



Inventarisierung - Linux

Alternative Authentifizierung mit RSA Key oder Sudo User

TITEL Inventarisierung - Linux
AUTOR Docusnap Consulting
DATUM 08.07.2021
VERSION 3.0 | gültig ab 01.10.2020

Die Weitergabe, sowie Vervielfältigung dieser Unterlage, auch von Teilen, Verwertung und Mitteilung ihres Inhaltes ist nicht gestattet, soweit nicht ausdrücklich durch die itelio GmbH zugestanden. Zuwiderhandlung verpflichtet zu Schadenersatz. Alle Rechte vorbehalten.

This document contains proprietary information and may not be reproduced in any form or parts whatsoever, nor may be used by or its contents divulged to third parties without written permission of itelio GmbH. All rights reserved.

INHALTSVERZEICHNIS

1.	EINLEITUNG	4
2.	RSA SCHLÜSSEL IN DOCUSNAP	5
2.1	RSA SCHLÜSSEL IN DOCUSNAP ERSTELLEN UND NUTZEN	5
2.2	IMPORT EINES VORHANDENEN RSA SCHLÜSSELS	7
2.3	RSA SCHLÜSSEL AUF DEM LINUX SYSTEM HINTERLEGEN	8
2.4	RSA SCHLÜSSEL FÜR DIE INVENTARISIERUNG VERWENDEN	11
2.5	MIGRIERTE RSA SCHLÜSSEL FÜR DIE INVENTARISIERUNG NUTZEN	12
3.	VERWENDUNG EINES SUDO USERS	13
3.1	SUDO KONFIGURATION DURCHFÜHREN	13
3.2	SUDO FÜR DIE INVENTARISIERUNG AKTIVIEREN	16

1. EINLEITUNG

Für die Inventarisierung von Linux Systemen stehen in Docusnap drei verschiedene Varianten bezüglich der Authentifizierung zur Verfügung:

- Root
- Sudo
- RSA-Schlüssel

Die alternativen für die Authentifizierung (sudo und RSA-Schlüssel) an den zu inventarisierenden Linux Systemen sind hilfreich, sollte Ihnen der root-User nicht zur Verfügung stehen oder der Zugriff mittels root-User über SSH gesperrt sein.

Weiterhin steht Ihnen noch die die skriptbasierte Inventarisierung für Linux Systeme zur Verfügung. Weiterführende Informationen befinden sich in dem dafür bereitgestellte HowTo: Docusnap Script Linux.

Dieses HowTo beschreibt die Nutzung eines oder mehrerer RSA Schlüssel sowie die notwendige Konfiguration zur Nutzung eines sudo Users.

2. RSA SCHLÜSSEL IN DOCUSNAP

2.1 RSA SCHLÜSSEL IN DOCUSNAP ERSTELLEN UND NUTZEN

Docusnap bietet Ihnen die Möglichkeit, RSA Schlüssel, im OpenSSH-Format, für die Linux Inventarisierung zu erstellen oder zu importieren. Hierfür können die folgenden Verschlüsselungsalgorithmen verwendet werden:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519
- ssh-rsa (kann von Docusnap erstellt werden)

RSA Schlüssel können in der Docusnap Administration erstellt und verwaltet werden. Navigieren Sie hierfür in die **Administration – Inventar - Private Key Management**.

Über die Schaltfläche **Neu** können Sie einen RSA Schlüssel erstellen. Geben Sie hierfür einen **Namen** ein und wählen Sie daraufhin **RSA Key erstellen**. Das Schlüsselpaar wird mit der `ssh-rsa` Methode verschlüsselt. Der verwendete Key wird anschließend nochmals verschlüsselt und in der Datenbank abgelegt. Eine Passphrase wird nicht erstellt.

Wir empfehlen nicht die Nutzung eines RSA-Schlüssels mit der Schlüsselvariante `ssh-rsa`.

Wir empfehlen die Nutzung eines RSA-Schlüssels des Typen `SSH-Ed25519 (AES256-CBC)`.

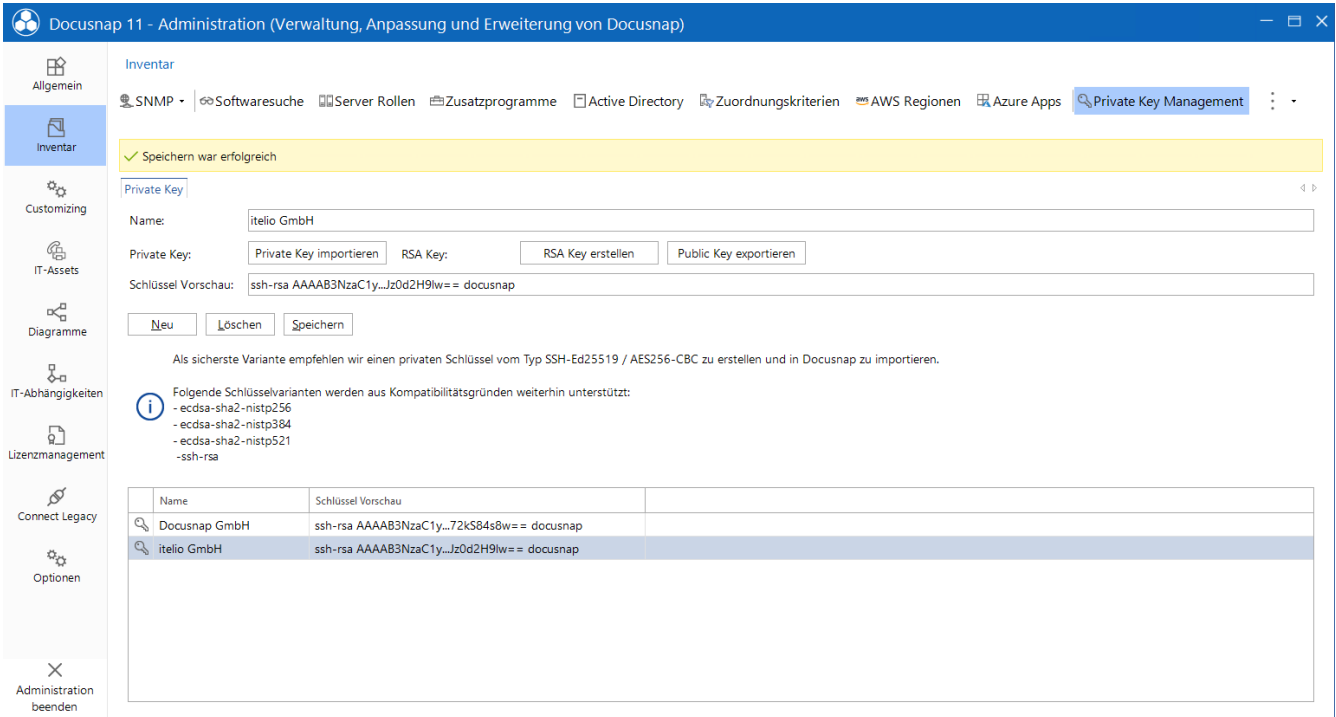
Möchten Sie die Sicherheit erhöhen und zusätzlich eine Passphrase oder einen aktuelleren Verschlüsselungsalgorithmus hinterlegen, können Sie den RSA Schlüssel mit einem Drittprodukt (z. B. PuTTY Key Gen oder `ssh-keygen`) erstellen.

Wenn die Erstellung abgeschlossen ist, können Sie dem Schlüssel eine Vorschau entnehmen – dies dient bei der Nutzung unterschiedlicher RSA Schlüssel zur besseren Identifizierung.

Nun wählen Sie **Speichern** und der RSA Schlüssel wurde erfolgreich angelegt.

Die zuvor genannten Schritte können Sie nach Belieben wiederholen, um beispielsweise RSA Schlüssel für die verschiedenen Mandanten in Ihrer Docusnap Umgebung zu erstellen und anschließend zu nutzen.

Über die Schaltfläche **PublicKey Exportieren** können Sie den öffentlichen Schlüssel exportieren und auf den Linux Systemen hinterlegen – siehe [Kapitel 2.3](#).



The screenshot shows the 'Private Key Management' section in the Docusnap Administration interface. A yellow banner at the top indicates 'Speichern war erfolgreich' (Save was successful). The form includes a 'Name' field with 'itelio GmbH', a 'Private Key' field with a preview of an RSA key, and buttons for 'Private Key importieren', 'RSA Key', 'RSA Key erstellen', and 'Public Key exportieren'. A table below lists existing keys for 'Docusnap GmbH' and 'itelio GmbH'. An information icon provides a note about key compatibility.

Private Key Management

✓ Speichern war erfolgreich

Private Key

Name: itelio GmbH

Private Key: Private Key importieren RSA Key: RSA Key erstellen Public Key exportieren

Schlüssel Vorschau: ssh-rsa AAAAB3NzaC1y...JzOd2H9lw== docusnap

Neu Löschen Speichern

Als sicherste Variante empfehlen wir einen privaten Schlüssel vom Typ SSH-Ed25519 / AES256-CBC zu erstellen und in Docusnap zu importieren.

i Folgende Schlüsselvarianten werden aus Kompatibilitätsgründen weiterhin unterstützt:

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

Name	Schlüssel Vorschau
Docusnap GmbH	ssh-rsa AAAAB3NzaC1y...72kS84s8w== docusnap
itelio GmbH	ssh-rsa AAAAB3NzaC1y...JzOd2H9lw== docusnap

Abbildung 1 - Navigation Docusnap Administration - RSA Schlüssel

2.2 IMPORT EINES VORHANDENEN RSA SCHLÜSSELS

Ein vorhandener RSA Schlüssel kann wie folgt nach DocuSnap importiert werden.

Navigieren Sie in die **Administration – Inventar – Private Key Management** und wählen Sie die Schaltfläche **Neu**.

Im nächsten Schritt vergeben Sie einen Namen für den Schlüssel und wählen die Schaltfläche **Private Key Importieren** – wählen Sie Ihren vorhandenen RSA Schlüssel aus.

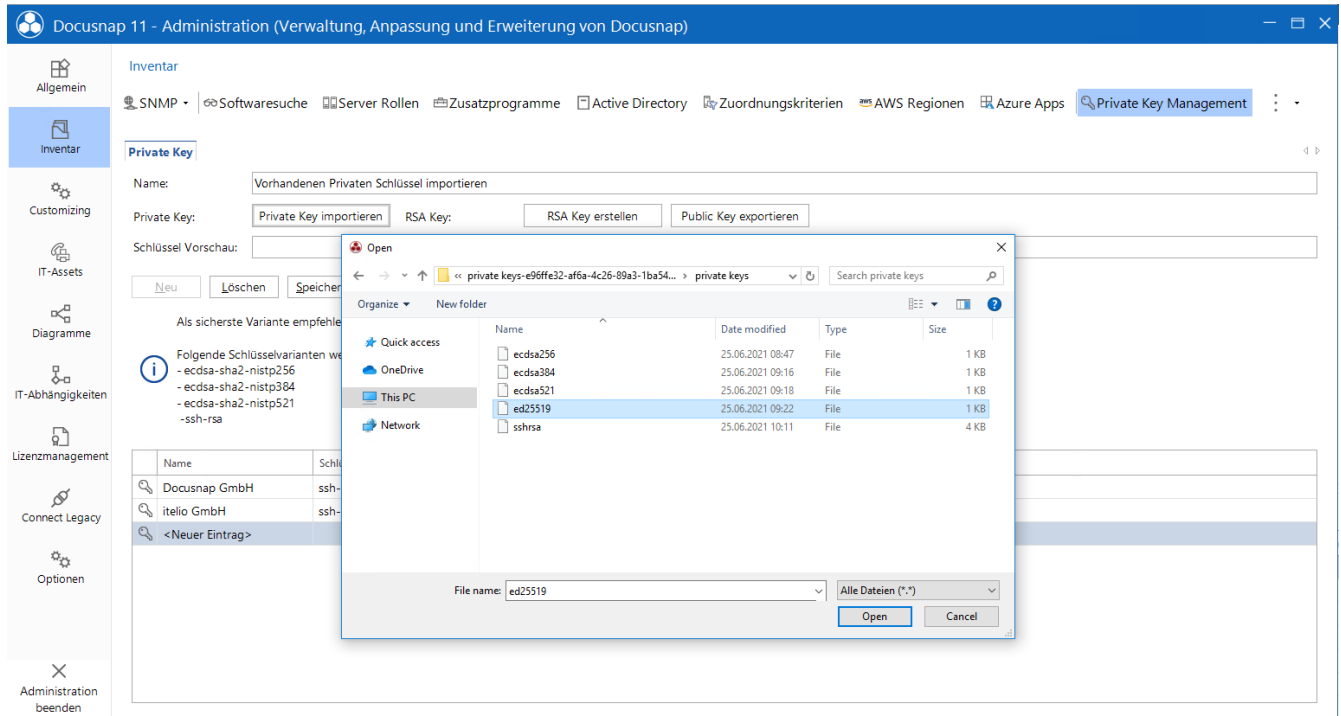


Abbildung 2 - RSA Schlüssel importieren

Wenn eine Passphrase für den Schlüssel verwendet wird, werden Sie nach dieser gefragt. Im Anschluss ist der Schlüssel in DocuSnap hinterlegt.

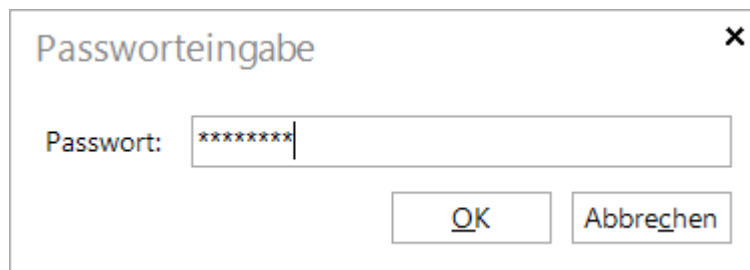


Abbildung 3 - Passphrase eingeben

Über die Schaltfläche **PublicKey Exportieren** können Sie den öffentlichen Schlüssel exportieren und auf den Linux Systemen hinterlegen – siehe [Kapitel 2.3](#).

2.3 RSA SCHLÜSSEL AUF DEM LINUX SYSTEM HINTERLEGEN

Die beschriebenen Schritte könnten sich ggf. unter den Linux Distributionen unterscheiden. Bitte informieren Sie sich vorab, in welchem Verzeichnis und welcher Datei der öffentliche Schlüssel für die besagte Distribution einzutragen ist. Das folgende Anwendungsbeispiel wird auf einem Ubuntu System (16.04.2 64-bit) durchgeführt.

In diesem HowTo wird die Software WinSCP verwendet, damit der öffentliche Schlüssel auf dem Linux System hinterlegt wird.

Öffnen Sie WinSCP und bauen die Verbindung zu dem Linux System auf.

Falls der Server beim Client noch nicht bekannt ist, wird eine Sicherheitsmeldung angezeigt. Klicken Sie auf „Yes“ um den Hostschlüssel in die Liste der vertrauenswürdigen Rechner aufzunehmen.

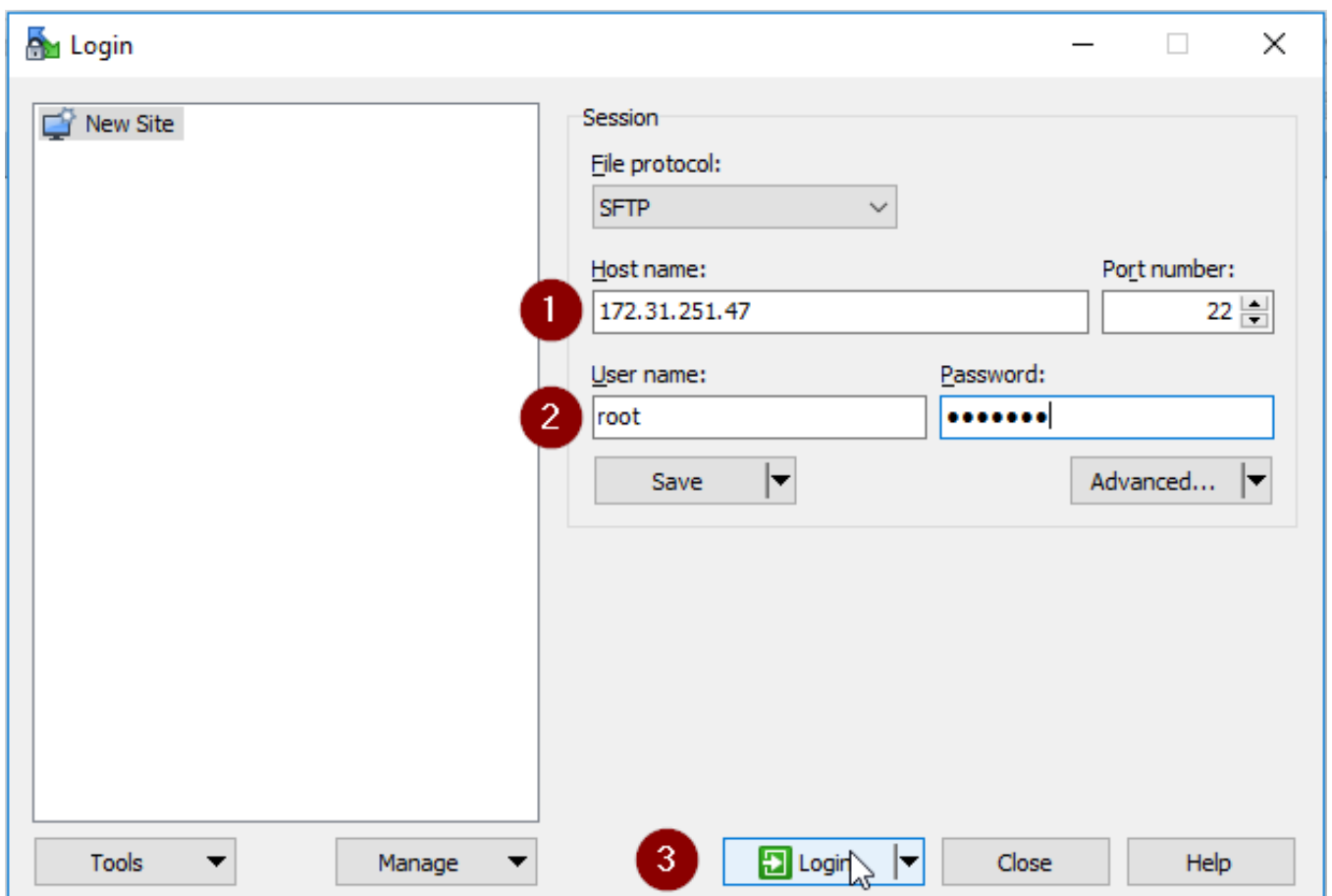


Abbildung 4 - WinSCP Verbindung aufbauen

Schritt 1

Nach dem Login wechselt WinSCP in das Homeverzeichnis des angemeldeten Benutzers. Sollte dies nicht der Benutzer sein mit dem Sie sich zukünftig über SSH verbinden, wechseln Sie in das entsprechende Homeverzeichnis.

Schritt 2

Werden versteckte Dateien und Ordner nicht angezeigt, dann klicken Sie bitte auf das Etikett, welches die Anzahl an versteckten Dateien anzeigt.

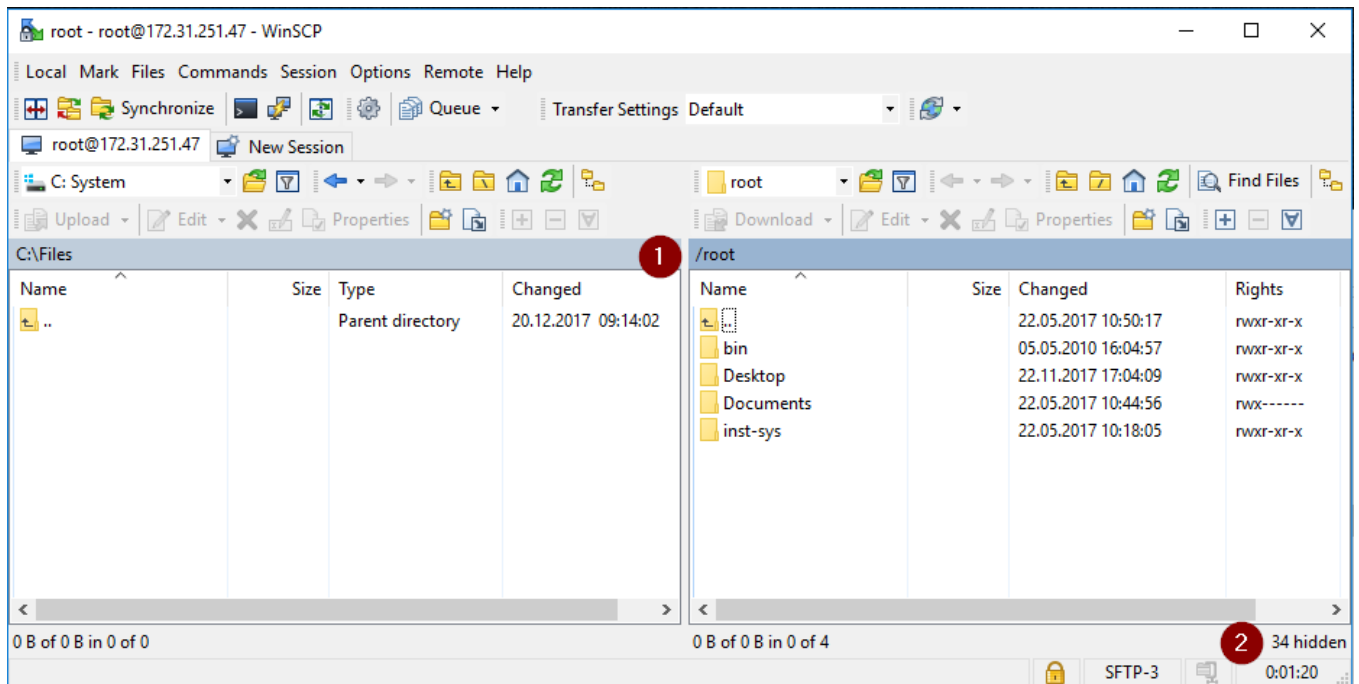


Abbildung 5 - Verbindung zum Zielsystem wurde aufgebaut

Wechseln Sie in das Verzeichnis `.ssh` und editieren dort die Datei `authorized_keys`.

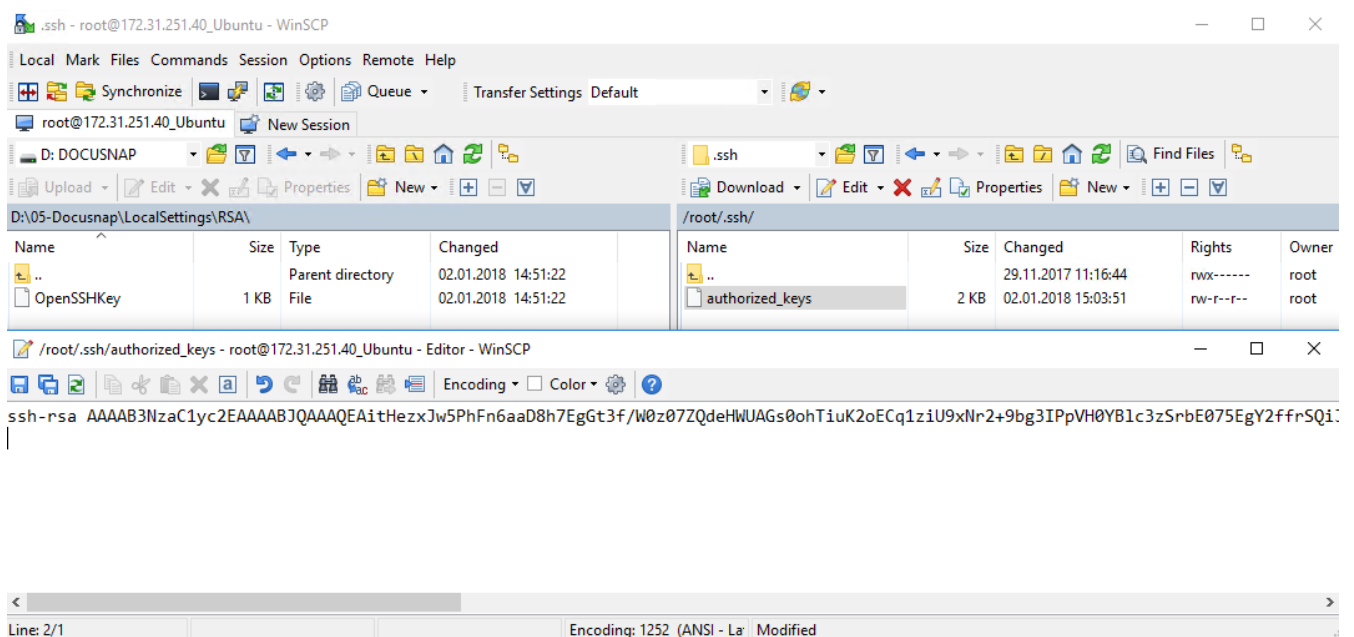


Abbildung 6 - Editieren der Datei `authorized_keys`

Um den zuvor erstellten RSA Schlüssel zu hinterlegen, wird ein Export des PublicKeys aus DocuSnap benötigt. Öffnen Sie dazu die **Administration – Inventar – RSA Schlüssel** und wählen die Schaltfläche **PublicKey Exportieren**. Speichern Sie die Datei ab. Öffnen Sie die Datei mit einem Texteditor und kopieren den PublicKey in die Zwischenablage.

Wechseln Sie zurück nach WinSCP und fügen Sie den PublicKey in einer neuen Zeile ein. Speichern Sie die Datei ab.

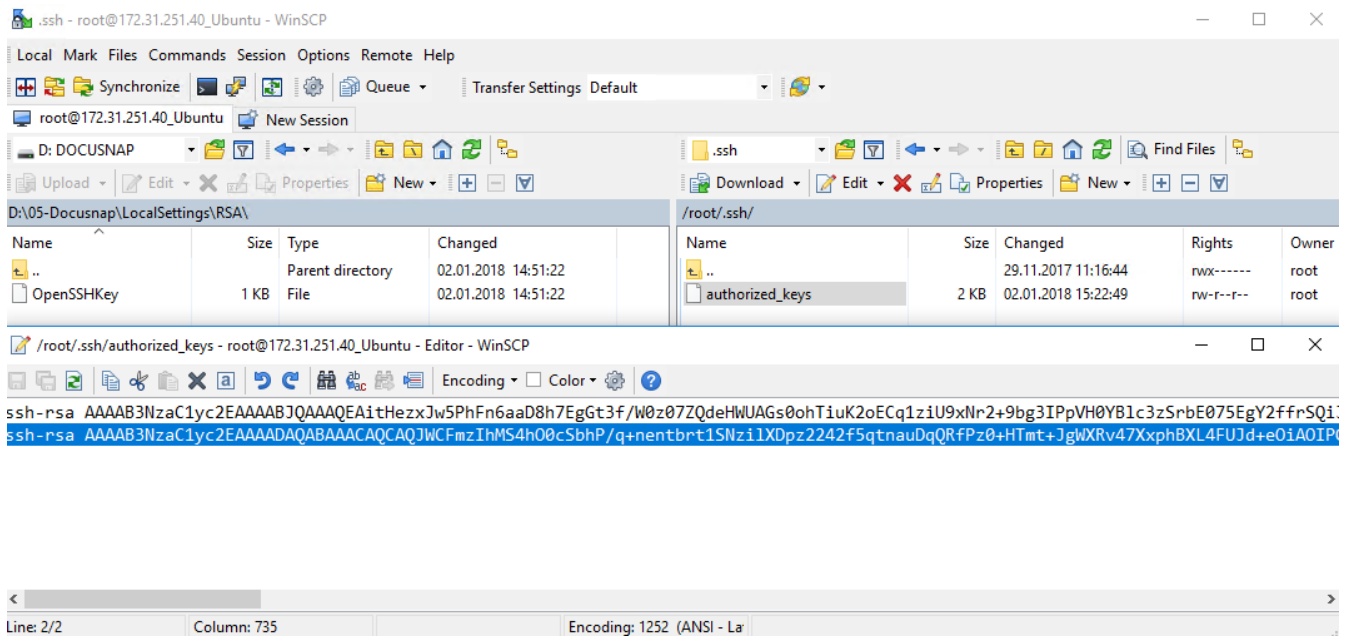


Abbildung 7 - RSA Schlüssel hinterlegen

Nun ist der PublicKey auf dem Zielsystem hinterlegt. Die Inventarisierung kann nun durchgeführt werden. Sie müssen nur den Benutzernamen in dem Assistenten angeben.

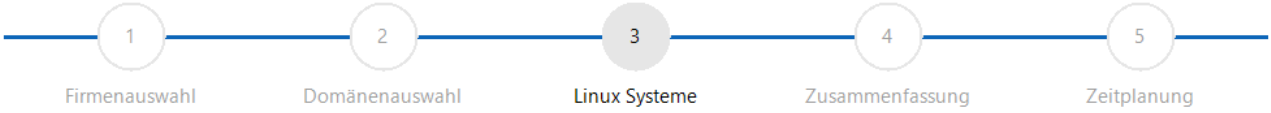
2.4 RSA SCHLÜSSEL FÜR DIE INVENTARISIERUNG VERWENDEN

Nachdem der öffentliche Schlüssel auf den Linux Systemen hinterlegt wurde, kann die Inventarisierung mit diesem durchgeführt werden. Öffnen Sie den Linux Inventarisierung-Assistenten. In Schritt 3 haben Sie nun die Auswahl darüber, welche Authentifizierung Sie verwenden möchten.

Sie können Private Schlüssel für gesamte IP-Bereiche auswählen und auch für einzelne Systeme. Die Vorauswahl aus den IP-Bereichen kann für einzelne Systeme überschrieben werden.

Wenn Sie keinen Privaten Schlüssel verwenden, muss ein Passwort hinterlegt sein. Sie können jedoch auch beide Authentifizierungsmöglichkeiten nutzen – RSA Schlüssel und Passwort. Beide Varianten werden geprüft, die erste, die Erfolg bei der Anmeldung hat, wird genutzt.

Inventarisierung
☐ ×



Linux Systeme inventarisieren

Erweiterte Optionen ▾

IP Bereich hinzufügen

IP von: ✕ IP bis: ✕

Benutzer: Passwort: ✕

Port: Sudo verwenden

Private Key: <kein Eintrag>
<kein Eintrag>
Docusnap GmbH
itelio GmbH

Systeme Vorhandenen Privaten Schlüssel importieren

Hostname: oder IP: ✕

Benutzer: Passwort: ✕

Port: Sudo verwenden

Private Key: <kein Eintrag>

	IP von	IP bis	
<input type="checkbox"/>	<Neuer Eintr...>		

Hostname: oder IP: ✕

Benutzer: Passwort: ✕

Port: Sudo verwenden

Private Key: <kein Eintrag>

	Hostname	IP Adresse	
<input checked="" type="checkbox"/>			

ⓘ Auswahl ist leer! Diesen Assistentschritt gegebenenfalls deaktivieren

Abbildung 8 - Auswahl des RSA Schlüssels

2.5 MIGRIERTE RSA SCHLÜSSEL FÜR DIE INVENTARISIERUNG NUTZEN

Sollten Sie bereits in Versionen vor Juli 2019 einen Privaten Schlüssel verwendet haben, dann wurde dieser automatisch migriert. Der migrierte Schlüssel wird auch automatisch bei zeitgesteuerten Linux Inventarisierungen verwendet – Sie müssen also keine Anpassungen durchführen!

3. VERWENDUNG EINES SUDO USERS

3.1 SUDO KONFIGURATION DURCHFÜHREN

Bevor Sie die Linux Inventarisierung mit einem Benutzer und dem sudo Befehl durchführen können, müssen Sie auf den Linux Systemen eine entsprechende sudo Konfiguration durchführen – diese wird Ihnen folgend beschrieben.

Beachten Sie bitte, dass der evtl. neu erstellte Benutzer eine zugeordnete Login Shell benötigt. Ist dies nicht der Fall, wird die Linux Inventarisierung, trotz korrekter SUDO Konfiguration unvollständig sein. Wir empfehlen daher die User mittels des Befehls Adduser anzulegen. Auf diesem Weg erfolgt automatisch die Zuordnung der Login Shell.

Für die Konfiguration steht Ihnen im Programmverzeichnis von DocuSnap – Standardpfad C:\Program Files\DocuSnap X\Tools\scripts zur Verfügung. In diesem Skript finden Sie alle Befehle, auf die der sudo User berechtigt wird.

Kopieren Sie das Skript auf das Linux System. In diesem HowTo wurde dafür die Software WinSCP verwendet.

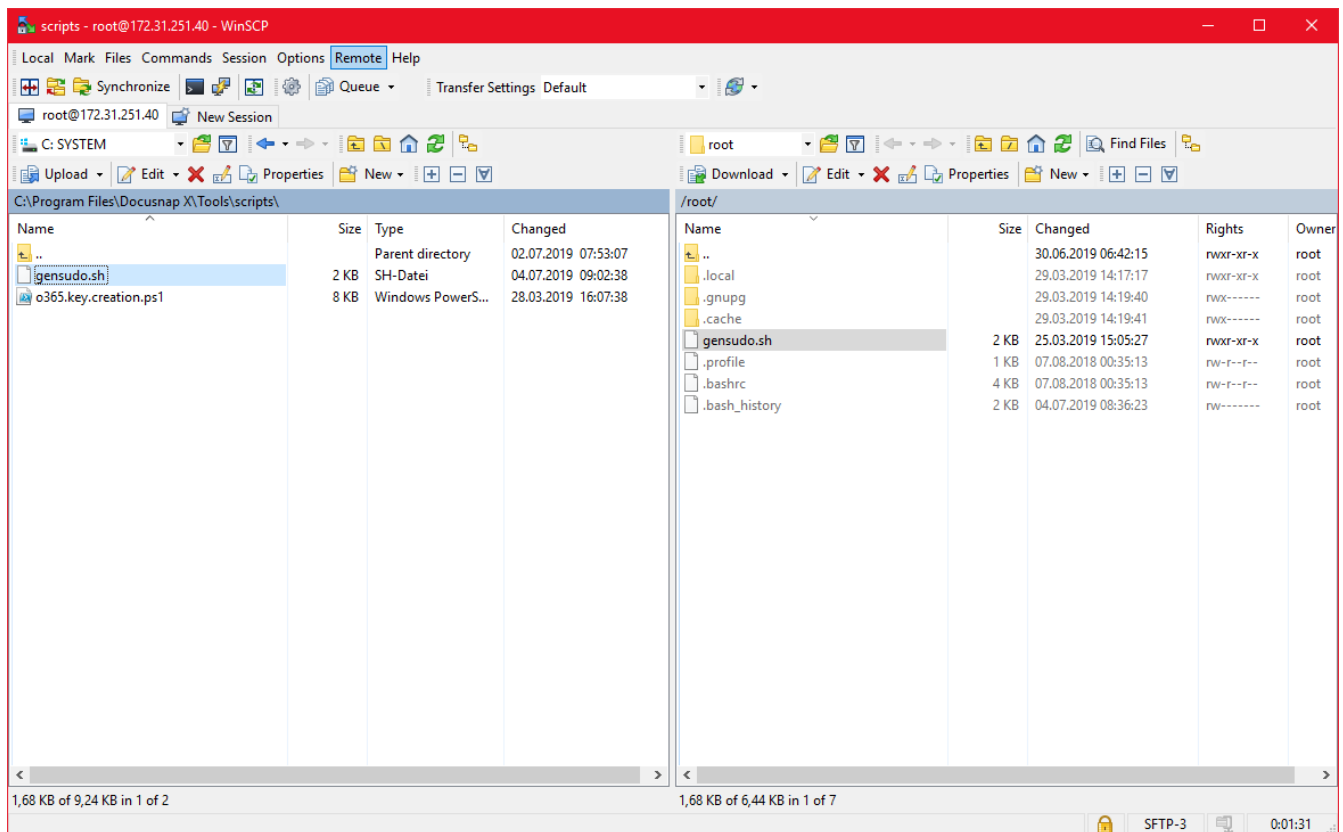
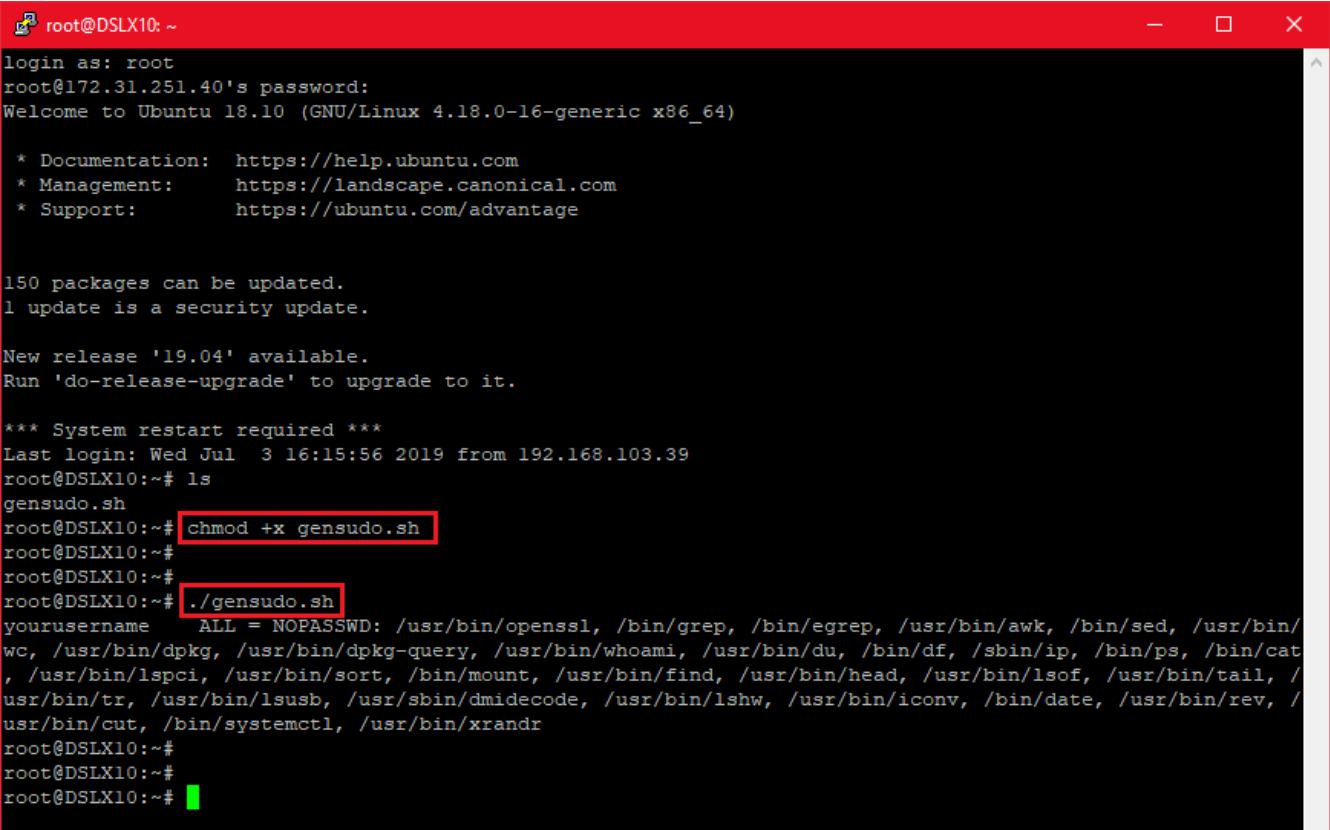


Abbildung 9 - Kopieren des Skripts

Verbinden Sie sich im Anschluss z.B. mit Putty auf die Konsole des Linux Systems, bearbeiten Sie das Skript, damit dieses ausführbar wird. Führen Sie es im Anschluss aus.

```
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/lusb, /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:~# █
```

Abbildung 10 - Skript ausführbar machen und ausführen

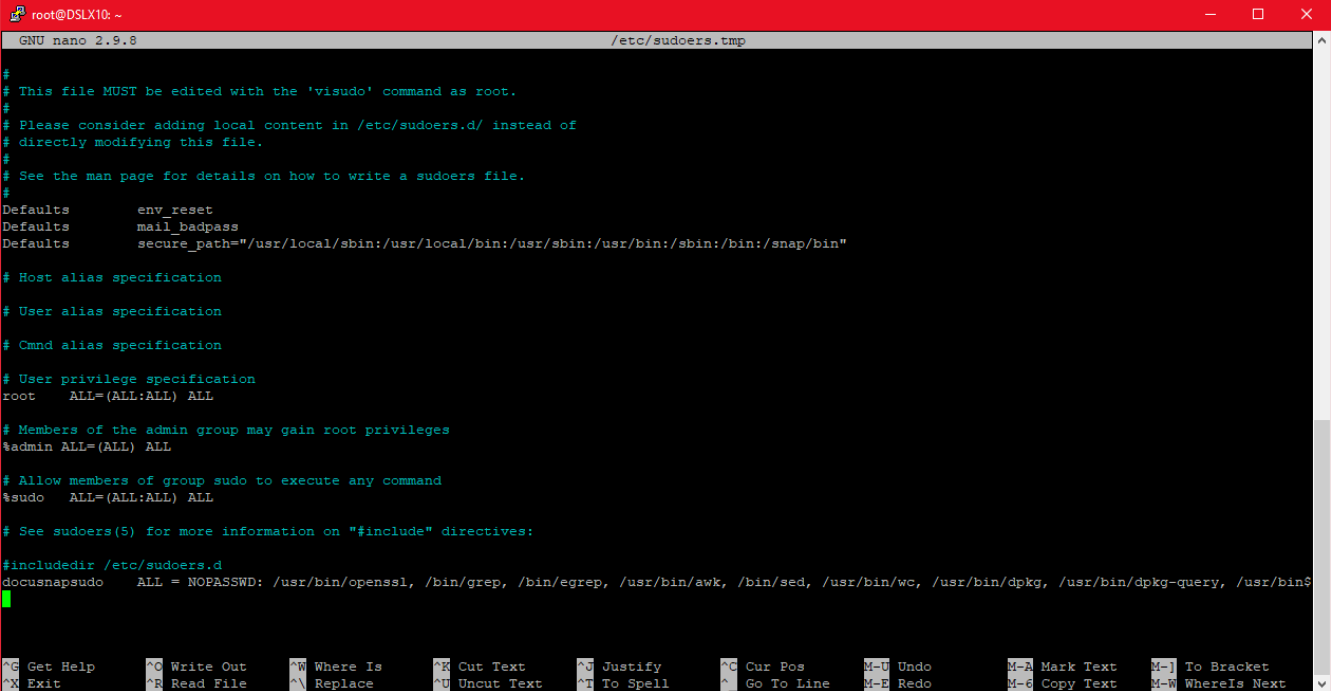
Kopieren Sie die Ausgabe und fügen Sie diese in einen Texteditor ein.

Zu Beginn der Ausgabe müssen Sie nun folgendes anpassen: **YourUserName** wechseln Sie mit dem Namen des sudo Users aus. Der angegebene User hat nach Abschluss der Konfiguration die Berechtigungen, die angegebenen Commands als root auszuführen.

```
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/lusb, /usr/sbin/dmidecode, /usr/bin/lshw, /usr/bin/iconv, /bin/date, /usr/bin/rev, /
usr/bin/cut, /bin/systemctl, /usr/bin/xrandr
```

Beachten Sie bitte, dass die vorherige Ausgabe des Skripts dem Stand vom 04.07.2019 entspricht. Inzwischen könnten hier Änderungen stattgefunden haben.

Kopieren Sie die angepasste Ausgabe und wechseln zurück nach Putty. Geben Sie in Putty visudo ein und wechseln Sie bis ans Ende der Datei und fügen Sie die Zwischenablage ein (rechte Maustaste).



```

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:

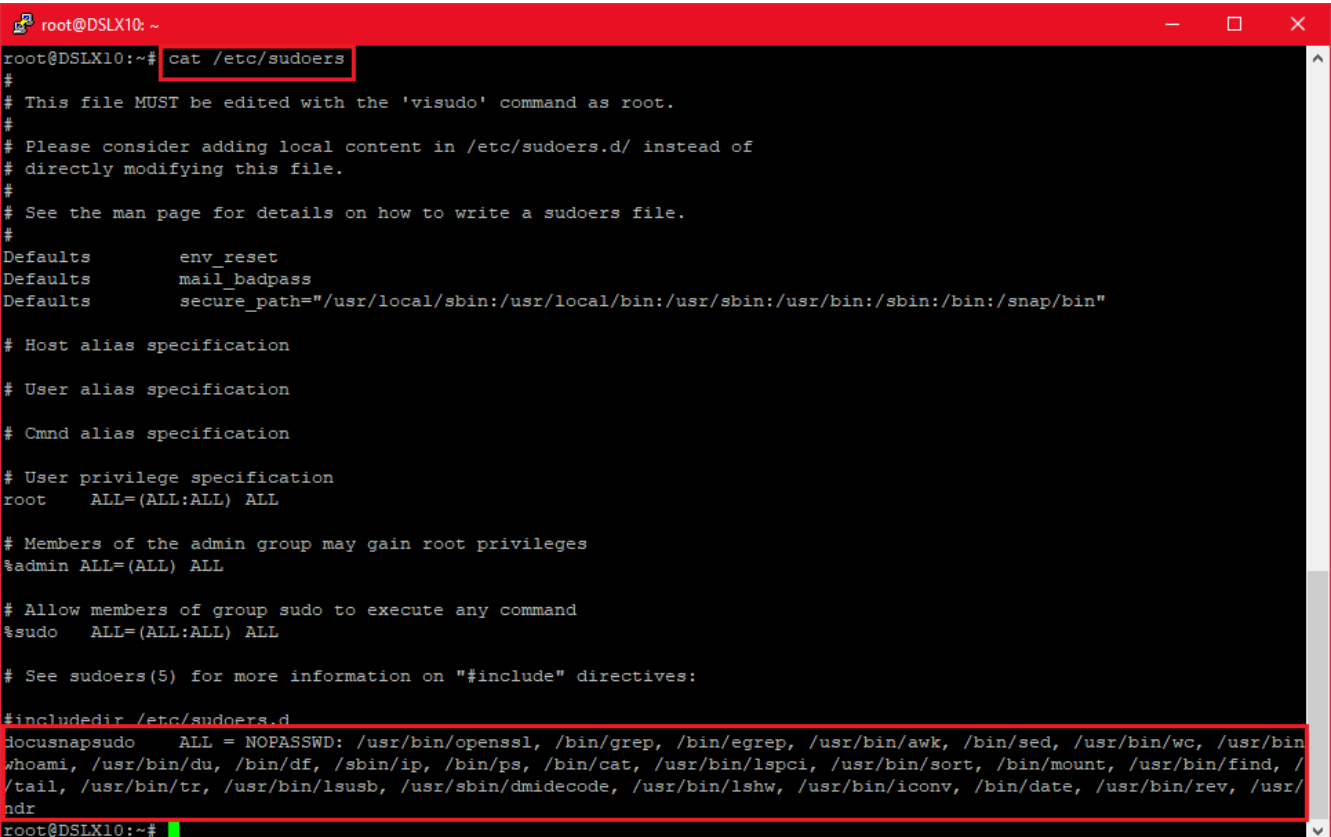
#include_dir /etc/sudoers.d
docusnapsudo    ALL = NOPASSWD: /usr/bin/openssl, /bin/grep, /bin/egrep, /usr/bin/awk, /bin/sed, /usr/bin/wc, /usr/bin/dpkg, /usr/bin/dpkg-query, /usr/bin/

```

Abbildung 11 - Eingefügtes Skript mit dem angepassten Benutzernamen

Beenden (Strg + X) und speichern (Y) Sie die Datei mit dem vorhandenen Dateinamen (Enter).

Mit dem Befehl `cat /etc/sudoers` können Sie prüfen, ob die Änderungen übernommen wurden.



```

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

```

Abbildung 12 - Überprüfung der Änderung

3.2 SUDO FÜR DIE INVENTARISIERUNG AKTIVIEREN

Die Inventarisierung über den sudo User aktivieren Sie daraufhin im Linux Inventarisierungs-Assistenten. Geben Sie einen IP Adressbereich an, den Benutzer, dessen Passwort und aktivieren Sie die Option Sudo verwenden.

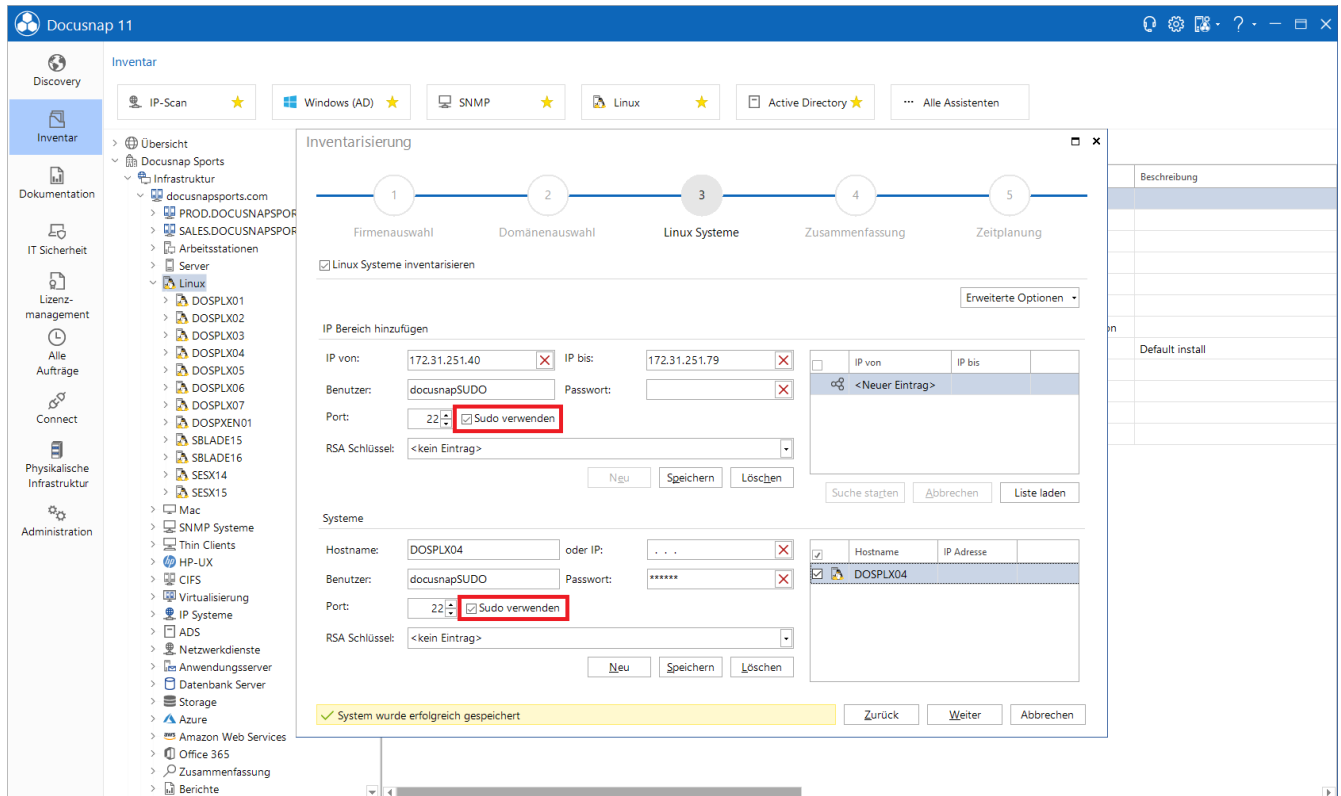


Abbildung 13 - Aktivierung von sudo

ABBILDUNGSVERZEICHNIS

ABBILDUNG 1 - NAVIGATION DOCUSNAP ADMINISTRATION - RSA SCHLÜSSEL	6
ABBILDUNG 2 - RSA SCHLÜSSEL IMPORTIEREN	7
ABBILDUNG 3 - PASSPHRASE EINGEBEN	7
ABBILDUNG 4 - WINSCP VERBINDUNG AUFBAUEN.....	8
ABBILDUNG 5 - VERBINDUNG ZUM ZIELSYSTEM WURDE AUFGEBAUT.....	9
ABBILDUNG 6 - EDITIEREN DER DATEI AUTHORIZED_KEYS	9
ABBILDUNG 7 - RSA SCHLÜSSEL HINTERLEGEN.....	10
ABBILDUNG 8 - AUSWAHL DES RSA SCHLÜSSELS.....	11
ABBILDUNG 9 - KOPIEREN DES SKRIPTS.....	13
ABBILDUNG 10 - SKRIPT AUSFÜHRBAR MACHEN UND AUSFÜHREN	14
ABBILDUNG 11 - EINGEFÜGTES SKRIPT MIT DEM ANGEPASSTEN BENUTZERNAMEN.....	15
ABBILDUNG 12 - ÜBERPRÜFUNG DER ÄNDERUNG.....	15
ABBILDUNG 13 - AKTIVIERUNG VON SUDO.....	16

VERSIONSHISTORIE

Datum	Beschreibung
11.01.2018	Version 1.0 erstellt
24.10.2018	Screenshots angepasst
02.07.2019	Änderungen bezüglich der RSA Schlüssel und Nutzung von sudo hinterlegt
24.04.2020	Version 3.0 - Überarbeitung des HowTos für Docusnap 11
29.06.2021	Überarbeitung der Nutzung von privaten Schlüsseln
