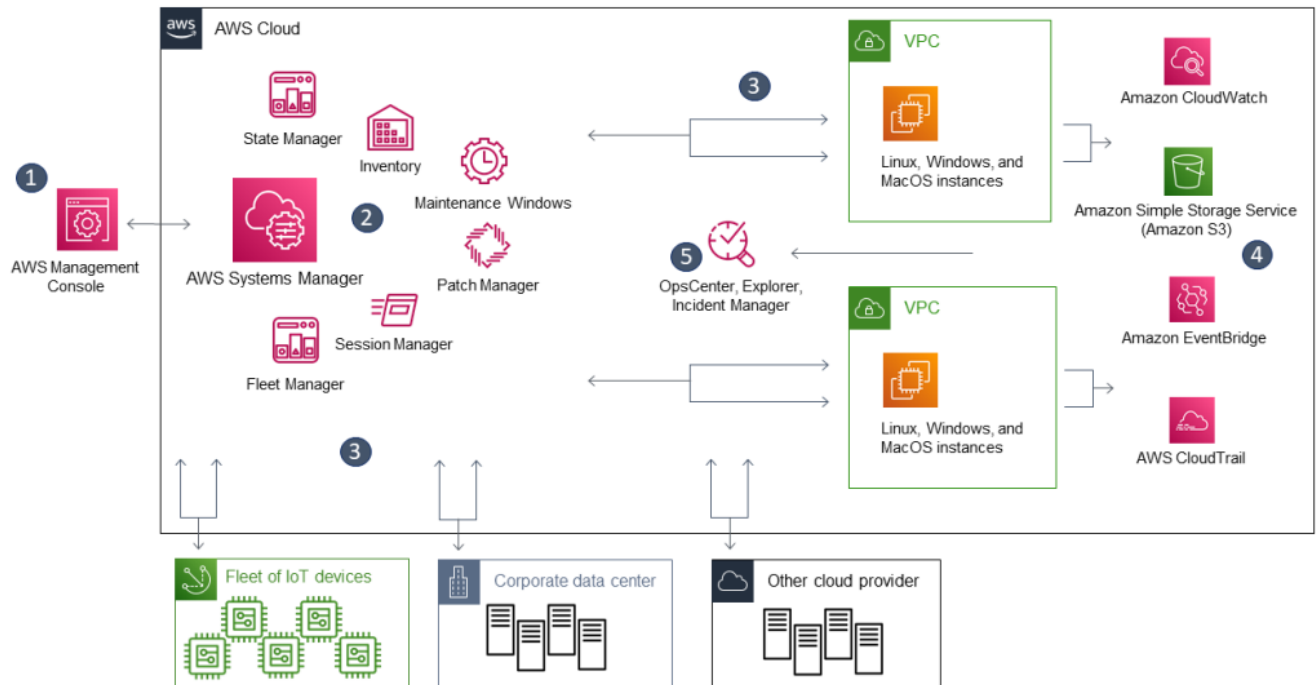


AWS SSM Network

VPC Private



- VPC Private Network Shell (VPN)

- SSM AWS , IGW EIP VPC

- EC2 SSH Password Key-Pair 가 .
 - Shell SSH .
 - AWS Client VPN , .

- AWS CLi AWS (VM / CT / Server)
 AWS Console Cloudshell 가

▪ 1) Private Network IAM

- 2) EC2 IAM Role 가
- 3) EC2 SSM Agent
- 4) AWS CLI EC2

1. Key IAM

Add user

1 2 3

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* SSM-Only

+ Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Select AWS credential type* ☒ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☐ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Add user

1 2 3 4 5

 **Success**
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://hostway-bmt.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶	SSM-Only	AKIAQ25632EPN7T2FFVT	***** Show

— IAM .

arn EC2 ID

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

{
  "Effect": "Allow",
  "Action": [
    "ssm:StartSession"
  ],
  "Resource": [
    "arn:aws:ec2:us-west-2:1234567890:instance/i-
ahe52134fxed6"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "ssm:TerminateSession"
  ],
  "Resource": [
    "arn:aws:ssm:*:*:session/${aws:username} - *"
  ]
}
]
}

```

Create policy

Review policy

Before you create this policy, provide the required information and review this policy.

Name* SSM-EC2-Connection

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Summary

Filter			
Service	Access level	Resource	Request condition
Allow (1 of 321 services) Show remaining 320			
Systems Manager	Limited: Write	Multiple	None

2. IAM Custom Role

VPC

EC2

Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Name, review, and create

Select trusted entity

Trusted entity type

☒ AWS service

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ Web identity

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

☒ EC2

Allows EC2 instances to call AWS services on your behalf.

☐ Lambda

Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Choose a service to view use case

- Role SSM InstanceCore

Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Name, review, and create

Add permissions

Permissions policies (Selected 1/754)

Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter

14 matches

"SSM" X

Clear filters

	Policy name ↗	Type	Description
☐	 AmazonEC2RoleforSSM	AWS m...	This policy will soon be deprecated. Please use AmazonSSManagedInstanceCore policy to enable AWS Systems Manager servic...
☐	 AmazonSSMAutomationApproverAccess	AWS m...	Provides access to view automation executions and send approval decisions to automation waiting for approval
☒	 AmazonSSManagedInstanceCore	AWS m...	The policy for Amazon EC2 Role to enable AWS Systems Manager service core functionality
☐	 AmazonSSMDirectoryServiceAccess	AWS m...	This policy allows SSM Agent to access Directory Service on behalf of the customer for domain-join the managed instance.
☐	 AmazonSSMFullAccess	AWS m...	Provides full access to Amazon SSM.
☐	 AmazonSSMAutomationRole	AWS m...	Provides permissions for EC2 Automation service to execute activities defined within Automation documents
☐	 AmazonSSMReadOnlyAccess	AWS m...	Provides read only access to Amazon SSM.
☐	 AmazonSSMMaintenanceWindowRole	AWS m...	Service Role to be used for EC2 Maintenance Window
☐	 AWSResourceAccessManagerReadOnlyAccess	AWS m...	Provides read only access to AWS Resource Access Manager.

- Role Name

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Description

Add a short explanation for this policy.

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Step 1: Select trusted entities

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "sts:AssumeRole"  
8       ],  
9       "Principal": {  
10        "Service": [  
11          "ec2.amazonaws.com"  
12        ]  
13      }  
14    ]  
15  }
```

EC2

가

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

 i-064f7ebc0bed75c74 (BAEK-Bastion)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

SSM-EC2-Connection-Role ▼



[Create new IAM role](#) 

Cancel

Save

3. EC2 SSM-Agent

Aamazon 2

```
[root@ip-10-10-20-201 ~]# sudo yum install -y  
https://s3.region.amazonaws.com/amazon-ssm-region/latest/linux  
_amd64/amazon-ssm-agent.rpm
```

Loaded plugins: extras_suggestions, langpacks, priorities,
update-motd

```
Cannot open:  
https://s3.region.amazonaws.com/amazon-ssm-region/latest/linux  
_amd64/amazon-ssm-agent.rpm. Skipping.
```

Error: Nothing to do

```
[root@ip-10-10-20-201 ~]# wget  
https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest  
/linux_amd64/amazon-ssm-agent.rpm
```

--2022-03-29 02:49:06--

```
https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest  
/linux_amd64/amazon-ssm-agent.rpm
```

```
Resolving s3.amazonaws.com (s3.amazonaws.com)...  
52.217.196.240
```

```
Connecting to s3.amazonaws.com  
(s3.amazonaws.com)|52.217.196.240|:443... connected.
```

HTTP request sent, awaiting response... 200 OK

Length: 26724168 (25M) [binary/octet-stream]

Saving to: 'amazon-ssm-agent.rpm'

```
100%[=====]  
=====>] 26,724,168  
12.7MB/s in 2.0s
```

2022-03-29 02:49:08 (12.7 MB/s) - 'amazon-ssm-agent.rpm' saved
[26724168/26724168]

```
[root@ip-10-10-20-201 ~]# rpm -Uvh amazon-ssm-agent.rpm
```

warning: amazon-ssm-agent.rpm: Header V4 RSA/SHA1 Signature,
key ID 693eca21: NOKEY

Preparing...

[100%]

Updating / installing...

1:amazon-ssm-agent-3.1.1080.0-1

[100%]

Created symlink from /etc/systemd/system/multi-
user.target.wants/amazon-ssm-agent.service to

```
/etc/systemd/system/amazon-ssm-agent.service.
```

```
[root@ip-10-10-20-201 ~]# systemctl enable amazon-ssm-agent
```

```
[root@ip-10-10-20-201 ~]# systemctl start amazon-ssm-agent
```

```
[root@ip-10-10-20-201 ~]# systemctl status amazon-ssm-agent
```

```
-- amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-03-29 02:53:54 UTC; 21s ago
     Main PID: 3355 (amazon-ssm-agent)
       CGroup: /system.slice/amazon-ssm-agent.service
               └─3355 /usr/bin/amazon-ssm-agent
               └─3382 /usr/bin/ssm-agent-worker
```

```
Mar 29 02:53:54 ip-10-10-20-201.us-west-2.compute.internal amazon-ssm-agent[3355]: 2022-03-29 02:53:54 INFO Agent will take identity f...EC2
```

```
Mar 29 02:53:54 ip-10-10-20-201.us-west-2.compute.internal amazon-ssm-agent[3355]: 2022-03-29 02:53:54 INFO [amazon-ssm-agent] using n...IPC
```

```
Mar 29 02:53:55 ip-10-10-20-201.us-west-2.compute.internal amazon-ssm-agent[3355]: 2022-03-29 02:53:54 INFO [amazon-ssm-agent] using n...IPC
```

```
Mar 29 02:53:55 ip-10-10-20-201.us-west-2.compute.internal amazon-ssm-agent[3355]: 2022-03-29 02:53:54 INFO [amazon-ssm-agent] using n...IPC
```

```
Mar 29 02:53:55 ip-10-10-20-201.us-west-2.compute.internal amazon-ssm-agent[3355]: 2022-03-29 02:53:54 INFO [amazon-ssm-agent] amazon-...0.0
```

```
Mar 29 02:53:55 ip-10-10-20-201.us-west-2.compute.internal amazon-ssm-agent[3355]: 2022-03-29 02:53:54 INFO [amazon-ssm-agent] OS: lin...d64
```

```
Mar 29 02:53:55 ip-10-10-20-201.us-west-2.compute.internal amazon-ssm-agent[3355]: 2022-03-29 02:53:54 INFO [CredentialRefresher] Iden...her
```

```
Mar 29 02:53:55 ip-10-10-20-201.us-west-2.compute.internal amazon-ssm-agent[3355]: 2022-03-29 02:53:55 INFO [amazon-ssm-agent] [LongRu...ess
```

```

Mar 29 02:53:55 ip-10-10-20-201.us-west-2.compute.internal
amazon-ssm-agent[3355]: 2022-03-29 02:53:55 INFO [amazon-ssm-
agent] [LongRu...ted
Mar 29 02:53:55 ip-10-10-20-201.us-west-2.compute.internal
amazon-ssm-agent[3355]: 2022-03-29 02:53:55 INFO [amazon-ssm-
agent] [LongRu...nds
Hint: Some lines were ellipsized, use -l to show in full.

```

4. AWS Cli SSM EC2

```

CT    AWSCLI    IAM API Key    .

##      Client IP
$ curl http://icanhazip.com
1.2.3.4

## AWSCLI
( ) SSM Session-Plugin    AWSCLI 1.16

$      curl
"https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o
"awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install

## Linux SSM Session-Manager Plugin
$      curl
"https://s3.amazonaws.com/session-manager-downloads/plugin/lat
est/linux_64bit/session-manager-plugin.rpm" -o "session-
manager-plugin.rpm"
$ rpm -Uvh session-manager-plugin.rpm
$ session-manager-plugin
The Session Manager plugin was installed successfully. Use the
AWS CLI to start a session.

##

$ aws configure
AWS Access Key ID [None]: AKIAQ25632EPN7T7FFVT
AWS Secret Access Key [None]:
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
Default region name [None]: us-west-2

```

Default output format [None]: json

SSM EC2

```
[root@node1 ~]# aws ssm start-session --target i-064f7ebc0bed75c74
```

Starting session with SessionId: SSM-Only-0a9041d6b13f368ce

sh-4.2\$ **bash**

[ssm-user@ip-10-10-20-201 bin]\$ ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
inet 10.10.20.201 netmask 255.255.255.0 broadcast 10.10.20.255

inet6 fe80::aa:14ff:fed7:abd prefixlen 64 scopeid 0x20<link>

ether 02:aa:14:d7:0a:bd txqueuelen 1000 (Ethernet)

RX packets 31846 bytes 8338621 (7.9 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 29180 bytes 6068149 (5.7 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[ssm-user@ip-10-10-20-201 bin]\$

<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>

https://docs.aws.amazon.com/ko_kr/systems-manager/latest/userguide/session-manager-working-with-install-plugin.html

https://docs.aws.amazon.com/ko_kr/systems-manager/latest/userguide/session-manager-getting-started.html