

RHCSA EX200 - Accessing linux systems LAB

- Log in and switch users in multiuser targets
- Access remote systems using SSH
- Configure Key-based authentication for SSH
- Securely transfer files between systems

```
csr@MainPC:~/Downloads$ ssh cloud_user@3.80.189.75
The authenticity of host '3.80.189.75 (3.80.189.75)' can't be established.
ED25519 key fingerprint is SHA256:4nFxuEkL7XMM8ehB0hYTUHPRJTYV0O8iyC8MsidjbUs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.80.189.75' (ED25519) to the list of known hosts.
(cloud_user@3.80.189.75) Password:
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
cloud_user@server1: ~ $ whoami ; groups
cloud_user
cloud_user wheel sysadmins
cloud_user@server1: ~ $ id
uid=1001(cloud_user) gid=1001(cloud_user) groups=1001(cloud_user),10(wheel),49999(sysadmins)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
cloud_user@server1: ~ $
```

This will show what happens and what files are sourced or executed when using different types of privilege elevations

```
cloud_user@server1: ~ $ sudo -i
[sudo] password for cloud_user:
root@server1: ~ # echo export SOURCED1=.bash_profile >> ~/.bash_profile ; echo 'echo $SOURCED1' >>
~/.bash_profile
root@server1: ~ # grep SOURCED .bash_profile
export SOURCED1=.bash_profile
echo $SOURCED1
root@server1: ~ # echo export SOURCED2=.bashrc >> ~/.bashrc ; echo 'echo $SOURCED2' >> ~/.bashrc
root@server1: ~ # grep SOURCED .bashrc
export SOURCED2=.bashrc
echo $SOURCED2
```

```
cloud_user@server1: ~ $ sudo -k ## When used without a command, invalidates the user's cached credentials
for the current session. The next time sudo is run in the session, a password must be entered if the security
policy requires authentication
cloud_user@server1: ~ $ sudo -i echo
[sudo] password for cloud_user:
.bashrc
.bash_profile
```

```
cloud_user@server1: ~ $ sudo -i passwd root
[sudo] password for cloud_user:
.bashrc
.bash_profile
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
cloud_user@server1: ~ $ su -c 'echo $PATH'
Password:
/home/cloud_user/.local/bin:/home/cloud_user/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
cloud_user@server1: ~ $ su - -c 'echo $PATH'
Password:
.bashrc
.bash_profile
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/root/bin
cloud_user@server1: ~ $
```

sudo = cloud_user

```
sudo -i = root user
```

```
su = cloud_user
```

```
su - = root user
```

Task 2 - access remote systems using ssh

Ssh to second server

```
cloud_user@server1: ~ $ ssh cloud_user@10.0.1.197
The authenticity of host '10.0.1.197 (10.0.1.197)' can't be established.
ECDSA key fingerprint is SHA256:FplhCnLMLm5YPqa00ssQIH/FEVGrxMaNkThmr4r8Aal.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.197' (ECDSA) to the list of known hosts.
Password:
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
cloud_user@server2: ~ $
```

Retrieving information from remote server and creating a file to input data

```
cloud_user@server1: ~ $ ssh -t cloud_user@10.0.1.197 df -hT >> server_health.txt
Password:
Connection to 10.0.1.197 closed.
cloud_user@server1: ~ $ ls
audit build init_pass mariadb_repo_setup Public server_health.txt Templates wget-1.19.5-
8.el8_1.1.x86_64.rpm
cloud_user@server1: ~ $ cat server_health.txt
Filesystem   Type     Size  Used Avail Use% Mounted on
devtmpfs    devtmpfs 1.8G   0 1.8G   0% /dev
tmpfs       tmpfs    1.9G   0 1.9G   0% /dev/shm
tmpfs       tmpfs    1.9G  17M 1.9G   1% /run
tmpfs       tmpfs    1.9G   0 1.9G   0% /sys/fs/cgroup
/dev/xvda2  xfs      20G  14G 6.7G  67% /
tmpfs       tmpfs    373M   0 373M   0% /run/user/1001
cloud_user@server1: ~ $ ssh -t cloud_user@10.0.1.197 df free >> server_health.txt
Password:
Connection to 10.0.1.197 closed.
cloud_user@server1: ~ $ cat server_health.txt
```

```
Filesystem Type Size Used Avail Use% Mounted on
devtmpfs devtmpfs 1.8G 0 1.8G 0% /dev
tmpfs tmpfs 1.9G 0 1.9G 0% /dev/shm
tmpfs tmpfs 1.9G 17M 1.9G 1% /run
tmpfs tmpfs 1.9G 0 1.9G 0% /sys/fs/cgroup
/dev/xvda2 xfs 20G 14G 6.7G 67% /
tmpfs tmpfs 373M 0 373M 0% /run/user/1001
```

df: free: No such file or directory

cloud_user@server1: ~ \$ free

	total	used	free	shared	buff/cache	available
Mem:	3818520	279104	2419652	18768	1119764	3297500
Swap:	8388604	0	8388604			

cloud_user@server1: ~ \$ ssh cloud_user@10.0.1.197

Password:

Register this system with Red Hat Insights: insights-client --register

Create an account or view all your systems at <https://red.ht/insights-dashboard>

Last login: Wed Apr 10 18:37:25 2024 from 10.0.1.151

cloud_user@server2: ~ \$ free

	total	used	free	shared	buff/cache	available
Mem:	3818520	241588	2697600	18764	879332	3336480
Swap:	8388604	0	8388604			

cloud_user@server2: ~ \$ exit

logout

Connection to 10.0.1.197 closed.

cloud_user@server1: ~ \$ ssh -t cloud_user@10.0.1.197 free >> server_health.txt

Password:

Connection to 10.0.1.197 closed.

cloud_user@server1: ~ \$ cat server_health.txt

```
Filesystem Type Size Used Avail Use% Mounted on
devtmpfs devtmpfs 1.8G 0 1.8G 0% /dev
tmpfs tmpfs 1.9G 0 1.9G 0% /dev/shm
tmpfs tmpfs 1.9G 17M 1.9G 1% /run
tmpfs tmpfs 1.9G 0 1.9G 0% /sys/fs/cgroup
/dev/xvda2 xfs 20G 14G 6.7G 67% /
tmpfs tmpfs 373M 0 373M 0% /run/user/1001
```

df: free: No such file or directory

	total	used	free	shared	buff/cache	available
Mem:	3818520	239348	2699840	18692	879332	3338776
Swap:	8388604	0	8388604			

Task 3 - creating a keygen to ssh to remote server

```
cloud_user@server1: ~ $ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/cloud_user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/cloud_user/.ssh/id_rsa.
Your public key has been saved in /home/cloud_user/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:Ag8dXpCf+hWNs+ftc4ltGtOET3s3vd6UKPAWwjCdlbg cloud_user@server1
The key's randomart image is:
+---[RSA 3072]----+
|  o++ +..  |
|  o.+o+ .  |
|  o o. +.o  |
|  + oE=..  |
|  o.S..=o  |
|  .. ==o.. o|
|  .o*+=.o+|
|  ..o=. =o=|
|  ..oo*.|
+----[SHA256]-----+
cloud_user@server1: ~ $ ssh-copy-id 10.0.1.197
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/cloud_user/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
Password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh '10.0.1.197'"
and check to make sure that only the key(s) you wanted were added.

cloud_user@server1: ~ $ ssh cloud_user@10.0.1.197
Register this system with Red Hat Insights: insights-client --register
```

Create an account or view all your systems at <https://red.ht/insights-dashboard>

Last login: Wed Apr 10 18:38:22 2024 from 10.0.1.151

cloud_user@server2: ~ \$

`eval` is used on a Unix or Linux system to execute the arguments as a shell command. The `eval` command is helpful when you want to execute a Unix or Linux command that has been saved in a variable

`ssh-agent` is a background program that handles passwords for SSH private keys. The `ssh-add` command prompts the user for a private key password and adds it to the list maintained by `ssh-agent`. Once you add a password to `ssh-agent`, you will not be prompted for it when using SSH or scp to connect to hosts with your public key.

```
cloud_user@server1: ~ $ eval $(ssh-agent -s)
```

```
Agent pid 3231
```

```
cloud_user@server1: ~ $ ssh-add
```

```
Identity added: /home/cloud_user/.ssh/id_rsa (cloud_user@server1)
```

```
cloud_user@server1: ~ $ ssh cloud_user@10.0.1.197
```

```
Register this system with Red Hat Insights: insights-client --register
```

```
Create an account or view all your systems at https://red.ht/insights-dashboard
```

```
Last login: Wed Apr 10 18:41:49 2024 from 10.0.1.151
```

```
cloud_user@server2: ~ $
```

Revision #1

Created 10 April 2024 17:45:16 by Cesar Gzz

Updated 10 April 2024 20:26:45 by Cesar Gzz