

NVS Greenex

Certificate monitoring in SAP

ABAP and Java

Table of Contents

Introduction.	3
Creating a user for the report.	4
Certificate repositories	5
Creating server accounts.	7
Creating a background task.....	9
Checking the correctness of the task.	11
Troubleshooting.....	12
Conclusion.....	13

Introduction.

One of the most important topics in SAP is the use of up-to-date certificates to ensure the smooth operation of the integration of secure communication channels.

This report is designed to monitor certificates stored in SAP (TLS-SSL) and timely warn about the upcoming expiration date, so that the administrator has the necessary time to take measures to remedy the situation.

The warning is issued 60 days before the end date of the certificate, however, this period can be changed by the `daysBeforeCertificatesExpired` parameter in the SP21 transaction.

The report receives information about certificates stored in SAP by polling the `sapgenpse` program

- `sapgenpse maintain_pk ...`
- `sapgenpse get_my_name ..`

Then the result obtained in text form is parsed (`parse`) and the end date is compared with the current one. When the threshold of 60 days is reached, a standard alert is generated with the sending of an email.

Based on the above, access to the operating system level is required for the report to work

.

Using this method allows you to extract certificates from both SAP ABAP and SAP JAVA systems.

Creating a user for the report.

Create an nvsmon user, if it does not already exist, with commands from root:

```
useradd -s /bin/bash -m nvsmon
```

passwd nvsmon and enter the password twice.

Provide the user with the ability to run selective commands via sudo:

to do this, create a file with the user's name in the /etc/sudoers.d folder.

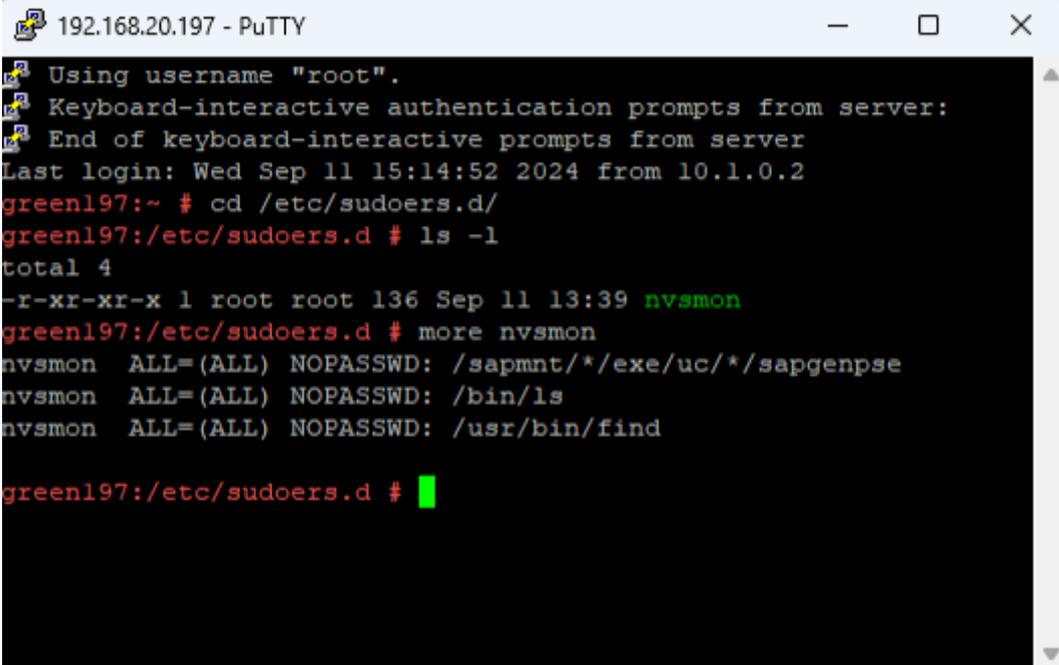
```
nvsmon ALL=(ALL) NOPASSWD: /sapmnt/*/exe/uc/*/sapgenpse
```

```
nvsmon ALL=(ALL) NOPASSWD: /bin/ls
```

```
nvsmon ALL=(ALL) NOPASSWD: /usr/bin/find
```

By doing this, you allow the user to run these commands on behalf of <sid>adm

without entering a password.

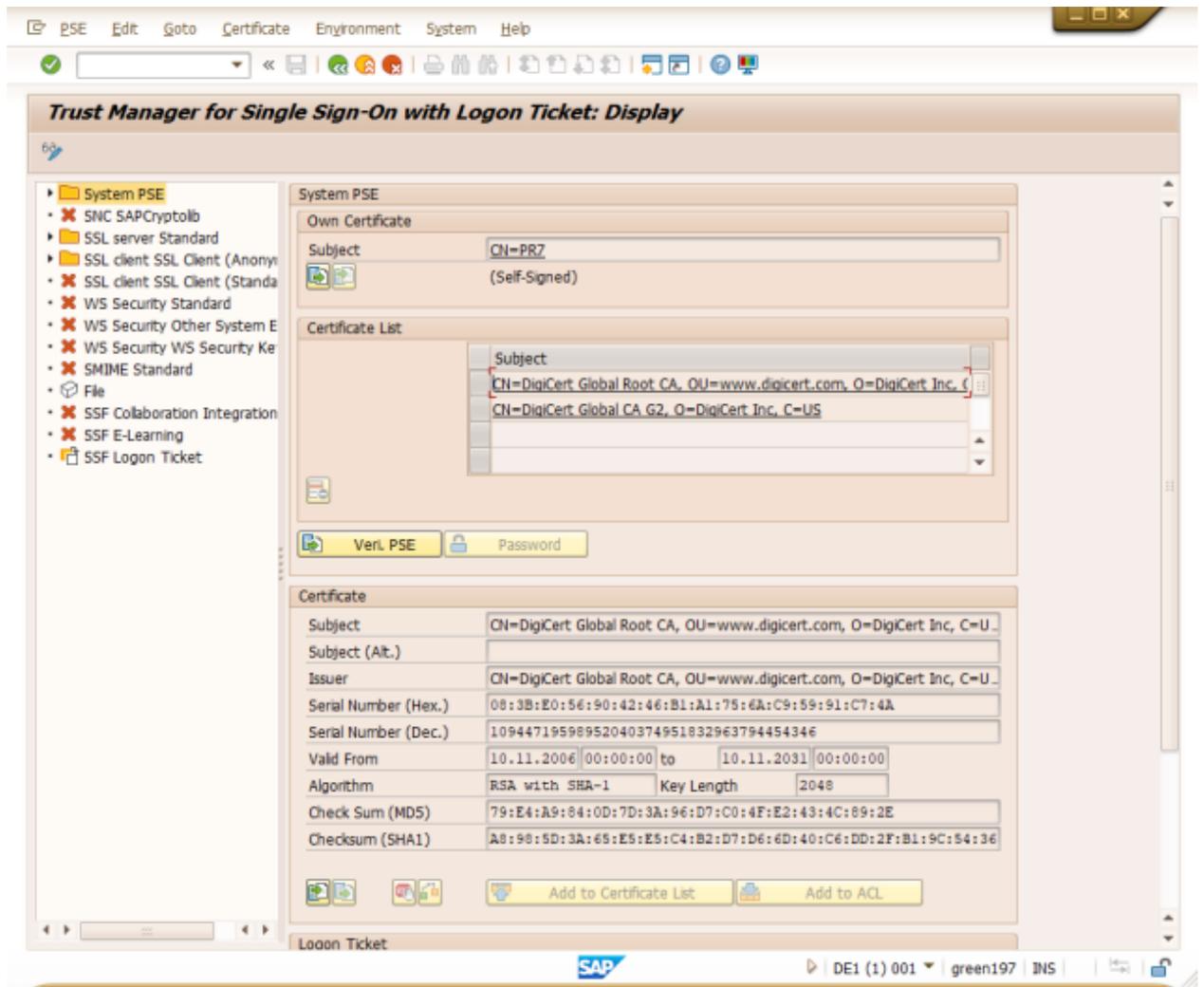


```
192.168.20.197 - PuTTY
Using username "root".
Keyboard-interactive authentication prompts from server:
End of keyboard-interactive prompts from server
Last login: Wed Sep 11 15:14:52 2024 from 10.1.0.2
green197:~ # cd /etc/sudoers.d/
green197:/etc/sudoers.d # ls -l
total 4
-r-xr-xr-x 1 root root 136 Sep 11 13:39 nvsmon
green197:/etc/sudoers.d # more nvsmon
nvsmon  ALL=(ALL) NOPASSWD: /sapmnt/*/exe/uc/*/sapgenpse
nvsmon  ALL=(ALL) NOPASSWD: /bin/ls
nvsmon  ALL=(ALL) NOPASSWD: /usr/bin/find
green197:/etc/sudoers.d # █
```

When using other reports, the user may have other additional records. Be careful when editing this file

Certificate repositories

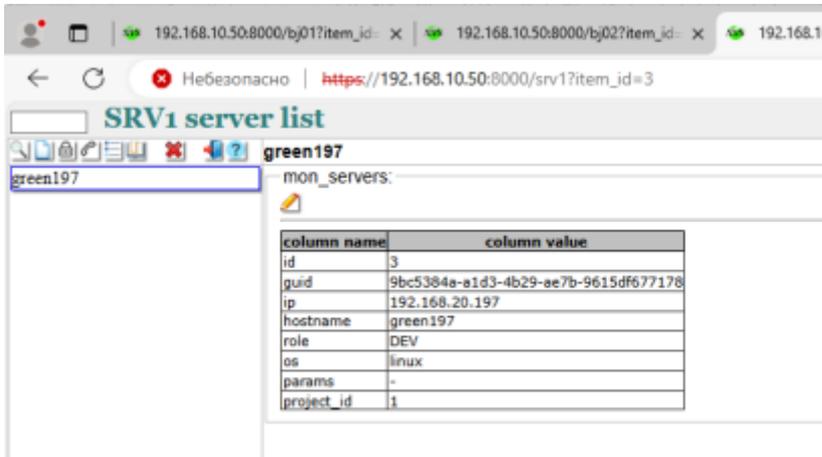
.pse files in SAP play the role of a repository (analogous to keystore.jks in java) – they store all certificates visible and imported through the STRUSTSSO2 transaction (in ABAP)



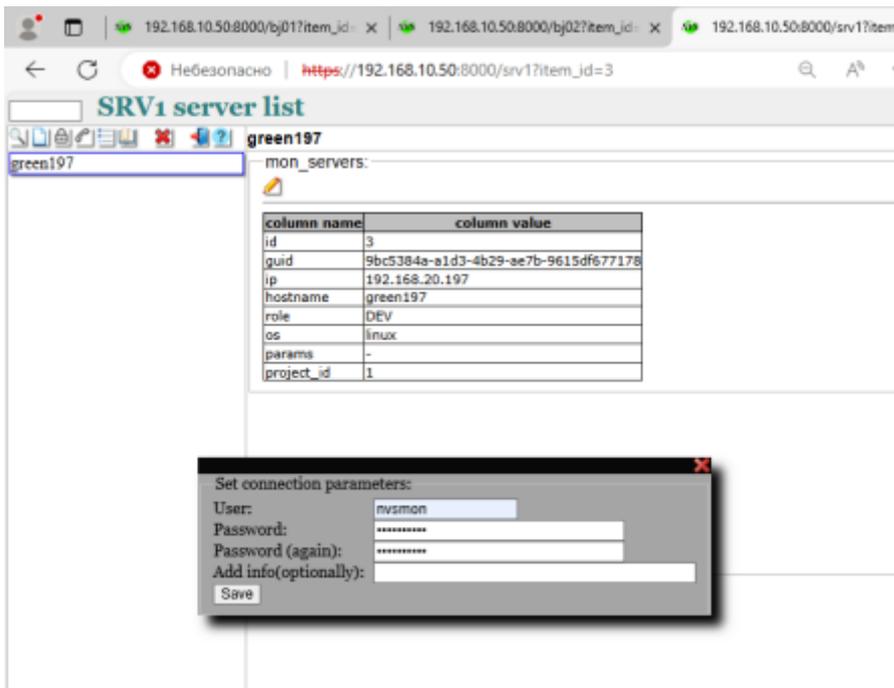
Creating server accounts.

In the SRV1 transaction, for each physical or virtual server, create a record with data for connection:

Specify the IP address, or hostname and the type of operating system: linux.



By clicking on the icon,  we enter the data of the user you created earlier.



www.nvs-itech.com

Check the connection by clicking on the icon : 

If the data is entered correctly, you should see a green flag and a message about the Linux version

 Linux green197 4.12.14-120-default #1 SMP Thu Nov 7 16:39:09 UTC 2019 (fd9dc36) x86_64 x86_64 x86_64
GNU/Linux

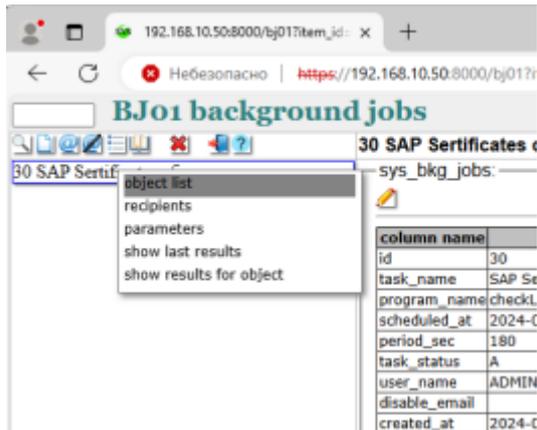
Creating a background task

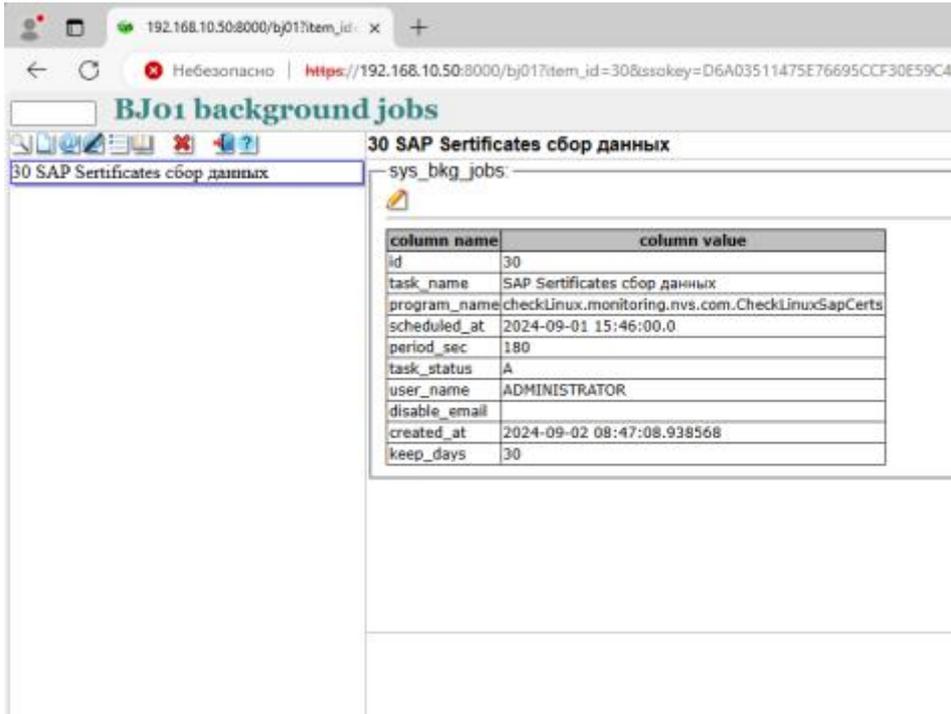
After creating users at the operating system level, create a new background task in BJ01, specify the type of program:

checkLinux.monitoring.nvs.com.CheckLinuxSapCerts

the required start time, the repetition period.

Through the context menu, go to transaction BJ02 and specify the servers for which the task will perform verification





The screenshot shows a web browser window with the address bar displaying a URL: `https://192.168.10.50:8000/bj01?item_id=30&ssakey=D6A03511475E76695CCF30E59C4`. The page title is "BJ01 background jobs". Below the title, there is a navigation bar with a search input and a list of items. The selected item is "30 SAP Certificates сбор данных".

The main content area displays the job details for "30 SAP Certificates сбор данных". The details are presented in a table with the following columns: "column name" and "column value".

column name	column value
id	30
task_name	SAP Certificates сбор данных
program_name	checkLinux.monitoring.nvs.com.CheckLinuxSapCerts
scheduled_at	2024-09-01 15:46:00.0
period_sec	180
task_status	A
user_name	ADMINISTRATOR
disable_email	
created_at	2024-09-02 08:47:08.938568
keep_days	30

Checking the correctness of the task.

To check the correctness and completeness of reading data from ps files, it is recommended

to check the entries in the job logs. To do this, use the icon 

to check the log entries of the background task.



The screenshot shows a web interface for monitoring SAP certificates. The title is "30 SAP Certificates сбор данных". Below the title, it says "Last 30 check results:". A table displays the results of the checks.

id	object_id	object_type	result_value	result_msg	is_alert	checked_at	past_min
151235	5	0.0				2024-09-11 09:45:59.0	0 minutes
151246	5	0.0		ERROR: In SAP system QA1 there is a certificate that IS EXPIRED Subject: Subject: CN=Int-eur-sdr-int-prc.nestle.com O=Nestl Ltd L=Vevey SP=Vaud C=CH Issuer: Issuer: CN=DigiCert TLS RSA SHA256 2020 CA1 O=DigiCert Inc C=US Not After: Not after: Wed Jun 28 02:59:59 2023 left days:-440	X	2024-09-11 09:45:59.0	2 minutes
151325	5	0.0				2024-09-11 09:45:59.0	2 minutes
151325	5	0.0				2024-09-11 09:42:59.0	5 minutes
151303	5	0.0				2024-09-11 09:42:59.0	5 minutes
151318	5	0.0		ERROR: In SAP system QA1 there is a certificate that IS EXPIRED Subject: Subject: CN=Int-eur-sdr-int-prc.nestle.com O=Nestl Ltd L=Vevey SP=Vaud C=CH Issuer: Issuer: CN=DigiCert TLS RSA SHA256 2020 CA1 O=DigiCert Inc C=US Not After: Not after: Wed Jun 28 02:59:59 2023 left days:-440	X	2024-09-11 09:42:59.0	5 minutes
151295	5	0.0				2024-09-11 09:38:59.0	8 minutes



The screenshot shows a table with certificate details. The columns are: Name, Issuer, Subject, Issuer, Not before, and Not after.

Name	Issuer	Subject	Issuer	Not before	Not after
OK QA1 Subject: CN=accessmail	Issuer: CN=accessmail		Validity - Not before: Mon Sep 26 12:58:03 2011 1193801186502	Not after: Fri Jan 1 00:00:00 2038 3850118000612	
OK QA1 Subject: CN=QA1 OU=SSL CLIENT	Issuer: CN=QA1 OU=SSL CLIENT		Validity - Not before: Fri Mar 10 18:09:08 2024 2401181269902	Not after: Fri Jan 1 00:00:00 2038 3803118000612	
OK QA1 Subject: CN=qa1@rsn-deib.com	Issuer: CN=qa1@rsn-deib.com		Validity - Not before: Fri Mar 10 18:09:08 2024 2401181269902	Not after: Fri Jan 1 00:00:00 2038 3803118000612	
ERROR QA1 Subject: CN=Int-eur-sdr-int-prc.nestle.com O=Nestl Ltd L=Vevey SP=Vaud C=CH	Issuer: CN=DigiCert TLS RSA SHA256 2020 CA1 O=DigiCert Inc C=US		Not before: Mon Jun 27 03:00:00 2022	Not after: Wed Jun 28 02:59:59 2023	
OK QA1 Subject: CN=PR1	Issuer: CN=PR1		Validity - Not before: Fri Apr 28 18:08:06 2024 2404281306612	Not after: Fri Jan 1 00:00:00 2038 3803118000612	

Attention: In order to avoid the situation of missing the expiration of important certificates

, it is recommended that after configuring the report, check whether they are all extracted by the monitor.

If the pse file is protected by a PIN and it is not added to the monitor, the data about such a certificate

will NOT be checked.

Troubleshooting

If the report does not see data, connect to the server under the nvsmom user

and try to run the commands:

```
sudo -u de1adm find /usr/sap/DE 1/ -name *.psy
```

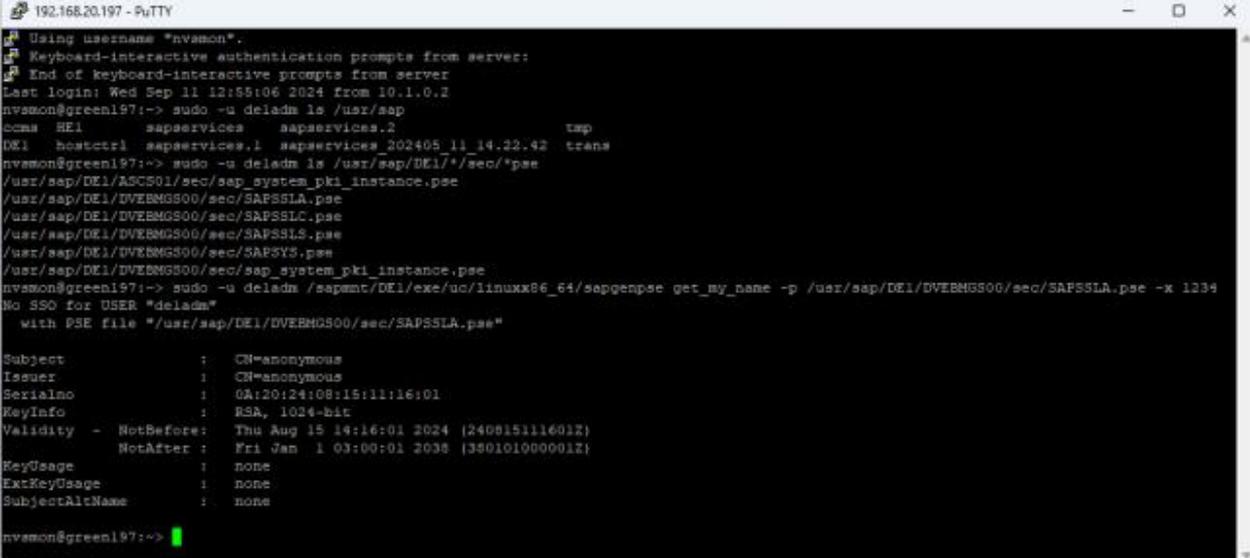
```
sudo -u de1adm /sapmnt/DE1/exe/uc/linux x86_64/sapgenpse get_my_name -p
```

```
//usr/sap/DE 1/DVEBMGS00/sec/SAPSSLA.pse -x 1234
```

where to replace the sid in the example is DE1 and the path to the pse file.

-x 1234 is the PIN value – substitute the current one or leave it as the default (1234). Even

an incorrect value helps to avoid hanging while waiting for input



```
192.168.20.197 - PuTTY
Using username "nvsmom".
Keyboard-interactive authentication prompts from server:
End of keyboard-interactive prompts from server
Last login: Wed Sep 11 12:55:06 2024 from 10.1.0.2
nvsmom@green197:~$ sudo -u deladm ls /usr/sap
ccms  DE1      sapservices      sapservices.2      tmp
DE1   hostctrl  sapservices.1    sapservices_20240511_14.22.42  trans
nvsmom@green197:~$ sudo -u deladm ls /usr/sap/DE1/*/*sec/*pse
/usr/sap/DE1/ASC501/sec/sap_system_pki_instance.pse
/usr/sap/DE1/DVEBMGS00/sec/SAPSSLA.pse
/usr/sap/DE1/DVEBMGS00/sec/SAPSSLC.pse
/usr/sap/DE1/DVEBMGS00/sec/SAPSSL3.pse
/usr/sap/DE1/DVEBMGS00/sec/SAPSYS.pse
/usr/sap/DE1/DVEBMGS00/sec/sap_system_pki_instance.pse
nvsmom@green197:~$ sudo -u deladm /sapmnt/DE1/exe/uc/linuxx86_64/sapgenpse get_my_name -p /usr/sap/DE1/DVEBMGS00/sec/SAPSSLA.pse -x 1234
No SSO for USER "deladm"
with PSE file "/usr/sap/DE1/DVEBMGS00/sec/SAPSSLA.pse"

Subject       : CN=anonymous
Issuer        : CN=anonymous
Serialno      : 0A:20:24:08:15:11:16:01
KeyInfo       : RSA, 1024-bit
Validity - NotBefore: Thu Aug 15 14:16:01 2024 (240815111601Z)
              NotAfter:  Fri Jan 1 03:00:01 2038 (380101000001Z)
KeyUsage      : none
ExtKeyUsage   : none
SubjectAltName: none

nvsmom@green197:~$
```

Conclusion

This report works similarly to other reports that receive data via the operating system by requesting ssh. If there is no response from the OS, check the necessary permissions in the `/etc/sudoers.d/nvsmon` file