MBCOM TECHNOLOGIES | vmware by Broadcom

Adria Forum 2025

Modernizing VMware Workloads with Azure VMware Solution (AVS)

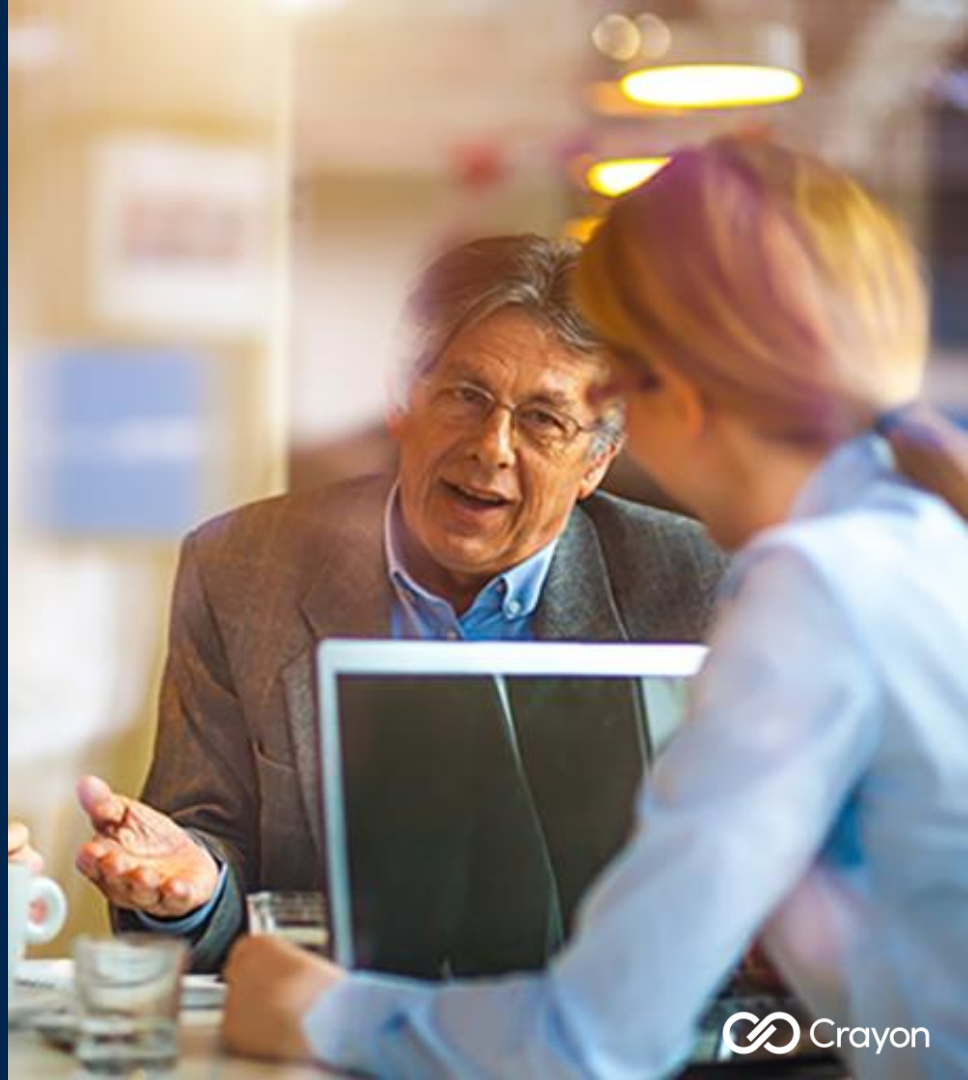
Miloš Živković

Cloud Architect - Crayon

14.10.2025.

Agenda

- VMware on Public Cloud – Concept & Architecture
- Crayon Migration assessment and Cloud adoption Framework
- Azure VMware Solution (AVS)
- Migration Strategies & Operational Model
- Vendor financing
- Q&A and Next Steps

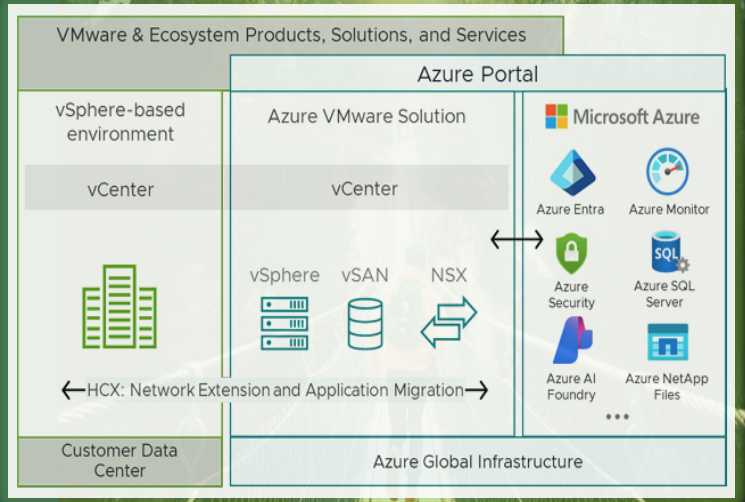


Crayon

Azure VMware Solution

Overview

Azure VMware Solution (AVS) enables organizations to seamlessly extend or migrate their existing on-premises VMware workloads to Azure. This service provides a consistent VMware experience, allowing you to run native VMware environments at scale in the cloud, managed by Microsoft and verified by VMware.



Key features:

- **Seamless Integration:** Maintain operational continuity with your on-premises VMware environments using familiar tools like vSphere, vSAN, and NSX.
- **Scalability:** Easily scale resources up or down based on business needs without the complexities of hardware procurement.
- **Access to Azure Services:** Integrate with native Azure services, enabling modernization and enhancement of your applications.

Crayon

Overview

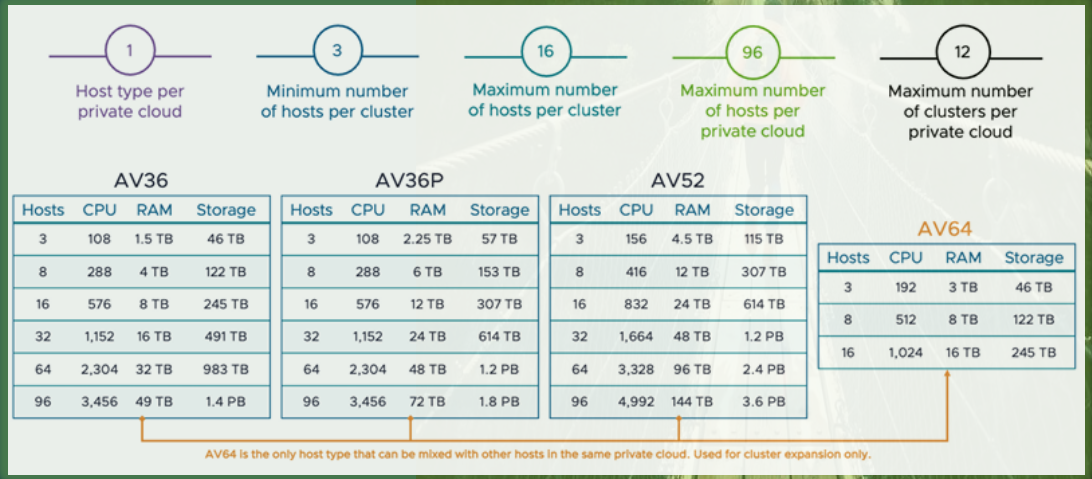
Compute

Node types and specifications:

- **AV36:** 36 physical cores, 576 GB memory, 3.2 TB NVMe cache, 15.2 TB SSD storage.
- **AV36P:** 36 physical cores, 768 GB memory, 1.5 TB Intel cache, 19.2 TB NVMe storage.
- **AV52:** 52 physical cores, 1536 GB memory, 1.5 TB Intel cache, 38.4 TB NVMe storage.
- **AV64:** 64 physical cores, 1024 GB memory, 3.84 TB NVMe cache, 15.36 TB NVMe storage. Note: AV64 is only available for expanding existing private clouds built with AV36, AV36P or AV52 nodes.

Each AVS cluster requires a minimum of three hosts.
Scale up to 16 hosts per cluster.
Multiple clusters can be deployed within a single private cloud.

VMware DRS (Distributed Resource Scheduler):
Automatically balances workloads to optimize performance and resource utilization.



Crayon

Overview

Storage

VMware vSAN for Hyper-Converged Storage:

AVS includes vSAN, a software-defined storage layer that aggregates Azure-hosted NVMe SSDs for high performance.

Scale-Out Storage Capacity:

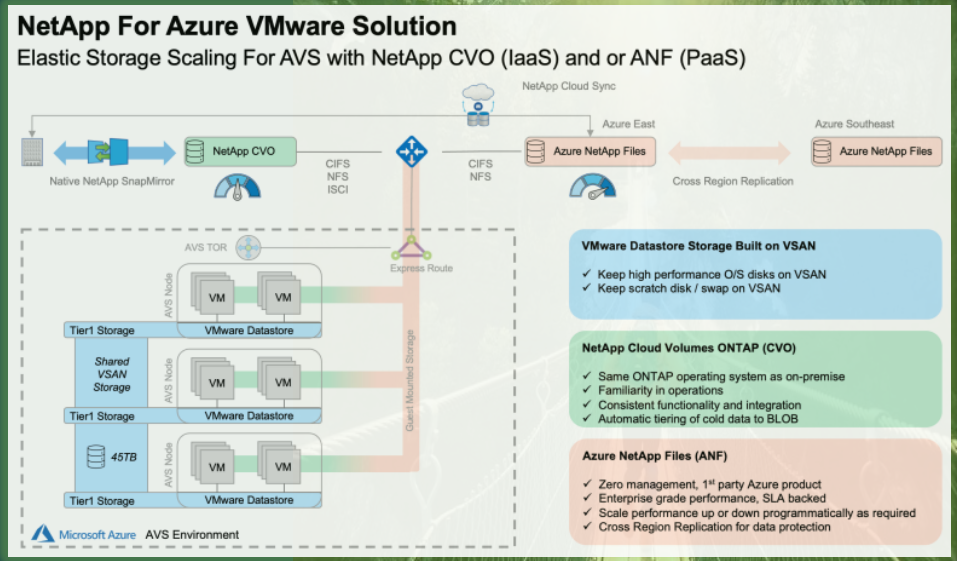
Add storage on-demand by scaling AVS hosts or using Azure Blob Storage integration.

vSAN RAID Levels & Storage Policies:

Define fault tolerance levels, data redundancy, and performance policies via VMware vSAN policies.

Azure NetApp Files for AVS:

Integrate Azure NetApp Files for NFS-based storage and high-performance data workloads.



Crayon

Overview

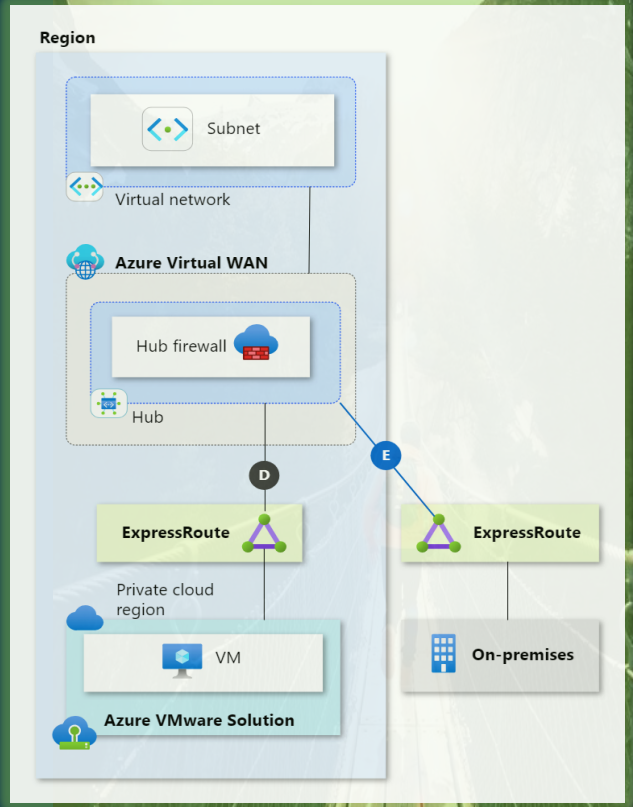
Network

Azure ExpressRoute or IPSec VPN for AVS: Establish private, high-speed connections between on-premises data centers and AVS.

NSX-T Network Virtualization: Enable micro-segmentation, security policies, and software-defined networking within AVS.

Hybrid Network Integration: AVS connects seamlessly to on-prem VMware workloads and Azure Virtual WAN, VPN, or SD-WAN solutions.

Azure-native Network Extensions: Leverage Azure Load Balancer, Firewall, and Private Link to enhance AVS networking.



Crayon

Identity & Access Management

Native vCenter Integration: AVS extends your on-premises vSphere environment into Azure while maintaining full vCenter Server access for managing VMware workloads.

Role-Based Access Control (RBAC):

- Within vSphere and NSX-T, AVS supports VMware-native roles and permissions (e.g., Read-Only, Administrator, Virtual Machine User).
- Azure IAM policies can be layered on top for additional security enforcement at the Azure subscription and resource group levels.

Integration with Existing On-Prem Permissions:

- Existing vSphere users and groups from your on-premises environment and AD can be extended into AVS, retaining the same permission sets.
- Azure Entra ID (formerly Azure AD) can be integrated with AVS, allowing hybrid identity and Single Sign-On (SSO) across both on-prem and cloud-based VMware workloads.

Multi-Factor Authentication (MFA) & Conditional Access:

- Secure vCenter logins with Azure MFA, enforcing conditional access policies based on location, device health, or risk level.
- Extend Zero Trust security principles by requiring MFA for privileged AVS administrators.

Resource Management

vSphere Cluster Management:

AVS runs on dedicated Azure bare-metal hosts, fully managed within vCenter Server, while maintaining native VMware resource organization features like Clusters, Resource Pools, and Folders.

Resource Pools & Folders:

Organize VMs into logical groups within vSphere, enabling resource allocation, workload prioritization, and policy enforcement across AVS environments.

Tagging & Subscription Integration:

Use Azure Resource Manager (ARM) tags to categorize AVS resources for cost tracking, governance, and policy enforcement.

Azure Resource Organization & Management:

- AVS resources reside in an Azure subscription, enabling Azure Policy enforcement, IAM access control, and cost monitoring.
- AVS as a Managed Resource - AVS is provisioned within Azure Resource Manager (ARM) for centralized management alongside other Azure services.
- Azure Resource Groups Integration

Governance & Compliance

Azure Policy for AVS:

- Define and enforce governance policies for AVS workloads using Azure Policy
- Create, assign, and manage policies that control or audit your resources (e.g. Enforce tagging standards, Restrict allowed resource locations, Audit monitoring compliance…)

VMware Security Hardening Guidelines:

Supports implementation of VMware's recommended guidelines and security configurations for vSphere, NSX-T, and vSAN to enhance the security posture of your AVS environment.

Regulatory Compliance:

- AVS is officially certified for several well-known regulatory compliance standards, including:
- ISO 27001: Information Security Management System standard.
- PCI-DSS: Payment Card Industry Data Security Standard.
- HIPAA: Health Insurance Portability and Accountability Act.
- GDPR: General Data Protection Regulation

Additionally, AVS meets other compliance standards such as ISO 27018, SOC 1, SOC 2, SOC 3, FedRAMP, HITRUST, MTCS, IRAP, ENS, and FERPA. These certifications demonstrate AVS's commitment to maintaining high security and compliance standards.

Security

vSphere & NSX-T Security:

NSX-T Distributed Firewall (DFW): Enforces micro-segmentation, controlling “east-west” traffic between AVS workloads.
NSX-T Gateway Firewall: Secures “north-south” traffic for inbound and outbound AVS connections.
VM Encryption: Protects VM disks using vSphere Native Key Provider or external KMS.

Azure Defender for AVS:

Threat Detection & Posture Management: Continuously scans AVS workloads for vulnerabilities and suspicious activity.
AI-Driven Malware Protection: Leverages Microsoft Defender for Cloud to block emerging threats.
Automated Compliance Monitoring: Assesses AVS security against regulatory standards.

Zero Trust Security for AVS:

Network Segmentation with NSX-T: Enforces least privilege access at the network layer.
Traffic Inspection with NSX IDPS: Analyzes East-West and North-South traffic for anomalies.
Conditional Access for vCenter Admins: Requires MFA for high-privilege accounts.
Endpoint Security Integration: Supports VMware Carbon Black, Palo Alto Prisma Cloud,…

Monitoring

Azure Monitor & Log Analytics:

Integrate AVS with Azure Monitor to track performance, logs, and security events, enabling centralized observability across cloud and on-prem environments.

VMware Aria Operations (formerly vRealize):

Utilize VMware-native monitoring for capacity planning, workload optimization, and proactive troubleshooting within AVS.NSX Intelligence & vSAN Health Monitoring – Analyze network traffic, storage health, and performance bottlenecks using built-in VMware insights.

Azure Sentinel Integration:

Forward AVS log data to Microsoft Sentinel for SIEM capabilities, advanced analytics, and threat detection.

3rd-Party Monitoring Tools:

AVS supports integrations with third-party solutions (e.g. Splunk, Datadog, New Relic, LogicMonitor…) for custom dashboards, log analytics, and multi-cloud observability.

BC / DR

(business continuity & disaster recovery)

VMware HCX for Live Migration:

Perform bulk live VM migrations with zero downtime, ensuring seamless workload mobility between on-premises and AVS.

VMware Site Recovery Manager (SRM):

Automate disaster recovery orchestration, enabling rapid failover and failback of AVS workloads.

Azure Site Recovery for Hybrid DR:

Extend disaster recovery (DR) protection using Azure-native DR services, supporting hybrid environments.

Multi-Region AVS DR:

Deploy AVS clusters across multiple Azure regions for geo-redundancy and high availability.

Backup Integration:

AVS supports Azure Backup for VM snapshots, long-term retention and geo-redundancy. Also, integrating with third-party backup solutions (e.g. Veeam, Commvault, Cohesity,…)

IaaC
(infrastructure as a code)

Terraform, Bicep & PowerCLI:
Automate AVS deployments and management using familiar Infrastructure as Code (IaaC) tools, via VMware APIs.

Azure Resource Manager (ARM) Templates:
Deploy Azure-native AVS resources using ARM templates.

Ansible for Configuration Management:
Use Ansible playbooks to automate AVS VM configurations and patching.

Billing & Cost Optimization

Pay-as-You-Go pricing per node type:

- AV36: $9.22 per hour ($6,638 per month) per node.
- AV36P: $10.96 per hour ($7,891 per month) per node.
- AV52: $21.68 per hour ($15,609 per month) per node.
- AV64: $15.76 per hour ($11,347 per month) per node.

Note: West Europe is used in example above. Prices and availability can vary based on region. Refer to Azure VMware Solution Pricing for the latest updates.

Azure VMware Solution Reserved Instances:

Save up to 60% on Pay-as-You-Go prices by committing to 1, 3, or 5-year reserved instances.

Azure Hybrid Benefit:

Bring existing Windows Server & SQL Server licenses to AVS, reducing licensing costs by up to 85%.

Integrated Billing with Azure:

AVS costs are fully managed within Azure billing, allowing budget tracking and forecasting.

Summary

Azure VMWare Solution (AVS)

Seamless VMware integration:
Minimal migration effort, fully VMware-compatible platform.

VMware native capabilities:
Built-in VMware stack (vSphere, vSAN, NSX-T):
- Monitoring and automation (VMware Aria Operations)
- Business continuity and DR (VMware HCX, SRM integration)
- Familiar VMware ecosystem (Horizon, Photon OS, VMware Tools)

Managed infrastructure:
Fully managed Azure-hosted VMware environment reduces infrastructure overhead.

Existing IT skills are fully usable:
No need for retraining, operational continuity can be maintained with existing VMWare expertise

MBCOM TECHNOLOGIES | vmware by Broadcom

Adria Forum 2025

Thank You