REVISED 6 NOVEMBER 2018

# ENVIRONMENT INFRASTRUCTURE DESIGN

vmware®

# Table of Contents

# VMware Workspace ONE Cloud-Based Reference Architecture - Environment Infrastructure Design

## Environment Infrastructure Design

Several environment resources are required to support a VMware Workspace ONE® deployment. In most cases these will already exist. It is important to ensure that minimum version requirements are met and that any specific configuration for Workspace ONE is followed. For any supporting infrastructure component that Workspace ONE depends on, that component must be designed to be scalable and highly available. Some key items are especially important when the environment is used for a multi-site deployment.

### Active Directory

Workspace ONE and VMware Horizon® Cloud Service™ on Microsoft Azure require an Active Directory domain structure for user authentication and management. Standard best practices for an Active Directory deployment must be followed to ensure that it is highly available.

Because cross-site traffic should be avoided wherever possible, configure AD sites and services so that each subnet used for desktops and services is associated with the correct site. This guarantees that lookup requests, DNS name resolution, and general use of AD are kept within a site where possible. This is especially important in terms of Microsoft Distributed File System Namespace (DFS-N) to control which specific file server users get referred to.

See *Active Directory Domain Configurations*, in the Getting Started with VMware Horizon Cloud Service on Microsoft Azure guide for details on supported Active Directory configurations and preparation steps.

Additionally, for Horizon Cloud Service on Microsoft Azure, set up dedicated organizational units (OUs) for the machine accounts for virtual desktops and RDSH servers. Consider blocking inheritance on these OUs to stop any existing GPOs from having an undesired effect.

### Group Policy

Group Policy objects (GPOs) can be used in a variety of ways to control and configure both Horizon Cloud Service on Microsoft Azure components and also standard Windows settings.

These policies are normally applied to the user or the computer Active Directory account, depending on where the objects are located in Active Directory. In a Horizon Cloud Service on Microsoft Azure environment, it is typical to set specific user policy settings for the specific Horizon Cloud Service session only when a user connects to it.

We also want to have user accounts processed separately from computer accounts with GPOs. This is where the loopback policy is widely used in any GPO that also needs to configure user settings. This is particularly important with VMware User Environment Manager™. User Environment Manager applies only user settings, so if the User Environment Manager GPOs are applied to

computer objects, loopback processing must be enabled.

Group policies can also be associated at a site level. Refer to the Microsoft Web site for details.

### DNS

The Domain Name System (DNS) is widely used in a Workspace ONE and Horizon Cloud Service on Microsoft Azure environment, from server components communication to clients and virtual desktops. Follow standard design principles for DNS, making it highly available. Additionally, ensure that:

- Forward and reverse zones are working well.
- Dynamic updates are enabled so that desktops register with DNS correctly.
- Scavenging is enabled and tuned to cope with the rapid cloning and replacement of virtual desktops.

### DHCP

In a Horizon Cloud Service on Microsoft Azure environment, desktops and RDSH servers rely on DHCP to get IP addressing information. DHCP must be allowed on the VM networks designated for these virtual desktops and RDSH servers.

Microsoft Azure has a built-in DHCP configuration that is a part of every VNet configured in Microsoft Azure. For more information, see IP Configurations in the Microsoft Azure documentation.

### Distributed File System

File shares are critical in delivering a consistent user experience. They store various types of data used to configure or apply settings that contribute to a persistent-desktop experience.

The data can include the following types:

- IT configuration data, as specified in User Environment Manager
- User settings and configuration data, which are collected by User Environment Manager
- Windows mandatory profile
- User data (documents, and more)
- ThinApp packages

The design requirement is to have no single point of failure within a site while replicating the above data types between the two data centers to ensure their availability in a site-failure scenario. This reference architecture uses Microsoft Distributed File System Namespace (DFS-N) with array-level replication.

### DFS Namespace

The namespace is the referred entry point to the distributed file system.

- A single entry point is enabled and active for profile-related shares to comply with the Microsoft support statements (for example, User Environment Manager user settings).
- Other entry points can be defined but disabled to stop user referrals to them. They can then be made active in a recovery scenario.
- Multiple active entry points are possible for shares that contain data that is read-only for end users (for example, User Environment Manager IT configuration data, Windows mandatory profile, ThinApp packages).

More detail on how DFS design applies to profile data can be found in the Component Design: User Environment Manager Architecture section of this guide.

### Certificate Authority

A Microsoft Enterprise Certificate Authority (CA) is often used for certificate-based authentication, SSO, and email protection. A certificate template is created within the Microsoft CA and is used by VMware Workspace ONE® UEM to sign certificate-signing requests (CSRs) that are issued to mobile devices through the Certificate Authority integration capabilities in Workspace ONE UEM and Active Directory Certificate Services.

The Microsoft CA can be used to create CSRs for VMware Unified Access Gateway™, VMware Identity Manager™, and any other externally facing components. The CSR is then signed by a well-known external CA to ensure that any device connecting to the environment has access to a valid root certificate.

Having a Microsoft Enterprise CA is a prerequisite for Horizon True SSO. A certificate template is created within the Microsoft CA and is used by True SSO to sign CSRs that are generated by the VM. These certificates are short-lived (approximately 1 hour) and are used solely for the purpose of single-signing a user in to a desktop through VMware Identity Manager without prompting for AD credentials.

Details on setting up a Microsoft CA can be found in the VMware Horizon Cloud Service on Microsoft Azure Administration Guide.

**Design decision:** A Microsoft Enterprise CA is set up to support certificate authentication for Windows 10 devices and to support the True SSO capability.

### Microsoft RDS Licensing

Applications published with Horizon Cloud Service on Microsoft Azure use Microsoft RDSH servers as a shared server platform to host Windows applications. Microsoft RDSH servers require licensing through a Remote Desktop Licensing service. It is critical to ensure that the Remote Desktop Licensing service is highly available within each site and also redundant across sites.

### Microsoft Key Management Service

To activate Windows (and Microsoft Office) licenses in a VDI environment, VMware recommends using Microsoft Key Management Service (KMS) with volume license keys. Because desktops are

typically deleted at logout and are recreated frequently, it is important that this service be highly available. See the Microsoft documentation on how best to deploy volume activation. It is critical to ensure that the KMS service is highly available within each site and also redundant across sites.

**Design decision**: For this reference architecture, Microsoft KMS was deployed in a highly available manner to allow desktops and RDSH servers to activate their Microsoft licenses.

### Microsoft Azure Environment Infrastructure Design

In this reference architecture, multiple Azure regional data centers were used to demonstrate multi-site deployments of Horizon Cloud Service on Microsoft Azure. We configured infrastructures in two Microsoft Azure regions (US East, US East 2) to facilitate this example.

Each region was configured with the following components.

**Table: Microsoft Azure Infrastructure Components**

| Component | Description |
|---|---|
| Management VNet | Microsoft Azure Virtual Network (VNet) configured to host shared services for use by the Horizon Cloud deployments. |
| - VNet peer (management to node) | Unidirectional network connection between two VNets in Microsoft Azure. Both the **Allow forwarded traffic** and **Allow Gateway Transit** options were selected in the VNet configuration to ensure proper connectivity between the two VNets. |
| - VNet peer (node to management) | Unidirectional network connection between two VNets in Microsoft Azure. Both the **Allow forwarded traffic** and **Allow Gateway Transit** options were selected in the VNet configuration to ensure proper connectivity between the two VNets. |
| Microsoft Azure VPN Gateway | VPN gateway resource provided by Microsoft Azure to provide point-to-point private network connectivity to another network. |
| Two Microsoft Windows Server VMs | Two Windows servers provide redundancy in each Microsoft Azure region for common network services. |
| - Active Directory domain controller | Active Directory was implemented as a service on each Windows server. Active Directory was configured according to Option 3 in Networking and Active Directory Considerations on Microsoft Azure for use with VMware Horizon Cloud Service. |
| - DNS server | DNS was implemented as a service on each Windows server. |
| - Windows DFS file share | A Windows share with DFS was enabled on each Windows server to contain the User Environment Manager profile and configuration shares. |
| Horizon Cloud control node VNet | Microsoft Azure VNet created for use of the Horizon Cloud Node. This VNet contains all infrastructure and user services components (RDSH servers, VDI desktops) provided by the Horizon Cloud node. |

We also leveraged two separate Microsoft Azure subscriptions to demonstrate that multiple nodes

could be deployed to different subscriptions and managed from the same Horizon Cloud Service with Microsoft Azure control plane.

For more detail on the design decisions that were made for Horizon Cloud node deployments, see the Component Design: Horizon Cloud Service on Microsoft Azure Architecture section of this guide.

### Network Connectivity to Microsoft Azure

You do not need to provide private access to Microsoft Azure as a part of your Horizon Cloud on Microsoft Azure deployments. The Microsoft Azure infrastructure can be provided from the Internet.

There are several methods for providing private access to infrastructure deployed to any given Microsoft Azure subscription in any given Microsoft Azure region, including by using a VPN or ExpressRoute configurations.

**Design decision:** As part of the validation for this reference architecture, we decided to leverage VPN connections from our on-premises data center to each of the two Microsoft Azure regions used for this design. This is the most typical configuration that we have seen in customer environments to date. See Connecting your on-premises network to Azure for more details on the options available to provide a private network connection to Microsoft Azure.

### Microsoft Azure Virtual Network (VNet)

In a Horizon Cloud Service on Microsoft Azure deployment, you are required to configure virtual networks (VNets) for use by the Horizon Cloud Node. You must have already created the VNet you want to use in that region in your Microsoft Azure subscription before deploying Horizon Cloud Service.

Note that DHCP is a service that is a part of a VNet configuration. For more information on how to properly configure a VNet for Horizon Cloud Service, see *Configure the Required Virtual Network in Microsoft Azure* in Getting Started with VMware Horizon Cloud Service on Microsoft Azure.

Another useful resource is the VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com