PUBLIC

SAP Adaptive Server Enterprise on AWS 16.0 SP03 PL07

Document Version: 1.0 – 2019-06-12

Quick Start Guide for BYOL Versions of SAP ASE on AWS

THE BEST RUN

Content

1 Overview

You can create an SAP ASE server on Amazon Web Services (AWS) by supplying your existing SAP ASE license.

The SAP ASE Bring Your Own License (BYOL) Amazon Machine Image (AMI) in the AWS Marketplace provides EC2 instances with certified operating system versions with the required operating system patches and software pre-installed. The BYOL model is an excellent way to begin migrating your existing on-premises data to the cloud.

The BYOL version of SAP ASE Server Enterprise version 16.0 SP03 PL07 on AWS runs on the following platform:

- Microsoft Windows Server 2016

The AMI provided by SAP was built from the following base AMI, which was available as of June 12, 2019, and contains fixes for the Meltdown and Spectre vulnerabilities that were included as of June 12, 2019:

- Microsoft Windows Server 2016 Base (ami-06bee8e1000e44ca4)

You should, however, watch for any new patches released by either AWS or your operating system vendors for these vulnerabilities and apply them as needed. Test the patches on a separate instance before applying them on a production instance to ensure that their installation does not break the application.

The BYOL version of SAP ASE supports almost all sizes and types available on AWS. However the recommended configuration is an `m5.4xlarge` with IO1 type storage for data devices. The SAP ASE AMI running on M5 instances with NVMe storage provides better database performance when compared to similar classes of EC2 types.

> **i Note**
>
> Use T2 instances only for testing and development purposes; do not use them in production environments.

Use the AWS pricing calculator at http://calculator.s3.amazonaws.com/index.html?key=calc-66EED67E-8369-42F2-A19F-495BE8840EE6 ➦ to understand the associated costs.

2 Prerequisites

There are a number of prerequisites to running the BYOL version of SAP ASE on AWS.

You must have:

Prerequisite	Description
An AWS account.	You are responsible for operating your own AWS account. Create an account at https://aws.amazon.com/ if you do not yet have one. Completing the account registration requires that you have a credit card.
The license required to use SAP ASE	Obtain your SAP ASE license through SAP, then download your license file from SAP Support Portal at https://support.sap.com/en/my-support/keys.html.
A key pair to secure the access to your AWS instance.	Make sure to make a note of the key name and store your `*.pem` file when prompted. Without the key pair, you cannot connect to your instance via SSH or Remote Desktop Connection (RDC, on Windows). Key pairs are region-specific. Make sure you create the key pair in the same AWS region in which you will later create your AWS instance. See *Amazon EC2 Key Pairs* in the Amazon EC2 *User Guide for Linux Instances* at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/index.html for information about creating a key pair.
An Amazon Virtual Private Cloud (VPC).	For details about creating your Amazon VPC for launching AWS instances, see the Amazon VPC document athttps://docs.aws.amazon.com/vpc/latest/userguide/index.html . AWS VPCs are virtual private networks you define for your resources. When you create your instance, you specify the VPC in which your instance runs. Generally, VPCs contain instances launched within it. These instances are isolated from the outside world; however, they can share information and connect to each other. You can communicate directly with your instance running on this VPC from your data center using SSH. You may use either the default Amazon VPC or configure your own when you deploy an instance. Often, users select the default VPC because it offers faster deployment. In this case, the user need not be concerned with their instance's

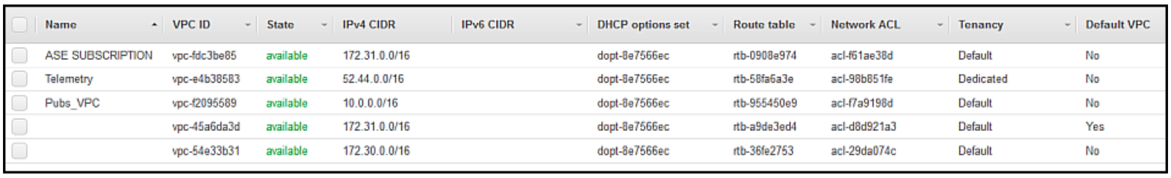
Prerequisite	Description
	visibility to other instances deployed in the default VPC. See Determine the Default VPC and Its Subnet [page 5] You can use the default VPC and the auto-generated security group (`SAP Adaptive Server Enterprise-16-0 SP03 PL06-AutogenByAWSMP-1`) or create your own. See Create Your Own VPC [page 7]
A Subnet	See Create Your Subnet [page 7]
An Internet Gateway	See Create Your Internet Gateway [page 9]
A Route Table	See Create Your Route Table [page 10]
A Security Group	See Create a Security Group [page 11]
An Elastic Network Interface (ENI)	See Create Your Elastic Network Interface (ENI) [page 12]

2.1 Determine the Default VPC and Its Subnet

Log in to AWS to determine your default VPC

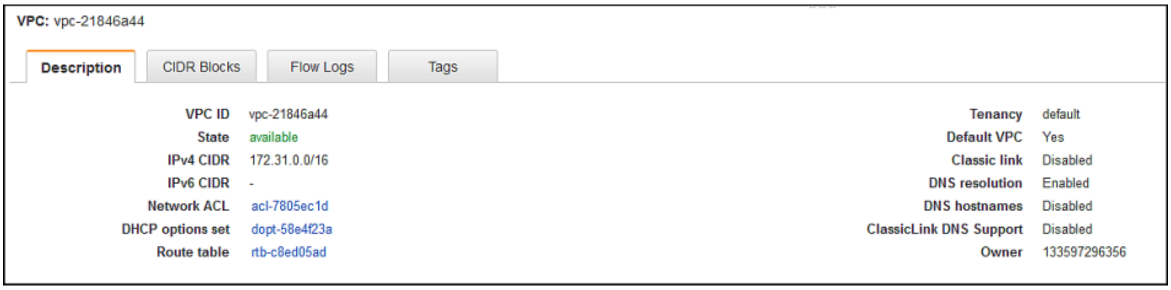
Procedure

1. From the *Services* page, select *VPC* (under the *Networking & Content Delivery* heading).
2. Select *Your VPCs* from the *VPC Dashboard*.
3. A value of *Yes* in the *Default VPC* column indicates the default VPC (vpc-45a6da3d in this example):



□	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table	Network ACL	Tenancy	Default VPC
□	ASE SUBSCRIPTION	vpc-fdc3be85	available	172.31.0.0/16		dopt-8e7566ec	rtb-0908e974	acl-f61ae38d	Default	No
□	Telemetry	vpc-e4b38583	available	52.44.0.0/16		dopt-8e7566ec	rtb-58fa6a3e	acl-98b851fe	Dedicated	No
□	Pubs_VPC	vpc-f2095589	available	10.0.0.0/16		dopt-8e7566ec	rtb-955450e9	acl-f7a9198d	Default	No
□		vpc-45a6da3d	available	172.31.0.0/16		dopt-8e7566ec	rtb-a9de3ed4	acl-d8d921a3	Default	Yes
□		vpc-54e33b31	available	172.30.0.0/16		dopt-8e7566ec	rtb-36fe2753	acl-29da074c	Default	No

   Make a note of the value for the *VPC ID* for the default VPC. You will use this VPC ID for your CFT when you configure your instance.
4. Verify the *DNS hostnames* line in the *Description* tab is set to *Enabled* for this VPC.



VPC: vpc-21846a44

Description | CIDR Blocks | Flow Logs | Tags

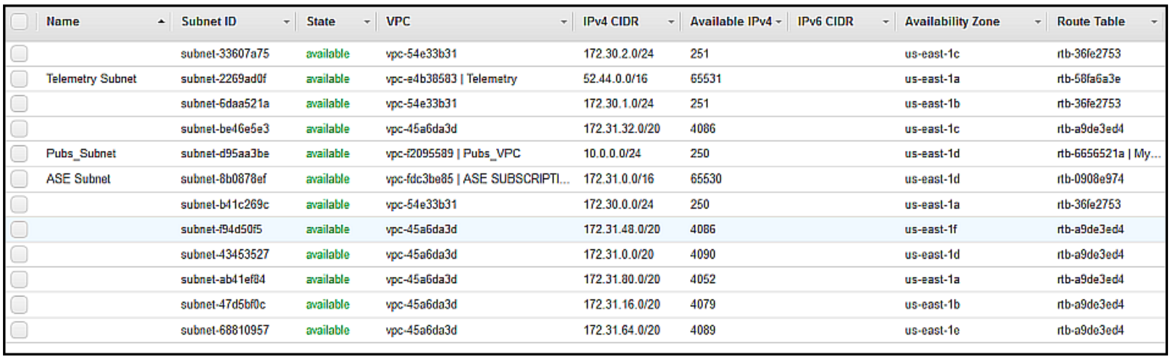
VPC ID	vpc-21846a44	Tenancy	default
State	available	Default VPC	Yes
IPv4 CIDR	172.31.0.0/16	Classic link	Disabled
IPv6 CIDR	-	DNS resolution	Enabled
Network ACL	acl-7805ec1d	DNS hostnames	Disabled
DHCP options set	dopt-58e4f23a	ClassicLink DNS Support	Disabled
Route table	rtb-c8ed05ad	Owner	133597296356

If it is not:

1. Select *Actions* > *Edit DNS hostnames*.
2. Check the box for *enable*.
3. Click *Save*.
4. Click *Close*.

See *DNS Support in Your VPC* on https://docs.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-hostnames for more information about enabling and disabling DNS hostnames.

5. Select *Subnets* from the *VPC Dashboard*.
6. Identify the VPC ID listed on the *VPC* column that is associated with the default VPC, and make a note of the subnet associated with this VPC (there may be many of them):



☐	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Route Table
☐		subnet-33607a75	available	vpc-54e33b31	172.30.2.0/24	251		us-east-1c	rtb-36fe2753
☐	Telemetry Subnet	subnet-2269ad0f	available	vpc-e4b38583 | Telemetry	52.44.0.0/16	65531		us-east-1a	rtb-58fa6a3e
☐		subnet-6daa521a	available	vpc-54e33b31	172.30.1.0/24	251		us-east-1b	rtb-36fe2753
☐		subnet-be46e5e3	available	vpc-45a6da3d	172.31.32.0/20	4086		us-east-1c	rtb-a9de3ed4
☐	Pubs_Subnet	subnet-d95aa3be	available	vpc-f2095589 | Pubs_VPC	10.0.0.0/24	250		us-east-1d	rtb-6656521a | My...
☐	ASE Subnet	subnet-8b0878ef	available	vpc-fdc3be85 | ASE SUBSCRIPTI...	172.31.0.0/16	65530		us-east-1d	rtb-0908e974
☐		subnet-b41c269c	available	vpc-54e33b31	172.30.0.0/24	250		us-east-1a	rtb-36fe2753
☐		subnet-f94d50f5	available	vpc-45a6da3d	172.31.48.0/20	4086		us-east-1f	rtb-a9de3ed4
☐		subnet-43453527	available	vpc-45a6da3d	172.31.0.0/20	4090		us-east-1d	rtb-a9de3ed4
☐		subnet-ab41ef84	available	vpc-45a6da3d	172.31.80.0/20	4052		us-east-1a	rtb-a9de3ed4
☐		subnet-47d5bf0c	available	vpc-45a6da3d	172.31.16.0/20	4079		us-east-1b	rtb-a9de3ed4
☐		subnet-68810957	available	vpc-45a6da3d	172.31.64.0/20	4089		us-east-1e	rtb-a9de3ed4

You will use this subnet when you configure your instance.

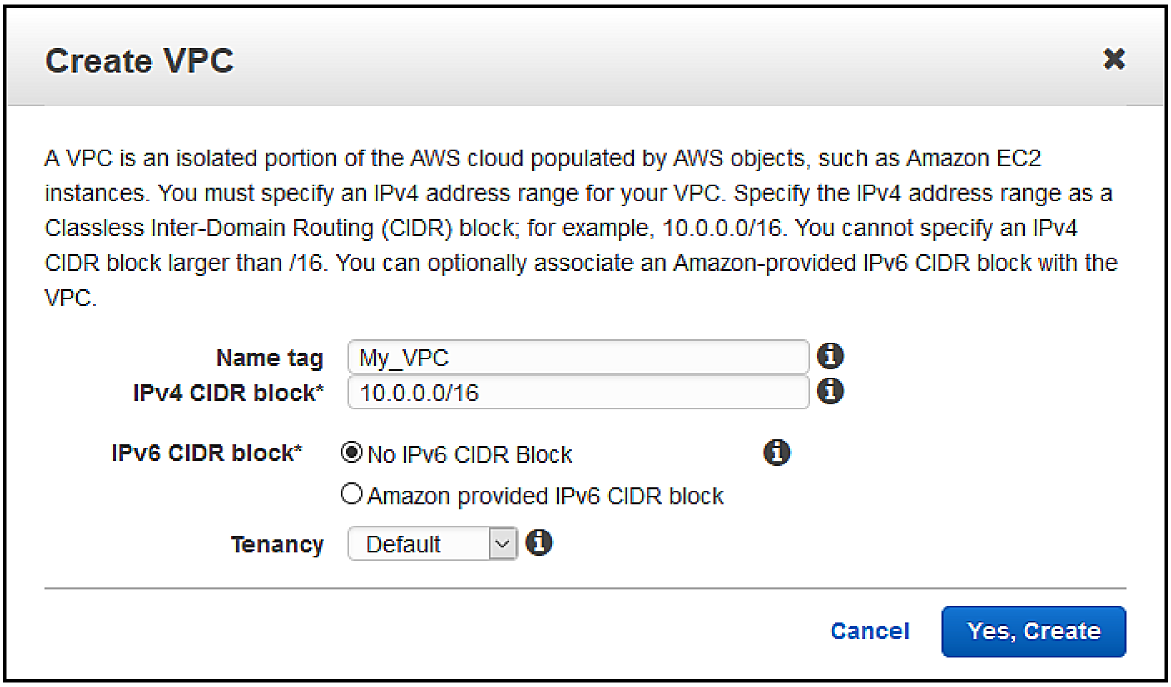
> **i Note**
>
> Subnets have internal IP addresses with their CIDR. Make a note of this IP address because they are used to limit the number of instances deployed in each subnet. For example, the number of instance deployable within the IPv4 CIDR for IP address 172.31.16.0/20 is:
>
> [2^{12} – (4 reserved instances) = 4,092]

2.2 Create Your Own VPC

Use the VPC dashboard to create your own VPC for SAP ASE on AWS

Procedure

1. From the *Services* page, select *VPC* from the *Networking & Content Delivery* section of your AWS console.
2. Select *Your VPCs* from the *Virtual Private Cloud* section of the *VPC Dashboard*.
3. Select *Create VPC*:



Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag: My_VPC

IPv4 CIDR block*: 10.0.0.0/16

IPv6 CIDR block*: ● No IPv6 CIDR Block ○ Amazon provided IPv6 CIDR block

Tenancy: Default

4. Enter the *Name tag* and *IPv4 CIDR block*.
5. Click *Yes, Create*.

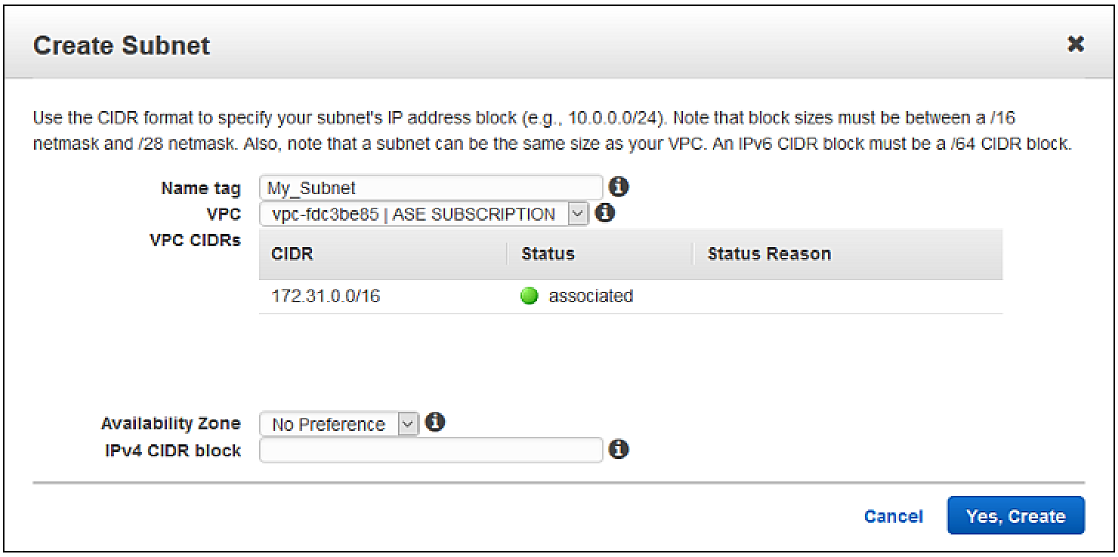
2.3 Create Your Subnet

Use the VPC dashboard to create a subnet for SAP ASE on AWS.

Procedure

1. From the *Services* page, select *VPC* (under the *Networking & Content Delivery* heading).

2. Select *Subnets* from the *VPC Dashboard*.
3. Select *Create subnet*:



Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: My_Subnet

VPC: vpc-fdc3be85 | ASE SUBSCRIPTION

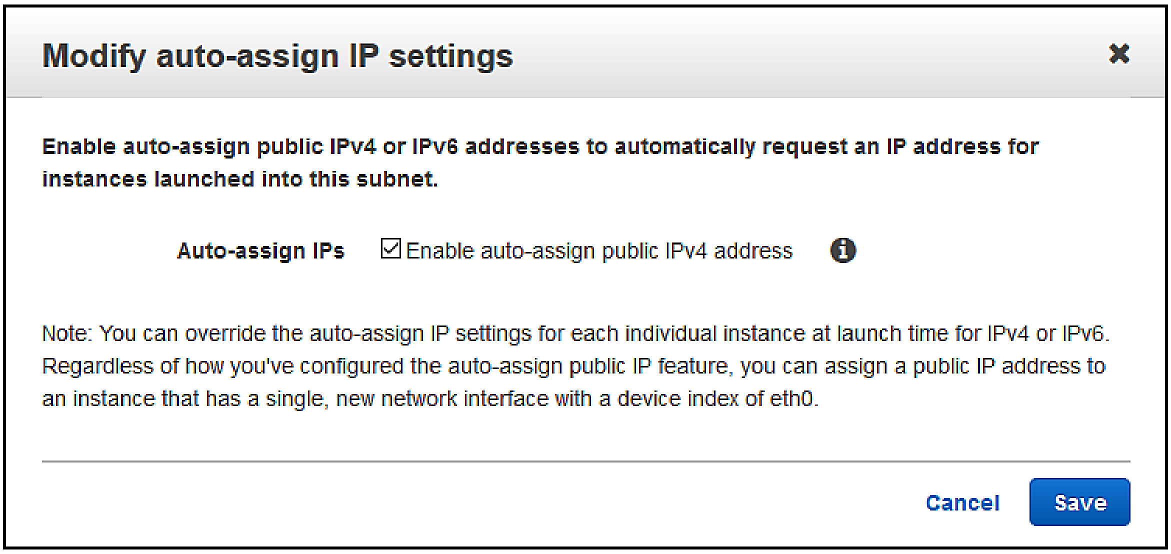
VPC CIDRs:

CIDR	Status	Status Reason
172.31.0.0/16	● associated	

Availability Zone: No Preference

IPv4 CIDR block:

4. Enter the *Name tag*, select the VPC, and enter a value for the *IPv4 CIDR block*.
5. Click *Create*.
6. Select the subnet you just created from the subnet list.
7. Select *Actions* > *Modify auto-assign IP settings*.
8. Select the check box for *Enable auto-assign public IPv4 address*:



Modify auto-assign IP settings

Enable auto-assign public IPv4 or IPv6 addresses to automatically request an IP address for instances launched into this subnet.

Auto-assign IPs ☑ Enable auto-assign public IPv4 address

Note: You can override the auto-assign IP settings for each individual instance at launch time for IPv4 or IPv6. Regardless of how you've configured the auto-assign public IP feature, you can assign a public IP address to an instance that has a single, new network interface with a device index of eth0.

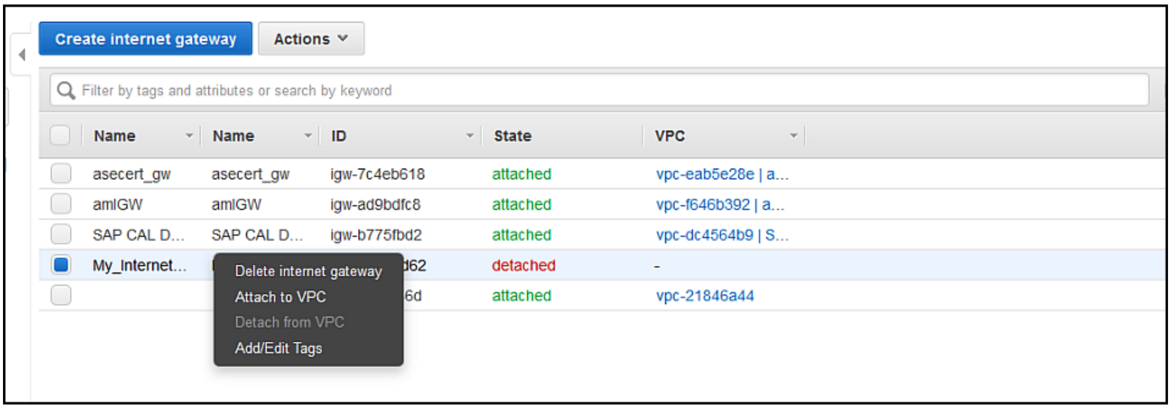
9. Click *Save*.

2.4 Create Your Internet Gateway

Use the VPC dashboard to create your own Internet gateway for SAP ASE on AWS.

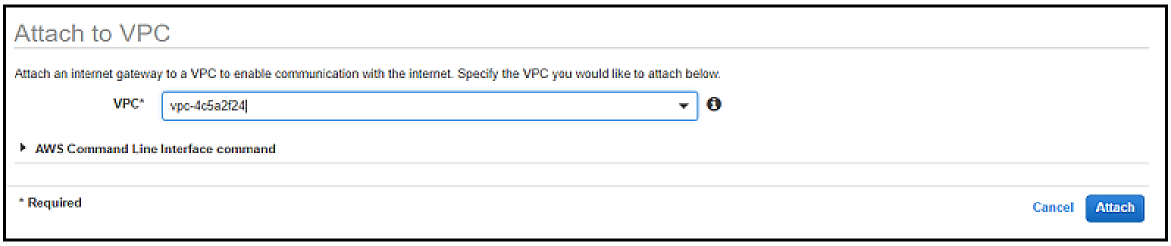
Procedure

1. From the *Services* page, select *VPC* (under the *Networking & Content Delivery* heading).
2. Select *Internet Gateways* from the *VPC Dashboard*.
3. Select *Create internet gateway*.
4. Enter the *Name Tag*.
5. Click *Create*, then *Close*.
6. Right-click on the internet gateway you just created and select *Attach to VPC*



	Name	Name	ID	State	VPC
□	asecert_gw	asecert_gw	igw-7c4eb618	attached	vpc-eab5e28e | a...
□	amIGW	amIGW	igw-ad9bdfc8	attached	vpc-f646b392 | a...
□	SAP CAL D...	SAP CAL D...	igw-b775fbd2	attached	vpc-dc4564b9 | S...
☑	My_Internet...		d62	detached	-
□			6d	attached	vpc-21846a44

7. Select the VPC and click *Attach*:



Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

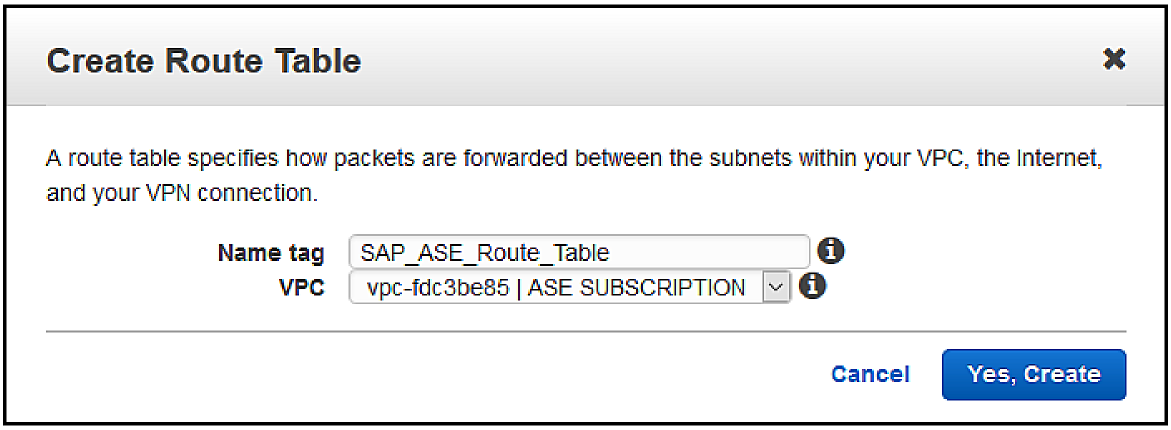
VPC* vpc-4c5a2f24

2.5 Create Your Route Table

Use the VPC dashboard to create your route table for SAP ASE on AWS.

Procedure

1. From the *Services* page, select *VPC* (under the *Networking & Content Delivery* heading).
2. Select *Route Tables* the *VPC Dashboard*.
3. Click *Create route table*.
4. Enter the *Name Tag* and select the VPC:



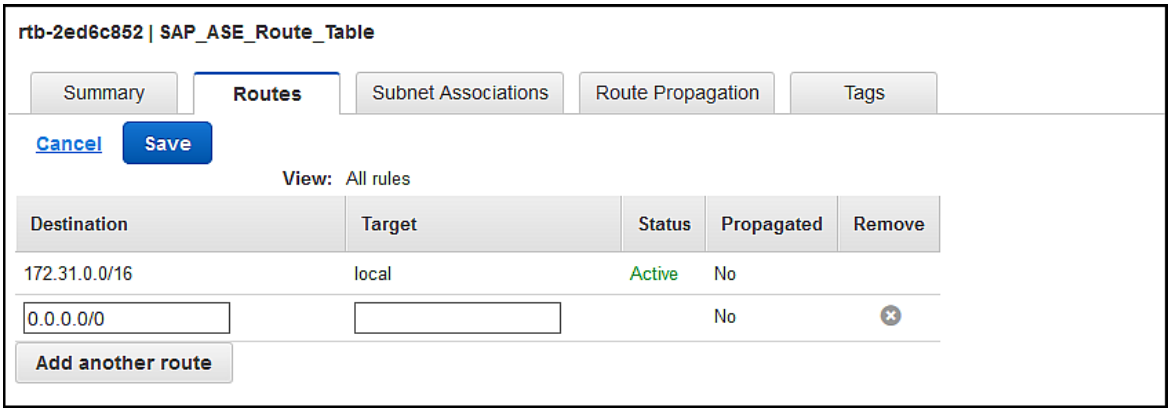
Create Route Table

A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

Name tag: SAP_ASE_Route_Table

VPC: vpc-fdc3be85 | ASE SUBSCRIPTION

5. Click *Yes, Create*.
6. Select the route you just created in the *Route Tables* page.
7. Select the *Routes* tab.
8. Select *Edit routes*
9. Select *Add route* to enter another destination and target:

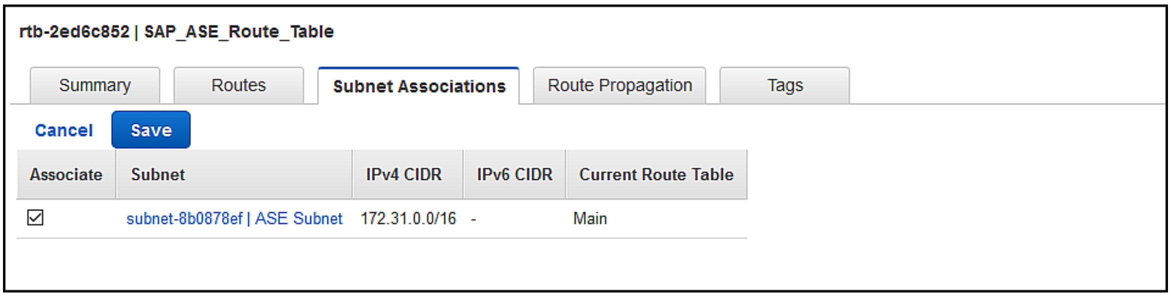


rtb-2ed6c852 | SAP_ASE_Route_Table

View: All rules

Destination	Target	Status	Propagated	Remove
172.31.0.0/16	local	Active	No	
0.0.0.0/0			No	⊗

10. Select the *Subnet Associations* tab.
11. Select *Edit subnet associations* to associate your subnet with a route table:



rtb-2ed6c852 | SAP_ASE_Route_Table

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
☑	subnet-8b0878ef | ASE Subnet	172.31.0.0/16	-	Main

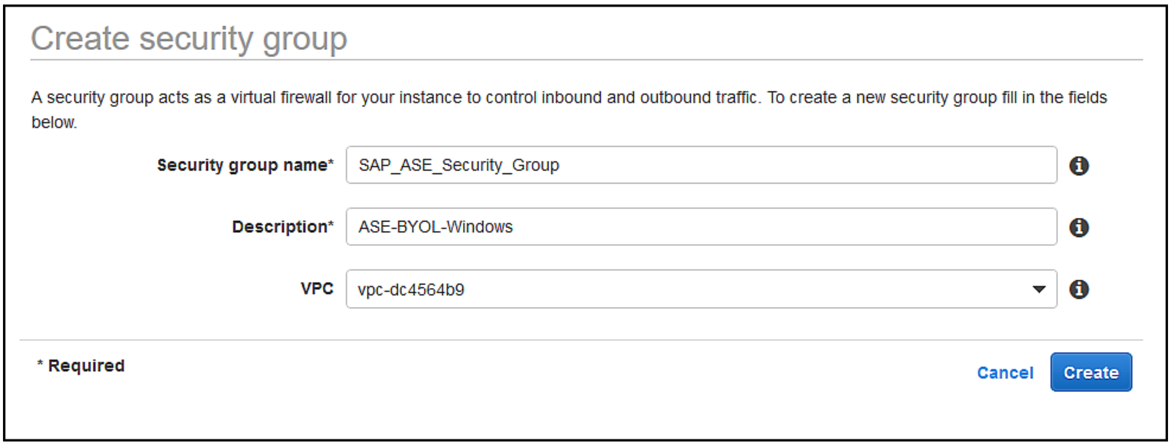
12. Click *Save* to keep the changes.

2.6 Create a Security Group

Use the VPC dashboard to create a security group for SAP ASE on AWS.

Procedure

1. From the *Services* page, select *VPC* (under the *Networking & Content Delivery* heading).
2. Select *Security Groups* from the *VPC Dashboard*.
3. Select *Create Security Group*.
4. Enter the *Security group name*, and *Description*, and *VPC* for the security group:



Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group fill in the fields below.

Security group name* SAP_ASE_Security_Group

Description* ASE-BYOL-Windows

VPC vpc-dc4564b9

* Required

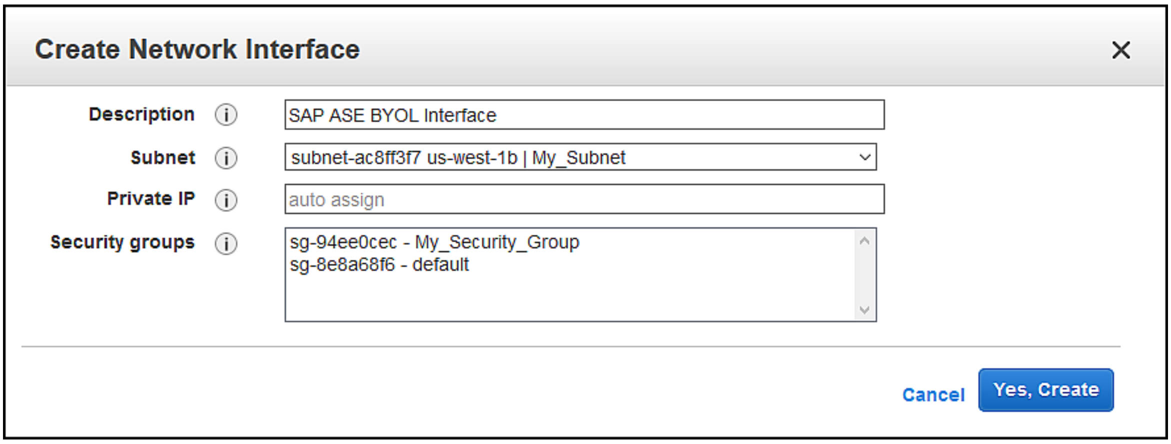
5. Click *Create*.
6. Select the security group you just created from the list of all security groups.
7. Select the *Inbound Rules* tab.
8. Click *Edit rules* and add ports 3389, 4283, and 5000 to the *Port Range* along with their *Source* and *Description*.
9. Click *Save*.

2.7 Create Your Elastic Network Interface (ENI)

Use the VPC dashboard to create your elastic network interface (ENI) for SAP ASE on AWS.

Procedure

1. Select *Network Interfaces* from the *Network & Security* section of the *EC2 Dashboard*.
2. Select *Create Network Interface*.
3. Enter the *Description*, *Subnet*, *Private IP*, and *Security Group*:



Create Network Interface

Description: SAP ASE BYOL Interface

Subnet: subnet-ac8ff3f7 us-west-1b | My_Subnet

Private IP: auto assign

Security groups: sg-94ee0cec - My_Security_Group
sg-8e8a68f6 - default

4. Click *Yes, Create*.
5. Select your network interface from the list on the *Network Interface* page and enter a *Name* tag.

3 Creating Your BYOL Instance

Configure the SAP ASE EC2 instance by providing information in the AWS wizard.

Procedure

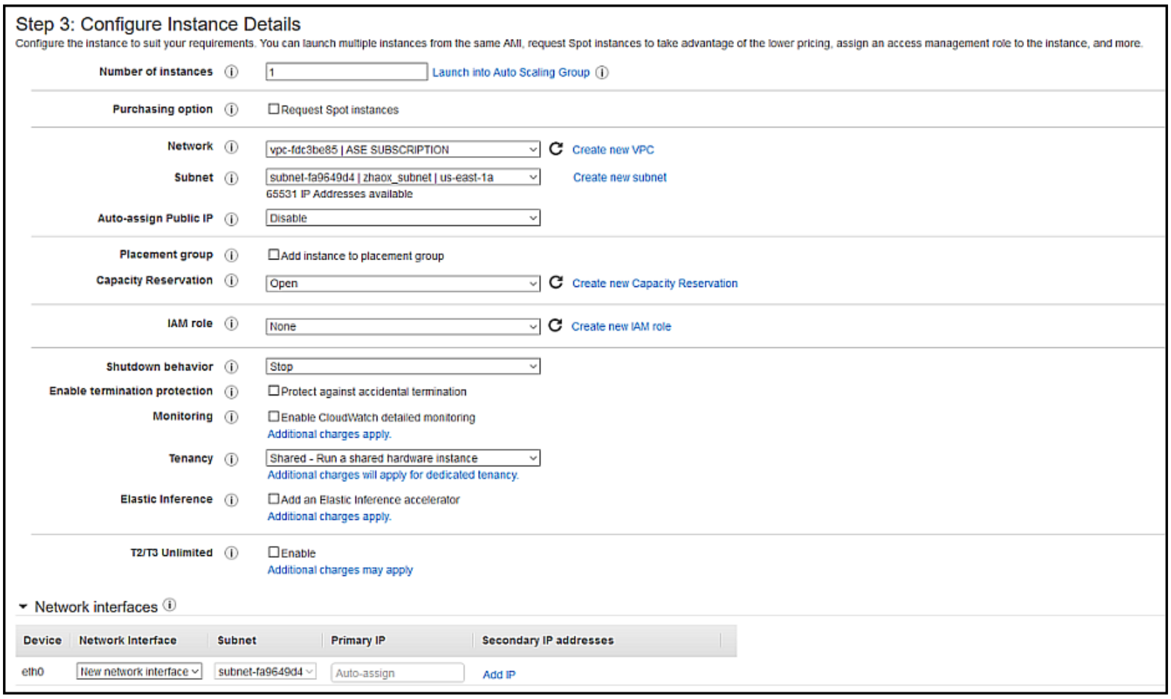
1. Log on to Amazon Market Place: https://aws.amazon.com/marketplace
2. Search for “SAP Adaptive Server Enterprise."
3. Select the version.
4. Select the *Region*, *Fulfillment Option*, and the *EC2 instance type* under *Pricing Information*, which comprise the bundled choice. The `m5.4xlarge` option should be sufficient for most users. If necessary, you can change the instance size later in the AWS console.
5. Click *Continue to Subscribe*.
6. Click *Continue to Configuration*.
7. Select the *Fulfillment Option*, *Software Version*, and the *Region* and click *Continue to Launch*.
8. Select *Choose Action* > *Launch through EC2*, and click *Launch*.
9. Select the *Instance Type* (use instances of size t2 for development and testing purposes only, and not for production).
10. You can either review the configuration and launch the EC2 instance, or configure the instance details by selecting:
    - *Review and Launch* – review the EC2 configuration and select *Launch* to create the EC2 instance. Select *Previous* to return to the *Choose an Instance Type* page.
    - *Next: Configure Instance Details* – a series of windows steps your through your EC2 configuration. Perform the steps described here: Configure the Instance Details [page 13].

3.1 Configure the Instance Details

Enter your configuration information for the instance.

Procedure

1. *Configure Instance Details* – make selections to configure the instance for your environment:



Step 3: Configure Instance Details

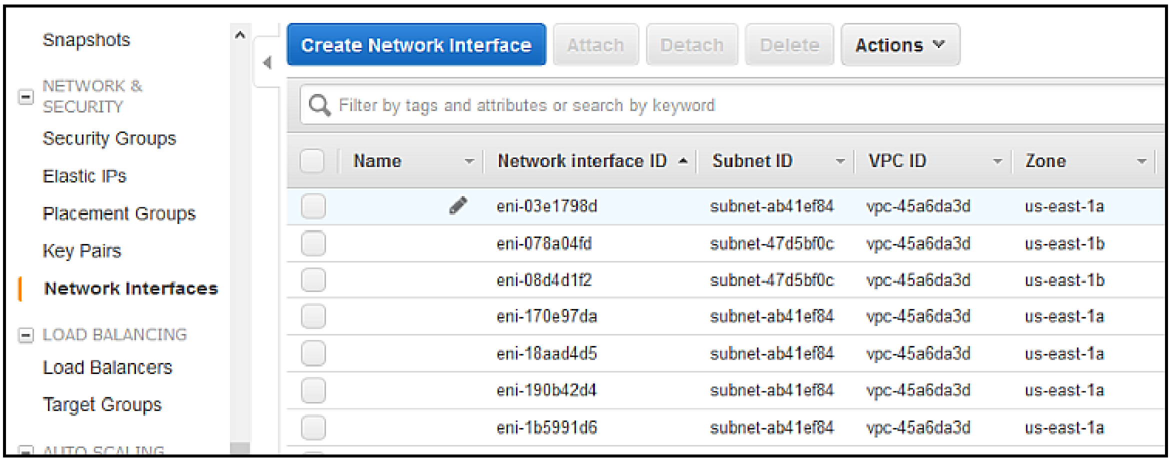
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1 — Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-fdc3be85 | ASE SUBSCRIPTION — Create new VPC
Subnet	subnet-fa9649d4 | zhaox_subnet | us-east-1a — Create new subnet 65531 IP Addresses available
Auto-assign Public IP	Disable
Placement group	□ Add instance to placement group
Capacity Reservation	Open — Create new Capacity Reservation
IAM role	None — Create new IAM role
Shutdown behavior	Stop
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.
Elastic Inference	□ Add an Elastic Inference accelerator Additional charges apply.
T2/T3 Unlimited	□ Enable Additional charges may apply

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interface	subnet-fa9649d4	Auto-assign	Add IP

To view the available VPC and ENI combinations, select *EC2 Dashboard* > *Network & Security* > *Network Interfaces*:



Name	Network interface ID	Subnet ID	VPC ID	Zone
	eni-03e1798d	subnet-ab41ef84	vpc-45a6da3d	us-east-1a
	eni-078a04fd	subnet-47d5bf0c	vpc-45a6da3d	us-east-1b
	eni-08d4d1f2	subnet-47d5bf0c	vpc-45a6da3d	us-east-1b
	eni-170e97da	subnet-ab41ef84	vpc-45a6da3d	us-east-1a
	eni-18aad4d5	subnet-ab41ef84	vpc-45a6da3d	us-east-1a
	eni-190b42d4	subnet-ab41ef84	vpc-45a6da3d	us-east-1a
	eni-1b5991d6	subnet-ab41ef84	vpc-45a6da3d	us-east-1a

Select:

- *Review and Launch* to create the EC2 instance
- *Next: Add Storage* to continue the configuration.

2. *Add Storage* – configure the EC2 storage, adding additional storage for data devices. You will mount these volumes later to `/opt/sap/data` (`E:\data` on Windows) for your database devices.

   Do not select the *Delete on Termination* option for data and log volumes: Accidentally terminating an instance leads to data loss. By default, *Delete on Termination* is enabled for the root volume containing the operating system, and for the SAP volume containing the SAP ASE software. This configuration may be acceptable if you configure all SAP ASE and database devices to be on other volumes (see Build and Configure SAP ASE on Linux [page 22] and Build and Configure SAP ASE on Windows [page 25]). However, you should set the *Delete on Termination* option appropriately for your specific use case.

This instance comes with the root volume and `/opt/sap` or `D:\SAP` (on Windows) pre-configured with gp2 EBS volumes. Use these storage types for data devices:

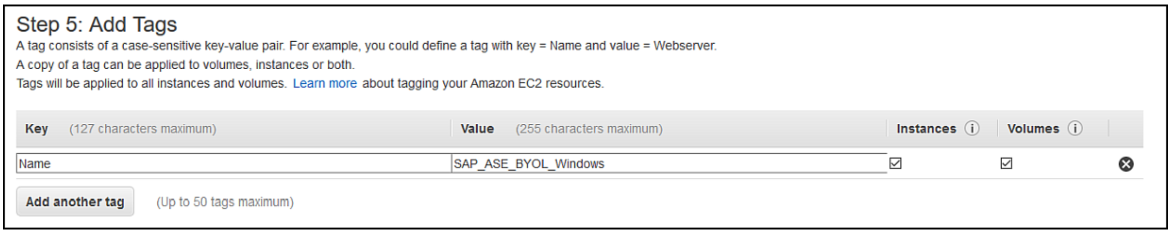
- Production – use io1
- Development and test – use gp2

You can add more storage after you launch the instance.

Select:

- *Review and Launch* to create the EC2 instance
- *Next: Add Tags* to continue the configuration.

3. *Add Tags* – add any tags that help identify your AWS resources (for example, a *Name* tag).



Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	Instances	Volumes	
Name	SAP_ASE_BYOL_Windows	☑	☑	⊗

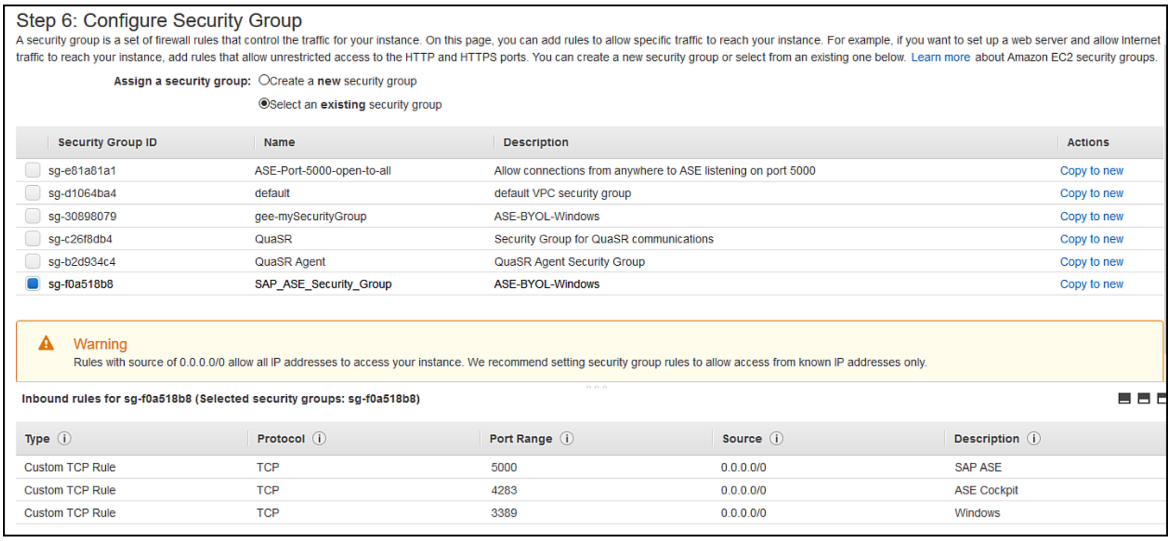
Select:

- *Review and Launch* to create the EC2 instance
- *Next: Configure Security Group* to continue the configuration.

4. *Configure Security Group* – BYOL instances are configured with:

- Linux – port 22 opened for 0.0.0.0/0 as their source address for all SSH logins from any IP address.
- Windows – port 3389 opened for 0.0.0.0/0 as their source address for all TCP logins using RDC from any IP address.

Change this to an IP address range that limits access to your host:



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

	Security Group ID	Name	Description	Actions
□	sg-e81a81a1	ASE-Port-5000-open-to-all	Allow connections from anywhere to ASE listening on port 5000	Copy to new
□	sg-d1064ba4	default	default VPC security group	Copy to new
□	sg-30898079	gee-mySecurityGroup	ASE-BYOL-Windows	Copy to new
□	sg-c26f8db4	QuaSR	Security Group for QuaSR communications	Copy to new
□	sg-b2d934c4	QuaSR Agent	QuaSR Agent Security Group	Copy to new
■	sg-f0a518b8	SAP_ASE_Security_Group	ASE-BYOL-Windows	Copy to new

⚠ Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Inbound rules for sg-f0a518b8 (Selected security groups: sg-f0a518b8)

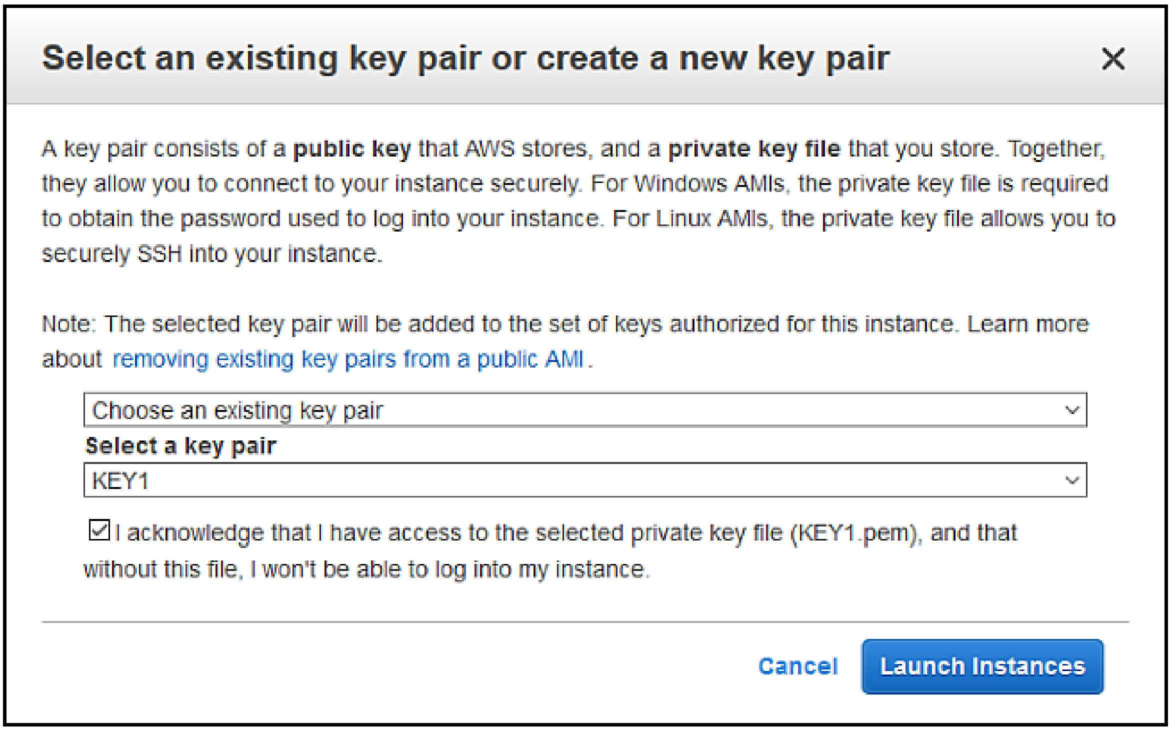
Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	5000	0.0.0.0/0	SAP ASE
Custom TCP Rule	TCP	4283	0.0.0.0/0	ASE Cockpit
Custom TCP Rule	TCP	3389	0.0.0.0/0	Windows

Based on the ports you selected for configuring SAP ASE, open up the ports like 5000, 4283, and so on for the required IP address range. See Default Settings in the SAP ASE Configuration Guide for UNIX for default SAP ASE port numbers here Default Settings.

Select *Review and Launch*.

5. Review your configuration and click *Launch* to create the EC2 instance or *Previous* to make changes.

6. Establish a key pair. Create a new or provide the name of an existing key pair. Key pairs are necessary to create an SSH or RDC (on Windows) connection to your instance. See nullnull*Amazon EC2 Key Pairs* in the Amazon EC2 *User Guide for Linux Instances* at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/index.html for information about creating key pairs in AWS.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair

Select a key pair

KEY1

☑ I acknowledge that I have access to the selected private key file (KEY1.pem), and that without this file, I won't be able to log into my instance.

7. Select the check box, acknowledging that you must have a key pair to log in to your instance.

> **i Note**
>
> Key pairs are region-specific.

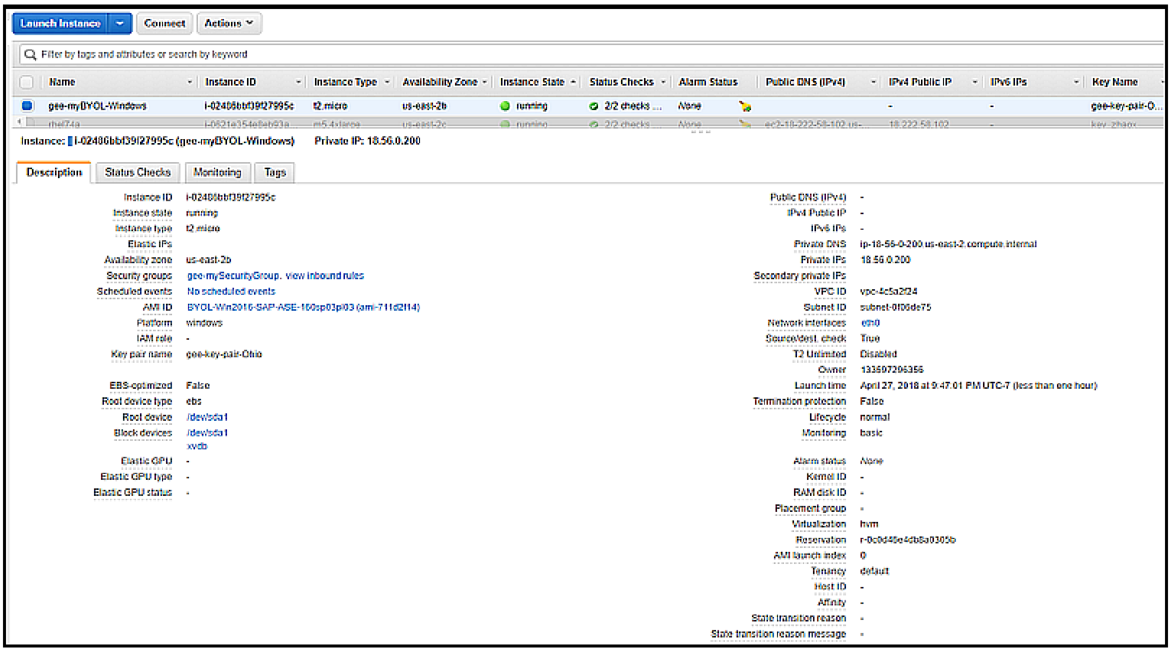
8. Click *Launch Instances*.

4 Post-Installation Configuration

Post-installation tasks include associating an Elastic IP address, configuring the security group, and uploading the license.

Procedure

1. Navigate to the *INSTANCES* > *Instances* tab on the *EC2 Dashboard* of the EC2 Management Console. Verify that the state of the AWS instance to which you want to connect is running:



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name
gee-myBYOL-Windows	i-02406bbf39f27995c	t2.micro	us-east-2b	running	2/2 checks ...	None		-	-	gee-key-pair-O...
rhel74a	i-0521a354e8eb93a...	m5.4xlarge	us-east-2c	running	2/2 checks ...	None	ec2-18-222-58-102.us-...	18.222.58.102	-	key_zhang...

Instance: i-02406bbf39f27995c (gee-myBYOL-Windows)   Private IP: 18.56.0.200

Instance ID	i-02406bbf39f27995c
Instance state	running
Instance type	t2.micro
Elastic IPs	
Availability zone	us-east-2b
Security groups	gee-mySecurityGroup. view inbound rules
Scheduled events	No scheduled events
AMI ID	BYOL-Win2016-SAP-ASE-160sp03p03 (ami-711d2f14)
Platform	windows
IAM role	-
Key pair name	gee-key-pair-Ohio
EBS-optimized	False
Root device type	ebs
Root device	/dev/sda1
Block devices	/dev/sda1 xvdb
Elastic GPU	-
Elastic GPU type	-
Elastic GPU status	-

Public DNS (IPv4)	-
IPv4 Public IP	-
IPv6 IPs	-
Private DNS	ip-18-56-0-200.us-east-2.compute.internal
Private IPs	18.56.0.200
Secondary private IPs	
VPC ID	vpc-4c5a2f24
Subnet ID	subnet-0f06de75
Network interfaces	eth0
Source/dest. check	True
T2 Unlimited	Disabled
Owner	133507296356
Launch time	April 27, 2018 at 9:47:01 PM UTC-7 (less than one hour)
Termination protection	False
Lifecycle	normal
Monitoring	basic
Alarm status	None
Kernel ID	-
RAM disk ID	-
Placement group	-
Virtualization	hvm
Reservation	r-0c0d40e4db8a0305b
AMI launch index	0
Tenancy	default
Host ID	-
Affinity	-
State transition reason	-
State transition reason message	-

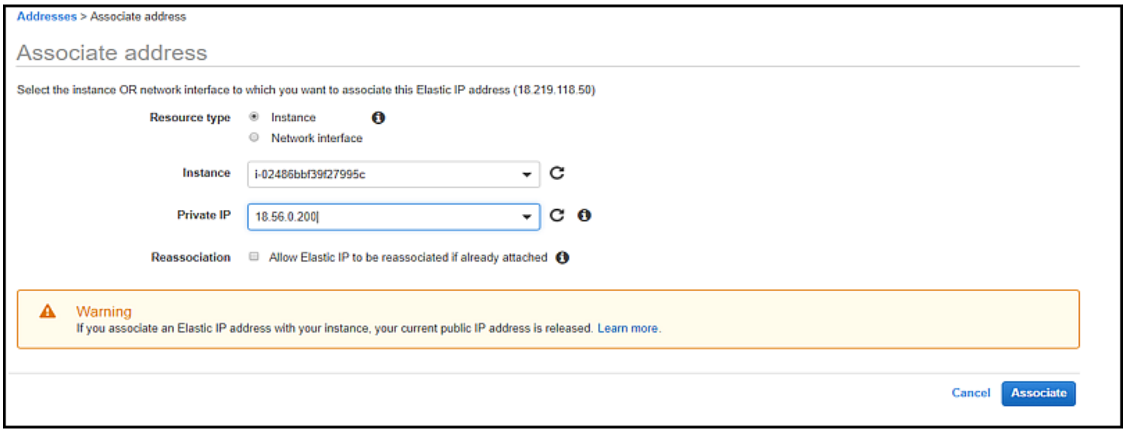
   If it is not running:

   1. Right-click on the instance.
   2. Select *Instance State* > *Start*.

2. Associate an Elastic IP address with the AWS instance. Elastic IP addresses ensure that you can connect to your instance with the same host name and IP address when it is restarted. See *Elastic IP Addresses* in the Amazon EC2 *User Guide for Linux Instances* at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html for more information about Elastic IP addresses. To associate an Elastic IP address with your instance:

   1. From the *EC2 Dashboard*, select *Elastic IPs* (under the *Network and Security* heading).
   2. Select the Elastic IP address that you want to associate with the AWS instance.
   3. Either right-click on the Elastic IP address and select *Associate*, or select *Actions > Associate*.
   4. Provide information for:
      - *Resource type* – select *Instance*

        - *Instance* – select the name of the instance you want this Elastic IP address associated with.
        - *Private IP* – select from the list.
    5. Indicate if you want to re-associate this Elastic IP address to this instance if it is already attached.
    6. Click *Associate*:



Addresses > Associate address

Associate address

Select the instance OR network interface to which you want to associate this Elastic IP address (18.219.118.50)

Resource type ● Instance ○ Network interface

Instance i-02486bbf39f27995c

Private IP 18.56.0.200

Reassociation □ Allow Elastic IP to be reassociated if already attached

Warning
If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more.

    7. Click *Close*.

    Make a note of the Elastic IP for future reference.

3. Select the *Network & Security* > *Security Groups* tab in the *EC2 Console*.
4. Create rules in your Security group that allow your TCP ports to be accessed (for example, 5000 for SAP ASE, 5001 for Backup Server, and 4283 for Cockpit). Restrict this group to a known set of IP addresses where your applications will be running.
5. Connect to your instance. See Log In To Your AWS EC2 Instance [page 20] for connection steps.
6. Switch to the user `sybase`:
    - Linux:
        1. Log in as the ec2 user.
        2. Issue:

```
sudo su - sybase
```

    - Windows:
        1. Log in as Administrator.
        2. Activate the `sybase` user and set the password.
        3. Log out.
        4. Log in again as the `sybase` user.
7. Run the `lmutil` to determine the host ID of your instance. For example:
    - Linux:

```
/opt/sap/SYSAM-2_0/bin/lmutil lmhostid
```

    - Windows:

```
D:\SAP\SYSAM-2_0\bin\lmutil.exe lmhostid
```

8. Obtain your SAP ASE license from SAP (see Keys at the SAP Support Portal Home at https://support.sap.com/en/my-support/keys.html for information about obtaining SAP licenses). Copy the license to the AWS instance in a file in the `/opt/sap/SYSAM-2_0/licenses` directory for Linux, or to the

D:\SAP\SYSAM-2_0\licenses directory for Windows. SAP ASE expects a license file with the .lic extension. The appropriate license is checked out after configuring and starting an SAP ASE server.

5 Log In To Your AWS EC2 Instance

You can connect to your AWS instance at the operating system level. For example, to change the default password of a user or to start or stop your SAP ASE server.

Log in on Linux

> **Note**
>
> Logging in to your EC2 instance requires a *.ppk file. See *Connecting to Your Linux Instance from Windows Using PuTTY* in the Amazon EC2 *User Guide for Linux Instances* at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html for more information about converting *.pem files to *.ppk files.

1. If necessary, download and configure the PuTTY and Pageant utilities.
2. Open PuTTY on your computer, and enter the connection information in the *Host Name* field in the format `ec2-user@<elastic_IP_address>` (for example, `ec2-user@170.168.127.89`*Connection* >) and enter the location of the *.ppk file for the key pair in the *SSH* > *Auth* > *Private key file for authentication* field.
3. Click *Open*. You are logged in to the EC2 instance as the user `ec2-user`.
4. Run the following to become user `sybase` for configuring SAP ASE (this uses `sudo` to log in as the `sybase` user and does not require a password):

   ```
   sudo su - sybase
   ```

   > **Note**
   >
   > The user `sybase` was created with a random password for installing SAP ASE on this instance. However, this login is denied because the `/etc/ssh/sshd_config` file includes this line:
   >
   > ```
   > DenyUsers sybase
   > ```
   >
   > You can change the password later for user `sybase`.

Log in on Windows

Initially logging in to your Windows instance requires that you:

1. Determine the Administrator password to connect to the Windows instance using RDC. Use this password to connect via RDC as described in the instructions in *Connecting to Your Windows Instance* in the Amazon EC2 *User Guide for Windows Instances* at https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/connecting_to_windows_instance.html .
2. Specify this password to connect to the instance and reactivate the `sybase` user:

1. Right-click on the Windows icon and select *Computer Management* on the Windows instance.
2. Select *Local Users and Groups* > *Users*.
3. Right-click the `sybase` user and select *Properties*.
4. If it is not already, clear the *Account is disabled* checkbox, then click *Apply*.
5. Right-click the *sybase* user, then select *Set Password*.
6. Click *Proceed* to acknowledge the warning.
7. Enter and confirm your new password.

> **i Note**
>
> After performing these post-installation steps, use RDC to log in to the Windows instance using the `sybase` user and the password you set here.

6 Build and Configure SAP ASE on Linux

Use response files to create SAP ASE on the Linux platform.

Procedure

1. Log in to Linux with the `ec2-user` key pair.
2. Become the root user:

   ```
   sudo su -
   ```

3. (Optional) If you want to use the simplified native access plan (SNAP) feature, disable the kernel's randomization security feature by performing the following as root:
   1. Edit the `/etc/sysctl.conf` file, adding this line to the end:

      ```
      kernel.randomize_va_space=0
      ```

   2. Run this command:

      ```
      /sbin/sysctl -p
      ```

4. Mount the data volumes you created in the Add Storage step here [page 13] under `/opt/sap/data`:
   1. Run `lsblk` to list the volumes. In this example, `xvdc` is the volume you created for database devices:

      ```
      #  lsblk
      NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
      xvda    202:0    0  20G  0 disk
      └─xvda1 202:1    0  20G  0 part /
      xvdb    202:16   0  10G  0 disk /opt/sap
      xvdc    202:32   0   8G  0 disk
      # ls -la /dev/disk/by-uuid/
      total 0
      drwxr-xr-x 2 root root 80 Mar 10 01:14 .
      drwxr-xr-x 4 root root 80 Mar 10 01:14 ..
      lrwxrwxrwx 1 root root 10 Mar 10 01:14 fa9cc700-a903-4f76-
      a587-3eeab0f95fc5 -> ../../xvdb
      lrwxrwxrwx 1 root root 11 Mar 10 01:14 fae07648-59ac-4fdb-8813-
      be968c6a6b54 -> ../../xvda1
      #
      ```

   2. Create a file system on the volume (this example uses an `ext4` volume type):

      ```
      # mkfs -t ext4 /dev/xvdc
      mke2fs 1.42.11 (09-Jul-2014)
      Creating filesystem with 2097152 4k blocks and 524288 inodes
      Filesystem UUID: f675b345-99b3-4e97-b021-fb08f824fc7c
      Superblock backups stored on blocks:
              32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
      Allocating group tables: done
      Writing inode tables: done
      Creating journal (32768 blocks): done
      Writing superblocks and filesystem accounting information: done
      #
      ```

3. Determine the `uuid` of the data volume:

   ```
   # ls -la /dev/disk/by-uuid/
   total 0
   drwxr-xr-x 2 root root 100 Mar 10 01:24 .
   drwxr-xr-x 4 root root  80 Mar 10 01:14 ..
   lrwxrwxrwx 1 root root  10 Mar 10 01:24 f675b345-99b3-4e97-b021-
   fb08f824fc7c -> ../../xvdc
   lrwxrwxrwx 1 root root  10 Mar 10 01:14 fa9cc700-a903-4f76-
   a587-3eeab0f95fc5 -> ../../xvdb
   lrwxrwxrwx 1 root root  11 Mar 10 01:14 fae07648-59ac-4fdb-8813-
   be968c6a6b54 -> ../../xvda1
   #
   ```

4. Add this volume information to the `/etc/fstab` file (this example adds volume `/opt/sap/data`):

   ```
   # cat /etc/fstab
   /dev/disk/by-label/ROOT / ext4 defaults 1 1
   UUID=fa9cc700-a903-4f76-a587-3eeab0f95fc5 /opt/sap ext4 defaults 0 2
   # echo "UUID=f675b345-99b3-4e97-b021-fb08f824fc7c /opt/sap/data ext4
   defaults 0 2" >> /etc/fstab
   # cat /etc/fstab
   /dev/disk/by-label/ROOT / ext4 defaults 1 1
   UUID=fa9cc700-a903-4f76-a587-3eeab0f95fc5 /opt/sap ext4 defaults 0 2
   UUID=f675b345-99b3-4e97-b021-fb08f824fc7c /opt/sap/data ext4 defaults 0 2
   # mount /opt/sap/data
   #
   ```

5. Become user `sybase` to configure SAP ASE:

   ```
   su - sybase
   ```

6. Edit the `srvbuild.adaptive_server.rs` response file (located in `/opt/sap/ASE-16_0/init/sample_resource_files/`) to point to the correct hostname, password, device sizes, and so on. Include the name of the device when you specify the path to the devices in the resource file (for example, `/opt/sap/data/master.dat`).

7. Use the `srvbuildres` utility with the response file you edited above to create the server, including the `srvbuildres -D` parameter to place SAP ASE configuration files outside of `<$SYBASE>`:

   ```
   /opt/sap/ASE-16_0/bin/srvbuildres -D /ase/config -r /opt/sap/ASE-16_0/init/
   sample_resource_files/srvbuild.adaptive_server.rs
   ```

   See "srvbuildres" in the SAP ASE *Utility Guide* at srvbuildres for information about running `srvbuildres`.

   > **i Note**
   >
   > Use the isql64 binary in `/opt/sap/OCS-16_0/bin` to connect if you are using `isql` to connect to the server. Some corporate firewalls may not allow you to connect to Amazon cloud. Communicate with your IT organization to resolve this.

8. SAP ASE is initially configured to accept any license. If served licenses are to be used and the license server contains licenses for multiple SAP ASE editions or different license types, use `sp_lmconfig` to specify the specific edition and license type. For example, to configure an SAP ASE Enterprise Edition licensed for Development and Test:

   ```
   sp_lmconfig "edition", "EE"
   go
   sp_lmconfig "license type", "DT"
   go
   ```

9. If required, install the SAP Host Agent. Some SAP ASE configurations (for example, HADR) require the SAP Host Agent. See *SAP Host Agent Installation* in at SAP Host Agent.
10. Edit the interfaces file to replace the `<hostname>` with the machine IP address. Use your Elastic IP address for the instance. On Linux, the interfaces file is in `$SYBASE/interfaces`.
11. Issue this from the command prompt:

    ```
    echo $LANG
    ```

    If the operating system does not return a value of POSIX for the LANG environment variable, issue this to set it to POSIX (this is on a C shell):

    ```
    setenv LANG POSIX
    ```

7 Build and Configure SAP ASE on Windows

Use Windows Remote Desktop Connection (RDC) to connect to your Windows instance.

Procedure

1. Mount the data volumes you created in the Add Storage step in Creating Your BYOL Instance [page 13] under `E:\data`. See instructions in *Making an Amazon EBS Volume Available for Use on Windows* in the Amazon EC2 *User Guide for Windows Instances* at https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ebs-using-volumes.html for mounting these volumes.
2. Modify the response files (located in `D:\SAP\ASE-16_0\sample\server`) for the servers you want to start for items such as hostname, password, device sizes, physical names, and so on. The response files available are:
    - `sybatch_ase.res` – SAP ASE
    - `sybatch_bs.res` – Backup Server
    - `sybatch_js.res` – Job Scheduler

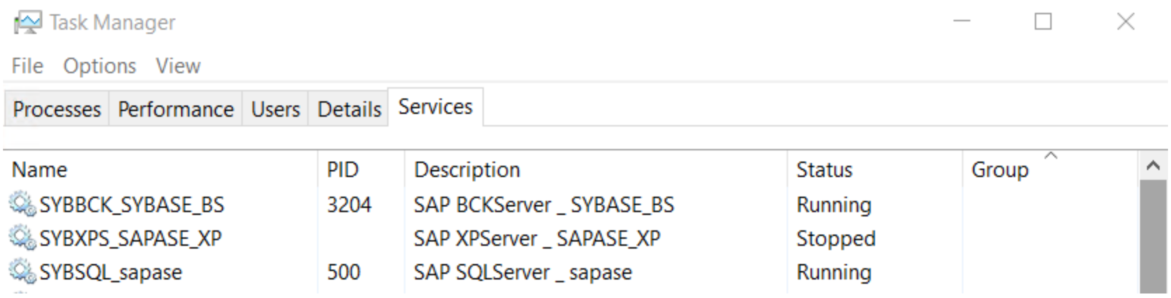
    XP Server does not require a response file.
3. Open a command prompt.
4. Run this command to set your environment variables:

    ```
    D:\SAP\SYBASE.bat
    ```

    The log files for the following step are saved in `E:\ase\config\ASE-16_0\init\logs`; make sure that the `E:\ase\config` directory exists. Verify that the log files do not contain any errors. If there are any failures, fix the issues and re-run the command.
5. Issue the `sybatch.exe` utility with the response files you edited above (include the `sybatch -D` parameter to place SAP ASE configuration files outside of `<$SYBASE>`):

    ```
    D:\SAP\ASE-16_0\bin\sybatch.exe -D E:\ase\config -r D:\SAP\ASE-16_0\sample
    \server\sybatch_ase.res
    ```

    Once the servers are running, the task manager displays their processes:

Name	PID	Description	Status	Group
SYBBCK_SYBASE_BS	3204	SAP BCKServer _ SYBASE_BS	Running	
SYBXPS_SAPASE_XP		SAP XPServer _ SAPASE_XP	Stopped	
SYBSQL_sapase	500	SAP SQLServer _ sapase	Running	

    See sybatch for more information about the utility.

6. SAP ASE is initially configured to accept any license. If served licenses are to be used and the license server contains licenses for multiple ASE editions, or different license types, use `sp_lmconfig` to specify the specific edition and license type. For example, to configure an SAP ASE Enterprise Edition licensed for Development and Test:

   ```
   sp_lmconfig "edition", "EE"
   go
   sp_lmconfig "license type", "DT"
   go
   ```

7. If required, install the SAP Host Agent. Some SAP ASE configurations (for example, HADR) require the SAP Host Agent. See SAP Host Agent Installation for more information.
8. Edit the interfaces file to replace the `<hostname>` with the machine IP address. Use your Elastic IP address for the instance. The interfaces file is at `%SYBASE%\ini\sql.ini` (if you included `sybatch -D` parameter, the interfaces file is at `D:\ase\config\ini\sql.ini` .

Next Steps

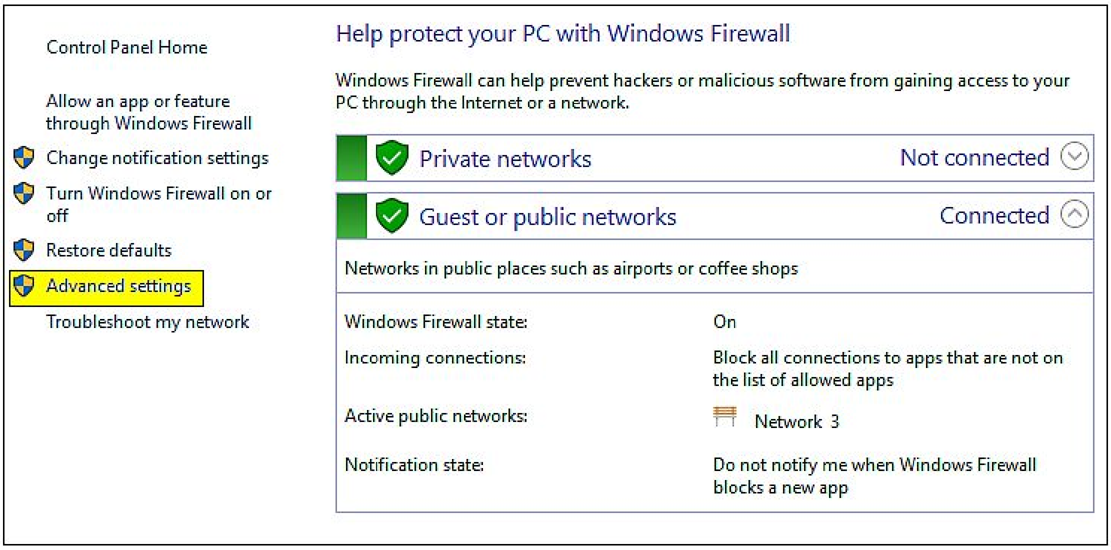
Configure your Windows AWS instance to allow remote connections. See Enabling AWS Windows Host Instance to Allow Connections [page 26] for information.

7.1 Enabling AWS Windows Host Instance to Allow Connections

By default, the firewall on an AWS Windows instance is enabled, blocking all incoming traffic. Configure your Windows AWS instance to allow remote connections to use specific port numbers to use applications like `isql` and ASE Cockpit to connect from an on-premises machine.

Procedure

1. Open the *Windows Firewall* application (find this by entering "Windows firewall" in the search window of your AWS instance) and go to *Advanced Settings*:



Control Panel Home

Allow an app or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

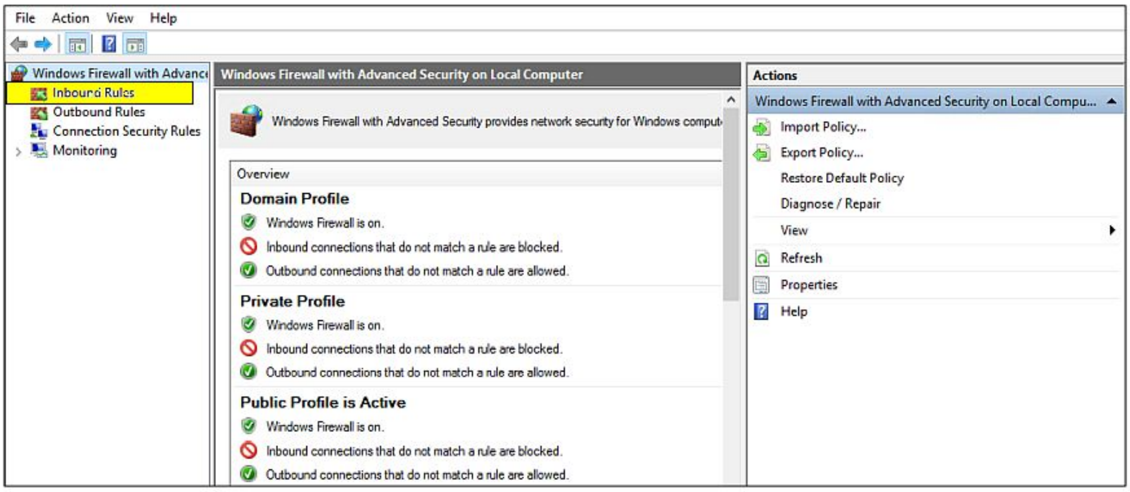
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Network 3
Notification state:	Do not notify me when Windows Firewall blocks a new app

2. In the *Inbound Rules* option in the *Advanced Settings* window, select *New Rule* in the *Actions* pane. This starts the *New Inbound Rule* wizard.



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows comput

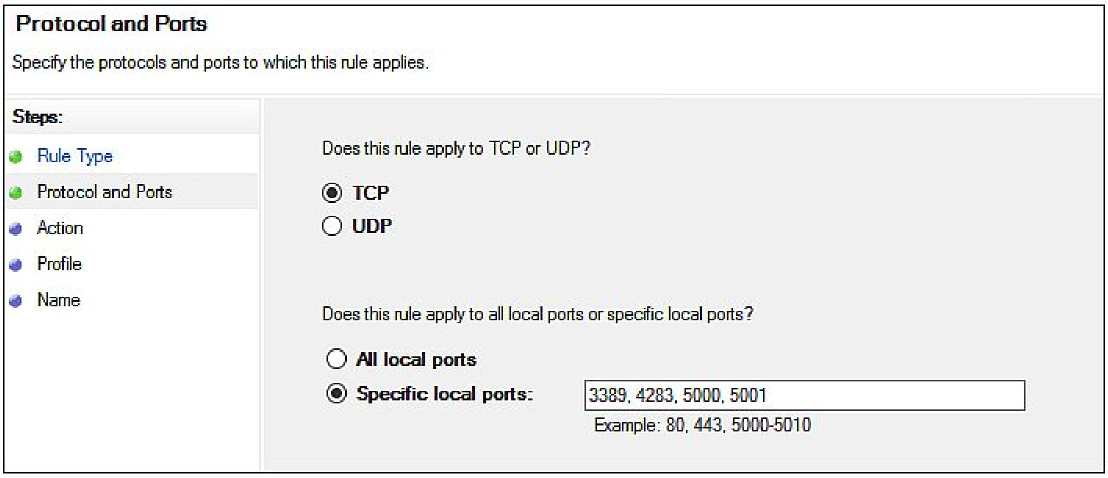
Overview

Domain Profile
- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile
- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active
- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

3. In the *Rule Type* step of the wizard, select *Port for the Rule Type* option in the *New Inbound Rule Wizard* and click *Next*.
4. In the *Protocol and Ports* step, specify the ports to which you want this rule to apply and click *Next*.



Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● TCP

○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports: 3389, 4283, 5000, 5001

Example: 80, 443, 5000-5010

5. In the *Action* step of the wizard, select *Allow the Connection* and click *Next*.
6. In the *Profile* step of the wizard, select the domain to which this rule applies and click *Next*.
7. In the *Name* step of the wizard, select the name of the rule and provide a description.
8. Click *Finish*. You can now connect from your on-premises machine using the Elastic IP address and the port number for SAP ASE.

8 Controlling Costs

You are responsible for operating your AWS account and paying your hosting costs.

To control your costs, stop your instance when you are not using it; you can quickly restart it when necessary.

To stop your instance, locate it in the AWS console, right-click the instance name and choose *Stop*. To start it again, choose *Start* from the menu instead.

Although AWS charges you very little for stopped instances, if you want to avoid monthly bills, you can terminate your instance so that it becomes permanently deleted. However, volumes are not deleted automatically, so make a note of any attached volumes that you want to delete.

To terminate your instance, locate it in the AWS console, right-click the instance name and choose *Terminate*. When you add EBS storage, do not select the *Delete on Termination* option for data and log volumes, so that accidentally terminating an instance does not lead to loss of data. When you terminate the instance, make sure you delete all associated EBS volumes that are not required.

AWS also provides tools to monitor your usage to better plan your budget. Choose *My Account / Console > Account Activity* from your menu on the top right corner of the screen to see your activity for the current month.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon ➦ : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
    - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
    - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon ➦: You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP