REVISED 6 NOVEMBER 2018

COMPONENT DESIGN: HORIZON CLOUD SERVICE ON MICROSOFT AZURE ARCHITECTURE

vmware®

Table of Contents

VMware Workspace ONE Cloud-Based Reference Architecture - Component Design: Horizon Cloud Service on Microsoft Azure Architecture

Component Design: Horizon Cloud Service on Microsoft Azure Architecture

Horizon® Cloud Service™ is available using a software-as-a-service (SaaS) model. This service comprises multiple software components.

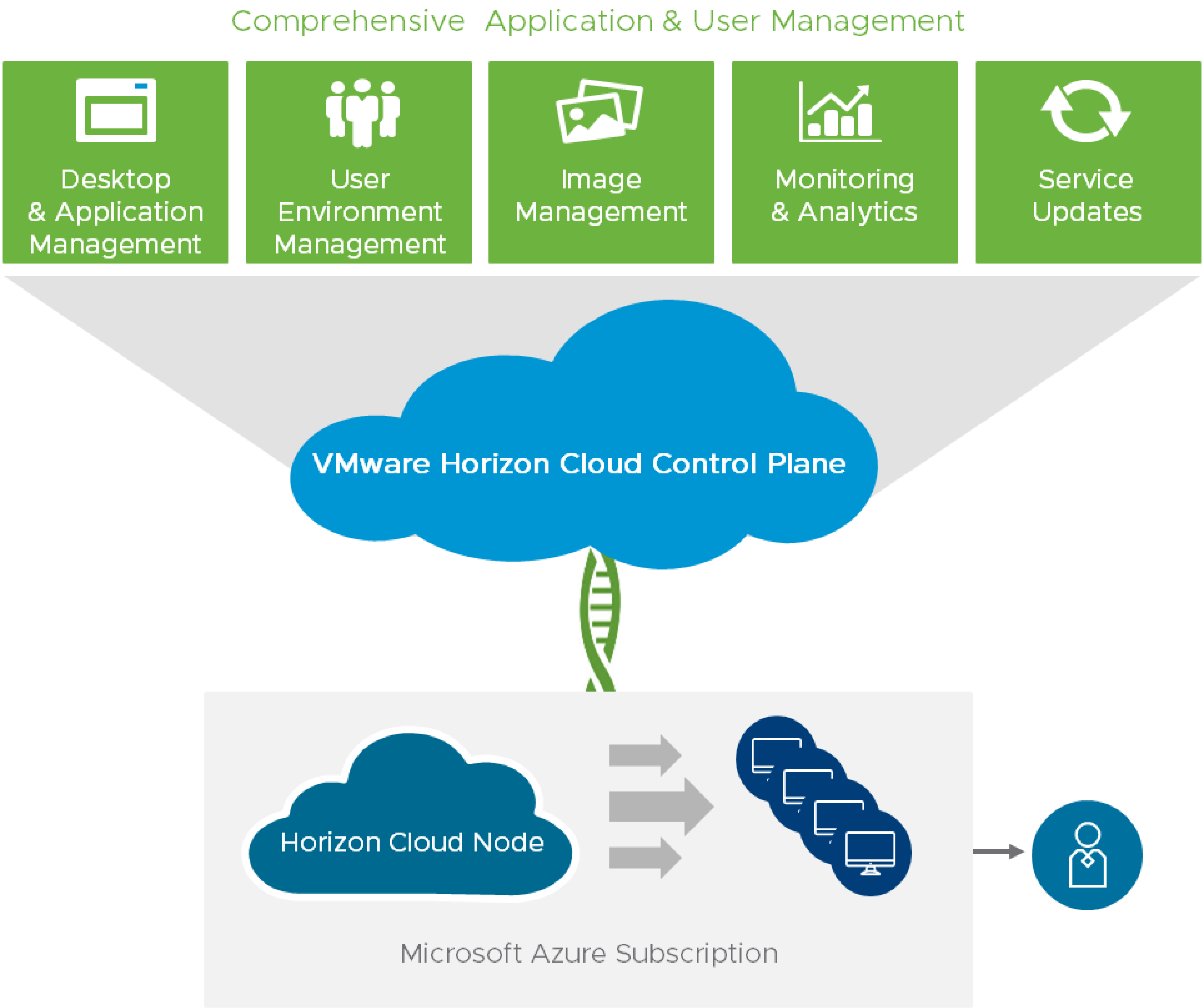
Comprehensive Application & User Management
Desktop & Application Management
User Environment Management
Image Management
Monitoring & Analytics
Service Updates
VMware Horizon Cloud Control Plane
Horizon Cloud Node
Microsoft Azure Subscription

Figure: Horizon Cloud Service on Microsoft Azure

Horizon Cloud Service provides a single cloud control plane, run by VMware, that enables the central orchestration and management of remote desktops and applications in your Microsoft Azure capacity, in the form of one or multiple subscriptions in Microsoft Azure.

VMware is responsible for hosting the Horizon Cloud Service control plane and providing feature updates and enhancements for a software-as-a-service experience. The Horizon Cloud Service is an application service that runs in multiple Amazon Web Services (AWS) regions.

The cloud control plane also hosts a common management user interface called the Horizon Cloud Administration Console, or Administration Console for short. The Administration Console runs in industry-standard browsers. It provides you with a single location for management tasks involving user assignments, virtual desktops, RDSH-published desktop sessions, and applications. This service is currently hosted in three AWS regions: United States, Germany, and Australia. The Administration Console is accessible from anywhere at any time, providing maximum flexibility.

Horizon Cloud on Microsoft Azure Deployment Overview

A successful deployment of Horizon Cloud on Microsoft Azure depends on good planning and a robust understanding of the platform. This section discusses the design options and details the design decisions that were made to satisfy the design requirements of this reference architecture.

The core elements of Horizon Cloud include**:**

- Horizon Cloud control plane
- Horizon Cloud node
- VMware Unified Access Gateway™
- Horizon Agent
- VMware Horizon® Client™

The following figure shows the high-level logical architecture of these core elements. Other components are shown for illustrative purposes.

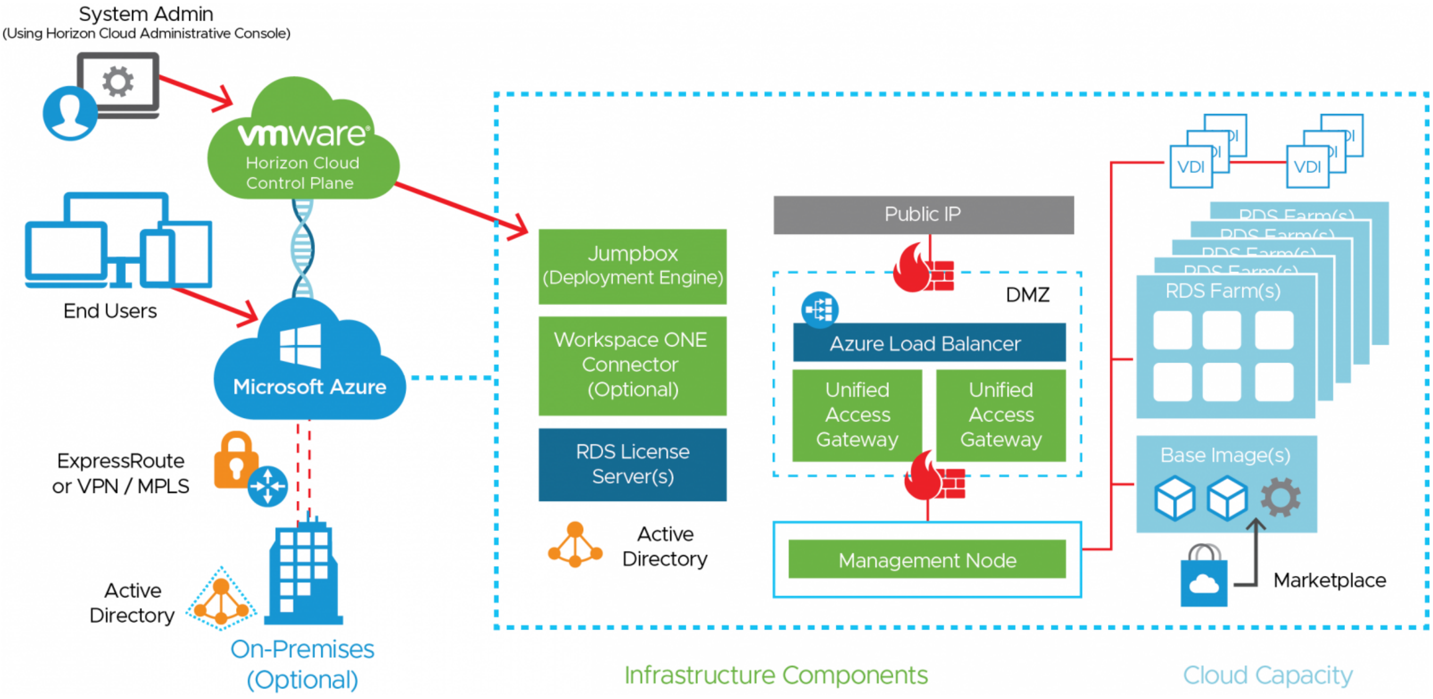

Figure: Horizon Cloud on Microsoft Azure Logical Architecture

This figure demonstrates the basic logical architecture of a Horizon Cloud Service node on your Microsoft Azure capacity.

- Your Microsoft Azure infrastructure as a service (IaaS) provides capacity.
- Your Horizon Cloud Service control plane is granted permission to create and manage resources with the use of a service principal in Microsoft Azure.
- You provide additional required components such as Active Directory, as well as optional components such as a Workspace ONE Connector or RDS license servers.
- The Horizon Cloud Service control plane initiates the deployment of the Horizon Cloud Service node, Unified Access Gateway appliances for secure remote access, and other infrastructure components that assist with the configuration and management of the Horizon Cloud Service infrastructure.
- After the Horizon Cloud Service node is deployed, you can connect the node to your own corporate AD infrastructure or create a new AD configuration in your Microsoft Azure subscription. You deploy VMs from the Microsoft Azure marketplace, which are sealed into images, and can be used in RDSH server farms.
- With the VDI functionality, you can also create Windows 10 assignments of both dedicated and floating desktops.

Horizon Cloud Service on Microsoft Azure includes the following components and features.

Table: Components of Horizon Cloud on Microsoft Azure

Component	Description
Jumpbox	The jumpbox is a temporary Linux-based VM used during environment buildout and for subsequent environment updates and upgrades. One jumpbox is required per Azure node only during platform buildout and upgrades.
Management node	The management node appliance provides access for administrators and users to operate and consume the platform. One management node appliance is constantly powered on; a second is required during upgrades.
Horizon Cloud control plane	This cloud-based control plane is the central location for conducting all administrative functions and policy management. From the control plane, you can manage your virtual desktops and RDSH server farms and assign applications and desktops to users and groups from any browser on any machine with an Internet connection. The cloud control plane provides access to manage all Horizon Cloud nodes deployed to your Microsoft Azure infrastructure in a single, centralized user interface, no matter which regional data center you use.
Horizon Cloud Administration Console	This component of the control plane is the web-based UI that administrators use to provision and manage Horizon Cloud desktops and applications, resource entitlements, and VM images. The Horizon Cloud Administration Console provides full life-cycle management of desktops and Remote Desktop Session Host (RDSH) servers through a single, easy-to-use web-based console. Organizations can securely provision and manage desktop models and entitlements, as well as native and remote applications, through this console. The console also provides usage and activity reports for various user, administrative, and capacity-management activities.
Horizon Agent	This software service, installed on the guest OS of all virtual desktops and RDSH servers, allows them to be managed by Horizon Cloud nodes.
Horizon Client	This software, installed on the client device, allows a physical device to access a virtual desktop or RDSH-published application in a Horizon deployment. You can optionally use an HTML client on devices for which installing software is not possible.
Unified Access Gateway	This gateway is a hardened Linux virtual appliance that allows for secure remote access to the Horizon Cloud environment. This appliance is part of the Security Zone (for external Horizon Cloud access) and the Services Zone (for internal Horizon Cloud access). The Unified Access Gateway appliances deployed as a Horizon Cloud node are load balanced by an automatically deployed and configured Microsoft Azure load balancer. The design decisions for load balancing within a node are already made for you.
RDSH servers	These Windows Server VMs provide published applications and session-based remote desktops to end users.

Scalability and Availability

When creating your design, keep in mind that you want an environment that can scale up when necessary, and also remain highly available. Design decisions need to be made with respect to some Microsoft Azure limitations, and with respect to some Horizon Cloud limitations.

Configuration Maximums for Horizon Cloud Service

Horizon Cloud on Microsoft Azure has certain configuration maximums you must take into account when making design decisions:

- Up to 2,000 concurrent active connections are supported per Horizon Cloud node.
- Up to 2,000 desktop and RDSH server VMs are supported per Horizon Cloud node.
- Up to 2,000 desktop and RDSH server VMs are supported per Microsoft Azure region or subscription.

To handle larger user environments, you can deploy multiple Horizon Cloud nodes, but take care to follow the accepted guidelines for segregating the nodes from each other. For example, under some circumstances, you might deploy a single node in two different Microsoft Azure regions, or you might be able to deploy two nodes in the same subscription in the same region as long as the IP address space is large enough to handle multiple deployments.

For more information, see *VMware Horizon Cloud Service on Microsoft Azure Service Limits* in the Getting Started with VMware Horizon Cloud Service on Microsoft Azure document. For information about creating subnets and address spaces, see *Configure the Required Virtual Network in Microsoft Azure* in Getting Started with VMware Horizon Cloud Service on Microsoft Azure.

Design decision: As part of the validation for this reference architecture, we deployed an environment capable of scaling to 6,000 concurrent connections or users. To meet this requirement, we deployed three Horizon Cloud nodes.

Configuration Maximums for Microsoft Azure Subscriptions

Horizon Cloud on Microsoft Azure leverages Microsoft Azure infrastructure to deliver desktops and applications to end users. Each Microsoft Azure region can have different infrastructure capabilities. You can leverage multiple Microsoft Azure regions for your infrastructure needs.

A Microsoft Azure region is a set of data centers deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network.

These deployments are a part of your Microsoft Azure subscription or subscriptions. A subscription is a logical segregation of Microsoft Azure capacity that you are responsible for. You can have multiple Microsoft Azure subscriptions as a part of the organization defined for you in Microsoft Azure.

A Microsoft Azure subscription is an agreement with Microsoft to use one or more Microsoft cloud platforms or services, for which charges accrue based either on a per-user license fee or on cloud-based resource consumption. For more information on Microsoft Azure subscriptions, see Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings.

Some of the limitations for individual Microsoft Azure subscriptions might impact designs for larger Horizon Cloud on Microsoft Azure deployments. For details about Microsoft Azure subscription limitations, see Azure subscription and service limits, quotas, and constraints.

Design decision: As part of the validation for this reference architecture, we deployed an environment capable of scaling to 6,000 concurrent connections or users. Each session involved a VDI desktop with 2 vCPUs (or cores), making a total requirement of 12,000 vCPUs. Microsoft Azure has a maximum of 10,000 vCPUs that can be allotted for any given Microsoft Azure subscription per region. Because our requirement for 12,000 vCPUs exceeds the maximum number of vCPUs allowed per subscription, we used multiple Microsoft Azure subscriptions.

If you plan to deploy 2,000 concurrent VDI user sessions in a single deployment of Horizon Cloud on Microsoft Azure, consider the VM configurations you require. If necessary, you can leverage multiple Microsoft Azure subscriptions for a Horizon Cloud on Microsoft Azure deployment. Note that you might also need to request increases in quota allotment for your subscription in any given Microsoft Azure region to accommodate your design.

Other Design Considerations

Several cloud- and SaaS-based components are included in a Horizon Cloud on Microsoft Azure deployment. The operation and design of these services are considered beyond the scope of this reference architecture because it is assumed that no design decisions you make will impact the nature of the services themselves. Microsoft publishes a Service Level Agreement for individual components and services provided by Microsoft Azure.

Horizon Cloud on Microsoft Azure uses Azure availability sets for some components included in the Horizon Cloud node—specifically for the two Unified Access Gateways that are deployed as a part of any Internet-enabled deployment.

You can manually build and configure Horizon Cloud nodes to provide applications and desktops in the event that you have an issue accessing a Microsoft Azure regional data center. Microsoft has suggestions for candidate regions for disaster recovery. See Business continuity and disaster recovery (BCDR): Azure Paired Regions.

As was mentioned previously, Horizon Cloud on Microsoft Azure has no built-in functionality to handle business continuity or regional availability issues. In addition, the Microsoft Azure services and features regarding availability are not supported by Horizon Cloud on Microsoft Azure.

Multi-site Design

You can deploy Horizon Cloud nodes to multiple Microsoft Azure regions and manage them all through the Horizon Cloud Administration Console. Each Horizon Cloud node is a separate entity and is managed individually. VM master images, assignments, and users must all be managed within each node. No cross-node entitlement or resource sharing is available. For this reference architecture, we deployed three Horizon Cloud nodes to Microsoft Azure.

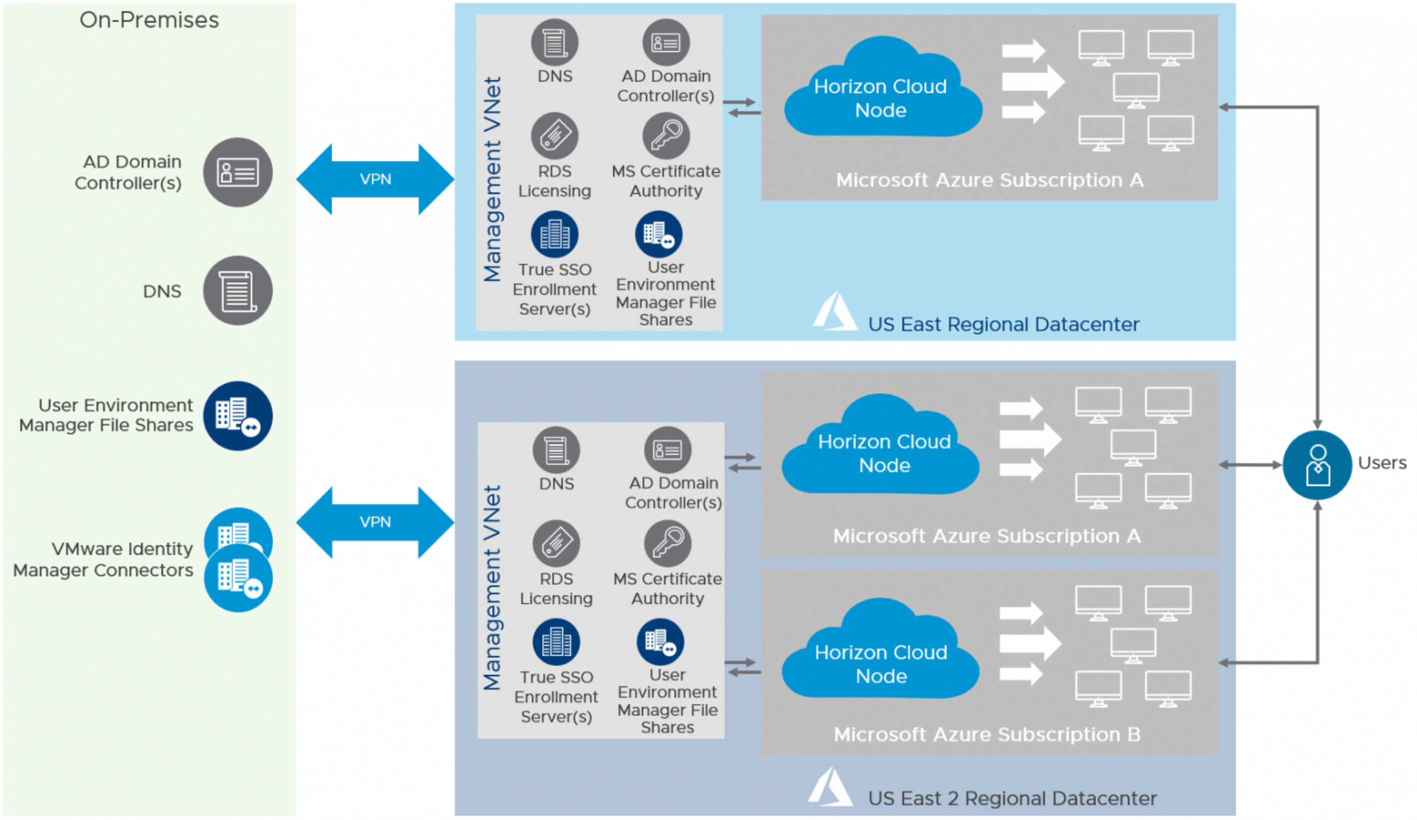
On-Premises
AD Domain Controller(s)
DNS
User Environment Manager File Shares
VMware Identity Manager Connectors
VPN
VPN
Management VNet
DNS
AD Domain Controller(s)
RDS Licensing
MS Certificate Authority
True SSO Enrollment Server(s)
User Environment Manager File Shares
Horizon Cloud Node
Microsoft Azure Subscription A
US East Regional Datacenter
Management VNet
DNS
AD Domain Controller(s)
RDS Licensing
MS Certificate Authority
True SSO Enrollment Server(s)
User Environment Manager File Shares
Horizon Cloud Node
Microsoft Azure Subscription A
Horizon Cloud Node
Microsoft Azure Subscription B
US East 2 Regional Datacenter
Users

Figure: Logical Diagram Showing Horizon Cloud on Microsoft Azure Node Deployments

We deployed two nodes to the US East Region of Microsoft Azure in different subscriptions. Although the same Microsoft Azure subscription could have been leveraged due to the small-scale tests that we were performing, we decided that using multiple subscriptions would be a common and valid architectural decision.

Note that a Split-horizon DNS configuration might be required for a multi-site deployment, depending on how you want your users to access the Horizon Cloud on Microsoft Azure environment.

Entitlement to Multiple Nodes

You can manually spread users across multiple Horizon Cloud on Microsoft Azure nodes. However, each Horizon Cloud node is managed individually and there is no way to cross-entitle users to multiple nodes. Although the same user interface is used to manage multiple Horizon Cloud nodes, you must deploy separate VM images, RDSH server farms, and assignments on each node individually.

You can mask this complexity from a user’s point of view by implementing VMware Identity Manager™ so that end users must use VMware Workspace ONE® to access resources. For example, you could entitle different user groups to have exclusive access to different Horizon Cloud on Microsoft Azure deployments, and then join each node to the same Active Directory. Note that although the method would work, there is currently no product support for automatically balancing user workloads across Horizon Cloud nodes.

External Access

You can configure each node to provide access to desktops and applications for end users located outside of your corporate network. By default, Horizon Cloud nodes allow users to access the Horizon Cloud environment from the Internet. When the node is deployed with this ability configured, the node includes a load balancer and Unified Access Gateway instances to enable this access.

If you do not select **Internet Enabled Desktops** for your deployment, clients must connect directly to the node and not through Unified Access Gateway. In this case, you must perform some post-deployment steps to create the proper internal network routing rules so that users on your corporate network have access to your Horizon Cloud environment.

If you decide to implement Horizon Cloud on Microsoft Azure so that only internal connections are allowed, you will need to configure your DNS correctly with a Split-horizon DNS configuration.

Optional Components for a Horizon Cloud on Microsoft Azure Deployment

You can implement optional components to provide additional functionality and integration with other VMware products:

- **True SSO enrolment server** – Deploy a True SSO enrolment server to integrate with VMware Identity Manager and enable single-sign-on features in your deployment. Users will be automatically logged in to their Windows desktop when they open a desktop from the Workspace ONE user interface.
- **VMware Identity Manager** – Implement and integrate the deployment with VMware Identity Manager so that end users can access all their apps and virtual desktops from a single unified catalog.
- **VMware User Environment Manager™** – Leverage User Environment Manager to provide a wide range of capabilities such as personalization of Windows and applications, contextual policies for enhanced user experience, and privilege elevation so that users can install applications without having administrator privileges.

Shared Services Prerequisites

The following shared services are required for a successful implementation of Horizon Cloud on Microsoft Azure deployment:

- **DNS** – DNS is used to provide name resolution for both internal and external computer names. See *Configure the Virtual Network's DNS Server* in Getting Started with VMware Horizon Cloud Service on Microsoft Azure.
- **Active Directory** – There are multiple configurations you can use for an Active Directory deployment. You can choose to host Active Directory completely on-premises, completely in Microsoft Azure, or in a hybrid (on-premises and in Microsoft Azure) deployment of Active Directory for Horizon Cloud on Microsoft Azure. For supported configurations, see *Active Directory Domain Configurations* in the in Getting Started with VMware Horizon Cloud Service on Microsoft

Azure.

- **RDS licensing** – For connections to RDSH servers, each user and device requires a Client Access License assigned to it. RDS licensing infrastructure can be deployed either on-premises or in a Microsoft Azure region based on your organization's needs. For details, see *License your RDS deployment with client access licenses (CALs)*.
- **DHCP** – In a Horizon environment, desktops and RDSH servers rely on DHCP to get IP addressing information. Microsoft Azure provides DHCP services as a part of the platform. You do not need to set up a separate DHCP service for Horizon Cloud Service on Microsoft Azure. For information on how DHCP works in Microsoft Azure, see *Address Types* in *Add, change, or remove IP addresses for an Azure network interface*.
- **Certificate services** – The Unified Access Gateway capability in your node requires SSL/TLS for client connections. To serve Internet-enabled desktops and published applications, the node deployment wizard requires a PEM-format file. This file provides the SSL/TLS server certificate chain to the node's Unified Access Gateway configuration. The single PEM file must contain the entire certificate chain, including the SSL/TLS server certificate, any necessary intermediate CA certificates, the root CA certificate, and the private key.

  For additional details about certificate types used in Unified Access Gateway, see *Selecting the Correct Certificate Type* in Deploying and Configuring VMware Unified Access Gateway. Also see the Environment Infrastructure Design section of this guide for details on how certificates impact your Horizon Cloud on Microsoft Azure deployment.

Authentication

One of the methods of accessing Horizon desktops and applications is through VMware Identity Manager. This requires integration between the Horizon Cloud Service and VMware Identity Manager using the SAML 2.0 standard to establish mutual trust, which is essential for single sign-on (SSO) functionality.

- When SSO is enabled, users who log in to VMware Identity Manager with Active Directory credentials can launch remote desktops and applications without having to go through a second login procedure when they access a Horizon desktop or application.
- When users are authenticating to VMware Identity Manager and using authentication mechanisms other than AD credentials, True SSO can be used to provide SSO to Horizon resources for the users.

For details, see *Integrate a Horizon Cloud Node with a VMware Identity Manager Environment* and see *Configure True SSO for Use with Your Horizon Cloud Environment* in the VMware Horizon Cloud Service on Microsoft Azure Administration Guide.

Design decision: For this reference architecture, the Horizon Cloud Service on Microsoft Azure nodes were integrated into a cloud-hosted instance of VMware Identity Manager. For more detail, see the Platform Integration section of this guide.

True SSO

Many user authentication options are available for logging in to VMware Identity Manager or Workspace ONE. Active Directory credentials are only one of these many authentication options. Ordinarily, using anything other than AD credentials would prevent a user from being able to SSO to a Horizon virtual desktop or published application through Horizon Cloud on Microsoft Azure. After selecting the desktop or published application from the catalog, the user would be prompted to authenticate again, this time with AD credentials.

True SSO provides users with SSO to Horizon Cloud on Microsoft Azure desktops and applications regardless of the authentication mechanism used. True SSO uses SAML, where Workspace ONE is the Identity Provider (IdP) and the Horizon Cloud node is the Service Provider (SP). True SSO generates unique, short-lived certificates to manage the login process. This enhances security because no passwords are transferred within the data center.

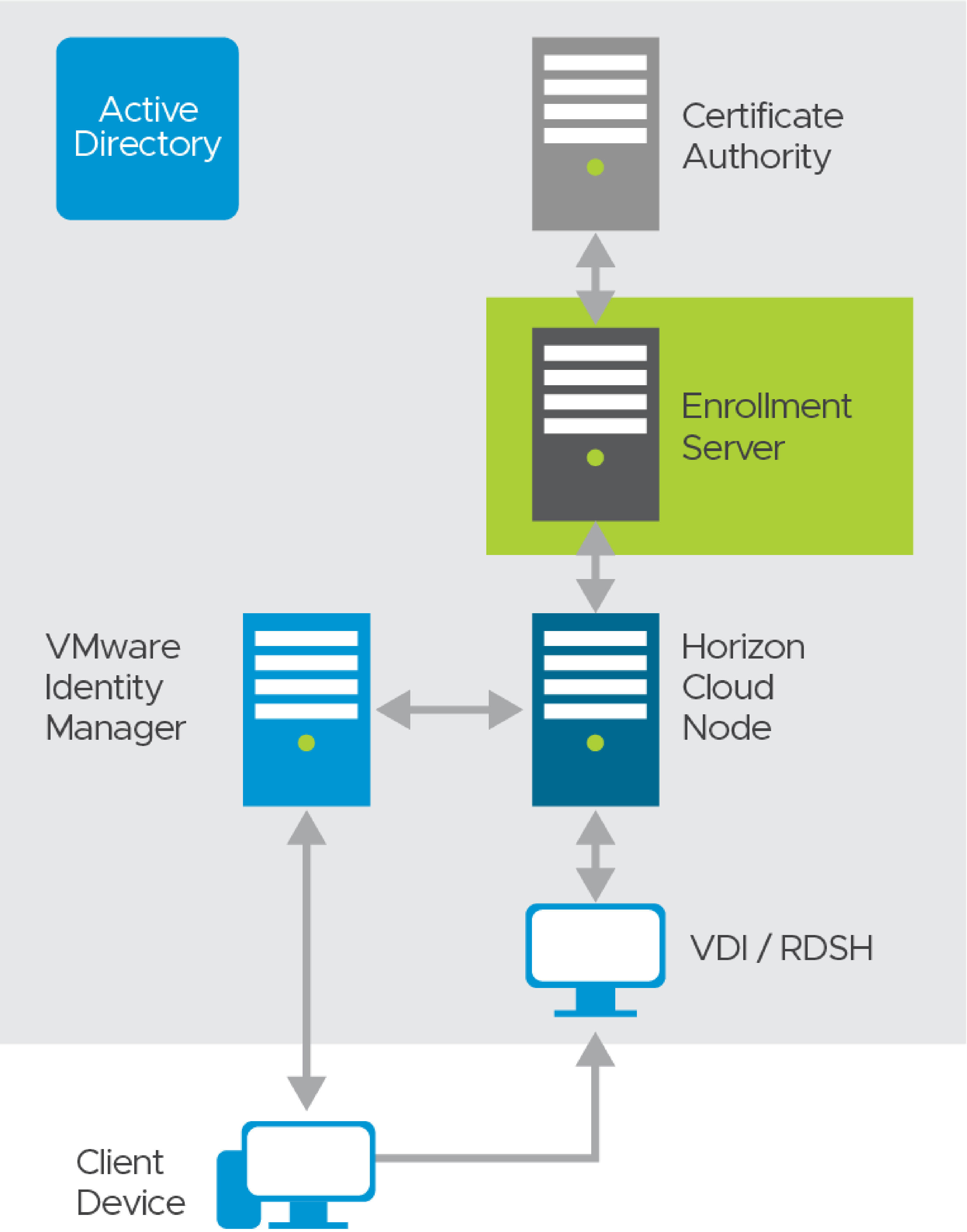
Active Directory
Certificate Authority
Enrollment Server
VMware Identity Manager
Horizon Cloud Node
VDI / RDSH
Client Device

Figure: True SSO Overview

True SSO requires a new service—the enrollment server—to be installed. You can install this component by following the steps in *Set up the Enrollment Server* in the VMware Horizon Cloud Service on Microsoft Azure Administration Guide.

Design Overview

For True SSO to function, several components must be installed and configured within the environment. This section discusses the design options and details the design decisions that satisfy the requirements.

Note: For more information on how to install and configure True SSO, see *Configure True SSO for Use with Your Horizon Cloud Environment* in the VMware Horizon Cloud Service on Microsoft Azure Administration Guide.

Enrollment Server

The enrollment server is responsible for receiving certificate-signing requests from the Connection Server and passing them to the Certificate Authority to sign using the relevant certificate template. The enrollment server is a lightweight service that can be installed on a dedicated Windows Server 2016 VM, or it can run on the same server as the MS Certificate Authority service .

A single enrollment server can easily handle all the requests from a single pod. However, to satisfy the requirements that the proposed solution be robust and able to handle failure, deploy *n*+1 enrollment servers.

Design decision: For this reference architecture, two enrollment servers were deployed to the same Microsoft Azure region to satisfy the requirements of handling 2,000 sessions and providing high availability. Each enrollment server was hosted on a dedicated Windows Server 2016 VM.

Two enrollment servers were deployed in the environment, and the Horizon Cloud node was configured to communicate with both enrollment servers. The enrollment servers can also be configured to communicate with two Certificate Authorities. By default, the enrollment servers use the Active / Failover method of load balancing.

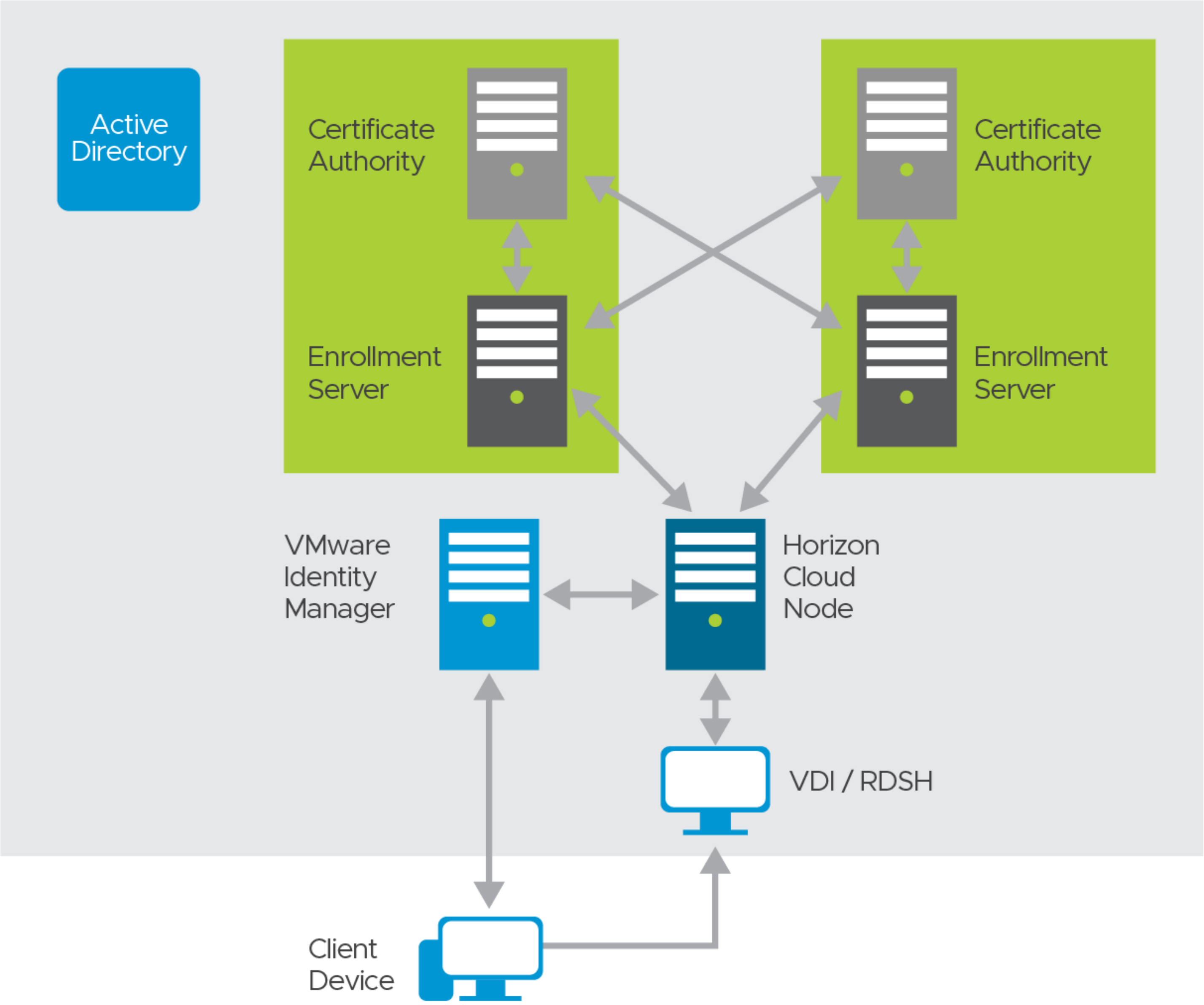

Figure: True SSO Availability and Redundancy

Design decision: For this reference architecture, the default mode of Active / Failover was sufficient to meet the requirements.

The enrollment servers should reside within the same Microsoft Azure region as the Horizon Cloud node.

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