DevOps Learning Notes

DevOps Learning Notes

Cloud Introduction

AWS Introduction

EC2 Introduction

EC2 Basics

EC2 Pricing Models

Linux Introduction

VI Editor & AWS Security Group

SSH Application

Linux Permissions

Sudo & System Log Files

Process & Performance Management

EBS Volume Management

EBS Snapshot - AMI & SNS

DevOps Learning Notes

44 views . 1 likes ♡ . 1 shares

Edwiki Trainings
1 Followers

FOLLOW

Sudo & System Log Files

In this lecture you are learning below concepts:

1. Sudo Permissions
2. Linux Default directories
3. system log files

Sudo Permissions:

Sudo stands for “Super user DO” and it will help to granting or to provide root privileges to normal user to run privileged commands. Normal Users can login using their username and password and can run administration commands using with sudo.

1. /etc/sudoers is the default configuration file for sudo.

```
[root@localhost ~]# ls -l /etc/sudoers
-r--r----- 1 root root 4375 Nov 26  2020 /etc/sudoers
[root@localhost ~]#
```

1. The file /etc/sudoers file has the set of rules that users to follow when using sudo command. It means whatever the commands access provided for user in /etc/sudoers file user can access or run those commands.
2. You use “visudo” command to edit sudoers configuration file. Editing the file using visudo commands helps to warn you if any syntax issues in the file.
3. Below examples configuration shows how to grant sudo su access to normal user ‘edwiki’

```
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
edwiki  ALL=(ALL)       NOPAASWD: /usr/bin/su
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOC
ATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL
```

Now “edwiki” can switch to “root” without being prompted for password.

```
[edwiki@localhost ~]$ sudo su -
Last login: Sat Feb  4 11:32:00 UTC 2023 on hvc0
[root@localhost ~]#
```

Below example allowed netstat command to run user whoever part of “devops” group.

```
## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL
%devops         ALL=(ALL)       NOPASSWD: /usr/bin/netstat
## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom
```

The edwiki user is part of devops group and now edwiki user is privileged to run netstat command without being prompted for root password.

```
 [edwiki@localhost ~]$ id edwiki
uid=1000(edwiki) gid=1000(edwiki) groups=1000(edwiki),1001(devops)
[edwiki@localhost ~]$ sudo netstat -tuplan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
```

X

here.

6. /mnt - Directory for overmount process during the boot time
7. /root – root user home directory
8. /tmp – temporary directory to store operation related temp files
9. /dev – All device specific files are located here

System log files:

Log file is the file where application or system related activity stored. Below are the some important system related log files that helps to check for any system errors, login activity etc..

/var/log/auth.log or **/var/log/secure**:

User login details like authentication logs for user login both successful and failure logins will store under secure file.

/var/log/boot.log:

Under boot.log system booting info wills save. If server have any issues at booting time those logs will store under boot logs.

/var/log/dmesg:

Under dmesg logs we can find device and driver related logs.

/var/log/messages:

Here we can see general messages related to os system. Messages will store all system related logs.

/var/log/yum.log:

Yum.log hold the data on any software installation or packages installation that used yum command.

SSH Password Less Authentication:

SSH application supports authenticating Linux users using private and public key pair.

You can change the authenticating method in the sshd_config configuration file.

Below is the parameter that you need to define in the sshd_config to set authentication method to password or key based.

```
PasswordAuthentication no/yes
```

You can generate SSH kay pair using below command which creates private and public key combinations and store them in ~/.ssh folder by default.

```
[pr@ip-172-31-52-242 ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/pr/.ssh/id_rsa):
Created directory '/home/pr/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
[pr@ip-172-31-52-242 ~]$
```

It created the keypair as below

```
[pr@ip-172-31-52-242 ~]$ ls -l ~/.ssh
total 8
-rw------- 1 pr pr 1675 Feb  4 05:00 id_rsa
-rw-r--r-- 1 pr pr  414 Feb   4 05:00 id  rsa.pub
```

```
[pr@ip-172-31-52-242 ~]$ cat ~/.ssh/authorized_keys
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDNfBN3UBoz8hLMLozPY0nWmmmd
6pWZPN+ibFx4KtXHFbdUW4Q1WFOQeHqzClcHROz14sQ6o4dAT28RZmtcF21
RfRvW3t0RVxJ4RfZgJqX+AVj2iqT1jHO2ZYktP3/BCtgOOVB1X6ipiNOFYxmA+m
hOplTbFkFpC9yjpjb5OJCbAml1nyHLLqaQHVjvGNscMhGNrJlk6JWW8Z20FgAt
3/dFbmmjRzZUNsuTWnArkpis5xeoJF0fyerQmAijD8hrNe4PPf4qbLPVATLtDw4
Hf2tUb7BwFa0x+QdNH04x23roAcaVok2byQYpge5BSJhvzczM8QfZOUu5u/DO
PKJReFWz pr@ip-172-31-52-242.ec2.internal
[pr@ip-172-31-52-242 ~]$
```

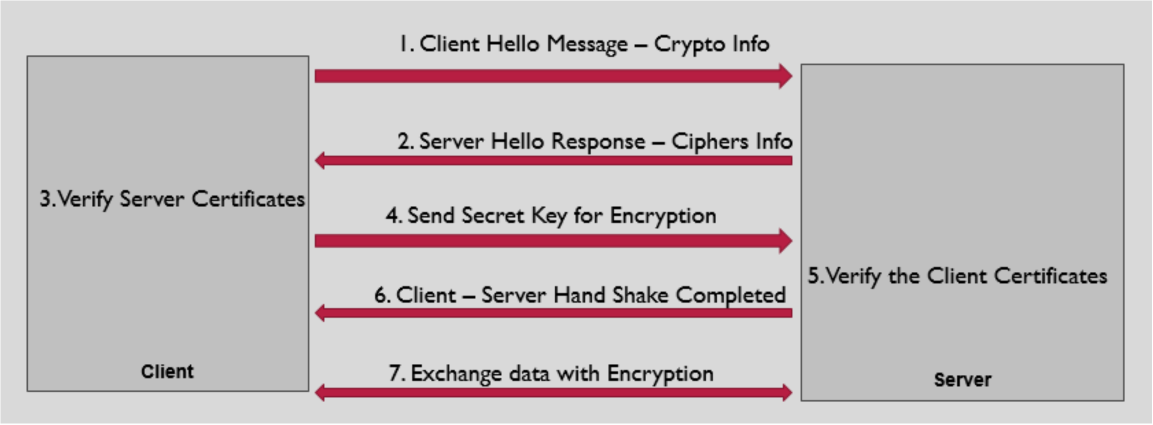
1. Attach the private key the client request to initiate the login request to the server
2. Ensure that the .ssh and authorized_keys files are secured with limited permissions allowing only owner can access them.

```
[pr@ip-172-31-52-242 ~]$ ls -ld ~/.ssh
drwx------ 2 pr pr 43 Feb  4 05:11 /home/pr/.ssh

[pr@ip-172-31-52-242 ~]$ ls -l ~/.ssh/authorized_keys
-rw------- 1 pr pr 414 Feb  4 05:00 /home/pr/.ssh/authorized_keys
```

NOTE: When you create key pair in AWS console it creates public and private keys. Private key is downloaded to your local system and public key is stored at AWS side and that public key will be placed in the EC2 instance default location to make password less authentication to the default user names like ec2-user for amazon linux systems.

Below diagram shows the SSH handshake process between client and server:


1. Client Hello Message – Crypto Info
2. Server Hello Response – Ciphers Info
3.Verify Server Certificates
4. Send Secret Key for Encryption
5.Verify the Client Certificates
6. Client – Server Hand Shake Completed
7. Exchange data with Encryption
Client
Server

Previous

Next

Comments(0)