VMware Cloud™ on AWS - Reference Architecture

Hybrid Cloud Identity and Access Management with Microsoft Active Directory and AWS IAM

This reference architecture details how on-prem Active Directory infrastructure can be extended to VMware Cloud on AWS Infrastructure. It also shows how AWS Identity and Access Management service along with STS and AWS AD Connector can be integrated with Windows Active Directory server hosted on VMware Cloud on AWS for user authentication and management of native AWS resources.

1. Deploy and configure **SDDC on VMC on AWS** in a region and availability zone that hosts most of the AWS native resources.

2. Setup **VPN connections and/or Direct Connect connections** so that on-prem users and VMware Cloud admins can access resources on VMC on AWS as a private network. Route based VPN is preferred as opposed policy based VPN for dynamic route propagation.

3. Setup **On Prem Router** and **Compute Gateway** with appropriate firewall rules to route the Infrastructure and end user workload traffic "to and from" Infrastructure and Workload segments. Setup **Management Gateway** with appropriate firewall rules to route all the administrative traffic including AD replication and management traffic "to and from" Management Appliances/VMs.

4. Deploy two Windows servers in VMC on AWS Infrastructure network segment and promote those Windows servers to domain controllers in the on-premises Active Directory forest, making AD DS highly available in the VMC on AWS Cloud. Configure Active Directory replication between on-prem and VMC on AWS hosted Windows AD server. All network traffic, between on-prem AD Server and VMC on AWS AD Server in SDDC, including AD DS communication, authentication requests and Active Directory replication is secured across the VPN tunnel or Direct Connect link.

5. Configure Amazon EC2 instances to join AD domain and use private DNS servers that are hosted on VMC on AWS. All network traffic, including AD DS communication and authentication requests between EC2 Instances and other Native AWS services flows through **Cross VPC ENI** with low latency high bandwidth connectivity. There will be no extra data egress charges for the data traffic passing through Cross VPC ENI and AWS resources that resides on same AZ as the VMC SDDC.

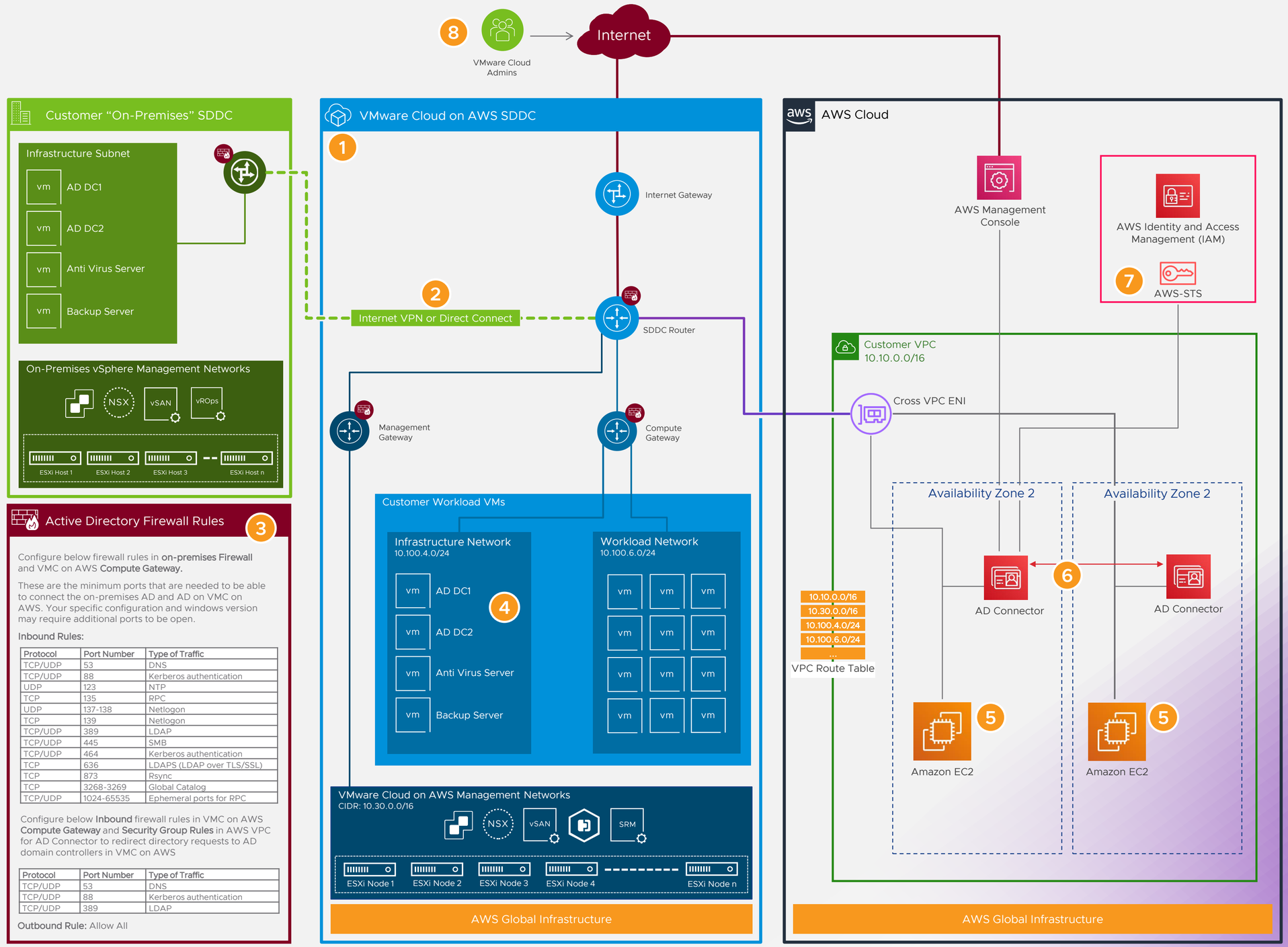
   These EC2 instances can now access AD domain controllers sitting on VMC on AWS for secure, low-latency directory services and DNS requests.

6. Configure AD Connector to perform LDAP authentication to Active Directory servers that are hosted on VMC on AWS. With this configuration, AD Connector can locate the nearest domain controllers by querying the SRV DNS records for the domain.

7. Setup **AD Connector** to call the **STS AssumeRole** method to assume **IAM role** and get temporary security credentials for user authentication. Using those temporary security credentials, AD Connector can construct a sign-in URL that users can use to access the AWS management console.

   In situations where a user is mapped to multiple IAM roles, at the sign-in screen, user will be presented with choice to select appropriate IAM role for that session. Such connected sessions last for one hour.

8. VMware Cloud Admins can now use the integrated AD authentication for AWS management console logins and manage AWS resources conveniently without requiring to remember multiple passwords.



Protocol	Port Number	Type of Traffic
TCP/UDP	53	DNS
TCP/UDP	88	Kerberos authentication
UDP	123	NTP
TCP	135	RPC
UDP	137-138	Netlogon
TCP	139	Netlogon
TCP/UDP	389	LDAP
TCP/UDP	445	SMB
TCP/UDP	464	Kerberos authentication
TCP	636	LDAPS (LDAP over TLS/SSL)
TCP	873	Rsync
TCP	3268-3269	Global Catalog
TCP/UDP	1024-65535	Ephemeral ports for RPC

Configure below **Inbound** firewall rules in VMC on AWS **Compute Gateway** and **Security Group Rules** in AWS VPC for AD Connector to redirect directory requests to AD domain controllers in VMC on AWS

Protocol	Port Number	Type of Traffic
TCP/UDP	53	DNS
TCP/UDP	88	Kerberos authentication
TCP/UDP	389	LDAP

Outbound Rule: Allow All

vmware | aws

VMware Cloud™ on AWS