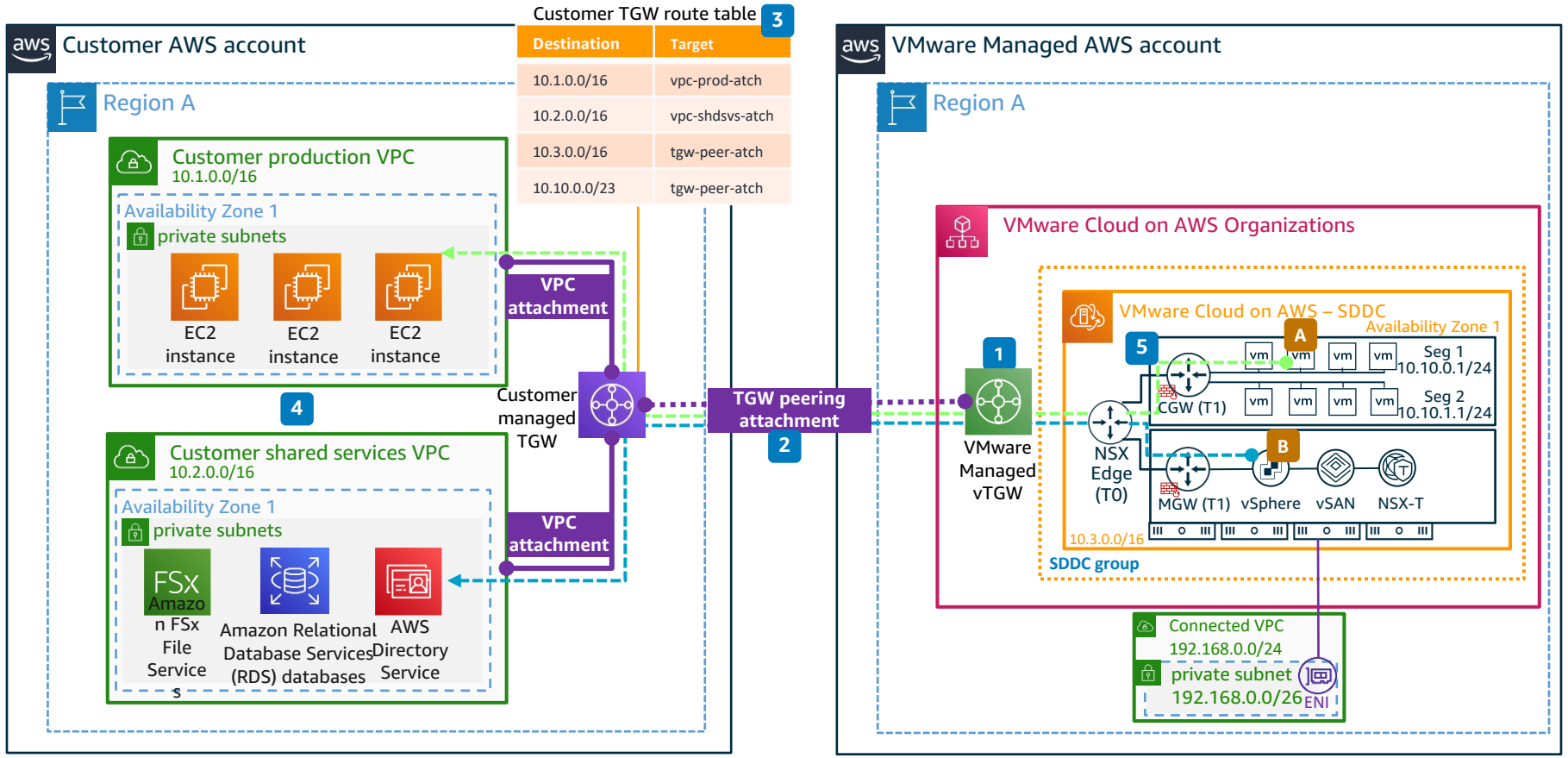
VMware Cloud on AWS – Simplifying Intra-Region Connectivity, Option 1

Simplify connectivity from SDDCs to existing or new AWS VPCs within the same AWS Region, utilizing a customer Transit Gateway (TGW) and VMware Transit Connect. Option 1 demonstrates how workloads within SDDCs can access production and shared AWS services within different customer VPCs, utilizing a TGW peering attachment.



1 **VMware Transit Connect** enables customers to build high-speed, resilient connections between their **VMware Cloud on AWS** Software Defined Data Centers (SDDCs) and other resources, including AWS networking services. Customers must create an **SDDC Group** to deploy a VMware Managed Transit Gateway (vTGW) within the **VMware Cloud on AWS** service. Refer to Create or Modify an SDDC Group for instructions.

2 Customers must create a TGW peering attachment between the customer TGW and vTGW. Refer to Getting Started with VMware Transit Connect Intra-Region Peering for VMware Cloud on AWS for instructions. To enable workloads within the SDDC to access other VPCs, define relevant subnet prefixes within the routes list, such as 10.1.0.0/16 and 10.2.0.0/16. Once the configuration has been applied, virtual machine (VM) traffic destined for those subnets will route across the TGW peering attachment to the customer TGW.

3 Customers need to update their TGW route table (*RT*) accordingly, creating static routes for SDDC based Networks across the TGW <-> vTGW peering attachment. Refer to Transit gateway route tables for instructions. **Note:** As there is no dynamic route propagation, any additional networks created within the SDDC will need static routes created. Route summarization should be utilized.

4 Customers may need to update their security groups (SGs) or Network Access Control Lists (NACLs) accordingly, to allow inbound and outbound access from workloads running within the SDDC. Refer to Work with security groups and Control traffic to subnets using Network ACLs for details.

5 Customers need to update their SDDC Compute Gateway (CGW) and Management Gateway (MGW) firewall policies accordingly, to allow inbound and outbound access from AWS services running within the VPCs attached to the customer TGW. Refer to Add Compute Gateway Firewall Rules to Enable SDDC Group Member Workload Connectivity for instructions.

A Traffic flow for workloads to access AWS services within a production VPC, via the customer TGW <-> vTGW peering attachment.

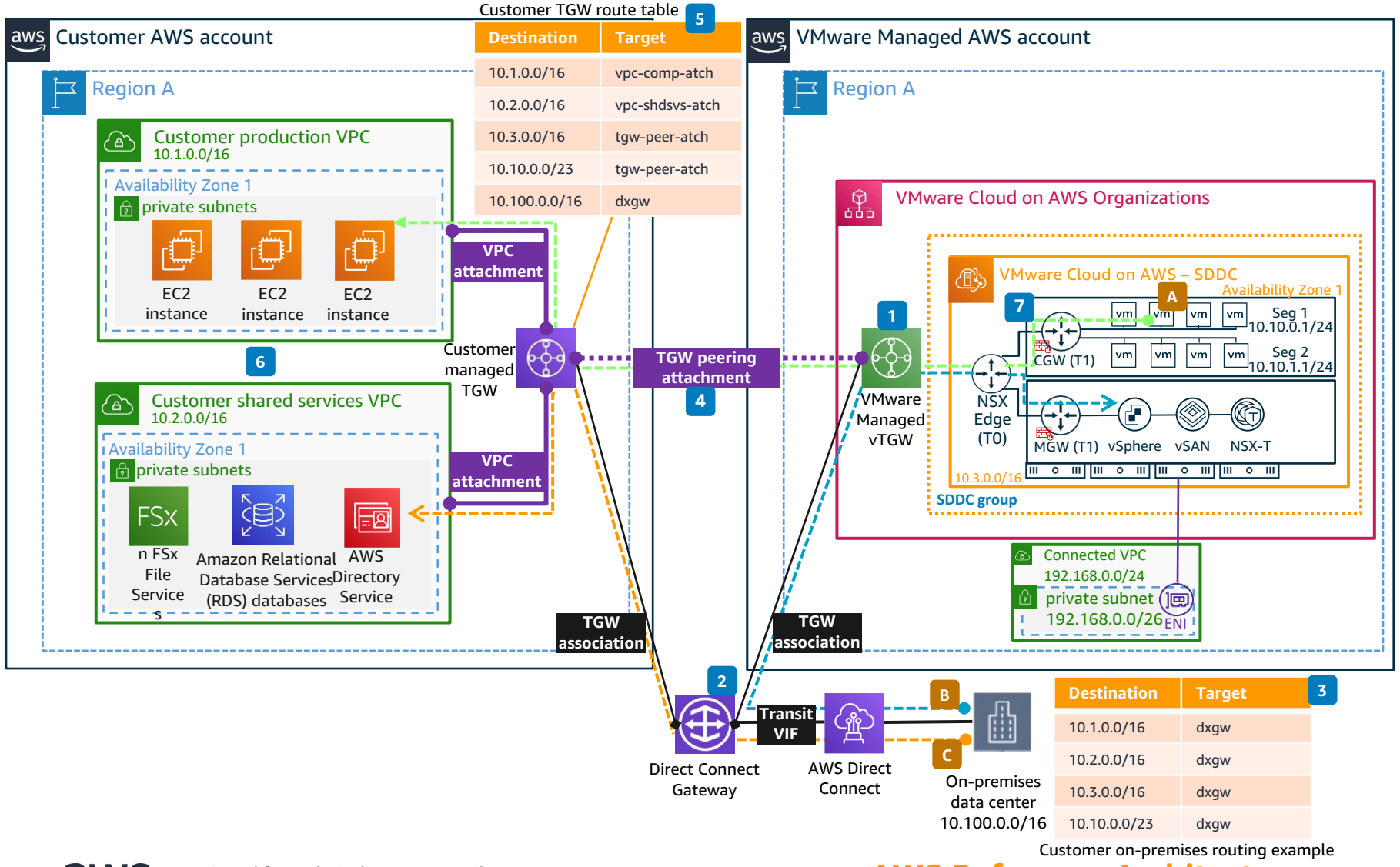
B Traffic flow for workloads to access AWS services within a shared services VPC, via the customer TGW <-> vTGW peering attachment.

Reviewed for technical accuracy April 7, 2022

AWS Reference Architecture

VMware Cloud on AWS – Simplifying Intra-Region Connectivity, Option 2

Simplify hybrid connectivity from on-premises facilities to AWS VPCs and SDDCs within the same AWS Region, utilizing a Customer Transit Gateway (TGW), VMware Transit Connect, Direct Connect (DX) and Direct Connect Gateway (DXGW). Option 2 demonstrates how on-premises networks can connect to SDDCs utilizing DX and DXGW. It also shows how workloads in SDDCs can access production and shared AWS services within different customer VPCs, utilizing a TGW peering attachment.



1. **VMware Transit Connect** enables customers to build high-speed, resilient connections between their **VMware Cloud on AWS** SDDCs and other resources, including AWS networking services. Customers must create an SDDC group to deploy a vTGW within the **VMware Cloud on AWS**. Refer to Create or Modify an SDDC Group for instructions.
2. Once the **vTGW** is deployed, customers can use their existing or new DXGW to facilitate simplified connectivity from on-premises facilities into the SDDC. Customers must create a TGW association on their DXGW to the vTGW. Refer to Attach a Direct Connect Gateway to an SDDC Group for instructions.
3. Once the new TGW association is in place, customers must update their on-premises routing and security policies accordingly to access workloads running within the SDDC.
4. Customers must create a TGW peering attachment between the customer TGW and vTGW. Refer to Getting Started with VMware Transit Connect Intra-Region Peering for VMware Cloud on AWS for instructions. To enable workloads within the SDDC to access other VPCs, define relevant CIDR prefixes within the Routes list; for example, 10.1.0.0/16 and 10.2.0.0/16. Once the configuration has been applied, VM traffic destined for those subnets will route across the TGW peering attachment to the customer TGW.
5. Customers need to update their TGW route table (RT) accordingly, creating static routes for SDDC-based networks across the TGW <> vTGW peering attachment. Refer to Transit gateway route tables for instructions. Note: As there is no dynamic route propagation, any additional networks created within the SDDC will need static routes created. Route summarization should be used.
6. Customers may need to update their security groups or NACLs accordingly, to allow inbound and outbound access from workloads running within the SDDC. refer to Work with security groups and Control traffic to subnets using Network ACLs for details.
7. Customers need to update their SDDC Compute Gateway (CGW) and Management Gateway (MGW) firewall policies accordingly, to allow inbound and outbound access from AWS services running within the VPCs attached to the customer TGW. Refer to Add Compute Gateway Firewall Rules to Enable SDDC Group Member Workload Connectivity for instructions.

A. Traffic flow for SDDC workloads to access AWS services within a production VPC, via the vTGW <-> TGW peering attachment.

B. Traffic flow for on-premises workloads to reach their SDDC, via the DXGW <-> vTGW.

C. Traffic flow for on-premises workloads to reach their VPCs, via the DXGW <-> customer TGW.

Reviewed for technical accuracy April 7, 2022

AWS Reference Architecture