Installing Anti-Webshell V2.0 on AWS



Table of Contents

1. Product Overview	4
1.1 Introduction	4
1.1.1 Prerequisites and Requirements	5
1.1.2 Region support	5
1.1.3 Architecture Diagrams	6
1.1.4 Use Cases	8
2. Planning Guidance	8
2.1 Security	8
2.2 Costs and Licenses	8
2.3 Sizing	9
3. Deployment steps	10
3.1 Step 1. Anti-Webshell Manager Installation	10
3.1.1 Create VPC and Subnet	10
3.1.2 Create Network ACLs	13
3.1.3 Create Security Group	17
3.1.4 Create RDS	21
3.1.5 Create Instance	22
3.2 Step 2. Anti-Webshell Manager Initial setting	
3.2.1 License Registration	
3.3 Step 3. Deploy the Anti-Webshell Agent	29
3.3.1 Linux	29
3.3.2 Windows	30
4. Operational Guidance	33
4.1 Supports Anti-Webshell Manager backup and restore in aws	
4.1.1 Anti-Webshell Manager backup and restore	33

SK infosec co., ltd.

	4.1.2 Amazon RDS backup and restore	. 34
	4.2 Manual Scaling Procedure for Anti-Webshell on AWS	.35
	4.3 Add AWS resources to Anti-Webshell Manager	. 36
	4.3.1 Add an AWS IAM role to Anti-Webshell Manager	. 36
	4.3.2 Solution Logging Procedure with S3 Bucket	. 39
	4.3.3 Anti-Webshell Manager Health Check with CloudWatch	.43
	4.4 Protect Docker containers	.44
	4.5 Routine Maintenance	.45
	4.6 Emergency Maintenance	.45
	4.6.1 Startup process	.45
	4.6.2 Health Check	.47
	4.6.3 Types of Anti-Webshell failures	.49
	4.6.4 Recovery procedure for Anti-Webshell failure	. 50
	4.6.5 Recovery procedure when Anti-Webshell recovery fails	. 52
	4.6.6 Anti-Webshell solution disaster recovery testing	. 52
	4.7 RTO	. 53
5	. System Management	. 53
5	. System Management 5.1 Log In	. 53 . 53
5	. System Management 5.1 Log In 5.2 Log Out	. 53 . 53 . 54
5	. System Management 5.1 Log In 5.2 Log Out 5.3 Main Menus	. 53 . 53 . 54 . 55
5	 System Management	. 53 . 53 . 54 . 55 . 56
5	 System Management	. 53 . 53 . 54 . 55 . 56 . 59
5	 System Management 5.1 Log In 5.2 Log Out 5.3 Main Menus 5.4 Registering the Webshell Detection Policy 5.5 Webshell Analysis/Countermeasure 5.6 Set event alerts and receive notifications 	. 53 . 53 . 54 . 55 . 56 . 59 . 60
5	 System Management 5.1 Log In 5.2 Log Out 5.3 Main Menus 5.4 Registering the Webshell Detection Policy 5.5 Webshell Analysis/Countermeasure 5.6 Set event alerts and receive notifications 5.7 Rollback 	. 53 . 53 . 54 . 55 . 56 . 59 . 60 . 61
5	 System Management	. 53 . 53 . 54 . 55 . 56 . 59 . 60 . 61
5	 System Management	. 53 . 54 . 55 . 56 . 59 . 60 . 61 . 61 . 62

SK infosec co., ltd.

	5.10 License management	62
	5.11 Patches and updates management	62
6.	Support	63
	6.1 Technical support	63
	6.2 Support Costs	63
	6.3 SLA	63
7.	Deploy the Quick Start	63
	7.1 Step 1. Set up a VPC	63
	7.2 Step 2. Deploying with AWS CloudFormation	64
	7.3 Step 3. Log in to the Anti-Webshell Manager Web Console	67
	7.4 Step 4. Deploy Anti-Webshell Agent to New Instances	68

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(<u>http://www.skinfosec.net/antiwebshell/en/service_request.html</u>)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: <u>http://www.skinfosec.net/antiwebshell/en/support.html</u>

- 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(<u>https://aws.amazon.com/ko/ec2/instance-types/</u>)

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	Count of Agent Instance type		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
 - You can find VPC settings at [EC2 Management Console > Services > Networking & Content Delivery > VPC]

aws	Services	i → Resour	ce Groups 🗸 👌	ŧ				Д [●] h
VPC Dashboard Filter by VPC:	•	Create VPC	Actions v					
Q Select a VPC		Q Filter by ta	gs and attributes or sea	rch by keyword				
Virtual Private		Name	· VPC ID	▲ Sta	te - IPv4	CIDR IP	6 CIDR E	HCP options set
Cloud		Manger	VPC	ava	ilable 172.2	22.0.0/16 -	c	lopt-982a9ff1
Your VPCs				ava	ilable 172.3	- 31.0.0/16	c	lopt-982a9ff1
Subnets								
Route Tables								
Internet Gateways								
Egress Only Internet Gateways								
DHCP Options Sets								
Elastic IPs								
Endpoints								
Endpoint Services		4						

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

aws s	ervices	 Resource Gro 	ups 🗸 🛠					ب ب
VPC Dashboard Filter by VPC:		Create subnet	actions V					
Q Select a VPC		Q Filter by tags and a	ttributes or search by keyword					
Virtual Private		Name -	Subnet ID	•	State -	VPC	IPv4 CIDR	Available IPv4.~
Cloud		Anti-Websh	subnet-67d75d0e		available	vpc-4d7bf924 Manger_V	172.22.0.0/20	4088
Your VPCs			subnet-7ff32404		available	vpc-c150fea8	172.31.32.0/20	4091
Subnets			subnet-a423c8e9		available	vpc-c150fea8	172.31.16.0/20	4086
Route Tables			subnet-c9f45fa0		available	vpc-c150fea8	172.31.0.0/20	4090
Internet Gateways								
Egress Only Internet Gateways								
DHCP Options Sets								

- 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_VP https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/UserGuide/USER_VP https://docs.aws.amazon.com/ko_kr/AmazonRDS/latest/UserGuide/USER_VP				

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	ТСР	443	Allow	Allows inbound HTTPS traffic from customer admin corporate IP
110	Public IPv4 address range of your customer admin corporate IP	ТСР	22	Allow	Allows inbound SSH traffic from customer admin corporate IP
130	Private IPv4 address range of customer web/was service network	ТСР	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	ТСР	32768-65535	Allow	Allows inbound RDS traffic from DB network
*	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	ТСР	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	ТСР	5432	Allow	Allows outbound responses to Anti-Webshell Manager RDS network.
*	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 <u>https://console.aws.amazon.com/vpc/</u>.
 - 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	ТСР	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	ТСР	12251-12259	Allow	Allows outbound responses to Manager on Anti- WebShell Manager network

*	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	ТСР	5432	Allow	Allows inbound Anti-Webshell Manager traffic from your Anti- Webshell Manager network
*	0.0.0/0	all	all	DENY	-

- Outbound rule

|--|

100	Private IPv4 address range of Anti-Webshell Manager IP	ТСР	32768-65535	Allow	Allows outbound responses to Anti- Webshell Manager network
*	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.
 - 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
Туре	Custom TCP Rule
Protocol	ТСР
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		
Туре	HTTPS		
Protocol	ТСР		
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	
Туре	SSH	
Protocol	ТСР	
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-	Description	

SK infosec co., ltd.

Agent SG		
	Agent SG	Agent SG

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

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

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
Туре	Custom TCP Rule
Protocol	ТСР
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	Description	

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.

🎁 AWS 🗸	Services 👻 Edit 👻	oport 🕶
INSTANCES Instances Spot Doguests	Create Security Group Actions V	• ?
Reserved Instances	Q Filter by tags and attributes or search by keyword	>
Dedicated Hosts	Name ✓ Group ID ▲ Group Name ✓ VPC ID ✓ Description	-
 IMAGES AMIs Bundle Tasks ELASTIC BLOCK STORI Volumes Snapshots 		
NETWORK & SECURITY Security Groups Elastic IPs Placement Groups Key Pairs	-	
🗨 Feedback 🔇 I	English © 2008 - 2016, Ama:es, Inc. or its affiliates. Albd. Privacy Policy Terms	ofUse

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
Туре	PostgreSQL
Protocol	ТСР
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		Tagging to identify assets
Value	Anti-Webshell Manager DB SG	Description	

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

aws	Services 🗸 Resource Groups 🗸	*		众 hyung0925@sk.com @ wshield ▼ Seou
	AWS Managem	ent Console		
	AWS services			Access resources on the go
	Find Services You can enter names, keywords or acronyms. Q Example: Relational Database Service,	database, RDS		Access the Management Console using the AWS Console Mobile App.
	Recently visited services			Explore AWS
	AWS Marketplace Subscriptions	CloudFormation	676 VFC	AWS Security Hub Centrally view and manage security alerts and
	All services			automate compliance checks. Learn more 🗹
	Compute EC2 Lightsail	Satellite Ground Station	Security, Identity, & Compliance IAM	Amazon RDS Set up, operate, and scale your relational
	ECR	Management & Governance	Resource Access Manager Cognito	database in the cloud. Learn more 🗹

- 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).

aws Services - Resou	ırce Groups 🐱 🔸		↓ hyung0925@sk.co	m @ wshield 👻 Seoul 👻
Amazon RDS ×	RDS > Snapshots			
Dashboard	Snapshots (1)	C	Owned by Me 🔻	Actions v Take s
Databases	Q Filter snapshots			Restore Snapshot 1
Performance Insights				Copy Snapshot
Snapshots	Snapshot	▼ DB instance or cluster ▼ S	napshot Creation Time	Share Snapshot
Automated backups				Migrate snapshot
Reserved instances	antiwebshellv2-manager-db-050919	antiwebshell-test-db II	hu Sep 05 14:35:08 GMT+900 2	Delete Snapshot
Subnet groups Parameter groups Option groups Events Event subscriptions				

Menu	Input Value				
	DB Engine: PostgreSQL (Default)				
	License model: postgresql-license (Default)				
Instance	• DB Instance Class: For instance type, see [2.3 Sizing].				
specifications	 Multi-AZ Deployment: Choose Single AZ deployment or Multi-AZ Deployment 				
	• Storage type: For Storage type, see [2.3 Sizing].				
	 Virtual Private Cloud (VPC): Choose the same existing VPC as your customer web tier 				
Network & Security	 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.

AWS Cloud	
VPC Public subnet Anti-Webshell Manager	Public subnet
Availability Zone 1	Availability Zone 2

1. Login to AWS management console and Click EC2.

aws	Services V Resource Groups V	*		û hyung0925@sk.com @ wshield ▼ Seoul ▼
	AWS Managem	ient Console		
	AWS services			Access resources on the go
	Find Services You can enter names, keywords or acronyms. Q Example: Relational Database Service	e, database, RDS		Access the Management Console using the AWS Console Mobile App. Learn more
	▼ Recently visited services B RDS	© EC2	🔲 ECS	Explore AWS
	Billing	WAF & Shield		Set up, operate, and scale your relational database in the cloud. Learn more 🔀
	All services Compute EC2 Lightsail [2] ECR ECS	 Satellite Ground Station Management & Governance AWS Ornanizations 	Security, Identity, & Compliance IAM Resource Access Manager Cognito	Amazon SageMaker Machine learning for every developer and data scientist. Learn more

2. Click Launch Instance



3. Create an instance with a shared AMI.

✓ Use the shared AMI that is provided by the vendor

aws Services -	Resource Grou	ps 🗸 🛧			۵	hyung0925@sk.com @ wshield 👻	Seoul 👻	Support 👻
1. Choose AMI 2. Choose Instanc	e Type 3. Configure I	nstance 4. Add Storage 5	Add Tags 6. Configure Sect	urity Group 7. Review				
Step 1: Choose an A An AMI is a template that contains t Marketplace; or you can select one	mazon Mach ne software configurat of your own AMIs.	ine Image (AMI) ion (operating system, applica	tion server, and applications) r	equired to launch your instan	ce. You can select ar	n AMI provided by AWS, our user com	Canc munity, or the	el and Exit
Q, Search for an AMI by entering	a search term e.g. "Wi	ndows"						×
Quick Start						I< <	1 to 10 of 10	AMIs > >
My AMIs	∆ An	tiwebshell_test4_190827 -	ami-025cfc942794945a8				Se	elect
AWS Marketplace	Roc	t device type: ebs Virtualization ty	be: hvm Owner: 938685826125	ENA Enabled: Yes			64-bl	it (x86)
Community AMIs	A An	tiwebshellv2.0_manager_(050919 - ami-0261b89993eb	403e1			Se	ect
▼ Ownership	Ant	webshellv2.0_manager_050919	e hvm Owner 938685826125	ENA Enabled: Yes			64-bi	it (x86)

- 4. Choose an Instance Type
 - ✓ For instance type, see [2.3 Sizing].
- 5. Next: Configure Instance Details

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

	vpcs.html	
	Auto-Assign Public IP: Use subnet setting (Enable)	
	 IAM Role: Select None or see [4.3 Solution Logging Procedu Bucket]. 	re with S3
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	Description	

- 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.

aws AWS Cloud	1	,,	
	C VPC	Public subnet	
		Anti-Webshell Manager	
		Availability Zone 1	

1. Login to AWS management console and Click EC2.

aws	Services ~ Resource Groups ~	\$		↓ hyung0925@sk.com @ wshield × Seoul ×
	AWS Managem	ient Console		
	AWS services			Access resources on the go
	Find Services You can enter names, keywords or acronyms. Q Example: Relational Database Service	e, database, RDS		Access the Management Console using the AWS Console Mobile App. Learn more 诸
	 Recently visited services RDS 	() EC2	I ECS	Explore AWS
	Billing	WAF & Shield		Amazon RDS Set up, operate, and scale your relational
	▼ All services			database in the cloud. Learn more [2]
	Compute EC2 Lightsail ECR ECR ECS	Satellite Ground Station Management & Governance AWS Ornanizations	 Security, Identity, & Compliance IAM Resource Access Manager Cognito 	Amazon SageMaker Machine learning for every developer and data scientist. Learn more 🔀

2. Click Launch Instance



3. Create an instance with a shared AMI.

✓ Use the shared AMI that is provided by the vendor

aws Services -	Resource Grou	ps 🗸 🛧			۵	hyung0925@sk.com @ wshield 👻	Seoul 👻	Support 👻
1. Choose AMI 2. Choose Instanc	e Type 3. Configure I	nstance 4. Add Storage 5	Add Tags 6. Configure Sect	urity Group 7. Review				
Step 1: Choose an A An AMI is a template that contains t Marketplace; or you can select one	mazon Mach ne software configurat of your own AMIs.	ine Image (AMI) ion (operating system, applica	tion server, and applications) r	equired to launch your instan	ce. You can select ar	n AMI provided by AWS, our user com	Canc munity, or the	el and Exit
Q, Search for an AMI by entering	a search term e.g. "Wi	ndows"						×
Quick Start						I< <	1 to 10 of 10	AMIs > >
My AMIs	∆ An	tiwebshell_test4_190827 -	ami-025cfc942794945a8				Se	elect
AWS Marketplace	Roc	t device type: ebs Virtualization ty	be: hvm Owner: 938685826125	ENA Enabled: Yes			64-bl	it (x86)
Community AMIs	A An	tiwebshellv2.0_manager_(050919 - ami-0261b89993eb	403e1			Se	ect
▼ Ownership	Ant	webshellv2.0_manager_050919	e: hvm Owner: 938685826125	ENA Enabled: Yes			64-bi	it (x86)

- 4. Choose an Instance Type
 - ✓ For instance type, see [2.3 Sizing].
- 5. Next: Configure Instance Details

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

		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	Description	

- 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.

system administration			
Group manage···· Analytics server man···· User managem···	Grade / Access Mana… External system	linka… System settings Audit / System Log Backup manage…	
	License Management		
	Usage / holding status	361 / 1000 is.	
	License Key is	is.	
		✓ apply	
	System management		
	Currently installed version	2.0.023 is.	
	Session timeout period	600 Minutes.	
	Failure threshold time is	5 Minutes.	
	Backup base date is	10 Is work.	
	The removal date is	15 Is work.	
		✓ apply	

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. $(1 \sim 2)$
- 2. Decompress the agent compression file in the /wagent directory. $(3 \sim 4)$
- 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. ([®])
- ✓ 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/
- (a) [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



- 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.

🔍 Anti Webshell Setup	
	Welcome to the Anti Webshell Setup Wizard
	This wizard will guide you through the installation of Anti Webshell.
	It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
为	Click Install to start the installation.
	[Instal] Cancel

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

🍳 Anti Webshell Setup	
	Completing the Anti Webshell Setup Wizard
	Anti Webshell has been installed on your computer.
	Click Finish to close this wizard.
	< Back Enish Cancel

 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.

Services						_	
<u>File Action View</u>	Help						
	à 🛃 🚺 📷 🕨 🔳 🕕 🕨						
🤹 Services (Local)	🖏 Services (Local)						
	Anti Webshell Service	Name 🔺	Description	Status	Startup Type	Log On As	
		💁 Anti Webshell Service		Started	Automatic	Local System	
	Stop the service	APM_APACHE2	Apache/2	Started	Automatic	Local System	
	Restart the service	APM_MYSQL5		Started	Automatic	Local System	
		🎑 Application Experie	Processes	Started	Manual	Local System	

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.

🖏 Services						_	
Eile Action View	Help						
	à 🗟 🛛 🖬 🕨 🔳 🕕 🕨						
🤹 Services (Local)	🔕 Services (Local)						
	Anti Webshell Service	Name 🔺	Description	Status	Startup Type	LogOn As	
		Anti Webshell Service		Started	Automatic	Local System	
	Stop the service	APM_APACHE2	Apache/2	Started	Automatic	Local System	
	Restart the service	APM_MYSQL5		Started	Automatic	Local System	
		Application Experie	Processes	Started	Manual	Local System	
		🥋 Application Identity	Determines		Manual	Local Service	

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

👰 Windows Task M	Windows Task Manager 📃 🗖										
<u>File Options View</u>	Help										
Applications Proces	ses Service:	s Perf	formance Ne	tworking Users	Ì.						
					_						
Image 🔺	User Name	CPU	Memory (Description							
dwm.exe	Administ	00	976 K	Desktop							
Ec2Config.exe	SYSTEM	00	16,324 K	EC2Config	1						
explorer.exe	Administ	00	9,564 K	Windows							
httpd.exe *32	SYSTEM	00	11,312 K	Apache H							
httpd.exe *32	SYSTEM	00	15,264 K	Apache H							
java.exe	SYSTEM	00	32,048 K	Java(TM)							
LogonUI.exe	SYSTEM	00	5,424 K	Windows							

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.

🔍 Services						_	
Eile <u>A</u> ction <u>V</u> iew	Help						
	à 📑 📔 🖬 🕨 🔳 💵 👘						
🤹 Services (Local)	🖏 Services (Local)						
	Anti Webshell Service	Name 🔺	Description	Status	Startup Type	Log On As	
		Anti Webshell Service		Started	Automatic	Local System	
	Stop the service	APM_APACHE2	Apache/2	Started	Automatic	Local System	
	Restart the service	APM_MYSQL5		Started	Automatic	Local System	
		Application Experie	Processes	Started	Manual	Local System	

2. The service has stopped.

🖏 Services						-	
Eile <u>A</u> ction <u>V</u> iew	Help						
	à 🗟 🛛 🖬 🕨 🔲 🕕 🕒						
🤹 Services (Local)	🔅 Services (Local)	-					
	Anti Webshell Service	Name 🔺	Description	Status	Startup Type	Log On As	▲
		💁 Anti Webshell Service			Automatic	Local System	
	Start the service	APM_APACHE2	Apache/2	Started	Automatic	Local System	
		🧠 APM_MYSQL5		Started	Automatic	Local System	
		Application Experie	Processes	Started	Manual	Local System	

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.

	EC2 Dashboard			Laun	nch Inst	ance	-	Connec	t	Actions A					
	Events														
	Tags	4		Q, I	Filter by	tags an	d attri	butes or sea	arch	h Get Windows Password					
	Reports				Name					Create Template From Inst	tance		nce ID 👻	Instance Type	Availability Zone
	Limits		È					_		Launch More Like This					
			Q		Anti-W	ebshell	on Cl	oud		Instance State			b271d7f3e7f19	m4.large	ap-northeast-2a
-	INSTANCES				antiwe	shellag	gent_a	amazon_tes	t	Instance State		Č.	9946978b05ffc	t2.small	ap-northeast-2c
I	Instances				MDS v	2.0						•	Create Image		-northeast-2a
	Launch Templates				MDS o	n Cloud	1			Networking		•	Bundle Instance	e (instance store AMI)	-northeast-2a
	Spot Requests				antiwe	oshell_t	est_R	DS		CloudWatch Monitoring		Þ	20f4d1337908e	m4.large	ap-northeast-2c
	Reserved Instances				antiwe	oshellag	gent_r	hel8_test			i-04	4e8	3dc2189f0a9f54	t2.small	ap-northeast-2c
	Dedicated Hosts				TEST						i-0	524	1018b616e080	m4.large	ap-northeast-2a

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).

aws	Services 🗸	Resource	e Groups 🖂	*						4	hyung0925	@sk.com @ \	wshield 👻	Seoul 👻	Support 👻
1. Choose AMI	2. Choose Instance T	ype 3. Co	nfigure Instance	4. Add Storage	5. Add Tags	6. Configure Ser	curity Group	7. Review							
Step 1: Cho An AMI is a templat Marketplace; or you	te that contains the a can select one of	software con your own AM	Iachine Im nfiguration (operat IIs.	age (AMI) ting system, appli	cation server, a	and applications)	required to la	aunch your	nstance. You ca	n select an	AMI provided	l by AWS, ou	r user com	Can munity, or th	cel and Exit e AWS
Q, Search for an /	AMI by entering a s	earch term e	.g. "Windows"												>
Quick Start													< ≺	1 to 10 of 10	AMIs >
My AMIs		Δ	Antiwebshe	II_test4_19082	7 - ami-025cfc	942794945a8								s	elect
AWS Marketpl	ace		Root device type:	ebs Virtualization	i type: hvm Ow	mer: 938685826125	ENA Enabled	d: Yes						64-1	oit (x86)
Community AM	Als	Δ	Antiwebshe	llv2.0_manage	r_050919 - an	ni-0261b89993e	b403e1							s	elect
 Ownership Owned by m 	0	Ĩ	Antiwebshellv2 Root device type:	.0_manager_0509 ebs Virtualization	/19 h type: hvm Ow	mer: 938685826125	ENA Enabled	d: Yes						64-1	bit (x86)

- 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.

	EC2 Dashboard	•			Lau	nch Instance	•	Connect	Actions 🔺				
	Events												
	Tags	I	4		Q,	Filter by tags and	attrit	butes or search	Connect Get Windows Password				
	Reports					Name			Create Template From Instance		nce ID 👻	Instance Type	Availability Zone
	Limits			L.	<u> </u>				Launch More Like This				
						Anti-Webshell or	n Clo	bud			b271d7f3e7f19	m4.large	ap-northeast-2a
	INSTANCES			17		antiwebshellage	nt a	mazon test	Instance State		9946978b05ffc	t2 small	an_northeast_2c
1	Instances					antiwobonioliago	inc_u	11102011_1031	Instance Settings		001001000000	12.51101	up-normoust-ze
	motaneco					MDS v2.0			Image		Create Image		-northeast-2a
	Launch Templates					MDS on Cloud			Networking	Þ	Bundle Instance	e (instance store AMI)	-northeast-2a
	Spot Requests					antiwebshell_tes	st_RI	DS	CloudWatch Monitoring	Þ	20f4d1337908e	m4.large	ap-northeast-2c
	Reserved Instances					antiwebshellage	nt_rł	hel8_test	i-04	4e8	8dc2189f0a9f54	t2.small	ap-northeast-2c
	Dedicated Hosts					TEST			i-0:	524	4018b616e080	m4.large	ap-northeast-2a

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

aws Services	s 🗸 Resourc	ce Groups 🗸	*						¢	hyung0925	@sk.com @	wshield 👻	Seoul 👻	Support	*
1. Choose AMI 2. Choose Ins	stance Type 3. C	Configure Instance	4. Add Storage	5. Add Tags	6. Configure Se	ecurity Group	7. Review								
Step 1: Choose an An AMI is a template that conta Marketplace; or you can select	Amazon I ins the software co one of your own A	Machine Imaconfiguration (operation AMIs.	age (AMI ing system, app) lication server, a	and applications	;) required to la	aunch your ins	tance. You can	select an	AMI provided	by AWS, ou	ur user com	Can munity, or th	cel and Ex e AWS	.it
Q, Search for an AMI by enter	ring a search term	n e.g. "Windows"													×
Quick Start												К <	1 to 10 of 10	AMIs >	>
My AMIs	Δ	Antiwebshel	I_test4_19082	7 - ami-025cfc	942794945a8								s	elect	
AWS Marketplace		Root device type:	ebs Virtualizatio	in type: hvm Ow	mer: 938685826125	ENA Enabled	t: Yes						64-t	oit (x86)	
Community AMIs	۵	Antiwebshel	lv2.0_manage	•r_050919 - am	ni-0261b89993e	eb403e1							s	elect	
 Ownership Owned by me 		Antiwebshellv2 Root device type:	.0_manager_050 ebs Virtualizatic	919 in type: hvm Own	mer: 938685826125	ENA Enabled	t: Yes						64-t	bit (x86)	

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).

MJ-Shie Anti-	Mebshell Management Ver, 2.0	· 분석/대용 예이진트 권리 당지패턴 관리	보고서 시스템 관리			월 wdc_admin일, 환영합니다. 프그아웃
시스템 관리 그를 관리	분석 서비 관리 사용자 관리 등급/급급	2관리 외부 시스템 연동 관리 시스템	성경 강사/시스명로그 백업관리			
○ 선탁삭제				전체 함복 경석	Q 검색	분석 세비 정보
No.	#3	0(0)2)	542	물작상태		- 별칭: 별칭을 인력해 주세요.
E 1	분석서비(메인)	172 31.19.34	2019/08/27 02:08:09	정상 동작 중		
E 2	서버2	172.31.19.222	2019/08/29 02:17:25			• 아이터- 아이터프 일찍에 주세죠.
						✓ 47 (0.25)B

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]

nagemen	t Ver, 2.0 Dash Board	Analysis Agent Pattern Report	System				
Agent Mi	anagement						P
New :	cript 💽 start 💽 Pause	🔊 Reset 🗿 Delete 🗸 Auto Quarantine 🗸 Manua	al Quarantine V Real-Time Detection V Periodic Detection			(3) AWS Instance List	Download
relete	AWS Instance ID	AWS Local Hostname	AWS Public Hostname *	AWS VPC ID	AWS Owner ID	AWS Subnet ID	AWS Tags
Use	1°0253504a275a85a13	ip-10-10-0-4.ap-northeast-2.compute.internal	ec2*13*125*214*194.ap*northeast*2.compute.amazonaws.···	vpcr01bta8bdct1a	874505372147	subnet:03b00ec0f3bff36a2	
Use	103568260294720125	ip*10*10*0*97.ap*nortneast*2.compute.internal	ec2"52"/8"96"110.ap*northeast*2.compute.amazonaws.com	vpc*u1bta8bdct1a	8/45053/214/	subnet-03000ecut30tt3ba2	

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.

AWS In	stance List V	liew								
No.	Owner Id	VPC ID	Instance ID	Tags	Public Hostname	Local Hostname	Subnet Id	Install Type 👻	Registration Date	
1	87450…	vpc-01bfa8bdcf1a…	i-035e826b2947…	Anti-Webshell-Agent	ec2-52-78-96-110.a…	ip-10-10-0-97.ap-northeas…	subnet-03b00ec0f…	Installed	2019-12-13 02:50:45	
2	87450…	vpc-01bfa8bdcf1a…	i-0253504a275a…	AntiWebshellManagerI…	ec2-13-125-214-194…	ip-10-10-0-4.ap-northeast	subnet-03b00ec0f…	Installed	2019-12-13 02:50:45	_
З	87450…	vpc-1f70ee77	i-043575ca134a…			ip-172-31-21-178.ap-nort…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
4	87450…	vpc-1f70ee77	i-021d35a5eba2…			ip-172-31-27-60.ap-north…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
5	87450…	vpc-1f70ee77	i-014b13efecb28…			ip-172-31-17-215.ap-nort…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
6	87450…	vpc-1f70ee77	i-02cf24513d9cb…	WebServer_test2-kjg-1…		ip-172-31-24-157.ap-nort…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
7	87450…	vpc-1f70ee77	i-05d8281c0a08…			ip-172-31-18-91.ap-north…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
8	87450…	vpc-1f70ee77	i-04130527dde4…	AWSWAF_webgoat2_t···		ip-172-31-23-60.ap-north…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
9	87450…	vpc-07b74cb8db3…	i-09665943cb10…	Webshell_HC_test_A		ip-10-13-0-52.ap-northeas…	subnet-09ad85a3…	Not Installed	2019-12-13 02:50:45	
10	87450…	vpc-1f70ee77	i-0dddfbf48a3eb…	ubuntu web-test-hj		ip-172-31-17-152.ap-nort…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
11	87450…	vpc-1f70ee77	i-049d73c8cc50…	Anti-Webshell Manage…		ip-172-31-6-227.ap-north…	subnet-95345ffd	Not Installed	2019-12-13 02:50:45	
12	87450…	vpc-1f70ee77	i-0dcd2163d8c6…		ec2-13-125-63-43.a…	ip-172-31-20-149.ap-nort…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
13	87450…	vpc-1f70ee77	i-014b53602a0b…			ip-172-31-27-30.ap-north…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
14	87450…	vpc-1f70ee77	i-045ba5f6b587…	test_hj		ip-172-31-20-198.ap-nort…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
15	87450…	vpc-1f70ee77	i-016cff34575a4…	agent_test_hj_190920		ip-172-31-25-152.ap-nort…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
16	87450…	vpc-1f70ee77	i-057a5ea84536…	Ethelis and the familie		ip-172-31-26-226.ap-nort…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
17	87450…	vpc-07b74cb8db3…	i-0a68a8a1fbb6a…	Webshell_HC_test_19…		ip-10-13-0-181.ap-northe	subnet-09ad85a3…	Not Installed	2019-12-13 02:50:45	
18	87450…	vpc-1f70ee77	i-0c1d5b9e2300…			ip-172-31-22-47.ap-north…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	
19	87450…	vpc-1f70ee77	i-0a966e89c7da…	DSA_windows_test-kj		ip-172-31-25-180.ap-nort…	subnet-e6cf16aa	Not Installed	2019-12-13 02:50:45	

Agent and Manager logging includes AWS metadata for easy management.

2019-12-13 02:32:52	[main] [INFO] > ##################################
[2019-12-13 02:32:52]	[main] [INFO] > W-Shield v2 Agent Start (cloud)!
[2019-12-13 02:32:52]	[main] [INF0] > ##################################
[2019-12-13 02:32:52]	[main] [INF0] > VERSION = 2.0.023A
[2019-12-13 02:32:52]	[main] [INF0] > ## OS TYPE = 2
[2019-12-13 02:32:52]	[main] [INFO] > ## Java Type = true
[2019-12-13 02:32:52]	[main] [INFO] > ## pwd = /wagent
[2019-12-13 02:32:52]	[main] [INF0] > ## [opt] java path = java
2019-12-13 02:32:52	[main] [INF0] > ## [opt] server ip =
2019-12-13 02:32:52	[main] [INFO] > ## [opt] log path =
2019-12-13 02:32:52	[main] [INFO] > ## [opt] ssl type = 0
2019-12-13 02:32:52	[main] [INF0] > [## lopt] log level = 0
2019-12-13 02:32:52	[main] [INF0] > init complete
2019-12-13 02:32:52	[main] [INFO] > resouce pass
2019-12-13 02:32:52]	[main] [INFO] > install start
2019-12-13 02:32:52]	[main] $[INFO] > INSTALL PROCESS :: run into = 10.10.0.4$
2019-12-13 02:32:52]	[main] [INFO] > INSTALL :: CONN START
2019-12-13 02:32:52]	[pool-2-thread-1] [INFO] > CONN :: SIARI
2019-12-13 02:32:52]	[pool-2-thread-1] [INF0] > CONN :: RANOK 1/3
2019-12-13 02:32:52]	[pool-2-thread-1] [INFO] > CONNECTION :: 1p = 10.10.0.4, port = 12259
2019-12-13 02:32:52]	[nioEventLoopGroup-2-1] [INFO] > ILS VI.2 Connetion protocol
2019-12-13 02:32:52]	[pool-2-thread-1] [INFO] > UPLOAD PROCESS ::: CANNOL FIND UDDREY
2019-12-13 02:32:52]	[pool-2-thread-1] [INFO] > UPLOAD PROCESS ::: SIEP 18273
2019-12-13 02:32:52]	[pool-2-thread-1] [INFO] > UPLOAD PROCESS ::: SIEP 2
2019-12-13 02:32:53]	[main] [INFO] > INSTALL :: CONN COMPLETE
2019-12-13 02:32:53]	[pool-2-thread-1] [INFO] > UPLOAD PROCESS ::: SIEP 182/3
	[DOOL-2-THFEAD-1] [INFO] > UPLOAD PROCESS ::: SIEP 2
	[main] [NFO] > aws into [instance-10] = 1-02330442/3683813
	[main] [INFO] > aws info [public-nostname] = ec2-13-125-214-194.ap-northeast-2.compute.amazonaws.com
	[main] [INFO] > aws info [(coat-nostname] = 19-10-10-0-4.ap-northeast-2.compute.internat
	[main] [NFO] \rightarrow aws into [vpc-10] = vpc-0101a300c11a/44e0
	[main] [NFO] > aws into [owner-id] = $5/43033/2147$
[2019-12-13 02:32:53]	[main] [invo] > aws into [subnet-id] = subnet-050000c013b1130a2

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



- 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
 - Access the AWS EC2 Management
 - 2) Select Instance > Instance and Check Anti-Webshell console

aws	service 🗸 Resource grou 🛠
EC2 Dashboard	▲ Launch instance ▼ connect work ▼
Тад	◀ Q search : anti ⊗ 필터 추가
Report	Name ·
Limits	Anti-Webshell_console
Instance	
Reserve	
Instance	
Launch lemplate	

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]



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

Create p	olicy				One 2
Policy revie	w				
	name*	Anti-Webshell_S3_logging Use alphanumeric and '+ =,. @' chi	aracters. Maximum 128 characters.		
Ex	planation				
		1000 characters maximum. Use alpha	numeric and '+ =,. @' characters.		
	summary	Q 필터:			
		service 👻	Access level	resource	Request condition
		Allowed (1/201 service) 200	remaining marks		
		83	Limits : list, read, write	BucketName string like All	none
- necessary					cancel Previous Policy review

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

Create role			One	2 3 4
 Permission Policy Association 				
Please select at least one policy to attach to the new role.				
Create policy				C
Policy filter v Q anti			•	Showing 1 Results
Policy name 👻	purpose of use	Explar	ation	
Anti-Webshell_S3_logging	none			
* necessary		cancel	Previous	Next: Permissions

- 5) Skip Add tag (optional)
- 6) "Anti-Webshell_S3_logging" is entered in the [Role name] field > Click [Create role] button

Review		
Before you create, enter the required information be	elow and review this role.	
Role name*	Anti-Webshell_S3_logging	
	Use alphanumeric and '+ =,. @' characters. Maximum 64 characters.	
Role description	Allows EC2 instances to call AWS services on your behalf.	
	1000 characters maximum. Use alphanumeric and '+ =,. @' characters.	
Trusted object	AWS service: ec2.amazonaws.com	
Policy	Anti-Webshell_S3_logging C	
Permission boundary	Permission boundaries not set	
The tag was not added.		
* necessary	cancel Previous	Create ro

- 4. Apply IAM role
 - 1) Access the AWS EC2 Management
 - 2) Select Instance > Instance and Check Anti-Webshell console

aws	service 🗸 Resource grou 🛧	
EC2 Dashboard	▲ Launch instance ▼ connect work ♥	
Тад	◀ Q search : anti ⊗ 필터 추가	
Report	Name ·	-
Limits	Anti-Webshell_console	
- Reserve		
Instance		
Launch Template		

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

	Launch instance 🔻 connect	work 🔦		
•	Q search : anti 💿 필터 추가	connect Get Windows Password		
	Name	Create Template From Instance Launch based on an existing instance	е	Instance type Availability Zone
	Anti-Webshell_console	Instance status	Þ	t2.medium ap-northeast-2a
		Instance settings	►	Add / Edit Tag
		image	►	Connect to an Auto Scaling Group
		Networking	►	Link / Replace IAM Roles
		CloudWatch Monitoring	►	Change instance type
			_	Shutdown Protection Changes
				View / change user data
				Change exit method
				Change T2 / T3 Unlimited
				Get system log
				Take instance screenshot
				Modify instance placement
				Modify capacity reservation settings
				Modify capacity reservation settings

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

Instance > Link / Replace	nstance > Link / Replace IAM Role							
Link / Replace	Link / Replace IAM Roles							
Choose an IAM role to associate with your instance. If you do not have an IAM role, choose Create New IAM Role to create a role in the IAM console. If an IAM role is already attached to your instance, the selected IAM role replaces the existing role. Instance ID I-0192107cae652f4ce (Anti-Webshell_console)								
	IAM role Anti-Webshell_S3_logging Create a New IAM Role							
* Required		cancel						

- 5. Modify & Run Sync Script
 - 1) Access Anti-Webshell Manager via SSH.
 - 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.



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.

4	Q Filter by tag	s and attributes or s	earch by keyword							0	к <	▲ •• 1 to 9 of 9	• >>
	Name				 Instance ID 	v	Instance Type 👻	Availability Zone 👻	Instance State 🔺	Status Checks 👻	Alarm	Status	Publi
	Anti-Web	shell on Cloud			i-0616b271d7f3	97f19	m4.large	ap-northeast-2a	running	2/2 checks	None	>	
	antiwebsh	ellagent_amazon_te	est		i-006a9946978b	05ffc	t2.small	ap-northeast-2c	stopped		None		Þ
	Instance: i-0	616b271d7f3e7f19	(Anti-Webshell	on Cloud)	Elastic IP: 52.78.7	8.217						_	
	Description	Status Checks	Monitoring	Tags	Usage Instructions								
	CloudW	atch alarms: 🥑 N	lo alarms config	ured								Create Ala	rm
	CloudWatcl	n metrics: Basic n	nonitoring. Enable	e Detailed N	Nonitoring				s	howing data for:	Last Ho	ur 🔻	÷

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

ltem	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	

Create Alarm				×				
You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define. To edit an alarm, first choose whom to notify and then define when the notification should be sent. Send a notification to: Manually enter a topic name With these recipients: awsAccount@domain.com Take the action: Recover this instance Status Check Failed (Instance) Count One of the instance Count Co								
Whenever Is For at least Name of alarm	Status Check Failed (Instance) Status Check Failed (Instance	es v Check-F	22:00 00:00 02:00	Ť				
Cancel Create Alarm								

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. <u>https://docs.aws.amazon.com/AmazonECS/latest/developerguide/using_data_volumes.html</u>

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)		
root 992	1 0 2014 7 01:26:36 java -Xms1024m -Xmx3072m -XX:Ne	wSize=256m -XX:MaxNewSize=768m -XX:Survivo
rRatio=4 -jar /	/server/wserver-rd-script	
2001 3648	1 0 10:00 ? 00:00:02 java -Xms128m -Xmx256m -Djava.	library.path=/wserver/lib -jar /wserver/wse
rver-sm main		
root 16304	1 0 10:18 7 00:00:00 /wserver/wserver-md	
root 16308	1 0 10118 7 00100100 /wserver/wserver-sys	
root 16335	(6304 0 10118 2 00100100 /wserver/wserver-ad 0 main	
root 16361	4304 0 10:18 ? 00:00:00 /wserver/wserver-ad 2 main	
root 16374	16304 0 10:18 ? 00:00:00 /wserver/wserver-ad 3 main	
root 16387	16304 0 10:18 7 00:00:00 /wserver/wserver-ad 4 main	
root 16401	6304 0 10:18 7 00:00:00 /wserver/wserver-ad 5 main	
root 16414 :	16304 0 10:18 ? 00:00:00 /wserver/wserver-ad 6 main	
root 16427	16304 0 10:18 7 00:00:00 /wserver/wserver-ad 7 main	
root 16442	16304 0 10:18 ? 00:00:00 /wserver/wserver-ad 8 main	
root 16457	16304 1 10:18 7 00:00:00 /wserver/wserver-rd 1 12321 1	
root 16567	16304 1 10:19 7 00:00:00 /wserver/wserver-rd 2 12321 1	
root 16761	16304 1 10:19 7 00:00:00 /wserver/wserver-rd 3 12321 1	
17001 17001	10304 2 10119 7 00100100 /wserver/wserver-in 4 12321 1	
17379 1	6304 0 10119 7 00100100 /wserver/wserver-tue	
root 17380	16304 0 10:19 7 00:00:00 /wserver/wserver-1sc	
abnormal		
abrioffialez	<i>\</i> /	
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							
<pre>normal ex) root 15599 0.1 24.6 2465996 951000 ? 51 2014 70:55 /usr/java/jrel.7.0_67/bin/java -Djava.util.logging.confi g.file=/usr/comcat7/conf/logging.properties -Dfile.encoding=UTF= -Dsun.jnu.encoding=UTF= -Dsun.io.unicode.encoding=UTe odeLittle -Djava.net.preferIPv45tacktrue -Djava.library.path=/usr/tomcat7/lib/sigar -Djava.net.preferIPv45tacktrue -Dus er.language=ko -Duser.region=KR -Xmsl024m -Xmxl024m -XX:NewSize=S12m -XX:MaxNewSize=S12m -XX:PermSize=S12m -XX:MaxPermSiz =S12m -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djava.endorsed.dirs=/usr/tomcat7/endorsed -clas path /usr/tomcat7/bin/bootstrap.jar/usr/tomcat7/tin/sigar.opiava.endorsed.dirs=/usr/tomcat7/endorsed -clas path /usr/tomcat7/bin/bootstrap.gar/usr/tomcat7/tomca</pre>								
abnormal ex	abnormal ex1)							
- Process not detected								
abnormal ex	abnormal ex)							

.file	=/usr/to	mcat	7/con	f/logging	.prope	rties -	Dfile	.encoding	The/mar	-Deun.	jnu.en	coding=	Diava D	sun.io	unicod	e.encodin	g=Onic
-lan	auanewir/	- Dez		ealoneX2	-Ymaid	24m - Xm	*1024	m -XX:Net	Streest	28 - XX	Mawle	USI PARS	12m -XX+	DermSt	ze=512m	-XX : MayB	ernSiz
51.2-	-Diava		1000	ing manad	ATRANA	anache	5016	Classio	dertoot	lananar	-Diau	a endor	and dire	Juner	LOBOAT 7	lendorsed	
	Inenteres		Part of the			line / war		him /wama	E-Sulls	daw _P		as base	-/uneles		Descal.	ine homen	lunele
acn .	/ 482/ 608	scat r	Din/1	DODUBULAS	- jar :/	usr/cos	Catil	Din/come	ac-juii.	Jar	Catall	na.pase	-/ 481/00	scac/	-Deares	1154 - ISCEDE-	/usr/t
scat7	-Djava.	10.0	spdir	=/usr/com	idat7/t	emp org	.apac	he.catal:	ina.star	cup.Bo	otstra	p start					
300	18230	0.	0 0.	0 106060	648	pts/2		10:22	0:00 /	bin/sh	/usr/	tomcat7	/bin/cat	alina.	sh star		
30	18233	. 0.	0 0.	0 3980	400	pts/2		10:22	0:00 /	usr/lo	cal/cr	000100/	sbin/cro	nolog	usr/to	mcat7/log	s/\$Y-\$
Nd.c	atalina.	out															
ot	18232	86.	12.	3 2331160	49165	2 pts/2	31	10:22	0:12 /	usr/ja	va/ire	1.7.0 6	7/bin/3a	va -D1	itu.ava	1.logging	.confi
P120	-/11/+/	MOAT.	1/000	f/logaing	- PROPA	TTINE -	DFile	encoding	HTTP-R	-Deurs	500.00	codings	TTP-A -D	-	untood	e encodin	and the inc
	-1044			- FANTENAS		-04		i have were sto	-halling	Inamas	# 7 / 3 4 ks	Intant	Diama a		Far T Deck	Cracker and	
Ser 10	ere -ple		ee-br	ererisva:	CACK-L	rue -b)	ava	LDIALY . p	CO-/USE	7 conce	517110	/ sigar	-Djava.m	se pre	LETTRAN.	SCACK-CIU	6 -003
r.lan	guage-xc	s -Du	ser.r	egion=XR	-X8.910	248 -308	x1024	m -XX:Net	/31ze=51	2E -XX	inMaxNe	w51ze=5	12m -XXI	Perm31	ze=512m	-XX:MaxP	erm31z
=512m	-Djava.	ucil.	.logg	ing.manag	er=ord	.apache	.juli	.ClassLo	aderLogM	lanager	-Djav	a.endor	sed.dirs	=/usr/	comcat7	/endorsed	-clas
path	/usr/tos	scat7	/bin/l	DOOTSTING	.sart/	usr/ton	cat7/	bin/tomo	st-juli.	jar -D	Catali	na.base	=/usr/ton	scat7	-Doatal	ina.home-	/usr/t

C. httpd process check

Order	Description	Command						
1	Manager ssh login(ROOT)	N/A						
2	httpd process check	ps -ef grep httpd						
normal ex)	normal ex)							
- A number of processes are searched. abnormal ex)								
- Pro	- Process not detected							

D. Manager UI Access test

Order	Description	Command
1	Manager UI Access test	Access https: //Manager IP
normal ex)		
	Monshield Anti-Webshell Managemen A Password	rt Ver, 2,0
abnormal ex	()	
Service T	emporarily Unavailable	
The server is tempor	arily unable to service your request due to maintenance downtime or capacity proble	ms. Please try again later.

E. Manager resource check

Order	Description	Command		
1	Manager ssh login(ROOT)	N/A		
2	Manager resource check	df		
[root@localf Filesystem /dev/mapper/ /dev/xvda1	nost ~]# df 1K-blocks Used Available Use% Mounter /VolGroup00-LogVol00 27678892 4189988 22060220 16% / 101086 36768 59099 39% /boot	i on		
tmpfs	524288 0 524288 0% /dev/sl	nm		

- 2) Agent Health check
 - A. Agent Process check

Order		Descr	iption		Command			
1	Manager login(WEB UI) Access https: //Manager IP					r IP		
2	"Failure" o Managem agent fails	output in [Ma ent]> [Opera s	nagement ating status	ement UI]> [Agent status] when an N/A				
ex)								
ine Settings ✔ M	Ianual Quarantine	Settings ✔ Real ti	me search setting	🛛 🗸 Periodic Searc	h Settings 🛃			
Management depa	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
a 14			

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	Anti-Webshell	12251.12250	Manager, Agent
(Agent install)	Manager	12251~12259	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.

Anti-Webshell	Management Ver, 2,0
2 10	
Password	
	Login

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).

Change Password First Login
You are logged for the first time, Please change your password, If you do not change automatically logged out.
Old Password * :
New Password * :
Password (Confirm) * :
Name * :
Email * :
Access IP(principal):
Access IP(deputy) :
Change 🤤 Change later

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.

W-shield Anti-Webshell Management Ver	r. 2.0 Dashboard Analysis Agent Report)	Information
DashBoard - 7 / 6 / 2016 PM 8:9:41		◯ Today	/ 🔘 Last 24 Hours 🔹 Last 7 days 💿 Last 30 days
Q Webshell Detection Status	Q Installation Status	Q Agent Status	Q Analyze Pattern Status
· Total Detection: ①(Non-analyze Detection: ①) · True Negative: 0 (Response: ①, Non-response: ①) · Exception: ①, False Positive: ①	 Installation Status: 2 Server: 1 (Analyze: 1, Management: 1) Agent: 1 	 Agent: Total <u>1</u> Non-operation: 0 (Stop: <u>0</u>, Error: <u>0</u>, Delete : 0) Operation: 1 (Detection complete: <u>1</u>, Running 	· Active Pattern: Total 225 · Global Pattern: 225 · Custom Pattern: 0
Group/Agent Status & Resource Status / Domain TOP5			
Group/Agent Status Display Set: Group/Agent All Agent	2	③ Display the Top-level	Webshell Detection Domain TOPS Ranking Domain Detection Sound No Searching Data.
Unclas			Management Resource Status[%]
Real-Time Webshell Detection Status		Real-Time Agent Error Detection	
Final Detection Date Group Installation Type	e Agent IP Level True Negat No Searching Data.	Group Agent	IP Domain Hostname S No Searching Data.
			>
I I Page 0 of 0 ▶ ▶ 😂 Per Page 50 🛩		No data to display 🛛 🖣 🖣 Page 💿 🛛 of 0 🗼 🖗	No data to display

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

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.
Webshell Detection Domain TOP 5	It shows top 5 domains with the most webshells detected up to date.
Management Resource Status	The management server's resource usage (CPU, MEMORY, DISK) will be displayed on a real-time basis.
Real-time Webshell Detection Status	The webshell detection status will be displayed on a real-time basis.
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.

W-shield Anti-Webshell Ma	nagei	ment	t Ver, 2.0	Dashb	oard Ar	M- nalysis	Agent	Report					a bcdef, V	Welcon
Group/Agent «	Age	nt Ma	inagement											Searc
😨 Open 😰 Close 💿 Refresh	10 1	Start	Pause	Reset	O Delet	e 🗸 /	Auto Quarantine	🖌 Manual Quara	ntine 🛛 🖌 Rei	al-Time Detection	🗸 Peri	odic Detection	👲 Downio	Inpu
Name	PI	No.	Gro	up	Agent		nstallation Type	P.≜	Domain	Management	Group	Analyze Cycle	Exter	Sta
 All ▶ [™] Unclassified 	0	1	Unclas	sified	[3] JS-PC		A-WINDOWS	192,168,148,1				Realtime	JSP ASP 4	Er

Configure a webshell analysis policy on the Policy Management window.

Policy Management											
Webshell Detection											
Policy Configuration			Detection	Directory Lis	t						
* Group:	Agent Group	🐼 Select Group	Detectio	Detection Directory List							
* Agent Name:	WIN-5VUJ31DMMNE		Inclu 🗸	Q Search	Directory(Essential)			🗸 Submit		
* (P)	172.31.29.218		No.	Detection	Directory				Delete		
Domain:			1	Include	D:/www.ro	ot			×		
Management Group:											
* Extension:	JSPIASPIASPXIPHPICERICDXIASAIINCIIDCISHTMICC	IIPLIPYIPHIPS1									
Except Extension:	If you register multiple item, Please separated by .										
Detection Limit (MB):	10	~									
CPU Usage Adjust:	10	÷									
Adjust Pattern:	🕼 Global Pattern 🕼 Custom Pattern										
Reanalyze Type: Analyze Periodic: Quarantine Type: Remote Monitoring: Version Information:	After initialization Information-based * Reanalysis settings are applied when you change Real-Time Repetition (60 min.) Sch Auto Quarantine Manual Quarantine Y N N 2.0.020	After changing the pattern. adule									
			~	Directory					Q Search	Reset	
Progress Status	loadu		Manager	Configuration	I(Alarm Cont	iguration)					
Tarrat Director: (Categori	7e Mana	der ID	Mohile	E-mail	Send Mail	Delete		
Target Directory: (Agent	admi	1		admin11@sk.com	OFF	×		
Complete (Directory: Complete File: ()										
			[Save Save	Close						

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. Doubleclick on the detected item displayed on the page to check its details.

Group/Agent	< Even	t Analyz	ze/Malware Response									
🖲 Open 📧 Close 🥥 Refresh	Start	2016	/06/08	0 👻	~ End : 2016/07	/08	23:59:59	A Sear	ch			
ame	Total	Event(7	1) True Negative(0)	False Positive(0)	Response(0)	Rollback(0)						
All	No	-Analyz	ze(71) True Negative(0)	Non-respo	nse(0) False Po	sitive (0) Re	ponse (0) Excepti	on (0) 1	Rollback (0) File Status	(71)		
Unclassified	-										Downle	nar
	are 1	No	Einal Detection Date	Group	Installation Tuna	Apant	10	Level	Dataction Pattern	Caracity	True Nenstina/Ealte Poriti	-
	279.1	1	2016-07-06 20:27:01	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_197	High	-	1
	10-11	2	2016-07-06 20:27:00	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LF2	WebShell_174	Middle	-	
	1007	3	2016-07-06 20:27:00	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_202	High		
	E	4	2016-07-06 20:27:00	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LF1	WebShell_174 and	Middle	-	
	51	5	2016-07-06 20:27:00	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LT1	WebShell_225 and ···	High	.8	
	121	6	2016-07-06 20:26:52	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_202	High	*	
	10	7	2016-07-06 20:26:52	Unclassified	A-WINDOWS	JS-PC	192,168,148,1	LO	WebShell_202	High	10	
	· E1	8	2016-07-06 20:26:52	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_011	High		
	121	9	2016-07-06 20:26:51	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_011	High		
	13	10	2016-07-06 20:26:51	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LT3	WebShell_180 and	High	True Negative	
	13	11	2016-07-06 20:26:50	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_181	Middle	-	
	0	12	2016-07-06 20:26:50	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_197	High	2	
	12	13	2016-07-06 20:26:50	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LF1	WebShell_174 and ···	Middle		
	5	14	2016-07-06 20:26:50	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_202	High	-	
	0	15	2016-07-06 20:26:49	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_202	High	14 14	
	123	16	2016-07-06 20:26:49	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_011	High		
	E	17	2016-07-06 20:26:49	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LT1	WebShell_211 and	High	3	
	12	18	2016-07-06 20:26:47	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_202	High	+	
	0	19	2016-07-06 20:26:47	Unclassified	A-WINDOWS	JS-PC	192.168.148.1	LO	WebShell_202	High	1	

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

Mail management	
The mail server IP is	is.
Mail server port is	is.
Outgoing mail address	is.
Detection Ship Settings 🔲 Web shell detection 📄 Change protection file 📄 Pr	ivacy detection
Webshell Shipment Spy Rename lazaretto delete except	tion 📄 False positive 📄 Clothing
✓ apply	

- 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.

port Management												
Generate Report Report Print Status												
int Report Configuration	Preview											
😥 Generate Report 🔘 Res	iset						1	PDF Down	nload 🔝	Excel Down	load 🛛 🔛 W	lord Do
Select Date									1.			
Specification Period												
 2016-07-01 2016-07-08 		Valadallal			at le the		he e le			1		
Date	Webshell detection system that is there may be a lot of vulnerabilities in the											
© 2016 👻 year	vulnerability of the system or business process. You must minimize risk through a separate vulnerability checks.											
© 07 month												
🔿 08 🖌 date				C. S. Market		and stars to						
Report Item												
Summary of Detection Status	0.48					Λ)					
Major Policy of System	Summar	y of detection	n status			J	/					
🗷 Detection Status at Group		Reporti	ng Period		Events	otal True	Total	Total Non-	Total False	Total	Total	
Detection Status at Web System		NEPOIN	ing renou		-veno 1	Vegative	Response	Response	Positive	Rollback	Exception	
Detail of Detection Status		2016-07-01	~ 2016-07-00	8	71	0	0	0	0	0	0	
Detail of Error List												
g Daily Detection Trend	System S	tatus of majo	or policy									
Report Print Type						Quar	antine					
Print Type: Group		Install	Status			Ty	pe		Analyzed	Period	4.	
	Analyze	d Managed	A	Ecclot	Managers	Auto	Manual	RealTime	Rene	at c	chedule	
								PERSONAL PROPERTY AND INCOME.	I MANTINA	41 1 3	C 1144711184	

Select Date	The period to create a report will be set. You can set the period by year, by month or by date.
2 Report Item	When a report is created, an item to be included will be selected.
8 Report Print Type	When a report is created, an agent to be included will be selected.
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. <u>https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html</u>

B. RDS Key Management

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

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.

License Management		
Usage / holding status		is.
License Key is		is.
	V apply	

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.

۵	▼ Seoul ▲ Support ▼
	US East (N. Verginia): us-east-1 US East (Ohio): us-east-2 US West (N. California): us-west-1 US West (Oregon): us-west-2
tains configuration information about the AWS resources you want to include in the nple template in Designer	Asia Pacfic (Hong Kong) ap-east-1 Asia Pacfic (Mumbai) ap-south-1 Asia Pacfic (Secul) ap-northeast-2 Asia Pacfic (Secul) ap-northeast-1 bit Dorte (Singapore) ap-southeast-1
sporties.	Asia Pacific (Tokyo), ap-northeast-2 Asia Pacific (Tokyo), ap-northeast-1 Canada (Central), ca-central-1
	Europe (Frankfurt) eu-central-1 Europe (Ireland) eu-west-1
 Upload a template file 	Europe (London) eu-west-2 — Europe (Paris) eu-west-3 Europe (Stockholm) eu-north-1
ntiwebshell/en/data/quickstart-skinfosec-antiwebshell-byol-cloudforma	tti Middle East (Bahrain) me-south-1
c.net/antiwebshell/en/data/quickstart-skinfosec-antiwebshell-	– South America (São Paulo) sa-east-1

- ✓ 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.

Rollback on failure	No	Acknowledgment	
		Acknowledginent	
apabilities			
	/		
	The following re	esource(s) require capabilities: [AWS::CloudFormation::Stat	ck]
	This template might	include Identity and Access Management (IAM) resources, which can include o	
			JICCDS.
	IAM users, and IAM	I roles with certain permissions. Ensure that the template you are using is from	a
	IAM users, and IAM trusted source. Lean	roles with certain permissions. Ensure that the template you are using is from a m more.	a a
	IAM users, and IAM busted source. Lean	roles with certain permissions. Ensure that the template you are using is from a m more.	a a
	IAM users, and IAM trusted source. Lear	roles with certain permissions. Ensure that the template you are using is from a more.	a a
	IAM users, and IAM trusted source. Lear Tacknowledge that this ter	roles with certain permissions. Ensure that the template you are using is from a more.	a
	IAM users, and IAM trusted source. Lear Tacknowledge that this ter	I roles with certain permissions. Ensure that the template you are using is from a m.more. mplate might cause AWS CloudFormation to create IAM resources.	a
	IAM users, and IAM trusted source. Lear Tacknowledge that this ter	I roles with certain permissions. Ensure that the template you are using is from a m.more. mplate might cause AWS CloudFormation to create IAM resources.	8

- 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

 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.

Anti-Webshell	Management Ver, 2,0
<u>.</u> 10	
A Password	

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).

Change Password First Login You are logged for the first time, Please change your password, If you do not change automatically logged out.
Old Password * :
New Password * :
Password (Confirm)
Change 🤤 Change later

2. License registration

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

License Management		
Use/Possession Status is	0 / 1	
License Key is		
	Apply	

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]