Avaya Solution & Interoperability Test Lab

Application Notes on Best Practices and Recommendations for Avaya Aura® Software Release 7.1.x on Amazon Web Services – Issue 1.0

Abstract

This Application Notes presents best practices, guidelines and recommendations for deployment and migration for Avaya Aura® software release 7.1.x on Amazon Web Services (AWS) Infrastructure as a service (IaaS) platform and provides recommendations for the AWS environment (e.g. Regions, Availability Zones, network connectivity, etc.).

Table of Contents

1. Scope of the document

These Application Notes present best practices, guidelines and recommendations for deployment and migration of Avaya Aura® software release 7.1.x on Amazon Web Services (AWS) Infrastructure as a service (IaaS) platform and provides recommendations for the AWS environment (e.g. Regions, Availability Zones, network connectivity, etc.).

2. Terminologies and Acronyms

Acronym / Term	Definition
AAC	Avaya Aura® Conferencing
AAM	Avaya Aura® Messaging
ACL	Access Control List
ADS	Avaya Diagnostic Server
AES	Avaya Aura® Application Enablement Services
AMI	Amazon Machine Image
AMS/AAMS	Avaya Aura® Media Server
ASBCE	Avaya Session Boarder Controller for Enterprise
AVP	Avaya Aura® Appliance Virtualization Platform
AWS	Amazon Web Services
AZ	Availability Zone
BSM	Avaya Aura® Branch Session Manager
CIDR	Classless Inter-Domain Routing
CM	Avaya Aura® Communication Manager
CM-Duplex	Avaya Aura® Communication Manager (Duplex)
EMS	Element Management System
ESS	Enterprise Survivable Server
IaaS	Infrastructure as a service
LSP	Local Survivable Processor
NAT	Network address translation
OVA	Open Virtualization Appliance
PS	Avaya Aura® Presence Services
PSTN	Public switched telephone network
QoS	Quality of Service
SDM	Solution Deployment Manager
SIT	System Integration Testing
SM	Avaya Aura® Session Manager
SMGR	Avaya Aura® System Manager
UAT	User Acceptance Testing
US	Avaya Aura® Utility Services
VE	Virtualization Enablement
VPC	Virtual Private Cloud
VPN	Virtual Private Network

3. Overview

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous; on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data.

Amazon Web Services (AWS) offers a suite of cloud-computing services that make up an on-demand computing platform. These services operate from various geographical regions across the world. The most central and best-known of these services arguably include Amazon Elastic Compute Cloud, also known as "EC2", and Amazon Simple Storage Service, also known as "Amazon S3". AWS have many different services, spanning a wide range, including compute, storage, networking, database, analytics, application services, deployment, management, mobile, developer tools and tools for the Internet of things.

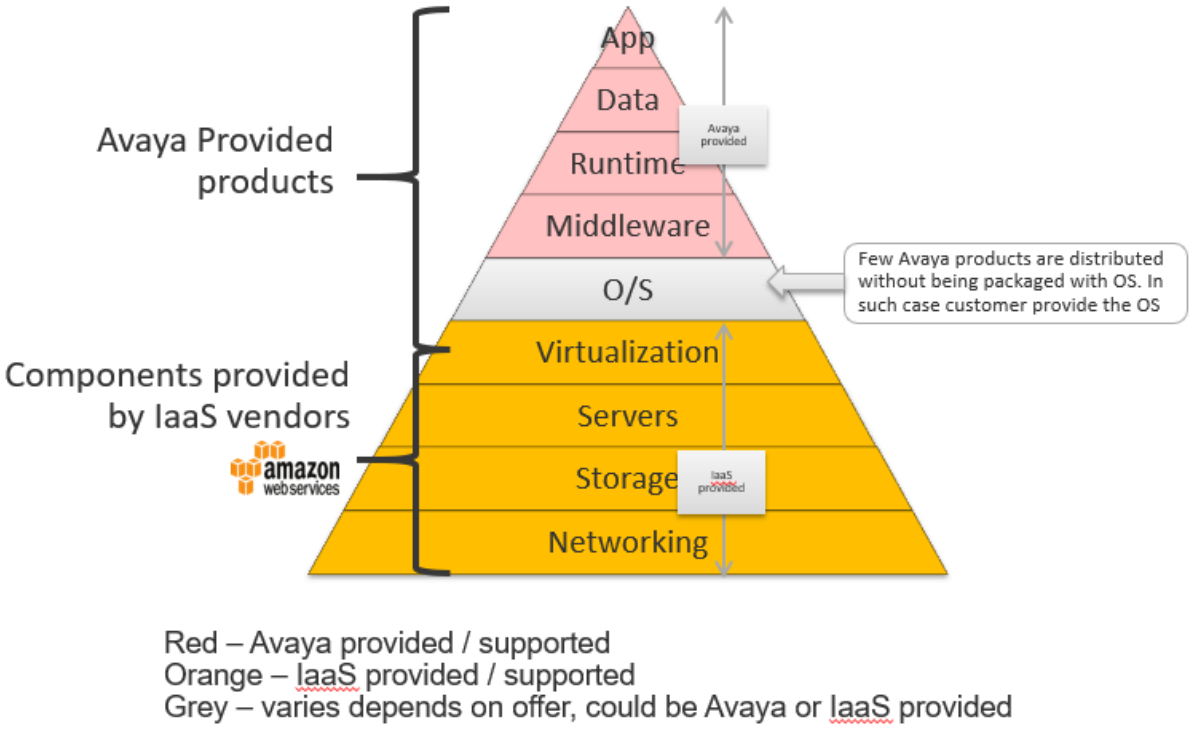
Infrastructure as a Service (IaaS) is an important service model which provides access to underlying compute resources. It allows the customers to utilize the infrastructure, typically based on a subscription-based pricing model. In general IaaS offers the following advantages for customers or business partners.

- Helps reduce capital expenditures on hardware procurements as AWS only charges on a pay per use basis.
- Helps reduce ongoing electricity, air conditioning, real estate costs to maintain own data center(s).
- Allows dynamically bringing up and tearing down capacities.
- Allows utilizing an IaaS environment for UAT/SIT environments
- Brings a consistency between deployment of data/web apps and real-time apps.

AWS Elastic Compute Cloud (EC2) is a leading IaaS.

Avaya Aura® software deployed on AWS IaaS platform would utilize different services of AWS e.g. compute, storage, networking, database, analytics. Avaya support these applications and the customer would purchase the applications from Avaya and then run them on their own AWS account and setup as per the guidelines from Avaya.

It is the customer's responsibility to ensure the Avaya Products they want deployed in AWS are listed in Section 4 otherwise the Avaya Product may not be supported in that environment.



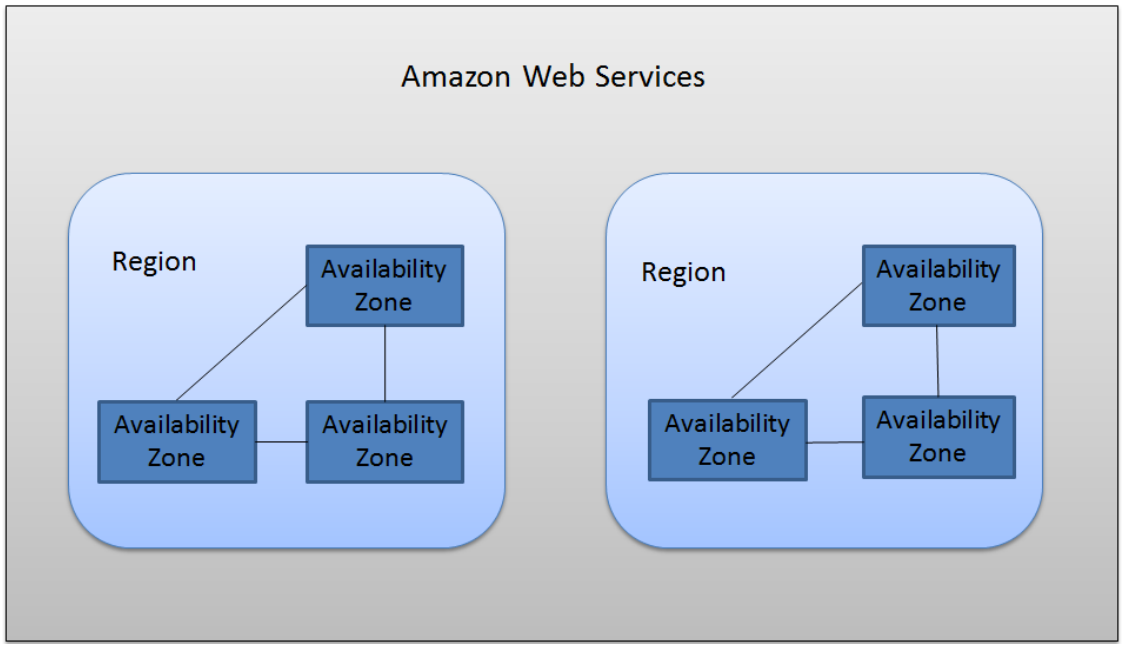
Following reasons are benefits to deploying applications into IaaS environments such as Amazon Web Services instead of investing further into new hardware in their own data center.

- Customers already have exposure to IaaS environment by utilizing their other applications. They would like to continue to use the IaaS capabilities to deploy more applications
- Customers would like to scale up and scale down the application footprints depending on varying business needs
- Reduction of capital expenditure (CAPEX) towards new hardware purchases
- Reduction of investment on the staff to maintain data center infrastructure
- Reduction of number of security checkpoints

AWS terminologies:

Region:
Each region is a separate geographical area. A region comprises Availability Zones. VPC is tied to a region and it cannot extend across regions.

Availability Zone:
Availability Zone is a distinct location within a region. Different Availability Zones within a region provides inexpensive low latency network between them. A VPC can extend across Availability Zones and each Availability Zone uses different IP subnets.



AWS connection options:

Across the Public Internet:
ASBCE would be connected to via the public internet for the external SIP endpoints.
Avaya Diagnostic Server would be able to reach out to Avaya via a NAT server from AWS.

VPN:
AWS supports VPN connections over the internet. The VPN connections would be used to connect from the customer enterprise network to the AWS customer VPC network. The VPN would go over the internet and the VPN tunnel would secure the traffic via encryption. Many customers do use public internet VPNs for VoIP traffic, but it is not recommended by Avaya as the network connection is not guaranteed.
When using a VPN, the traffic routes directly to and from the customer enterprise and the AWS network. Both the customer network and AWS would run firewalls, but the IP addresses would be directly contactable without going through NAT.

Direct Connect:

AWS Direct Connect establishes a dedicated network connection between your premises and AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment with increase bandwidth throughput and provides more consistent network experience than Internet-based connections.

AWS Direct Connect provides security and QoS to the data links. This would be Avaya's recommended AWS to customer enterprises connection type for AWS. It is possible to have very high connection bandwidth.

4. Avaya Aura® software supported on AWS

No	Product Name	Footprint	AWS Instance Type	Storage (GB) *
1	Avaya Aura® System Manager R7.1.x	Profile 2	m4.2xlarge	105
		Profile 3	m4.2xlarge	250
2	Avaya Aura® Session Manager R7.1.x	Profile 1	c4.xlarge	90
		Profile 2	c4.2xlarge	90
		Profile 3	c4.2xlarge	125
		Profile 4	c4.4xlarge	125
		Profile 5	c4.8xlarge	175
3	Avaya Aura® Communication Manager R7.1.x (Simplex)		m4.large	64
4	Avaya Aura® Communication Manager R7.1.x (Duplex)		c4.xlarge	64
5	Avaya Aura® Utility Services R7.1.x		t2.micro	20
6	Avaya Aura® Presence Services R7.1.x	Avaya Breeze™ Profile 2	m4.xlarge	80
		Avaya Breeze™ Profile 3	c4.2xlarge	80
		Avaya Breeze™ Profile 4	m4.2xlarge	150
		Avaya Breeze™ Profile 5	c4.4xlarge	300
7	Avaya Aura® Media Server R7.8 (Software only)	250 MPU	c4.xlarge	50
		1000 MPU	c4.2xlarge	50
		1900 MPU	c4.4xlarge	50
8	Avaya Aura® Application Enablement Services R7.1.x (Software only)	Profile 1	m3.medium	30
		Profile 2	c4.large	30
		Profile 3	c3.xlarge	30
9	Avaya Diagnostic Server R3.0 (Software only)		m4.xlarge	230
10	SAL Policy Manager with SSH Proxy R3.0 (Software only)		m4.large	
11	Avaya Session Border Controller for Enterprise R7.2	Standalone (Four NICs)	c4.2xlarge	160
12	Standalone Avaya WebLM R7.1.x	Profile1	t2.medium	30
		Profile2	t2.medium	30

* Note: Supported storage type is “General purpose SSD (GP2)” for all applications.

5. Unsupported and Limitations

Following features are not supported by Avaya Aura® software on AWS.

- System Manager SDM functionalities like upgrade, patching, auto-migration and virtual machine lifecycle management.
- IPv6 support on AWS
- Changing IP address of application deployed on AWS
- High Availability for ASBCE, AAMS, AES, PS on AWS.
- ASBCE Migration

6. Guidelines for AWS Environment

This section mentions the generic guidelines and best practices for AWS environment. For more information, refer to the AWS documentation.

6.1. Selecting AWS Region

Choosing an AWS region is the first decision to make when you set up your AWS components.

A region is a geographic area where AWS has data centers. Each region has 2 or more Availability Zones, which are independent data centers that are located close to each other. Availability Zones are used for redundancy and for data replication. For services such as EC2, you can choose which Availability Zone you want your instances to be launched into.

If most of your users access your application from within North America, then it typically makes sense to deploy your software in an AWS region located in the US or Canada. However, there are many other factors.

Following factors should be considered for selecting AWS Region for deploying Avaya Aura® software on AWS:

1. Supported AWS Services and instance types

Avaya Aura® software on AWS requires following AWS region specific services:
- Amazon Elastic Compute Cloud (EC2)
- Amazon Virtual Private Cloud (VPC)
- Amazon Simple Storage Service (S3)

All existing AWS regions support these services.

As of today, required EC2 instance types for Avaya Aura® software are available in all the AWS regions. However, at the time of actual deployment, it is recommended to ensure that required instance types are available on AWS region. For information about required instance types for different Avaya Aura® software, refer Setion-4 of this document or refer Avaya document for "Deploying Avaya Aura® software on Amazon Web Services"

2. Customer Proximity and Latency

The basic norm is to choose a region close to the customers. For instance, if most of the users access the application from within North America, it typically makes sense to deploy the

software in an AWS region located in the US or Canada, which further results in lowest network latency and the quick response.

Note: Customer must ensure to remain within network limit rules like latency for Avaya applications to be supported

3. Cost

Costs of the AWS Services would be different for different geographical regions. Amazon also has a cost calculator which gives a glance of the monthly costs based on the inputs. The AWS Simple Monthly Calculator helps customers and other prospects to estimate their monthly AWS bill more efficiently. Using this tool, they can add, modify and remove services from their 'bill' and it will recalculate their estimated monthly charges automatically.

4. Number of Availability Zones in a Region

All AWS regions do not have the same number of Availability Zones. The number of Availability Zones varies by regions, however all regions have at least 2 Availability Zones.
If you are building solution with strict availability, you should probably stay away from those regions that only have 2 Availability Zones. If one AZ in those regions is temporarily unavailable, you would be left with only 1 AZ to process all your traffic. When there is only 1 AZ left, there will be various failover mechanisms triggered by AWS and by other customers, bringing more load to that one AZ, which may put potential downtime.
Basically, if you have high availability requirements then you should stick to those regions with 3 or more AZs.

5. Security and compliance

Customer may have strict security and compliance, which forces them to select only few regions. In that case, the customer has to select an AWS region which is matching their security and compliance requirement.

6.2. AWS network connectivity guidelines

6.2.1. Generic guidelines and recommendation for AWS VPC

Following criteria should be considered while creating VPC:

- Ensure that your VPC network range (CIDR block) does not overlap with your organization's other private network ranges.
- Single VPC can spread across Availability Zones.
- It is recommended to use single VPC in a Region for Avaya Aura® software to avoid data transfer charges across VPCs.
- Ensure to size your VPC CIDR block which can accommodate sufficient IP addresses including future growth on number of application. It is not possible to increase/modify the VPC CIDR block once setup is up and running.
- Divide your VPC network range evenly across all available Availability Zones (AZs) in a region (at least across 2 AZs). Each Availability Zone network should be sub-divided in to six different subnets considering you plan to deploy ASBCE (two public and four private subnets). If there are no plans to deploy ASBCE, each Availability Zone network should be sub-divided in to at least three subnets (one public and two private subnets).
- Do not allocate all network addresses at once; instead ensure that you reserve some address space for future use.
- Create two separate route tables one each for private and public subnets. Only public route table should be given internet gateway routing, while private subnets should be give routing for enterprise subnets across direct connect or VPN.
- Deploy AWS NAT gateway in a public subnet.
- Configure separate AWS security groups for ASBCE and Avaya Aura® software. Allow only required transport ports in the security groups. For list of required ports, refer to Avaya port matrix document.

6.2.2. AWS VPC connectivity with corporate Data Center

There are mainly three options available to connect customer data centers and customer sites with AWS VPC. Multiple sites can be connected to AWS VPC private network. The following are the options:

1. AWS Direct connect
2. Hardware VPN
3. Software VPN

Avaya recommends using direct connect for connecting corporate data centers with AWS VPC, however, customers can use hardware or software VPN. In all case it is the responsibility of customers to ensure the required network quality.

Note:

- AWS uses IPsec for VPN connectivity which has IPsec overheads. These overheads are more significant if media packets are traversing across VPN tunnel. Hence, care must be taken during planning for network bandwidth to accommodate these network overheads. For example, calls with G729 media codecs consume roughly twice bandwidth over AWS IPsec VPN compared to bandwidth over plain internet.

6.2.3. Connecting multiple branches

Avaya Aura® software supports large number of branch locations. Customers wishing to use large number of branch locations would need to use one of the following options due to AWS supports limited number of VPN connections.

AWS provides VPN connection over public internet from AWS to the customer network. By default, VPN connections limit is 10. This can be increased up to 50 VPN connections by requesting to AWS support but still it is not sufficient for solution with more than 50 branch locations.

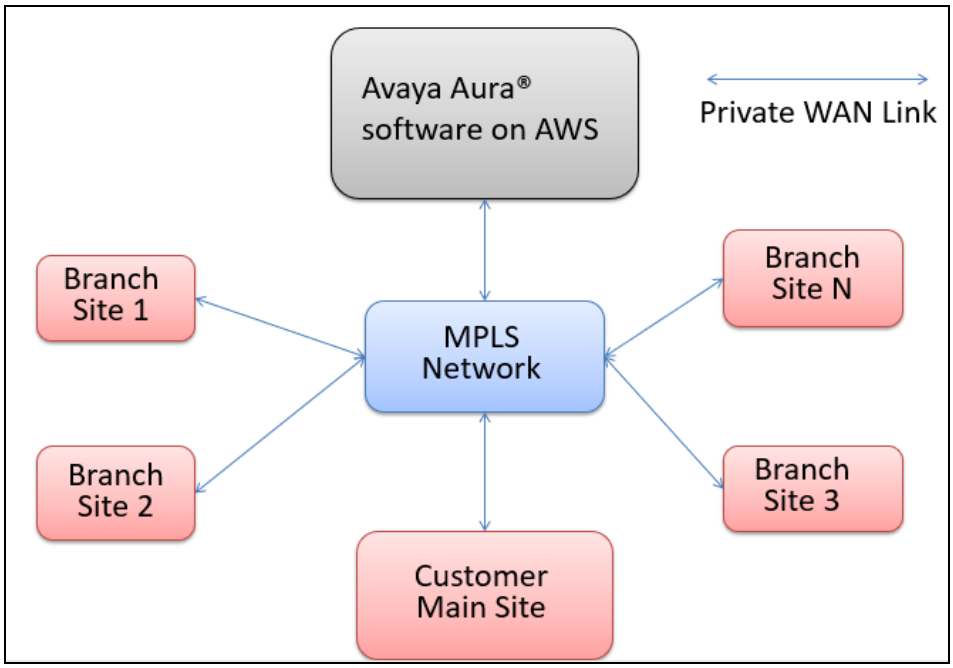
If customer is planning to connect large number of branches, they would need to use one of the following options:

Customer can deploy software based VPNs in their VPC and support any number of VPNs, using more software VPN instances as required. But public internet based VPNs are not optimal for business critical voice data and Avaya recommends that a direct connection based network is used.

It is recommended to use one of the following options for connecting large number of branches:

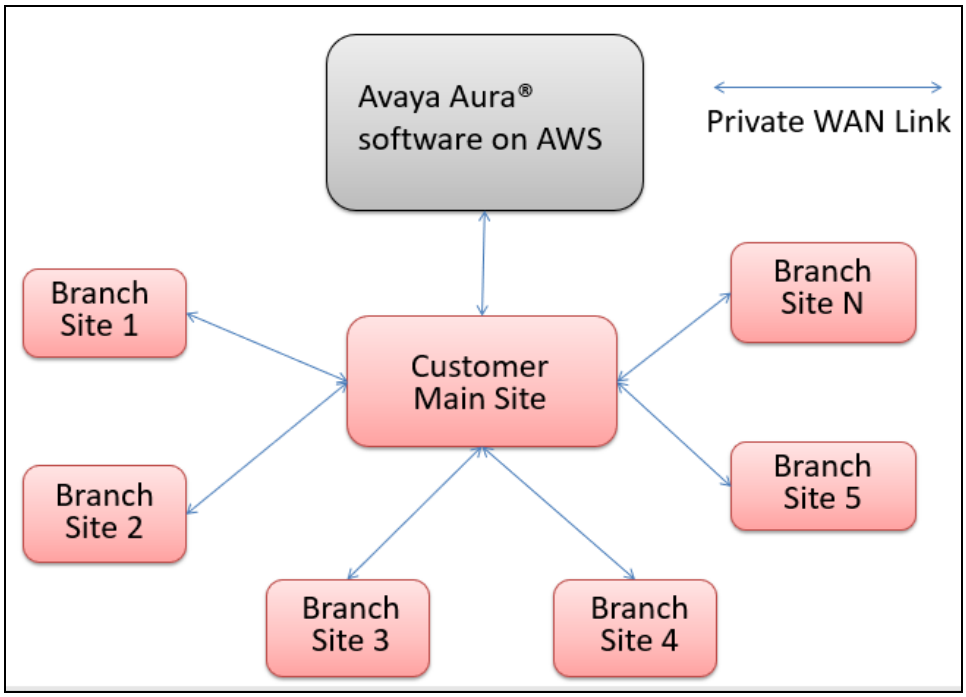
1. MPLS from Data service provider which will connect all the customer sites via MPLS network.

Figure 1 - Large number of Branch gateways via MPLS network



2. AWS direct connect at customer main site and use this customer main site to connect all the branches.

Figure 2 - Hub and spoke setup for large number of branch gateways



6.2.4. Network considerations for ASBCE

- ASCBE external interface should be placed in dedicated public subnet for remote SIP endpoints. AWS network ACLs should be configured to block traffic between ASBCE public subnet with all other subnets of a VPC.
- ASBCE internal interface should be placed in private subnet created for ASBCE.
- ASCBE management interface to be placed in dedicated private subnet.
- Configure separate AWS security group for external interface of ASBCE. It should allow required ports from remote endpoints on internet. For details about required ports, refer Avaya port matrix document.

6.3. Security

- Do not assign public IP to any of the Avaya Aura® software other than ASBCE.
- Do not allow all the traffic in AWS security groups. Allow only required network subnets and required ports. For details about port matrix for Avaya products, refer Avaya port matrix documents.

Follow the AWS security best practices. Refer AWS whitepaper for security best practices:

https://aws.amazon.com/whitepapers/aws-security-best-practices/

7. Use case for Avaya Aura® software on AWS

There are the following high level customer use cases for AWS based deployment of Avaya Aura® software:

1. Fresh deployment of Avaya Aura® software on AWS
2. Avaya Aura® software in hybrid mode
3. Migrating Avaya Aura® software on AWS

7.1. Fresh deployment of Avaya Aura® software on AWS

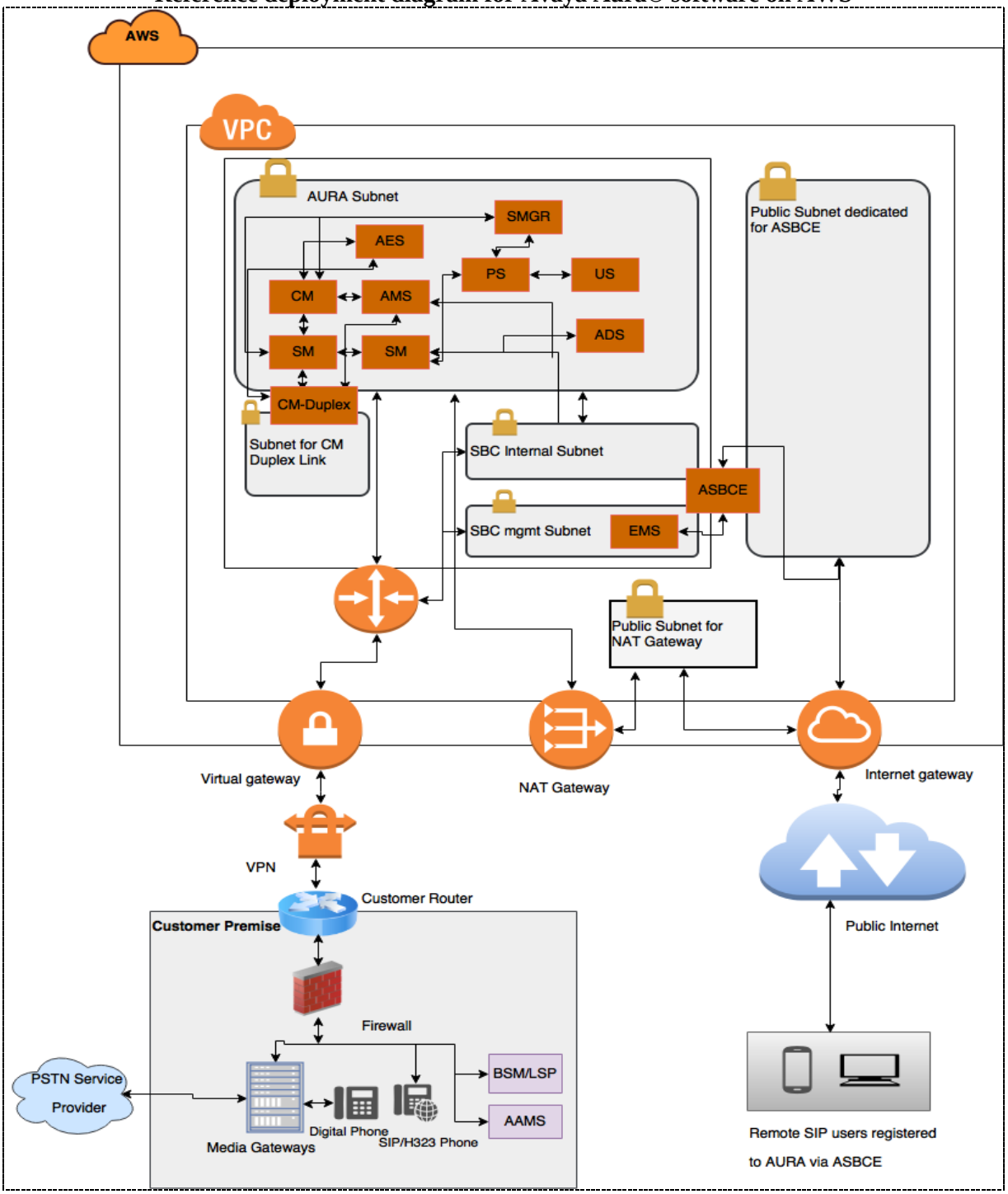
There are two options for fresh deployment of Avaya Aura® software on AWS.

1. Single Datacenter on AWS
2. Dual Datacenter on AWS

7.1.1. Single Datacenter on AWS

Use Case: Customer setting up new Avaya Aura® software with a single datacenter on AWS.

Reference deployment diagram for Avaya Aura® software on AWS



Following is the overall solution consideration for deployment of Avaya Aura® software on AWS using single Datacenter.

1. AWS Data center:

- Deploy Avaya Aura® software (SMGR, SM, CM, AAMS, AES, US, ADS, PS) on AWS VPC private subnet created for Avaya Aura® software. Refer Section-4 of this document for the list of software supported on AWS. Avaya Aura® Communication Manager second interface for CM-Duplex should be deployed in separate private subnet created for CM duplication link.
- Deploy ABSCE for remote SIP endpoints on DMZ.
- Create three subnets for ASBCE in AWS VPC. Two private subnets, one each for ASBCE Management interface and ASBCE internal interface and one public subnet for ASBCE external interface.
- AWS public elastic IP addresses are assigned to ASBCE external interface.

2. Customer premises:

- Connect customer enterprise network to AWS VPC using AWS Direct connect or VPN (AWS Direct connect is recommended).
- Protect customer network using customer firewall. (Note: H323 inspection must be disabled in customer firewall if H323 endpoints are used)
- There should not be any Network Address Translation (NAT) involved between customer on premises network and AWS VPC.
- Deploy Avaya Aura® Messaging, Avaya Aura® Conferencing and Avaya Media Gateways (G450, G430) on premises.
- Deploy LSP/BSMs on branch premises for local survivability.
- Deploy Avaya Aura® Media Server on premises for endpoints in enterprise network.
- Endpoints (SIP and H323) are in enterprise network and directly registered to Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

3. Remote Endpoints from public internet:

- Remote worker endpoints (SIP only) from internet are registered to Avaya Aura® Session Manager via ASBCE.
- ASBCE configured with Media un-anchoring for remote SIP endpoints calls. Media can flow directly between remote endpoints considering remote endpoints are directly reachable (behind the same NAT device) and there are similar capabilities between remote endpoints and ASBCE.

4. Trunk termination for public trunk calls:
- PSTN trunks are terminated on Media Gateways deployed on customer premises.
- SIP trunk terminated on ASBCE deployed on AWS (911, lawful intercept is customer responsibility)

5. Media Bandwidth consideration:

- Media traffic occupies significant bandwidth between customer location and AWS which results in higher bandwidth requirement from service provider as well as significant data transfer charges from AWS.
- It is recommended to use Media Gateways or Media server co-located with Endpoints for Media. This will ensure that Media does not flow between customer location and AWS for calls within enterprise network.
- Note: AWS uses IPsec for VPN connectivity which has IPsec overhead. This overhead is more significant if media packets are traversing across VPN tunnel.

7.1.2. Dual Data Center on AWS

Use Case: Customer setting up new Avaya Aura® software with primary and secondary datacenters on AWS.

Dual datacenters can be deployed across different AZs in a Region or they can be deployed across two different AWS Regions.

Note: It is recommended to refer AWS documentation for more information about AWS Regions and Availability Zones before planning Dual Data center solution.

7.1.2.1 Data centers across AZs

Each AWS region contains at least two Availability Zones. As each Availability Zone is isolated, it can be used to achieve datacenter redundancy. So, if failures occur, which affects one Availability Zone, datacenter at other Availability Zone will provide the redundancy for Avaya Aura® software.

Caution: As both datacenters are in single region, any outage of entire region cannot provide redundancy. To avoid such situation, it is recommended to use geo-redundant datacenters deployed across AWS regions. For more information about Datacenters across AWS regions, refer Section-7.1.2.2.

1. AWS Primary Data center:

- AWS Availability Zone (Let's say 1a) will act as a primary datacenter.
- Deploy primary Avaya Aura® software (SMGR, SM, CM, AMS, AES, US, ADS, PS) on Availability Zone 1a.
- Deploy ABSCE for remote SIP endpoints on DMZ in Availability Zone 1a.

2. AWS Secondary Data center:

- Different AWS Availability Zone (Let's say 1b) of the same AWS Region will act as a secondary datacenter.
- Deploy Geo redundant Avaya Aura® software (SMGR, SM, ESS, AMS, AES, ADS, PS) on Availability Zone 1b.
- Deploy ABSCE for remote SIP endpoints on DMZ in Availability Zone 1b.

Other on premises deployment and consideration for remote SIP endpoints, Trunk termination, and media bandwidth recommendation will remain same as mentioned in single datacenter section 7.1.1.

Advantages:

- It is easy to manage AWS infrastructure due to use of only single region for dual data center solution.
- Only single VPC is required.
- As both data centers are in same AWS region, data transfer charges between datacenters are very trivial.
- Very low latency between datacenters.
- No need to create and manage separate VPN to connect two datacenters as both are in same AWS VPC

Disadvantage:

- As both datacenters are in single region, any outage of entire region cannot provide redundancy.

7.1.2.2 Data centers across regions

Each AWS region is a separate geographic area and completely independent. Datacenters can be deployed across two different AWS regions to achieve the redundancy. So, if an outage occurs in an AWS region, the datacenter at the other region will provide redundancy for Avaya Aura® software.

There are AWS charges for data transfer between AWS regions. For more information on Data transfer charges, refer to AWS documentation for Data transfer pricing.

Note: It is customer's responsibility to ensure network connectivity between AWS regions.

1. AWS Primary Data center:

- Select one AWS region that will act as a primary datacenter.
- Deploying Avaya Aura® software (SMGR, SM, CM, AMS, AES, US, ADS, PS) on AWS region1.
- Deploying ABSCE for remote SIP endpoints on DMZ in AWS region1.

2. AWS Secondary Data center

- Select different AWS region that will act as a secondary datacenter.
- Deploying Avaya Aura® software (SMGR, SM, ESS, AMS, AES, ADS, PS) AWS region2.
- Deploying ABSCE for remote SIP endpoints on DMZ in AWS region2.

Other deployment for on premises and consideration for remote SIP endpoints, trunk termination, and media bandwidth recommendation will remain the same as mentioned in single datacenter section 7.1.1.

However, there are the following disadvantages of using two different regions for dual data centers compared to using two different Availability Zones of same region:

- AWS Data transfer charges between regions.
- Customer has to manage two different AWS regions which are independent.
- Customer needs to create and manage network connection between VPCs in two different AWS regions.
- Higher latency between datacenters.

7.2. Hybrid deployment of Avaya Aura® software

Avaya Aura® software is supported in hybrid mode between customer premises and AWS public cloud.

Note: For hybrid deployment of Avaya Aura® software, the customer has to ensure quality of network related parameters like dedicated bandwidth, consistency, network latency, etc. Avaya recommends using AWS direct connect for all AWS based deployment.

There are following high level uses cases for running Avaya Aura® software in hybrid deployment mode.

1. Datacenters in Hybrid mode
2. Products in Hybrid mode

7.2.1. Datacenters in Hybrid mode

Use Case: Customer wants a dual datacenter solution with primary data center on premises and secondary data center on AWS.

- Customer enterprise network is connected to AWS VPC using AWS Direct connect or VPN (AWS Direct connect is recommended over VPN).
- Customer network is protected using on premises Firewall. (Note: H323 inspection must be disabled in customer firewall if H323 endpoints are used)
- There should not be any NAT involved between customer on premises network and AWS VPC.
- Avaya Aura® software (SMGR, SM, CM, AMS, AES, US, ADS, PS) for primary datacenter are deployed on customer premises.
- Deploying geo redundant Avaya Aura® software (SMGR, SM, ESS, AMS, AES, ADS, PS) for secondary datacenter on AWS VPC.
- Avaya Aura® Messaging, Avaya Aura® Conferencing and Avaya Media Gateways (G450, G430) deployed on premises.
- Primary ASBCE is deployed on customer premises and secondary ASBCE is deployed on AWS VPC for remote SIP endpoint.
- Avaya Aura® Media servers deployed on premises for endpoints in enterprise network.
- Endpoints (SIP and H323) are in enterprise network and directly registered to Avaya Aura® Session Manager and Avaya Aura® Communication Manager with on premises data center as primary and AWS datacenter as secondary
- Remote worker endpoints (SIP only) from internet are registered to Avaya Aura® Session Manager via ASBCE with on premises data center as primary and AWS datacenter as secondary.

7.2.2. Products in Hybrid Mode

Use Case: Customer wants to run Avaya Aura® software in hybrid mode between AWS datacenter and customer on premises datacenter.

Note: SM and PS are not supported in Hybrid mode as latency between SM and PS (Breeze) should not be more than 7 milliseconds.

Customer has flexibility to deploy Avaya Aura® software on premises or on AWS in any combination (except SM, PS) depending on customer business needs.
Just to mention one example, existing customer has a CM, SM, and SMGR deployed on-premises in New Jersey. They want to expand their operations in Seattle area. They want to add a new CM and SM to provide communication services in the Seattle branch. In order to avoid capital expenditure on new hardware and possibly the real estate, customer opts in for availing the infrastructure from AWS. Customer may deploy new CM and SM into AWS, and manage these instances deployed from the existing SMGR.

7.3. Migrating Avaya Aura® software on AWS

Use Case: Customer has Avaya Aura® software running on premises and wants to migrate to AWS.

Customer can migrate Avaya Aura® software running on VMware, AVP or System platform with 6.x or 7.x release to AWS. Customer can migrate all applications in single phase or in multiple phases by running applications in hybrid mode.

This section mentions high level guidelines for migrating Avaya Aura® software on AWS. Refer individual product documents for more detailed information, steps and limitations for migration of Avaya Aura® software.

Note:

- Migration of Avaya Aura® software on AWS required planning and downtime as network parameters may change on AWS.
- ASBCE migration is not supported as of now. However, customer can install new ASBCE on AWS and configure. Refer supported capacity of ASBCE on AWS before planning for ASBCE on AWS as ASBCE has reduced capacity on AWS compared to on premises based deployment.

License management:

Following are the use cases for managing licenses when an AWS supported application is migrated from Avaya Aura® Appliance Virtualization Platform on Avaya-provided server or from VMware in customer provided Virtualized Environment to AWS:

- If the WebLM service is moved from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to AWS, all applications that host licenses on that WebLM must regenerate the licenses as the WebLM service is also moved. In Release 7.1, AWS supports the WebLM that is integrated with System Manager.

- If the WebLM service is not moved from existing Appliance Virtualization Platform on Avaya provided server or from VMware in customer-provided Virtualized Environment to AWS, but only the AWS supported applications move to AWS, then you do not have to regenerate the license for those applications that move to AWS.

- If a customer is using standalone WebLM on Appliance Virtualization Platform on Avaya provided server or on VMware in customer-provided Virtualized Environment and the customer wants to move the Licensing Services to AWS, then all the licenses need to migrate to the centralized System Manager Release 7.1 with integrated WebLM in AWS and the supported AWS applications that move need to regenerate the license files.

Following are the use cases for migrating Avaya Aura® software on AWS.

1. Migrating entire solution from Customer Premises to AWS
2. Phase Migration from Customer Premises to AWS

1. Migrating entire solution from Customer Premises to AWS

Use Case: Customer wants to migrate all Avaya Aura® software from customer premises to AWS public cloud.

Customer will need to arrange for extra licenses for migrating all Avaya Aura® software on AWS public cloud.

Recommended approach is to create entire core Avaya Aura® software solution with 7.1 releases on AWS. Complete the basic configuration and provide the required licenses. Ensure that the setup is ready before starting the migration. Take the appropriate downtime as migration to AWS requires few configuration changes related to IP addresses once data migration is done. Migrate the data of individual applications from on premises to AWS.

Following is the high-level procedure for migrating Avaya Aura® software solution on AWS cloud.

- Create AWS environment and connect AWS datacenter with existing customer datacenter (AWS direct connect is recommended). Refer Secion-3 of this document as well as AWS documentation for guidelines on AWS environment and connectivity.
- Create the fresh Avaya Aura® software setup on AWS while keeping the on premises setup up and running.
- Complete the initial configuration of Avaya Aura® software applications and provide the required licenses.
- Take the required downtime for migrating Data on AWS.
- Migrate the configuration of on premises SMGR to AWS SMGR using SMGR data migration utility. Refer SMGR document for migration of SMGR.
- Update the SMGR configuration with new IP addresses for all the elements and entities like SM, PS, CM etc. deployed on AWS.
- Migrate the data of other Avaya Aura® software on AWS and update them with the new IP address of SMGR.
- Update the CM node name configuration with required IP addresses like updating the security module IP address of SM, AMS IP address, ESS IP address, etc.
- Update the configuration of AES with the new IP address of CM.
- Update the configurations for all the on premises components like AAM, AAC, Media gateways, BSM/LSP etc. with the new IP addresses of the elements on AWS.
- Update the required configuration of other services like DNS, DHCP, Avaya utility services with the new IP addresses of AWS elements so the endpoints can be migrated to AWS servers
- Ensure that all elements are properly replicated and synchronized with SMGR.
- Ensure that all the entity links, trunks are up, media gateways and media servers are in service with CM on AWS.

2. Phased Migration from Customer Premises to AWS

Use Case: Customer wants to migrate Avaya Aura® software in different phases from customer premises to AWS public cloud.

As Avaya Aura® software can be deployed in hybrid mode (except SM and PS) between customer premises and AWS cloud, it is possible to perform migration of Avaya Aura® software in phases.

Following is the high-level procedure for migrating Avaya Aura® software on AWS cloud. However, customers can select any sequence for migrating Avaya Aura® software as Hybrid mode deployment is supported.

- Create AWS environment and connect AWS datacenter with existing customer datacenter (AWS direct connect is recommended). Refer Secion-3 of this document as well as AWS documentation for guidelines on AWS environment and connectivity.
- First migrate the standby components on AWS like standby SMGR, ESS.
- Deploy new SMGR on AWS and migrate the data from on premises SMGR. Update the configuration of all other elements with new IP address of SMGR.
- If customer moves the licensing services to AWS integrated in SMGR 7.1 on AWS, then all the licenses needs to be regenerated or migrated.
- Migrate SM and Breeze cluster for PS together on AWS (Standalone PS over Breeze). Update the SMGR configuration with new IP addresses of SM, Breeze and PS. Update the SM secmod IP address in CM node name and in required places for SIP endpoints.
- Migrate CM on AWS. Update the new IP address of CM in SMGR, AES, Media gateways, Media servers and in required places for H323 endpoints.
- Install the standalone AAMS on AWS. (Note: Refer capacity of AAMS on AWS before migrating AAMS from on premises to AWS as AAMS has different capacity on AWS compared to on-premises based deployment).

8. Guidelines on Cost Estimation

Note: This section (including example shown) is limited to provide guidance on how to use AWS monthly calculator to estimate the cost. Avaya is not responsible for anything relating to its use. Refer to AWS documents for correct up to date details on pricing.

8.1. AWS Pricing overview:

AWS offers you a pay-as-you-go approach for pricing for cloud services. With AWS you pay only for the individual services you need, for as long as you use them, and without requiring long-term contracts or complex licensing. AWS pricing is similar to how you pay for utilities like water or electricity. You only pay for the services you consume, and once you stop using them, there are no additional costs or termination fees.

AWS provides simple online monthly calculator for Estimate your monthly bill. Following is the link for AWS monthly calculator.

https://calculator.s3.amazonaws.com/index.html

The following AWS services need to be considered for Avaya Aura® software to estimate the AWS monthly cost:

1. Amazon EC2
2. Amazon S3
3. Amazon VPC
4. AWS Direct Connect
5. AWS Support

If you are using any additional AWS services, then they need to be considered for estimating the AWS monthly cost. However, for Avaya Aura® software, no additional AWS services are required.

Amazon EC2 provides various billing options for reserved instances which provide you with a discount compared to On-Demand pricing. With reserved instances, you pay for the entire term regardless of actual use. You can choose to pay for your reserved instance upfront, partially upfront, or monthly, depending on the payment option specified for the reserved instance.

Choose your billing option for Amazon EC2 instances from available options. Reserved instances are recommended for long term production systems while on demand is suitable for lab use and short team trials. The following are a few details for On-demand and reserved EC2 instances. For the latest and more details, refer to AWS documents on EC2 pricing.

On-Demand:

`With On-Demand instances, you pay for compute capacity by per hour or per second depending on which instances you run. No longer-term commitments or upfront payments are needed. You can increase or decrease your compute capacity depending on the demands of your application and only pay the specified per hourly rates for the instance you use.

On-Demand instances are recommended for:

- Users that prefer the low cost and flexibility of Amazon EC2 without any up-front payment or long-term commitment
- Applications with short-term, spiky, or unpredictable workloads that cannot be interrupted
- Applications being developed or tested on Amazon EC2 for the first time

Reserved instances:

Reserved instances provide you with a significant discount compared to On-Demand instance pricing. In addition, when reserved instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.

For applications that have steady state or predictable usage, reserved instances can provide significant savings compared to using On-Demand instances.

Reserved instances are recommended for:

- Applications with steady state usage
- Applications that may require reserved capacity
- Customers that can commit to using EC2 over a 1-year or 3-year term to reduce their total computing costs

8.2. Estimate cost using AWS monthly calculator:

List down following estimated items, which will be used to feed AWS monthly calculator.

1. List down number of EC2 machines to be deployed on AWS with their required AWS instance type and hard disk volumes. Also decide on Billing Option for EC2.
2. Estimate the intra region data transfer, number of elastic public IPs and data transfer over internet using public IPs. Public elastic IP is only needed for ASBCE.
3. Estimate the S3 storage used for storing OVAs.
4. List down the required AWS direct connect ports and speed of the direct connect ports.
5. Estimate the Data transfer over AWS direct connect.
6. List the number of VPN connections required.
7. Estimate the Data transfer over VPN connections.
8. Estimate the Data transfer over NAT Gateway.
9. Consider the intended AWS support plan.
10. List down the usage of other AWS services if any (Not required for Avaya Aura® software)

Once the above information is ready, just fill the details inside AWS monthly calculator for estimating the AWS monthly cost. The following section explains how to calculate cost with a simple example.

Example:

Let us take the simple example of Avaya Aura® software with single Data center deployed on AWS with SMGR, SM, CM Simplex, CM Duplex and ASCBE. This example is limited to provide guidance on how to use AWS monthly calculator to estimate the cost.

Open the AWS simple monthly calculator using following link:

https://calculator.s3.amazonaws.com/index.html

Click on “Reset All” button to reset all the fields in calculator before filling the estimated data.

On the service Tab, click the “Amazon EC2” tab. On this page, you can fill details about Amazon EC2 instances, Amazon EC2 dedicated Hosts, Amazon EBS volumes and Data Transfer.

Note: In this page, do not fill in the Data Transfer estimated over Direct connect and VPN as they would be filled in respective page of Direct connect and VPC.

Choose the appropriate AWS region where EC2 instances are going to be deployed.

Add the amazon EC2 instances for SMGR, SM, CM Simplex, and ASBCE with appropriate instance type under Amazon EC2 Instances. Also add the Amazon EBS volumes for SMGR, SM, CM Simplex, CM Duplex and ASBCE under Amazon EBS volume. Add two Amazon EC2 Dedicated hosts of type C4 per CM Duplex pair under the Amazon EC2 Dedicated Hosts.

Enter the Intra-Region Data Transfer amount under the Data Transfer. Add one elastic IP address per ASBCE. Also add estimated Data Transfer Out and Data Transfer In from/to ASBCE's external interface.

Click on "Amazon S3" under Services Tab and enter the Storage amount under Standard Storage. For Avaya Aura® software, Amazon S3 storage is required to store OVAs.

Click "AWS Direct Connect" under Service Tab to add direct connect port. Enter the number of ports, port speed, Location and estimated Data transfer over direct connect.

Click "Amazon VPC" under Service Tab to add the number of VPN connections and number of NAT Gateways connections along with respective Data Transfer.

Click "AWS Support" under Service Tab. Choose region and select intended support plan.

Finally click on the "Estimate of Your Monthly Bill" Tab adjacent to Service Tab to see the summary of estimated monthly bill. You can save the calculated link and share it by clicking "Save and Share" Button. Monthly calculation can also be exported to CSV by clicking "Export to CSV" button.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com