SharePoint Inventory

Inventory SharePoint farms

TITLE	SharePoint Inventory
AUTHOR	Docusnap Consulting
DATE	12/12/2023
VERSION	3.0	valid from 11/27/2023

CONTENTS

1. Introduction

This document describes the inventory of SharePoint farms (On-Premise!).

During the SharePoint inventory, problems can occur due to the use of PsExec. This document provides solutions to fix these problems, as well as alternatives for a successful inventory.

2. Requirements

For a successful and complete inventory of the SharePoint farm, a user is required to have administrative rights to all resources within the farm. By resources, we mean the following:

- Web application
  - Web page collection
    - Web pages
      - Lists and document libraries

Usually, this is the farm administrator. This refers to the user you used to install the SharePoint farm. The farm administrator usually also has permission to access the SharePoint database.

Even with this user, it is still not guaranteed that this user has permissions to all the previously mentioned resources! For example, it is possible to configure explicit administrators on each website collection.

If the user used does not have the complete permissions, the SharePoint inventory will be incomplete.

Further it is to be considered that for the inventory of the SharePoint farm PsExec is used. A PsExec connection to a SharePoint server is established and then the inventory is done.

The PsExec connection requires local administration permissions. If Microsoft's best practice approach is followed, the farm administrator will not have local administration permissions on the SharePoint server.

More detailed information about used ports, protocols and required permissions can be found in the whitepaper for inventories.

3. SharePoint Inventory

For the network inventory, start the SharePoint Scan Wizard:

- Discovery - All Wizards - SharePoint
- Inventory - All Wizards - SharePoint
- All Jobs - All Wizards - SharePoint

In step 2, a user with the previously described permissions is required - on the SharePoint server (local admin) as well as the SharePoint farm.

In step 3, a server is specified that is part of the SharePoint farm. It is not necessary to explicitly specify each farm server.

3.1 Sources of error

3.1.1 Incomplete inventory

The most common error is that the user used is not fully authorized on the SharePoint farm!

If you receive this message during the inventory, the user's authorizations must be checked again!
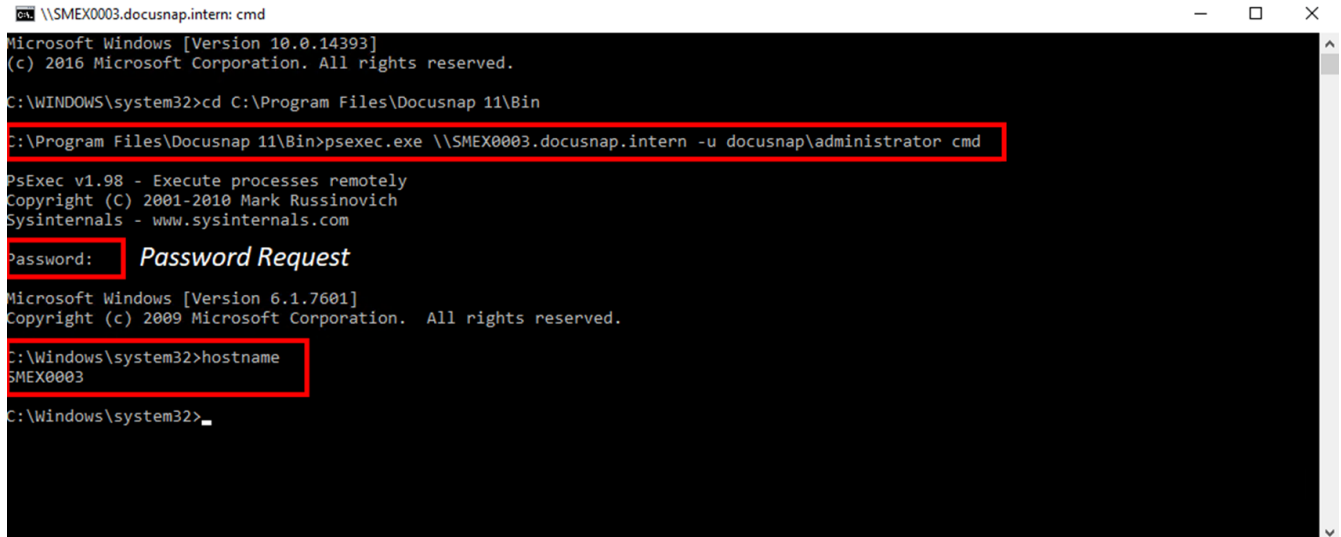
3.1.2 Check PsExec connection

As already described in chapter 2, PsExec is used for the SharePoint inventory.

PsExec is classified as dangerous by some anti-virus products (currently Sophos is especially known for this), which is why it is not allowed to run by default. None of the PsTools contain viruses, but were used by viruses, thus triggering the antivirus message.

Check PsExec connection:

- Open command line as administrator and go to the following path
    - C:\Program Files\Docusnap 13\Bin
- Now run PSExec with the following parameters
    - psexec.exe \\hostname cmd
        - by using the parameter -u domain\username - you can specify another user for the connection

Figure 1 - Check PsExec connection

If this connection cannot be established successfully, the anti-virus product on the target computer should be deactivated as a test. If the connection is now successful, PsExec must be enabled or allowed to run within the anti-virus product. If psexec.exe is not present in the installation directory, the local antivirus may have already deleted it or moved it to quarantine.

For more detailed testing options, see the HowTo Inventory - PSExec in our Knowledge Base.

3.1.3 Inventory file contains no information

If the Inventory file contains no information, no data could be inventoried from the SharePoint farm. The reasons for this can vary. The most common cause concerns authentication issues due to "**multi-hop**" when SharePoint and SQL server are running separately. In this case, installing a Discovery Service directly on SharePoint server or using the script variant will help.

More detailed information about this error message can be found in the Feedback_Farm.dat file. This file can be found in the folder
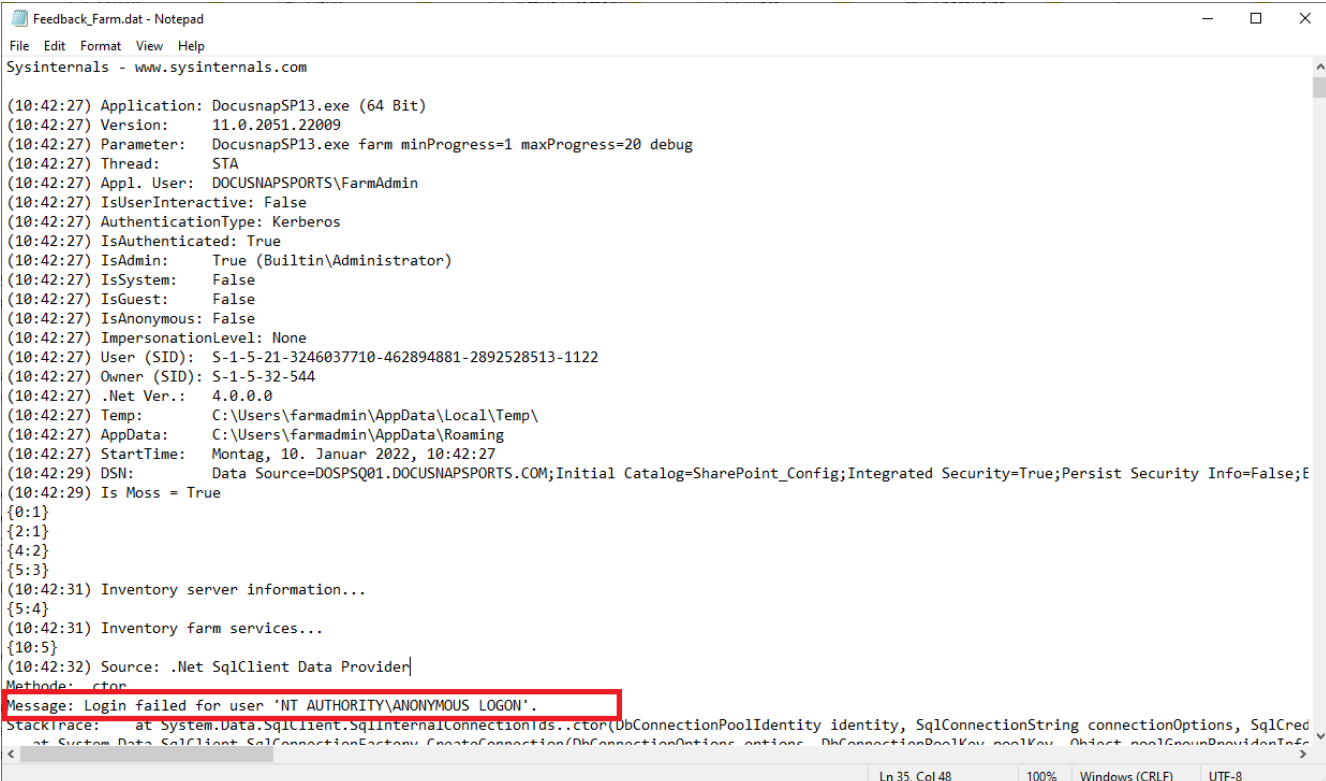
-   C:\ProgramData\Docusnap\Temp\Client   or   Server\"cryptic   folder"\Scan\SharePoint\SharePoint Server\"cryptic folder"
-   E.G.: C:\ProgramData\Docusnap\Temp\Client\kc0IMRHNn0KrTh7tUYuRfQ\scan\SharePoint\DSSP01\d35e 982e-f65b-493a-8868-15f7dfa20112

It is now important to distinguish which discovery service is doing the inventory. In each case, the file is located on the system on which this Discovery Service is running.

-   Client
-   server
-   Remote Discovery

An overview of the Discovery Services and on which systems they are executed can be found in the Docusnap Discovery Service Configuration - via the title bar:

Inside the Feedback_Farm.dat file you can now find the detailed information of the SharePoint inventory and more information why the inventory was not successful.

Figure 2 - Authentication problems multi-hop

```
*Feedback_Farm.dat - Notepad

File   Edit   Format   View   Help

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

(10:45:12 AM) Application: DocusnapSP13.exe (64 Bit)
(10:45:12 AM) Version:      11.0.2051.22009
(10:45:12 AM) Parameter:    DocusnapSP13.exe farm minProgress=1 maxProgress=20 debug
(10:45:12 AM) Thread:        STA
(10:45:12 AM) Appl. User:   DSRA\Administrator
(10:45:12 AM) IsUserInteractive: False
(10:45:12 AM) AuthenticationType: NTLM
(10:45:12 AM) IsAuthenticated: True
(10:45:12 AM) IsAdmin:       True (Builtin\Administrator)
(10:45:12 AM) IsSystem:      False
(10:45:12 AM) IsGuest:       False
(10:45:12 AM) IsAnonymous: False
(10:45:12 AM) ImpersonationLevel: None
(10:45:12 AM) User (SID):   S-1-5-21-3436755931-1367079096-3492215590-500
(10:45:12 AM) Owner (SID): S-1-5-32-544
(10:45:12 AM) .Net Ver.:    4.0.0.0
(10:45:12 AM) Temp:         C:\Users\administrator.DSRA\AppData\Local\Temp\
(10:45:12 AM) AppData:      C:\Users\administrator.DSRA\AppData\Roaming
(10:45:12 AM) StartTime:   Monday, January 10, 2022, 10:45:12 AM
(10:45:22 AM) Can't access Sharepoint SDK (Timeout)
Connecting to DSSP01.DSRA.LOCAL...


Starting PsExec service on DSSP01.DSRA.LOCAL...


Connecting with PsExec service on DSSP01.DSRA.LOCAL...


Copying C:\Program Files\Docusnap 11\Bin\DocusnapSP13.exe to DSSP01.DSRA.LOCAL...
```

Ln 30, Col 1   100%   Windows (CRLF)   UTF-8

Figure 3 - SharePoint SDK cannot be reached

4. Script-based SharePoint Inventory

Docusnap offers the possibility to run the SharePoint inventory locally. For this purpose, three executable files are available in the folder C:\Program Files\Docusnap 13\Tools:

- Discovery-Sharepoint-2007.exe - SharePoint Server 2007
- Discovery-Sharepoint-2010.exe - SharePoint Server 2010
- Discovery-Sharepoint.exe - SharePoint Server 2013 and higher

By using the script variant, the authentication problems due to multi-hop can be bypassed (SharePoint and SQL Server are run on separate systems).

4.1 Performing a Script-based Inventory

For the local SharePoint inventory to be performed, in the simplest case, the appropriate file must be copied to the system and run with a user, with the appropriate permissions on the SharePoint farm.

The result is a DSI file, which is then read by Docusnap using file import. The file import wizard can be found as follows:

- Discovery - All Wizards - File Import
- Inventory - All Wizards - File Import
- All Jobs - All Wizards - File Import

4.2 Parameters

If the executables are called with the parameter /help or /?, you will get an overview of all parameters.

The supposedly most important parameter is o=<path>. With this, the generated ZIP file can be placed on a central share and imported by Docusnap. More information can be found in the following chapter. It is important here that the executing user also has write permissions to the defined target path.

4.3 Automate script execution

The big advantage of Docusnap is that data is regularly and automatically inventoried and therefore up to date. This can also be achieved with script inventories.

The first step is to automate the execution of the script. Among other things, this can be done with a software distribution, as well as with Windows on-board means - task scheduling.

Switch to the Task Scheduler of your SharePoint server and create a new task.

In the **General** tab, enter a name and select the security options:

> Use the following user account: User with full SharePoint permissions (FarmAdmin)
>
> Run regardless of user logon
>
> Run with highest privileges
>
> Configure for: Select the appropriate operating system

In the **Trigger** tab, you can configure the script execution schedule - for example:

> Start Task: On a schedule
>
> Weekly, repeat every 1 week on: Sunday

In the **Actions** tab you define the execution of the Discovery-SharePoint.exe

> We recommend creating a hidden share on the Docusnap server / system that runs the Docusnap Discovery Service.
>
> On this share place the Discovery-SharePoint.exe and result file
>
> z. B.   \\SRV-Docu\DocusnapScript$\Scripts
>
> \\SRV-Docu\DocusnapScript$\Account Name#Domain.FQDN[1]
>
> Within this share / subfolder the executing user can read and write

> **Action**: Start program
>
> **Program / script**: \\SRV-Docu\DocusnapScript$\Scripts\Discovery-SharePoint.exe
>
> **Arguments**: -O "\\SRV-Docu\DocusnapScript$\Your Account#intern.local"
>
> > The -O parameter redirects the result files to the specified path. The user performing the inventory must have write permissions on this path.

The newly created task ensures that the inventory is run regularly and automatically.

....

[1] The specification of the folder structure corresponds to the standard of the multi-company import and causes that you are also prepared for possibly future scenarios.

It should always be ensured that the current version of the script file is used! This means that after an update of Docusnap you also exchange the script files! A best practice approach for this can be found in the chapter - Keeping used script files up to date.

The next step is to set up the import of the inventory as a job. Note that during an import job, you can also automatically import the results of the other script-based inventories.

Open the Script Import Wizard:

- Discovery - All Wizards – File Import.
- Inventory - All Wizards - File Import
- All Orders - All Wizards - File Import

In **step 1**, select your company or your customer's company.

In **step 2**, select the Docusnap Server service or a discovery service you created.

In **step 3**, select the directory where the generated result file will be stored:

> In the recommended configuration, this folder is located locally on the Docusnap Server or on the system that provides the discovery service

> Additional directories can also be added for the remaining script executions

In **step 6**, you configure the scheduling.

Besides the simple script import, you can also use the global script import. This allows you to import scripts for multiple companies and/or domains at the same time.

4.4 Keeping used script files up to date

We generally recommend installing a Docusnap Discovery Service (DDS) at least on the system where the Docusnap Server has been configured when using one / the script variants. Additional DDSs can be placed in the decentralized networks (sites, VLANs, etc.).

In the DDS settings, you can specify an additional directory for storing the inventory modules (script files). This causes the script files to be automatically replaced when Docusnap is updated, so they are always up-to-date.

Install and configure the DDS - a HowTo can be found in our Knowledge Base.

After configuration, go to the Settings tab and set the storage directory:

- C:\DocusnapScript\Scripts.

Then share the folder over the network: \\SRV-Docu\DocusnapScript$.

You can use this share again to call the script file

- \\SRV-Docu\DocusnapScript$\Scripts\Discovery-SharePoint.exe

and to store the JSON files:

- \\SRV-Docu\DocusnapScript$\Company#Domain.FQDN

LIST OF FIGURES

Version history

Date	Description
January 11, 2022	Version 1.0 HowTo created
December 22, 2022	Version 2.0 – Revision for Docusnap 12
November 27, 2023	Version 3.0 - Revision of the HowTo for Docusnap 13