific hosts
- Failover and VM restart done at the Tenant Appliance layer
- De-duplication done at NFS storage layer with up to 95% space saving

NAS is used for storage of virtual desktops and virtual desktop patterns. This shared location allows starting a desktop on any of the tenant hosts.

NAS hardware is capable of fast cloning, thin provisioning, and de-duplication.

VMware recommends clustered storage for redundancy. In addition, each NFS storage head should connect to a resilient switching layer with bonded Ethernet between each NFS storage head and switch. This increases the available bandwidth and resiliency.

Some of the reasons for choosing NAS over SAN are:

- Each NAS mount point can be shared to the entire data center.
- There is no built-in limit to the number of hosts that can mount a single NAS mount point.
- Capacity management can be done at data center granularity.
- Failure of any individual head can be handled automatically by software. No manual intervention is required.
- Single NAS head can host multiple tenants, using NFS export controls to provide firm tenant separation. Certain NAS heads can also be configured into virtual NAS heads to further improve tenant separation.

The four primary goals of any storage solution for VDI space are:

- Rapid manufacturing of virtual desktops
- Data de-duplication to reduce overall storage footprint
- Increased IOPS capacity
- Reduced cost

5.2 Tenant Data Storage

VMware recommends that user's do not store data inside of the virtual desktop. Instead user data directories, such as the My Documents folder, should be redirected to a separate storage location. There are several reasons for this:

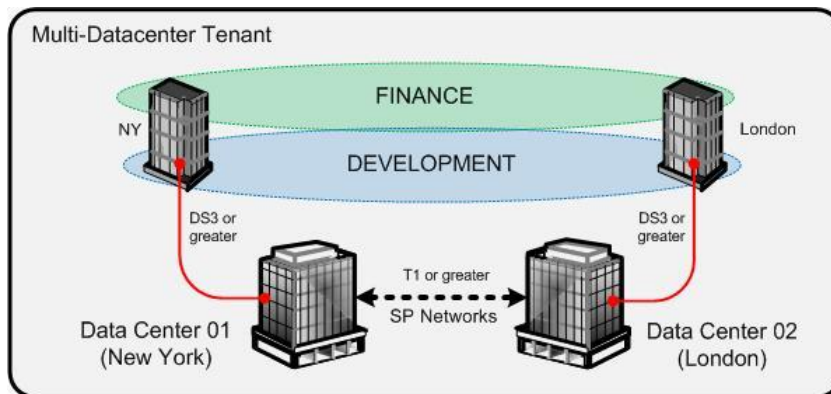
- The storage used for desktop images is highly optimized for performance: high speed FC or SAS disk is required; other optimizations are potentially in place to improve I/O. The storage requirements and performance profile for user data is significantly different from the desktop images and thus a different class of storage can be used.
- Protecting data that is stored inside of a virtual desktop requires that each of the virtual desktops is backed up individually. If user data is redirected to a CIFS share, the external storage can be better protected and maintained independently to the desktop image.
- There are several options for tenant data storage. A tenant's user data can be:
 - Collocated with the Desktops in the Service Provider's Data Center — the service provider can offer an add-on service that provides storage space for user data. Typically this would be CIFS storage as a service where the service provider offers secure tenant specific user data containers based on CIFS shares with integration into the tenant's own Active Directory.
 - In the Tenant's Own Data Center — Access to file shares and other data from the Virtual Desktops would be over the site-to-site VPN or MPLS connection between the tenant and service provider data centers. This connection is often referred to as the backhaul connection. Performance of the backhaul connection depends on the latency between the tenant and service provider data centers. In certain cases, the backhaul connection can be optimized with a WAN accelerator.
 - In the Cloud — the tenant can use a cloud storage service for storing user data.

6 Networking between Data Centers

As noted above, a tenant network can be separated into functional pools rather than only into geographic locations. For example, Tenant C in the example can be divided into Sales, Manufacturing and Finance through the creation of pools since a pool is a logical unit that can span multiple geographic locations. Virtual desktops within a pool have no awareness of where their VM is located; end users should only be concerned with their user experience. Alternatively, pools could be aligned to a specific SLA or use case (i.e. stateless pool versus stateful pool).

Figure 6-1 shows a segment of the example network in which Tenant C is divided into organizational functions by pools rather than geographic locations. Finance and Development each have staff located in both New York and London.

Figure 6–1 Multiple Data Centers



6.1 Traffic between Data Centers

SPs that maintain multiple data centers require network connectivity between the data centers for data sync operations and application traffic. The SP nodes in each data center need to be able to communicate with each other using their IP addresses (NAT will not work). This can be accomplished via a VPN tunnel.

The traffic between data centers tends to be bursty in nature. But experience suggests that a T1 connection between data centers is sufficient to handle all cases without a disruption of service.

Note that the Horizon DaaS management resource overhead scales independently of the number of tenant virtual desktops. Increasing the number of virtual desktops reduces the percentage of the cost of an installation that is required by Horizon DaaS management alone. The Horizon DaaS management overhead is an increasingly smaller portion of the cost of operation as data centers are scaled out with the addition of virtual desktops.

It is important to realize that the example used in this document is a set of calculation methods based on a hypothetical case in order to demonstrate the methods. Optimization of tenant virtual desktops could reduce the number of required desktops resulting in decreases in the number of physical servers.

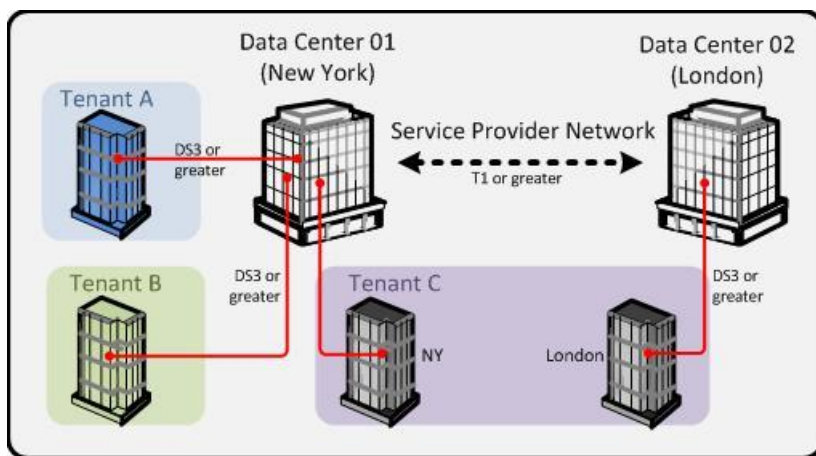
7 Sample Deployment

In order to practice the concepts in this document we have created a hypothetical Horizon DaaS network to accommodate 30,000 virtual desktops. Examples of calculations concerning resources are based on the architecture of this network (Figure 7-1).

The sample network consists of two SP data centers located in New York and London. There are three tenants:

- Tenant A is located in New York and consists of 5,000 virtual desktops.
- Tenant B is also located in New York and consists of 5,000 virtual desktops.
- Tenant C has two geographical locations and consists of a total of 20,000 virtual desktops:
 - 5,000 in New York
 - 15,000 in London

Figure 7-1 Sample Network used in this Document



7.1 Horizon DaaS Management Appliances Required for Tenant A

The following appliances are necessary for the initial Tenant A deployment. We will require the minimum two physical servers to provide physical server level HA. Table 7-1 describes how the Horizon DaaS appliances are allocated on the two Horizon DaaS management hosts.

Table 7-1 : Sample Appliance Estimate (Single Tenant)

		Number of Horizon DaaS Appliances Required	
	Horizon DaaS Management Appliance	Mgmt Host A	Mgmt Host B
SP	Service Provider Appliance	1	1
SP	Resource Manager Appliance	1	1
Tenant			
A	Tenant Appliance	1	1

Remember that virtual desktops cannot be deployed on the Horizon DaaS management hosts. Also, if dtRAM appliances are required, they could optionally be installed on the management host as well or on dedicated dtRAM hosts.

7.2 Horizon DaaS Management Appliances Required for Tenant B

To add Tenant B to the New York data center we simply need to add the additional tenant appliances required to support Tenant B. Additional appliances are indicated in bold font in Table 7-2.

Table 7-2 : Sample Appliance Estimate (Two Tenants)

		Number of Horizon DaaS Appliances Required	
	Horizon DaaS Management Appliance	Mgmt Host A	Mgmt Host B
SP	Service Provider Appliance	1	1
SP	Resource Manager Appliance	1	1
Tenant			
A	Tenant Appliance	1	1
B	Tenant Appliance	1	1

After adding Tenant B we now have four Horizon DaaS Management Appliances running on each Horizon DaaS management host.

7.3 Desktop Host Requirements for Tenant A and Tenant B

Considering the size of these tenants, we have the advantage of being able to use very large servers. For this example we will use the largest servers specified in this document, although in reality we may use this opportunity to explore even higher density compute options.

Desktops per server	Cores	RAM (GB)
120	12	192

Using this server, each tenant will require 42 servers to reach 5000 desktops.

7.4 Additional Data Centers and Tenant C

When adding an additional data center, it is necessary to localize some of the SP appliances which results in some additional overhead cost. However, we also gain efficiencies with the ability to provide data center level HA. For instance, the example includes Tenant C headquartered in London - with 5,000 desktops in New York and 15,000 desktops hosted at a new data center in London. (The additional appliances are indicated in bold font in Table 7-3.)

Table 7-3 Additional Data Center Appliance Estimates

		Number of Horizon DaaS Appliances Required			
	Horizon DaaS Management Appliance	Mgt Host A (NY)	Mgt Host B (NY)	Mgt Host C (London)	Mgt Host D (London)
SP	Service Provider Appliance	1	1	1	1
SP	Resource Manager Appliance	1	1	1	1
Tenant					
A	Tenant Appliance	1	1		
B	Tenant Appliance	1	1		
C	Tenant Appliance	1	1	3	3

After adding Tenant C there are a total of five management appliances on each Horizon DaaS management host in NY and five management appliances on each Horizon DaaS management host in London.

7.5 Storage: Three Tenants in Two Data Centers

Published figures for de-duplication suggest a conservative 75% reduction in storage required. Note that since most virtual desktops can consist largely of duplicated operating system components, the de-duplication savings are typically larger.

For the two data centers described above, the storage requirements under these assumptions are summarized in Table 7-4.

Table 7-4 Sample Storage Estimate (Two Data Centers)

Data Center	NY	London
Total Desktop VM disk	450.0 TB	450.0 TB
Total Desktop VM disk assuming 75% de-duplication factor	112.5 TB	112.5 TB

Note the significant savings realized by current de-duplication technology using the fairly conservative estimate of 75%. To meet these targets, de-duplication functionality must exist on the primary storage system.

8 Planning a Production Environment

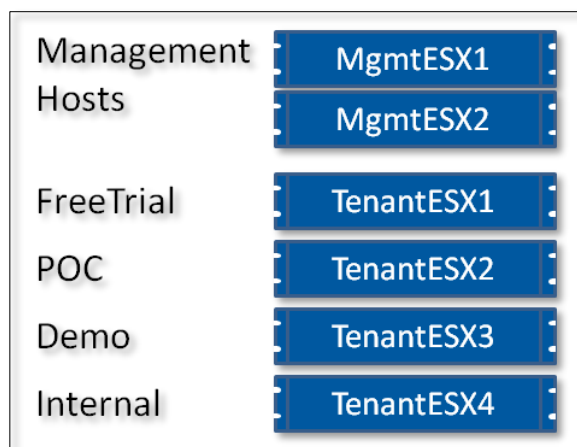
Through VMware's own experiences operating the Horizon DaaS Cloud service, we developed a successful sales model that we offer as part of the Horizon DaaS Blueprint. The process makes use of several dedicated environments to allow prospective customers to experience how simple and productive a DaaS option can be. When initially deploying your production environment we will deploy four tenants. Each of these has a specific purpose in the sales cycle.

The initial tenant we typically configure is the Demo environment. This will become your showcase environment to enable your sales team to show off what DaaS has to offer. The goal is to configure this tenant with static and dynamic pools consisting of Windows 7, Windows server desktops, Windows XP and Ubuntu desktops. This tenant also affords the install team the best opportunity to test the environment infrastructure.

Typically the next tenant we deploy is an internal tenant for use by the service provider. The purpose of this environment is to enable your sales and technical teams to begin using hosted desktops themselves. How better to evangelize the service than if your teams are using the service themselves and are better able to understand customer concerns and the many additional opportunities that come from hosted Desktops.

The final two tenants are directly tied to sales enablement – i.e. let customers see firsthand how simple DaaS can be. The Free Trial environment allows potential customers access to a non-persistent Windows server desktop after a quick enrollment process. This is a key sales lead driver and introduces customers to your service offering. Once your sales team has qualified a lead, you can provide a full static Windows 7 POC desktop for the customer to trial for a short period of time. The goal of the POC environment is to quickly engage prospective customers so they can see how quick and easy DaaS can be and so they can test their own applications in the cloud on their own.

Figure 8–1 Sample Data Center Wiring Diagram



9 Data Protection

9.1 Horizon DaaS Appliance Backup

With the exception of the database embedded in the Horizon DaaS appliance, the appliance is disposable: it is not required that an entire appliance be backed up. VMware provides backup and restore scripts for the embedded databases with the platform. The backup scripts should be executed daily. The most recent backups should be kept on site for fast retrieval access. Additionally, a rotation should be identified to send backups offsite. If the Horizon DaaS appliances reside on external storage that is snapshot and replication capable, that could be considered as an alternate backup strategy.

9.2 Desktop Backup

If user data is properly redirected to external file shares, backup of individual desktops should not be required because the desktop can easily be recreated. However, the gold images used to create the desktops should be backed up on a regular basis. Because a gold image is a powered off virtual machine, the backup should be performed by the service provider. The service provider could use snapshots and replication from the storage system as a strategy to protect the gold image(s). This has the benefit of being able to restore quickly and the ability to provide disaster recovery. A more traditional backup scheme could also be implemented if desired.

9.3 User Data Backup / Replication

The user data redirected from the desktop should be backed up on a regular basis. Using storage system snapshots and replication can be an effective strategy with the ability to restore individual files to a specific point in time. A traditional backup could also be used to provide a similar backup capability.

If user data is stored either at the service provider or tenant data center, file shares should be replicated if high availability and/or disaster recovery is desired. If user data is stored in the cloud, coordination will need to take place with the cloud storage provider in order to understand how to implement HA.

10 Security

10.1 Platform Security

10.1.1 Appliance Services

The service provider, resource manager, tenant and desktop manager appliances act as both clients and servers of several internal platform services. SSL is employed to ensure communication for these services is secure. This involves encrypting the communication channel, and verifying that a certificate identifying the appliance running the service exists and is valid for that appliance.

Every Horizon DaaS deployment generates its own unique Certificate Authority (CA) key pair and certificate during the bootstrap phase of the primary service provider appliance in the first data center. This CA is then used to sign the certificates for the appliances, including the primary service provider itself. The certificate for an appliance is created during its installation step. A key pair and Certificate Signing Request (CSR) are generated initially. The CSR is then copied to the primary service provider appliance for signing, and the signed certificate copied back to the appliance being installed. At no time is the private key for any appliance ever transmitted. The CA certificate is also copied to the appliance and is installed in a trusted certificate store. This process is repeated whenever an appliance is restored, and will generate a new certificate each time. Unlike other appliances, the primary service provider containing the CA cannot be restored. It is important to maintain the appropriate backups for it, and to follow the procedures for promoting another service provider appliance to be the primary in the event of an unrecoverable appliance failure.

When an appliance makes a request to a service (i.e., is acting as a client), it establishes an SSL connection to port 8443 of the appliance running the service (i.e., the server). The server responds with its certificate and the client verifies that it trusts the server by checking that its trusted certificate store contains a certificate for the CA that signed the server certificate. It also validates the properties of the certificate, including the expiration date, and whether the IP address in the certificate matches the IP address it used to make the request.

10.1.2 DaaS Agent Services

The DaaS agent acts as a client of services running on the tenant and desktop manager appliances. SSL is employed to ensure communication for these services is secure. This involves encrypting the communication channel, and verifying that a certificate identifying the appliance running the service exists and is valid for that appliance.

The DaaS agent must be provided with the CA certificate generated by the Horizon DaaS platform. The CA certificate is used to verify that the tenant and desktop manager appliances are trusted. Otherwise, it will refuse to connect to the appliances. The CA certificate can be downloaded from Pattern Management section

of the Enterprise Center. When configuring a new gold pattern, the certificate file should be copied to the certificate folder in the DaaS agent installation folder before the gold pattern is sealed.

When the DaaS agent makes a request to a service (i.e., is acting as a client), it establishes an SSL connection to port 8443 of the appliance running the service (i.e., the server). The server responds with its certificate and the DaaS agent verifies that it trusts the server by checking that its certificate folder contains a certificate for the CA that signed the server certificate. It also validates the properties of the certificate, including the expiration date, and whether the IP address in the certificate matches the IP address it used to make the request.

11 Role Separation and Administration

The Horizon DaaS Platform presents three browser-based graphical user interface portals:

- Service Center
- Enterprise Center
- Desktop Portal

11.1 Service Center

The Service Center is used by the Service Provider administrators to manage the data center resources, such as hosts, storage and the Horizon DaaS Management Appliances. The service center also enables the management of tenant contracts defining tenant models and quotas as well as the configuration of tenant appliances and networks.

The Service Center supports creating and assigning additional roles and permissions among the Service provider administrators to securely distribute management tasks among larger organizations.

11.2 Enterprise Center

The Enterprise Center is used by the enterprise administrators (Tenant Administrators) to manage their virtual infrastructure. Each Enterprise has its own customizable Enterprise Center portal. Enterprise administrators can provision both static and dynamic pools of desktops based on templates that they have customized or new templates that they might upload. Enterprise administrators can also add additional domains and map groups or individuals to either specific virtual desktops or pools.

The Enterprise Center supports creating and assigning additional roles and permissions among the Service provider administrators to securely distribute management tasks among larger organizations.

11.3 Desktop Portal

The Desktop Portal enables individual users to connect to their virtual desktops. Every tenant has their own customizable portal. Users login to the portal and have the option of being directly connected to a desktop they have defined as their default, or presented with a list of available desktops and enabled to choose which virtual desktop to connect to. Users can also set default protocols per VM and additional protocol customizations. Users can connect to the Desktop Portal from a variety of clients including thin clients (both WTOS based WYSE clients and any thin clients running Windows Embedded), thick clients (such as PCs running Windows, Mac OS or Linux) as well as iOS and Android based mobile devices.

The Desktop Portal facilitates connections using a wide variety of remoting protocols.

- RDP (Microsoft) – Microsoft’s Remote Desktop Protocol is a very strong protocol with broad support. The protocol supports a good multi-media experience when less than 20ms of latency, and good user experience when using office productivity apps when latency is under 50ms.
- PCoIP (VMware) – The PCoIP experience provides a very good multi-media user experience in situations with both high latency and constrained bandwidth.
- RGS (HP) – Remote Graphics Software developed by HP primarily for WAN deployments provides good multimedia support with latency as high as 100ms when provided ample bandwidth. RGS is particularly popular for graphics-intense use cases like CAD.
- HTML5 (Ericom) – This client allows you to access your desktop via any HTML5-compatible web browser. It does not require any additional plug-ins, add-ons or installation of any kind on the end user device which makes this suitable for devices such as Chrome OS Netbooks.
- NX (Linux) – Enables access to Linux Desktops

Appendix A NetApp

This appendix lists Horizon DaaS Platform information specific to the NetApp environment.

Supported Hardware	NetApp FAS Series, NetApp V-Series, and IBM N-Series
NFS Permissions	NFS permissions must be manually configured such that the required hypervisors have root access to the appropriate NFS exports.
Access Credentials	In order for the Horizon DaaS Resource Manager to properly access the NetApp API, a service account must be created. This account must have special privileges in order to make the API calls. The specific privileges required are included in a tech note in the Customer Knowledge Base.
Data ONTAP®	<p>The Horizon DaaS Platform is qualified to work with the following versions of Data ONTAP:</p> <ul style="list-style-type: none">• Data ONTAP 7-mode<ul style="list-style-type: none">• V7 (7.3.1 or greater)• V8 (8.0.x, 8.1.x, 8.2.x)• Clustered Data ONTAP (supported with vCenter using VSC)<ul style="list-style-type: none">• V8 (8.1.x, 8.2.x)
Virtual Storage Console	<p>The NetApp Virtual Storage Console (VSC) is a plugin for VMware vCenter leveraged by the Horizon DaaS Platform for rapid cloning of virtual machines. The following versions of VSC are supported:</p> <ul style="list-style-type: none">• 4.1-P1, 4.2.1

Licenses	<p>FlexClone – FlexClone provides the ability for the Horizon DaaS Platform to clone gold images in the matter of seconds (optional for Horizon DaaS but recommended)</p> <p>FlexScale – FlexScale is the tuneable software component to Flash Cache. FlexScale allows different caching modes to be used based on the type of workload (optional for Horizon DaaS but recommended)</p> <p>Multistore – Provides the ability to use vFiler for added tenant security and data mobility (optional for Horizon DaaS but recommended)</p> <p>NFS – This is the base license required to use the NetApp filer for NFS (required by Horizon DaaS)</p> <p>A-SIS – ASIS is the deduplication engine in ONTAP (optional for Horizon DaaS but recommended)</p> <p>NearStore – A NearStore license is required when using ASIS deduplication (optional for Horizon DaaS but recommended)</p> <p>SnapMirror – A SnapMirror license is required for thin replication (optional for Horizon DaaS but recommended if requiring site HA/DR)</p>
NetApp & Horizon DaaS Best Practices	See the document Guidelines for Virtual Desktop Storage Profiling and Sizing on the NetApp website.

A.1 Best Practices

VMware recommends the following best practices in the NetApp environment:

- **File System Alignment** - File system misalignment is a known issue in virtual environments and can cause performance issues for virtual machines (VMs) and therefore could impact the performance of a Horizon DaaS virtual desktop deployment. It is therefore critically important that the NetApp file system alignment practices are followed as per [Best Practices for File System Alignment in Virtual Environments](#). Note that this issue is not unique to NetApp storage arrays and can occur with any storage array from any vendor.
- **Separate Aggregate for Management** – It is recommended to create a separate aggregate at a smaller size to support Horizon DaaS management functions where they are hosted on shared NFS storage. The reason for this is to separate the management I/O load from the virtual desktop I/O load.
- **Maximize Aggregate Size for Desktops** – It is recommended to create an aggregate at the maximum size supported for the particular model of NetApp filer. The reason for this is to include as many spindles as possible to spread data across to have optimum I/O performance.
- **Minimize the number of Volumes** – It is recommended to minimize the number of volumes that are deployed to host virtual desktops. The reason for this is that data deduplication is done within the context of a volume. So, the more data in a single volume the greater chance of data blocks being deduplicated.
- **Separate Volume and NFS Shares per Tenant** – For maintainability, separation, protection and portability purposes, it is recommended that a separate volume hosting NFS shares is created for each tenant's virtual desktops. For smaller tenant deployments, it might not be appropriate to follow the separate volume rule due to reduced efficiencies.
- **vFiler** – It is recommended for an extra layer of security that each tenant have a Multistore vFiler instance created to host the virtual desktops. A vFiler container could also be used to secure and segregate tenant user data if hosted at the SP. vFiler functionality creates logical access separation within the same NetApp filer and would allow integration into the tenant's own Active Directory.

- **Separate Volume to host swap, temp and winpage files** – This is required to separate redundant data from the volumes hosting the base desktop image. This approach reduces the redundant data that would otherwise be locked into snapshots and also replicated for DR. These volumes should have ASIS (de-duplication) disabled.
- **Enable Deduplication** – It is recommended to enable ASIS deduplication for the virtual desktop and any user data host volumes. Note that this needs to be enabled on a per volume basis (disabled by default). Important: when setting up deduplication on the Storage Efficiency tab for a volume, make sure you check the "Scheduled" radio-button, not "On-demand" or "Automated".
- **Use NetApp FlexClone** – It is highly recommended that NetApp FlexClone be utilized for desktop provisioning operations. The ability to provision with FlexClone is built into the Horizon DaaS Platform. FlexClone technology is hardware-assisted rapid creation of space-efficient, writable, point in time images of individual files. FlexClone provides the ability to clone hundreds and possibly thousands of desktop images from a base desktop image providing significant cost, space and time savings.
- **Use SecureAdmin** – The Horizon DaaS Platform supports SSL and non-SSL access to the NetApp filer. By default, the Horizon DaaS Resource Manager will attempt to communicate with the NetApp filer via SSL. There is a configuration parameter to use non-SSL communication. Please refer to Horizon DaaS documentation regarding the specific setting. In order to use SSL to communicate with the NetApp filer, SecureAdmin must be installed and configured.
- **Use FlashCache** – It is highly recommended that FlashCache be used to provide a large front end read cache. This helps lighten the I/O load on the disks and thus helps deal with high read I/O load such as boot storms. The size of the FlashCache varies depending on the FAS model. With a clustered NetApp, each filer head should have its own FlashCache card.
- **Use Snapshots** – Snapshots can provide an almost instantaneous way to protect and recover appliance, user data, and gold images. Snapshots do not affect performance and provide the ability for very fast restores.
- **SnapMirror for DR** – SnapMirror can be used to replicate desktop and/or user data offsite in the case of a site failure. SnapMirror complements NetApp FlexClone and deduplication providing a 'thin replication' capability where the data reduction persists during the replication process.

A.2 Configuring Your vFiler

To enable the Horizon DaaS Platform to see your NetApp vFiler you need to enable httpd and create an account. Use the following commands as an example, these need to be run in the context of the appropriate vFiler (not on the root vFiler)

```
options httpd.admin.enable on
```

```
useradmin role add desktone_role -c "Role for Deskstone API Support" -a login-http-admin,api-license-list-info,api-system-get-info,api-system-get-version,api-system-get-ontapi-version,api-nfs-status,api-nfs-exportfs-list-rules-2,api-nfs-exportfs-modify-rule-2,api-clone-start,api-clone-stop,api-clone-list-status,api-vfiler-list-info
```

```
useradmin group add deskstone_group -c "Group for Deskstone" -r deskstone_role
```

```
useradmin user add deskstone -c "Service account for Deskstone" -n "Deskstone SA" -g deskstone_group
```

A.3 Desktop DR Deployment Strategies

Multiple Data Center Desktop Images: SnapMirror can be used to replicate VM images between multiple data centers. Should a user's primary data center become inaccessible, replicated images would be available in an alternate data center to provide that user's primary desktop.

Multiple Data Center User Data: SnapMirror can be used to replicate data between multiple data centers. Should any data center become inaccessible, replicated user data would be available in an alternate data center.

Backup: Snapshot and SnapRestore can be used to backup and restore VM images and user data.

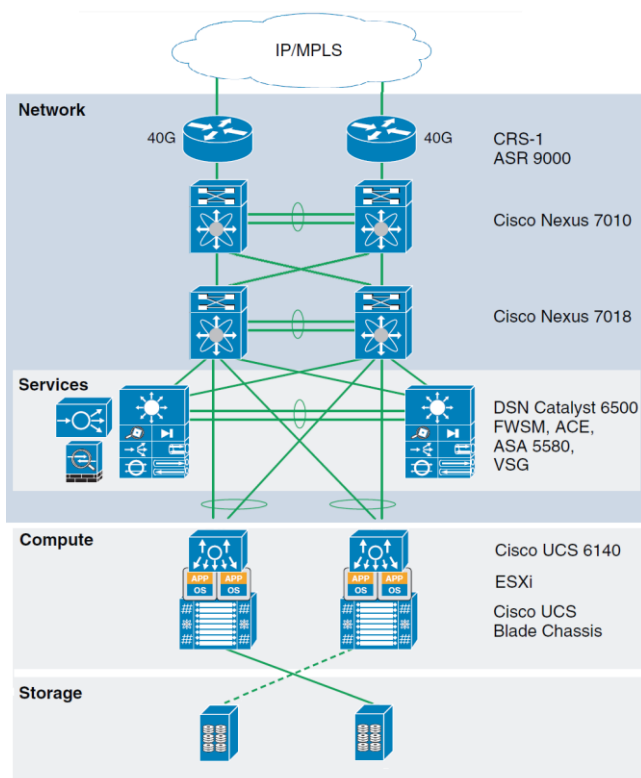
Appendix B Cisco Virtualized Multi-Tenant Data Center (VMDC)

The Cisco® Virtualized Multi-Tenant Data Center (VMDC) architecture is a set of specifications and guidelines for creating and deploying a scalable, secure, and resilient infrastructure that addresses the needs of cloud computing. To develop a trusted approach to cloud computing, Cisco VMDC combines the latest routing and switching technologies, advancements in cloud security and automation, and leading edge offerings from cloud ecosystem partners. Cisco VMDC enables service providers (SPs) to build secure public clouds and enterprises to build private clouds with the following benefits:

- Reduced time to deployment - Provides a fully tested and validated architecture that enables technology adoption and rapid deployment.
- Reduced risk - Enables enterprises and service providers to deploy new architectures and technologies with confidence.
- Increased flexibility - Enables rapid, on-demand workload deployment in a multi-tenant environment using a comprehensive automation framework with portal-based resource provisioning and management capabilities.
- Improved operational efficiency - Integrates automation with multi-tenant resource pools (compute, network, and storage) to improve asset use, reduce operational overhead, and mitigate operational configuration errors.

For more information about the Cisco VMDC Framework go to <http://cisco.com/go/vmdc>

B.1 VMDC 2.2 Solution Components



Please consider the following defines the versions tested. Please contact your Cisco representative for the latest version of the VMDC architecture.

Features	Components
Network	Cisco Nexus® 7010, 7018, NXOS 5.2.1 Data center services node – Cisco Catalyst® 6509-E Switch (with Virtual Switching System [VSS]), IOS 12.2(33)SXJ Cisco ASR 9000, XR 4.1.0 Cisco ASR 1006, XE 3.4.0 15.1(3)S
Services	Cisco Virtual Security Gateway, 4.2(1)SV1(2) Cisco Virtual Network Management Center: 1.2(1b) Cisco Adaptive Security Appliance 5585-60X, 8.4.2 Cisco ACE30 Application Control Engine Module, A 4.2.1
Compute	Cisco Unified Computing System™ (UCS™), 1.4(2b) Cisco UCS 5108 Blade Server Chassis Cisco UCS 6248 Fabric Interconnect Cisco UCS B230 M2 Blade Server Cisco UCS M71KR-E Emulex Converged Network Adapter (CNA) Cisco UCS M81KR Virtual Interface Card (VIC)
Virtualization	VMware® vSphere™ 4.1 U1 VMware ESXi 4.1U1 Hypervisor Nexus N1010-x
Storage	NetApp FAS3170 and NetApp FAS6080 with ONTAP 8.0.2

B.2 Suggested components for trial and POC environments

When deploying an initial trial or Proof of Concept environment you might need to augment your environment in order to test key aspects of the Horizon DaaS Multi-Tenant platform. A basic environment can be constructed using the following Cisco components:

Component	Use
ASR 1001	Routing, VRF and VLAN tagging
ASA 5505	VPN termination and firewall
Catalyst Switch	VLAN
UCS	Compute
NetApp	Storage

Platform Install Checklist – Install Using vCenter

Before you can install the Horizon DaaS Platform, you first need to complete the tasks listed in this document. Contact your VMware customer service representative for help with any of these prerequisites. A Service Provider Installation Worksheet and two Tenant Installation worksheets are included at the end of this document to help organize and collect all the information needed to start the install.

1. Build the network infrastructure required to support multi-tenancy, typically accomplished with VLAN tagging for network separation at layer 2 and VRFs to isolate tenants and allow for a separate routing table for each tenant. See Section 4. Network Resources for more detail.
 - ☐ Confirm the management network is reachable from the service provider network.
2. Install and configure your storage system. See Section 5. Storage Resources for more details.
3. Install three appropriately sized ESX Hosts with ESXi 5.0 or 5.1. Version 4.x is not supported with a vCenter installation and, as of this writing (Feb 7, 2014) ESXi 5.5 is not supported yet. Two hosts will be used for management with the third host for the Test Tenant. See the Compute Resources section in the Desktop Blueprint for more sizing details. ESX hosts must be configured with a minimum of an ESXi Standard license (do not use the free version; the free license will not work).
 - ☐ On each of the management hosts add all five of the required networks. Sample configuration can be found in section 4.5.
 - Management Network – For ESXi / vCenter
 - Service Provider Network – For the Desktop SP Appliances
 - Link Local Network – Not Routed – For all the Desktop Appliances
 - Tenant 1 Network – For the 1st Tenant Appliances and Desktops
 - Tenant 2 Network – For the 2nd Tenant Appliances and Desktops
 - ☐ On each of the management hosts add the Service Provider mount/LUN to the ESXi hosts.
 - ☐ On each tenant host add just the Management, Link Local, and Tenant networks.
4. Install and configure required network services. The Service Provider requires NTP, Active Directory and DNS services. The Test and POC Tenants will require their own Active Directory, DNS and DHCP services.
5. Assign IPs to Service Provider Nodes from the Service Provider network.
6. Service Provider AD Setup (Confirm settings with ADEplorer)
7. Assign IPs to Tenant Appliances from the Test Tenant network and POC Tenant network.

Service Provider Installation Worksheet

Appliance “SP1” Network Bootstrap

Addition to Multi-DC Setup?	Are you building a new environment or joining an existing one. Usually the answer is No for a new environment.
Datacenter name	Unique to each physical site
Linklocal backbone VLAN ID	VLAN ID number or DVS Port Profile Name (as seen in vCenter)
Linklocal backbone IP for eth1	169.254.x.x – Host IP for appliance SP1 – ALL linklocal IPs start from this one IP so leave room in the subnet for the dtRAMs (if needed)
dt linklocal backbone mask in CIDR Format (0-32)	16 (recommended for production) or 24 (ok to use in poc environments)
SP VLAN ID	VLAN ID number or DVS Port Profile Name (as seen in vCenter)
“SP1” Host IP for eth0	x.x.x.x – Actual Host IP for SP1 appliance (not the floating)
SP Network mask in CIDR Format (0-32)	
SP Network Gateway	GW of SP Network
Hostname of SP1 appliance	FQDN Needed ex: name.domain.suffix
DNS Server IP	IP of DNS Server – Just one
NTP server (one per line)	IP of NTP Servers – more than one if needed
Is this an HA Setup?	Usually Yes even if only one management host is currently available
SP Floating IP Address	Floating IP of SP Pair – only needed in HA setup
psql Database Password	(do not have to write it on sheet but please have one in mind for the install)
Password for user “desktone” – Will be used for all appliances	(do not have to write it on sheet but please have one in mind for the install)

SP Domain Bootstrap

NETBIOS name	Name of Domain - what you put before the \ when you log in - VMWARE (for example)
Domain Suffix	vmware.com
AD Protocol	ldap or ldaps
AD Protocol Port	389 or 636
Primary DNS Server IP	Usually same as table above
Context	DC=VMWARE,DC=COM
Domain Bind Account*	CN=Joe Smith,CN=Users
Domain Bind Account Pswd	password for above account
Super Admin (SC Access)	Distinguished Name w/out Context - Admin Group for SP Appliance GUI Access (Service Center). For example, CN=serviceadmins,CN=groups

* To find domain bind acct, go to server manager, then "View -> Advanced Features" to turn on the "Attribute Editor" tab. Find the user, then user properties, then go to "Attribute Editor" and find the "distinguishedName" field. That is the account name needed, minus the end DC sections that make up the domain suffix.

Management Hosts

Host	Name or IP	Management Account / Pswd	Memory Over-Allocation Ratio	CPU Over-Allocation Ratio
vCenter	IP or FQDN	Login/Pass of user that the appliances will use to connect to vCenter	NA	NA
MgtHost1	Name as seen in vC		1.0	10
MgtHost2	Name as seen in vC		1.0	10

Service Provider NetApp NFS Storage with VSC

(Only needed if storage is a NetApp and is using the VSC vCenter plugin)

Use	NetApp Name or IP *	Account / Password
Service Provider	IP or FQDN	
Tenant 1	IP or FQDN	
Tenant 2	IP or FQDN	
Tenant etc...	IP or FQDN	

* Important: When adding a storage system to the Desktone Platform, the Address field must match how the VSC plug-in was discovered for vCenter. If the plug-in 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.

Service Provider Appliance Information

Node Use	VM / Appliance Hostname	Service Provider IP
Service Provider 2	Name of VM	SP Host IP - NOT LL IP - NOT FQDN
Tenant Resource Manager 1	Name of VM	SP Host IP - NOT LL IP - NOT FQDN
Tenant Resource Manager 2	Name of VM	SP Host IP - NOT LL IP - NOT FQDN

Tenant 1 – Installation Worksheet

The following table lists the fields you will need to specify in the Service Center when installing a tenant.

Field	Values	Sample Value / Notes
Tenant VLAN ID or DVS Name		115 or Tenant-1-Net
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 /VM Name		TenantA-Node1
Primary Tenant Appliance IP Address		172.16.115.21
Secondary Tenant Appliance/VM Name		TenantA-Node2
Secondary Tenant Appliance IP Address		172.16.115.22
Floating IP Address		172.16.115.20
Tenant vCenter		DNS name or IP of host
Tenant vCenter User name		HostMgtAcct
Tenant vCenter Password		hostPsswd

Tenant Management Hosts

(vCenter info is only needed if an additional Tenant vCenter is used)

Host	Name or IP	Management Account / Pswd	Memory Over-Allocation Ratio	CPU Over-Allocation Ratio
Tenant vCenter	IP or FQDN	Login/Pass of user that the Horizon DaaS Appliances will use to connect to vCenter	NA	NA
MgtHost1	Name as seen in vC		1.5	10
MgtHost2	Name as seen in vC		1.5	10

Optionally, if you are configuring the Tenant Active Directory, you also need the following tenant info.

Field	Values	Sample Value / Notes
NETBIOS Name	Name of Tenant Domain - what you put before the \ when you log in	TENANT
Domain Suffix		tenant.com
AD Protocol	ldap or ldaps	ldap or ldaps
AD Protocol Port	389 for ldap or 636 for ldaps (or custom)	389 or 636
Context	Full context (see example)	dc=tenant,dc=com
Primary DNS Server IP	Tenant DNS Server	172.16.115.2
Domain Bind Account / Service Account *	Can be a standard domain user.	CN=Joe Smith,CN=Users
Domain Bind / Service Account Password	(do not have to write it on sheet but please have one in mind for the install)	Password for the above account
Domain Join Account	Domain Join Acct - can be standard user but needs unlimited AD join.	dtjoindomain (name only)
Domain Joint Account Password	password for above acct	Password for the above account
Super Admin Group (Tenant EC Access)	Tenant group of people who can administer the Tenant Enterprise Center	cn=T1admin,ou=groups
Tenant User Group(s)	AD Group(s) allowed to access desktops	cn=portalusers,ou=groups

* To find domain bind acct, go to server manager, then "View -> Advanced Features" to turn on the "Attribute Editor" tab. Find the user, then user properties, then go to "Attribute Editor" and find the "distinguishedName" field. That is the account name needed, minus the end DC sections that make up the domain suffix.

Optionally, if you are configuring a dtRAM, you will also need to collect the following.

Node	External IP	Tenant IPs for em0 (IPs in tenant netwk)	Link local backbone IP for em1 *	Crossover IP for em2 **
	EXTERNAL	INTERNAL	MANAGEMENT	CROSSOVER
Tenant-dtram1		A Tenant Network IP	169.254. .	192.168.1.
Tenant-dtram2		A Tenant Network IP	169.254. .	192.168.1.
dtRAM-vip1	IP to use from Internet	A Tenant Network IP		
Network Mask (CIDR)		(0-32)	16 (prod) or 24 (poc)	28
Network Gateway				
DNS Server				

* The Link Local IPs are NOT dynamically assigned to the dtRAM like the other appliances. Therefore, sufficient network space should be reserved for all the dtRAMs, keeping in mind that two IPs are needed for *each* Tenant that uses a dtRAM.

** The Crossover Link is a point-to-point link between the two dtRAM appliances for state information and failover.

Tenant 2 – Installation Worksheet

The following table lists the fields you will need to specify in the Service Center when installing a second tenant.

Field	Values	Sample Value / Notes
Tenant VLAN ID or DVS Name		115 or Tenant-2-Net
Tenant Gateway		172.18.115.1
Tenant DNS Name		172.18.115.2 (AD server)
Tenant Subnet mask		255.255.255.0
Primary Tenant Appliance /VM Name		TenantB-Node1
Primary Tenant Appliance IP Address		172.18.115.21
Secondary Tenant Appliance/VM Name		TenantB-Node2
Secondary Tenant Appliance IP Address		172.18.115.22
Floating IP Address		172.18.115.20
Tenant vCenter		DNS name or IP of host
Tenant vCenter User name		HostMgtAcct
Tenant vCenter Password		hostPsswd

Tenant Management Hosts

(vCenter info is only needed if an additional Tenant vCenter is used)

Host	Name or IP	Management Account / Pswd	Memory Over-Allocation Ratio	CPU Over-Allocation Ratio
Tenant vCenter	IP or FQDN	Login/Pass of user that the Horizon DaaS Appliances will use to connect to vCenter	NA	NA
MgtHost1	Name as seen in vC		1.5	10
MgtHost2	Name as seen in vC		1.5	10

Optionally, if you are configuring the Tenant Active Directory, you also need the following tenant info.

Field	Values	Sample Value / Notes
NETBIOS Name	Name of Tenant Domain - what you put before the \ when you log in	TENANT2
Domain Suffix		tenant2.com
AD Protocol	ldap or ldaps	ldap or ldaps
AD Protocol Port	389 for ldap or 636 for ldaps (or custom)	389 or 636
Context	Full context (see example)	dc=tenant2,dc=com
Primary DNS Server IP	Tenant DNS Server	172.18.115.2
Domain Bind Account / Service Account *	Can be a standard domain user.	CN=Joe Smith,CN=Users
Domain Bind / Service Account Password	(do not have to write it on sheet but please have one in mind for the install)	Password for the above account
Domain Join Account	Domain Join Acct - can be standard user but needs unlimited AD join.	dtjoindomain (name only)
Domain Joint Account Password	password for above acct	Password for the above account
Super Admin Group (Tenant EC Access)	Tenant group of people who can administer the Tenant Enterprise Center	cn=T2admin,ou=groups
Tenant User Group(s)	AD Group(s) allowed to access desktops	cn=portalusers,ou=groups

* To find domain bind acct, go to server manager, then "View -> Advanced Features" to turn on the "Attribute Editor" tab. Find the user, then user properties, then go to "Attribute Editor" and find the "distinguishedName" field. That is the account name needed, minus the end DC sections that make up the domain suffix.

Optionally, if you are configuring a dtRAM, you will also need to collect the following.

Node	External IP	Tenant IPs for em0 (IPs in tenant netwk)	Link local backbone IP for em1 *	Crossover IP for em2 **
	EXTERNAL	INTERNAL	MANAGEMENT	CROSSOVER
Tenant-dtram1		A Tenant Network IP	169.254. .	192.168.1.
Tenant-dtram2		A Tenant Network IP	169.254. .	192.168.1.
dtRAM-vip1	IP to use from Internet	A Tenant Network IP		
Network Mask (CIDR)		(0-32)	16 (prod) or 24 (poc)	28
Network Gateway				
DNS Server				

* The Link Local IPs are NOT dynamically assigned to the dtRAM like the other appliances. Therefore, sufficient network space should be reserved for all the dtRAMs, keeping in mind that two IPs are needed for *each* Tenant that uses a dtRAM.

** The Crossover Link is a point-to-point link between the two dtRAM appliances for state information and failover.