Healthcare on Azure VMware Solution

VMware Architecture

Table of contents

Healthcare on Azure VMware Solution

Executive Summary

Over the past few years, it has been made clear that hospitals are critical ecosystems that support their local communities. Unfortunately, during this time it has also made them targets for ransomware and strained their already burdened IT staff. The ability to seamlessly migrate life-critical workloads to the cloud has become paramount. With operational risks such as ransomware and limited IT staff, cloud is not only appealing but is becoming a necessity for hospital IT environments. While some stakeholders may have doubts about the cloud and its capabilities, the reality is that many government entities provide their communities with cloud-based services that are deemed as life-critical. With that in mind, cloud adoption can be tiered in a systematic approach, by leveraging the existing application model and migrating secondary or tertiary workloads. Migrating healthcare workloads to Azure VMware Solution can address these issues.

Audience and Purpose

This reference architecture is intended for customers, IT architects, consultants, and administrators involved in the early phases of planning, design, and deployment of Electronic Health Record (EHR) solutions using Azure VMware Solution. It is assumed that the reader is familiar with the concepts and operations of VMware vSphere® and Epic. This document is high-level design guidance for the Epic EHR and Azure VMware Solution. This document does not cover Operational Database and Analytic Database on Azure VMware Solution.

Azure VMware Solution

Azure VMware Solution is a first-party Microsoft service that delivers the VMware Software-Defined Data Center (SDDC) stack as a managed service—sold, operated, and supported by Microsoft—running natively on bare-metal infrastructure in the Microsoft Azure Cloud. Azure VMware Solution is a VMware Cloud Verified platform that offers vSphere, VMware vSAN™, and VMware NSX-T™, while being seamlessly integrated into Microsoft Azure infrastructure and management tools. With Azure VMware Solution, you can modernize your infrastructure by seamlessly moving vSphere-based workloads directly to Microsoft Azure without application changes. Because Azure VMware Solution uses the same VMware SDDC components you use on-premises, you can leverage the same skills and tools you use every day to build an elastic, hybrid, and scalable platform for your existing or new vSphere applications.

The Compelling Economics of Azure VMware Solution

While there are other cloud offerings, Azure VMware Solution provides a path to the cloud with a unique set of features. It also provides additional value to organizations looking to make the jump to the cloud while addressing the needs of different stakeholders in the organization.

Lower cost for Microsoft applications for business owners:

- Free extended security updates for Windows and SQL Server 2008 and 2012
- Support for Microsoft 365 in VMware Horizon® virtual desktop environments
- Bring and use existing on-premises Windows and SQL Server licenses with Azure Hybrid Benefit

Simplify multi-environment operations for IT administration teams:

- Unified consumption, licensing, and billing with other Azure services
- Support for Azure Resource Manager automation templates
- Events, alerts, and logs exposed in both environments

Deliver modern applications in optimized environments for developers:

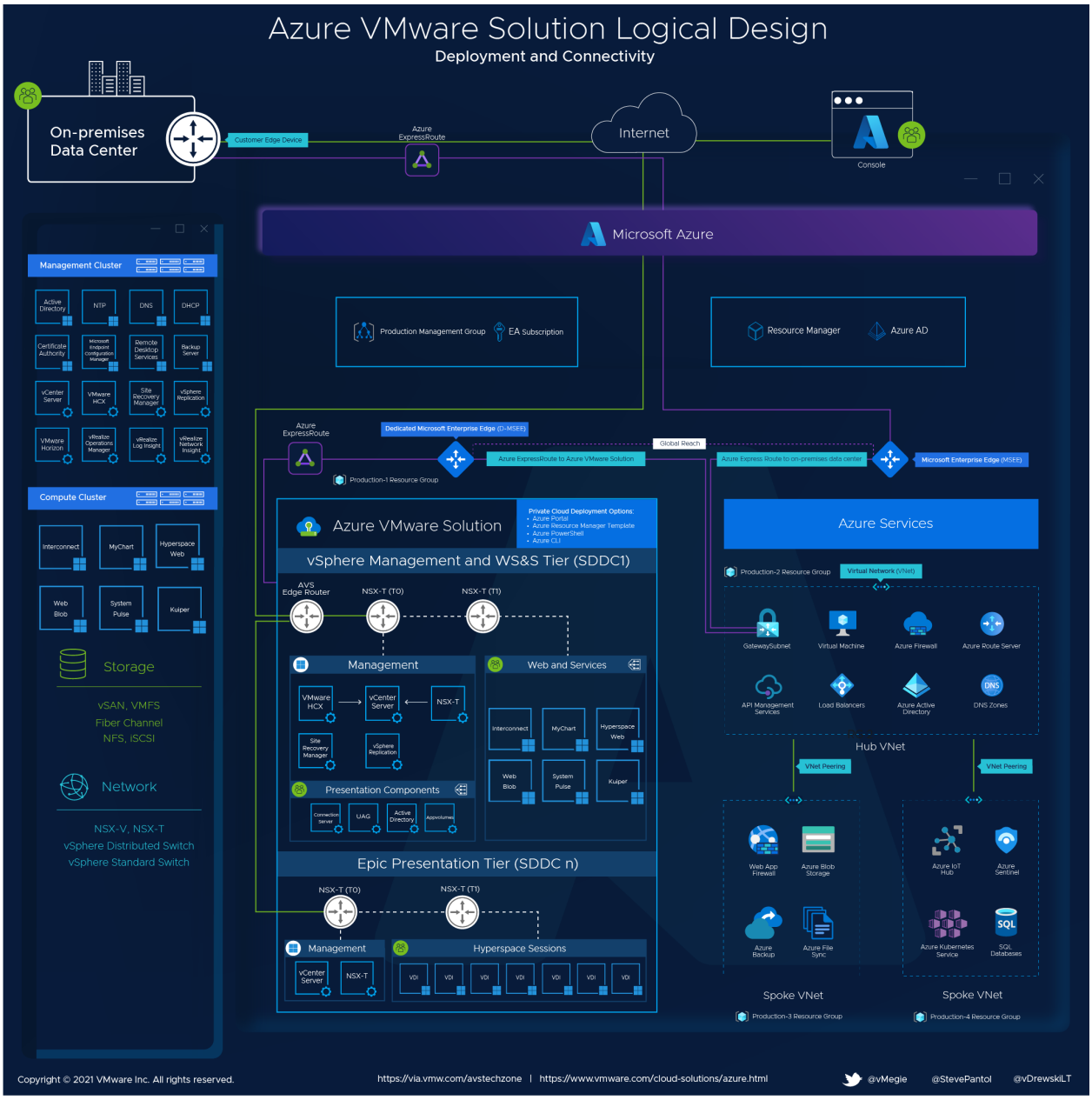
- Seamless access to Azure's market-leading PaaS services
- Integration of VMware SDDC management into Azure portal
- Unified permissions and access control across both environments
- Deploy cloud-native applications on the VMware Tanzu® enterprise-grade Kubernetes platform on Azure VMware Solution

Solution Deployment

Overview

Azure VMware Solution delivers VMware-based private clouds in Azure. The private cloud hardware and software deployments are fully integrated and automated in Azure. The cloud is deployed and managed through the Azure portal, CLI, or PowerShell. The diagram below illustrates a private cloud within its own Azure Resource Group, with adjacent connectivity to various native Azure services located in another resource group. The private cloud is hosted on VMware vSphere clusters with vSAN storage, managed by VMware vCenter®, utilizing NSX-T for network connectivity. NSX-T network traffic is routed to an AVS Top of Rack switch then to Microsoft Edges and out to other Azure services, the internet, or even on-premises.

Healthcare workloads such as Epic require sizing and configuration guidance; refer to your Epic Hardware and Configuration Guide. In the example architecture below the Web and Services and Presentation tiers can be either migrated to Azure VMware Solution using VMware HCX® or they can be hosted in a workload augmentation scenario such as disaster recovery or increased demand. For the Database in production, it is highly recommended to work with your Epic TSE and VMware to ensure the success of your deployment.



General AVS Architecture Recommendations

Discovery and analysis of the existing environment are necessary to determine the appropriate number of hosts and clusters

needed in the AVS private cloud. It is required to determine the aggregate resource demands of the workloads you intend to deploy in the AVS private cloud. Storage capacity will also need to be considered—to remain eligible for the AVS SLA, a cluster must not exceed 75% consumption of usable disk space. Storage policies (RAID-1, RAID-5, RAID-6) will factor into usable storage calculations and impact the required host count. The cluster can be scaled up and down as needed.

Tools such as vRealize Operations Manager and vRealize Operations Cloud can be used to analyze current resource allocation and demand, make re-sizing recommendations, and forecast the number of AVS hosts needed to support migration.

Each cluster requires a minimum of three hosts and supports a maximum of 16 hosts. Keep this in mind during sizing calculations and, if necessary, create multiple clusters to account for scalability if there is a plan to use the maximum number of hosts.

Leverage the Epic Hardware Configuration Guide for virtual machine sizing. Use the same configuration per VM as mentioned in the guide.

AVS36 host type configuration:

- Two Intel 18-core, 2.3 GHz, processors
- 576 GB RAM
- Two dual-port 25GbE network adapters, configured as two vmnics for ESXi system traffic and two vmnics for workload traffic
- Two 1.6 TB NVMe storage devices and eight 1.92 TB SSDs, organized into two vSAN disk groups with a 3.2 TB NVMe cache tier and a 15.2 TB capacity tier

This server configuration may be different than the physical servers mentioned in the Epic Hardware Configuration Guide.

Cluster Configuration

An AVS private cloud will start with a single cluster with 3-16 hosts. Up to 12 clusters can be created in each AVS private cloud, with up to 96 hosts distributed between those clusters. All AVS management VMs, including vCenter, NSX Manager, and HCX components will be placed on the first cluster.

Storage Configuration

AVS uses vSAN as the core storage. For the Epic presentation and web and services tiers, it is recommended to use RAID 5/6. Leverage RAID 1 for database VMs where needed such as Temp and Log VMDKs. Storage Policy Based Management options are dependent on the number of hosts available to the cluster.

Please refer to the vSAN design guide for vSAN storage policy configuration scenarios.

Connectivity Providers

You should choose the best ExpressRoute providers for your location. Otherwise, you risk losing access to Azure resources completely due to a single provider's failure.

ExpressRoute Circuit

Check that your organization meets the ExpressRoute prerequisite requirements to connect to Azure. Selection of the ExpressRoute Virtual Network Gateways will determine the action max linked private clouds. ExpressRoute Global Reach can be used to link two ExpressRoute connections. One connection should come from each organizational data center.

Traffic Manager Configuration

Traffic Manager can be configured to use priority routing. Traffic Manager will send all requests to the primary area unless it becomes impossible to reach the primary region. In that case, it will fail and move to an alternate region. See the Traffic Manager Routing Methods article for more information.

Traffic Manager allows you to create a health probe for each endpoint. This reference architecture provides additional details for each application that leverages Traffic Manager.

It is recommended to conduct an operational readiness test before falling back to your primary region. This includes ensuring that all VMs are correctly configured and that the subsystems of the applications are in good health. When you are ready for your primary region to become active again, perform a manual failback.

Azure Regions and Availability Zones

Business continuity is a continuum. Different failure scenarios can lead to different recovery point objectives (RPOs) or recovery time objectives (RTOs). This section contains Azure-specific advice for mitigating, preventing, and recovering from various failure

situations. These recommendations should be used together with those in the Azure Business Continuity Technical Solutions Guide. It focuses on considerations for both on-premises and self-hosted environments.

Note: Not all Azure Regions offer Azure VMware Solution. If high availability is a requirement, use more than one available Azure Region.

Recommendation:

- Host failure: Scale up the presentation or web workloads to ensure that one host failure does not impact the overall tier(s).
- Region and Availability Zone failure: Currently, Microsoft allows regional deployments of AVS without the ability to target specific Availability Zones. It is recommended to deploy different clusters in different regions and control the distribution of traffic using Azure Traffic Manager. Control of VDI session distribution can also be controlled via Cloud Pod Architecture in Horizon.

Load Balancer Strategy

This section covers the general load-balancing strategy for Epic on Azure:

- Traffic Manager: Azure Traffic Manager allows you to route client requests for services such as MyChart and EpicCare Link, Healthy Planet Link and Care Everywhere over the public internet to your primary region of Azure VMware Solutions resources which host these workloads.
- ExpressRoute: Send client requests directly from your private network via Azure ExpressRoute. This is done through the ExpressRoute Gateway to the Shared Infrastructure Vet. Global Reach connects the Azure VMware Solution networking to Azure Native Services and back to your private network Load balancer. You can use your third-party load-balancing solution to create virtual IP addresses. ExpressRoute allows you to connect with other networks.

Recommendations

To provide high availability for Epic's web and service tiers of Epic on Azure, you can use a third-party load balancer.

You should be familiar with the vendor and have established support relationships. Choose a load balancer that is large enough to handle the network's peak throughput needs. To properly size load balancers for Azure deployments, work with Microsoft and your load-balancing vendor. A centralized load balancing control plane will be key to efficient management of the load balancing infrastructure and appliances.

Install load balancers within the Management Subnet of the Primary Region’s Vet. Similar work should be done within the Azure VMware Solution SDDC environments that host the Web and Services, VDI presentation, and general workload tiers. Utilize load balancing solutions with cookie-based session affinity.

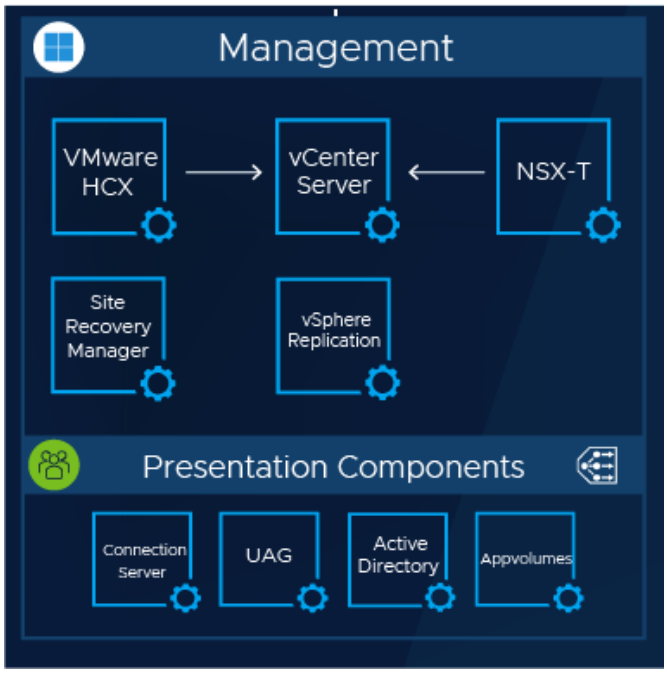
Load balancing is a critical element of the environment. All load-balanced applications will fail if there is a loss in load balancing. These are the failure scenarios to consider when assessing a load-balancing solution:

- Load Balancer Appliance failure: Chose a load balancer solution with high-availability capability. Consider stateful session routing and recovery of session services in a failure scenario.
- Availability Zone failure: Make sure you use all three availability areas in your primary Azure area to protect against a single availability-zone failure causing load balancer failures in the entire region.
- Primary Region failure: In a primary region failure, the availability of other regions is temporarily lost until failover cutover occurs. Deployment of the load balancing solution to support production loads in this alternate region is key to a successful cutover.

Management Cluster Infrastructure

This section focuses on strategies and guidance when implementing shared infrastructure services in Azure VMware solution. The shared services are required for Epic and supplemental services within the environment. VMware HCX and NSX-T provide network extensibility in a lift-and-shift scenario. We will be focusing on extending and adding services to create a hybrid environment.

The Infrastructure Management Cluster is comprised of the following components:



VMware Infrastructure Control Plane

- VMware vCenter
- VMware NSX-T Managers
- VMware Hybrid Cloud Extension (HCX)
- VMware Site Recovery Manager (SRM)
- VMware vSphere Replication

VMware Horizon VDI Presentation Control Plane

- VMware Horizon Unified Access Gateways
- VMware Horizon Connection Servers
- VMware Horizon AppVolumes Servers

Microsoft Services

- Microsoft Active Directory w/ DNS & NTP Services
- MS AD Certificate Services (or 3rd Party Certificate Authority)

Extend Active Directory, DNS, Certificate Authority Services

Refer to the design guidelines provided by the third-party Certificate Authority vendor to enable high availability throughout the hybrid environment.

Refer to Microsoft Server and Active Directory guidance for proper design and extension of the Active Directory infrastructure. Below are the high-level functions that will need to take place to extend the Domain Controller services to AVS:

- The existing customer domain stays on-premises as the authoritative source for the identity for domain.com.
- Create an additional set of Active Directory Domain Controllers (DCs) on the Azure VMware Solution infrastructure. Create a dedicated overlay network to land the AD services within NSX-T.
- The new Active Directory VMs should mirror the configuration of services of the on-prem AD Domain Controllers where applicable. It is recommended to deploy with Microsoft DNS options to simplify the integrations that exist between AD and DNS.
- Join the existing domain. The Active Directory services will start establishing a sync between on-prem Active Directory Domain Controllers and the new Active Directory DCs VM on AVS.
- The Certificate Authority (CA) service within AD can be used as a third-party Certificate Authority product within the enterprise environment.

- DNS forwarding needs to occur for unresolved queries to Azure DNS. Optional DNS configuration back to on-premises and the AVS DC is recommended.
- Active Directory is used in the Hyperspace layer for presentation.

Deploy Horizon Infrastructure Servers

The Web and Services figure below assumes the use of Horizon VDI Management for the Presentation Tier.

Horizon Cloud Pod Architecture (CPA) is the design that will allow for a hybrid landing zone both on-premises and in the AVS infrastructure. CPA pods are deployed in separate SDDCs, which allows for their own resource pools. The Hyperspace design can be active/active, active/passive, or hybrid. The design should consider high availability and multi-AZ where applicable.

Please refer to the Horizon Cloud Pod Architecture documentation for more information.

Ensure VDI control layers are in place in each of the Availability Zones and Data Center Clouds.

Separate AVS SDDCs should be deployed for simplified management of the Presentation Tiers. Infrastructure management, RBAC, and security posture are key topics when multiple teams provide high touch within the environment.

Create a dedicated network overlay for the VDI management components

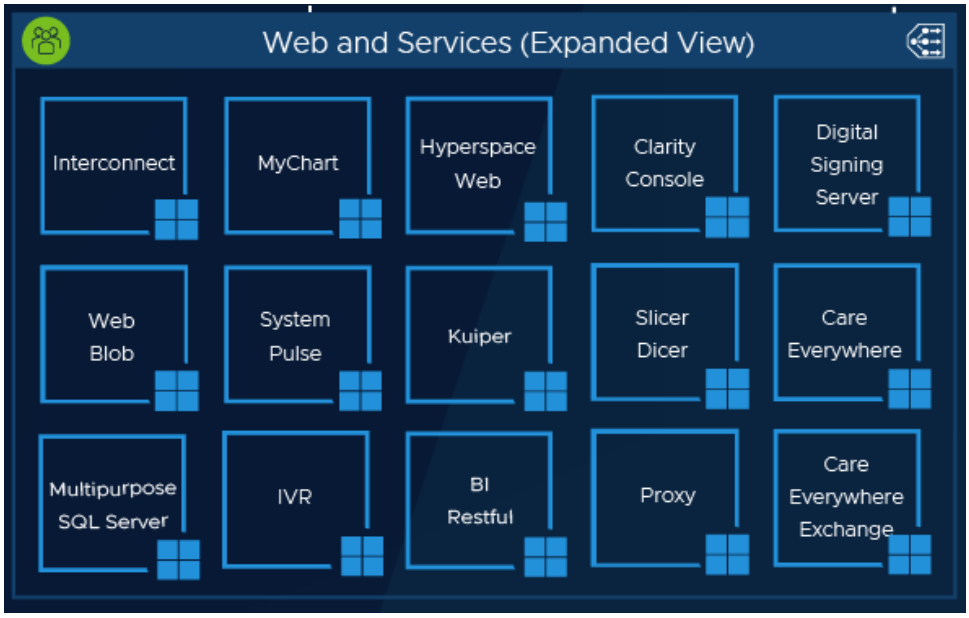
Install the Horizon infrastructure: Unified Access Gateways, Connection Servers, AppVolumes Servers

The Horizon Unified Access Gateway Appliances will reply to incoming session requests and connect the user to the appropriate Cloud Pod through the Horizon infrastructure. Customers looking to adopt the newer Universal Broker architecture can leverage this option through Horizon Cloud. Templates of the desired VDI image will be placed within the VDI control layers. Load balancing plays a key role in proper session distribution in the VDI management layers of the infrastructure.

Web and Services Tier Infrastructure

This section focuses on strategies and guidance when implementing the Web and Services Tier in Azure VMware Solution. VMware HCX and NSX-T provide network extensibility in a lift-and-shift scenario. We will be focusing on migrating workloads from the on-premises infrastructure directly into Azure VMware Solution.

Below is an example of the Web and Services Tier VMs within their own AVS cluster. Refer to the Epic Hardware Configuration Guide for Virtual Machine Sizing. Use the same configuration per VM as mentioned in the guide.



Architecture Recommendations

For most scenarios, the following documents will apply. There might be situations in which the recommendations referenced in the document links below may be deviated from. Use best practice and vendor guidance where appropriate.

It is expected that Azure VMware Solutions prerequisites and initial deployment have already taken place. Please refer to the additional resources section at the end of this document for planning and deployment guidance.

Requirements

Secondary Cluster Creation for Web and Services Tier VMs within AVS infrastructure: Placement of the Web and Services (WSS) workloads will be separate from the management infrastructure VMs. Clustering by use-case will allow scaling independently and mitigate reaching AVS maximums. The secondary cluster will utilize the same control plane as the first management cluster that was created upon deployment of the Azure VMware Solution.

- Active Directory Services within AVS infrastructure: Ensure proper object replication has taken place and service availability can be confirmed.
- DNS Services within AVS infrastructure: When enabled with the domain controllers, replication will occur automatically.
- Certificate Authority Services with AVS infrastructure: Ensure CA services are available on all sides of the environment and high-availability design testing has taken place.

HCX and Workload Migration from On-Premises to AVS

HCX Advanced is the default edition. An upgrade to Enterprise is needed to support the migration of the Web and Services Tier workloads. Open a support request with Azure, ask for HCX Enterprise and a new license key will be provisioned.

HCX deployment is done through the Azure portal as an add-on. Downloading the HCX Connector OVA and deploying the virtual appliance to the on-premises VCSA is a manual task. Please refer to the following documents regarding HCX deployment.

- Install VMware HCX on Azure VMware Solution (Microsoft)
- VMware HCX Product Documentation

Ensure proper testing and confirm the desired outcomes of VM mobility before the production workload migration.

HCX will provide the layer-2 extension of the on-premises environment to the AVS landing zone. It is required to utilize HCX Enterprise for the enhanced functionality of Replication Assisted vMotion (RAV) and additional optimization mechanisms (MON).

HCX provides encryption, packet optimization, and service fidelity to ensure the success of the migration.

HCX focuses on 3 main tasks:

1. Extend the existing network
2. Migrate workloads to a modern SDDC
3. Migrate network to NSX

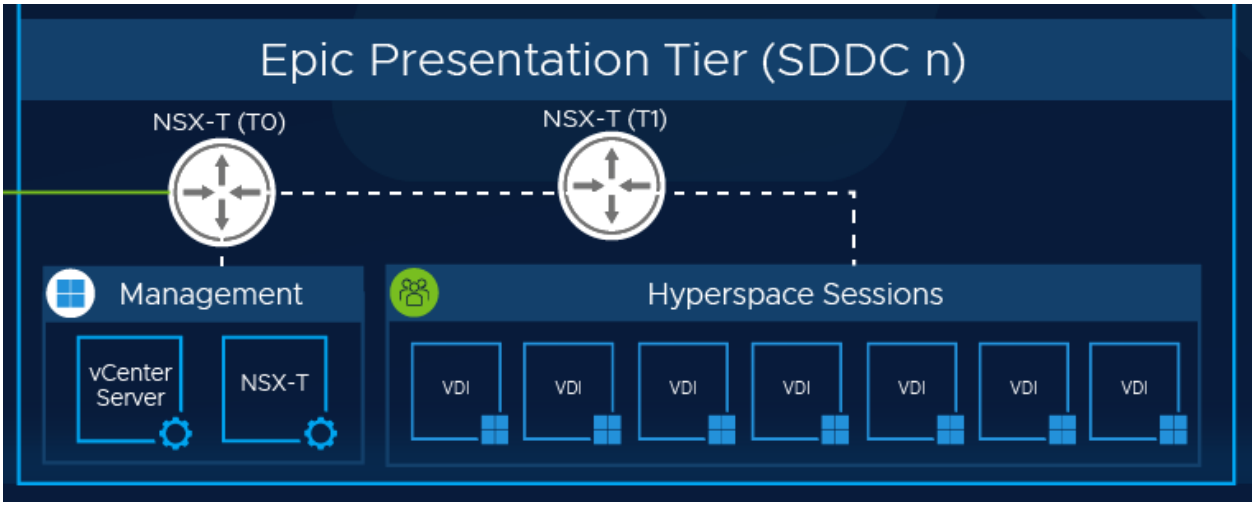
Refer to EHR vendor documentation for the failover process and preparation for service downtime. Below are the high-level functions that will take place during a workload migration with HCX.

- Confirm the creation of the second cluster has taken place where Web and Services VMs will reside. The AVS workflows should automatically configure the proper routing and apply connectivity to the AVS management control plane.
- Ensure the high availability of the workload being migrated. Focus on network sensitivities and recovery methodologies that may take place during a workload move.
- It is assumed that the Layer-2 extension configuration has taken place before the movement of the workloads. Refer to the AVS HCX Network Extension Designlet.
- Within HCX, create the virtual machine group to migrate from source to destination. The destination will be the secondary cluster dedicated to WSS.
- Utilize RAV and MON options when migrating to minimize downtime and ensure efficiencies within the traffic flow from the data center to AVS.
- Cut over the networks from the primary data center to AVS via NSX-T.
- Modify VIP(s) within the load balancing infrastructure for configuration cleanup.
- Clean up HCX resources when they are no longer needed.

VDI Presentation Tier Infrastructure

This section focuses on strategies and guidance when implementing the VDI Presentation Tier in Azure VMware Solution. We will be focusing on the Horizon Cloud Pod Architecture and how it correlates to Azure VMware Solution.

Below is an example of the Presentation Tier VMs within their own AVS SDDC dedicated to Hyperspace VDI session access. Refer to the Epic Hardware Configuration Guide for virtual machine sizing. Use the same configuration per VM as mentioned in the guide.



Additional AVS SDDCs for Hyperspace Sessions

Choosing the best ExpressRoute Edge Gateway determines the maximum number of AVS SDDCs that can interconnect. Refer to ExpressRoute Edge Gateway documentation from Microsoft to verify bandwidth and connectivity requirements are met for future growth.

Below are the high-level functions when planning and deploying multiple AVS SDDCs for Hyperspace and general VDI Sessions:

- Plan in accordance with the Cloud Pod Architecture design guidance. The session entry points should start with the Universal Broker services in the Horizon Cloud (or Unified Access Gateways) and trickle down into the AVS Infrastructures or back to on-premises. Proper routing and load balancing is key to a great user experience.
- Dedicate n number of SDDCs for Hyperspace Sessions for the VDI resource pools. There will be a 1:1 ratio within each infrastructure. 1x AVS SDDC: 1x Horizon Cloud Pod.
- The vCenter and NSX Managers in each of the SDDC environments should be lightweight; bare essential control planes for the Horizon Connection Servers to connect into.
- It is recommended to dedicate cluster 1 in each of the AVS SDDCs for management workloads: vCenter and NSX Managers (misc. lightweight workloads to support security/localized necessary). Land the VDI sessions into cluster 2 and subsequent clusters after. For heavier workloads and monitoring, the first AVS SDDC cluster that holds Shared General Purpose Workloads may be a suitable infrastructure. Another option is to create a dedicated cluster in the first AVS SDDC for these heavy workloads to reside.
- Implement VDI session best practices for security within NSX (micro-segmentation, port and services monitoring, and others)
- Consider a customized vSAN Storage Policy within the deployment template to enable features such as erasure coding and increased FTT (resiliency) depending on session and user requirements.

Summary and Additional Resources

Recommendations

For most scenarios, the following documents will apply. There may be situations in which the recommendations referenced in the document links below may be deviated from. Use best practice and vendor guidance where appropriate.

It is expected that Azure VMware Solutions prerequisites and initial deployment have already taken place. Please refer to the following resources for planning and deployment guidance.

- Refer to the AVS Planning and Deployment Guide
- Shared Responsibility Model
- Microsoft SQL Server on AVS Best Practices Guide
- Best Practices for Epic on VMware vSAN

Conclusion

Azure VMware Solution offers Epic customers the ability to seamlessly migrate healthcare workloads to the cloud while maintaining consistent performance and operational excellence by leveraging their existing VMware investments, skills, and tools with familiar technology including vSphere, HCX, NSX-T, and vSAN.

Changelog

The following updates were made to this guide:

Date	Description of Changes
2022/07/22	

About the Author and Contributors

Christian Rauber, Staff Mission-Critical Workloads Solution Architect in the Cloud Infrastructure Business Group at VMware, authored this paper with contributions from the following members:

- Drew Tsang, Staff Cloud Infrastructure Architect, VMware
- Jeremiah Megie, Principal Cloud Solutions Architect, VMware
- Steve Pantol, Sr. Technical Marketing Architect, VMware