TECHNICAL PAPER

Aruba CX Data Center

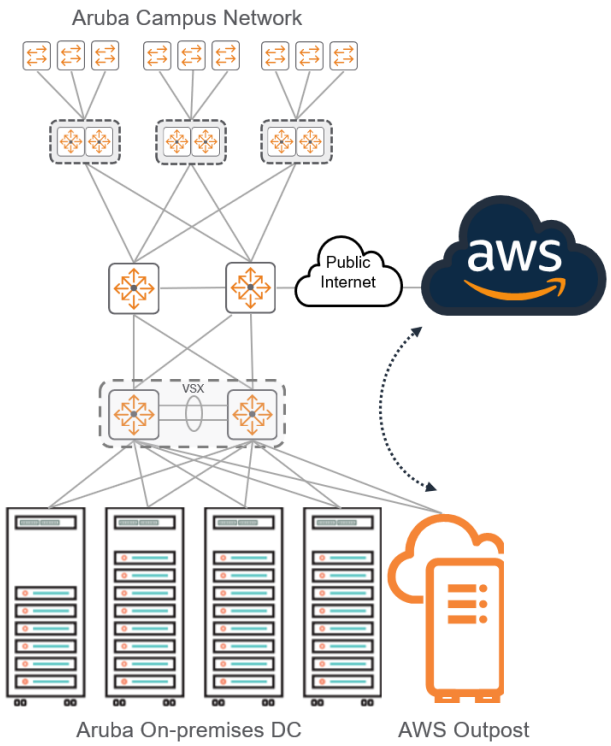
CONNECTING TO AWS OUTPOSTS

INTRODUCTION

The Aruba portfolio of CX switches simplifies data center networking via intelligent automation, distributed analytics and always-on infrastructure. The Aruba CX 8000 series delivers high performance spine and leaf 10/25/40/100GbE in a compact form factor and a wide variety of port configurations for both on-premise data centers and colocation facilities.

AWS Outposts is a fully managed service that extends AWS infrastructure, services, APIs, and tools to customer premises. By providing local access to AWS managed infrastructure, AWS Outposts enables customers to build and run applications on premises using the same programming interfaces as in AWS Regions, while using local compute and storage resources for lower latency and local data processing needs. This technical paper will describe how to extend Aruba data centers with AWS Outposts in order to deploy a hybrid cloud solution.

Figure 1 Aruba Data Center with AWS Outposts

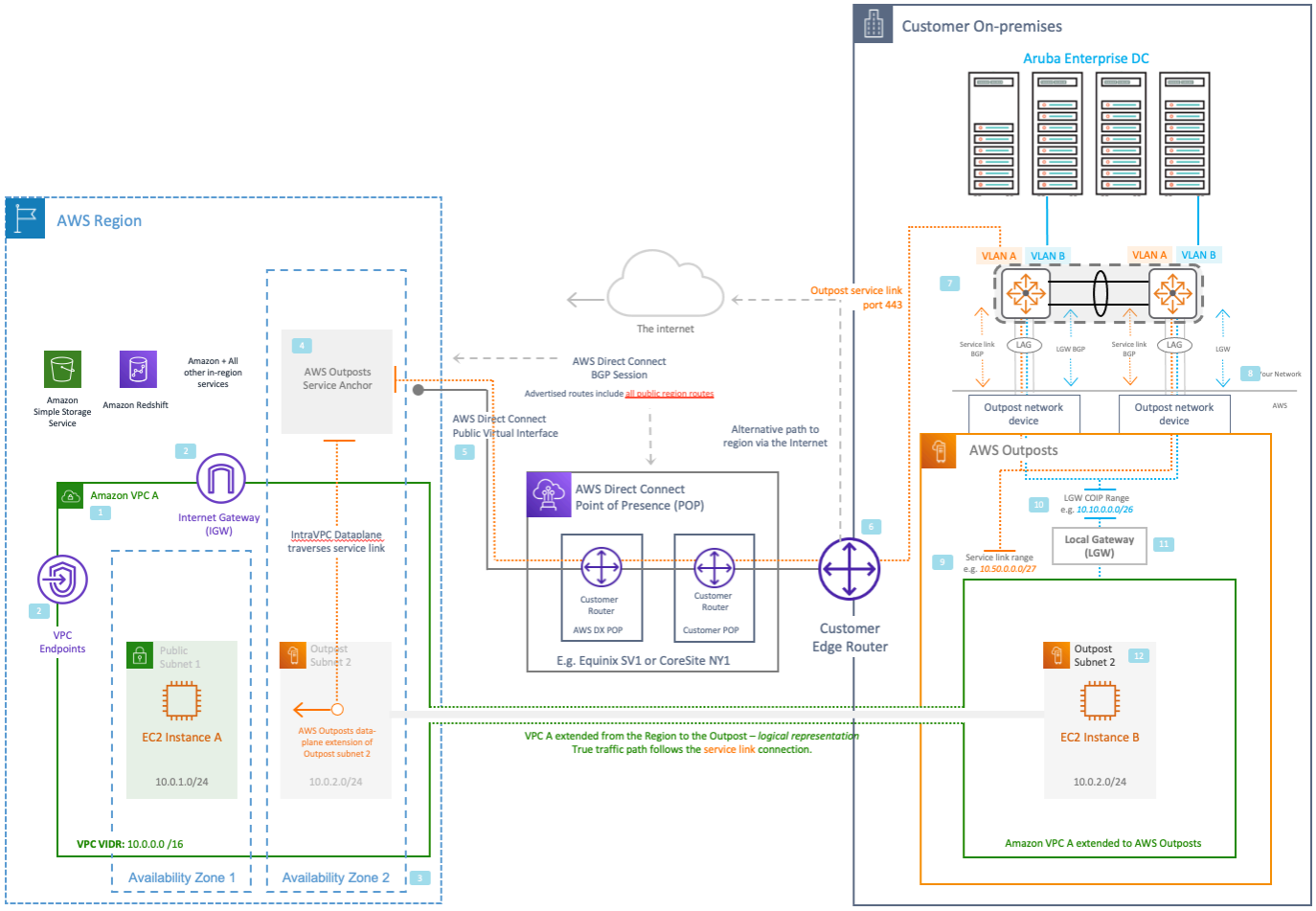


SOLUTION OVERVIEW

Extending private data centers with AWS Outposts provide the necessary integration to allow local workloads to interact with AWS workloads on-premises with support for high bandwidth, low latency, security and high availability. A hybrid cloud approach puts each application in its ideal environment while creating a seamless experience between public and private which helps simplify operations and maximize ease and agility while maintaining proper controls.

Each Outpost rack has a pair of networking devices, each with support of up to 400Gbps of connectivity using 1GigE, 10GigE, 40GigE and 100GigE fiber connections. On each Outpost the fiber patch panels on the top of the rack serve as a demarcation point between the on-premises data center infrastructure and the AWS managed equipment. That demarcation will be implemented using an LACP link bundle that will carry two VLANs for each outpost networking device. The VLANs separate AWS management, control and intra-VPC traffic from local traffic destined to the data center. Routing information is exchanged using dedicated eBGP sessions for each of the VLANs. The use of the separate eBGP sessions provide load balancing and segmentation between the AWS traffic and local LAN traffic. The Outpost link subnets need to be globally routable or translated using NAT at the Internet edge for outbound session establishment from Outpost to the AWS public IPs. The following figure shows the AWS Outpost rack architecture integrated with an Aruba on-premises data center.

Figure 2 Aruba Data Center with AWS Outposts

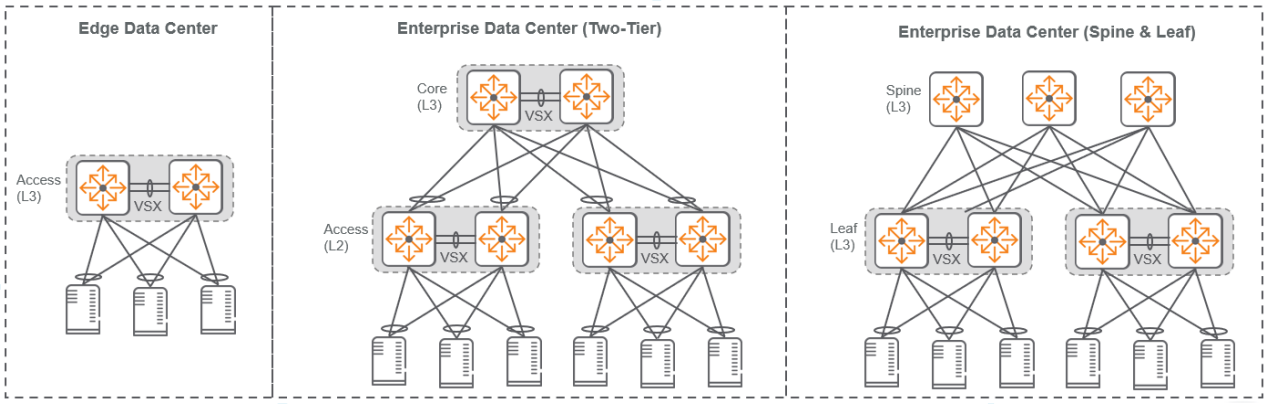


1. Multiple AWS Virtual Private Cloud (VPC) can be associated with the same outpost.
2. Region level services can be connected to from the outpost via intra-VPC connectivity.
3. An outpost is homed to an availability zone.
4. AWS Outposts service link anchor is created within the availability zone of your choosing and fronted by public Amazon IPs or coming soon with private IPs within a VPC of your choosing if using Outposts Private Connectivity.
5. An AWS Direct Connect public virtual interface (VIF) can be used to connect back to the AWS Outposts service anchor IPs or coming soon with private VIF usingAWS Outposts private connectivity.
6. An edge router with either a Direct Connect connection back to the region or public internet can be used to reach the Outposts service anchor in the region.
7. Aruba AOS-CX switches, configured as per the deployment guidance documented in this guide
8. Demarcation between the Aruba on-premises data center and the Outpost.
9. The service link infrastructure range is used to address infrastructure in the outpost that needs connectivity back to the Outpost anchor in the AWS region.
10. The “Customer Owned IP” range (CoIP), is used to address instances inside the Outpost with Elastic IPs from this range that need connectivity to on-premises workloads.
11. The LGW provides the NAT function between the Outpost VPC range and the appropriate Elastic IPs from the COIP range.
12. An Outpost subnet, created in an Amazon VPC, in an account that has an Outpost associated with it.

DEPLOYMENT SCENARIOS

The following figure highlights the most common deployment models for Aruba AOS-CX based data centers. All designs implement VSX LAG to provide multi-chassis LACP link bundles for compute nodes and live upgrades for non-disruptive software updates. Spine and leaf topologies allow a layer-3 fabric that eliminates the need for loop avoidance protocols while providing high availability, non-oversubscribed forwarding and low latency. Workload mobility is supported across all designs using standards-based layer-2 access or VXLAN overlays with a MP-BGP EVPN control plane.

Figure 3 Aruba Data Center Deployment Scenarios



The connectivity requirements of an AWS Outpost rack are a combination of LACP layer-2 link bundles that are carrying dual VLANS and BGP peering for route exchange at the demarcation point. Because of the requirements it is recommended to connect the Outpost rack directly to a layer-3 enabled VSX pair of Aruba AOS-CX switches.

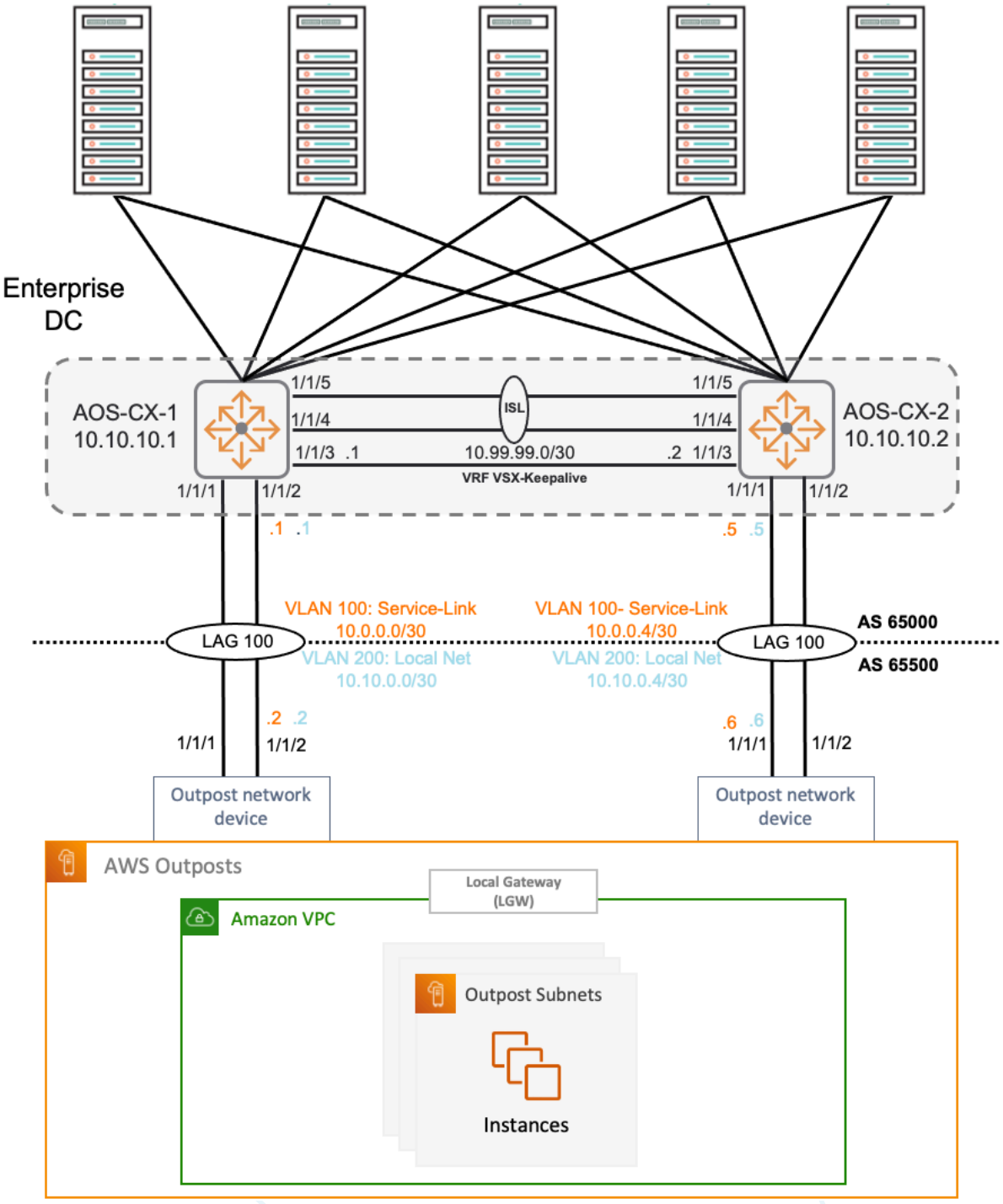
In an Aruba Edge data center the Outpost rack is directly attached to the access switch hosting on-premises compute nodes. For a two-tier topology with layer-2 access the Outpost rack should be connected to the layer-3 core. For a spine & leaf data center the Outpost rack should be connected to a border leaf because it is an external routing domain to the fabric.

This document is not meant to be an extensive data center or AWS VPC deployment guide and will focus on the connectivity requirements between the two solutions at the demarcation point while providing some guidance around IP connectivity that my impact your routing design and external connectivity to the AWS cloud.

DETAILED TOPOLOGY

The following figure illustrates the detailed connectivity requirements for the integration between an Aruba AOS-CX VSX pair and the Outpost network devices. The configuration procedures documented in this guide reflect the physical ports in the topology diagram.

Figure 4 Detailed Solution Deployment



DEPLOYMENT PROCEDURES

The following procedures will provide step-by-step guidance for configuring the AOS-CX switches that interconnect to the AWS Outpost rack. Plan for the VLAN and IP addressing scheme for the deployment prior to the configuration of the AOS-CX switches. The VLAN and IP information must also be provided to AWS prior to the installation.

VLAN Planning

Each Outpost requires two VLANs that are used to separate data paths between the on-premises network and the Outpost network:

- **Service link VLAN** – Enables communication between the Outpost and the AWS Region for both management of the Outpost and intra-VPC between the AWS Region and Outpost.
- **Local gateway VLAN** – Enables VPC traffic from Outpost into the local data center, Internet connectivity for the local AWS EC2 instances is also offered using this VLAN

IP Subnet Planning

A point-to-point network is required at the demarcation point for each VLAN. In this guide we will use the following IP addresses, /31 point-to-point addresses could be used as well:

VLAN	Description	Subnet	Aruba AOS-CX	AWS Outpost
100	CX-1 to OND-1 Service Link	10.0.0.0/30	10.0.0.1	10.0.0.2
200	CX-1 to OND-1 Local Gateway	10.10.0.0/30	10.10.0.1	10.10.0.2
100	CX-2 to OND-2 Service Link	10.0.0.4/30	10.0.0.5	10.0.0.6
200	CX-2 to OND-2 Local Gateway	10.10.0.4/30	10.10.0.5	10.10.10.6

The service link infrastructure subnet is a /26 CIDR range that is used to provide connectivity to the AWS Region via the service link VLAN. The service link subnet must be on routable space or translated at the Internet edge using NAT to establish connectivity to the AWS Region. The service link subnet could also use private connectivity, must be a range that is routable over your direct connect private virtual interface and reachable from your Outposts connectivity VPC.

A second /26 or larger subnet CIDR range must also be provided to AWS, for the Outpost local gateway to communicate between local EC2 instances and the data center. The local gateway range is called the CoIP (Customer owned IP range).

For external BGP configuration an Autonomous System (AS) number (2-byte or 4-byte) must be assigned to the data center and Outpost rack. The valid values for AWS are private AS numbers (64512-65535 or 4200000000-4294967294). In this guide we will use 65000 for the AOS-CX pair and 65500 for the Outpost. The /26 subnets for service link and local connectivity do not need to be configured on the AOS-CX switches as they will be advertised from the Outpost corresponding BGP session.

AOS-CX Base Configuration

On each AOS-CX switch, perform the following steps.

Step 1 Configure the switch host name.

```
hostname AOS-CX-Switch
```

Step 2 Configure the unrestricted administrator password.

```
user admin password plaintext [password]
```

Step 3 Require a username and password for console access using local credentials.

```
aaa authentication login console local
```

Step 4 Set the idle timeout for device access to 60 minutes (1 hour).

```
cli-session
    timeout 60
```

Step 5 Enable SSH server for inbound connections in the default vrf.

```
ssh server vrf default
```

Step 6 Configure a login banner.

```
banner motd #
Property of example.com !! Unauthorized use prohibited !!
#
```

Step 7 Configure the domain name and domain name servers.

```
ip dns domain-name example.local
ip dns server-address 8.8.8.8
ip dns server-address 8.8.4.4
```

Step 8 Configure the network time protocol (NTP) with time zone and daylight savings time.

```
clock timezone pst8pdt
ntp enable
ntp server 10.2.120.40 iburst
```

Step 9 Configure HTTP Secure (HTTPS) server for web access.

```
https-server vrf default
```

AOS-CX VSX Configuration

On each AOS-CX switch, perform the following steps.

Step 1 Configure the ISL LAG interface between the two switches. Select the native VLAN and allow all VLANs to be trunked. Enable LACP mode active.

```
interface lag 128
    no shutdown
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
    lacp mode active
```

Step 2 Configure at least two ISL physical interfaces between the two switches. Set the MTU to 9198.

```
interface 1/1/4
    no shutdown
    mtu 9198
    lag 128
interface 1/1/5
    no shutdown
    mtu 9198
    lag 128
```

Step 3 Configure a keepalive VRF to create an isolated network between the two switches.

```
vrf VSX-Keepalive
```

Step 4 Configure the keepalive physical interface between the two switches. Attach the keepalive VRF to the interface. Configure an IP subnet that is not used anywhere else in your network, so it is easily identified.

```
interface 1/1/3
    no shutdown
    vrf attach VSX-Keepalive
    description VSX Keepalive
    ip address 10.99.99.1/30
```

Step 5 Configure VSX. Define a common system-mac for L2 protocols. Make one switch primary and the other switch secondary. Use the keepalive interface IP addresses and VRF as the peer and source address.

```
vsx
    system-mac 00:00:10:10:10:01
    inter-switch-link lag 128
    role primary
    keepalive peer 10.99.99.2 source 10.99.99.1 vrf VSX-Keepalive
```

Step 6 For the other switch in the VSX pair, repeat this procedure using the appropriate values.

AOS-CX Layer-2 Configuration

On each AOS-CX switch, perform the following steps.

Step 1 Configure the VLANs used for service link and local gateway to Outpost.

```
vlan 100
    name AWS Service-Link
vlan 200
    name AWS Local_Net
```

Step 2 Configure the LACP bundles used to Outpost Network Devices

```
interface lag 100
    no routing
    vlan trunk allowed 100,200
    lacp mode active
    no shutdown
interface 1/1/1
    description to AWS OND-1
    lag 100
interface 1/1/2
    description to AWS OND-1
    lag 100
```

AOS-CX Layer-3 Configuration

On each AOS-CX switch, perform the following steps.

Step 1 Configure the loopback IP address, this will be used as the router-id for OSPF and BGP.

```
interface loopback 1
    ip address 10.10.10.1/32
```

Step 2 Configure the IP addresses associated with the service link and local network VLANs to the Outpost network devices.

```
interface vlan100
    description AWS Service-Link
    ip address 10.0.0.1/30
interface vlan200
    description AWS Local Net
    ip address 10.10.0.1/30
```

Step 3 Configure the BGP process and neighbors to Outpost. Activate the BGP session for IPv4 unicast routing. External BGP will use the VLAN IPs for session establishment.

```
router bgp 65000
    neighbor 10.0.0.2 remote-as 65500
    neighbor 10.0.0.2 update-source vlan 100
    neighbor 10.10.0.2 remote-as 65500
    neighbor 10.10.0.2 update-source vlan 200
    address-family ipv4 unicast
        neighbor 10.0.0.2 activate
        neighbor 10.10.0.2 activate
    exit-address-family
```

Step 3 Configure redistribution between BGP and routing protocol used in the data center. The steps will vary depending on your IGP design, please refer to AOS-CX user guide for configuration guidance.

ADDITIONAL REFERENCES

https://docs.aws.amazon.com/outposts/index.html

https://www.arubanetworks.com/products/networking/switches/