Inventory - Linux

Alternative authentication with private key or Sudo user

TITLE	Inventory - Linux
AUTHOR	Docusnap Consulting
DATE	6/5/2024
VERSION	4.0 | valid from January 05, 2023

TABLE OF CONTENTS

1. INTRODUCTION

For the inventory of Linux systems, Docusnap offers three different variants regarding authentication:

- Root
- Sudo
- Private Keys

The alternatives for authentication (sudo and Private Keys) on the Linux systems to be inventoried are helpful if the root user is not available or access by root users via SSH is blocked.

Furthermore, the script-based inventory for Linux systems is also available. Further information can be found in the provided HowTo: Docusnap Script Linux.

This HowTo describes the use of one or more Private Keys and the necessary configuration to use a sudo user.

2. PRIVATE KEYS IN DOCUSNAP

2.1 CREATE AND USE PRIVATE KEYS IN DOCUSNAP

Docusnap offers you the possibility to create or import RSA keys, in OpenSSH format, for Linux inventory. The following encryption algorithms can be used for this purpose:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519
- ssh-rsa (can be created by Docusnap)

Private keys can be created and managed in Docusnap administration.

- Administration - Inventory – Private Key Management

Click the **New** button to create an RSA key. Enter a **name** for this and choose **Create RSA Key**. The key pair is encrypted using the ssh-rsa method. The key used is then encrypted again and stored in the database. A passphrase is not created.

If you want to increase security and additionally store a passphrase, you can create the private key with a third-party product (e.g. PuTTY Key Gen or ssh-keygen).

When creation is complete, you can preview the key - this is useful for better identification when using different keys.

Now select **Save** and the key has been successfully created.

You can repeat the above steps as often as you like, for example to create keys for the different clients in your Docusnap environment and then use them.

With the button **Export PublicKey** you can export the public key and store it on the Linux systems - see chapter 2.3.

2.2 IMPORT OF AN EXISTING PRIVATE KEY

An existing private key can be imported to Docusnap as follows.

- Docusnap - Management - Inventory - Private Key Management New

In the next step, assign a **Name** to the key and select the **Import Private Key** button - select your existing private key.

If a passphrase is used for the key, you will be asked for it. The key is then stored in Docusnap.

With the button **Export PublicKey** you can export the public key and store it on the Linux systems - see chapter 2.3.

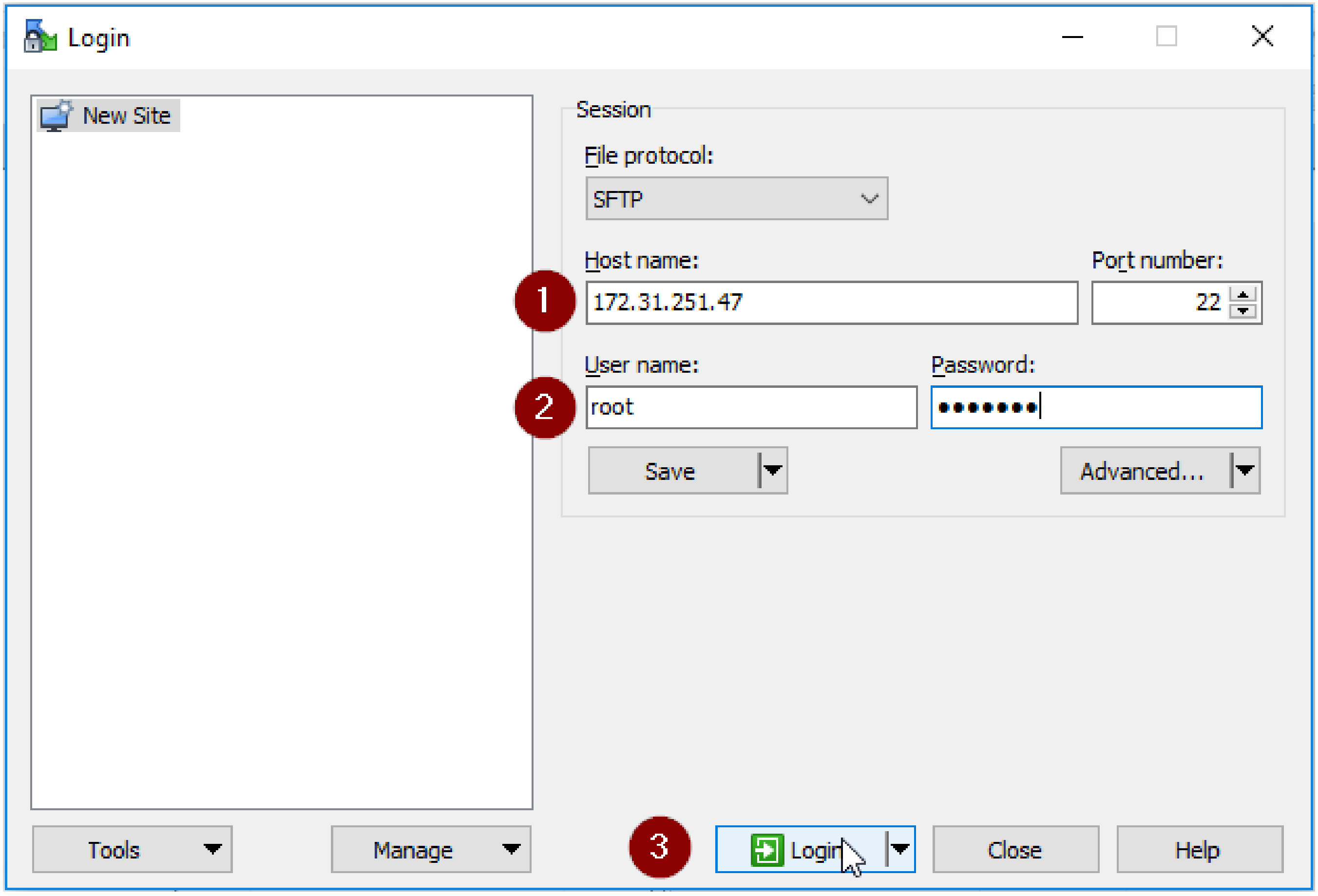
2.3 DEPOSIT KEY ON LINUX SYSTEM

The described steps might differ between the Linux distributions. Please inform yourself in advance in which directory and which file the public key for your distribution is to be entered. The following application example is performed on a Ubuntu system (16.04.2 64-bit).

In this HowTo the software WinSCP is used, so that the public key is deposited on the Linux system.

Open WinSCP and establish the connection to the Linux system.

If the server is not yet known to the client, a security message is displayed. Click Yes to add the host key to the list of trusted machines.



File protocol: SFTP

Host name: 172.31.251.47

Port number: 22

User name: root

Password: •••••••

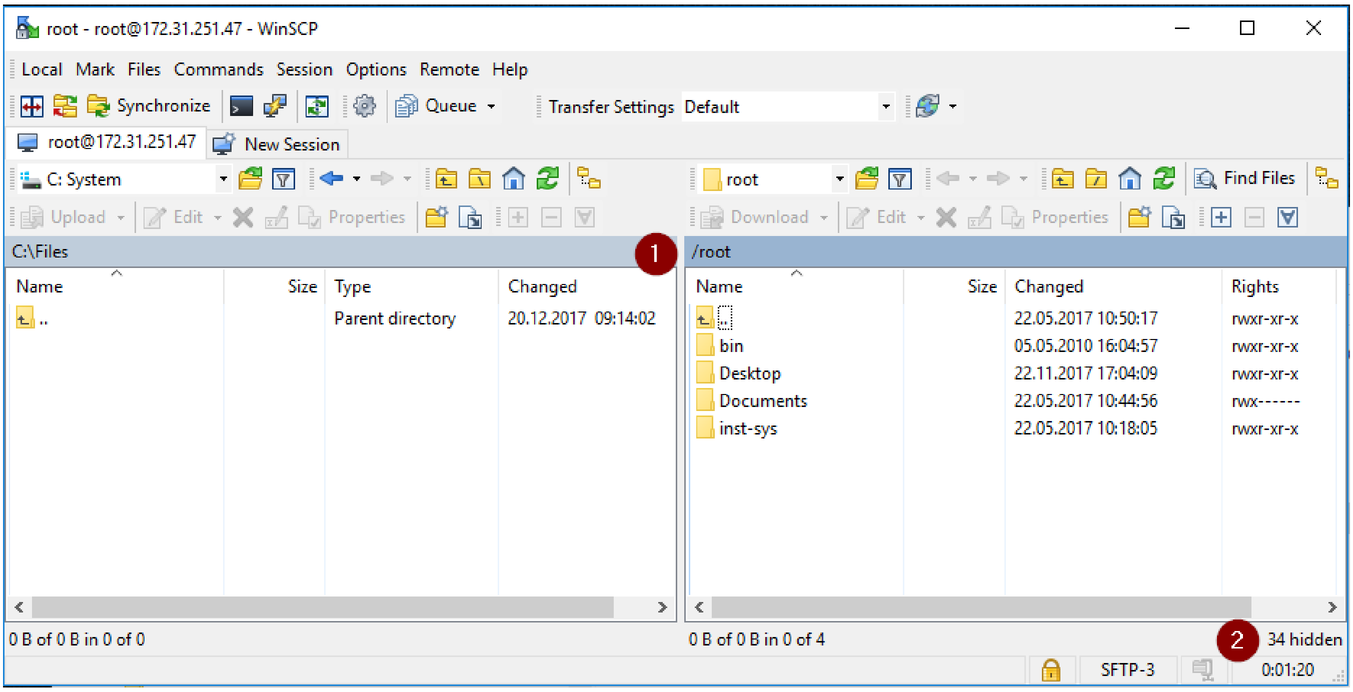
Fig. 1 - Establishing a WinSCP Connection

Step 1

After login, WinSCP changes to the home directory of the logged in user. If this is not the user you connect to via SSH in the future, change to the corresponding home directory.

Step 2

If hidden files and folders are not displayed, please click on the label that shows the number of hidden files.


root - root@172.31.251.47 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
root@172.31.251.47
New Session
C: System
root
Find Files
Upload
Edit
Properties
Download
1
2
SFTP-3
0:01:20

C:\Files

Name	Size	Type	Changed
..		Parent directory	20.12.2017 09:14:02

/root

Name	Size	Changed	Rights
..		22.05.2017 10:50:17	rwxr-xr-x
bin		05.05.2010 16:04:57	rwxr-xr-x
Desktop		22.11.2017 17:04:09	rwxr-xr-x
Documents		22.05.2017 10:44:56	rwx------
inst-sys		22.05.2017 10:18:05	rwxr-xr-x

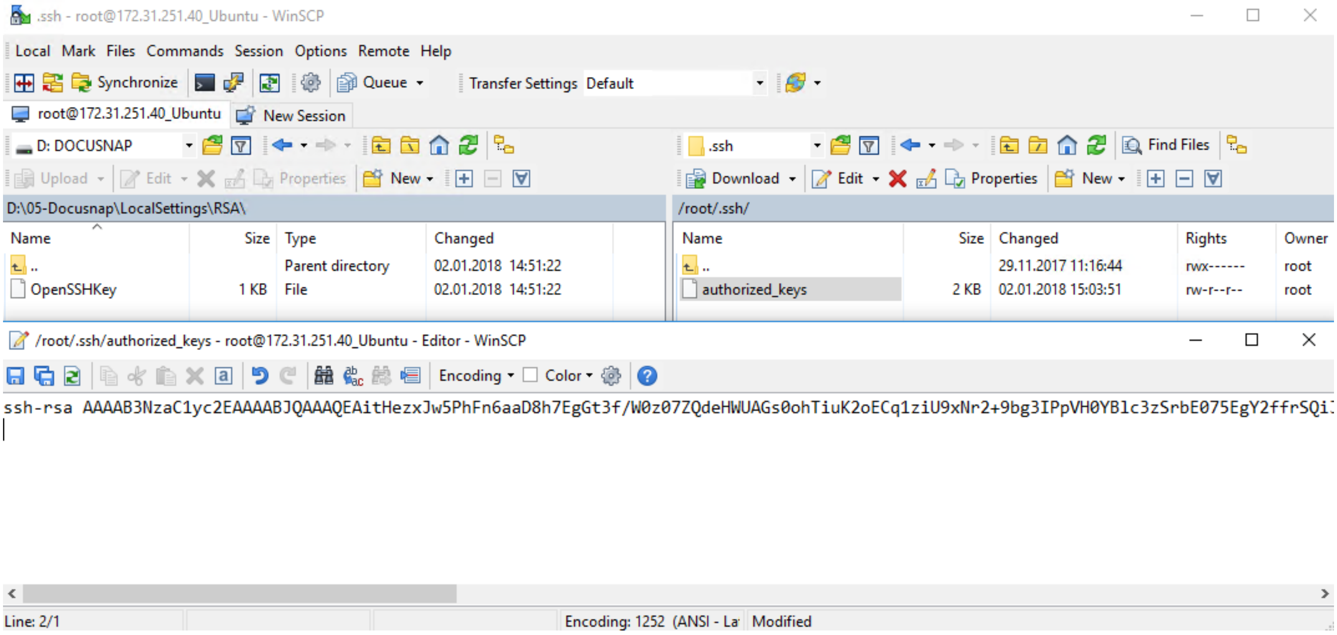
0 B of 0 B in 0 of 0

0 B of 0 B in 0 of 4

34 hidden

Fig. 2 - Connection to the Target System Established

Change to the directory .ssh and edit the file authorized_keys there.


.ssh - root@172.31.251.40_Ubuntu - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
root@172.31.251.40_Ubuntu
New Session
D: DOCUSNAP
.ssh
Find Files
Upload
Edit
Properties
New
Download
/root/.ssh/authorized_keys - root@172.31.251.40_Ubuntu - Editor - WinSCP
Encoding
Color

D:\05-Docusnap\LocalSettings\RSA\

Name	Size	Type	Changed
..		Parent directory	02.01.2018 14:51:22
OpenSSHKey	1 KB	File	02.01.2018 14:51:22

/root/.ssh/

Name	Size	Changed	Rights	Owner
..		29.11.2017 11:16:44	rwx------	root
authorized_keys	2 KB	02.01.2018 15:03:51	rw-r--r--	root

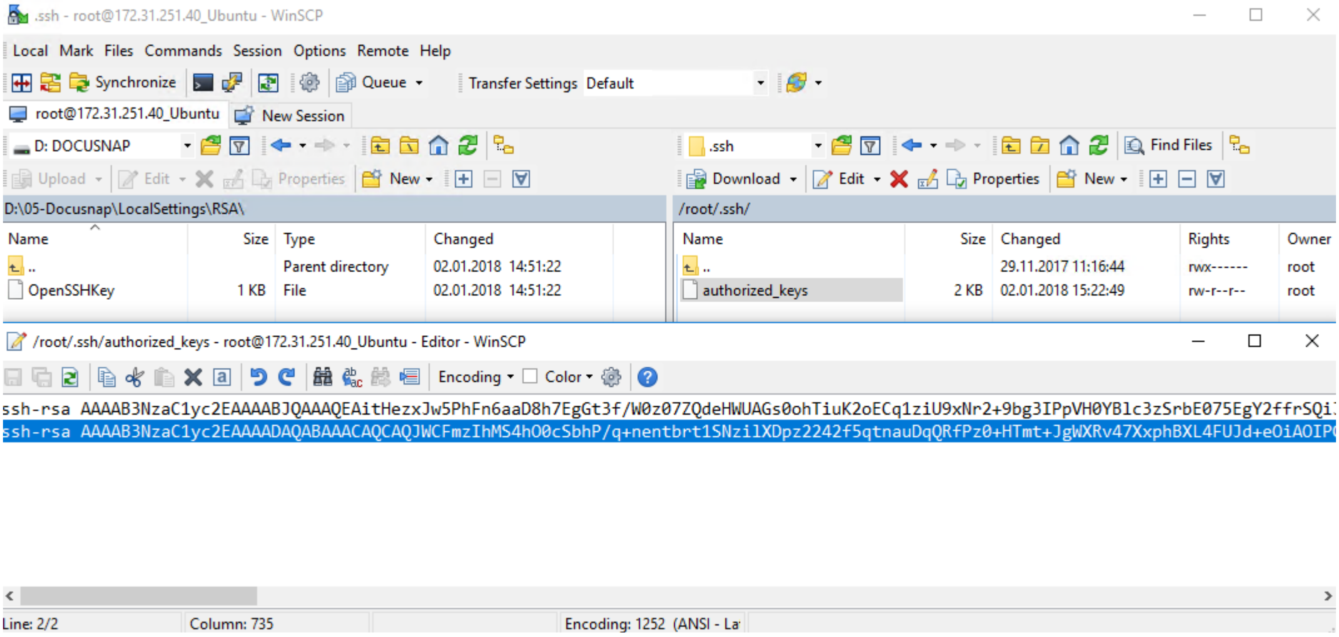
```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAitHezxJw5PhFn6aaD8h7EgGt3f/W0z07ZQdeHWUAGs0ohTiuK2oECq1ziU9xNr2+9bg3IPpVH0YBlc3zSrbE075EgY2ffrSQi
```

Line: 2/1 Encoding: 1252 (ANSI - La Modified

Fig. 3 - Editing the authorized_keys File

To store the previously created key, an export of the PublicKey from Docusnap is required. Open the Docusnap - Management - Inventory – Private Key Management and select the button Export PublicKey. Save the file. Open the file with a text editor and copy the PublicKey to the clipboard.

Switch back to WinSCP and insert the PublicKey in a new line. Save the file.


.ssh - root@172.31.251.40_Ubuntu - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
root@172.31.251.40_Ubuntu
New Session
D: DOCUSNAP
Upload
Edit
Properties
New
.ssh
Find Files
Download
Edit
Properties
New
/root/.ssh/authorized_keys - root@172.31.251.40_Ubuntu - Editor - WinSCP
Encoding
Color

D:\05-Docusnap\LocalSettings\RSA\

Name	Size	Type	Changed
..		Parent directory	02.01.2018 14:51:22
OpenSSHKey	1 KB	File	02.01.2018 14:51:22

/root/.ssh/

Name	Size	Changed	Rights	Owner
..		29.11.2017 11:16:44	rwx------	root
authorized_keys	2 KB	02.01.2018 15:22:49	rw-r--r--	root

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAitHezxJw5PhFn6aaD8h7EgGt3f/W0z07ZQdeHWUAGs0ohTiuK2oECq1ziU9xNr2+9bg3IPpVH0YBlc3zSrbE075EgY2ffrSQi
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCAQJWCFmzIhMS4hO0cSbhP/q+nentbrt1SNzilXDpz2242f5qtnauDqQRfPz0+HTmt+JgWXRv47XxphBXL4FUJd+eOiAOIP
```

Line: 2/2 Column: 735 Encoding: 1252 (ANSI - La

Fig. 4 - Store private key

The PublicKey is now stored on the target system. The inventory can now be carried out. You only need to specify the user name in the wizard.

2.4 USING THE PRIVATE KEY FOR THE INVENTORY

After the public key has been deposited on the Linux systems, the inventory can be carried out with it. Open the Linux Inventory Wizard.

- Discovery – All Wizards – Linux
- Inventar – All Wizards – Linux
- Alle Aufträge – All Wizards – Linux

In **step 3** you have the choice of which authentication you want to use.

You can select private keys for entire IP ranges and also for individual systems. The preselection from the IP ranges can be overwritten for individual systems.

If you do not use a private key, a password must be deposited. However, you can also use both authentication options - private key and password. Both variants are checked, the first one that is successful in the registration is used.

3. USE OF A SUDO USER

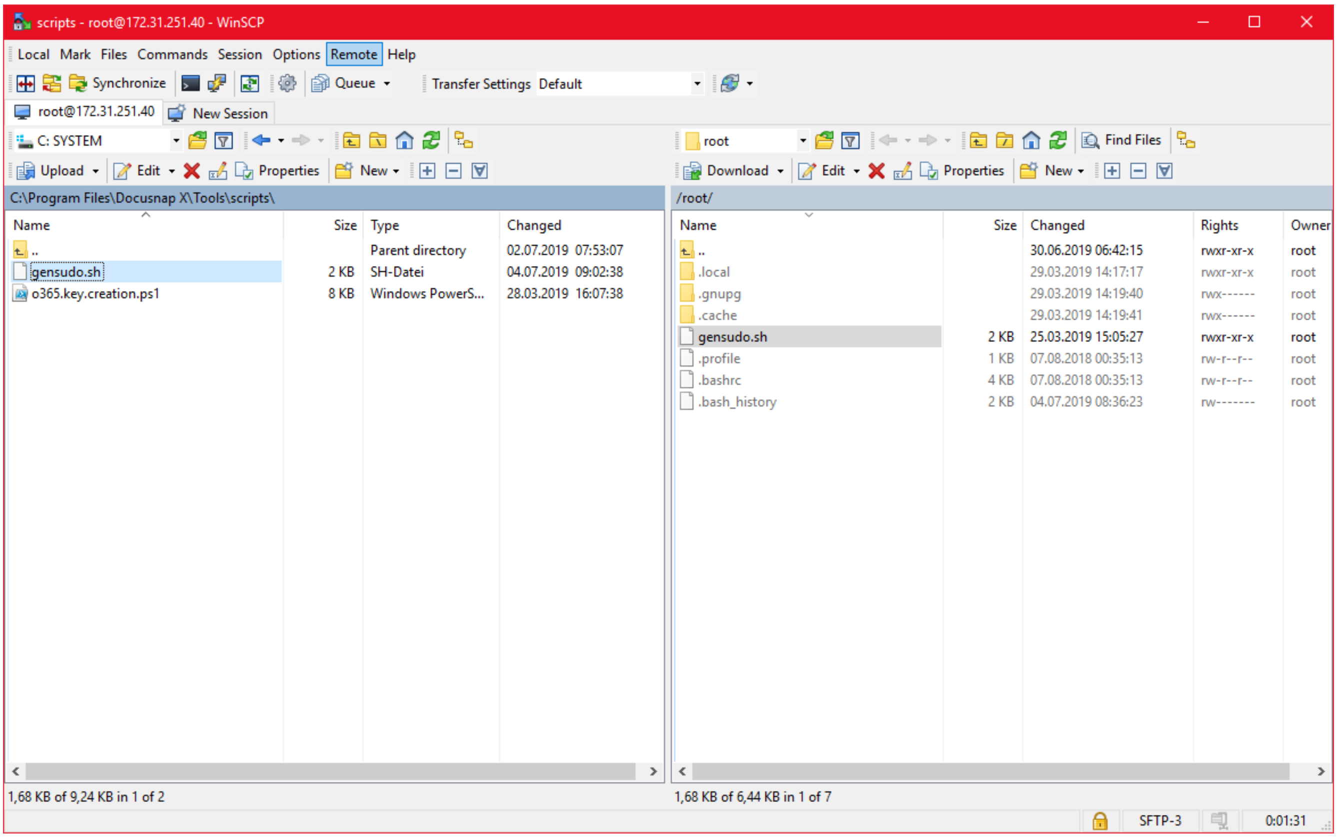
3.1 PERFORM SUDO CONFIGURATION

Before you can perform the Linux inventory with a user and the sudo command, you must perform a sudo configuration on the Linux systems - this is described below.

Please note that the possibly newly created user needs an assigned login shell. If this is not the case, the Linux inventory will be incomplete even if the SUDO configuration is correct. Therefore we recommend to create the user with the command **Adduser**. This way the login shell will be assigned automatically.

For the configuration you can use the Docusnap program directory - default path **C:\Program Files\Docusnap 13\Tools\scripts**. In this script you will find all commands to which the sudo user is authorized.

Copy the script to the Linux system. In this HowTo the software WinSCP was used.



C:\Program Files\Docusnap X\Tools\scripts\

Name	Size	Type	Changed
..		Parent directory	02.07.2019 07:53:07
gensudo.sh	2 KB	SH-Datei	04.07.2019 09:02:38
o365.key.creation.ps1	8 KB	Windows PowerS...	28.03.2019 16:07:38

1,68 KB of 9,24 KB in 1 of 2

/root/

Name	Size	Changed	Rights	Owner
..		30.06.2019 06:42:15	rwxr-xr-x	root
.local		29.03.2019 14:17:17	rwxr-xr-x	root
.gnupg		29.03.2019 14:19:40	rwx------	root
.cache		29.03.2019 14:19:41	rwx------	root
gensudo.sh	2 KB	25.03.2019 15:05:27	rwxr-xr-x	root
.profile	1 KB	07.08.2018 00:35:13	rw-r--r--	root
.bashrc	4 KB	07.08.2018 00:35:13	rw-r--r--	root
.bash_history	2 KB	04.07.2019 08:36:23	rw-------	root

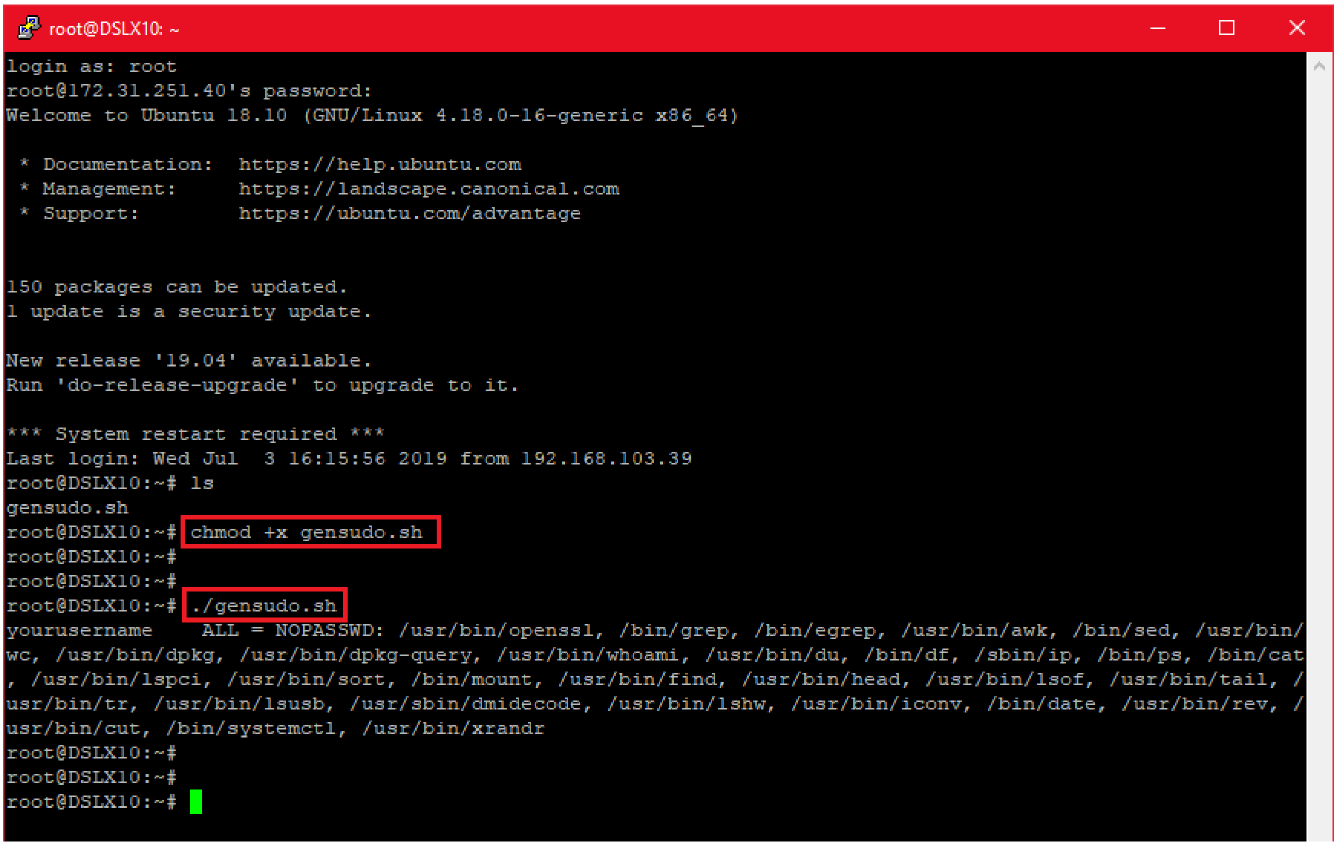
1,68 KB of 6,44 KB in 1 of 7

0:01:31

Fig. 5 - Copying the Script

Then connect e.g. with Putty to the console of the Linux system, edit the script to make it executable. Run it afterwards.

```
chmod +x Gensudo.sh
./gensudo.sh
```



```
login as: root
root@172.31.251.40's password:
Welcome to Ubuntu 18.10 (GNU/Linux 4.18.0-16-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


150 packages can be updated.
1 update is a security update.

New release '19.04' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Wed Jul  3 16:15:56 2019 from 192.168.103.39
root@DSLX10:~# ls
gensudo.sh
root@DSLX10:~# chmod +x gensudo.sh
root@DSLX10:~#
root@DSLX10:~#
root@DSLX10:~# ./gensudo.sh
yourusername    ALL = NOPASSWD: /usr/bin/openssl, /bin/grep, /bin/egrep, /usr/bin/awk, /bin/sed, /usr/bin/
wc, /usr/bin/dpkg, /usr/bin/dpkg-query, /usr/bin/whoami, /usr/bin/du, /bin/df, /sbin/ip, /bin/ps, /bin/cat
, /usr/bin/lspci, /usr/bin/sort, /bin/mount, /usr/bin/find, /usr/bin/head, /usr/bin/lsof, /usr/bin/tail, /
usr/bin/tr, /usr/bin/lsusb, /usr/sbin/dmidecode, /usr/bin/lshw, /usr/bin/iconv, /bin/date, /usr/bin/rev, /
usr/bin/cut, /bin/systemctl, /usr/bin/xrandr
root@DSLX10:~#
root@DSLX10:~#
root@DSLX10:~#
```

Fig. 6 - Making a Script Executable and Executing it

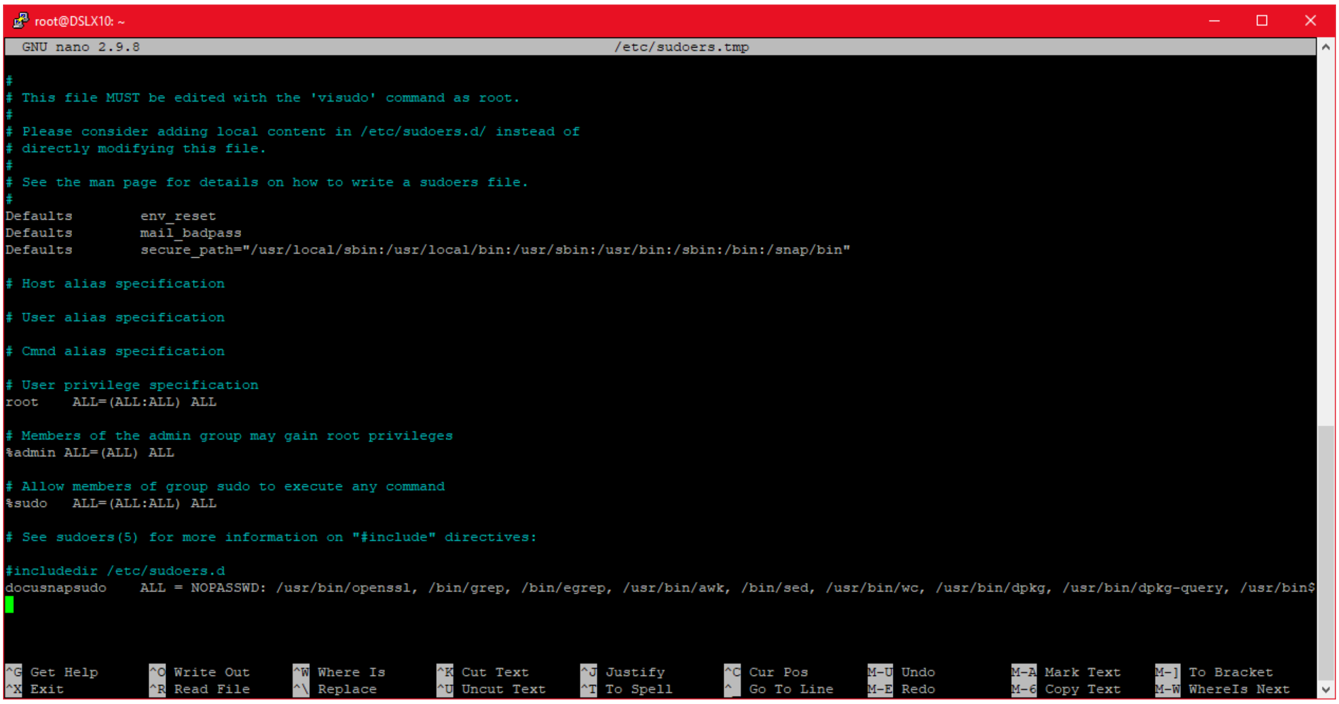
Copy the output and paste it into a text editor.

At the beginning of the output you have to change the following: Change YourUserName with the name of the sudo user. After completion of the configuration, the specified user has the permissions to execute the specified commands as root.

yourusername ALL = NOPASSWD: /usr/bin/openssl, /bin/grep, /bin/egrep, /usr/bin/awk, /bin/sed, /usr/bin/wc, /usr/bin/dpkg-query, /usr/bin/whoami, /usr/bin/du, /bin/df, /sbin/ip, /bin/ps, /bin/cat, /usr/bin/lspci, /usr/bin/sort, /bin/mount, /usr/bin/find, /usr/bin/bin/head, /usr/bin/lsof, /usr/bin/tail, /usr/bin/tr, /usr/bin/lsusb, /usr/sbin/dmidecode, /usr/bin/lshw, /usr/bin/iconv, /bin/date, /usr/bin/rev, /usr/bin/cut, /bin/systemctl, /usr/bin/xrandr

Please note that the previous version of the script was as of 07/04/2019. Changes could have taken place in the meantime.

Copy the custom output and switch back to Putty. Type visudo in Putty and go to the end of the file and paste the clipboard (right mouse button).

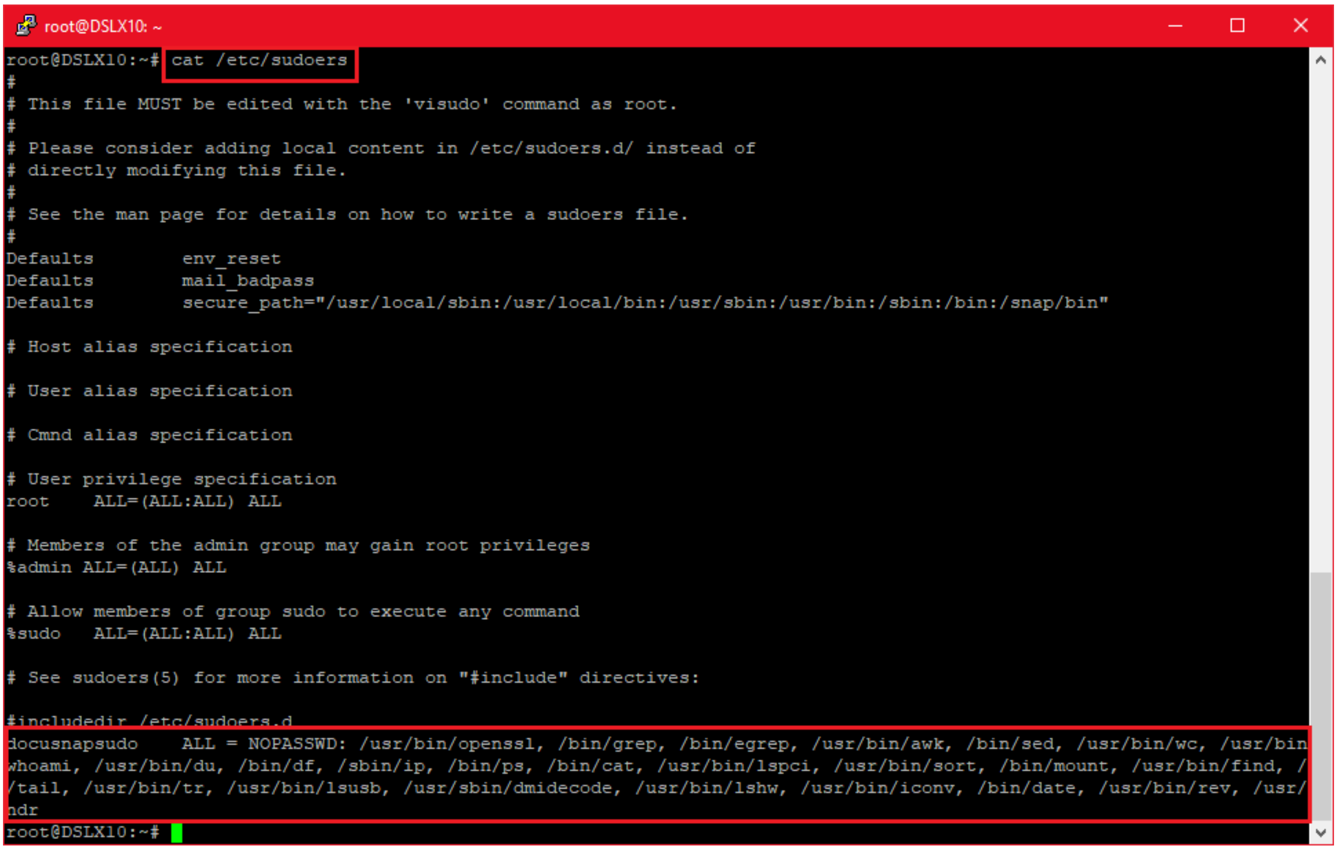


```
  GNU nano 2.9.8                                                  /etc/sudoers.tmp

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
docusnapsudo    ALL = NOPASSWD: /usr/bin/openssl, /bin/grep, /bin/egrep, /usr/bin/awk, /bin/sed, /usr/bin/wc, /usr/bin/dpkg, /usr/bin/dpkg-query, /usr/bin$



^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo        M-A Mark Text   M-] To Bracket
^X Exit         ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell     ^_ Go To Line   M-E Redo        M-6 Copy Text   M-W WhereIs Next
```

Fig. 7 - Inserted Script with Custom Username

Exit (Ctrl + X) and save (Y) the file with the existing filename (Enter).

You can use the cat /etc/sudoers command to check whether the changes have been applied.



```
root@DSLX10:~# cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
docusnapsudo    ALL = NOPASSWD: /usr/bin/openssl, /bin/grep, /bin/egrep, /usr/bin/awk, /bin/sed, /usr/bin/wc, /usr/bin
whoami, /usr/bin/du, /bin/df, /sbin/ip, /bin/ps, /bin/cat, /usr/bin/lspci, /usr/bin/sort, /bin/mount, /usr/bin/find, /
/tail, /usr/bin/tr, /usr/bin/lsusb, /usr/sbin/dmidecode, /usr/bin/lshw, /usr/bin/iconv, /bin/date, /usr/bin/rev, /usr/
ndr
root@DSLX10:~#
```

Fig. 8 - Reviewing the Change

3.2 ACTIVATE SUDO FOR INVENTORY

The inventory via the sudo user can then be activated in the Linux inventory wizard. Enter an IP address range, the user, his password and activate the option Use Sudo.

LIST OF FIGURES

VERSION HISTORY

date	description
January 11, 2018	Version 1.0 created
October 24, 2018	Changed Screenshots
April 24, 2020	Version 3.0 - Revision of the HowTo for Docusnap 11
January 5, 2023	Version 4.0 – Revision of the HowTo for Docusnap 12