Installing Anti-Webshell V2.0 on AWS

Table of Contents

1. Product Overview

This document assumes that you have used AWS before and are familiar with AWS services. If you are new to AWS, see the Getting Started section of the AWS documentation. You should also be familiar with the following AWS technologies:

- Amazon VPC – The Amazon Virtual Private Cloud (Amazon VPC) service lets you provision a private, isolated section of the AWS Cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
- Amazon EC2 – The Amazon Elastic Compute Cloud (Amazon EC2) service enables you to launch virtual machine instances with a variety of operating systems. You can choose from existing Amazon Machine Images (AMIs) or import your own virtual machine images.
- AWS CloudFormation – AWS CloudFormation enables you to create and provision AWS infrastructure components reliably and predictably, using a JSON scripting environment. This Quick Start uses AWS CloudFormation templates to configure and automate the Anti-Webshell deployment.
- Amazon RDS – Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

1.1 Introduction

Anti-Webshell v2.0 (“Anti-Webshell”), a webshell detection/countermeasure solution by SK Infosec, is designed to prevent any damage or leakage of the resource and information of a web server, and any damage associated with web server used as an origin of a cyber attack, by detecting and countering any webshell file that has been illegally installed through the abuse of the web server’s vulnerability. Anti-Webshell provides full webshell detection/countermeasure to protect your AWS infrastructure. This solution can be deployed on AWS.

- Webshell - It refers to a web-based shell program. In general, a web server supports a certain function or syntax that can execute console-based commands in case of such web script languages as PHP, ASP and JSP. If someone abuses such function or syntax, he can disguise himself as a normal user who created a shell program to use SSH or Telnet on the web. Any malicious webshell can be uploaded through a web server’s vulnerability. Furthermore, it can be used as a hacking tool to trigger various attacks (e.g. reading of web pages’ source codes, insertion of malicious scripts, uploading of files, data leakage from servers and databases, etc.) through the execution of system commands.

1.1.1 Prerequisites and Requirements

This topic describes the prerequisites and resource requirements for installing Anti-Webshell on Amazon Web Services (AWS).

- Prerequisites

Anti-Webshell AMI's are completely self contained. You don't need to install any additional software. Basic AWS skills are sufficient to deploy Anti-Webshell on AWS. Simple deployments involve just EC2. Anti-Webshell AMI's are available as BYOL model. Since Anti-Webshell AMI's are available on AmazonLinux and Centos, you can choose the OS you are familiar with.

You need to register in our customer portal(http://www.skinfosec.net/antiwebshell/en/service_request.html)to get the trial license. Once you get the trial license you need to upload the license to your running EC2 instance.

Anti-Webshell Agent installer(.tar, .exe) can be obtained from the following link:
http://www.skinfosec.net/antiwebshell/en/support.html

- Requirement

Installing Anti-Webshell requires the following virtual machines (VMs):

VM Name (TAG)	VM type	Default VM Count
Anti-Webshell Manager	M4.large or M5.large	2
Anti-Webshell Manager DB	db.m4.large or db.m5.large	2

*VM Count may change based on customer environment.

1.1.2 Region support

The following regions are supported on BYOL

Region code	Region Name	Remarks
us-east-1	US East (N. Virginia)	-
us-east-2	US East (Ohio)	-
us-west-1	US West (N. California)	-

eu-central-1	EU (Frankfurt)	-
eu-west-1	EU (Ireland)	-
eu-west-2	EU (London)	-
eu-west-3	EU (Paris)	-
ap-southeast-1	Asia Pacific (Singapore)	-
ap-southeast-2	Asia Pacific (Sydney)	-
ap-south-1	Asia Pacific (Mumbai)	-
ap-northeast-1	Asia Pacific (Tokyo)	-
ap-northeast-2	Asia Pacific (Seoul)	-
sa-east-1	South America (São Paulo)	-
ca-central-1	Canada (Central)	-

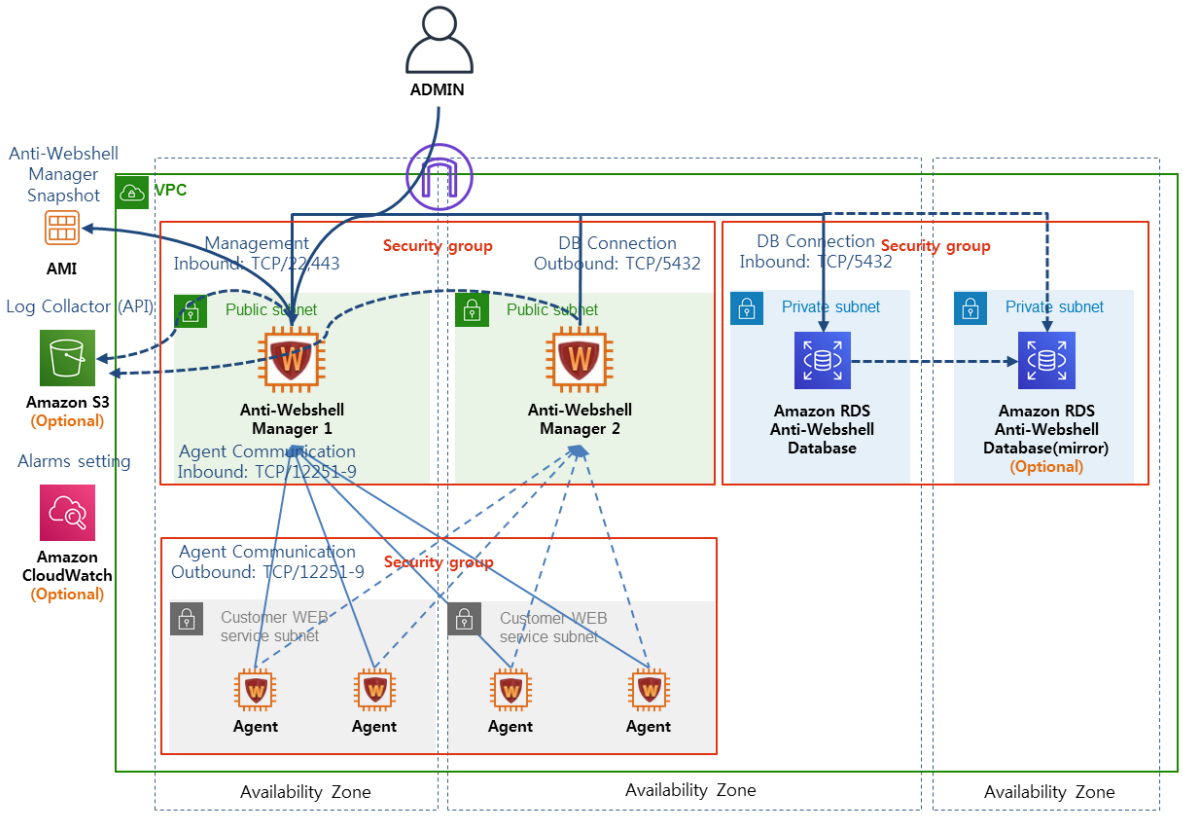
1.1.3 Architecture Diagrams

This Architecture Diagrams deploys the Anti-Webshell Manager to the VPC you set up, including the following components:

- In the Public Subnet, Anti-Webshell Manager EC2 Instance
- In the Private Subnet, High availability anti-webshell database and mirror
- In the Customer WEB service Subnet, Install Agent on customer ec2 instance
- Perform Backup and Recovery Using an AMI(Amazon Machine Image)
- Solution event log collection and S3bucket storage (central log collection)
- Operational monitoring and alerts through integration with Amazon Cloud Watch service and health check of Anti-Webshell Manager

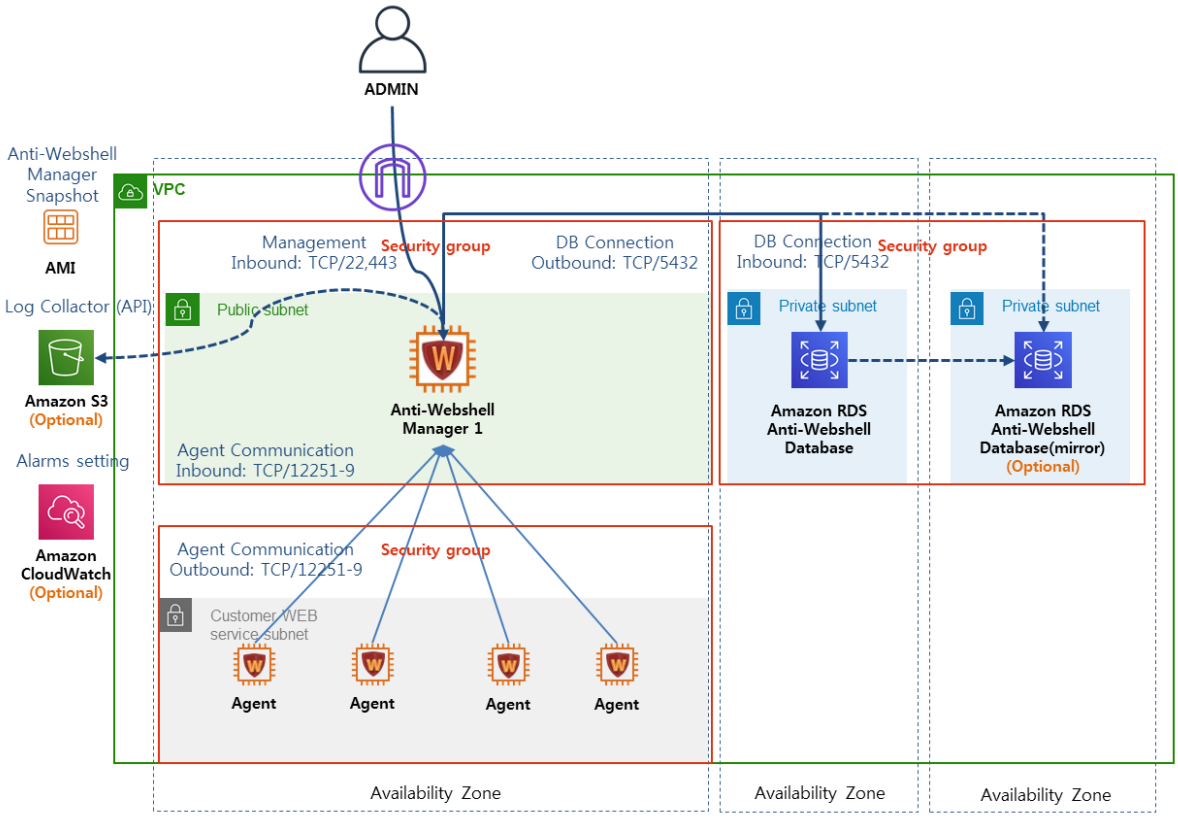
A. High availability Configuration

In this example, a more sizable configuration as an example High availability configuration that incorporates Anti-Webshell replication capability to support high availability and disaster recovery.



B. Single Configuration

If cost reduction is a top priority, a single configuration is possible. When a single instance configuration is deployed, there will be service outage during downtime. The single instance configuration is cheaper than multiple AZ configuration. Create instance 1 in a single AZ configuration.



1.1.4 Use Cases

Anti-Webshell Solution use cases, please refer to the lower part of the link.

- http://www.skinfosec.net/antiwebshell/en/antiwebshell_05.html

2. Planning Guidance

2.1 Security

The only thing you need to be able to install/control you Anti-Webshell Manager deployment is SSH access (key-based authentication/sudo or similar mechanisms are preferred)

- ✓ Not using AWS root credentials for access.

2.2 Costs and Licenses

Anti-Webshell supports BYOL license. BYOL licensing are available from your reseller or distributor and provides the same ordering practice across all private and public clouds, no matter what the platform is. You must activate a license for the first time you access the instance from the GUI or CLI before you can start using various features.

License Cost

License Volume	Monthly Price	Annual Price
Count of Agent	$ 100	$ 1200

Full list of billable AWS services

You are responsible for the cost of the AWS services. The cost of the resources created by the Manual varies based on how many instances you want to protect. For details, see the pricing pages(https://aws.amazon.com/pricing/) for each AWS service you will be using in this Manual.

A. EC2 Instance(essential)

B. EBS(essential)

C. RDS(essential)

D. S3(optional)

E. Cloudwatch(optional)

2.3 Sizing

Anti-Webshell AMI's supports the following Instance specification on AWS. For up-to-date information on each instance type, see the following links(https://aws.amazon.com/ko/ec2/instance-types/)

A. Manager Instance type or EBS Volume size:

Count of Agent	Instance type	vCPU	Memory(GiB)	EBS Volume	EBS Volume Type
~ 20	M4.large or M5.large	2	8	500 GB	General Purpose SSD (gp2)
~ 50	M4.xlarge or M5.xlarge	4	16	1 TB	General Purpose SSD (gp2)
~ 100	M4.2xlarge or M5.2xlarge	8	32	2 TB	General Purpose SSD (gp2)
~ 200	M4.4xlarge or M5.4xlarge	16	64	4 TB	General Purpose SSD (gp2)

B. RDS Instance type or Storage size:

Count of Agent	Instance type	vCPU	Memory(GiB)	Allocated storage	Storage Type
1 ~ 200	db.M4.large or db.M5.large	2	8	100 GiB	General Purpose SSD

C. Agent Instance specification: All instance types that support the JDK

✓ Supported version:

JDK Version	Agent Version
8.x	2.0.017, 2.0.018, 2.0.019, 2.0.021, 2.0.022, 2.0.023
7.x	2.0.017, 2.0.018, 2.0.019, 2.0.021, 2.0.022, 2.0.023
6.x	2.0.017, 2.0.018, 2.0.019, 2.0.021, 2.0.022, 2.0.023

3. Deployment steps

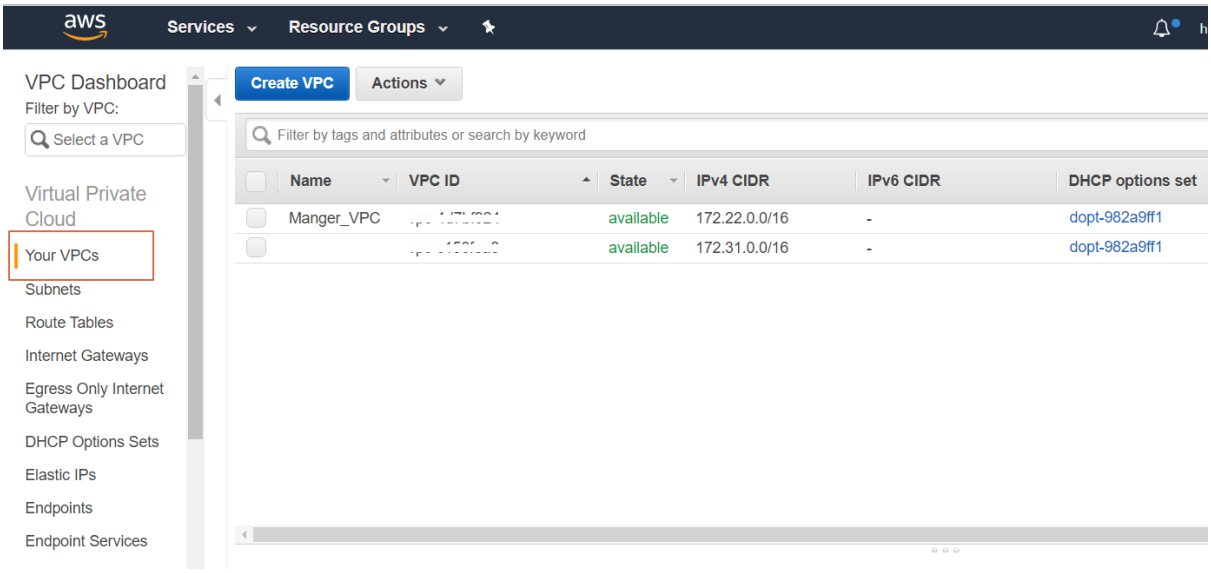
3.1 Step 1. Anti-Webshell Manager Installation

3.1.1 Create VPC and Subnet

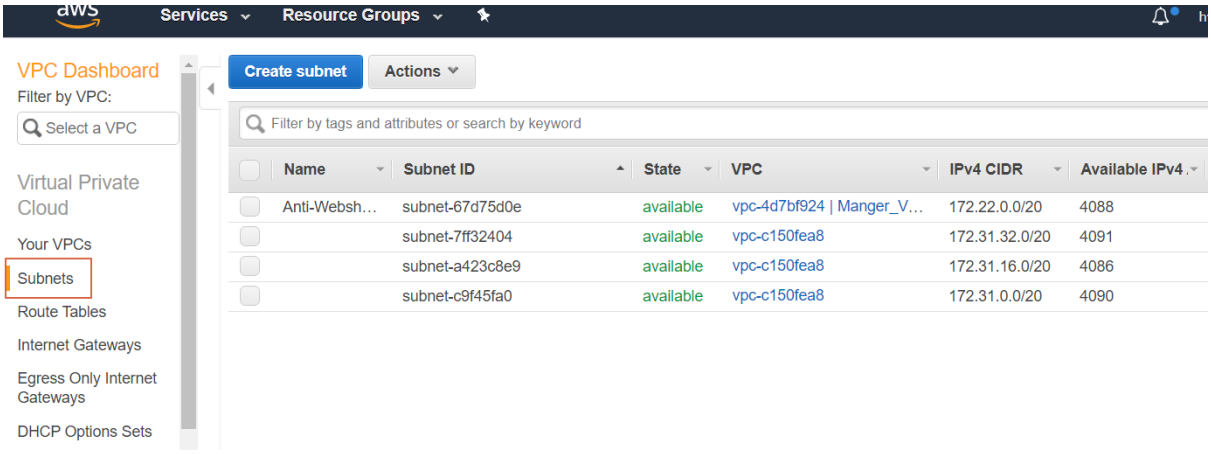
Anti-webshells are installed in existing VPC where customer service is built. And it is installed in public subnet to manage Anti-Webshell.

A. Check Existing VPC and Subnet

1. You can find VPC settings at [EC2 Management Console > Services > Networking & Content Delivery > VPC]



2. You can find subnet settings at [EC2 Management Console > Services > Networking & Content Delivery > VPC > Subnets]



B. Create Anti-Webshell Manager Subnet

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Subnets, Create subnet.
3. Specify the subnet details as necessary and choose Create.

Menu	Input Value
Name tag	Anti-Webshell Manager subnet
VPC	Choose the same existing VPC as your customer web tier
VPC CIDRs	-
Availability Zone	Refer to [1.1.3] Architecture Diagrams to select.
IPv4 CIDR block	For information about Subnet group, see the following link:

	https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_Subnets.html

C. Create Anti-Webshell Manager subnet2

✓ Skip if the current configuration is Single Az configure

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Subnets, Create subnet.
3. Specify the subnet details as necessary and choose Create.

Menu	Input Value
Name tag	Anti-Webshell Manager subnet2
VPC	Choose the same existing VPC as your customer web tier
VPC CIDRs	-
Availability Zone	Refer to [1.1.3] Architecture Diagrams to select.
IPv4 CIDR block	For information about Subnet group, see the following link: https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_Subnets.html

D. Create Anti-Webshell Manager RDS Subnet

RDS creates a private subnet by following these steps

1. Create RDS Primary private subnet, [EC2 Management Console > Services > Networking & Content Delivery > VPC > Subnets]and click on the [Create subnet] button.

Menu	Input Value
Name tag	Anti-Webshell Manager RDS Primary subnet
VPC	Choose the same existing VPC as your customer web tier
VPC CIDRs	-
Availability Zone	Refer to [1.1.3] Architecture Diagrams to select.
IPv4 CIDR block	For information about Subnet group, see the following link: https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_Subnets.html

2. Create Secondary private subnet, [EC2 Management Console > Services > Networking & Content Delivery > VPC > Subnets]and click on the [Create subnet] button.

Menu	Input Value

Name tag	Anti-Webshell Manager RDS Secondary subnet
VPC	Choose the same existing VPC as your customer web tier
VPC CIDRs	-
Availability Zone	Refer to [1.1.3] Architecture Diagrams to select.
IPv4 CIDR block	For information about Subnet group, see the following link: https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_Subnets.html

3. Create RDS subnet group, [EC2 Management Console > Services > Database > Subnet groups > Create DB Subnet Group] and click on the [Create DB subnet Group] button.

Menu	Input Value
Name	Anti-Webshell Manager RDS subnet group
Description	Anti-Webshell Manager RDS private subnet group
VPC	Choose the same existing VPC as your customer web tier
Availability Zone	Refer to [1.1.3] Architecture Diagrams to select.
Subnet	Select [Anti-Webshell Manager RDS Primary subnet], [Anti-Webshell Manager RDS Secondary subnet] and click on the [Add subnet] button *For information about Subnet group, see the following link https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/UserGuide/USER_VPC.html#USER_VPC.CreateDBSubnetGroup

3.1.2 Create Network ACLs

Optional: If you need an additional layer of security, you can create a network ACL and add rules.

A. Create Anti-Webshell Manager Network ACL

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Network ACLs.
3. Choose Create Network ACL.
4. In the Create Network ACL dialog box, optionally name your network ACL, and then select the ID of your VPC from the VPC list, and choose Yes, Create.

Menu	Input Value
Name tag	Anti-Webshell Manager NACL
VPC	Choose the same existing VPC as your customer web tier

5. In the navigation pane, choose Network ACLs.

6. In the details pane, choose either the Inbound Rules or Outbound Rules tab, depending on the type of rule that you need to add, and then choose Edit.

- Inbound Rule

Rule#	Source IP	Protocol	Port	Allow/Deny	Comments
100	Public IPv4 address range of your customer admin corporate IP	TCP	443	Allow	Allows inbound HTTPS traffic from customer admin corporate IP
110	Public IPv4 address range of your customer admin corporate IP	TCP	22	Allow	Allows inbound SSH traffic from customer admin corporate IP
130	Private IPv4 address range of customer web/was service network	TCP	12251-12259	Allow	Allows inbound Agent traffic from your customer web/was service network
140	Private IPv4 address range of Anti-Webshell Manager RDS network	TCP	32768-65535	Allow	Allows inbound RDS traffic from DB network
*	0.0.0.0/0	all	all	DENY	-

- Outbound rule

Rule#	Dest IP	Protocol	Port	Allow/Deny	Comments
100	Public IPv4 address range of your customer corporate IP Network	TCP	32768-65535	Allow	Allows outbound responses to the customer admin corporate IP. Network ACLs are stateless, therefore this rule is required to allow response traffic for inbound requests.
110	Private IPv4 address range of customer	TCP	49152-65535	Allow	Allows outbound responses to Agent on your

	web/was service network				customer web/was service network network.
120	Private IPv4 address range of Anti-Webshell Manager RDS network	TCP	5432	Allow	Allows outbound responses to Anti-Webshell Manager RDS network .
*	0.0.0.0/0	all	all	DENY	-

7. When you are done, choose Save.
8. Associating a Subnet with a Network ACL, In the navigation pane, choose Network ACLs, and then select [Anti-Webshell Manager NACL].
9. In the details pane, on the Subnet Associations tab, choose Edit. Select the Associate check box for the [Anti-Webshell Manager subnet] and [Anti-Webshell Manager subnet2] to associate with the network ACL, and then choose Save.

B. To add rules to network ACL for your customer web tier

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose existing network ACL for your customer's web service
3. In the details pane, choose either the Inbound Rules or Outbound Rules tab, depending on the type of rule that you need to add, and then choose Edit.

- Inbound rule

Rule#	Source IP	Protocol	Port	Allow/Deny	Comments
100	Private IPv4 address range of Anti-WebShell Manager network	TCP	49152-65535	Allow	Allows inbound responses to Agent from Manager

- Outbound rule

Rule#	Dest IP	Protocol	Port	Allow/Deny	Comments
110	Private IPv4 address range of Anti-WebShell Manager network	TCP	12251-12259	Allow	Allows outbound responses to Manager on Anti-WebShell Manager network

*	0.0.0.0/0	all	all	DENY	-

4. When you are done, choose Save.

C. Create Anti-Webshell Manager DB Network ACL

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Network ACLs.
3. Choose Create Network ACL.
4. In the Create Network ACL dialog box, optionally name your network ACL, and then select the ID of your VPC from the VPC list, and choose Yes, Create.

Menu	Input Value
Name tag	Anti-Webshell Manager DB NACL
VPC	Choose the same existing VPC as your customer web tier

5. In the navigation pane, choose Network ACLs.
6. In the details pane, choose either the Inbound Rules or Outbound Rules tab, depending on the type of rule that you need to add, and then choose Edit.

- Inbound Rule

Rule#	Source IP	Protocol	Port	Allow/Deny	Comments
100	Private IPv4 address range of Anti-Webshell Manager IP	TCP	5432	Allow	Allows inbound Anti-Webshell Manager traffic from your Anti-Webshell Manager network
*	0.0.0.0/0	all	all	DENY	-

- Outbound rule

Rule#	Dest IP	Protocol	Port	Allow/Deny	Comments

100	Private IPv4 address range of Anti-Webshell Manager IP	TCP	32768-65535	Allow	Allows outbound responses to Anti-Webshell Manager network
*	0.0.0.0/0	all	all	DENY	-

7. When you are done, choose Save.

8. Associating a Subnet with a Network ACL, In the navigation pane, choose Network ACLs, and then select [Anti-Webshell Manager NACL].

9. In the details pane, on the Subnet Associations tab, choose Edit. Select the Associate check box for the [Anti-Webshell Manager RDS Primary subnet] and [Anti-Webshell Manager RDS Secondary subnet] to associate with the network ACL, and then choose Save.

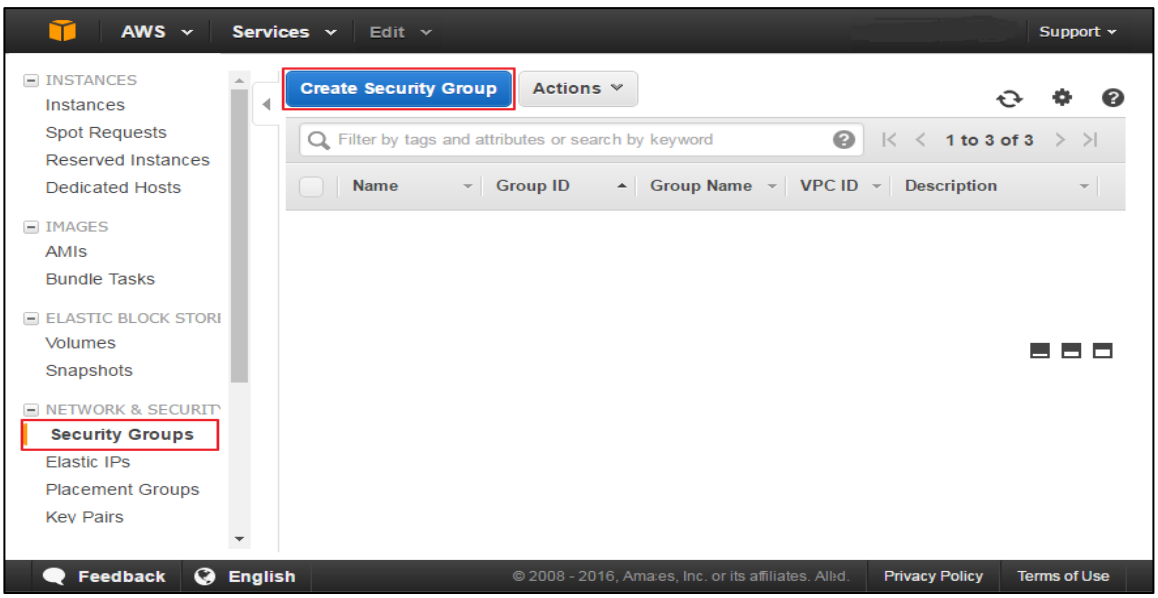
3.1.3 Create Security Group

You need to set up security groups for the Anti-Webshell management server and the agent to communicate with each other.

A. Create Anti-Webshell Manager Security Groups

1. Access the AWS Ec2 Management Console.

2. Select [NETWORK & SECURITY > Security Groups] and click on the Create Security Group button.



3. As shown below, add a new rule to the Inbound rule.

Menu	Input Value
Security Group name	Anti-Webshell Manager-Agent SG
Description	Anti-Webshell Manager-Agent SG
VPC	Choose the same existing VPC as your customer web tier
Type	Custom TCP Rule
Protocol	TCP
Port Range	12251 - 12259
Source	Custom, Agent installation band and group name

Menu	Input Value
Security Group name	Anti-Webshell Manager-Https SG
Description	Anti-Webshell Manager-Https SG
VPC	Choose the same existing VPC as your customer web tier
Type	HTTPS
Protocol	TCP
Port Range	443
Source	Customer Admin Corporate IP

Menu	Input Value
Security Group name	Anti-Webshell Manager-SSH SG
Description	Anti-Webshell Manager-SSH SG
VPC	Choose the same existing VPC as your customer web tier
Type	SSH
Protocol	TCP
Port Range	22
Source	Customer Admin Corporate IP

4. Add a Name TAG to [Tags] as follows

Menu	Input Value	Menu	Input Value
Tag key	Name	Description	Tagging to identify assets
Value	Anti-Webshell Manager-		

	Agent SG		

Menu	Input Value	Menu	Input Value
Tag key	Name	Description	Tagging to identify assets
Value	Anti-Webshell Manager-Https SG		

Menu	Input Value	Menu	Input Value
Tag key	Name	Description	Tagging to identify assets
Value	Anti-Webshell Manager-SSH SG		

B. Create Anti-Webshell Agent Security Groups

Add new rules to the Outbound rules of the EC2 Instance where the Agent will be installed as shown in the table below.

Menu	Input Value
Security Group name	Anti-Webshell Agent-Manager SG
Description	Anti-Webshell Agent-Manager SG
VPC	Choose the same VPC as your customer web tier
Type	Custom TCP Rule
Protocol	TCP
Port Range	12251 - 12259
Destination	Custom, Anti-Webshell Manager installation band and group name

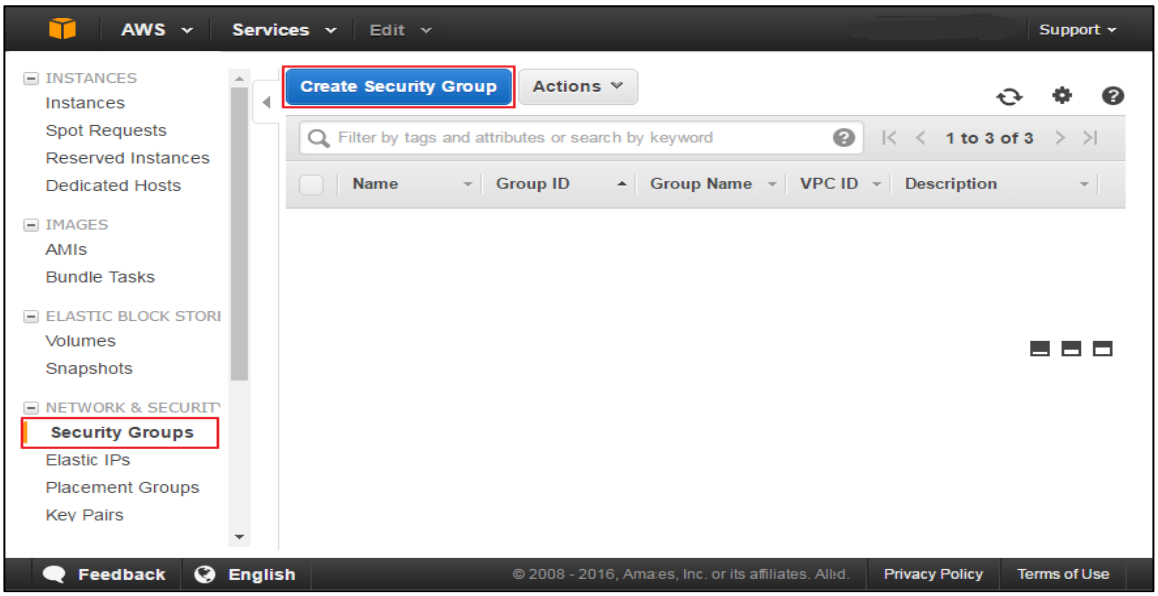
- Add a Name TAG to [Tags] as follows

Menu	Input Value	Menu	Input Value
Tag key	Name	Description	Tagging to identify assets
Value	Anti-Webshell Agent SG		

C. Create Anti-Webshell Manager RDS Security Groups

1. Access the AWS Ec2 Management Console.

2. Select [NETWORK & SECURITY > Security Groups] and click on the Create Security Group button.



3. As shown below, add a new rule to the Inbound rule.

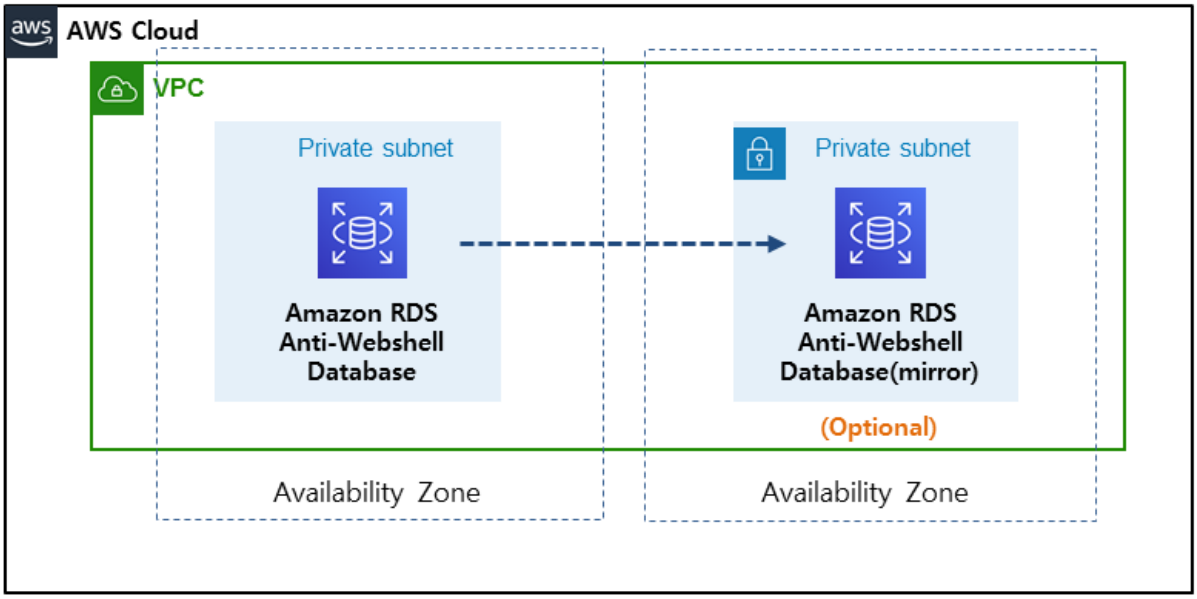
Menu	Input Value
Security Group name	Anti-Webshell Manager DB SG
Description	Anti-Webshell Manager DB SG
VPC	Choose the same existing VPC as your customer web tier
Type	PostgreSQL
Protocol	TCP
Port Range	5432
Source	Custom, Anti-Webshell Manager installation band and group name

4. Add a Name TAG to [Tags] as follows

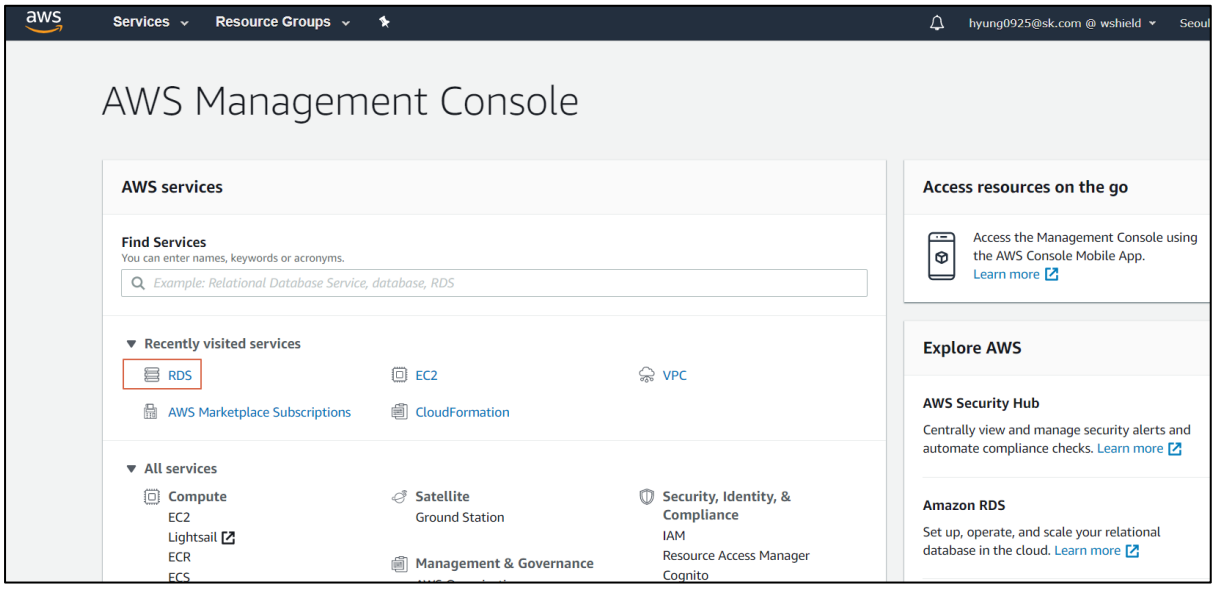
Menu	Input Value	Menu	Input Value
Tag key	Name	Description	Tagging to identify assets
Value	Anti-Webshell Manager DB SG		

3.1.4 Create RDS

Create a RDS Instance by restoring from the shared Anti-Webshell Manager DB RDS snapshot by the vendor

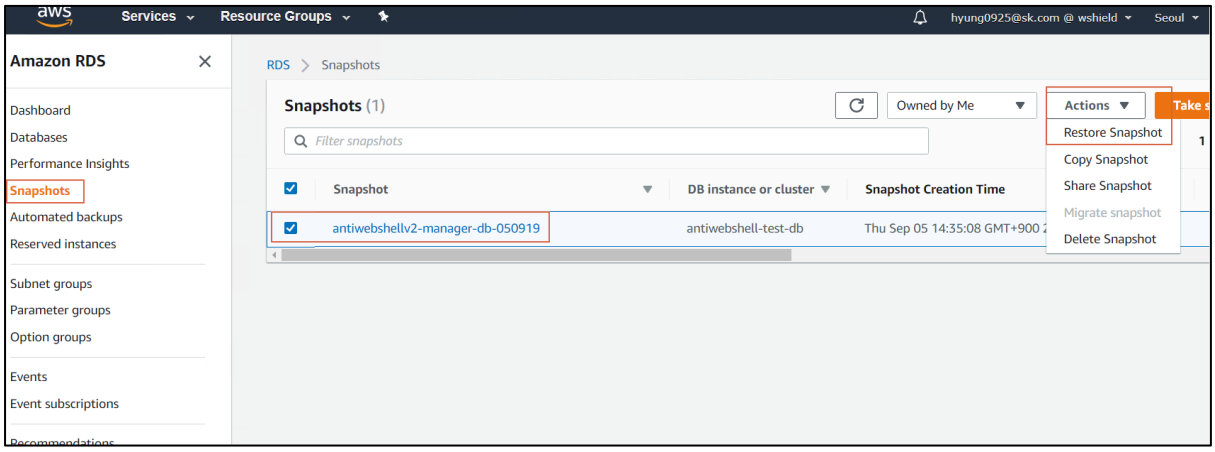


1. Login to AWS management console and Click RDS



2. Create RDS instance from a shared Snapshot

   ✓ Use the shared RDS Snapshot with the Account ID you created when you applied to the portal(http://www.skinfosec.net/antiwebshell/en/service_request.html).

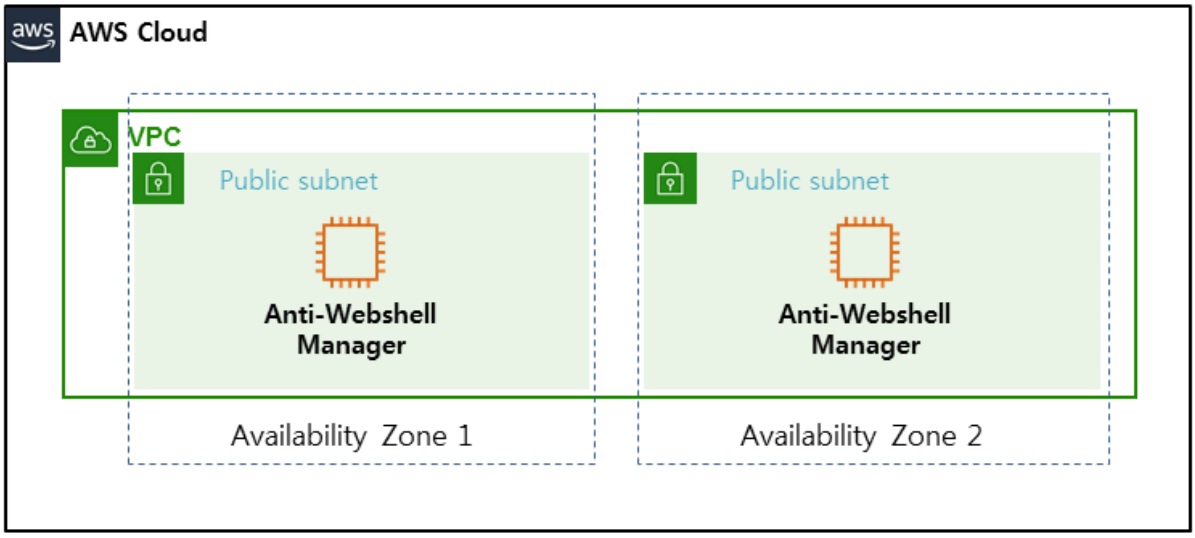


Menu	Input Value
Instance specifications	• DB Engine: PostgreSQL (Default) • License model: postgresql-license (Default) • DB Instance Class: For instance type, see [2.3 Sizing]. • Multi-AZ Deployment: Choose Single AZ deployment or Multi-AZ Deployment • Storage type: For Storage type, see [2.3 Sizing].
Network & Security	• Virtual Private Cloud (VPC): Choose the same existing VPC as your customer web tier • Subnet group: Choose existing Subnet group [Anti-Webshell Manager RDS subnet group] • Public accessibility: No • VPC security groups: Choose existing VPC security groups [Anti-Webshell Manager DB SG]
ETC	• If not informed, Select Default Option

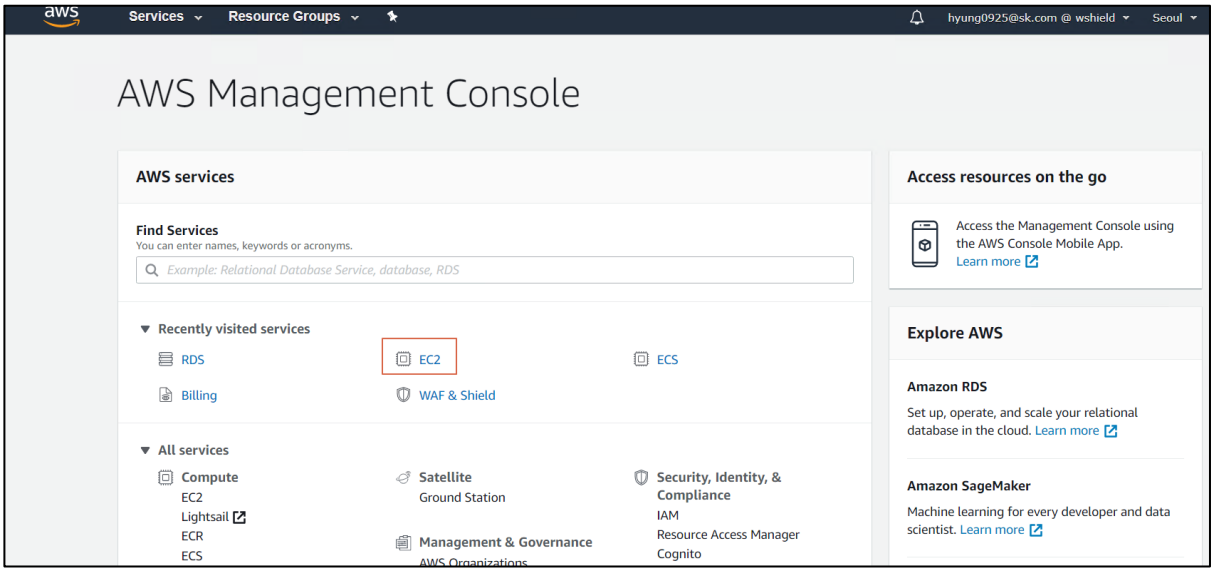
3.1.5 Create Instance

A. High availability configuration deployment

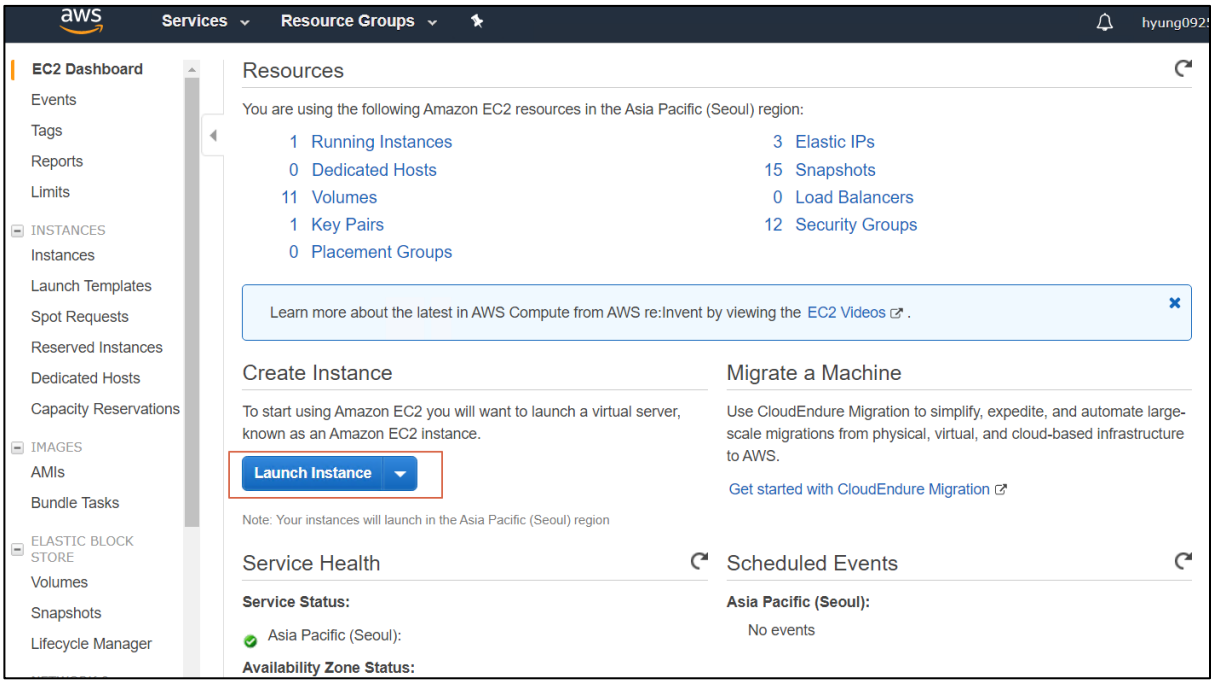
Basically, configuration is recommended for multiple AZs, and the Anti-Webshell Manager AMI is shared from the vendor to create an instance for each AZ.



1. Login to AWS management console and Click EC2.

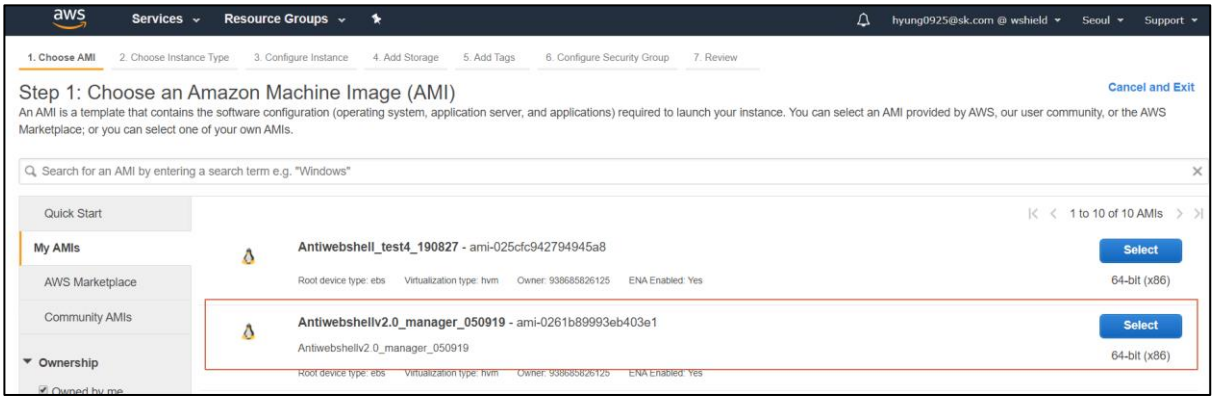


2. Click Launch Instance



3. Create an instance with a shared AMI.

   ✓ Use the shared AMI that is provided by the vendor



4. Choose an Instance Type

   ✓ For instance type, see [2.3 Sizing].

5. Next: Configure Instance Details

Menu	Input Value
Configure Instance Details	• Number of Instance: 1 • Network: For information about VPC, see the following link https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/working-with-vpcs.html • Subnet: For information about Subnet, see the following link https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/working-with-

	vpcs.html • Auto-Assign Public IP: Use subnet setting (Enable) • IAM Role: Select None or see [4.3 Solution Logging Procedure with S3 Bucket].
ETC	• If not informed, Select Default Option

6. Next: Add Storage
   - ✓ For instance type, see [2.3 Sizing].
7. Next: Add Tags
   - ✓ Tagging Anti-Webshell Manager EC2 Instance

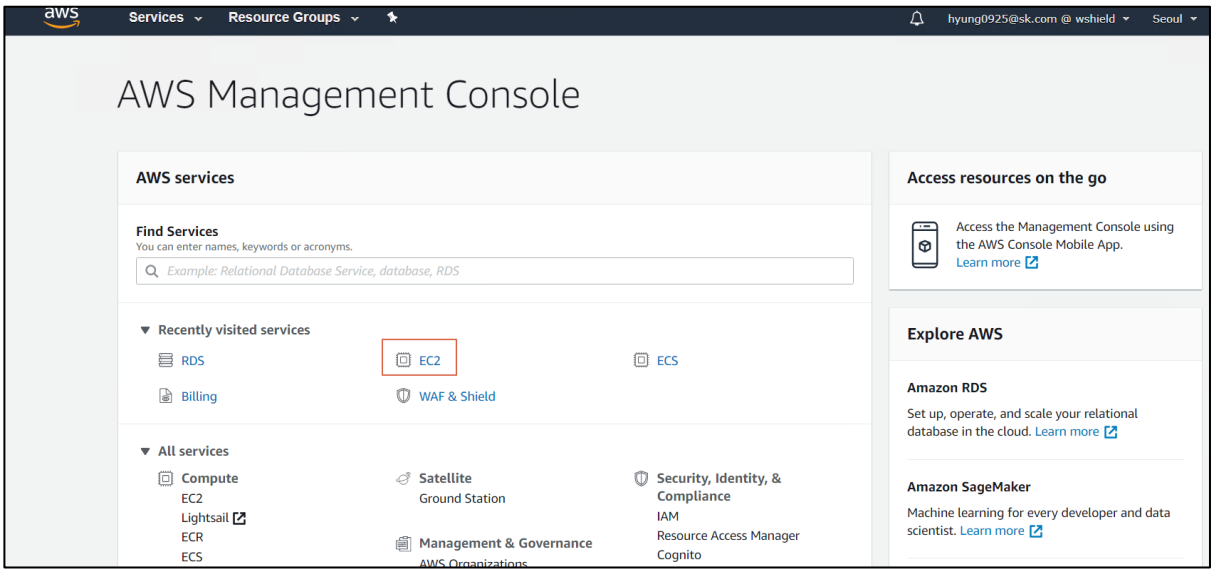
Menu	Input Value	Menu	Input Value
Tag key	Name	Description	Tagging to identify assets
Value	Anti-Webshell Manager		

8. Next: Configure Security Group
   - ✓ Select an existing security group: [Anti-Webshell Manager-Agent SG], [Anti-Webshell Manager-Https SG], [Anti-Webshell Manager-SSH SG]
9. Create one more instance of the ec2 in another AZ.

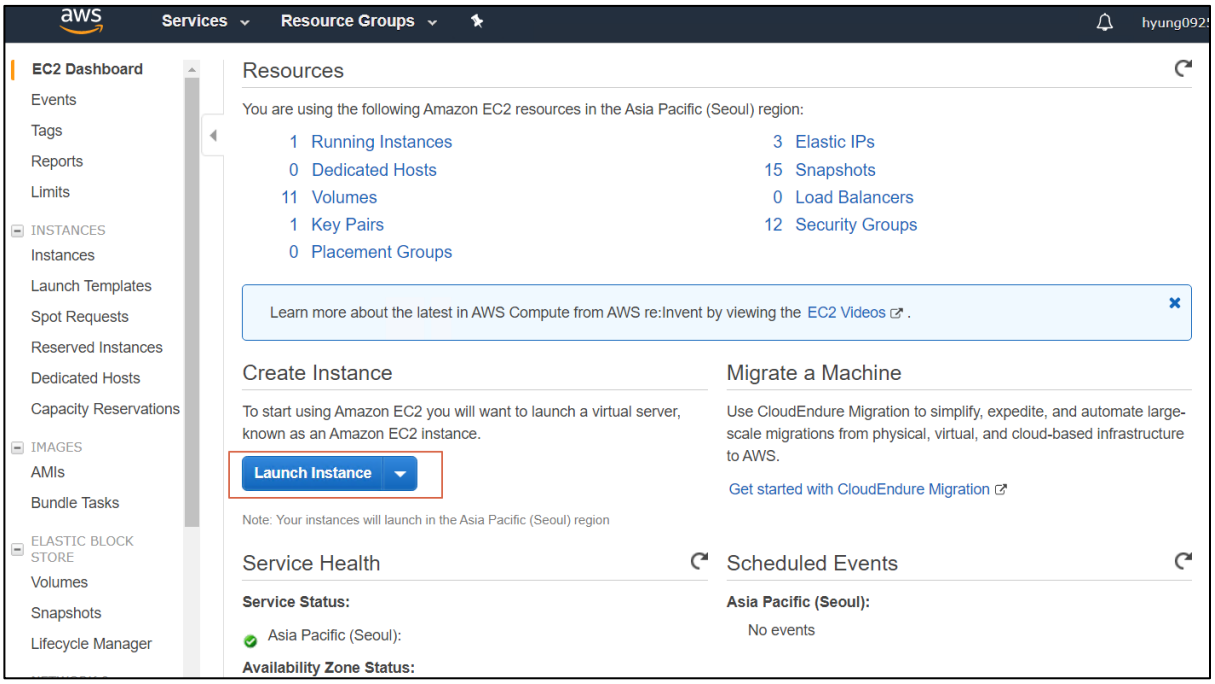
B. Single configuration deployment

When a single instance configuration is deployed, there will be service outage during downtime. The single instance configuration is cheaper than multiple AZ configuration.Create instance 1 in a single AZ configuration.

1. Login to AWS management console and Click EC2.

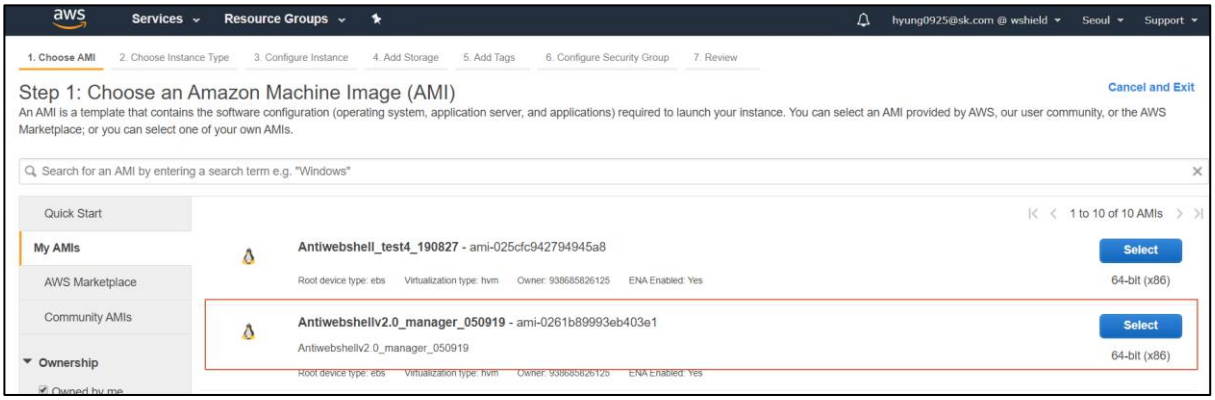


2. Click Launch Instance



3. Create an instance with a shared AMI.

   ✓ Use the shared AMI that is provided by the vendor



4. Choose an Instance Type

   ✓ For instance type, see [2.3 Sizing].

5. Next: Configure Instance Details

Menu	Input Value
Configure Instance Details	• Number of Instance: 1 • Network: For information about VPC, see the following link https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/working-with-vpcs.html • Subnet: For information about Subnet, see the following link https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/working-with-

	vpcs.html • Auto-assign Public IP: Use subnet setting (Enable) • IAM Role: Select None or see [4.3 Solution Logging Procedure with S3 Bucket].
ETC	• If not informed, Select Default Option

6. Next: Add Storage

   ✓ For instance type, see [2.3 Sizing].

7. Next: Add Tags

   ✓ Tagging Anti-Webshell Manager EC2 Instance

Menu	Input Value	Menu	Input Value
Tag key	Name	Description	Tagging to identify assets
Value	Anti-Webshell Manager		

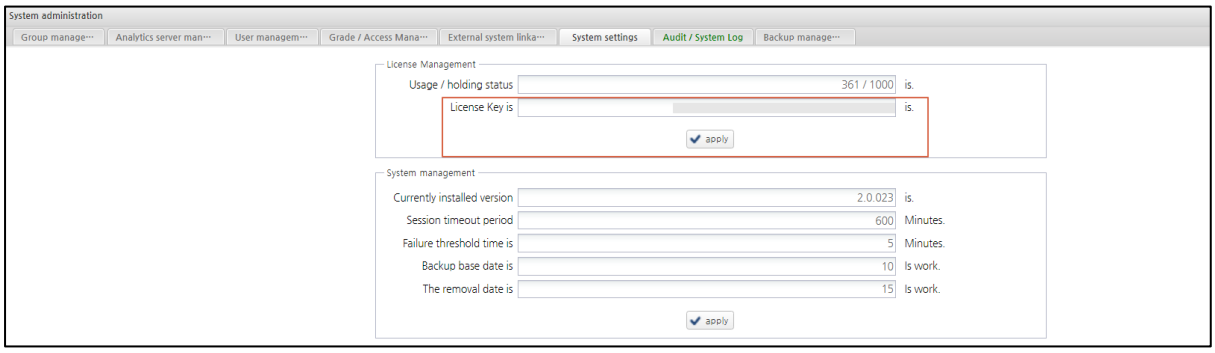
8. Next: Configure Security Group

   ✓ Select an existing security group: [Anti-Webshell Manager-Agent SG], [Anti-Webshell Manager-Https SG], [Anti-Webshell Manager-SSH SG]

3.2 Step 2. Anti-Webshell Manager Initial setting

3.2.1 License Registration

After logging in, enter the license key and click the [Apply] button.



3.3 Step 3. Deploy the Anti-Webshell Agent

3.3.1 Linux

A. Installing and Starting the Program

This program installation section describes how to complete installation on a Linux platform.

1. Create a wagent directory in the /(root) directory. (①~②)
2. Decompress the agent compression file in the /wagent directory. (③~④)
3. Assign an execution authority (755) to the script file. (⑤)
4. Enter Anti-Webshell Manager Private IP in the “/wagent/Install.dat” file. (⑥)
5. Run the wagent. (⑦)
6. Check how the wagent is running. (⑧)

✓ If it is running normally, the wagent module will be displayed.

```
① [root@localhost ~]# mkdir /wagent
② [root@localhost ~]# cd /wagent
③ [root@localhost wagent]# cp /tmp/aws_wagent_linux.tar /wagent/
④ [root@localhost wagent]# tar -xvf ./aws_wagent_linux.tar
⑤ [root@localhost wagent]# chmod 755 /wagent/*.sh
⑥ [root@localhost wagent]# vi ./install.dat
[Anti-Webshell Manager Private IP];

⑦ [root@localhost wagent]# ./wagent_run.sh
⑧ [root@localhost ~]# ps -ef |grep jar
root@ubuntu:~# ps -ef |grep jar
root      8405     1  0 Jul06 ?        00:06:44 java -Xms128m -Xmx256m -Djava.library.path=/wa
gent/lib -jar /wagent/WShield-M2.jar
root     12771  8405  0 16:35 ?        00:00:03 java -Xms128m -Xmx256m -Djava.library.path=/wa
gent/lib -jar /wagent/WShield-M.jar &
root     12889 12826  0 16:54 pts/0    00:00:00 grep --color=auto jar
root@ubuntu:~#
```

B. Shutting Down the Program

1. Navigate to the wagent directory. (①)
2. Shut down the wagent module. (②)
3. Check if the wagent module has been shut down successfully. (③)

✓ If it has been shut down successfully, the wagent module will not be displayed.

```
① [root@localhost ~]# cd /wagent
② [root@localhost ~]# wagent_stop.sh
③ [root@localhost ~]# ps -ef |grep jar
```

```
[localhost:/wagent]ps -ef |grep jar
    root 331904 258178   0 17:08:48  pts/2  0:00 grep jar
[localhost:/wagent]
```

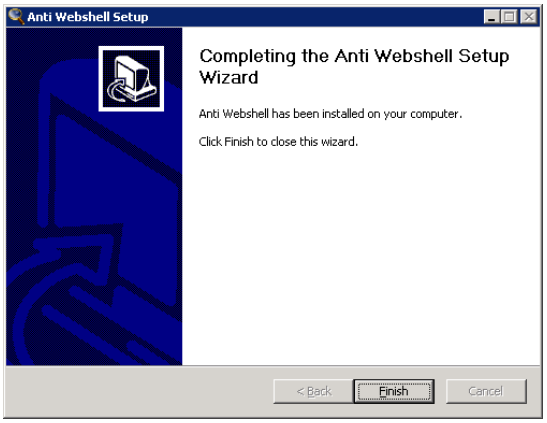
3.3.2 Windows

A. Installing and Starting the Program

This program installation section describes how to complete installation on a Windows platform.

1. Run the WSAgentInstall.exe file. When the starting page appears, click on the [Install] button.

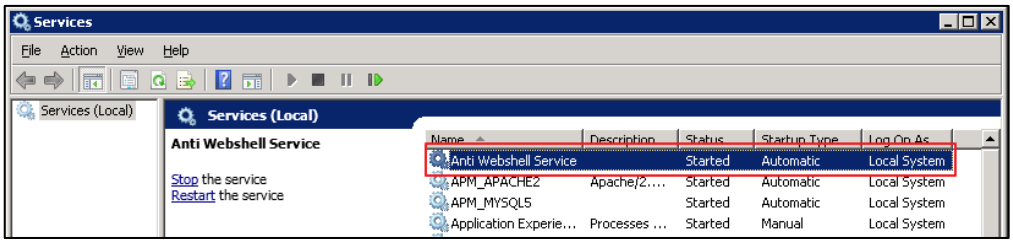
2. When a window pops up after installation has been completed, click on the [Finish] button.



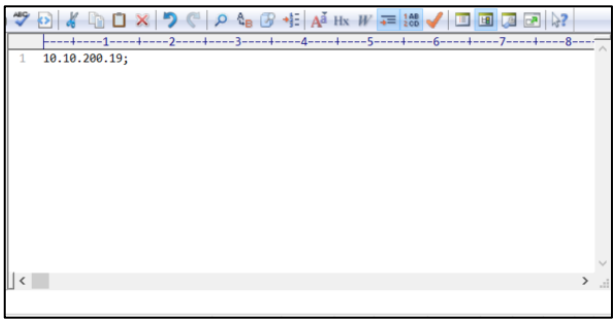
3. run the following Windows menus [Control Panel > System and Security > Administrative Tools > Services].

As shown below, the status of the Anti Webshell service module is displayed as “Started” on the service list.

Click on the “Stop the service” line.



4. Enter Anti-Webshell Manager Private IP in the “C:\AntiWebshell\Install.dat” file.

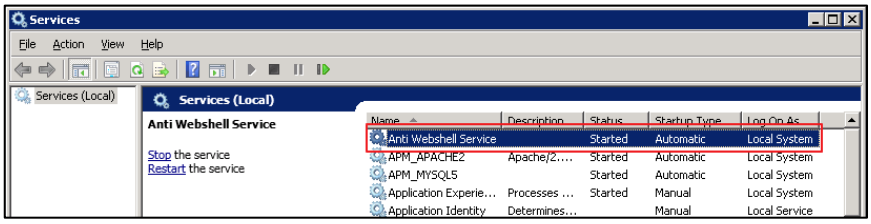


5. Run is Anti-Webshell Service.

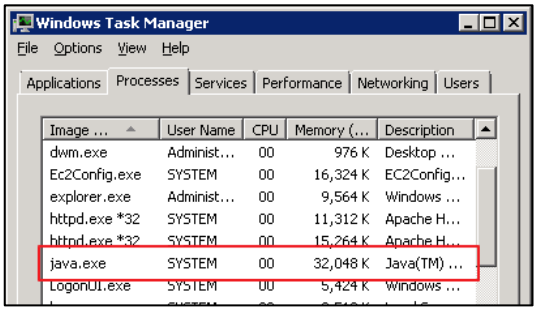
Run the following Windows menus: [Control Panel > System and Security > Administrative Tools > Services].

As shown below, the status of the Anti Webshell service module is displayed as “Stop” on the service list.

Click on the “Start the service” line.



One or two java.exe modules are currently running the process list of Windows Task Manager.

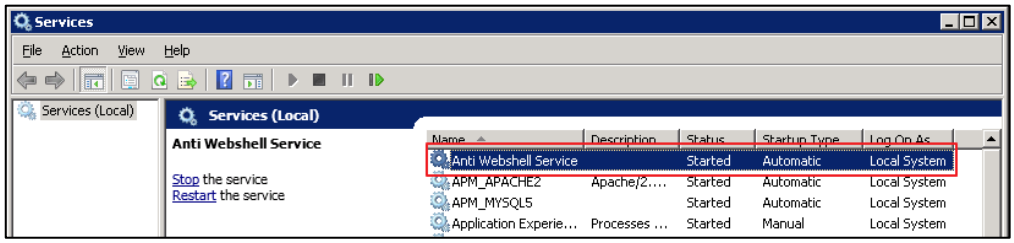


B. Shutting Down the Program

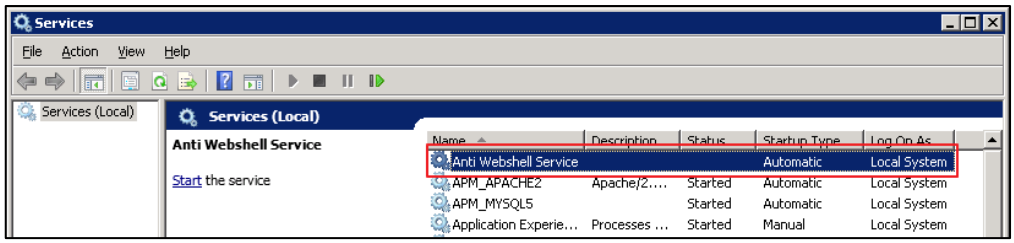
1. If you want to shut down the wagent module, run the following Windows menus [Control Panel > System and Security > Administrative Tools > Services].

As shown below, the status of the Anti Webshell service module is displayed as “Started” on the service list.

Click on the “Stop the service” line.



2. The service has stopped.

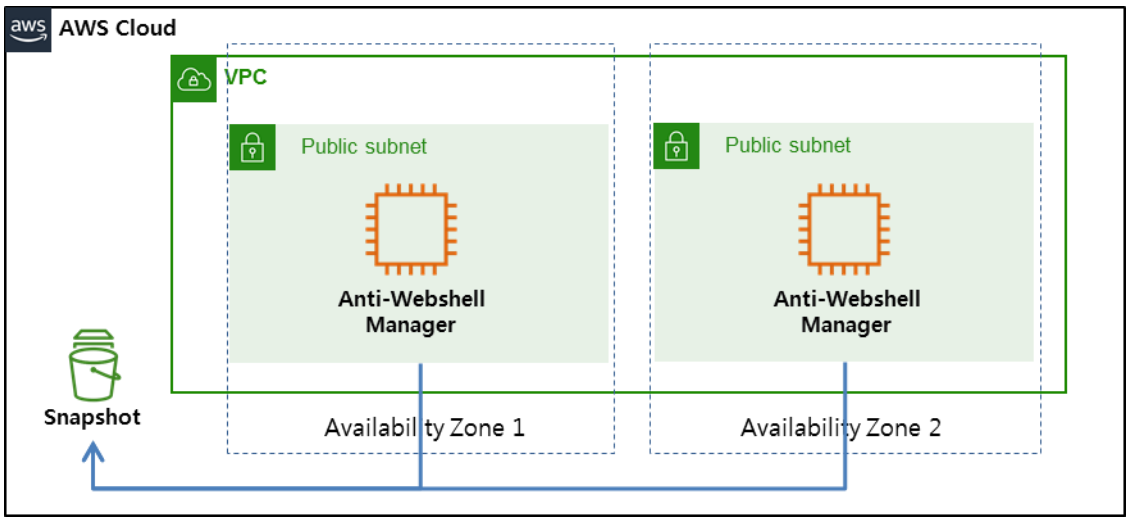


4. Operational Guidance

4.1 Supports Anti-Webshell Manager backup and restore in aws

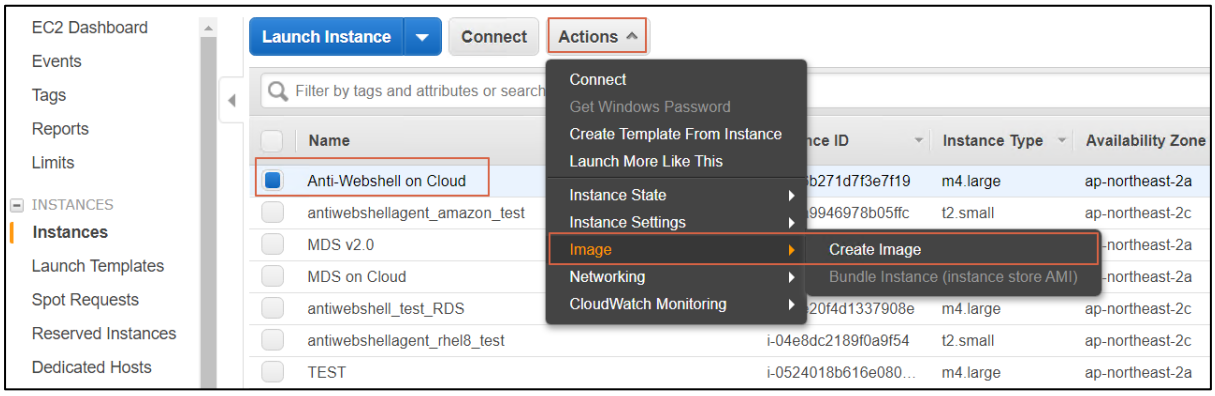
4.1.1 Anti-Webshell Manager backup and restore

Anti-Webshell Manager is deployed in two AZs (when possible) to provide high availability



A. Backup(Snapshot)

1. Create an image (AMI) with the Anti-Webshell Manager.

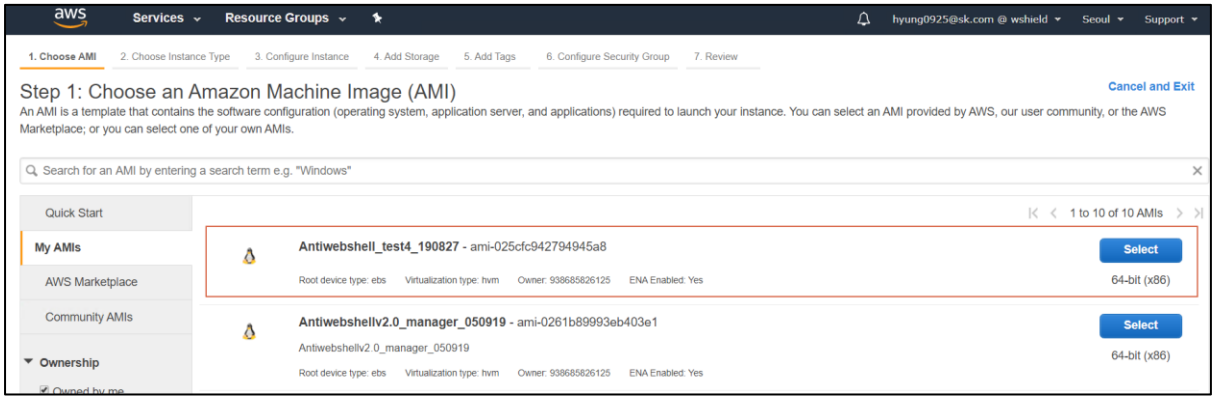


2. Create Image

Menu	Input Value
Image name	Anti-Webshell Manager backup(1 or 2)
Image description	Anti-Webshell Manager backup(1 or 2)
No reboot	Uncheck
Instance Volumes	Default configure

B. Restore

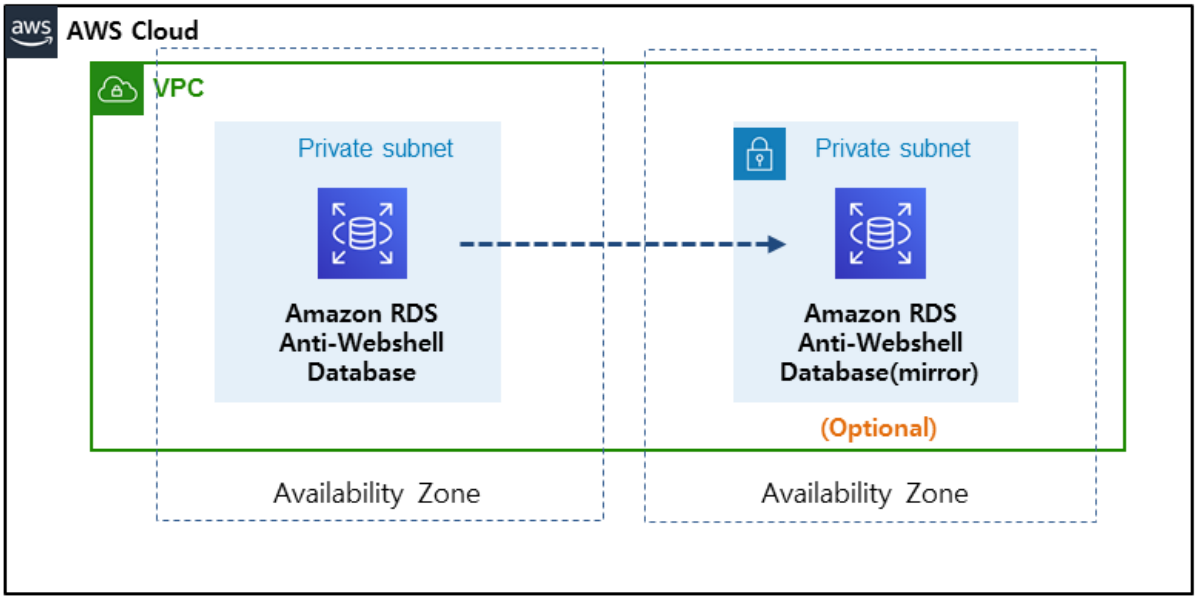
1. Choose an Amazon Machine Image (AMI).



2. Select to create AMI(snapshot) , see [3.1.5 Create Instance].

4.1.2 Amazon RDS backup and restore

Amazon RDS, used by Anti-Webshell Manager, is deployed in two Availability Zones (if available) to provide high availability at the database tier.



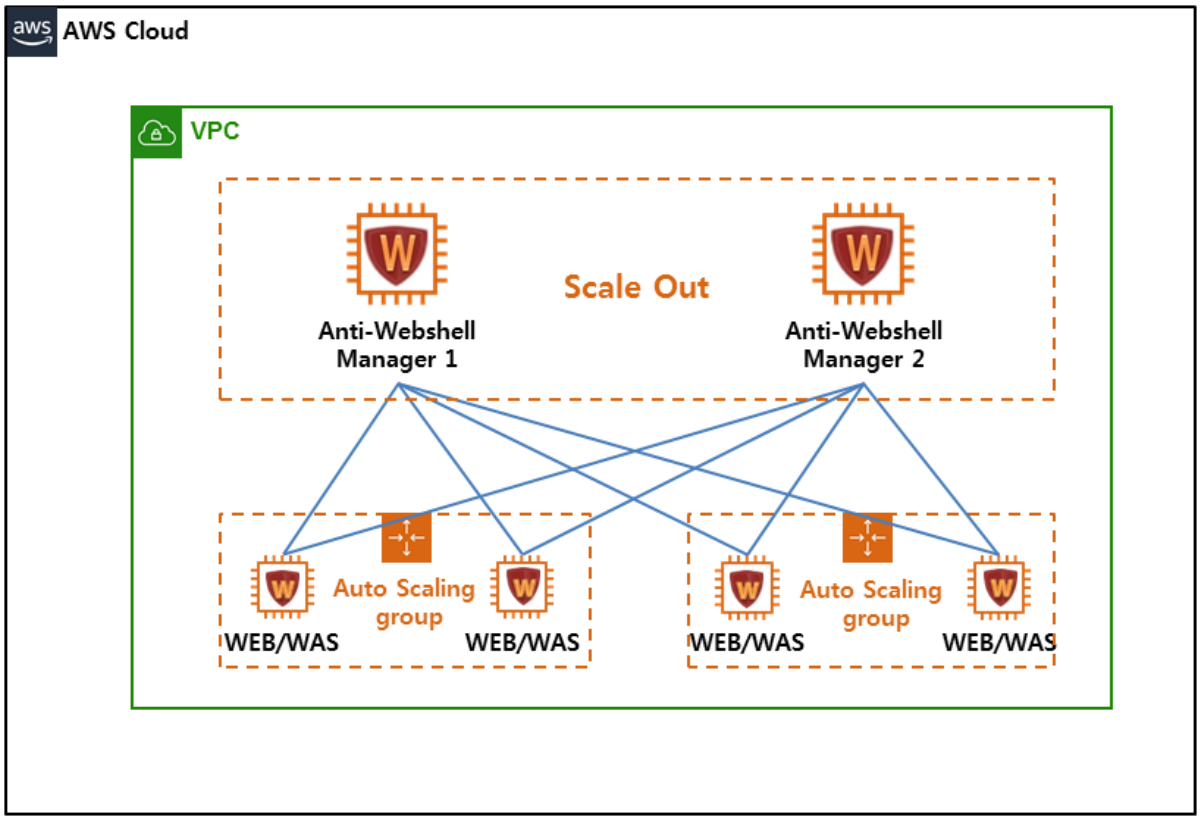
- When installing RDS, check the "Multi-AZ Deployment: Multi-AZ Deployment" setting.

- See the following link for how to create an RDS Mult-AZ Deployment.

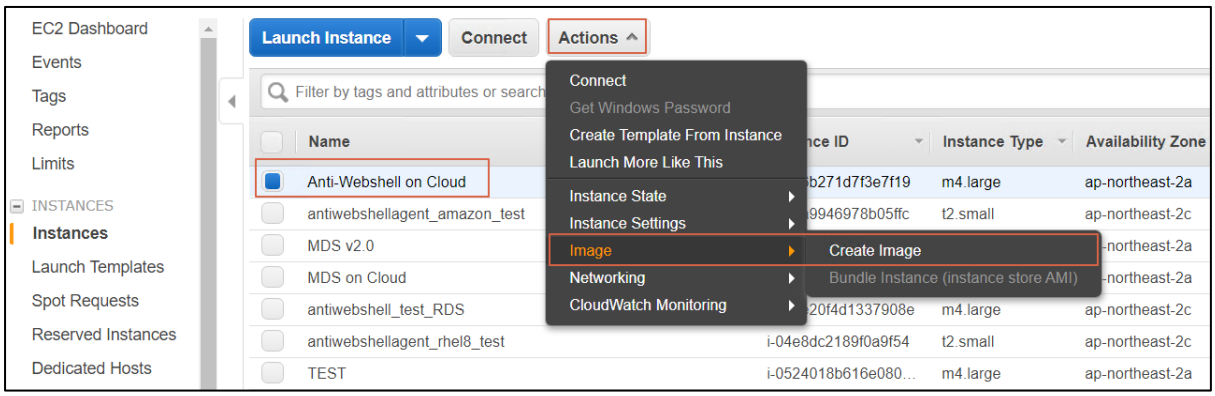
https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

4.2 Manual Scaling Procedure for Anti-Webshell on AWS

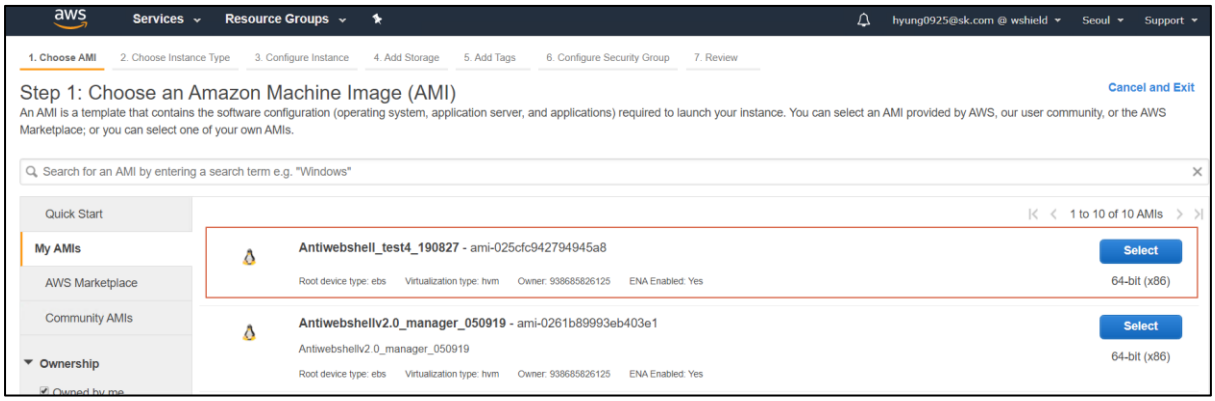
The following Manual Scaling procedures support high availability of Anti-Webshell on AWS.



1. Create an image (AMI) with the Anti-Webshell Manager.

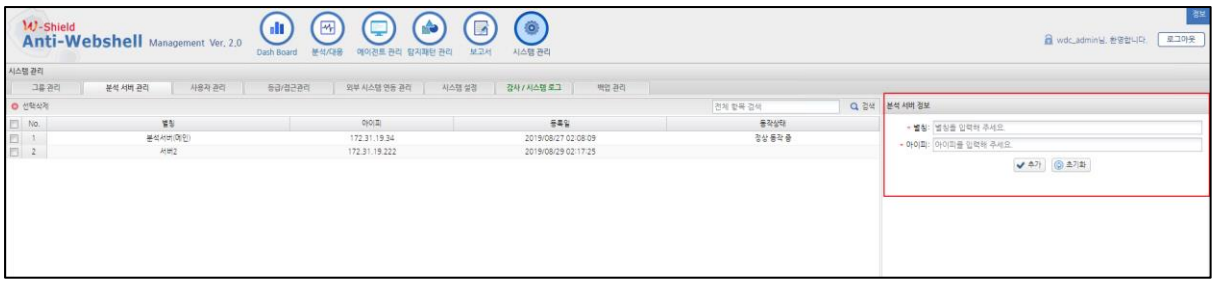


2. If you necessary Scale Out, create additional instances with the created image(AMI).



3. Add Register the IP of Anti-Webshell Manager 2.

In [Anti-Webshell Manager Web Console> System Management> Analysis Server Management> Analysis Server Information], enter and add an alias and IP (* private IP of the added Anti-Webshell Manger).



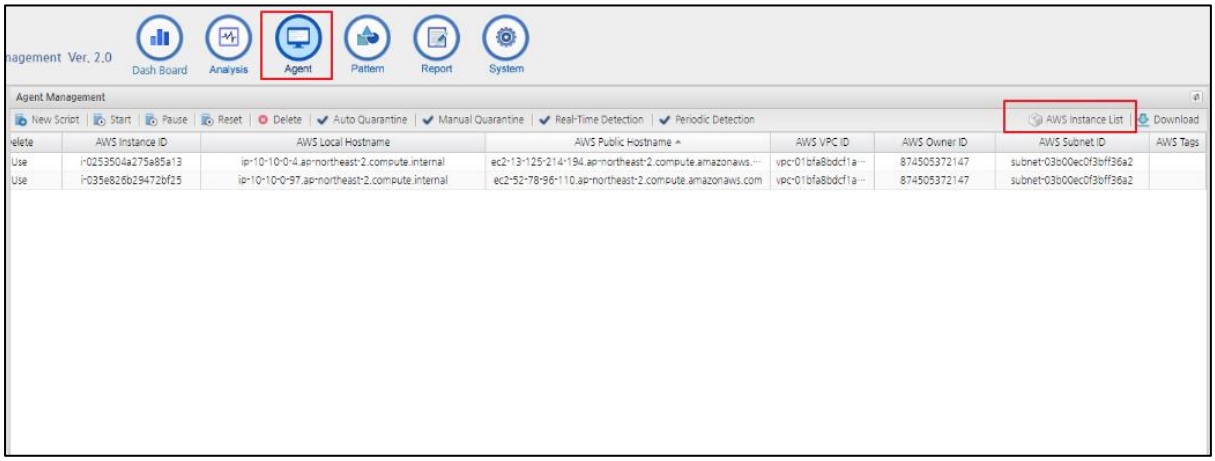
4.3 Add AWS resources to Anti-Webshell Manager

4.3.1 Add an AWS IAM role to Anti-Webshell Manager

Optional: When you add an AWS IAM role to Anti-Webshell Manager, all the Amazon EC2 under that account are imported into Anti-Webshell Manager and become visible in one of these locations:

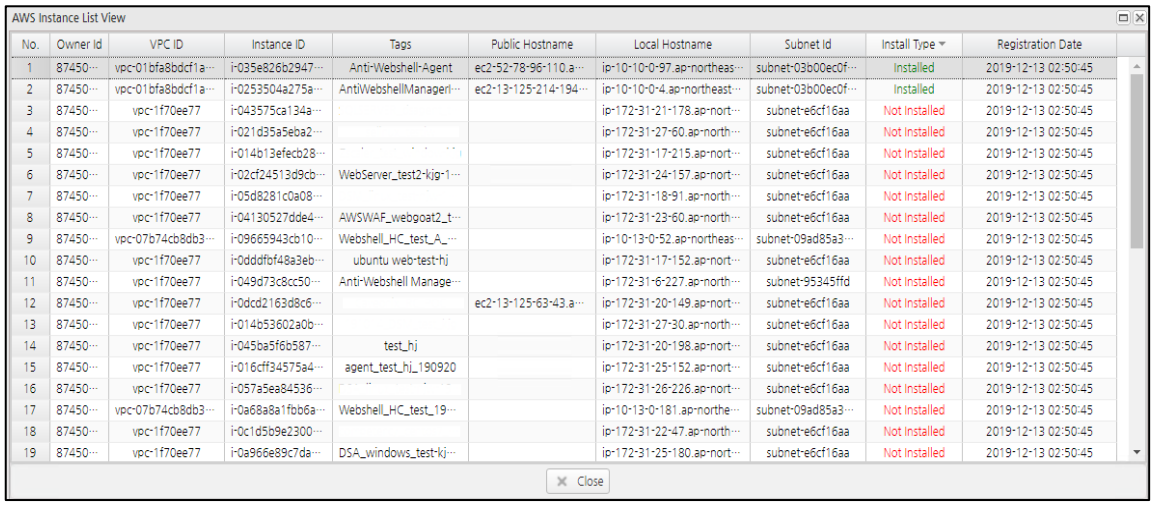
A. EC2 instance with Agent installed in [Agent] menu

B. All EC2 instances in the AWS account where Anti-Webshell Manager is installed in [Agent] menu > [AWS Instance List]

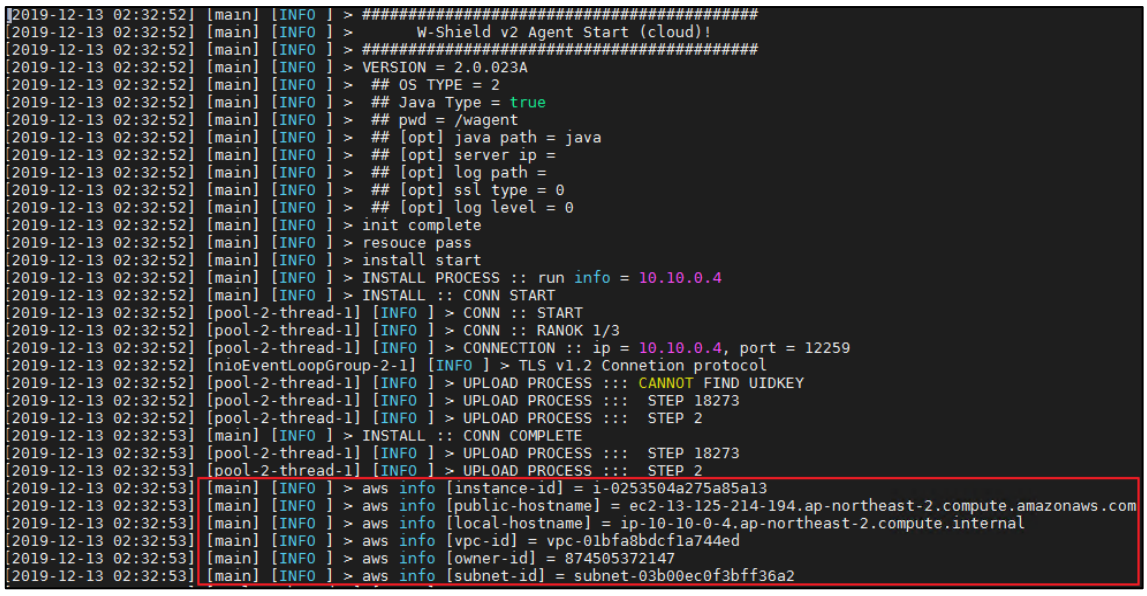


The benefits of adding an AWS IAM role, are:

- Changes in your EC2 inventory are automatically reflected in Anti-Webshell Manager.
- Your EC2 instances are organized into agent install info and EC2 metadata in the manager, which lets you easily see which instances are protected and which are not.
- You get AWS Metadata(Account ID, VPC, Subnet, Instance ID, Public DNSname, local DNSname, Tags), You can sort and filter using AWS Metadata.



- Agent and Manager logging includes AWS metadata for easy management.



You can do this with the following procedure.

1. Create IAM policy

    1) Access the AWS IAM Management

2) Select Policy > [Create policy] button

3) Click JSON tap > Input JSON data > Click [Policy review] button

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "cloudconnector",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "iam:ListAccountAliases",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "sts:AssumeRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

4) “Anti-Webshell_IAM_role” is entered in the [name] field > Click [Policy review] button

2. Create IAM role

1) Access the AWS IAM Management

2) Select role > [Create role] button

3) Click [AWS service] and [EC2], [Next: permissions] button

4) Check policy “Anti-Webshell_IAM_role”, Click [Next: permissions] button

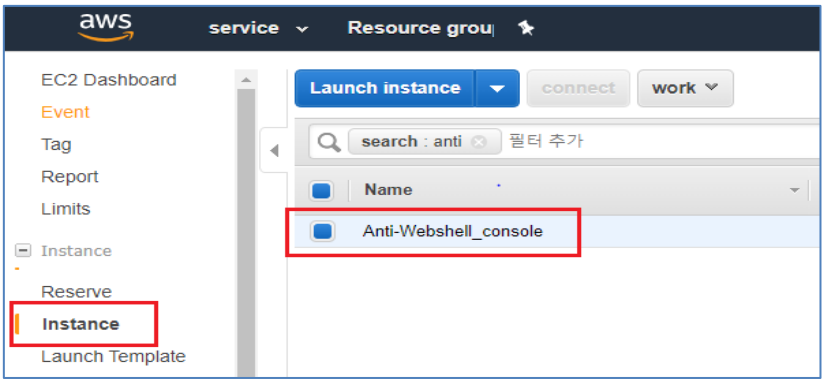
5) Skip Add tag (optional)

6) “Anti-Webshell_IAM_role” is entered in the [Role name] field > Click [Create role] button

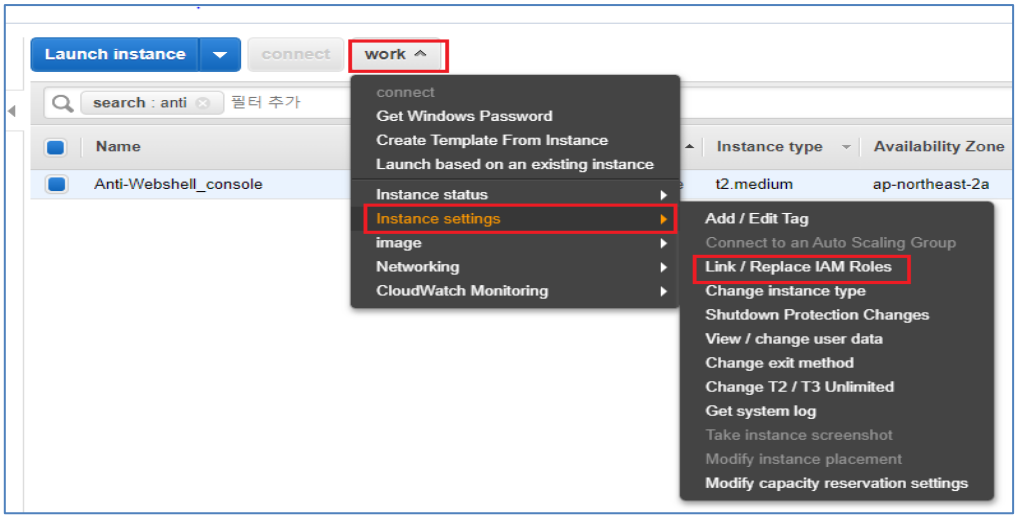
3. Apply IAM role

1) Access the AWS EC2 Management

2) Select Instance > Instance and Check Anti-Webshell console



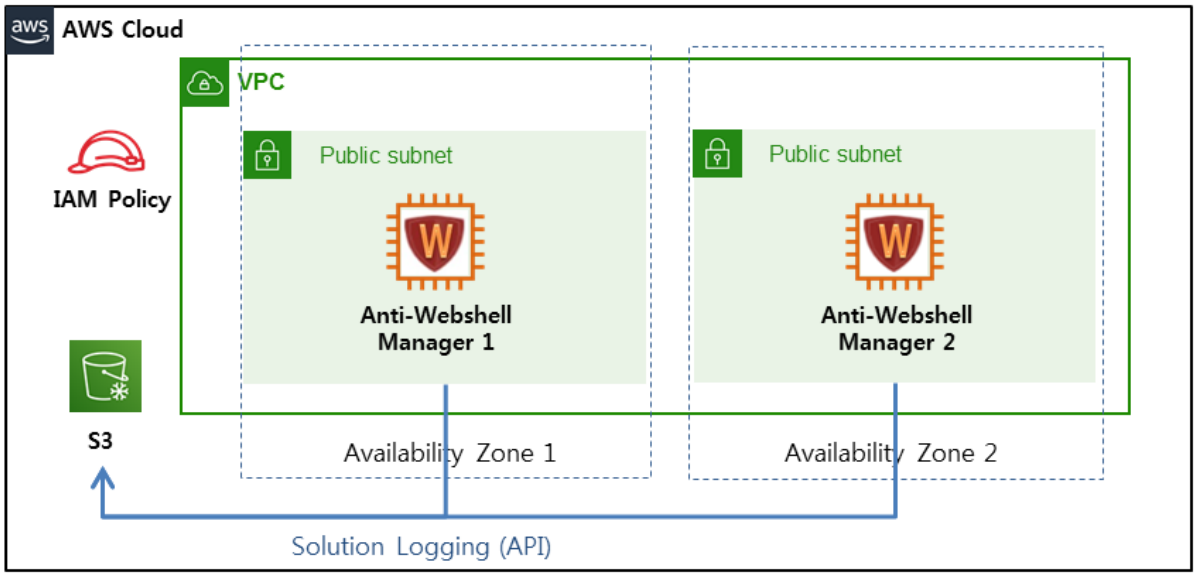
3) Click [work] button > Instance settings > Link / Replace IAM role



4) Select “Anti-Webshell_IAM_role” IAM role and Click [apply] button

4.3.2 Solution Logging Procedure with S3 Bucket

Optional: S3 Bucket to provide centralized solution logging.



SYNC through the AWS CLI to periodically store solution logs in an S3 bucket.

You can do this with the following procedure.

1. Create a S3 Bucket

   See the following link for how to create an S3.

   https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/gsg/CreatingABucket.html

2. Create IAM policy

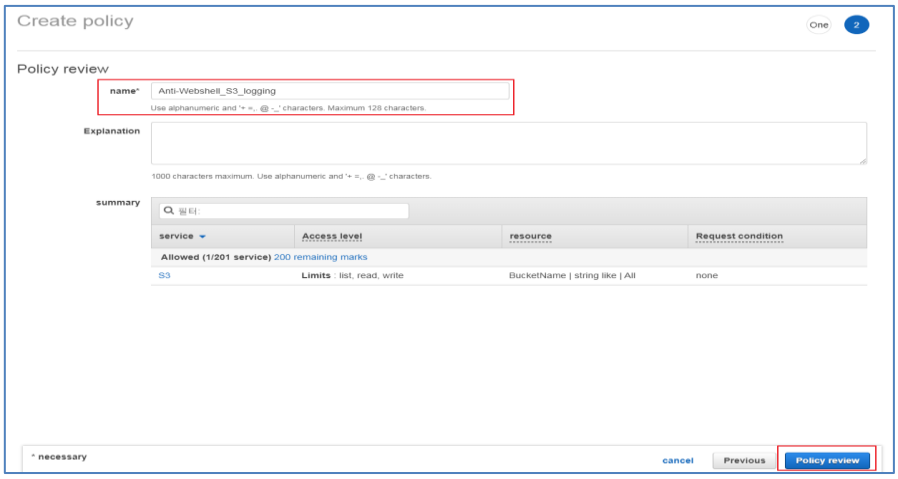
   If you are going to use S3, Anti-Webshell requires S3 access in order to create bucket and manage it. The IAM user used to manage it must have the following permissions. This shows access to all buckets in your S3 console. You can restrict to specific bucket using the appropriate resource arn.

   1) Access the AWS IAM Management
   2) Select Policy > [Create policy] button
   3) Click JSON tap > Input JSON data > Click [Policy review] button

      - Modify [s3bucket name]

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                    "Effect": "Allow",
                    "Action": [
                            "s3:GetObject",
                            "s3:ListBucket",
                            "s3:PutObject"
                    ],
                      "Resource": [
                            "arn:aws:s3:::[s3bucket name]/*"
                    ]
                }
        ]
}
```

   4) “Anti-Webshell_S3_logging” is entered in the [name] field > Click [Policy review] button



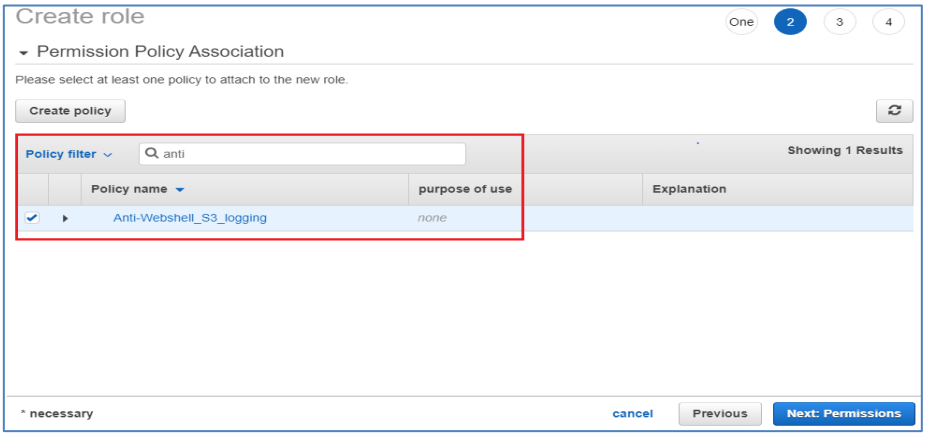
3. Create IAM role

   1) Access the AWS IAM Management

   2) Select role > [Create role] button

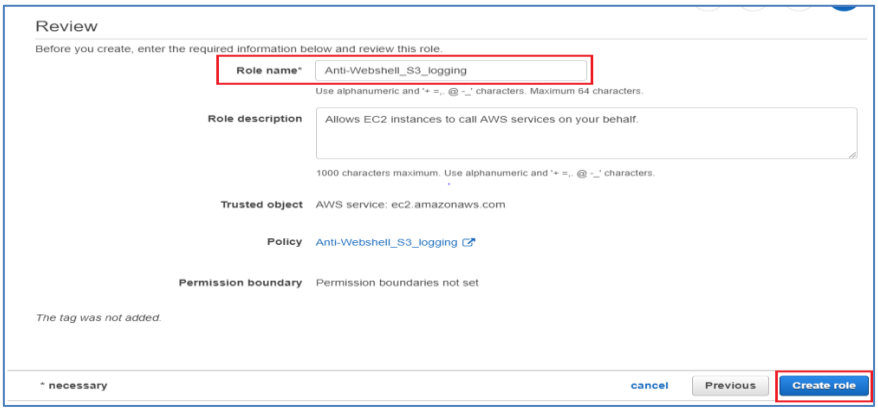
   3) Click [AWS service] and [EC2], [Next: permissions] button

   4) Check policy “Anti-Webshell_S3_logging”, Click [Next: permissions] button



   5) Skip Add tag (optional)

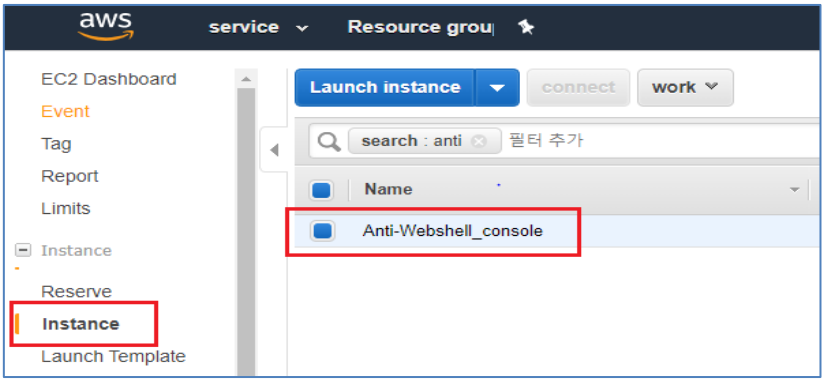
   6) “Anti-Webshell_S3_logging” is entered in the [Role name] field > Click [Create role] button



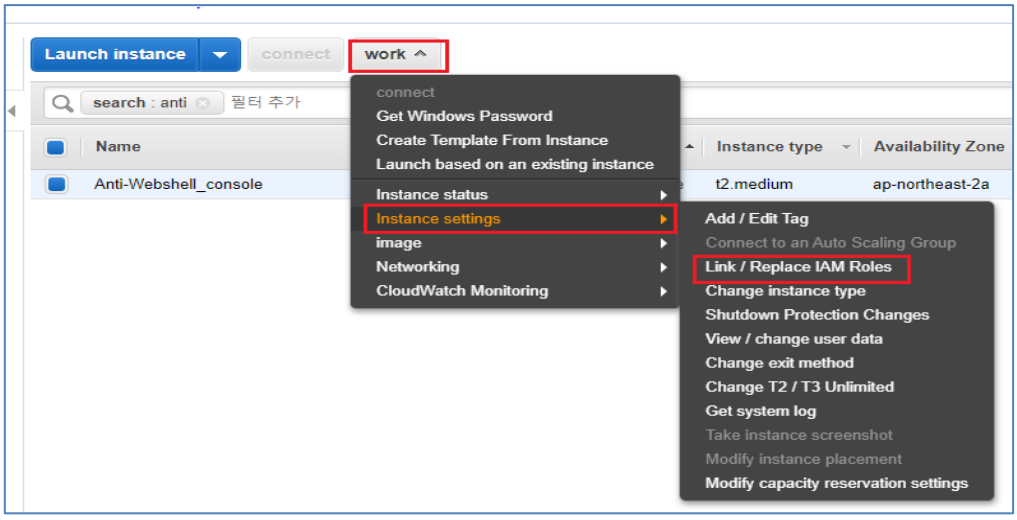
4. Apply IAM role

   1) Access the AWS EC2 Management

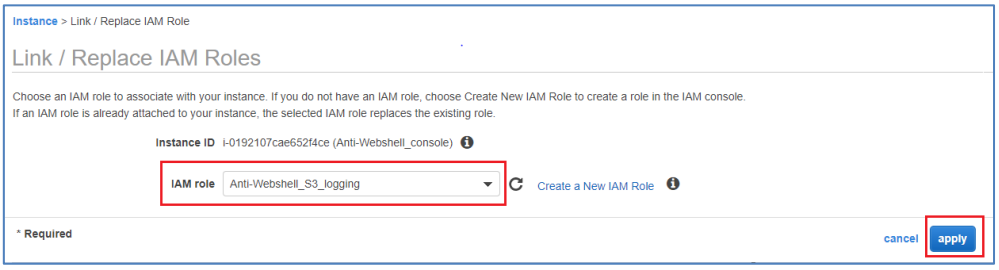
   2) Select Instance > Instance and Check Anti-Webshell console



   3) Click [work] button > Instance settings > Link / Replace IAM role



   4) Select Anti-Webshell_S3_logging IAM role and Click [apply] button



5. Modify & Run Sync Script

   1) Access Anti-Webshell Manager via SSH.

   2) In /wserver/s3sync/wserverlog_s3sync.conf, enter the S3 bucket name to store the log (①~②)

   3) Run /wserver/s3sync/wserverlog_s3sync.sh. (③)

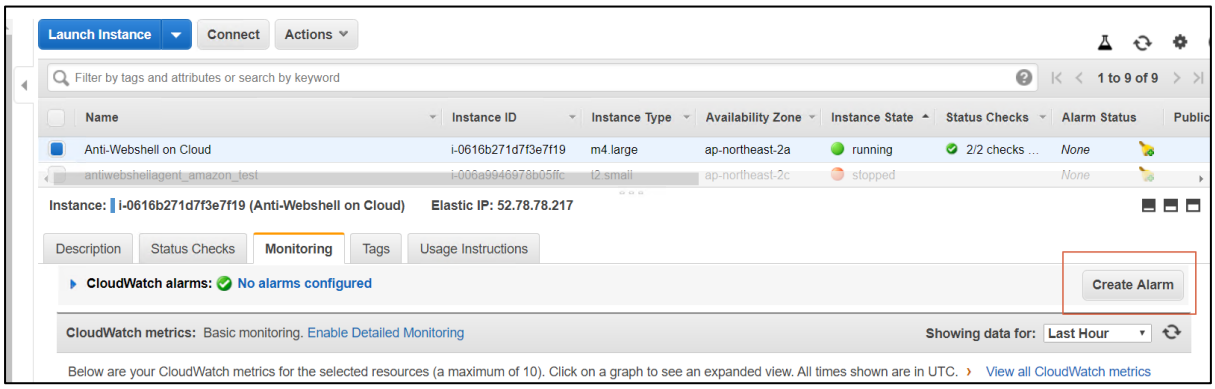
After that, the solution log (/wserver /log) is SYNC to the Private IP path of the S3 bucket set every 5 minutes.

```
① [root@localhost ~]# cd /wserver/s3sync/
② [root@localhost ~]# vi ./wserverlog_s3sync.conf
   - Modified s3bucketname
③ [root@localhost ~]# ./wserverlog_s3sync.sh
```

4.3.3 Anti-Webshell Manager Health Check with CloudWatch

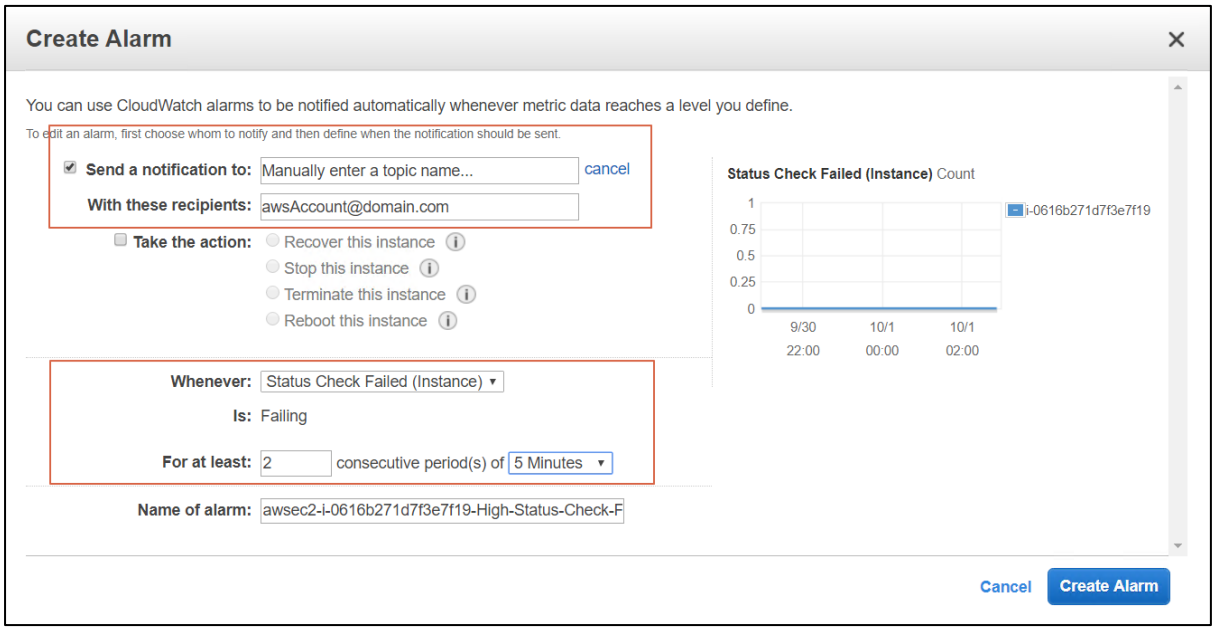
Optional: Integrates with CloudWatch to support Anti-Webshell Manager health checks with the following settings

1. Create an alarm on the deployed Anti-Webshell Manager instance.



2. Create an alarm after setting the policy in the Create Alarm tab as shown below.

Item	Input Value	Remarks
Send a notification to	Email to be notified	
Whenever	Status Check Failed(Instance)	
For at least	2 consecutive periods of 5 Minutes	



4.4 Protect Docker containers

Anti-Webshell protects your Docker hosts and containers running on Amazon ECS or Linux distributions. Anti-Webshell can do the following:

- Provide Webshell detection for the file systems used on Docker hosts and within the containers

Note

Anti-Webshell Docker protection works at the OS level. This means that the Agent must be installed on the Docker host's OS, not inside a container.

Anti-Webshell protection for the Docker host and containers

The following Anti-Webshell Agent can be used to protect the Docker host and containers:

- Webshell Detection
- Webshell Analysis/Decryption(Deobfuscation)
- Webshell Quarantine(Rename, Quarantine, delete)

Deployment considerations and limitations

- Anti-Webshell protects Amazon ECS and EC2 Instance for Docker containers in Linux environments.

- Since Anti-Webshell Agent detects webshell in file systems, the directory containing Webroot and Websource of each container must be set as Data volume.

  see the following link for set data volume for docker container or Amazon ECS.
  https://docs.aws.amazon.com/AmazonECS/latest/developerguide/using_data_volumes.html

4.5 Routine Maintenance

The latest releases and technical support services are available to help you get the most out of your product.

Maintenance costs are determined by the developer's policy and include the services associated with the latest release development and upgrade.

The details of maintenance and technical support may vary according to the license agreement.

Maintenance is largely divided as follows.

- Routine Maintenance: Routine maintenance is carried out according to the maintenance contract.

- Emergency Maintenance: Emergency maintenance is carried out according to the maintenance contract.

The maintenance scope is as follows.

- Check solution

- Managing certificates

- Patch and Upgrade

4.6 Emergency Maintenance

4.6.1 Startup process

1) Manager Startup process

A. Start

Order	Description	Command
1	Manager ssh login(ROOT)	N/A
2	Manager process start	/wserver/wserver-run.sh

3	Tomcat process start (Run in order)	1) shutdown.sh 2) startup.sh
4	httpd process start	service httpd restart

*Manager Process starts automatically on reboot

B. stop

Order	Description	Command
1	Manager ssh login(ROOT)	N/A
2	Manager process stop	/wserver/wserver-stop.sh
3	Tomcat process stop	shutdown.sh
4	httpd process stop	service httpd stop

2) Agent Startup process

A. Start

OS	Description	Command
Linux	Agent process start	/wagent/wagent_run.sh
Window	Agent process start	Start > run > "services.msc" > Anti-webshell service Run

*Agent Process starts automatically on reboot

B. stop

Order	Description	Command
Linux	Agent process stop	/wagent/wagent_stop.sh
Window	Agent process stop	Start > run > "services.msc" > Anti-webshell service Stop

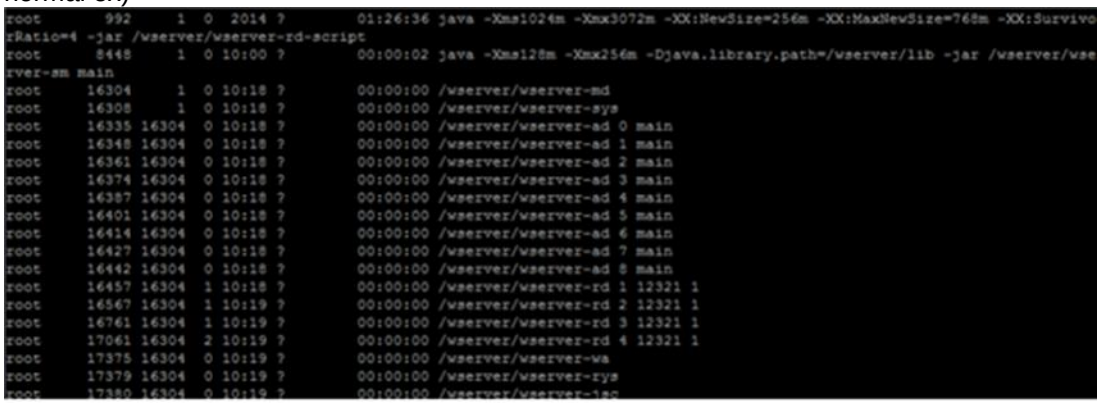
4.6.2 Health Check

1) Manager Health check

A. Manager Process check

Order	Description	Command
1	Manager ssh login(ROOT)	N/A
2	Manager process check	ps -ef | grep wserver

normal ex)



abnormal ex)

Process not detected

B. Tomcat process check

Order	Description	Command
1	Manager ssh login(ROOT)	N/A
2	Tomcat process check	ps -ef | grep tomcat

normal ex)

abnormal ex1)

- Process not detected

abnormal ex)

```
root     15869  0.1 24.6 2485996 980920 ?      Sl   2014  70:55 /usr/java/jrel.7.0_67/bin/java -Djava.util.logging.confi
g.file=/usr/tomcat7/conf/logging.properties -Dfile.encoding=UTF-8 -Dsun.jnu.encoding=UTF-8 -Dsun.io.unicode.encoding=Unic
odeLittle -Djava.net.preferIPv4Stack=true -Djava.library.path=/usr/tomcat7/lib/sigar -Djava.net.preferIPv4Stack=true -Dus
er.language=ko -Duser.region=KR -Xms1024m -Xmx1024m -XX:NewSize=512m -XX:MaxNewSize=512m -XX:PermSize=512m -XX:MaxPermSiz
e=512m -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djava.endorsed.dirs=/usr/tomcat7/endorsed -clas
spath /usr/tomcat7/bin/bootstrap.jar:/usr/tomcat7/bin/tomcat-juli.jar -Dcatalina.base=/usr/tomcat7 -Dcatalina.home=/usr/t
omcat7 -Djava.io.tmpdir=/usr/tomcat7/temp org.apache.catalina.startup.Bootstrap start
root     18230  0.0  0.0 106060   648 pts/2    S    10:22   0:00 /bin/sh /usr/tomcat7/bin/catalina.sh start
root     18231  0.0  0.0   3980   400 pts/2    S    10:22   0:00 /usr/local/cronolog/sbin/cronolog /usr/tomcat7/logs/%Y-%
m-%d.catalina.out
root     18232 86.4 12.3 2331160 491692 pts/2  Sl   10:22   0:12 /usr/java/jrel.7.0_67/bin/java -Djava.util.logging.confi
g.file=/usr/tomcat7/conf/logging.properties -Dfile.encoding=UTF-8 -Dsun.jnu.encoding=UTF-8 -Dsun.io.unicode.encoding=Unic
odeLittle -Djava.net.preferIPv4Stack=true -Djava.library.path=/usr/tomcat7/lib/sigar -Djava.net.preferIPv4Stack=true -Dus
er.language=ko -Duser.region=KR -Xms1024m -Xmx1024m -XX:NewSize=512m -XX:MaxNewSize=512m -XX:PermSize=512m -XX:MaxPermSiz
e=512m -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djava.endorsed.dirs=/usr/tomcat7/endorsed -clas
spath /usr/tomcat7/bin/bootstrap.jar:/usr/tomcat7/bin/tomcat-juli.jar -Dcatalina.base=/usr/tomcat7 -Dcatalina.home=/usr/t
omcat7 -Djava.io.tmpdir=/usr/tomcat7/temp org.apache.catalina.startup.Bootstrap start
```

C. httpd process check

Order	Description	Command
1	Manager ssh login(ROOT)	N/A
2	httpd process check	ps -ef | grep httpd

normal ex)

- A number of processes are searched.

abnormal ex)

- Process not detected

D. Manager UI Access test

Order	Description	Command
1	Manager UI Access test	Access https: //Manager IP

normal ex)

abnormal ex)

Service Temporarily Unavailable

The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later.

E. Manager resource check

Order	Description	Command
1	Manager ssh login(ROOT)	N/A
2	Manager resource check	df

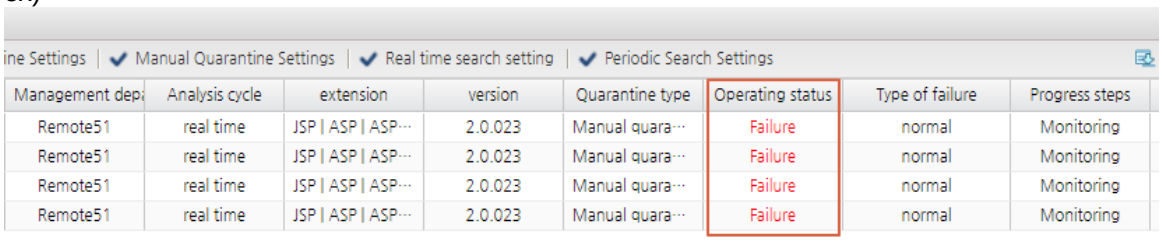
```
[root@localhost ~]# df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
                      27678892   4189988  22060220  16% /
/dev/xvda1              101086     36768     59099  39% /boot
tmpfs                   524288         0    524288   0% /dev/shm
```

2) Agent Health check

A. Agent Process check

Order	Description	Command
1	Manager login(WEB UI)	Access https: //Manager IP
2	"Failure" output in [Management UI]> [Agent Management]> [Operating status] when an agent fails	N/A

ex)



Management dep	Analysis cycle	extension	version	Quarantine type	Operating status	Type of failure	Progress steps
Remote51	real time	JSP | ASP | ASP···	2.0.023	Manual quara···	Failure	normal	Monitoring
Remote51	real time	JSP | ASP | ASP···	2.0.023	Manual quara···	Failure	normal	Monitoring
Remote51	real time	JSP | ASP | ASP···	2.0.023	Manual quara···	Failure	normal	Monitoring
Remote51	real time	JSP | ASP | ASP···	2.0.023	Manual quara···	Failure	normal	Monitoring

4.6.3 Types of Anti-Webshell failures

1) Manager

- Manager failure due to AZ failure
- Insufficient server resources - EBS capacity
- Network blocking by security devices

2) Agent

- Agent failure due to Instance or AZ failure
- Insufficient agent installation server resources - EBS capacity
- Network blocking by security devices

4.6.4 Recovery procedure for Anti-Webshell failure

1) Manager

When a Manager failure occurs, recovery is proceeding in the following order.

Case 1. Manager failure due to AZ failure

1. Manager process restart

A. Stop Manager according to [4.6.1 Startup process > 1) Manager Startup process > B. stop] procedure

B. Start Manager according to [4.6.1 Startup process > 1) Manager Startup process > A. start] procedure

2. Manager Instance reboot

Case 2. Insufficient server resources - EBS capacity

1. Optimize Manager resource capacity

If the capacity of "/" is 100%, optimization measures are required.

Proceed to next step to optimize.

- data or data optimize script path: /wserver/data

A. Run /wserver/data/dataclean.sh

B. Check the disk size using the “df -h” command

2. Manager process restart

A. Stop Manager according to [4.6.1 Startup process > 1) Manager Startup process > B. stop] procedure

B. Start Manager according to [4.6.1 Startup process > 1) Manager Startup process > A. start] procedure

3. Manager Instance reboot

Case 3. Network blocking by security devices

1. Network and SecurityGroup Check

Source	Destination	Port	Use
WEB/WAS Server (Agent install)	Anti-Webshell Manager	12251~12259	Manager, Agent communication

2. Manager process restart

A. Stop Manager according to [4.6.1 Startup process > 1) Manager Startup process > B. stop] procedure

B. Start Manager according to [4.6.1 Startup process > 1) Manager Startup process > A. start] procedure

3. Manager Instance reboot

2) Agent

When a Agent failure occurs, recovery is proceeding in the following order.

Case 1. Agent failure due to Instance or AZ failure

- Agent process restart

A. Stop Agent according to [4.6.1 Startup process > 2) Agent Startup process > B. stop] procedure

B. Start Agent according to [4.6.1 Startup process > 2) Agent Startup process > A. start] procedure

Case 2. Insufficient agent installation server resources- EBS capacity

1. Optimize agent installation server resource capacity

If the capacity of "/" is 90%~100%, optimization measures are required.

Proceed to next step to optimize.

A. Optimize agent installation server resource

B. Check the disk size using the “df -h” command

2. Agent process restart

A. Stop Agent according to [4.6.1 Startup process > 2) Agent Startup process > B. stop] procedure

B. Start Agent according to [4.6.1 Startup process > 2) Agent Startup process > A. start] procedure

Case 3. Network blocking by security devices

1. Network and SecurityGroup Check

Source	Destination	Port	Use
WEB/WAS Server (Agent install)	Anti-Webshell Manager	12251~12259	Manager, Agent communication

2. Agent process restart

A. Stop Agent according to [4.6.1 Startup process > 2) Agent Startup process > B. stop] procedure

B. Start Agent according to [4.6.1 Startup process > 2) Agent Startup process > A. start] procedure

4.6.5 Recovery procedure when Anti-Webshell recovery fails

1) Manager

Depending on whether there is a snapshot when Manager recovery fails, you can either recover or choose to reinstall.

A. Recreate AMI with snapshot of existing Installation Manager

B. Manager reinstall

- Reinstall Manager according to [3.1.2 Create Instance] procedure

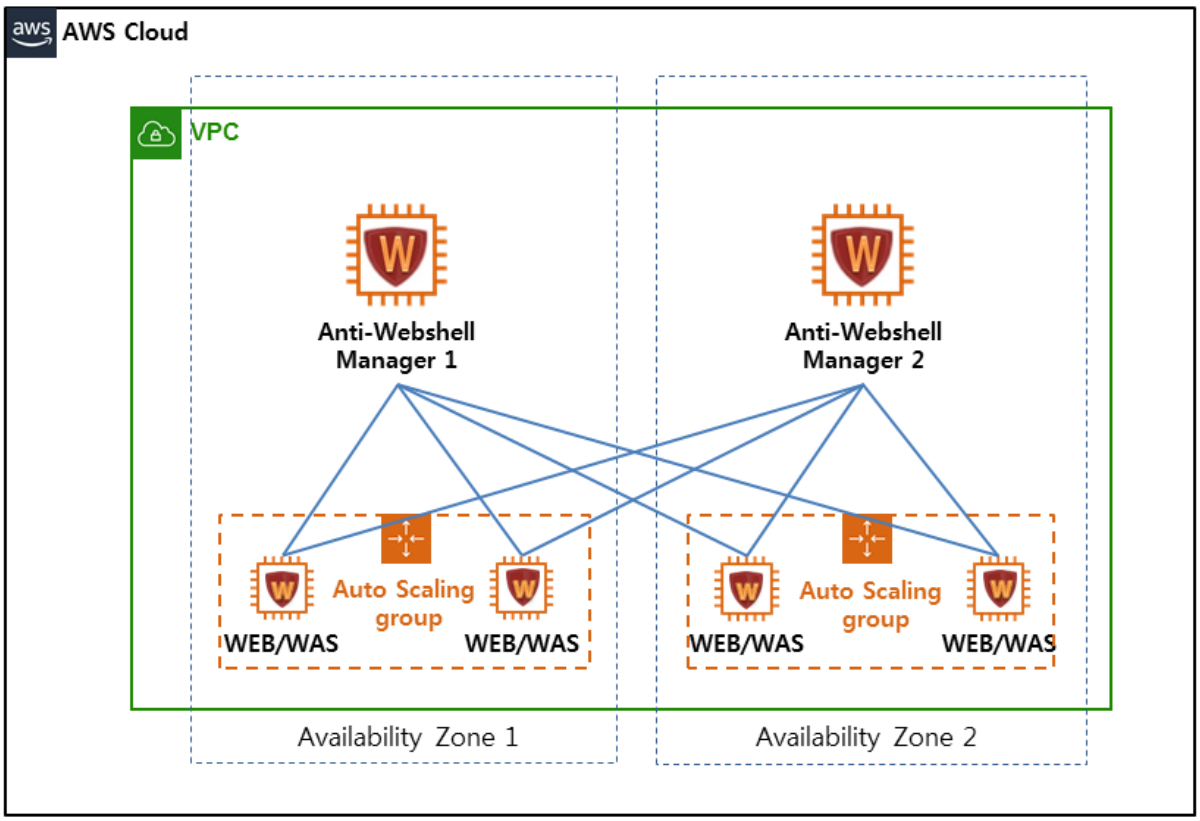
2) Agent

- Redeploy Agent according to [3.3 Step 3. Deploy the Anti-Webshell Agent] procedure

4.6.6 Anti-Webshell solution disaster recovery testing

When using multiple AZ configurations, proceed with the disaster recovery test in the following order.

This test is intended for various failure situations such as service, instance, and AZ failures.



1) Anti-Webshell Manager 1 Instance stop

2) Access Anti-Webshell Manager 2 and check whether the service is normal.

3) Anti-Webshell Manager 1 Instance start

4) Access Anti-Webshell Manager 1 and check whether the service is normal.

4.7 RTO

When a single configuration is deployed, an RTO will occur when a Manager failure occurs. You need recreate AMI with snapshot of existing installation manager and reinstall Manager AMI. At this point RTO will occur at least 10 minutes to a maximum of 30 minutes

5. System Management

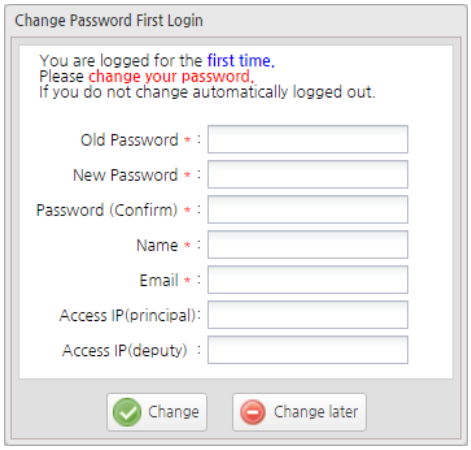
5.1 Log In

Run a web browser (Firefox, Chrome, Internet Explorer 10 or higher) on a manager PC. Then, type in ‘https://Anti-Webshell manager public ip’ in the web browser’s address bar and press the [Enter] or click on the [Navigate] button. To log in to the Anti-Webshell management server’s Web Manager, type in the manager ID and password entered when installing the agent, and click on the [Login] button.

Menu	Description
ID	Type in the manager ID entered (created) when installing the agent.
Password	The initial password was set as 1infosec!@# by default. After the first login, you should change the password.

At the first login, a window for changing your password and entering your e-mail address will pop up. Enter the existing password, a new password and some manager information, and then click on the [Change] button.

A password must be 8 digits or longer, and must contain special character(s) and number(s).



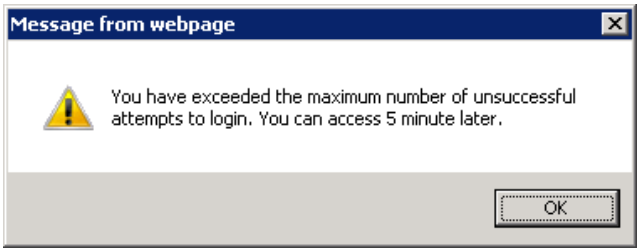
5.2 Log Out

If you want to log out after using the Anti-Webshell server, press the “Log Out” at the upper right corner. The security policy settings will remain valid even after logged out.

Cautions

Account Lockout

If you enter invalid manager passwords for the management server’s Web Manager 5 times in a row, your account will be locked out for 5 minutes so that no authentication can be executed. Try an authentication process after unlocked. If you type in a valid password while locked out, the following message will be displayed.



Automatic Logout

If no keyboard or mouse entry has been executed for the specified time set by a web manager of the Anti-Webshell server after logged in as the manager, the interactive session with the manager will automatically end, hence forcing the manager automatically log out.

Loss of Password

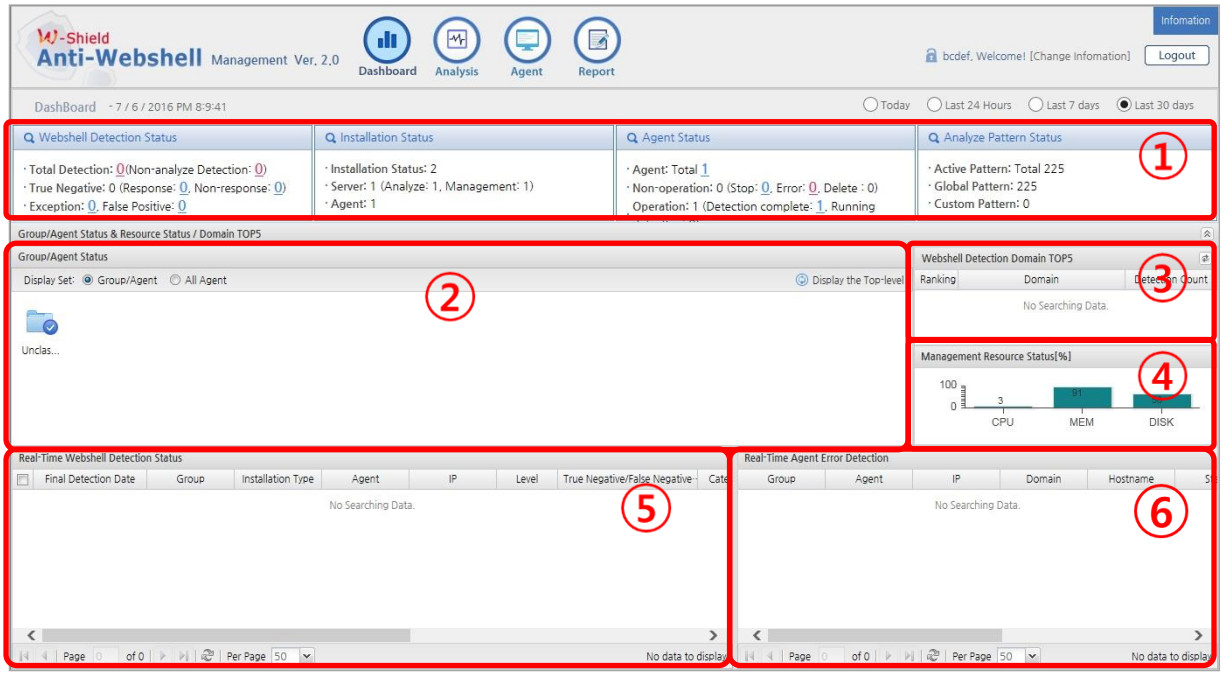
Any Anti-Webshell manager’s password cannot be recovered if lost. Please take extra care not to lose your password.

5.3 Main Menus

The following submenus comprise the management server's security management:

Menu	Description
Dash board	It is the first page you will see when accessing the management server's Web UI. In addition, it provides various detection statuses (e.g. webshell detection status, installation status, agent status, analysis pattern status, etc.).
Analysis	Depending on an agent policy, it identifies a file to be added, modified or webshell-detected. In addition, it provides relevant features required to block the execution of certain functions (e.g. Delete, Isolate, Rename, etc.).
Agent	It provides relevant features required to query, register, modify or delete an agent policy.
Report	It provides relevant features required to draft a report about system operation details and webshell detection/countermeasure details.

If you click on the Dashboard icon, the information about webshell detection status and system operation status will be displayed.



Category	Description
❶ Status Summary	• Webshell detection status • Installation status • Agent status • Analysis pattern status

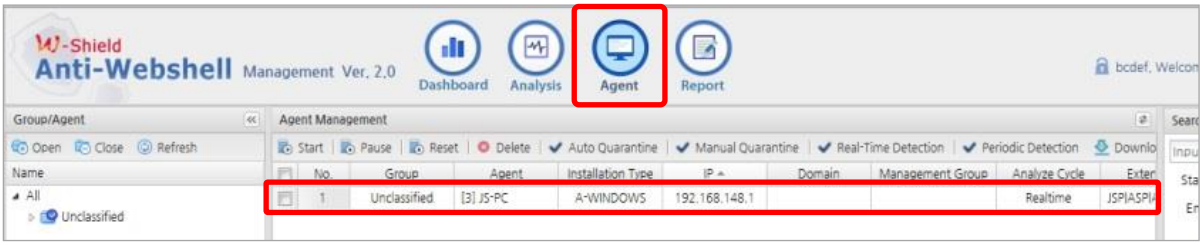
❷ Group/Agent Status	The operation status of an installed agent will be displayed on a server to be controlled. Each server represents an agent policy (menu: **Agent**). If you hover the mouse over it, relevant information will be displayed on the Tool Tips. You can check each server's status information.
❸ Webshell Detection Domain TOP 5	It shows top 5 domains with the most webshells detected up to date.
❹ Management Resource Status	The management server's resource usage (CPU, MEMORY, DISK) will be displayed on a real-time basis.
❺ Real-time Webshell Detection Status	The webshell detection status will be displayed on a real-time basis.
❻ Real-time Agent Error Detection	All agent errors detected will be displayed on a real-time basis.

Cautions

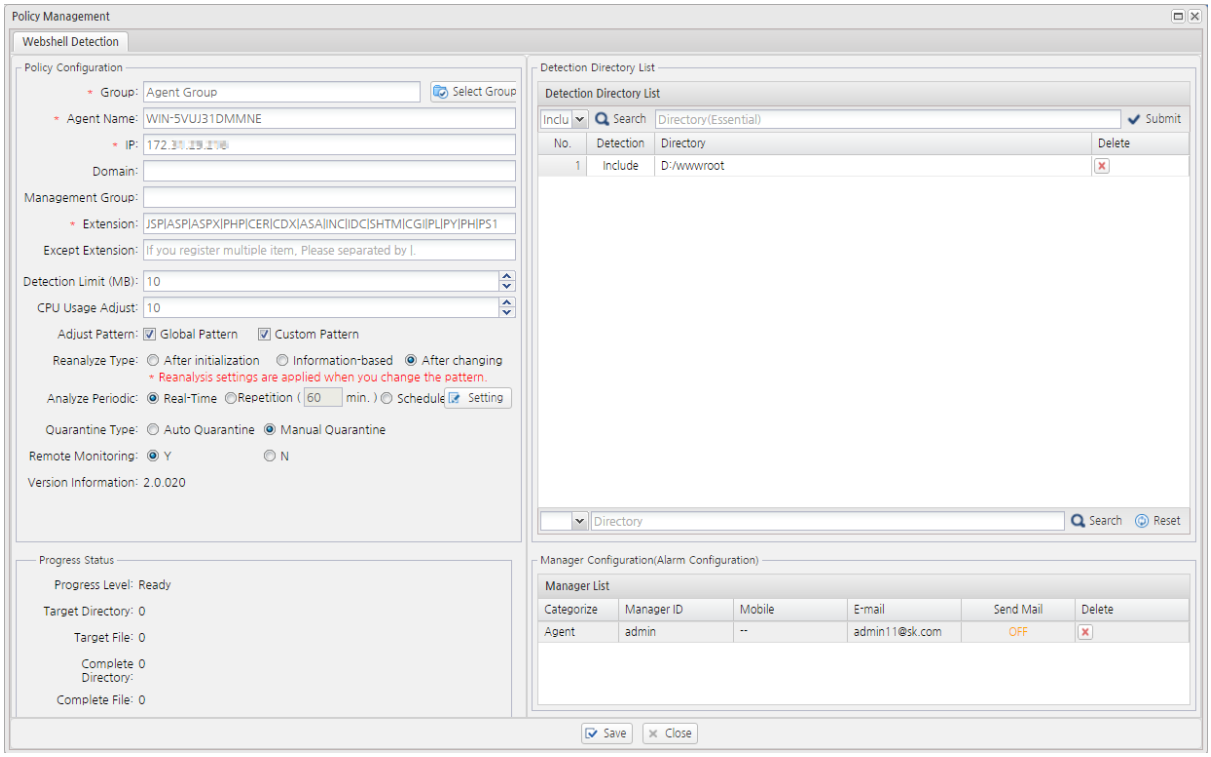
Agent Error
When an agent error is occurred, a webshell cannot be detected normally.
When any error is occurred, check if an agent is currently running and if the communication between the management server and the agent is working properly. Then, take proper countermeasures.

5.4 Registering the Webshell Detection Policy

Click on the [Agent] menu at the top of the Manager Page. Double-click on the agent item displayed on the page to open the Policy Management window.



Configure a webshell analysis policy on the Policy Management window.



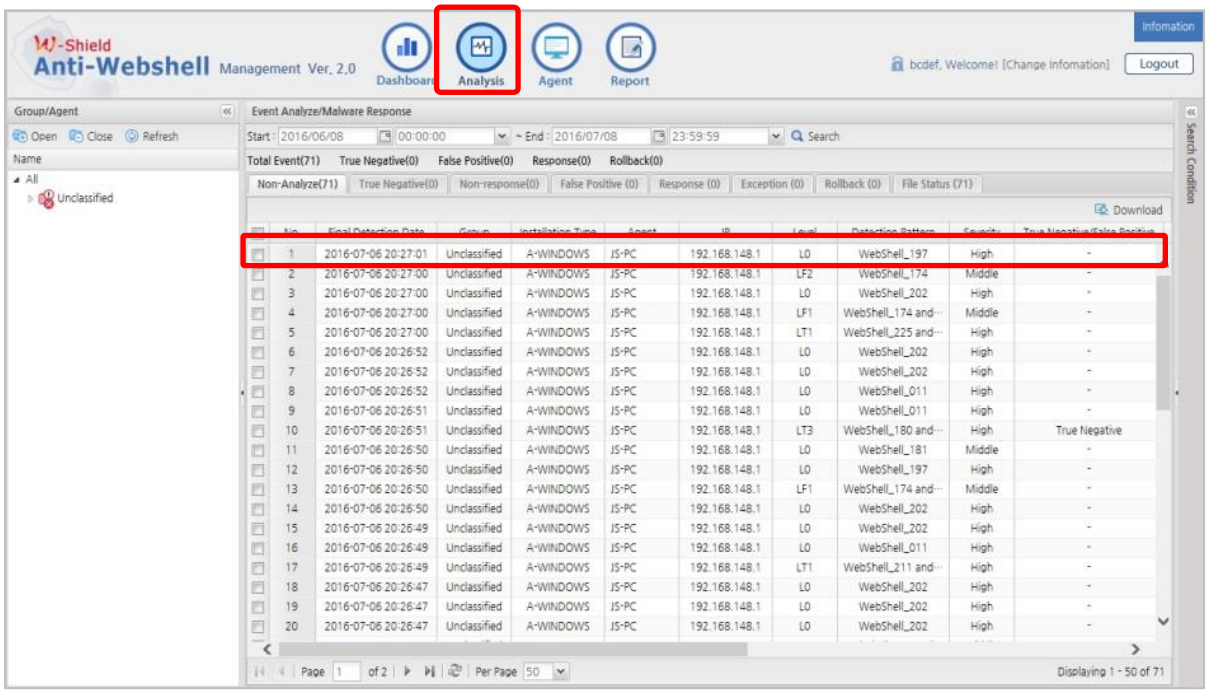
Category	Description
Group	Name of a group to which an agent belongs
Agent Name	Name of an agent
IP	IP address of an agent
Domain	Web server domain where an agent is installed e.g.) www.skinfosec.co.kr
Management Group	Information about an agent manager or management division
Extension	File extension of a file to be analyzed
Except Extension	File extension of a file to be excluded from analysis
Detection Limit (MB)	Setting of the size of a file to be analyzed (0~10Mb) e.g.) If “5” is entered, any file with size over 5MB will be excluded from analysis.
CPU Usage Adjust	Adjustment of an agent program’s CPU usage
Adjust Pattern	Setting of certain patterns to be applied to analysis • Global pattern: Pattern provided by the program manufacturer • Unique pattern: Pattern created based on user needs ⇨ These are default settings. Therefore, no change is allowed.

Reanalyze Type	Reanalysis methods when a policy is changed • After initialization: Once initialized, all files to be analyzed will be reanalyzed. • Information-based: Those files that have been modified within 1 years will be reanalyzed. • After Changing: Those files that have been created or modified after a policy was changed will be reanalyzed.
Analyze Periodic	Setting of the analysis cycle of a server to be detected • Real-time: Real-time detection • Recurring: Cycle-based detection (hours/minutes) • Schedule: Schedule-based detection
Quarantine Type	Whether the quarantine of a detected webshell file is to be performed automatically or manually will be determined. If the quarantine type is set to be automatic when attempting to detect webshells, only the webshells detected as true negative ones will be automatically moved to the quarantine station.
Remote Monitoring	Setting of remote control service • Y: Enabling of remote control service (additional fee incurred) • N: In-house operation without any additional service
Progress Status	Display of an agent's analysis progress • Progress Level: Analyzing / Downloading / Waiting • Target Directory: Number of directories to be analyzed • Target file: Number of files to be analyzed • Complete Directory: Number of directories analyzed • Complete File: Number of files analyzed
Detection Directory List	Click on the Search button to select a directory. Then, decide if the directory will be included in or excluded from analysis, and submit it accordingly. • If there are many directories to be analyzed, higher-depth directories should be submitted as 'included' ones while lower-depth directories should be submitted as 'excluded' ones. • If there are few directories to be analyzed, only the directories to be analyzed should be submitted as 'included' ones.
Manager List	Specify an agent manager and decide whether to send an alert e-mail to the manager or not. • The "Send Mail" option is set "ON" if you want to send an e-mail to the specified e-mail address when a webshell is detected.

5.5 Webshell Analysis/Countermeasure

When a webshell is detected, an alert e-mail will be sent to a registered e-mail address, or the webshell will be displayed on the Dashboard's Real-Time Webshell Detection Status. When a webshell is detected, the manager shall perform analysis. If it is confirmed to be a webshell, he shall take proper countermeasures (e.g. Delete, Isolate, Rename File, etc.).

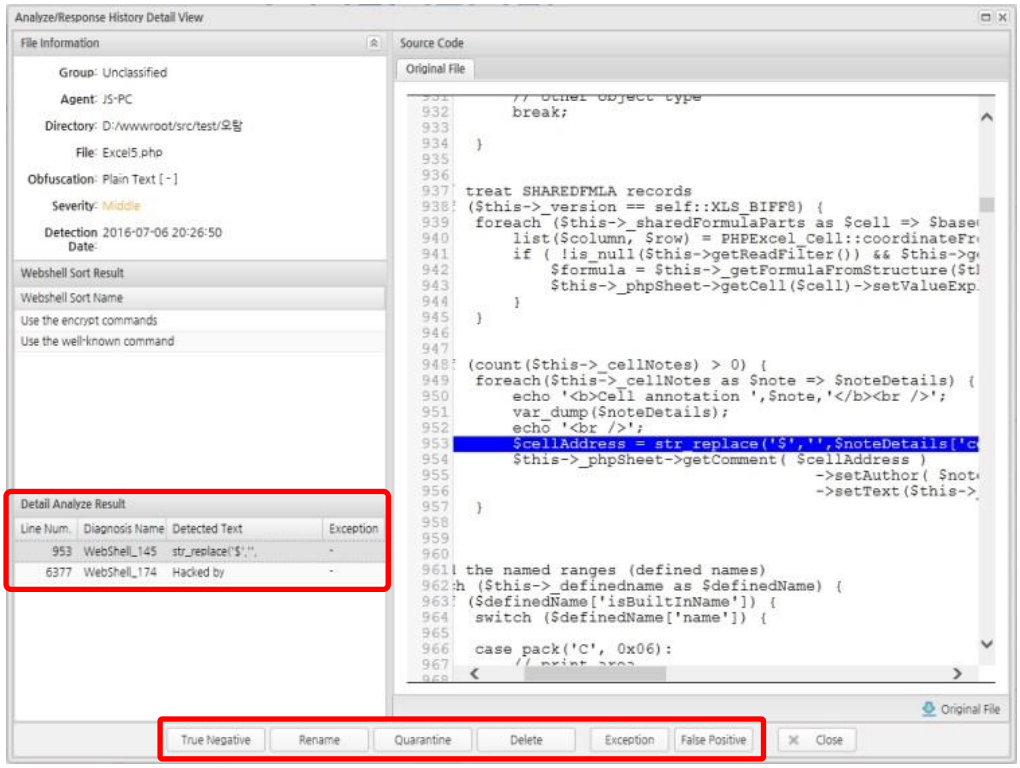
When a webshell is detected, click on the [Analysis] menu at the top of the Manager Page. Double-click on the detected item displayed on the page to check its details.



If you click on an item displayed on the Detail Analyze Result, the item will be moved from the Source Code in the right to a corresponding location. If it is confirmed to be a webshell based on the analysis result, immediate countermeasures should be taken to prevent its execution. See the table below for proper countermeasures.

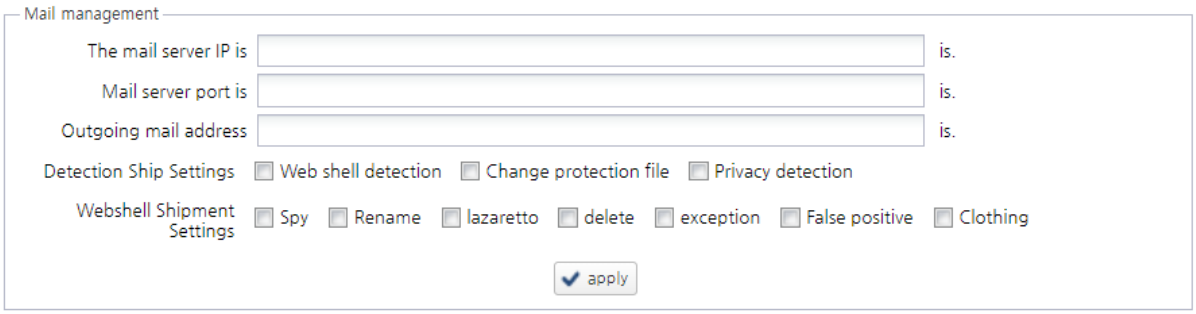
Category	Description
True Negative	If the detected file was confirmed to be a webshell file, it will be set as a "True Negative" webshell. This is required for the categorization of management UIs, and is used for managing all detected files. The following measures should be taken: Rename, Move to Quarantine Station, Delete, and so forth.
Rename	The name and extension of a webshell-detected file will be edited to prevent its execution.
Quarantine	A webshell-detected file will be isolated to the quarantine station to prevent its execution. The quarantine station's location is as follows: Windows (C:\AntiWebshell\data\qrnt); Linux (/wagent/data/qrnt/).
Delete	A webshell-detected file will be deleted to prevent its execution. Since any deleted file cannot be restored, extra caution should be taken.

Exception	If a detected file is confirmed not to be a webshell file, future detection will be disabled. Since no analysis is performed for any disabled file even after it has been edited, extra caution should be taken.
False Positive	If a detected file is confirmed not to be a webshell, it will be set as a false positive one. If a false positive file is edited, analysis will be performed again.



5.6 Set event alerts and receive notifications

Click on the [System administration] menu at the top of the Manager Page. Click on the system settings item displayed on the page. Can set event alerts in Mail management



1. The mail server IP is : Enter mail server IP

2. Mail server port is : Enter mail server port

3. Outgoing mail address : Enter mail server address

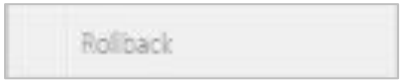
4. Detection Ship Settings : Check for detection types to be notified

5. Webshell Shipment Settings : Check Webshell processing types to be notified

5.7 Rollback

Rollback is a function designed to restore an item quarantined (Rename, Quarantine, Exception, False Positive) to its original state. If it is confirmed to be a normal file after quarantined, it will be restored to its original state.

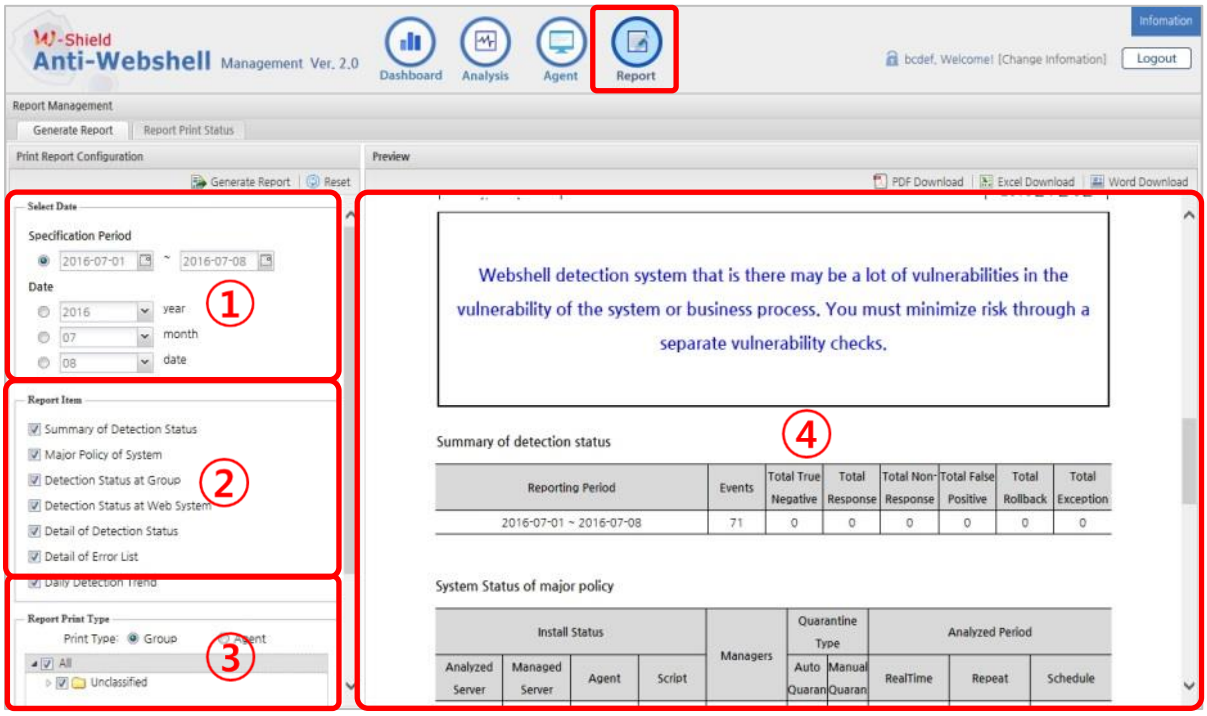
Navigate to each tab menu **(True Negative | False Positive | Response | Exception)** on the **[Analysis] menu**, select an item to be restored, and select [Rollback] on a popup menu. Then, it will be restored to its original state.



5.8 Drafting a Report

Click on the [Report] menu at the top of the Manager Page. Click on the item displayed in the right to draft a report.

You can download a drafted report in PDF, MS-Word or MS-Excel.



Category	Description

❶ Select Date	The period to create a report will be set. You can set the period by year, by month or by date.
❷ Report Item	When a report is created, an item to be included will be selected.
❸ Report Print Type	When a report is created, an agent to be included will be selected.
❹ Preview	Depending on an item selected, a drafted report can be previewed.

5.9 KEY Rotation management

A. S3 Key management

If necessary, SSE-S3 can be configured to support S3 encryption.

See the following link for KEY management for S3 encryption.
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html

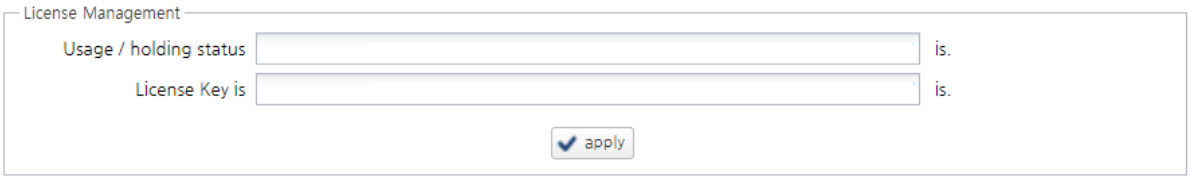
B. RDS Key Management

See the following link for KEY management for RDS encryption.
https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/UserGuide/Overview.Encryption.Keys.html

5.10 License management

1. View license

Click on the [System administration] menu at the top of the Manager Page. Click on the system settings item displayed on the page. Can check the available licenses and register license keys in License Management.



2. Edit license

Can edit licenses in License Management. Registered licenses cannot be deleted. New license registration is entered in the [License Key is] field and click the [Apply] button

5.11 Patches and updates management

The patches/updates will be automatically processed quarterly according to the license agreement

6. Support

6.1 Technical support

The scope of technical support services is provided only for the functions specified in the document such as the integrated manual.

The technical support scope is as follows.

- 24 X 7 Disability / Technical Support
- Installation support: installation guide and installation manual

Technical support contacts are as follows.

- E-mail : wshield-skinfosecaws@sk.com

6.2 Support Costs

Technical support is provided under a license agreement.

6.3 SLA

SLA is provided under a license agreement.

7. Deploy the Quick Start

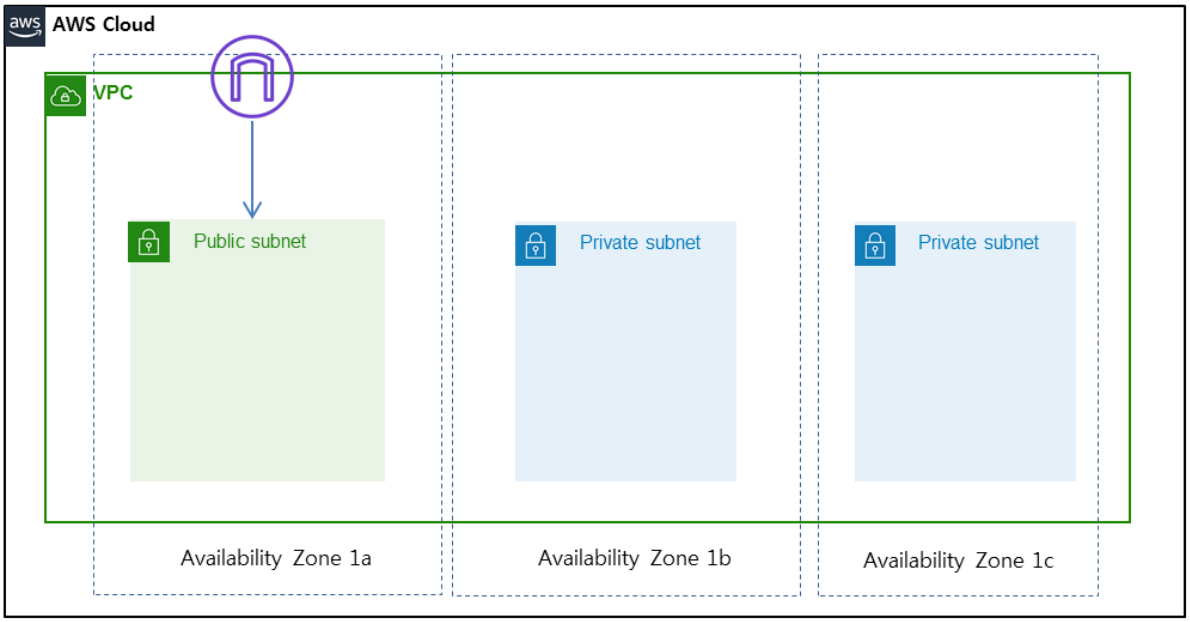
The AWS CloudFormation templates provided with this Quick Start automate the deployment of Anti-Webshell on the AWS Cloud.

7.1 Step 1. Set up a VPC

The AWS Quick Start deploys Anti-Webshell into an existing VPC. Before you launch the Quick Start, you must create a VPC that has two private subnets in different Availability Zones, and one public subnet with an attached internet gateway

- ✓ **Important:** Although it is possible to use the Quick Start to deploy Anti-Webshell into a default VPC with all public subnets, this is not recommended because of the large attack surface it creates.

Prerequisite VPC architecture:



7.2 Step 2. Deploying with AWS CloudFormation

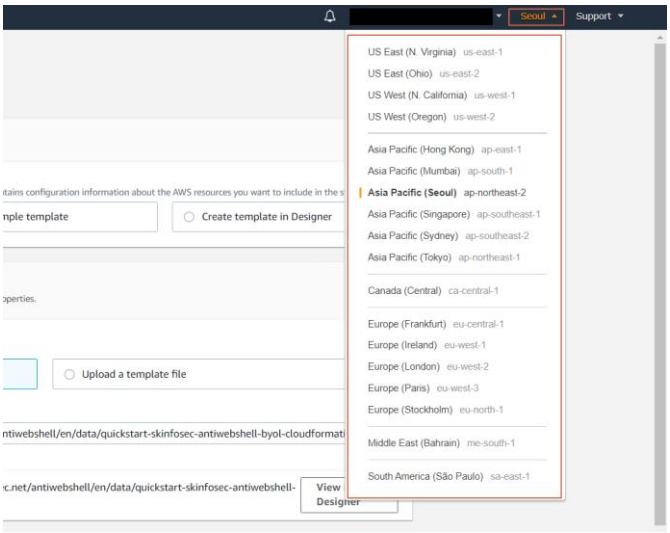
In this step, you will launch an AWS CloudFormation template that deploys Anti-Webshell into your existing VPC.

- ✓ You are responsible for the cost of the AWS services used while running this Quick Start reference deployment, and licensing fees for Anti-Webshell. There is no additional cost for using this Quick Start. See the pricing pages for each AWS service you will be using in this Quick Start for full details.

1. Sign in to your AWS account.
2. Use the following links to launch the AWS CloudFormation template.

   Launch Quick Start for BYOL option

3. The template is launched in the ap-northeast-2 (Seoul) region by default. You can change the region by using the region selector in the navigation bar.



✓ For information about region support, see the following section: [1.1.2 Region support]

4. On the Select Template page, keep the default URL for the AWS CloudFormation template, and then choose Next.

5. On the Specify Details page, provide the details about your Amazon VPC and how you want Anti-Webshell to be deployed in it.

   Network Configuration:

Parameter label	Parameter name	Default	Description
VPC for Anti-Webshell Components	AWSVPC	Requires input	The VPC where the Quick Start resources will be deployed. This VPC must contain one private subnets and one public subnet with a connected internet gateway.
Public Subnet for Anti-Webshell Managers	AntiWebshellSubnet	Requires input	The subnet to deploy the Anti-Webshell Manager and load balancers in. This subnet must be in the VPC specified by the VPC for Anti-Webshell Components parameter and must be a public subnet with an attached internet gateway.
Primary private subnet for RDS	AntiWebshell DatabaseSubnet1	Requires input	The private subnet where the Amazon RDS database will be deployed. This subnet must be in the VPC specified by the VPC for Anti-Webshell Components parameter.
Secondary private subnet for RDS	AntiWebshell DatabaseSubnet2	Requires input	The private subnet where the Amazon RDS database will be deployed. This subnet must be in the VPC specified by the VPC for Anti-Webshell Components parameter.

Anti-Webshell Manager Configuration:

Parameter label	Parameter name	Default	Description
EC2 Key Pair for SSH access	AWSKeyPairName	Requires input	The key pair that will be used to launch the EC2 instances that contain the Anti-Webshell Manager. This key pair can be used

			to create an SSH connection to your Anti-Webshell Manager.
AntiwebshellManager InstanceType	AntiwebshellManager InstanceType	M5.large	-
IAM role is added to AntiWebshell Manager	AntiWebshellManager IAMPolicyName	Anti-Webshell_IAM_role	An IAM role is created with the specified name and applied to the Anti-Webshell Manager.

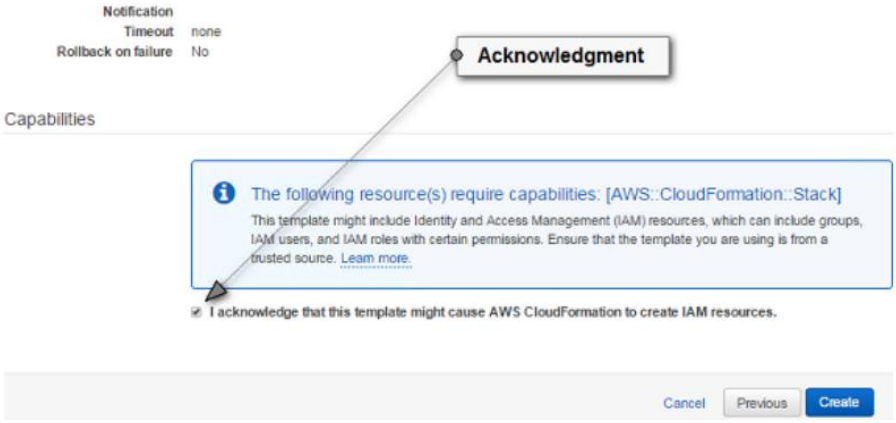
RDS Configuration:

Parameter label	Parameter name	Default	Description
Administrator password for RDS Instance	DatabaseAdminPassword	Requires input	The password for the Amazon RDS administrator account. This must be 8-41 characters long and can only contain alphanumeric characters or these special characters: !^*-_+
DatabaseInstanceType	DatabaseInstanceType	DB.M5.Large	-

When you finish reviewing and customizing the parameters, choose Next.

6. On the Options page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you're done, choose Next.

7. On the Review page, review and confirm the template settings. Under Capabilities, select the check box to acknowledge that the template will create IAM resources. Anti-Webshell Manager requires this access to be able to see your AWS instances and protect them. console.



8. Choose Create to deploy the stack.

9. Monitor the status of the stack. When the status displays CREATE_COMPLETE, the Anti-

Webshell deployment is ready.

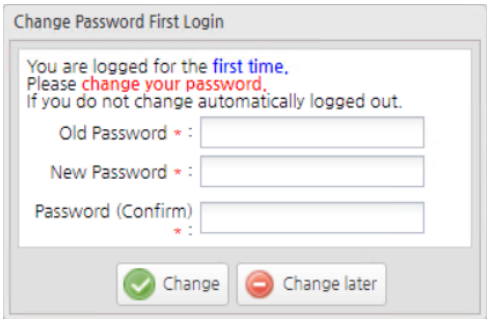
7.3 Step 3. Log in to the Anti-Webshell Manager Web Console

1. Run a web browser (Firefox, Chrome, Internet Explorer 10 or higher) on a manager PC. Then, type in 'https://Anti-Webshell manager public ip' in the web browser's address bar and press the [Enter] or click on the [Navigate] button. To log in to the Anti-Webshell management server's Web Manager, type in the manager ID and password entered when installing the agent, and click on the [Login] button.

Menu	Description
ID	wdc_admin (default)
Password	The initial password was set as 1infosec!@# by default. After the first login, you should change the password.

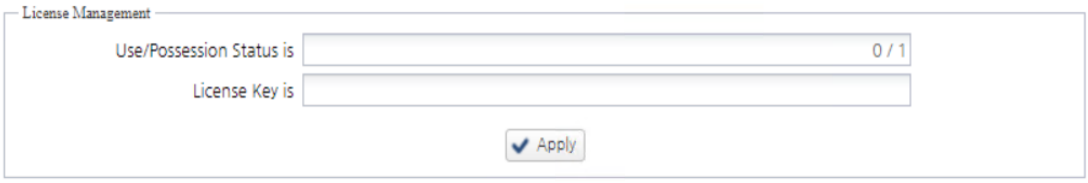
At the first login, a window for changing your password will pop up. Enter the existing password, a new password and some manager information, and then click on the [Change] button.

A password must be 8 digits or longer, and must contain special character(s) and number(s).



2. License registration

Register your license. New license registration is entered in the [License Key is] field and click the [Apply] button



7.4 Step 4. Deploy Anti-Webshell Agent to New Instances

Now that you have Anti-Webshell in your AWS Cloud account, you can start protecting your instances. For information on how to deploy agents, follow [3.3 Step 3. Deploy the Anti-Webshell Agent]