NVS Greenex

Мониторинг сертификатов в SAP ABAP и Java

Оглавление

Введение.

Одной из важнейших тем в SAP является использование актуальных сертификатов для обеспечения бесперебойной работы интеграции защищенных каналов связи.

Данный отчет предназначен для контроля хранящихся в SAP сертификатов (TLS-SSL) и своевременного предупреждения о наступающем истечении срока годности, для того чтобы у администратора было необходимое время для принятия мер по исправлению ситуации.

Предупреждение выдается за **60** дней до конечной даты сертификата, однако этот срок можно изменить параметром daysBeforeCertificateIsExpired в транзакции SP21.

Отчет получает информацию о хранящихся в SAP сертификатов путем опроса программы sapgenpse

- **sapgenpse maintain_pk** ...
- **sapgenpse get_my_name** ..

  Затем результат получаемый в текстовом виде разбирается (parse) и конечная дата сравнивается с текущей. При достижении порога в 60 дней генерируется стандартный алерт с отправкой письма.

Исходя из вышеизложенного, для работы отчета необходим доступ на уровень операционной системы.

Использование данного способа позволяет извлекать сертификаты как из систем SAP ABAP так и SAP JAVA.

Создание пользователя для отчета.

Создайте пользователя nvsmon, если он еще не существует командами из под root:

useradd -s /bin/bash -m nvsmon

passwd nvsmon и дважды введите пароль.

Предоставьте пользователю возможность запускать выборочные команды через sudo:

для этого создайте в папке /etc/sudoers.d файл с именем пользователя.

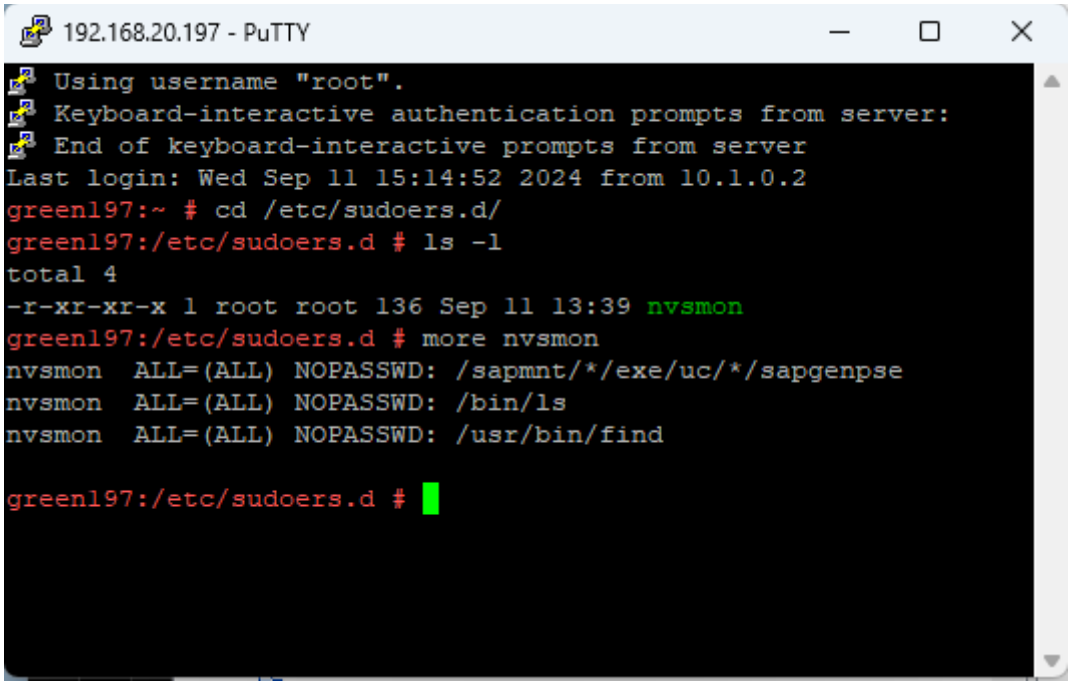
nvsmon ALL=(ALL) NOPASSWD: /sapmnt/*/exe/uc/*/sapgenpse

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

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

Этим вы разрешаете пользователю запускать данные команды от лица <sid>adm

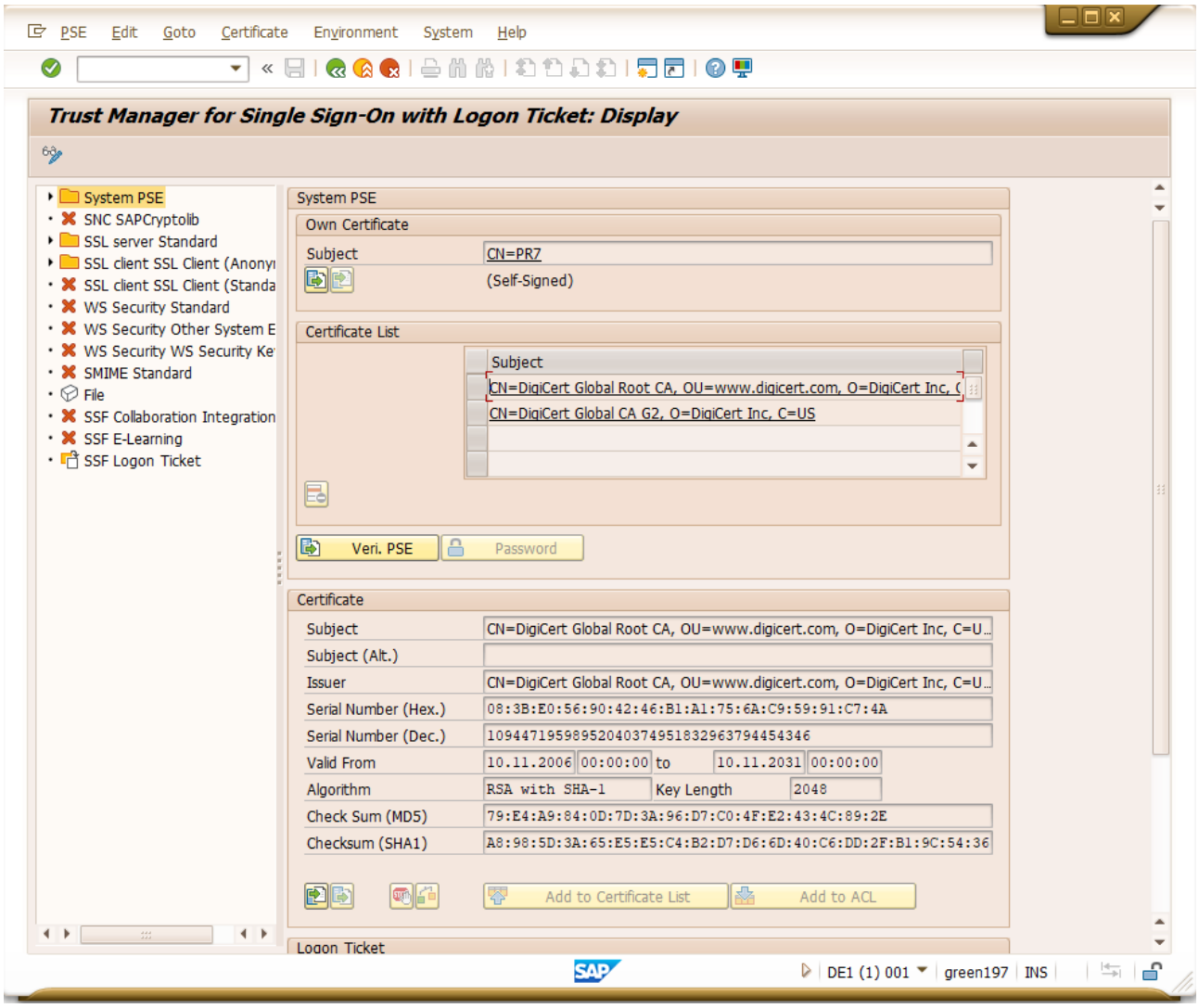
без ввода пароля.



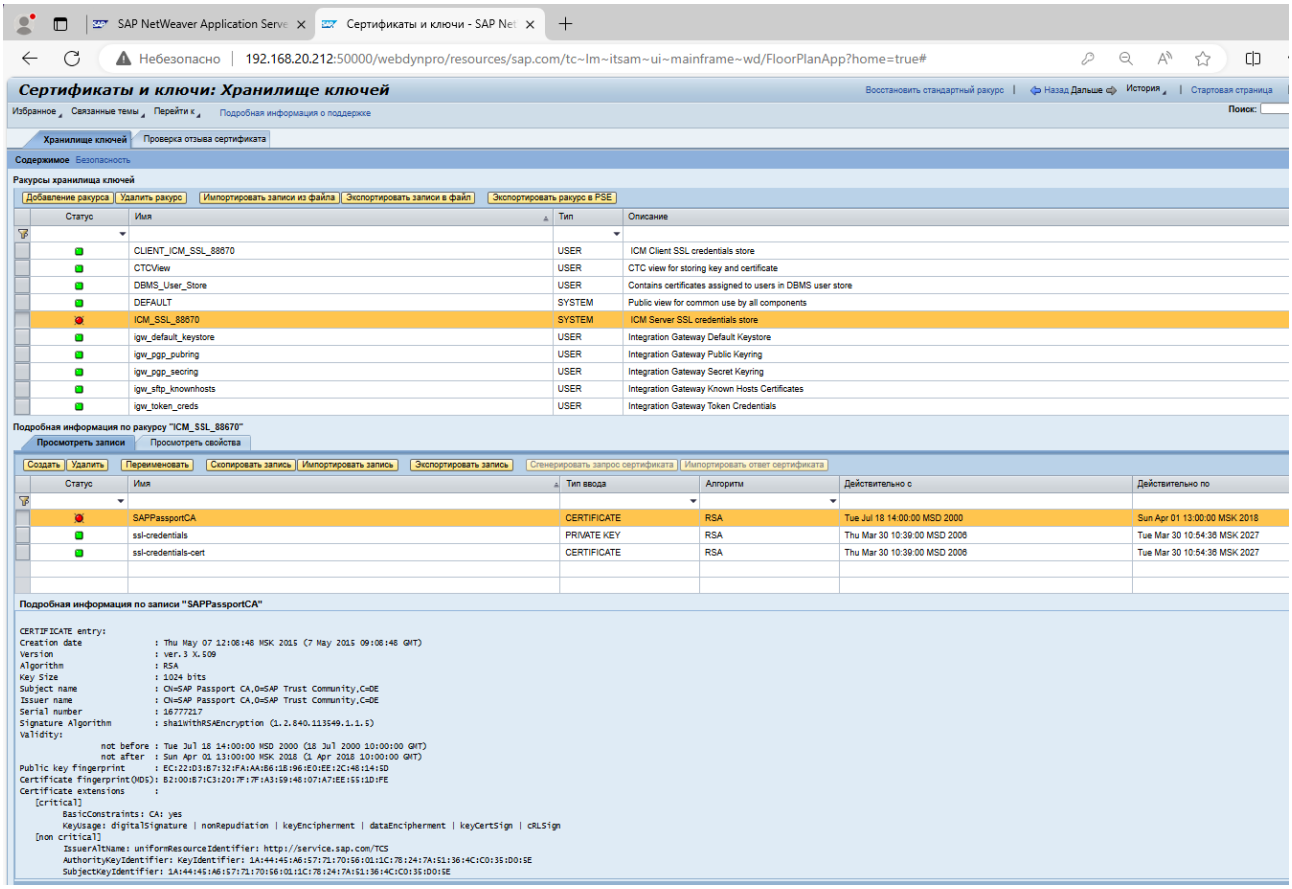
При использовании других отчетов у пользователя могут быть другие дополнительные записи. Будьте внимательны при редактировании данного файла.

Хранилища сертификатов

.pse файлы в SAP играют роль хранилища (аналог keystore.jks в java) – в них хранятся все сертфикаты, видимые и импортируемые через транзакцию STRUSTSSO2 (в ABAP)



и через web интерфейс в SAP JAVA



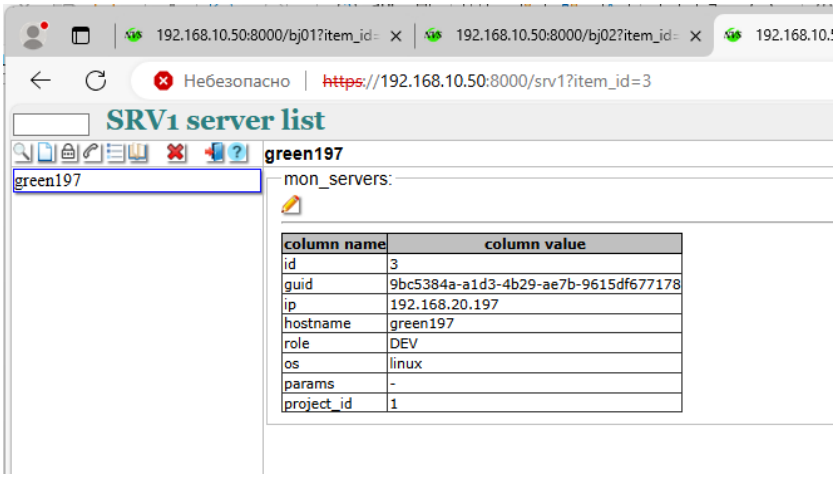
Отчет поддерживает ввод одного общего пароля (pin) для чтения всех .pse файлов.

Если sapgenpse защищен подобным PIN вы можете ввести его через параметр defaultSapgenpsePin в sp21. Если pin не подходит, монитор игнорирует данный файл и данные из него не попадают в отчет.

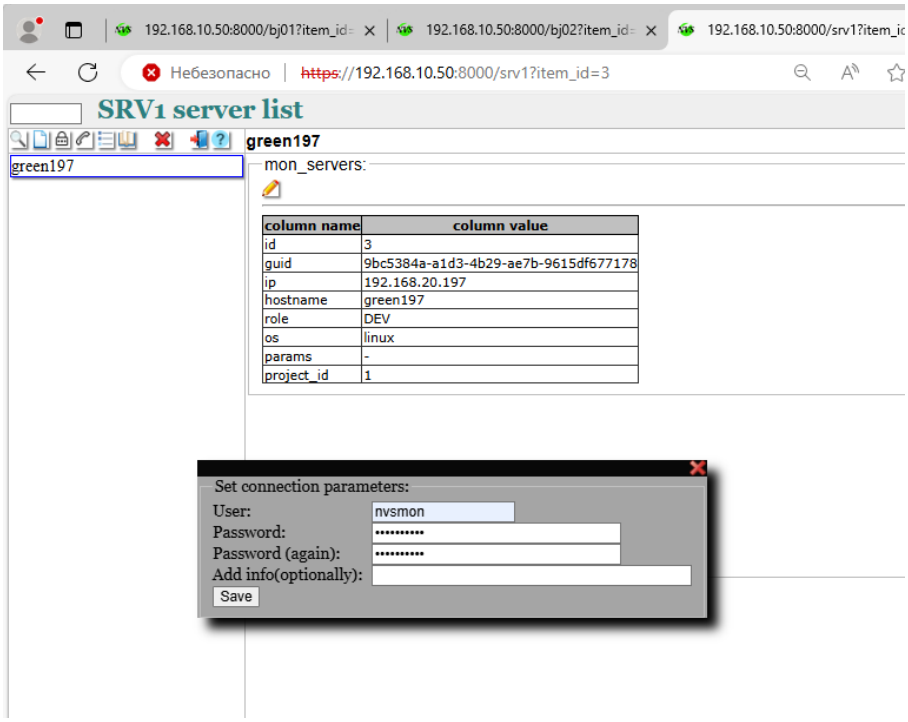
Создание учетных записей серверов.

В транзакции SRV1 для каждого физического или виртуального сервера создайте запись с данными для подключения:

Укажите IP адрес, либо hostname и тип операционной системы: linux.

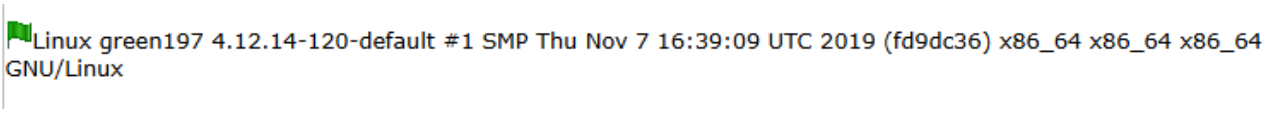


Нажав на иконку вводим данные пользователя которого вы создали ранее.



Проверьте соединение нажав на иконку : 

Если данные введены корректно, вы должны увидеть зеленый флаг и сообщение о версии линукса.



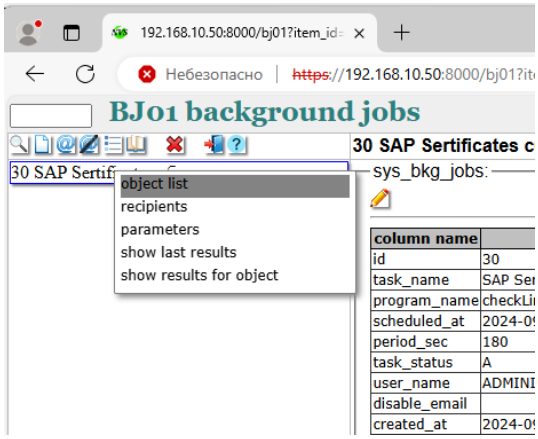
Создание фонового задания

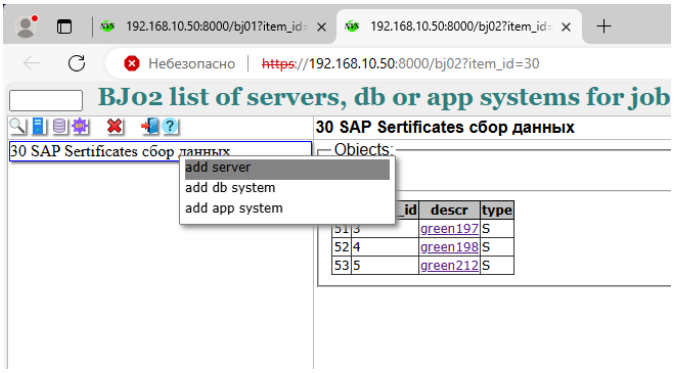
После создания пользователей на уровне операционной системы, создайте новую фоновую задачу в BJ01, укажите тип программы:

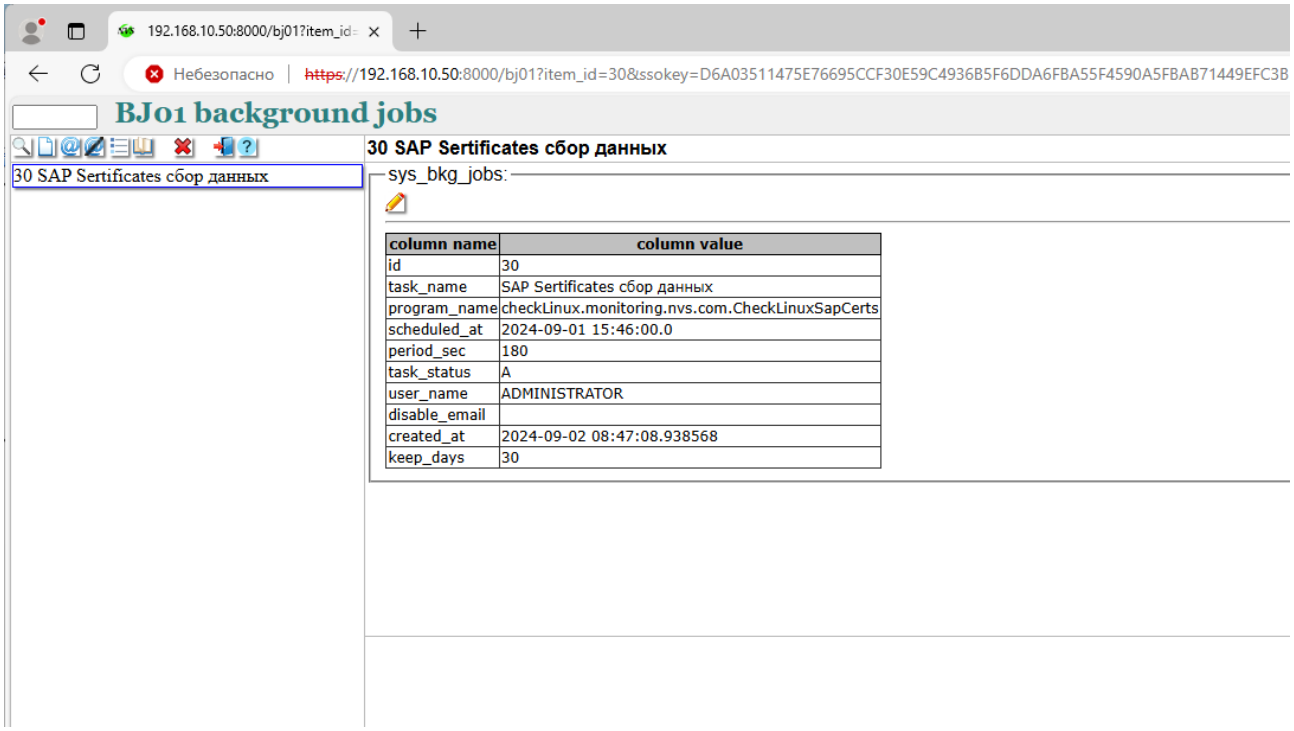
checkLinux.monitoring.nvs.com.CheckLinuxSapCerts

необходимый момент старта, период повторения.

Через контекстное меню перейдите в транзакцию BJ02 и укажите сервера для которых задание будет выполнять проверку:



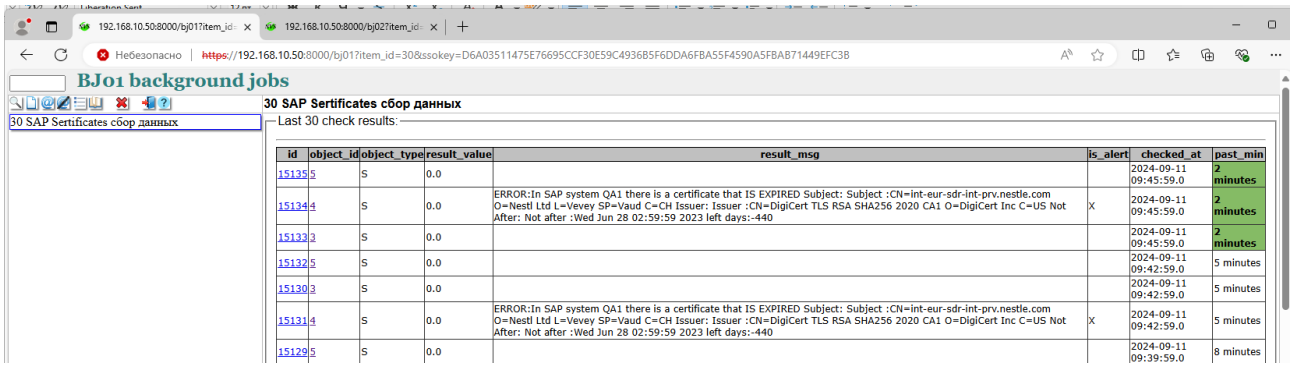



192.168.10.50:8000/bj01?item_id=
Небезопасно
https://192.168.10.50:8000/bj01?item_id=30&ssokey=D6A03511475E76695CCF30E59C4936B5F6DDA6FBA55F4590A5FBAB71449EFC3B
BJ01 background jobs
30 SAP Sertificates сбор данных
30 SAP Sertificates сбор данных
sys_bkg_jobs:
column name
column value
id
30
task_name
SAP 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

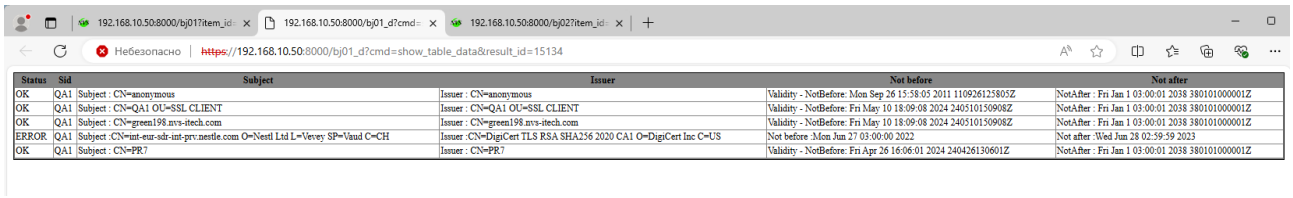
Проверка корректности работы задания.

Для проверки корректности и полноты считывание данных из pse файлов рекомендуется проверить записи в логах работы задания. Для этого с помощью иконки 

проверьте записи в логах фонового задания.



id	object_id	object_type	result_value	result_msg	is_alert	checked_at	past_min
15135	5	S	0.0			2024-09-11 09:45:59.0	2 minutes
15134	4	S	0.0	ERROR:In SAP system QA1 there is a certificate that IS EXPIRED Subject: Subject :CN=int-eur-sdr-int-prv.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
15133	3	S	0.0			2024-09-11 09:45:59.0	2 minutes
15132	5	S	0.0			2024-09-11 09:42:59.0	5 minutes
15130	3	S	0.0			2024-09-11 09:42:59.0	5 minutes
15131	4	S	0.0	ERROR:In SAP system QA1 there is a certificate that IS EXPIRED Subject: Subject :CN=int-eur-sdr-int-prv.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
15129	5	S	0.0			2024-09-11 09:39:59.0	8 minutes



Status	Sid	Subject	Issuer	Not before	Not after
OK	QA1	Subject : CN=anonymous	Issuer : CN=anonymous	Validity - NotBefore: Mon Sep 26 15:58:05 2011 110926125805Z	NotAfter : Fri Jan 1 03:00:01 2038 380101000001Z
OK	QA1	Subject : CN=QA1 OU=SSL CLIENT	Issuer : CN=QA1 OU=SSL CLIENT	Validity - NotBefore: Fri May 10 18:09:08 2024 240510150908Z	NotAfter : Fri Jan 1 03:00:01 2038 380101000001Z
OK	QA1	Subject : CN=green198.nvs-itech.com	Issuer : CN=green198.nvs-itech.com	Validity - NotBefore: Fri May 10 18:09:08 2024 240510150908Z	NotAfter : Fri Jan 1 03:00:01 2038 380101000001Z
ERROR	QA1	Subject :CN=int-eur-sdr-int-prv.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=PR7	Issuer : CN=PR7	Validity - NotBefore: Fri Apr 26 16:06:01 2024 240426130601Z	NotAfter : Fri Jan 1 03:00:01 2038 380101000001Z

Внимание: Во избежание ситуации пропуска об истечении важных сертификатов рекомендуется после настройки отчета проверить все ли они извлекаются монитором.

Если файл pse защищен PIN , и тот не добавлен в монитор, данные о таком сертификате проверяться НЕ БУДУТ.

Troubleshooting

Если отчет не видит данных, подключитесь к серверу под пользователем nvsmon

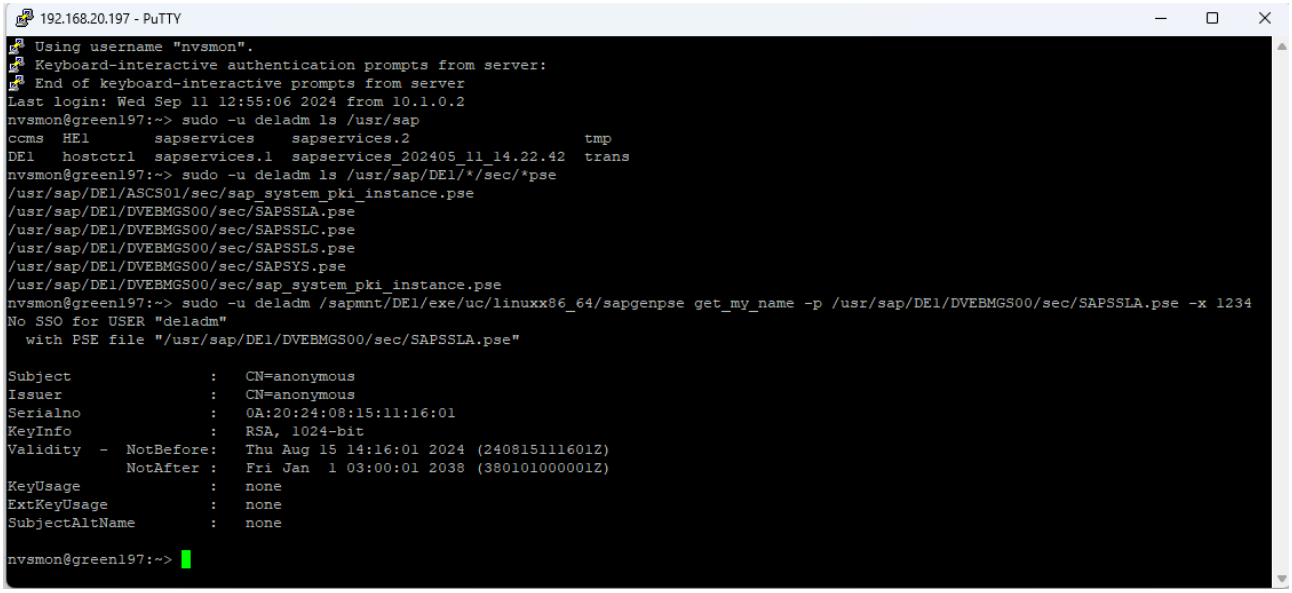
и попробуйте выполнить команды:

sudo -u de1adm find /usr/sap/DE1/ -name *.pse

sudo -u de1adm /sapmnt/DE1/exe/uc/linuxx86_64/sapgenpse get_my_name -p /usr/sap/DE1/DVEBMGS00/sec/SAPSSLA.pse -x 1234

где замените sid в примере это DE1 и путь до pse файла.

-x 1234 – это значение PIN – подставьте актуальное или оставьте по умолчанию (1234). Даже неправильное значение помогает избегать зависание на ожидании ввода.



Заключение

Данный отчет работает аналогично другим отчетам, получаемым данные через операционную систему путем запроса ssh. При отсутствии ответа от OS проверьте необходимые полномочия в файле /etc/sudoers.d/nvsmon