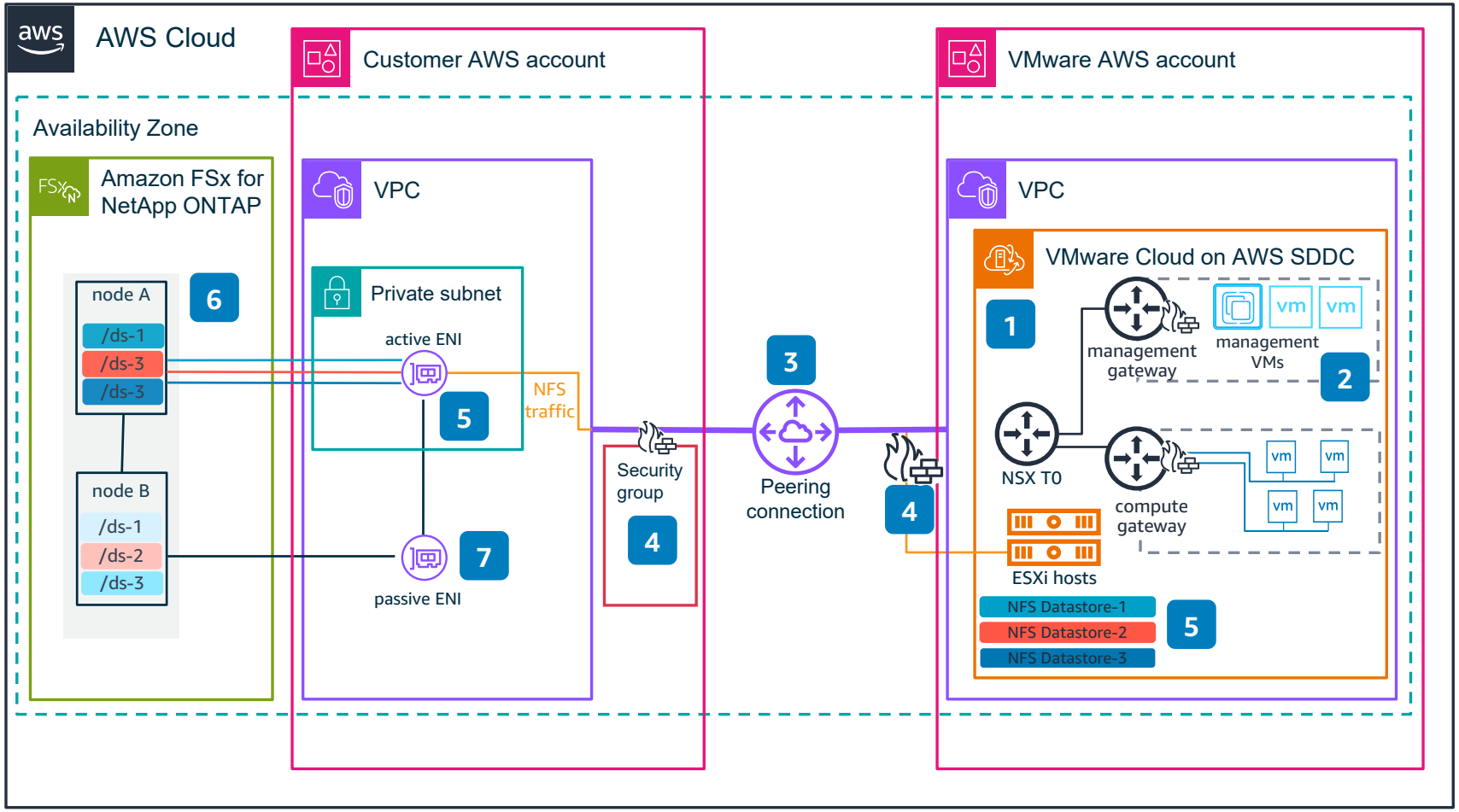
Amazon FSx for NetApp ONTAP Datastores with VMware Cloud on AWS using VPC Peering

This architecture details how to connect Amazon FSx for NetApp ONTAP file systems that are hosted on AWS to VMware Cloud on AWS as vSphere datastores on a single Software-Defined Datacenter (SDDC) Using VPC Peering.



1. **VMware Cloud on AWS Software-Defined Datacenter** (SDDC) is deployed in the VMware-managed account in a single Availability Zone (AZ) configuration.

2. SDDC management components, including vCenter Server, NSX Manager and the HCX management appliances, run on a datastore powered by VMware vSAN, which aggregates the local storage from AWS bare-metal hosts.

3. A Virtual Private Cloud (VPC) peering connection is a connection between two VPCs. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The customer contacts their customer success or account representative and requests VCP peering. The owner of the *requester (VMware) VPC* sends a request to the owner of the *accepter (customer) VPC* to create the VPC peering connection. The owner of the accepter VPC needs to accept the VPC peering connection request to activate the VPC peering connection.

4. The customer contacts VMware support to finalize the VPC peering. VMware updates the network routes to use the peering connection. The customer does the same in their VPC and configures any security group rules to allow NFS traffic.

5. NFS storage traffic flows from the datastore mounted on the ESXi host through the VPC peering connection. From here, the storage traffic is routed to the active **Amazon FSx for NetApp ONTAP** elastic network interface (ENI) to the **FSx for ONTAP** file system.

6. A Single-AZ file system powered by **FSx for ONTAP** is deployed in the same AWS Availability Zone as the SDDC.

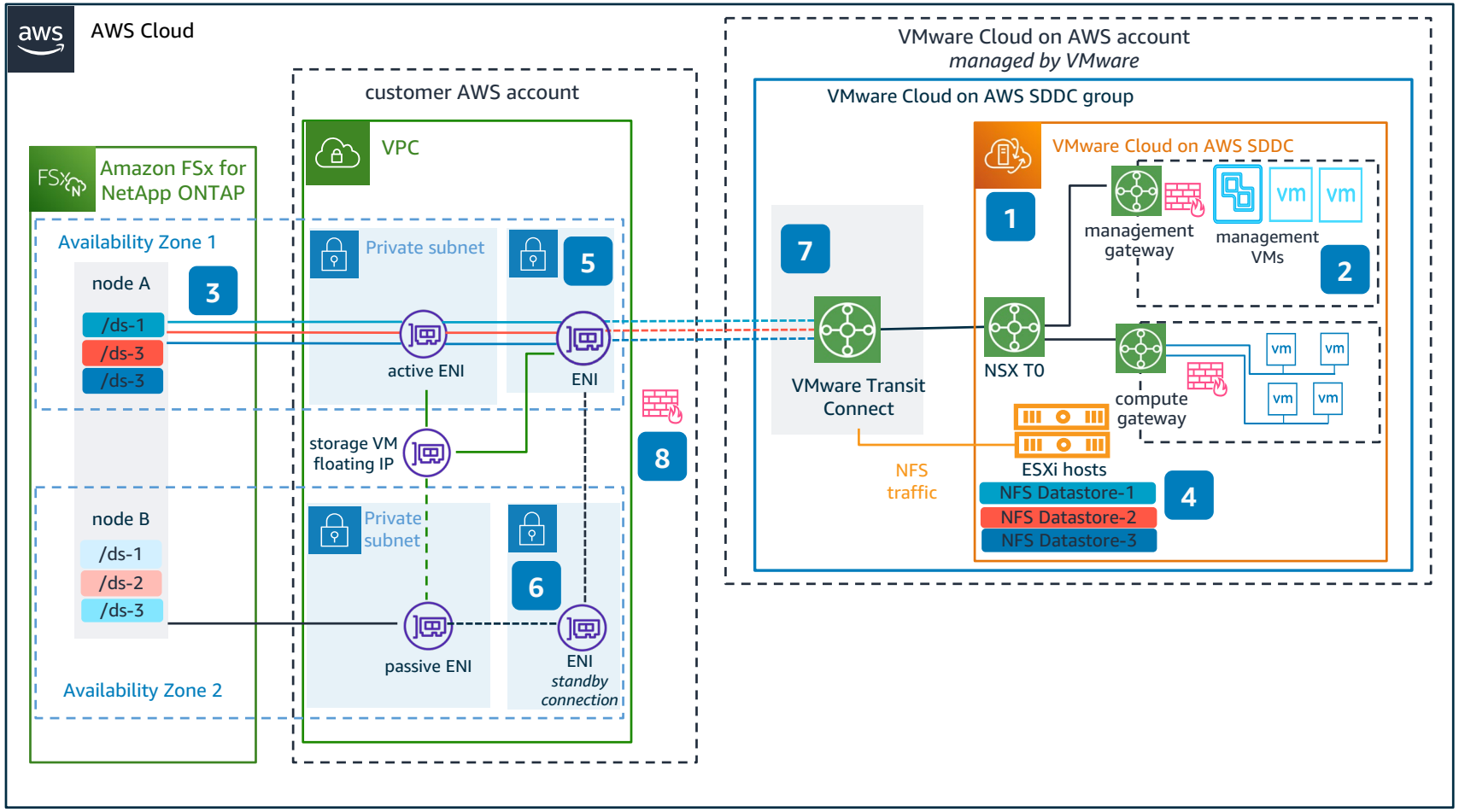
7. When a failure impacts the **FSx for ONTAP** file system on the primary node, **FSx for ONTAP** automatically fails over to the secondary node. The standby connection with passive ENI becomes the active ENI and resumes communication between the SDDC and the **FSx for ONTAP** file system.

Reviewed for technical accuracy January 9, 2024

AWS Reference Architecture

Amazon FSx for NetApp ONTAP Datastores with VMware Cloud on AWS

This architecture details how to connect Amazon FSx for NetApp ONTAP file systems that are hosted on AWS to VMware Cloud on AWS as vSphere datastores on a single Software-Defined Datacenter (SDDC).



1. **VMware Cloud on AWS Software-Defined Datacenter** (SDDC) is deployed in the VMware-managed account in an SDDC group in a single Availability Zone (AZ) configuration. One or more SDDCs can be added in an SDDC group for network file system (NFS) supplemental storage access.

2. SDDC management components, including vCenter Server, NSX Manager and the HCX management appliances, run on a datastore powered by VMware vSAN, which aggregates the local storage from AWS bare-metal hosts.

3. A Multi-AZ file system powered by **Amazon FSx for NetApp ONTAP (FSx for ONTAP)** is deployed across two AWS Availability Zones. VMware Transit Connect establishes a connection with the external virtual private cloud (VPC) that hosts the file system in the customer account.

4. NFS storage traffic flows from the datastore mounted on the ESXi host to VMware Transit Connect. From here, Transit Connect routes the storage traffic to the AWS Transit Connect attachment in the customer-managed VPC, where it is finally routed to the active **FSx for ONTAP** elastic network interface (ENI) to the **FSx for ONTAP** file system.

5. The **AWS Transit Gateway** ENI connects the customer VPC to VMware Transit Connect. This is different from the cross account ENI and can be deployed in a dedicated 28-bit subnet or within the **FSx for ONTAP** subnet.

6. When a failure impacts the **FSx for ONTAP** file system in the primary Availability Zone, **FSx for ONTAP** automatically fails over to the file system in the secondary Availability Zone. The standby connection with passive ENI becomes the active ENI to enable communication between the SDDC and the **FSx for ONTAP** file system.

7. VMware Transit Connect is a VMware-managed regional router powered by **AWS Transit Gateway**. It is automatically deployed when an SDDC group is created. The SDDC group provides connectivity between the **FSx for ONTAP** NFS volumes to ESXi hosts running in the SDDC.

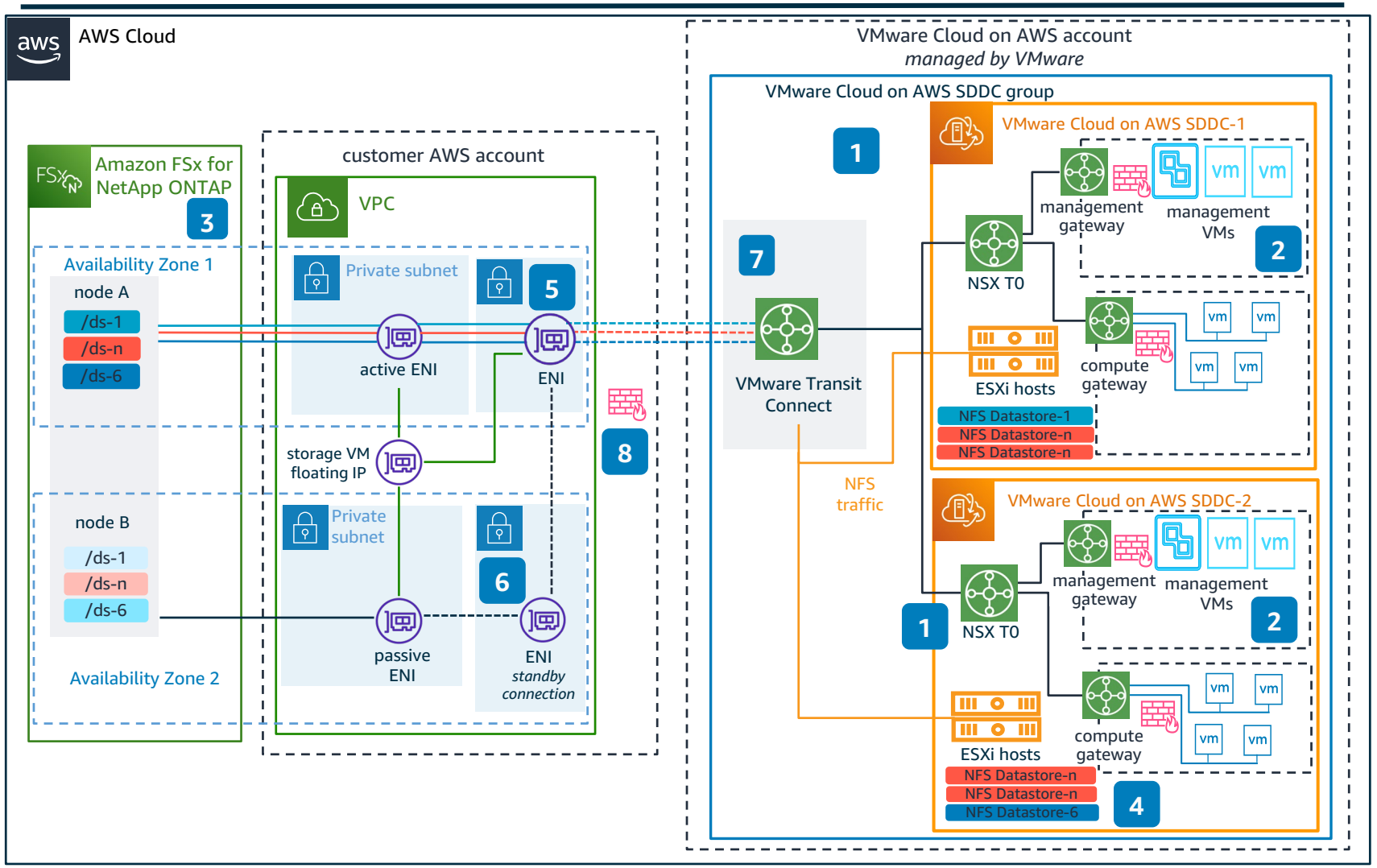
8. Configure the security group in your AWS VPC to allow incoming NFS traffic from the ESXi host management subnet. SDDC NSX firewall configuration is not required.

Reviewed for technical accuracy January 9, 2024

AWS Reference Architecture

Amazon FSx for NetApp ONTAP Datastores with VMware Cloud on AWS

This architecture details how to connect Amazon FSx for NetApp ONTAP file systems hosted on AWS to VMware Cloud on AWS as vSphere datastores on multiple SDDCs.



1. **VMware Cloud on AWS SDDC** is deployed in the VMware-managed account in an SDDC group in a single Availability Zone configuration. One or more SDDCs can be added in an SDDC group for NFS supplemental storage access.
2. SDDC management components, including vCenter Server, NSX Manager and the HCX appliances, run on a datastore powered by VMware vSAN, which aggregates the local storage from AWS bare-metal hosts.
3. A Multi-AZ file system powered by **Amazon FSx for NetApp ONTAP** is deployed across two AWS Availability Zones. VMware Transit Connect establishes a connection with the external VPC that hosts the file system in the customer account.
4. NFS storage traffic flows from the datastore mounted on the ESXi to VMware Transit Connect. From here, Transit Connect routes the storage traffic to the AWS Transit Connect attachment in the customer-managed VPC, where it is finally routed to the active **FSx for ONTAP** ENI to the **FSx for ONTAP** file system.
5. The **AWS Transit Gateway** ENI connects the customer VPC to VMware Transit Connect. This is different from the cross account ENI and can be deployed in a dedicated 28-bit subnet or within the **FSx for ONTAP** subnet.
6. When a failure impacts the **FSx for ONTAP** file system in the primary Availability Zone, **FSx for ONTAP** automatically fails over to the file system in the secondary AZ. The standby connection with passive ENI becomes the active ENI to enable communication between the SDDC and the **FSx for ONTAP** file system.
7. VMware Transit Connect is a VMware-managed regional router powered by **AWS Transit Gateway**. It is automatically deployed when an SDDC group is created. The SDDC group provides connectivity between the **FSx for ONTAP** NFS volumes to ESXi hosts running in the SDDC.
8. Configure the security group in your AWS VPC to allow incoming NFS traffic from the ESXi host management subnet. SDDC NSX firewall configuration is not required.

Reviewed for technical accuracy January 9, 2024

AWS Reference Architecture