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 daysBeforeCertificateIsExpired 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.

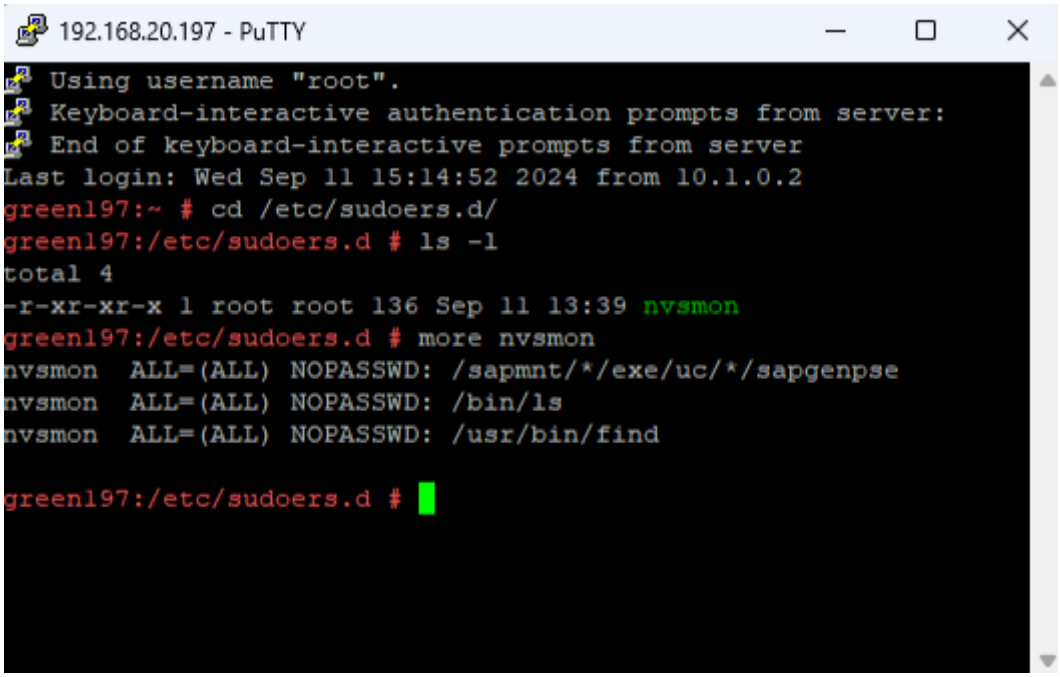
nvsmon ALL=(ALL) NOPASSWD: /sapmnt/*/exe/uc/*/sapgenpse

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.

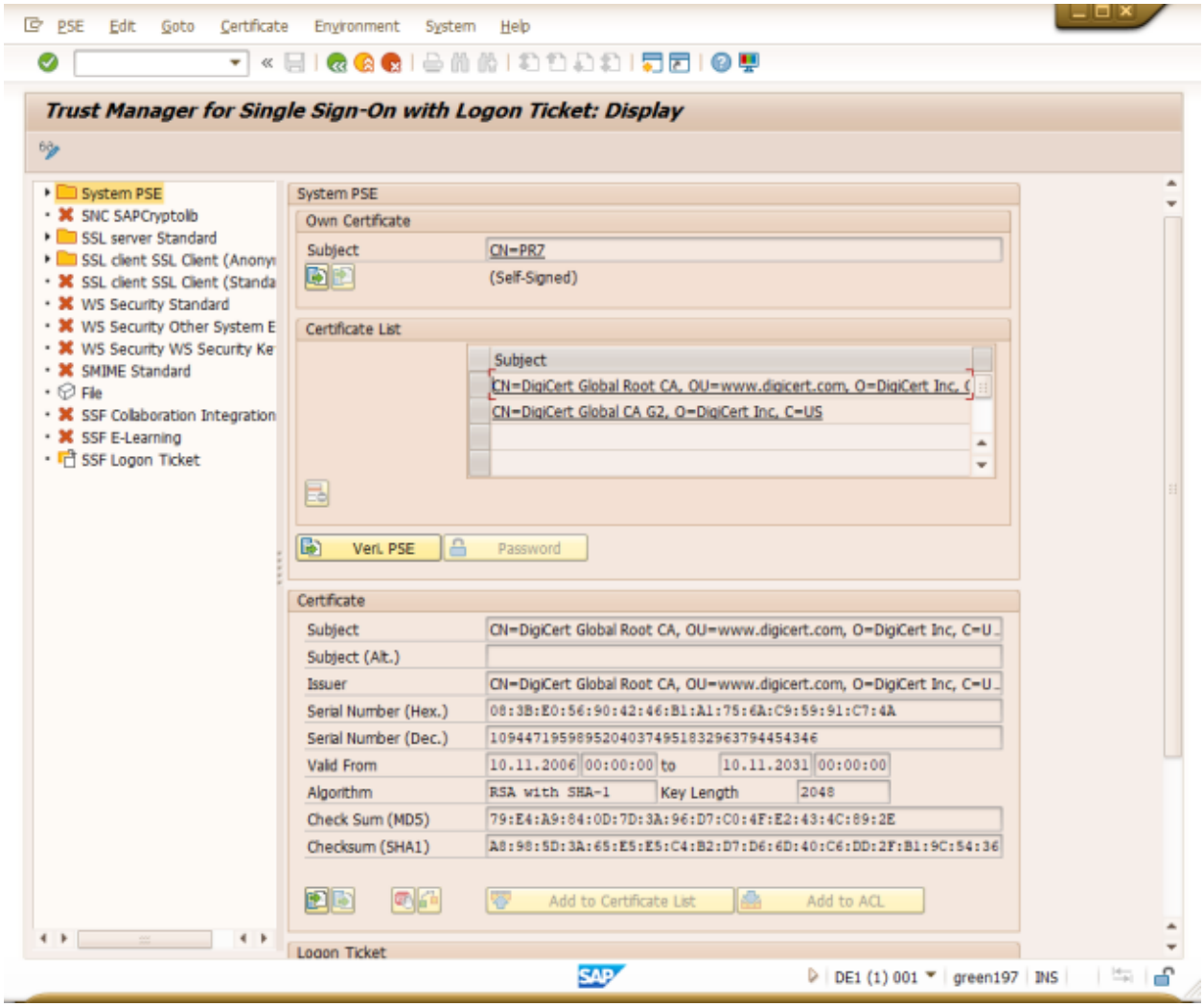


When using other reports, the user may have other additional

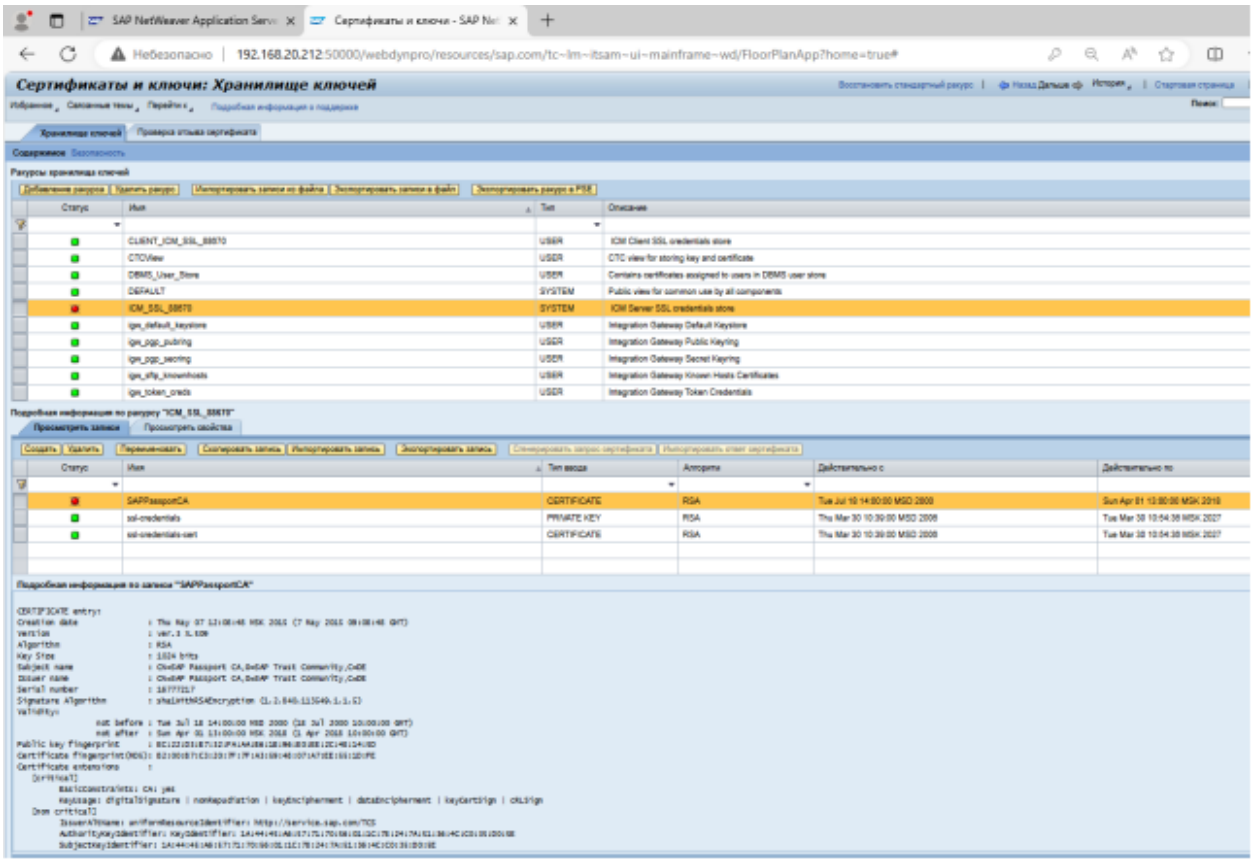
records. Be careful when editing this file

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)



and via the web interface in SAP JAVA



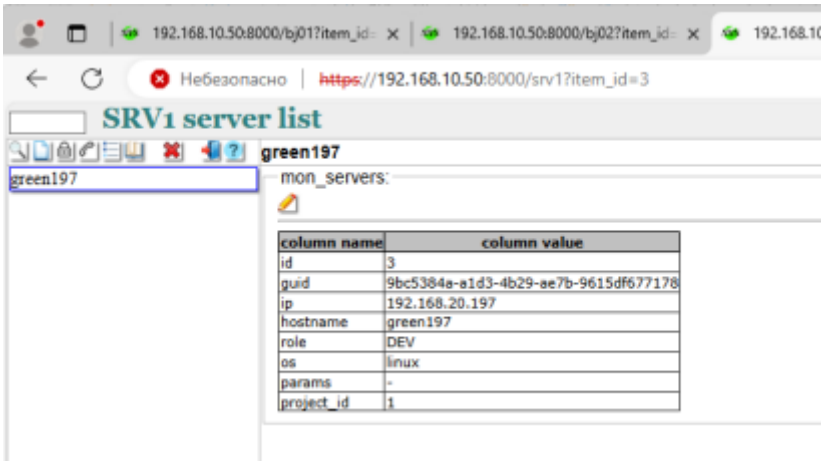
The report supports entering a single shared password (pin) for everyone to read.pst files.

If sapgenpse is protected by a similar PIN, you can enter it through the parameter defaultSapgenpsePin in sp21. If the pin does not match, the monitor ignores this file and the data from it does not get into the report.

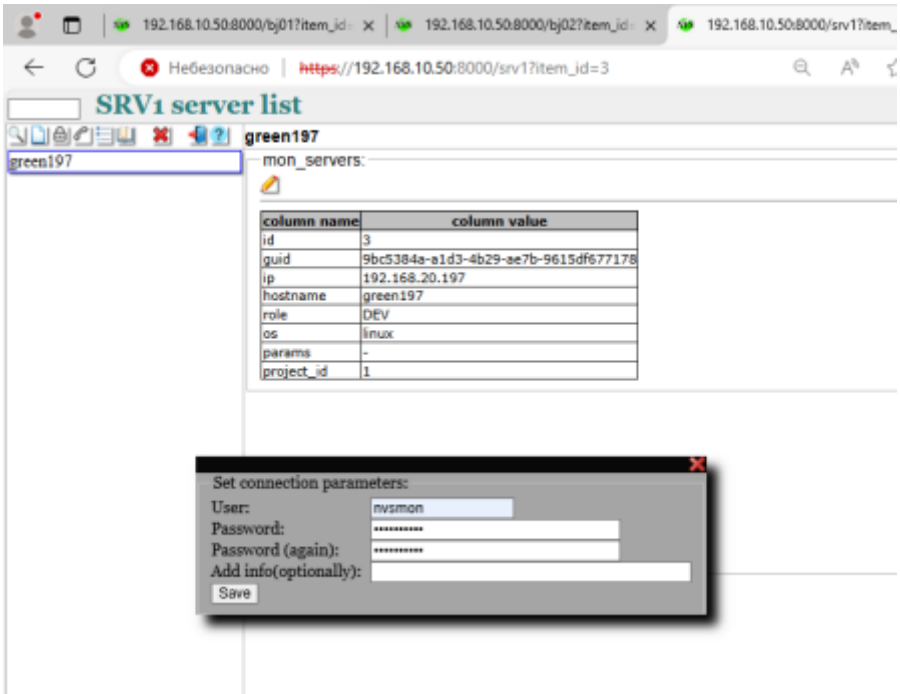
Creating server accounts.

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.



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

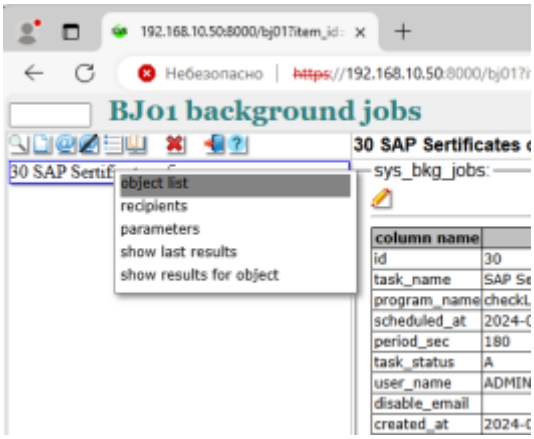
Creating a background task

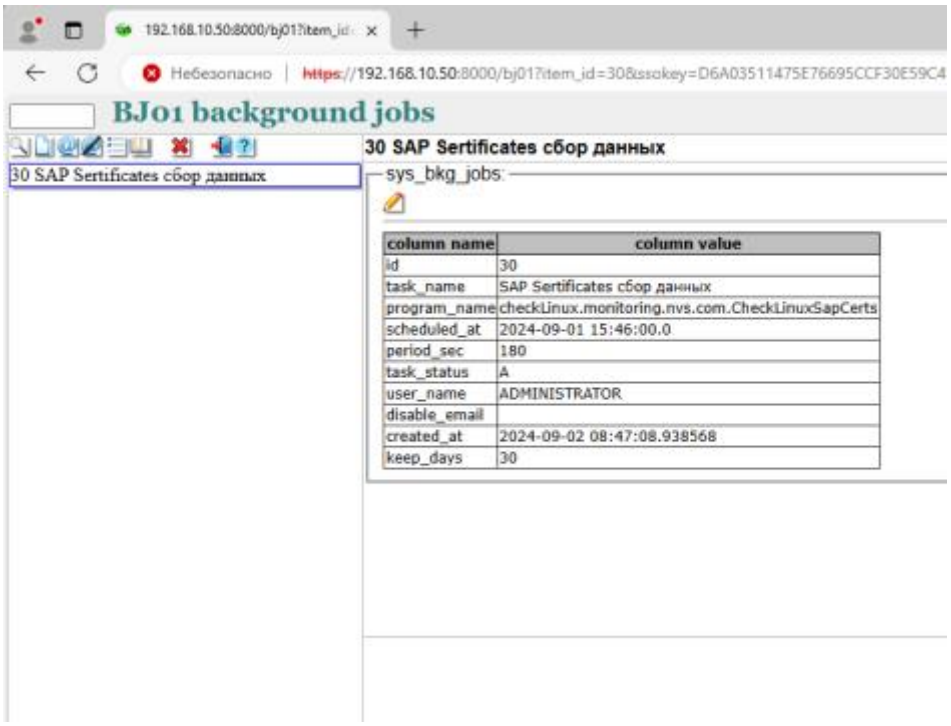
After creating users at the operating system level, create a new background task in BJ01, specify the type of program:

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



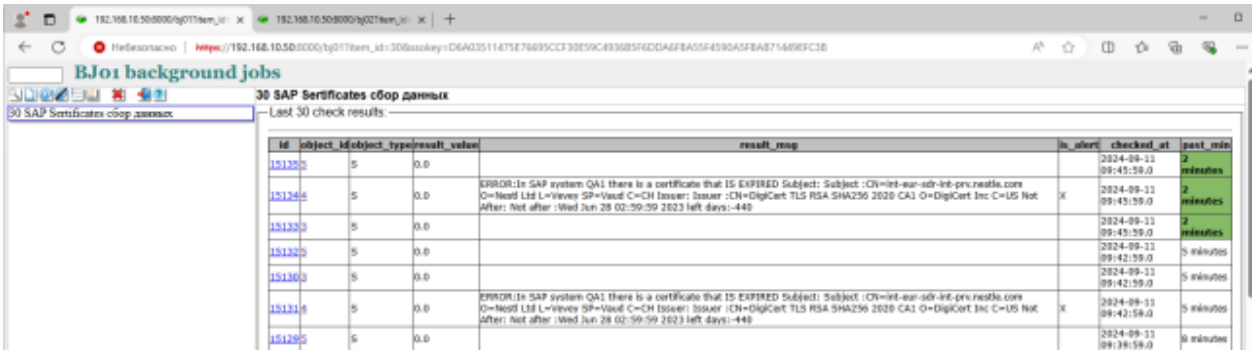

192.168.10.50:8000/bj01?item_id
Небезопасно
https://192.168.10.50:8000/bj01?item_id=30&ssokey=D6A03511475E76695CCF30E59C4
BJ01 background jobs
30 SAP Sertificates сбор данных
30 SAP Sertificates сбор данных
sys_bkg_jobs
column name
column value
id
30
task_name
SAP Sertificates сбор данных
program_name
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 blog entries of the background task.



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 nvsmon user

and try to run the commands:

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

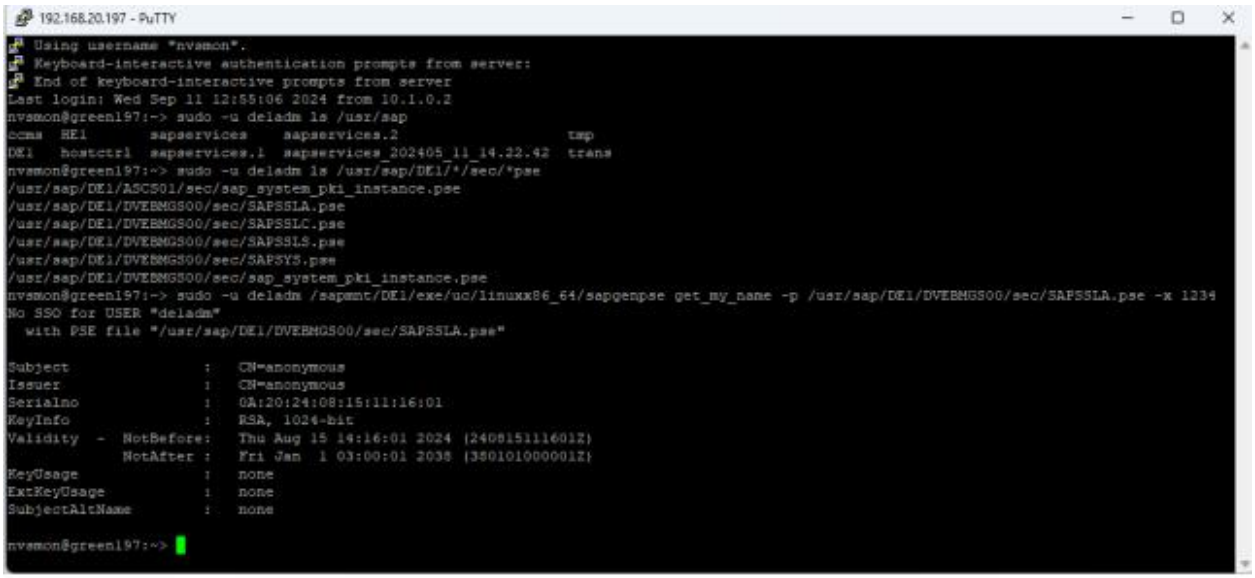
sudo -u de1adm /sapmnt/DE1/exe/uc/linux x86_64/sapgenpse get_my_name -p

//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



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