



Inventory - Linux

Alternative authentication with RSA key or Sudo user

TITLE	Inventory - Linux
AUTHOR	Docusnap Consulting
DATE	7/8/2021
VERSION	3.0 valid from October 01, 2020

This document contains proprietary information. The reproduction and distribution of this document as a whole or in part as well as the utilization and disclosure of its contents to third parties without the express authorization by itelio GmbH are prohibited. Offenders will be held liable for the payment of indemnification. All rights reserved.

TABLE OF CONTENTS

1.	INTRODUCTION	4
2.	RSA KEY IN DOCUSNAP	5
2.1	CREATE AND USE RSA KEYS IN DOCUSNAP	5
2.2	IMPORT OF AN EXISTING RSA KEY	7
2.3	DEPOSIT RSA KEY ON LINUX SYSTEM	8
2.4	USING THE RSA KEY FOR THE INVENTORY	11
2.5	USE MIGRATED RSA KEYS FOR INVENTORY PURPOSES	12
3.	USE OF A SUDO USER	13
3.1	PERFORM SUDO CONFIGURATION	13
3.2	ACTIVATE SUDO FOR INVENTORY	16

1. INTRODUCTION

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

- Root
- Sudo
- RSA key

The alternatives for authentication (sudo and RSA 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 RSA keys and the necessary configuration to use a sudo user.

2. RSA KEY IN DOCUSNAP

2.1 CREATE AND USE RSA 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)

RSA keys can be created and managed in Docusnap administration. Navigate to the **Management - 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.

We do not recommend using an RSA key with the ssh-rsa key variant.

We recommend using an RSA key of the type SSH-Ed25519 (AES256-CBC).

If you want to increase security and additionally store a passphrase, you can create the RSA 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 RSA keys.

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

You can repeat the above steps as often as you like, for example to create RSA 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](#).

Docusnap 11 - Management (Configuring, Customizing and Extending of Docusnap)

General

Inventory

Customizing

IT Assets

Diagrams

IT Correlations

License Management

Connect Legacy

Options

Close Management

Inventory

SNMP

Software Search

Server Roles

Additional Tools

Active Directory

Assignment Criteria

AWS Regions

Azure Apps

Private Key Management

Private Key

Name: itelio GmbH

Private Key: Import Private Key RSA Key: Create RSA Key Export Public Key

Key Preview: ssh-rsa AAAAB3NzaC1y...Jz0d2H9lw== docusnap

New Delete Save

As the most secure variant, we recommend creating a private key of type SSH-Ed25519 / AES256-CBC and importing it into Docusnap.

The following key variants are still supported for compatibility reasons:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-rsa

Name	Key Preview
Docusnap GmbH	ssh-rsa AAAAB3NzaC1y...72kS84s8w== docusnap
itelio GmbH	ssh-rsa AAAAB3NzaC1y...Jz0d2H9lw== docusnap

Fig. 1 - Navigation Docusnap Management - RSA Key

2.2 IMPORT OF AN EXISTING RSA KEY

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

Navigate to the Docusnap - Management - Inventory - Private Key Management and select the New button.

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

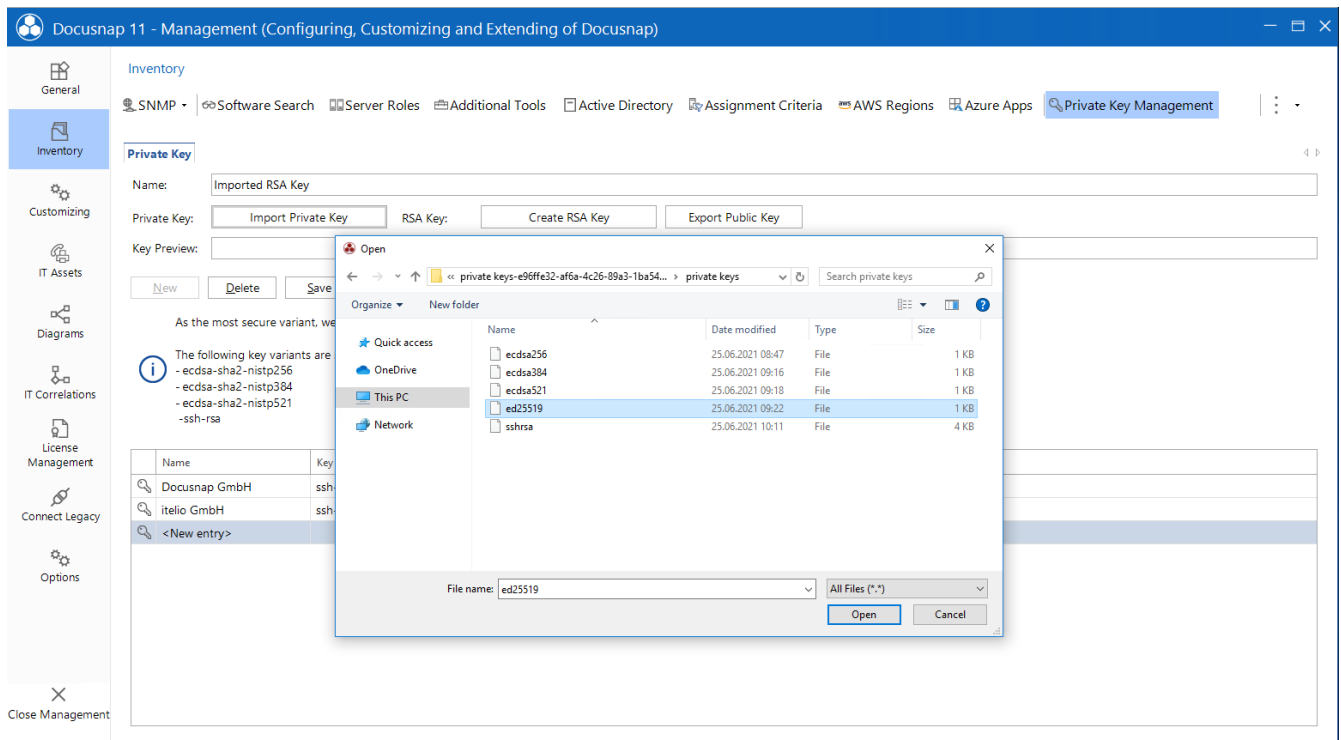


Fig. 2 - Importing RSA Keys

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

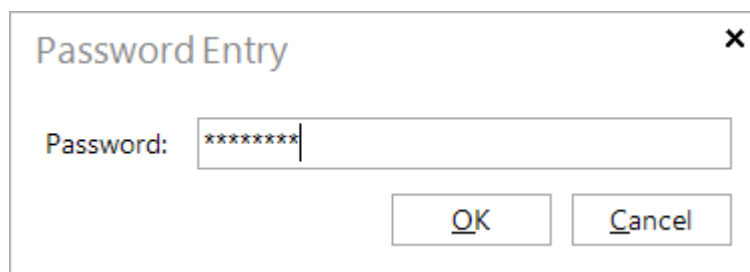


Fig. 3 - Entering a Passphrase

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 RSA 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.

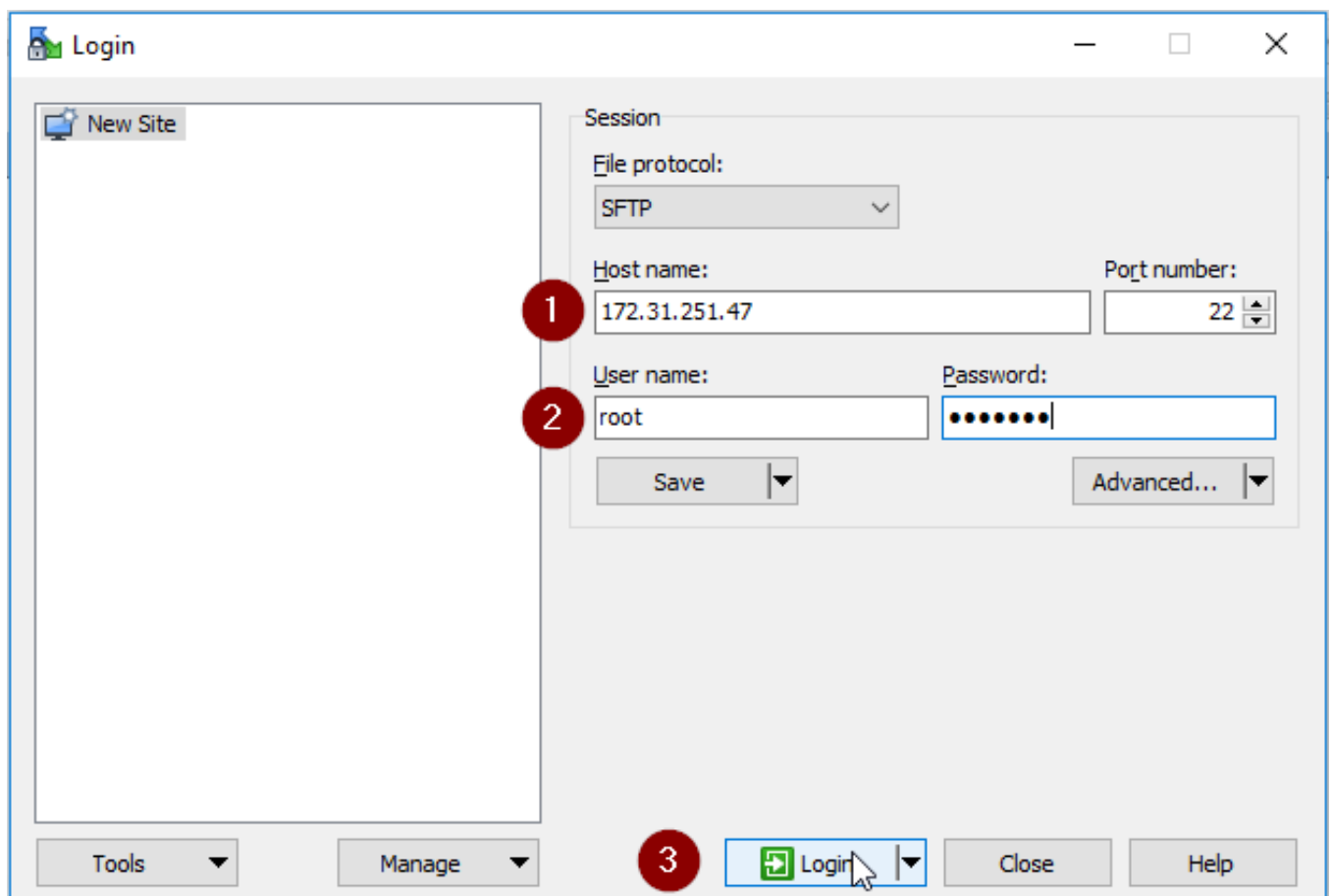


Fig. 4 - Establishing a WinSCP Connection

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.

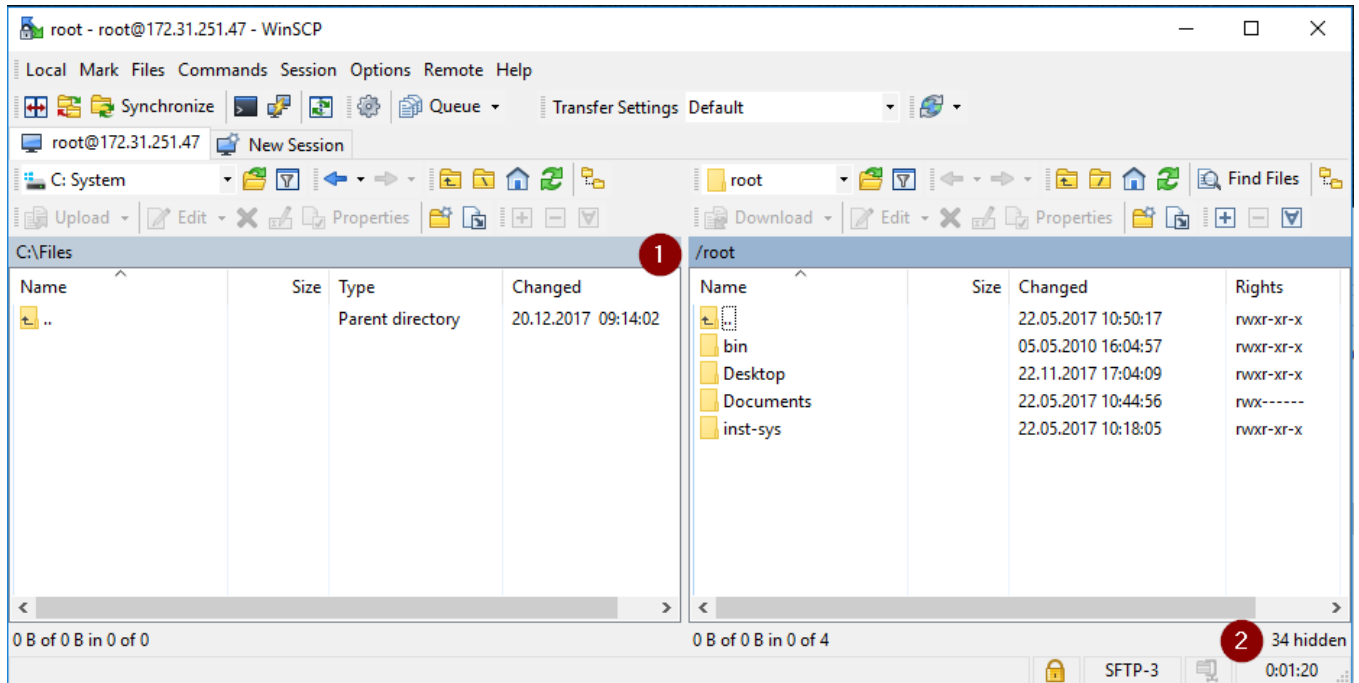


Fig. 5 - Connection to the Target System Established

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

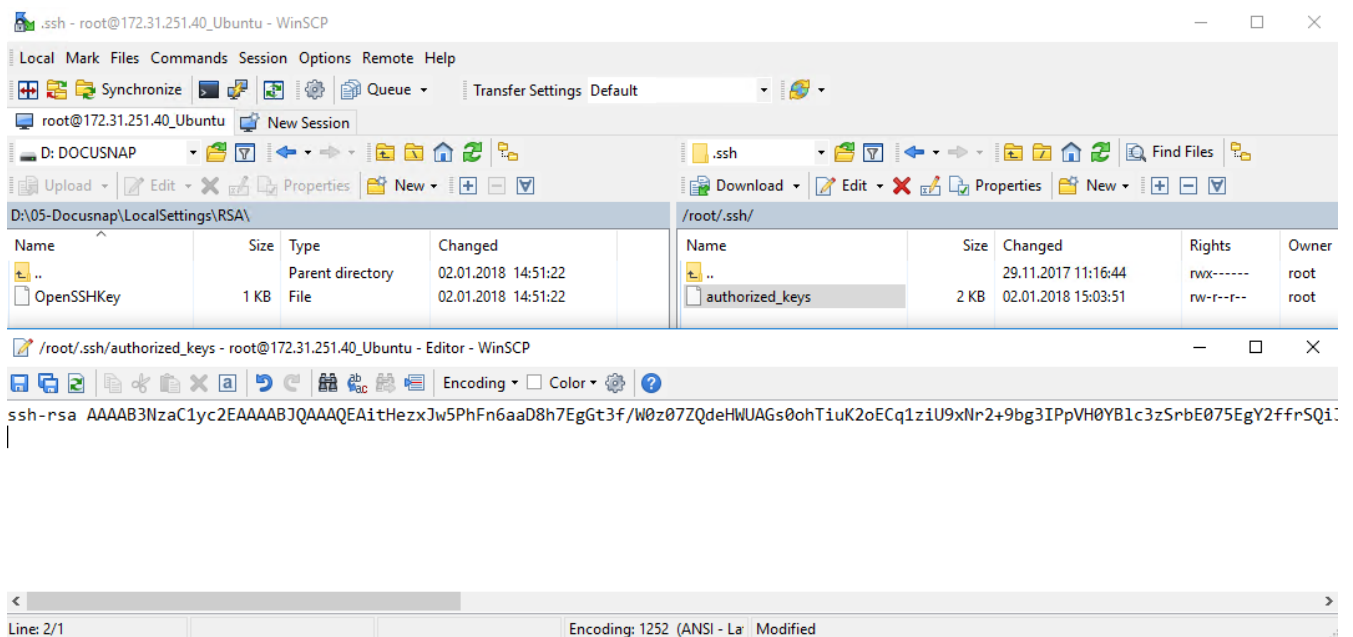


Fig. 6 - Editing the `authorized_keys` File

To store the previously created RSA key, an export of the PublicKey from Docusnap is required. Open the Docusnap - Management - Inventory - RSA Key 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.

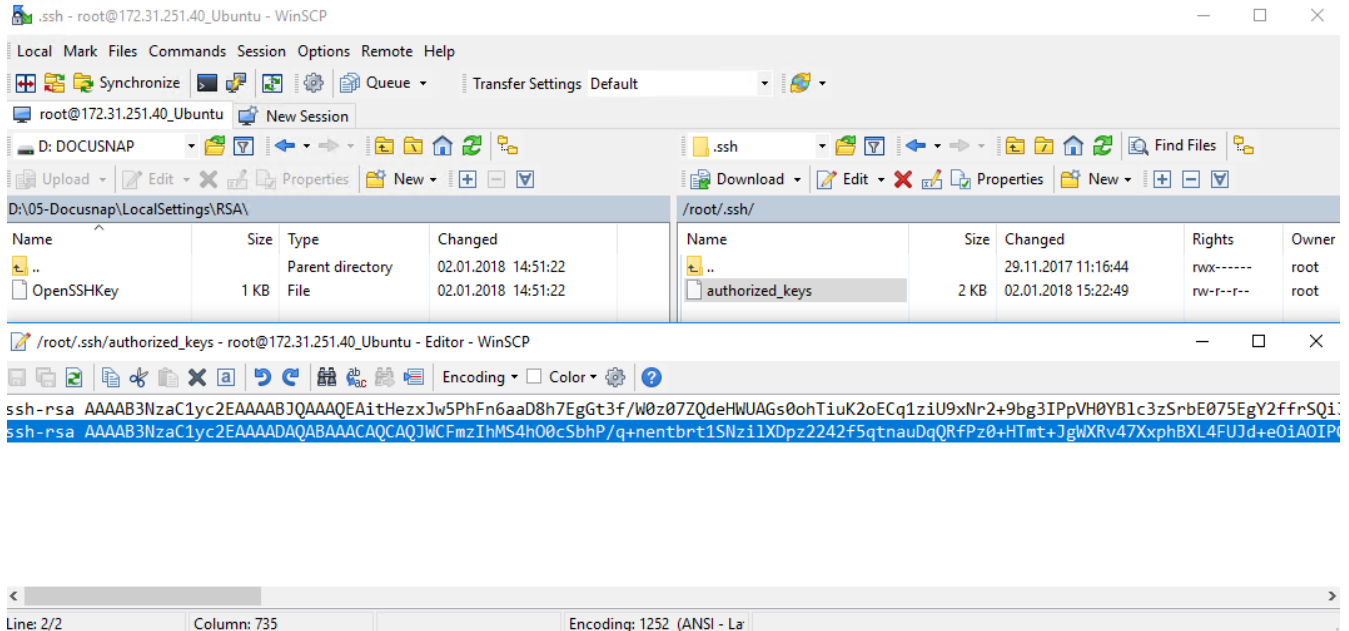


Fig. 7 - Store RSA Key

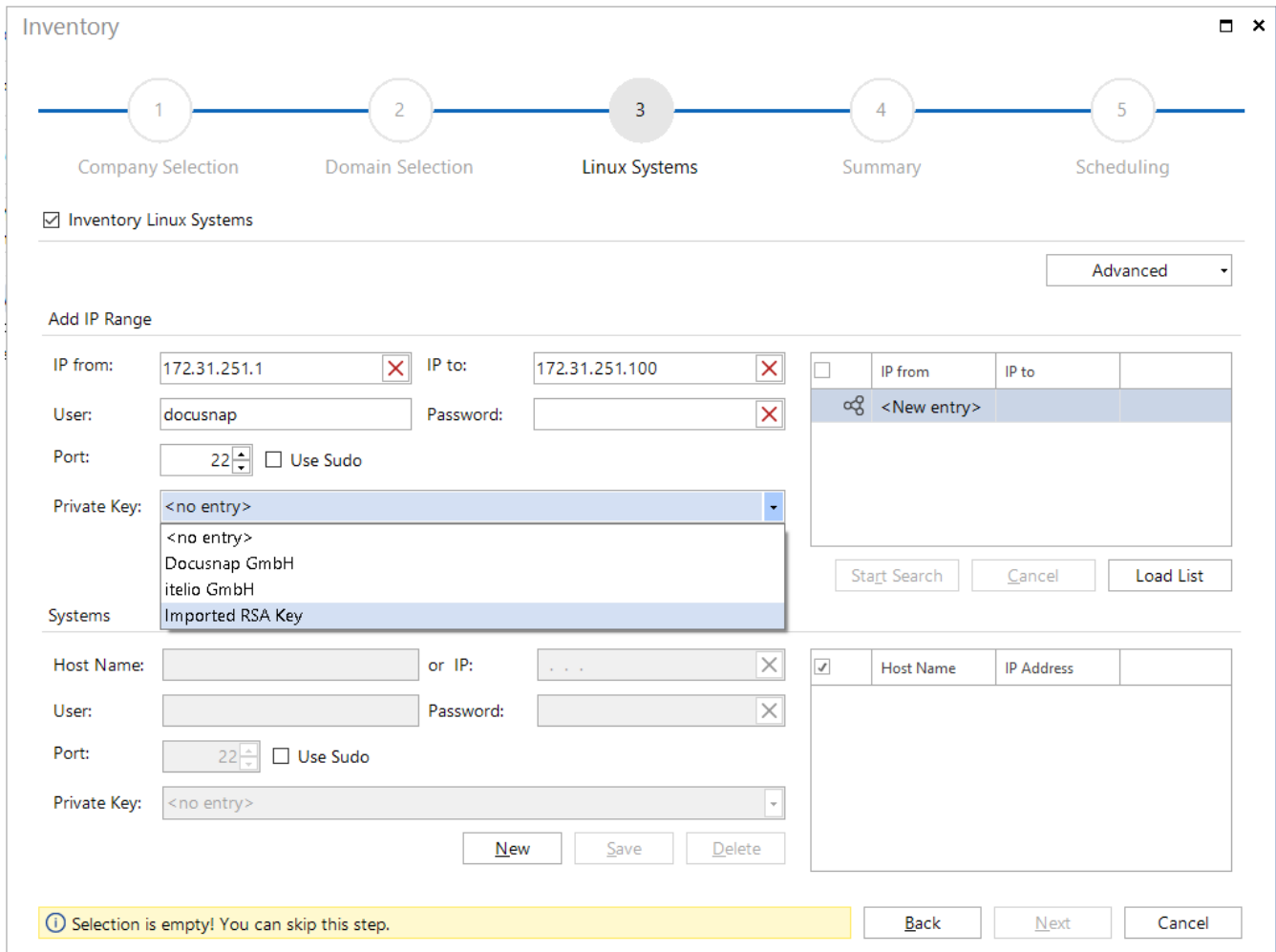
The PublicKey is now stored on the target system. The inventory can now be carried out. You only need to specify the user name in the wizard.

2.4 USING THE RSA 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. In step 3 you have the choice of which authentication you want to use.

You can select RSA 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 an RSA key, a password must be deposited. However, you can also use both authentication options - RSA key and password. Both variants are checked, the first one that is successful in the registration is used.



Inventory

1 Company Selection 2 Domain Selection 3 Linux Systems 4 Summary 5 Scheduling

☒ Inventory Linux Systems

Advanced

Add IP Range

IP from: 172.31.251.1 IP to: 172.31.251.100

User: docusnap Password:

Port: 22 ☐ Use Sudo

Private Key: <no entry>

Systems

Host Name: or IP: . . .

User: Password:

Port: 22 ☐ Use Sudo

Private Key: <no entry>

New Save Delete

Selection is empty! You can skip this step.

Back Next Cancel

Fig. 8 - Selection of the RSA Key

2.5 USE MIGRATED RSA KEYS FOR INVENTORY PURPOSES

If you have already used an RSA key in versions prior to July 2019, it was migrated automatically. The migrated key is also automatically used for scheduled Linux inventories - so you don't have to make any adjustments!

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 X\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.

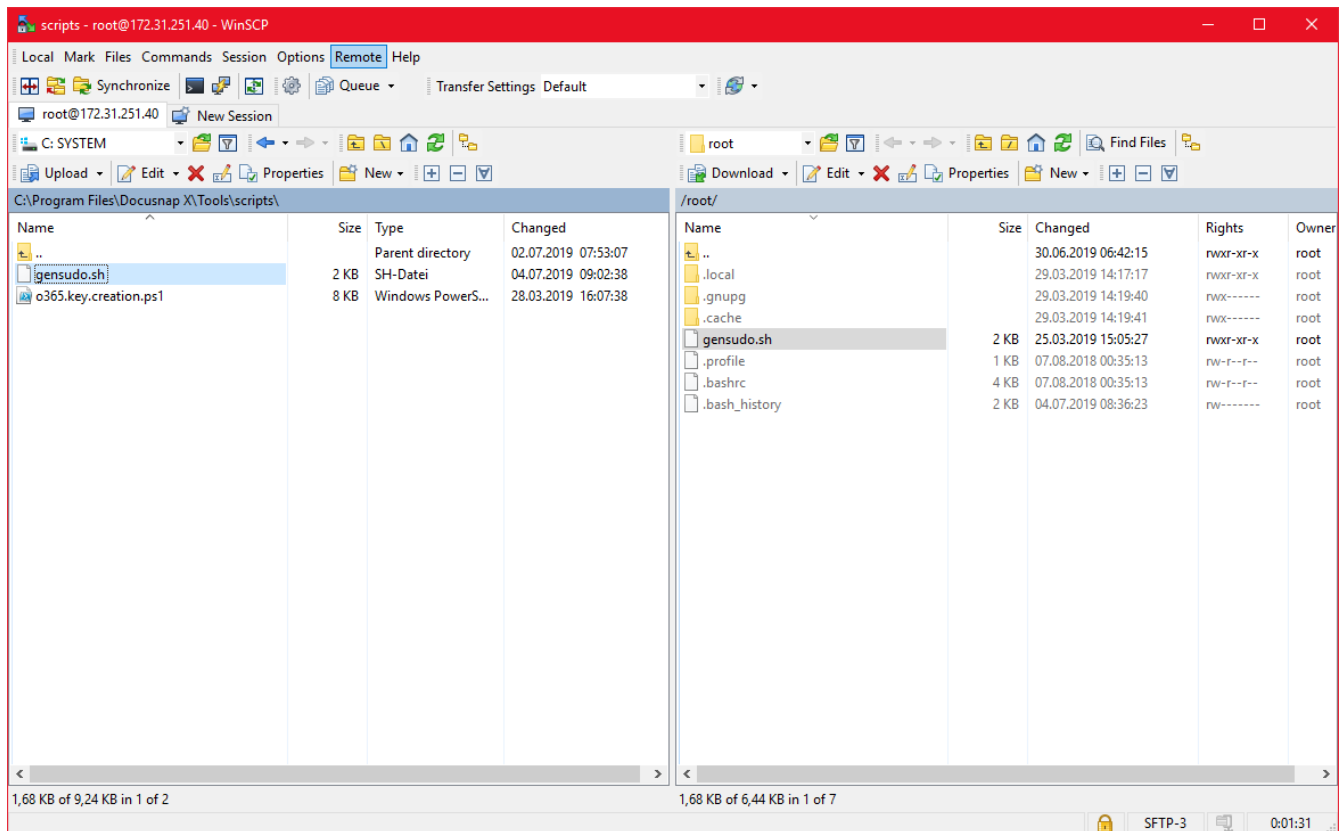
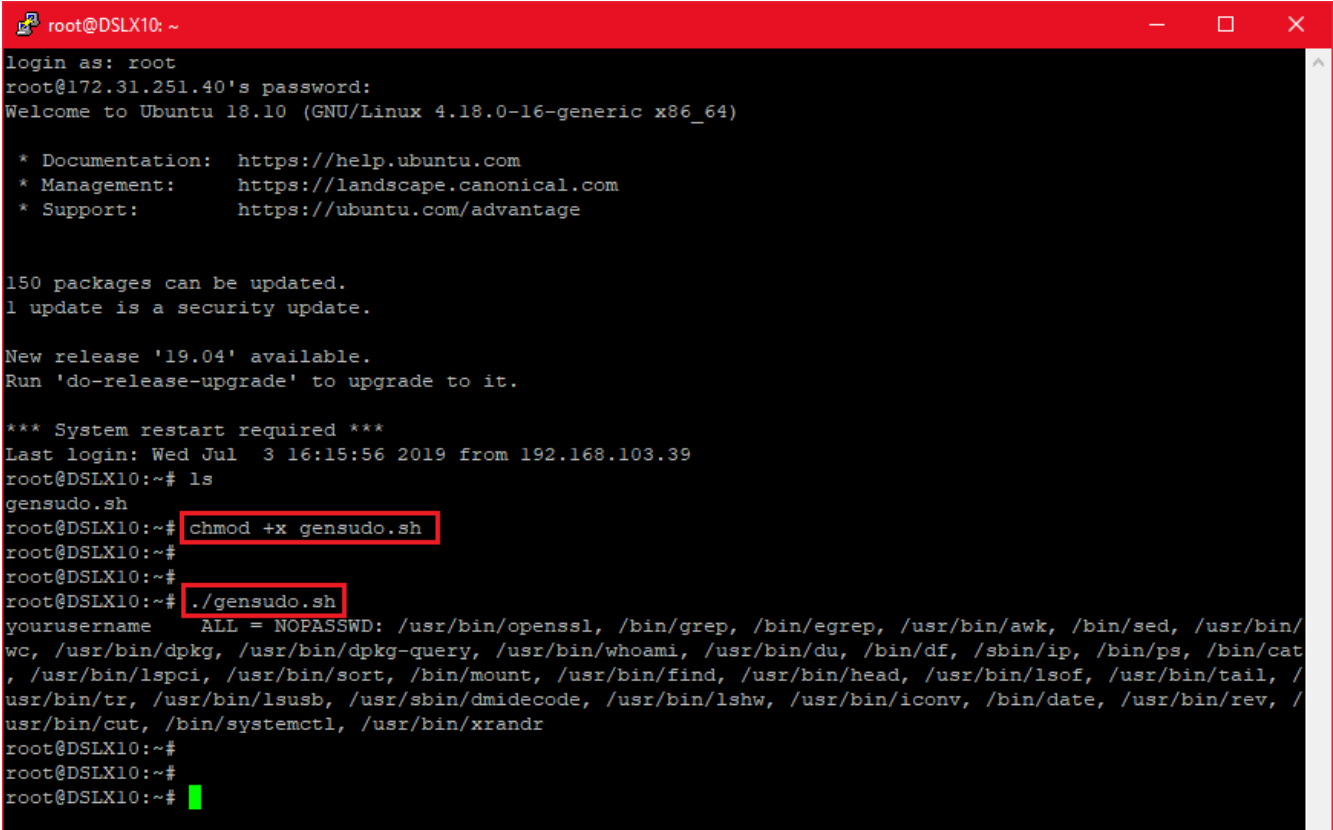


Fig. 9 - Copying the Script

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
```



```
root@DSLX10: ~
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/lshw, /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. 10 - Making a Script Executable and Executing it

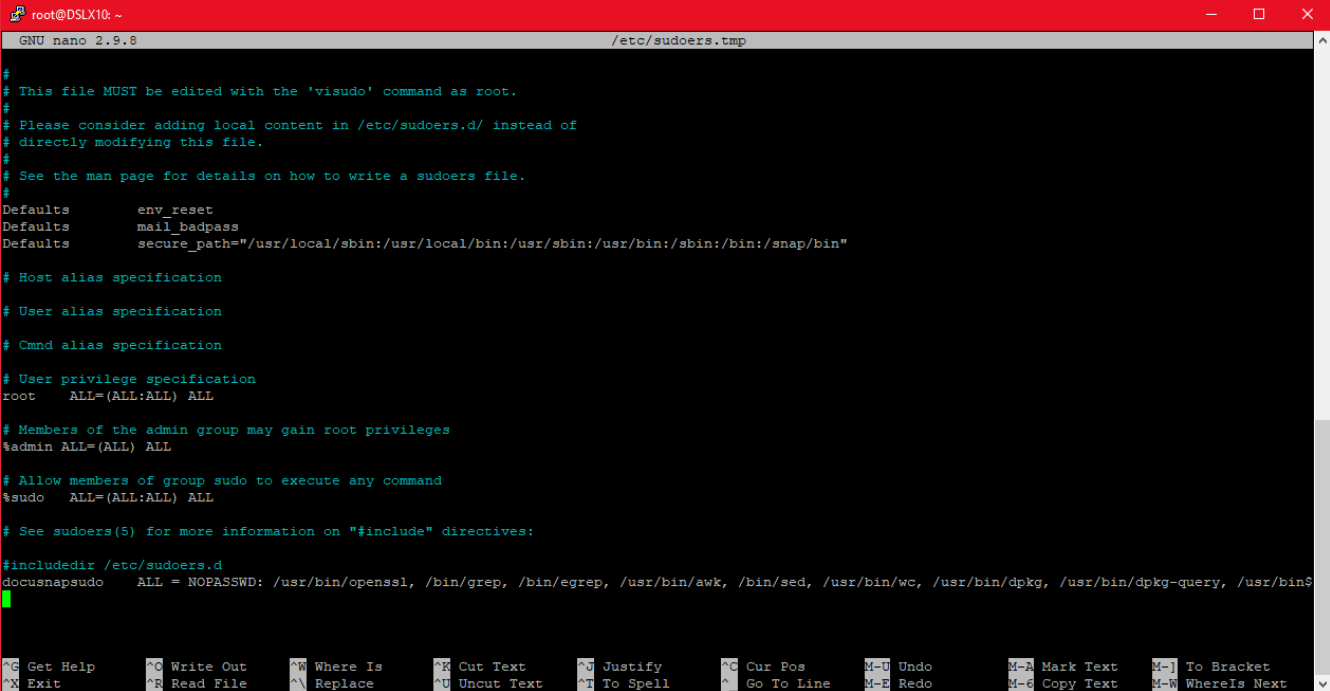
Copy the output and paste it into a text editor.

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/head, /usr/bin/lsof, /usr/bin/tail,
/usr/bin/tr, /usr/bin/lshw, /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).



```

root@DSLX10: ~
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:

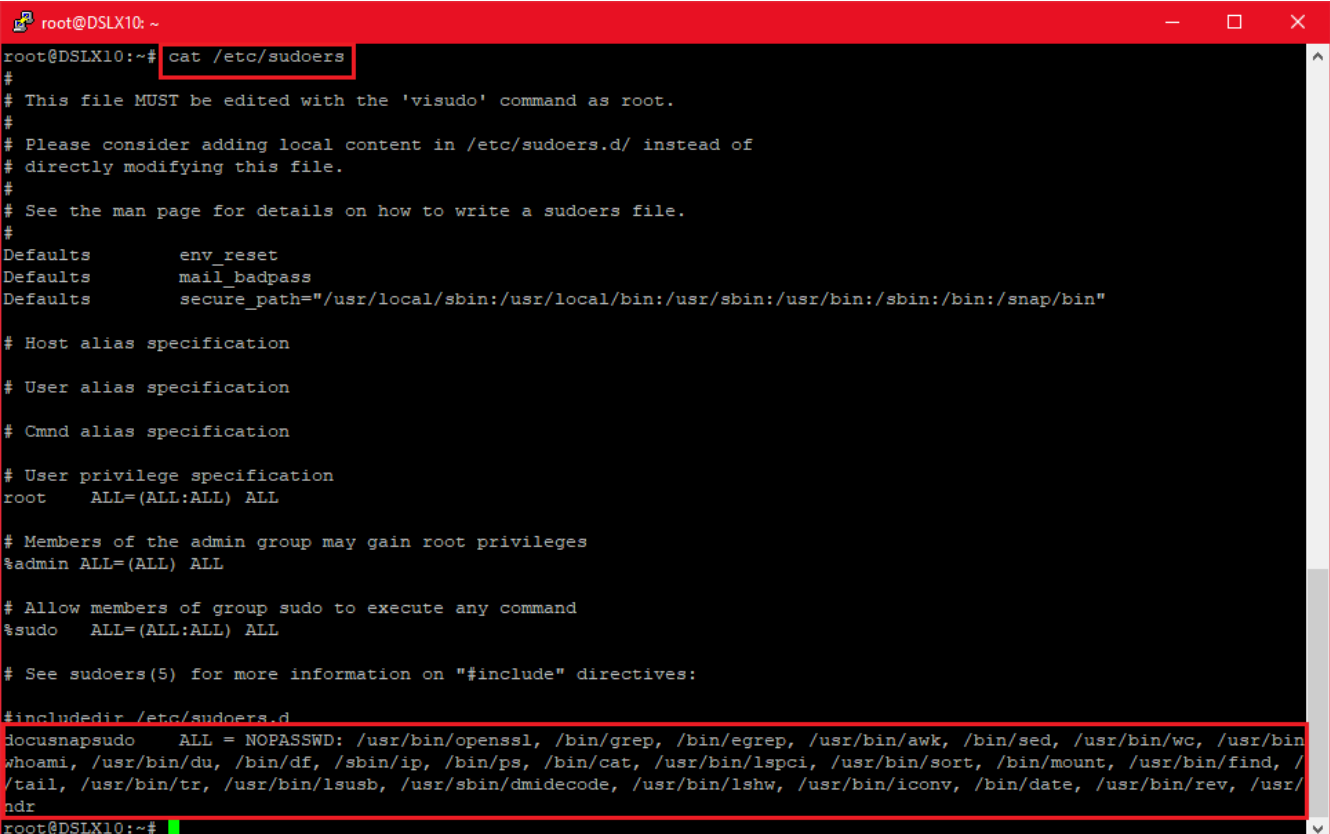
#include_dir /etc/sudoers.d
docusnapsudo    ALL = NOPASSWD: /usr/bin/openssl, /bin/grep, /bin/egrep, /usr/bin/awk, /bin/sed, /usr/bin/wc, /usr/bin/dpkg, /usr/bin/dpkg-query, /usr/bin/

```

Fig. 11 - 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: ~
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"

# 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:

#include_dir /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/lscusb, /usr/sbin/dmidecode, /usr/bin/lshw, /usr/bin/iconv, /bin/date, /usr/bin/rev, /usr/
ndr
root@DSLX10:~#

```

Fig. 12 - 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.

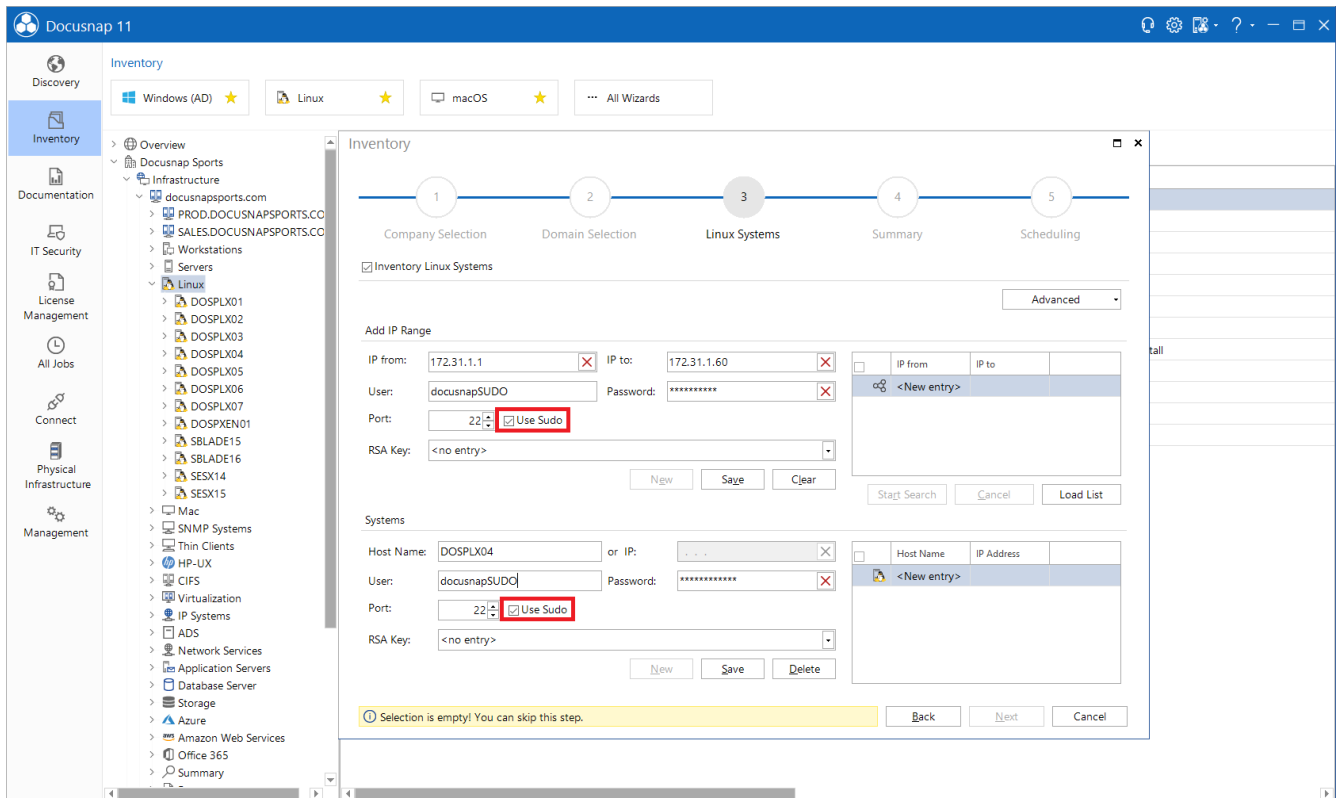


Fig. 13 - Activating sudo

LIST OF FIGURES

FIG. 1 - NAVIGATION DOCUSNAP MANAGEMENT - RSA KEY	6
FIG. 2 - IMPORTING RSA KEYS.....	7
FIG. 3 - ENTERING A PASSPHRASE	7
FIG. 4 - ESTABLISHING A WINSCP CONNECTION.....	8
FIG. 5 - CONNECTION TO THE TARGET SYSTEM ESTABLISHED.....	9
FIG. 6 - EDITING THE AUTHORIZED_KEYS FILE	9
FIG. 7 - STORE RSA KEY	10
FIG. 8 - SELECTION OF THE RSA KEY	11
FIG. 9 - COPYING THE SCRIPT	13
FIG. 10 - MAKING A SCRIPT EXECUTABLE AND EXECUTING IT	14
FIG. 11 - INSERTED SCRIPT WITH CUSTOM USERNAME.....	15
FIG. 12 - REVIEWING THE CHANGE.....	15
FIG. 13 - ACTIVATING SUDO	16

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 HowTos for Docusnap 11



Docusnap[®]

-=www.docusnap.com/support=- proudly presents
© itelio GmbH - www.itelio.com