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 7
 - 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	h the same access type and permis	sions. Learn more		
User name*	SSM-Only			
	• Add another user			
Select AWS access type				
Select how these users will primarily ac an assumed role. Access keys and aut	ccess AWS. If you choose only prog ogenerated passwords are provided	rammatic access, it does NOT p 1 in the last step. Learn more	prevent users from accessing the	
Select AWS credential type*	Access key - Programmatic Enables an access key ID ar other development tools.	access ad secret access key for the AV	VS API, CLI, SDK, and	
	Password - AWS Manageme Enables a password that allo	ent Console access ows users to sign-in to the AWS	Management Console.	
Add user		1	2 3 4 5	
Success You successfully created the users instructions for signing in to the AV you can create new credentials at Users with AWS Management Cor	s shown below. You can view and downlo VS Management Console. This is the last any time. nsole access can sign-in at: https://hostw	ad user security credentials. You car t time these credentials will be availa ay-bmt.signin.aws.amazon.com/cons	n also email users ble to download. However, sole	
Lownload .csv				
User		Access key ID	Secret access key	
🕨 🔮 SSM-Only		AKIAQ25632EPN7T2FFVT	********* Show	

arn

_

IAM

EC2 ID

.

```
{
```

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

```
"arn:aws:ec2:us-west-2:1234567890:instance/i-
```

ahe52134fxed6"

Review policy

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

Name*	SSM-EC2-Connection				
	Maximum 128 characters. Use alphar	laximum 128 characters. Use alphanumeric and '+=,.@' characters.			
Summary	Q Filter				
	Service 🔻	Access level	Resource	Request condition	
	Allow (1 of 321 services) Sh	ow remaining 320			
	Systems Manager	Limited: Write	Multiple	None	

EC2

VPC

2. IAM Custom Role

IAM > Roles > Create role

Step 1 Select trusted entity	Select trusted entity
Step 2	Trusted entity type
Step 3 Name, review, and create	AWS service Allow AWS services Allow AWS services Allow AWS services Allow addition of the services Allow addition of the services and party to perform actions in this account. Allow addition of the services Allow addition of th
	SAML 2.0 federation Custom trust policy Allow users federated with SAML 2.0 from a corporate directory to perform acions in this account. Create a custom trust policy to enable others to perform acions 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

IAM > Roles > Create role Step 1 Select trusted entity	Add permissions		
Step 2 Add permissions	Permissions policies (Selected 1/754) Choose one or more policies to attach to your new role.		Create Policy (2
Step 3	Q Filter policies by property or policy name and press enter		14 matches < 1 > 🛞
	"SSM" X Clear filters		
	■ Policy name 🖉 🗢	Туре 🗢	Description
	AmazonEC2RoleforSSM	AWS m	This policy will soon be deprecated. Please use AmazonSSMManagedInstanceCore 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
	AmazonSSMManagedinstanceCore	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.
Dolo Nomo			

- Role Name

IAM > Roles > Create role

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.	
SSM-EC2-Connection-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



EC2



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' 26.724.168 ==========>1 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... Updating / installing...

/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-ssmagent.service; enabled; vendor preset: enabled)

Active: active (running) since Tue 2022-03-29 02:53:54 UTC; 21s ago

Main PID: 3355 (amazon-ssm-agen)

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

 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]

 amazon-ssm-agent[3355]:
 2022-03-29
 02:53:55
 INFO [amazon-ssm-agent]

 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 AWSCli 1.16) SSM Session-Plugin (\$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86 64.zip" -o "awscliv2.zip" unzip awscliv2.zip sudo ./aws/install SSM Session-Manager Plugin ## Linux \$ curl "https://s3.amazonaws.com/session-manager-downloads/plugin/lat est/linux 64bit/session-manager-plugin.rpm" - 0 "sessionmanager-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]: AKIA025632EPN7T7FFVT [None]: AWS Secret Access Key yxQ61Yw/y5/kkZAU0fdXmKgZZc2azstSE1h+z4w2 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) dropped 0 overruns 0 carrier 0 TX errors 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) bytes 0 (0.0 B) RX packets 0 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-start ed-install.html https://docs.aws.amazon.com/ko_kr/systems-manager/latest/userg uide/session-manager-working-with-install-plugin.html https://docs.aws.amazon.com/ko_kr/systems-manager/latest/userg uide/session-manager-getting-started.html

AWS AMI ? CMK AMI AWS , 가 (Terminated) # # AMI IAM IAM { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["ec2:ModifyImageAttribute"], "Resource": ["arn:aws:ec2:uswest-2::image/<0e9fcdb7ae40e8f4c>" ## id (ami-xxxxxxxxxxxxxxxxxxx XXX)] }] } 가 # KMS Key 가 AWS Account KMS # AMI

다른 AWS 계정 arn:aws:iam::431 126652:root 다른 AWS 계정 추가



EC2 가

AWS Docs : https://aws.amazon.com/ko/blogs/security/how-to-share-encrypte d-amis-across-accounts-to-launch-encrypted-ec2-instances/

CentOS 7 APM

가

yum

yum

Image OS : CentOS 7.6.1810 Minimal # 가 yum install -y epel-release # Apache 2.4.52 RPMs (codeit) сd /etc/yum.repos.d/ && wget https://repo.codeit.guru/codeit.el`rpm -q --qf "%{VERSION}" \$(rpm -q --whatprovides redhat-release)`.repo # 가 yum info httpd Loaded plugins: fastestmirror Loading mirror speeds from cached hostfile * base: mirror.kakao.com * epel: hk.mirrors.thegigabit.com * extras: mirror.kakao.com * remi-safe: mirror.bebout.net * updates: mirror.navercorp.com Installed Packages Name : httpd Arch : x86 64 : 2.4.52 Version Release : 1.codeit.el7 Size : 4.3 M : installed Repo From repo : CodeIT

가

Summary : Apache HTTP Server URL : https://httpd.apache.org/ : ASL 2.0 License Description : The Apache HTTP Server is a powerful, efficient, and extensible : web server. # Apache yum --enablerepo=CodeIT install httpd mod ssl # PHP 7.4 Remi Repository install v u m https://rpms.remirepo.net/enterprise/remi-release-7.rpm # PHP 7.4 yum repolist all | grep -i php yum --enablerepo=remi-php74 install php php-opcache php-gd php-mysql php-xml # MariaDB 10.3 cat << EOF | tee /etc/yum.repos.d/MariaDB.repo</pre> [mariadb] name = MariaDBbaseurl = http://yum.mariadb.org/10.3/centos7-amd64 gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB apacheck=1 enabled=0 EOF # MariaDB 10.3 yum -y install --enablerepo=mariadb MariaDB-server MariaDBclient MariaDB-backup # APM [root@localhost ~]# php -v PHP 7.4.28 (cli) (built: Feb 15 2022 13:23:10) (NTS) Copyright (c) The PHP Group Zend Engine v3.4.0, Copyright (c) Zend Technologies with Zend OPcache v7.4.28, Copyright (c), by Zend Technologies [root@localhost ~]# mysql --version mysql Ver 15.1 Distrib 10.3.34-MariaDB, for Linux (x86 64)

using readline 5.1 [root@localhost ~]# httpd -v Server version: Apache/2.4.52 (codeit) Server built: Dec 20 2021 11:29:54

가 가

Windows 2012

Windows Server 2012

Windows 2012 1

.

Windows Server 2012

Windows Server 2012

.

•

gpedit.msc

Ð	실행 ×
	프로그램, 폴더, 문서, 또는 인터넷 주소를 입력하여 해당 항목을 열 수 있습니다.
열기(0):	gpedit.msc ✓
	확인 취소 찾아보기(B)

.

가



<u>I</u>	로컬 그룹	룹 김	정책 편집기 📃 🗖 🗙	:
파일(F) 동작(A) 보기(V)	도움말(H)			
🗢 🏟 🖄 🖬 🗟 👔	F			
☐ 이벤트 전달 ∧ ☐ 인터넷 정보 서비스	🎽 연결			
 자격 증명 사용사 인 자동 실행 정책 	연결 개수 제한		설정	-
작업 스케줄러 장치 및 드라이버 호 조리 유서	<u>정책 설정</u> 편집	^	E 지중 다시 건설 E Allow users to connect remotely by using Remote Desktop E 콘솔 세션에 로그인한 관리자의 로그오프 거부	구(구(구(
등표 급신 태블릿 PC	표구 사망: Windows Server 2003 이상		E Keep-alive 연결 간격 구성	구
 □ 등 서비스 □ TS 라이선스 □ 원격 데스크톱 서 □ TS 세션 브로 □ 라이선스 □ 라이선스 □ 보안 □ 세션 시간 제 □ 연결 □ 원격 세션 환 □ 응용 프로그림 □ 임시 폴더 □ 장치 및 리소: □ 프로필 □ 프로필 	설명: 원격 데스크톱 서비스에서 서버에 대한 동시 연결 수를 제한할지 여 부를 지정합니다. 이 설정을 사용하면 서버에서 활성 화할 수 있는 원격 데스크톱 서비 스 세션 수를 제한할 수 있습니다. 이 수가 초과되면 추가 사용자가 연결을 시도할 때 서버가 사용 중 이므로 나중에 다시 시도하라는 오 류 메시지가 사용자에게 표시됩니 다. 세션 수를 제한하면 시스템 리 소스를 사용하는 세션 수가 제한되 므로 성능이 향상됩니다. 기본적으		 ● 연결 개수 제한 ■ 앱 등록을 완료하기 위해 사용자 로그인 일시 중단 ■ 터미널 서비스 사용자 세션의 원격 제어 규칙 설정 ■ Select network detection on the server(서버에서 네트워크 ■ Select RDP transport protocols(RDP 전송 프로토콜 선택) ■ 원격 데스크톱 서비스 사용자를 하나의 원격 데스크톱 서비 ■ 목록에 없는 프로그램의 원격 시작 허용 ■ CPU FSS(Fair Share Scheduling) 사용 안 함 	ネ ネネネネネネ
	도 KD 세션 오슬드 시미는 원격 네 스크트 <u>프바이스 베셔 스크 페히히</u>		< III	>
< III >	\확장/(표준/			

[

]

.	ę	변결 개수 제한	_ D X
📴 연결 개수 제한		이전 설정(P) 다음 설정	!(N)
 ● 구성되지 않음(C) 설명: ○ 사용(E) ○ 사용 안 함(D) 지원: 	Windows Server 2003	이상	
옵션:		도움말:	Y
TS 최대 허용 연결 1 연결을 제한하지 않으려면 999	999를 입력하십시오.	원격 데스크톱 서비스에서 서버에 대한 동시 여부를 지정합니다. 이 설정을 사용하면 서버에서 활성화할 수 있 서비스 세션 수를 제한할 수 있습니다. 이 수 용자가 연결을 시도할 때 서버가 사용 중이드 도하라는 오류 메시지가 사용자에게 표시되 하면 시스템 리소스를 사용하는 세션 수가 저 상됩니다. 기본적으로 RD 세션 호스트 서버 비스 세션 수를 제한하지 않으며 관리용 원격 의 원격 데스크톱 서비스 세션을 허용합니다 이 설정을 사용하려면 서버에 대해 최대값으 입력합니다. 연결 수를 제한하지 않으려면 9 다. 상태를 사용으로 설정하면 Windows 버전 및 원격 데스크톱 서비스 모드와 일치하는 지정 수가 제한됩니다.	연결 수를 제한할지 △ 났는 원격 데스크톱 가 초과되면 추가 사 으로 나중에 다시 시 니다. 세션 수를 제한 1한되므로 성능이 향 = 원격 데스크톱 서 취 데스크톱은 두 개 로 지정할 연결 수를 99999를 입력합니 시버에서 실행되는 된 수로 최대 연결 설정하면 그룹 정책 ✓
		확인 적	위소 적용(A)
[]	. (, TS 2)	

9	අ	년결 개수 제한 📃 🗖 🗙
📷 연결 개수 제한		이전 설정(P) 다음 설정(N)
 ○ 구성되지 않음(C) 설명: ● 사용(E) ○ 사용 안 함(D) 지원: 	Windows Server 2003	
옵션:		도움말:
TS 최대 허용 연결 2 연결을 제한하지 않으려면 999	 1999를 입력하십시오.	원격 데스크톱 서비스에서 서버에 대한 동시 연결 수를 제한할지 여부를 지정합니다. 이 설정을 사용하면 서버에서 활성화할 수 있는 원격 데스크톱 서비스 세션 수를 제한할 수 있습니다. 이 수가 초과되면 추가 사 용자가 연결을 시도할 때 서버가 사용 중이므로 나중에 다시 시 도하라는 오류 메시지가 사용자에게 표시됩니다. 세션 수를 제한 하면 시스템 리소스를 사용하는 세션 수가 제한되므로 성능이 향 상됩니다. 기본적으로 RD 세션 호스트 서버는 원격 데스크톱 서 비스 세션 수를 제한하지 않으며 관리용 원격 데스크톱 수 비스 세션 수를 제한하지 않으며 관리용 원격 데스크톱은 두 개 의 원격 데스크톱 서비스 세션을 허용합니다. 이 설정을 사용하려면 서버에 대해 최대값으로 지정할 연결 수를 입력합니다. 연결 수를 제한하지 않으려면 9999999를 입력합니 다. 상태를 사용으로 설정하면 Windows 버전 및 서버에서 실행되는 원격 데스크톱 서비스 모드와 일치하는 지정된 수로 최대 연결 수가 제한됩니다. 상태를 사용 안 함 또는 구성되지 않음으로 설정하면 그룹 정책 ▼
		확인 취소 적용(A)

2

[

가

,

]

<u>I</u>	로컬 그룹 정책 편집기	_ _ X
파일(F) 동작(A) 보기(V)	도움말(H)	
🗢 🍬 🖄 📰 🗟 🛛		
C 이벤트 전달 ^ 인터넷 정보 서비스	은 연결	
 자격 증명 사용자 인 자동 실행 정책 작업 스케줄러 	원격 데스크톱 서비스 사용자를 하나 설정 의 원격 데스크톱 서비스 세션으로 제 한 때 Allow users to connect remotely by using	a Remote Desktop
🦰 장치 및 드라이버 호 🦰 종료 옵션 🎬 태블릿 PC	<u>정책 설정</u> 편집	거부
터미널 서비스 TS 라이선스 에 위격 데스크토 세	요구 사항: Windows Server 2003 이상 비한 면결 개수 세한 한 앱 등록을 완료하기 위해 사용자 로그인 일 비해 터미널 서비스 사용자 세션의 원격 제어 구	일시 중단 구 규칙 설정 구
· · · · · · · · · · · · · · · · · · ·	열명: 이 정책 설정으로 사용자를 하나 의 원격 데스크톱 서비스 세션으 로 제한할 수 있습니다. 도 정말 전 에스크토 서비스 사용자를 하나 등 Select RDP transport protocols(RDP 전송	버에서 네트워크 구 프로토콜 선택) 구
입 오건 입 세션 시간 제 입 연결 ■ > 입 위경 세셔 하	이 정책 설정을 사용하면 원격 데 스크톱 서비스를 사용하여 원격으 로 로 고요하는 사용자가 해당 서버	·····································
▷ 전국 제권 된 응용 프로그램 입 임시 폴더 입 장치 및 리소: 프로필	외 포크는 이는 지공지가 해당 지미 에서 하나의 세션(활성 또는 연결 이 끊긴 상태)으로 제한됩니다. 사 용자가 연결이 끊긴 상태에서 세션 을 종료하면 다음 로그은할 때 사 용자가 해단 세션에 자동으로 다. ♥	
🦰 프린터 리디릭 🗸		>
	\왁상/#순/	

•

🐓 🛛 원격 데스크톱 서	비비스 사용자를 하나의	원격 데스크톱 서비스 세션으로 제한 🛛 🗕 🗖 🗙
🔚 원격 데스크톱 서비스 시	사용자를 하나의 원격 데스크	톱 서비스 세션으로 제한 이전 설정(P) 다음 설정(N)
◉ 구성되지 않음(C) 설등	8:	<u>^</u>
○ 사용(E)		
○ 사용 안 함(D)		▼
A1	원: Windows Server 2003 (이상 ^
옵션:		도움말:
		 이 정책 설정으로 사용자를 하나의 원격 데스크톱 서비스 세션으로 지한할 수 있습니다. 이 정책 설정을 사용하면 원격 데스크톱 서비스를 사용하여 원격으로 로그온하는 사용자가 해당 서버에서 하나의 세션(활성 또는 연결이 끊긴 상태)으로 제한됩니다. 사용자가 연결이 끊긴 상태에서 세션을 종료하면 다음 로그온할 때 사용자가 해당 세션에 자동으로 다시 연결됩니다. 이 정책 설정을 사용하지 않으면 사용자가 원격 데스크톱 서비스를 사용하여 원하는 수만큼 동시 원격 연결을 설정할 수 있습니다. 이 정책 설정을 구성하지 않으면 그룹 정책 수준에서 이 정책 설정의 지정되지 않습니다.
		×
		확인 취소 적용(A)

•

🐓 🏾 원격 데스크튐	톱 서비	스 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한 🛛 🗕 🗖 🗙
📆 원격 데스크통 서비	스 사용	자를 하나의 원격 데스크톱 서비스 세션으로 제한 이전 설정(P) 다음 설정(N)
○ 구성되지 않음(C)	설명:	
○ 사용(E)		
◉ 사용 안 함(D)		✓
	지원:	Windows Server 2003 이상
옵션:		도움말:
		 이 정책 설정으로 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한할 수 있습니다. 이 정책 설정을 사용하면 원격 데스크톱 서비스를 사용하여 원격으로 로그온하는 사용자가 해당 서비에서 하나의 세션(활성 또는 연결이 끊긴 상태)으로 제한됩니다. 사용자가 연결이 끊긴 상태에서 세션을 종료하면 다음 로그온할 때 사용자가 해당 세션에 자동으로 다시 연결됩니다. 이 정책 설정을 사용하지 않으면 사용자가 원격 데스크톱 서비스를 사용하여 원하는 수만큼 동시 원격 연결을 설정할 수 있습니다. 이 정책 설정을 구성하지 않으면 그룹 정책 수준에서 이 정책 설정이 지정되지 않습니다.
		확인 취소 적용(A)

.



CentOS 7 (1)

,

.

CentOS 7

가

,

,

(

)

,

가

LVM : Default		가 ,	
가			
	T 3 78 #		71
			71
XIS			
1.			
(OS)	
# ip addr			
<pre># vi /etc/sysconfig/network-scripts/if</pre>	fcfg-eth0		
 BOOTPROTO=none			
IPV6INIT=no			
IPV6_AUTOCONF=no			
IPV6_DEFROUTE=no			
IPV6_FAILURE_FATAL=no			
IPV6_ADDR_GEN_MODE=Stable-privacy			
ONBOOT=ves #	/		
yes			
IPV6_PRIVACY=no			
IPADDR=192.168.122.243			
NETMASK=255.255.255.0			
GATEWAY = 192.168.122.1			
DNS1=0.0.0.0			
<pre># systemctl restart network</pre>			
# ip addr			
eth0 IP			
<pre># ping -c 4 google.com #</pre>			
google.com ping statistics			

,

4 packets transmitted, 4 received, 0% packet loss, time 3094ms rtt min/avg/max/mdev = 82.692/83.010/83.554/0.492 ms

,

2.

CentOS 7 timedatectl

timedatectl

RTC time : NTP enabled : NTP NTP synchronized : NTP RTC in local TZ : RTC Time zone

timedatectl list-timezones | grep -i Asia*

- # timedatectl set-timezone Asia/Seoul
- # timedatectl

3. Hostname

CentOS 7

hostname localhost.localdomain

hostnamectl
Static hostname: localhost.localdomain

hostnamectl set-hostname newhostname

hostnamectl
Static hostname: newhostname

4. SELinux

SELinux

vi /etc/sysconfig/selinux

,

SELINUX=disabled . . .

.

shutdown -r now

getenforce
Disabled

5. root 가

root

•

ps -ef | grep sshd
systemctl enable sshd

vi /etc/ssh/sshd_config
. . .
PermitRootLogin=no

systemctl restart sshd

6.

. . .

vi /etc/profile.d/timeout.sh
TMOUT=600
export TMOUT

su

•

chmod +x /etc/profile.d/timeout.sh

source /etc/profile
echo \$TMOUT
600

7.

.

history

vi /etc/profile.d/history.sh

HISTTIMEFORMAT="%F %T -- " export HISTTIMEFORMAT

chmod 644 /etc/profile.d/history.sh
source /etc/profile.d/history.sh

hisotry

999 2022-04-06 14:50:10 -- vi /etc/profile.d/history.sh 1000 2022-04-06 14:50:19 -- chmod 644 /etc/profile.d/history.sh 1001 2022-04-06 14:50:28 -- source /etc/profile.d/history.sh 1002 2022-04-06 14:50:30 -- history

8.

localectl
System Locale: LANG=en_US.UTF-8
VC Keymap: us
X11 Layout: us

```
# localectl list-locales | grep -i kr
ko_KR
ko_KR.euckr
ko_KR.utf8
# localectl set-locale LANG=ko_KR.UTF-8
# localectl set-keymap kr
# localectl set-x11-keymap kr
# localectl
System Locale: LANG=ko_KR.UTF-8
VC Keymap: kr
X11 Layout: kr
```

•