Inventory - PSExec

Inventories via PSExec – Analysis and Bug Fixes

TITLE	Inventory - PSExec
AUTHOR	Docusnap Consulting
DATE	8/2/2022
VERSION	1.1 | valid from 7/12/2022

CONTENTS

1. Introduction

PSExec is used for the following scans:

- Exchange
- SharePoint
- GPO
- Windows Fallback scan

By default, PSExec is located in one of the following directories:

- Docusnap Server and Client
  - %ProgramFiles%\Docusnap 11\bin\psexec.exe
- Optional: Discovery Service
  - %ProgramData%\Docusnap\Discovery\discovery\plugins\AUFZÄHLENDER-ORDNER\Bin\psexec.exe
  - %ProgramFiles%\Docusnap Discovery\bin\psexec.exe

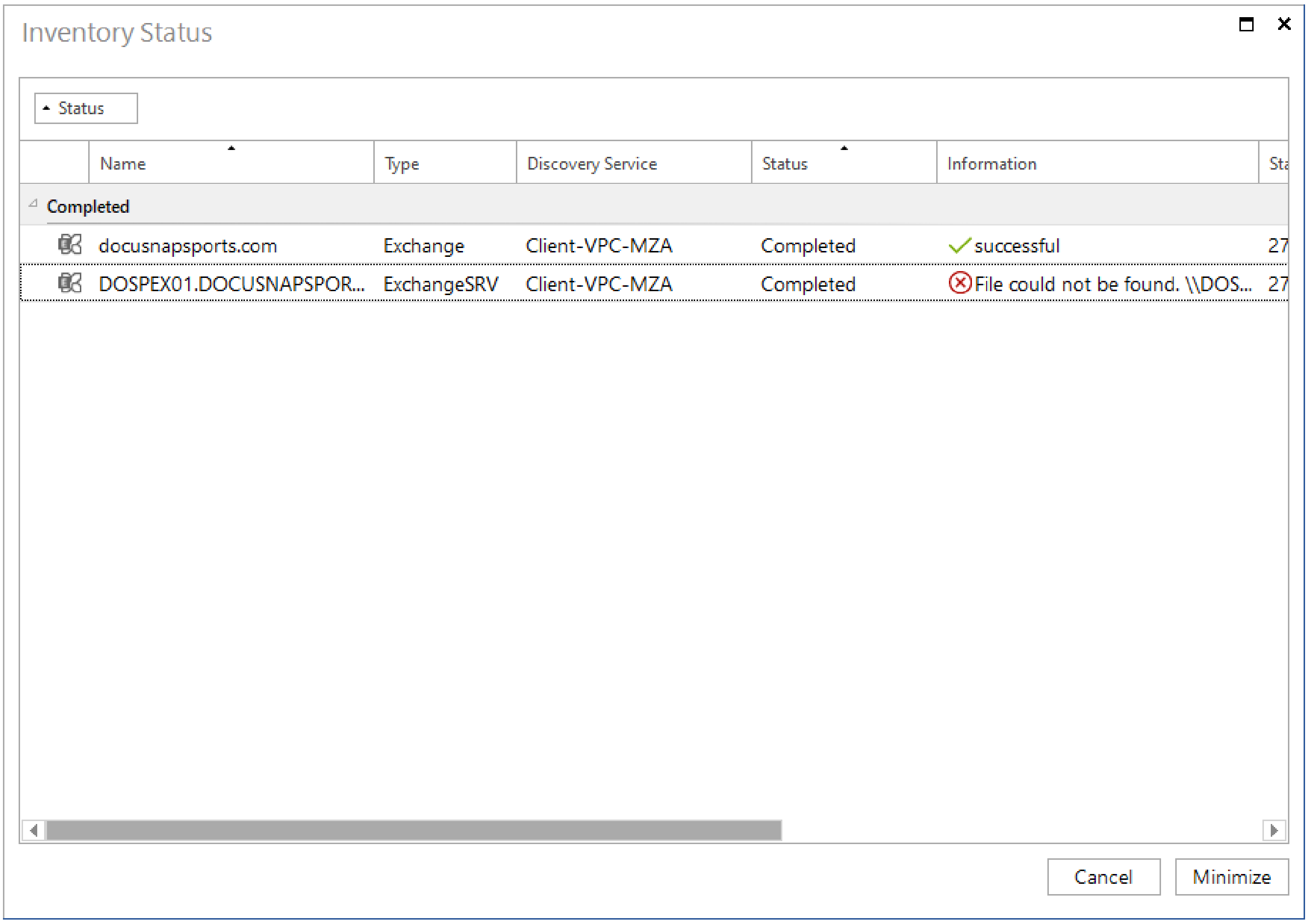
If Docusnap was installed in a different directory, this path may be different.

PSExec establishes a connection to the inventory system and copies the inventory file to the system. After the scan, the result file is copied back to the Docusnap server and imported there. Therefore, it is necessary to be able to establish a PSExec connection to the inventory system. This HowTo describes the analysis of a failing PSExec connection, as well as troubleshooting.

- In chapter 2 the error message *File could not be found* is discussed
- Chapter 3 describes a solution approach for the message Mount of remote share failed

2. File could not be found

If no PSExec connection is possible, in most cases the error message **File could not be found** is displayed. This error can have different reasons



Inventory Status

Status

Name	Type	Discovery Service	Status	Information	Sta
Completed					
docusnapsports.com	Exchange	Client-VPC-MZA	Completed	✓ successful	27
DOSPEX01.DOCUSNAPSPOR...	ExchangeSRV	Client-VPC-MZA	Completed	⊗ File could not be found. \\DOS...	27

Figure 1 - File could not be found

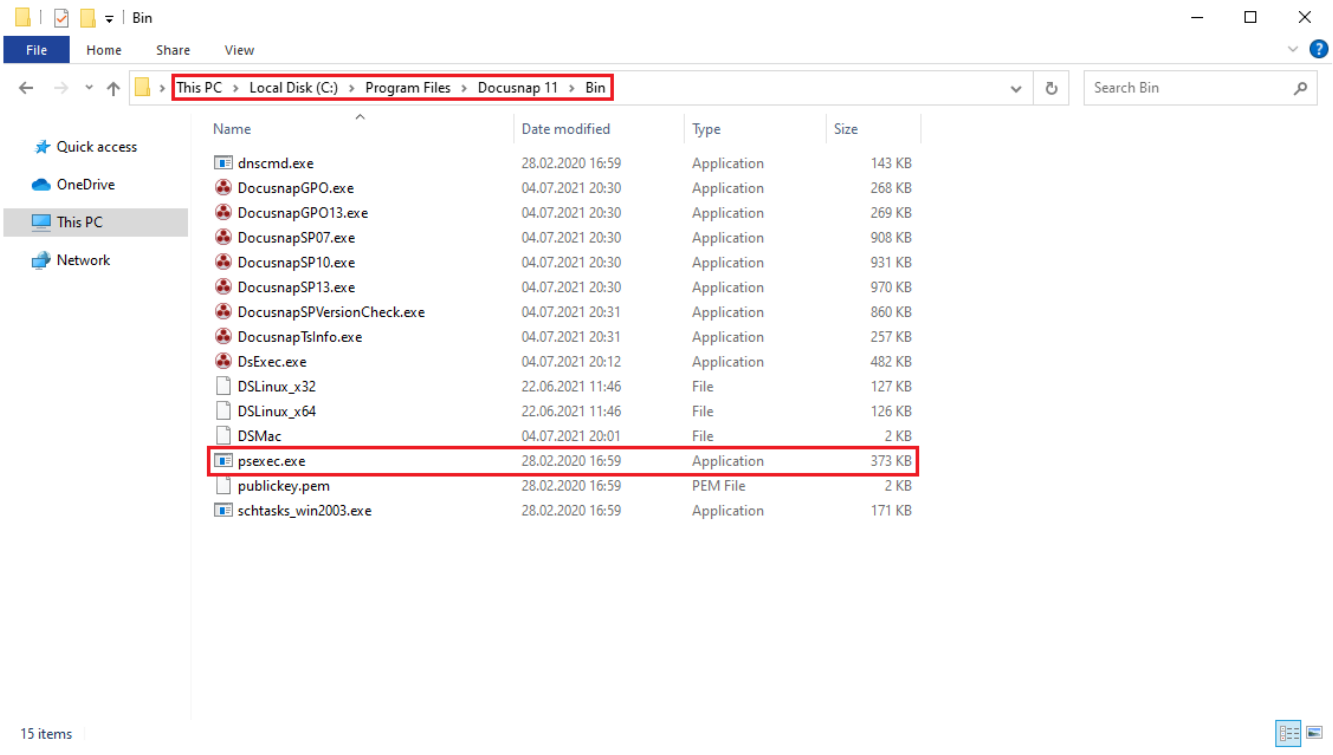
2.1 Connection test

If this error is displayed, a manual PSExec connection test to the target system should be performed first.

It is important that the test is performed with the same user that is used for the scan.

To do this, first run CMD or PowerShell in the appropriate user context.

PSExec is located in the installation directory of Docusnap in the Bin folder - e.g. C:\Program Files\Docusnap 11\Bin.



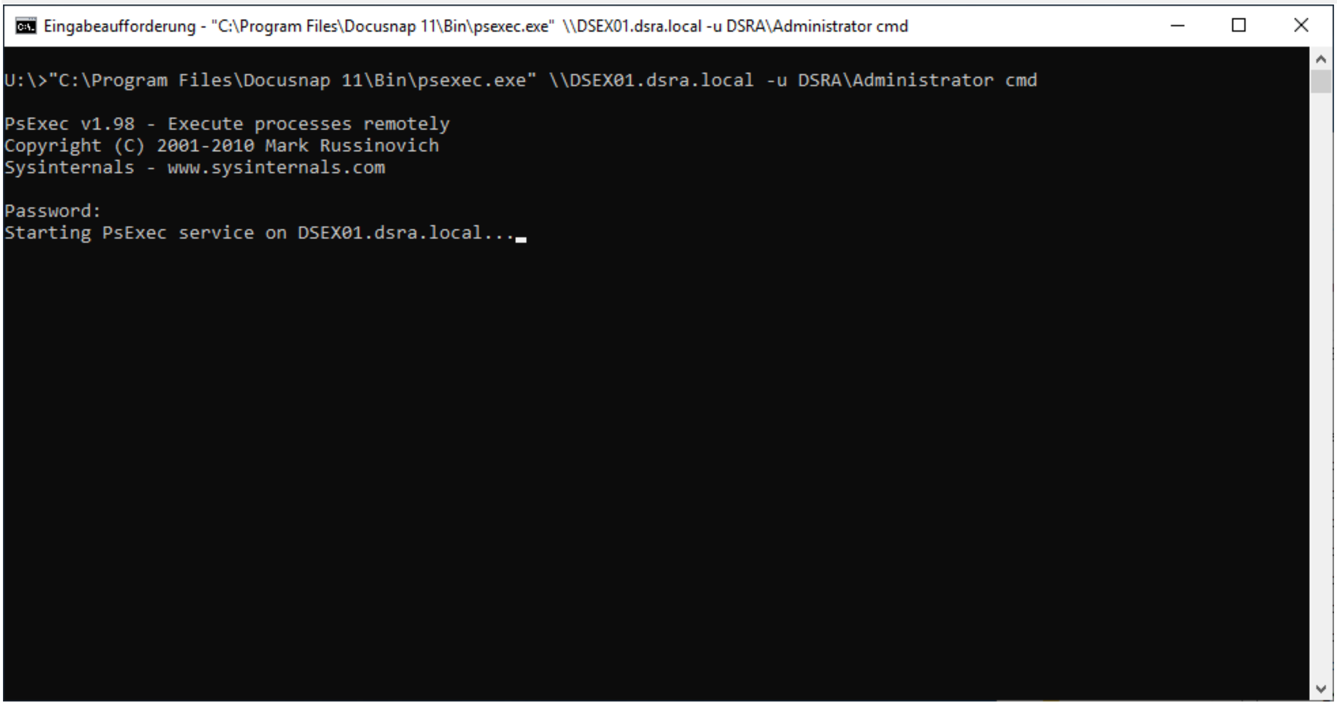
This PC › Local Disk (C:) › Program Files › Docusnap 11 › Bin

Name	Date modified	Type	Size
dnscmd.exe	28.02.2020 16:59	Application	143 KB
DocusnapGPO.exe	04.07.2021 20:30	Application	268 KB
DocusnapGPO13.exe	04.07.2021 20:30	Application	269 KB
DocusnapSP07.exe	04.07.2021 20:30	Application	908 KB
DocusnapSP10.exe	04.07.2021 20:30	Application	931 KB
DocusnapSP13.exe	04.07.2021 20:30	Application	970 KB
DocusnapSPVersionCheck.exe	04.07.2021 20:31	Application	860 KB
DocusnapTsInfo.exe	04.07.2021 20:31	Application	257 KB
DsExec.exe	04.07.2021 20:12	Application	482 KB
DSLinux_x32	22.06.2021 11:46	File	127 KB
DSLinux_x64	22.06.2021 11:46	File	126 KB
DSMac	04.07.2021 20:01	File	2 KB
psexec.exe	28.02.2020 16:59	Application	373 KB
publickey.pem	28.02.2020 16:59	PEM File	2 KB
schtasks_win2003.exe	28.02.2020 16:59	Application	171 KB

Figure 2 - PSExec Path

The connection test is performed via the following command:

```
psexec.exe \\TargetSystem -u Domain\User cmd
```



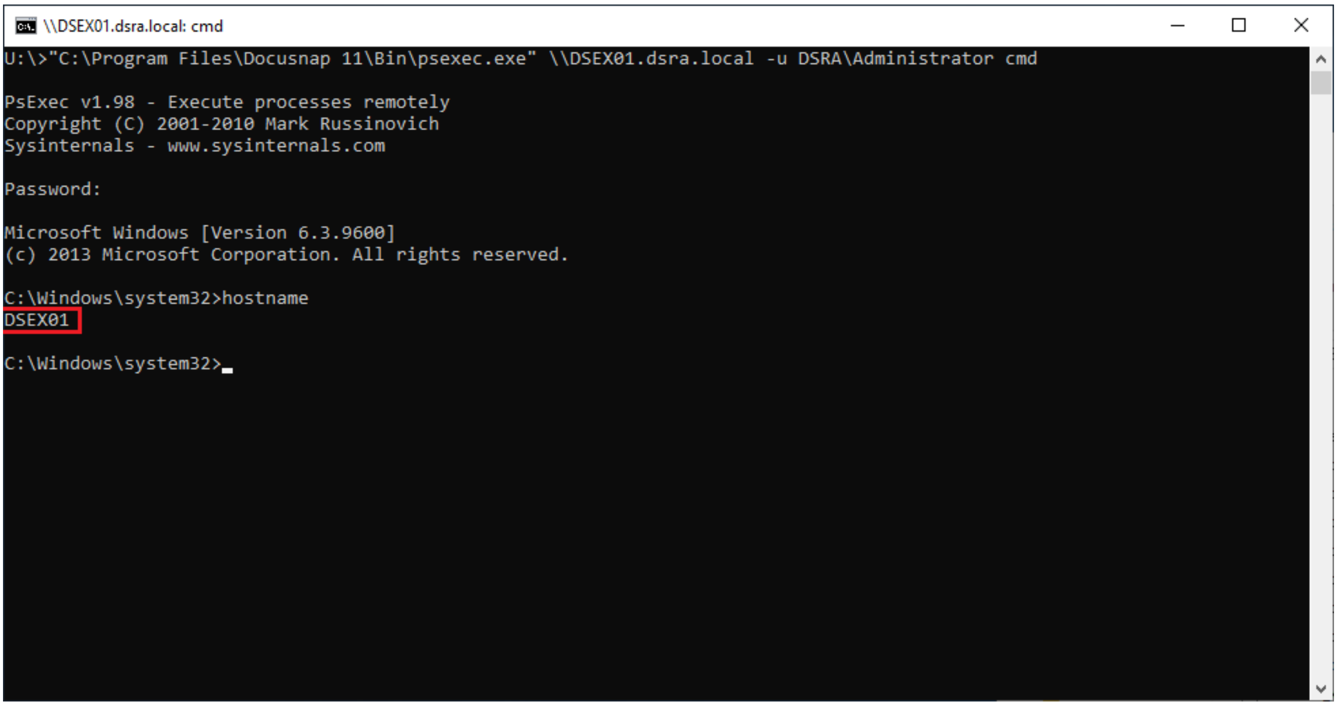
Eingabeaufforderung - "C:\Program Files\Docusnap 11\Bin\psexec.exe" \\DSEX01.dsra.local -u DSRA\Administrator cmd

```
U:\>"C:\Program Files\Docusnap 11\Bin\psexec.exe" \\DSEX01.dsra.local -u DSRA\Administrator cmd

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

Password:
Starting PsExec service on DSEX01.dsra.local..._
```

Figure 3 - PSExec Connection Test

There is no feedback during the password entry.

If the connection is successful, the **hostname** command can also be executed. As a result, the host name of the remote system should be displayed.



\\DSEX01.dsra.local: cmd

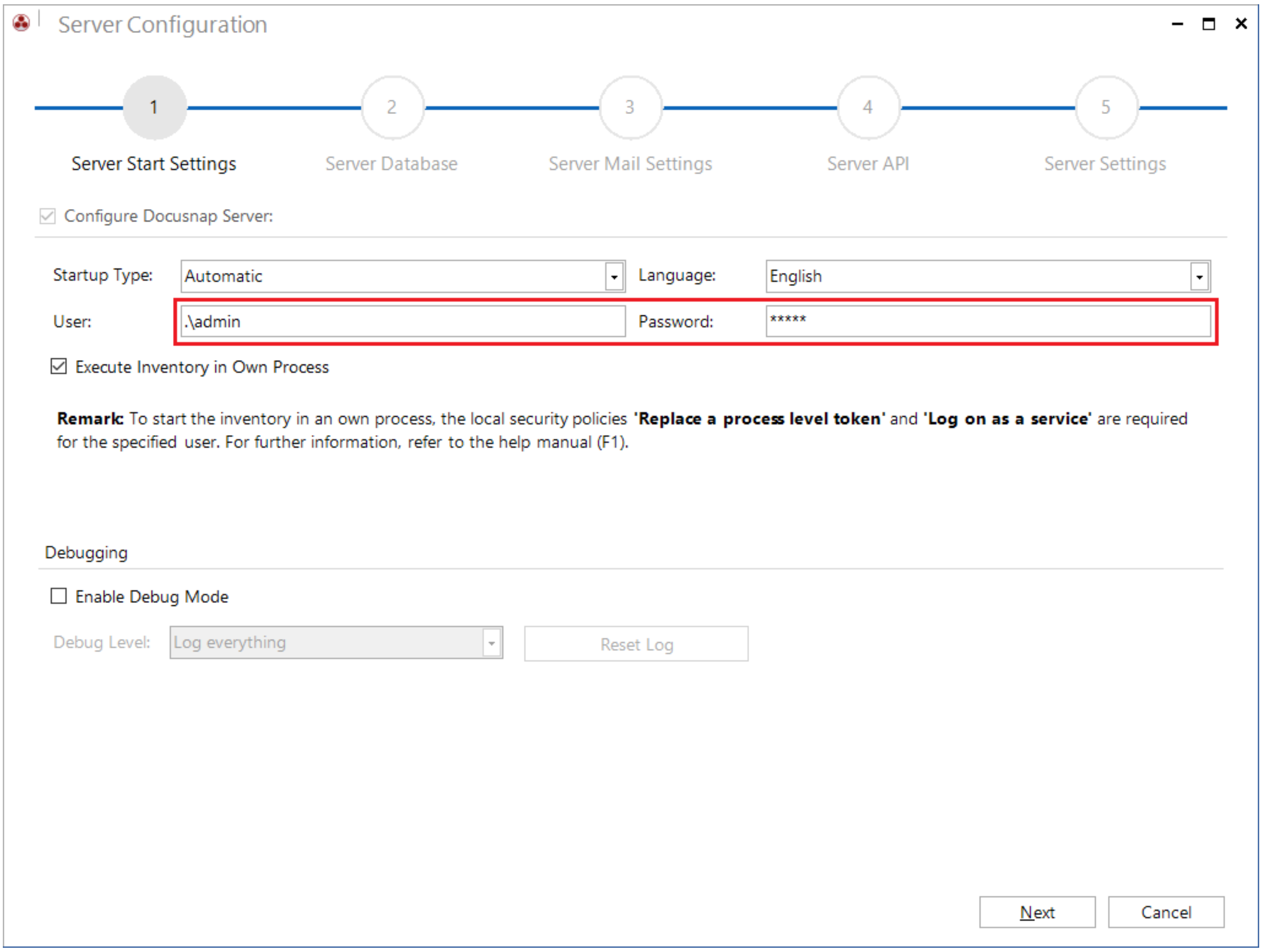
```
U:\>"C:\Program Files\Docusnap 11\Bin\psexec.exe" \\DSEX01.dsra.local -u DSRA\Administrator cmd

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

Password:

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
DSEX01

C:\Windows\system32>_
```

Figure 4 - PSExec Hostname

2.1.1 Connection test successful

If the connection test is successful, problems on the part of PSExec can be excluded.

In this case, the Docusnap server configuration should be checked. In the first step of the server configuration, it is possible to define a user.



☑ Configure Docusnap Server:

Startup Type: Automatic

Language: English

User: .\admin

Password: *****

☑ Execute Inventory in Own Process

Remark: To start the inventory in an own process, the local security policies '**Replace a process level token**' and '**Log on as a service**' are required for the specified user. For further information, refer to the help manual (F1).

Debugging

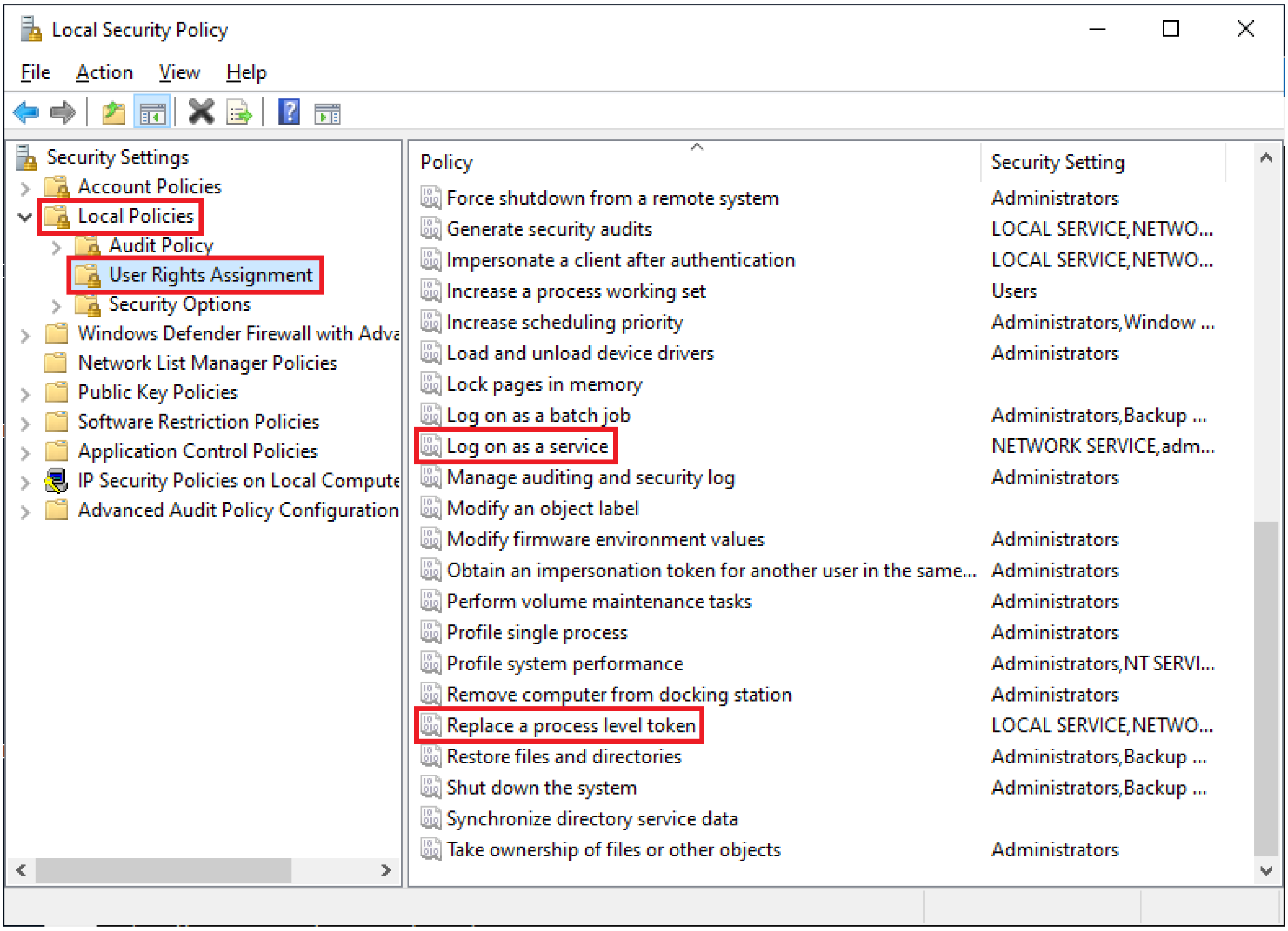
☐ Enable Debug Mode

Debug Level: Log everything

Figure 5 - Docusnap Server Configuration

If a user is set here, it should be checked whether this user is set in the required local security policies **Log on as a service** and **Replace a process level token**.

1. Open Local Security Policies via Windows search with **secpol.msc**
2. Local Policies
3. User Rights Assignment
4. Open **Log on as service** and check if the server service user is set
5. Open **Replace a process level toke**_n_ and check if the server service user is set

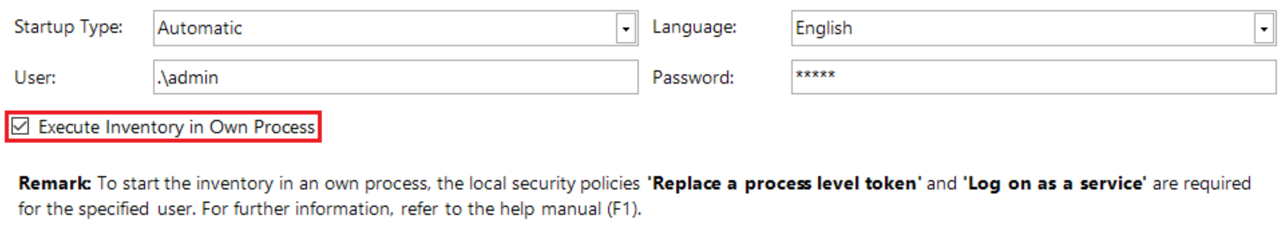


- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Defender Firewall with Adva
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Policy	Security Setting
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWO...
Impersonate a client after authentication	LOCAL SERVICE,NETWO...
Increase a process working set	Users
Increase scheduling priority	Administrators,Window ...
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	Administrators,Backup ...
Log on as a service	NETWORK SERVICE,adm...
Manage auditing and security log	Administrators
Modify an object label	
Modify firmware environment values	Administrators
Obtain an impersonation token for another user in the same...	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Profile system performance	Administrators,NT SERVI...
Remove computer from docking station	Administrators
Replace a process level token	LOCAL SERVICE,NETWO...
Restore files and directories	Administrators,Backup ...
Shut down the system	Administrators,Backup ...
Synchronize directory service data	
Take ownership of files or other objects	Administrators

Figure 6 - Local Security Policies

If all security policies are already set, you can check in the Docusnap Server configuration if the option **Execute Inventory in Own Process** is enabled. This should be set.



Startup Type:	Automatic	Language:	English
User:	.\admin	Password:	*****

☑ Execute Inventory in Own Process

Remark: To start the inventory in an own process, the local security policies '**Replace a process level token**' and '**Log on as a service**' are required for the specified user. For further information, refer to the help manual (F1).

Figure 7 - Execute Inventory in Own Process

2.1.2 Connection test failed

If the connection test fails, the following steps should be checked.

Permissions

A user who is a local administrator on the target system must be used for the connection.

Antivirus

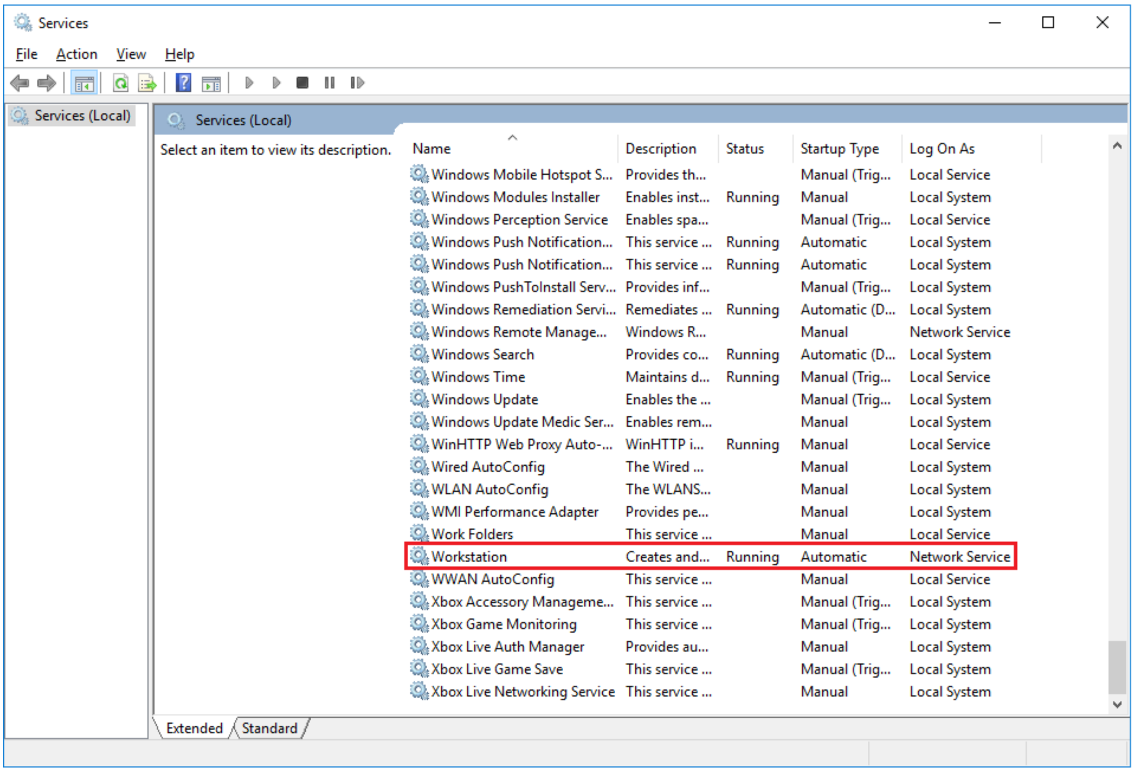
Often the connection fails because PSExec is blocked by the installed antivirus solution. Usually, a warning message appears in the antivirus console on the system that the execution of PSExec has been blocked.

Sometimes it can also happen that the PSExec.exe is deleted on the Docusnap system. In this case, PSExec will no longer be in the corresponding path at all.

To prevent this error in the future, an exception for PSExec must be set up in the antivirus solution.

Services

If a workstation is scanned, the workstation service must be executed.

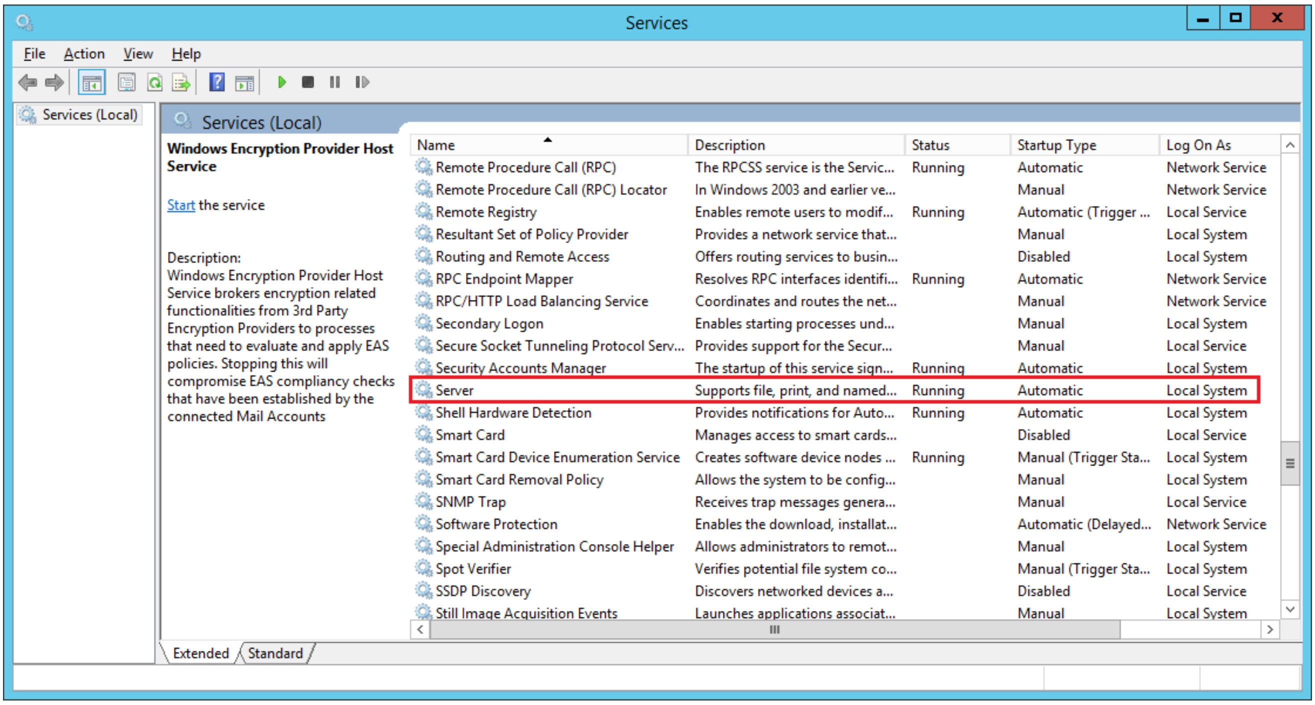


Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
Windows Mobile Hotspot S...	Provides th...		Manual (Trig...	Local Service
Windows Modules Installer	Enables inst...	Running	Manual	Local System
Windows Perception Service	Enables spa...		Manual (Trig...	Local Service
Windows Push Notification...	This service ...	Running	Automatic	Local System
Windows Push Notification...	This service ...	Running	Automatic	Local System
Windows PushToInstall Serv...	Provides inf...		Manual (Trig...	Local System
Windows Remediation Servi...	Remediates ...	Running	Automatic (D...	Local System
Windows Remote Manage...	Windows R...		Manual	Network Service
Windows Search	Provides co...	Running	Automatic (D...	Local System
Windows Time	Maintains d...	Running	Manual (Trig...	Local Service
Windows Update	Enables the ...		Manual (Trig...	Local System
Windows Update Medic Ser...	Enables rem...		Manual	Local System
WinHTTP Web Proxy Auto-...	WinHTTP i...	Running	Manual	Local Service
Wired AutoConfig	The Wired ...		Manual	Local System
WLAN AutoConfig	The WLANS...		Manual	Local System
WMI Performance Adapter	Provides pe...		Manual	Local System
Work Folders	This service ...		Manual	Local Service
Workstation	Creates and...	Running	Automatic	Network Service
WWAN AutoConfig	This service ...		Manual	Local Service
Xbox Accessory Manageme...	This service ...		Manual (Trig...	Local System
Xbox Game Monitoring	This service ...		Manual (Trig...	Local System
Xbox Live Auth Manager	Provides au...		Manual	Local System
Xbox Live Game Save	This service ...		Manual (Trig...	Local System
Xbox Live Networking Service	This service ...		Manual	Local System

Figure 8 - Workstation Service

On a server, this is the server service



Services (Local)

Windows Encryption Provider Host Service

Start the service

Description:
Windows Encryption Provider Host Service brokers encryption related functionalities from 3rd Party Encryption Providers to processes that need to evaluate and apply EAS policies. Stopping this will compromise EAS compliancy checks that have been established by the connected Mail Accounts

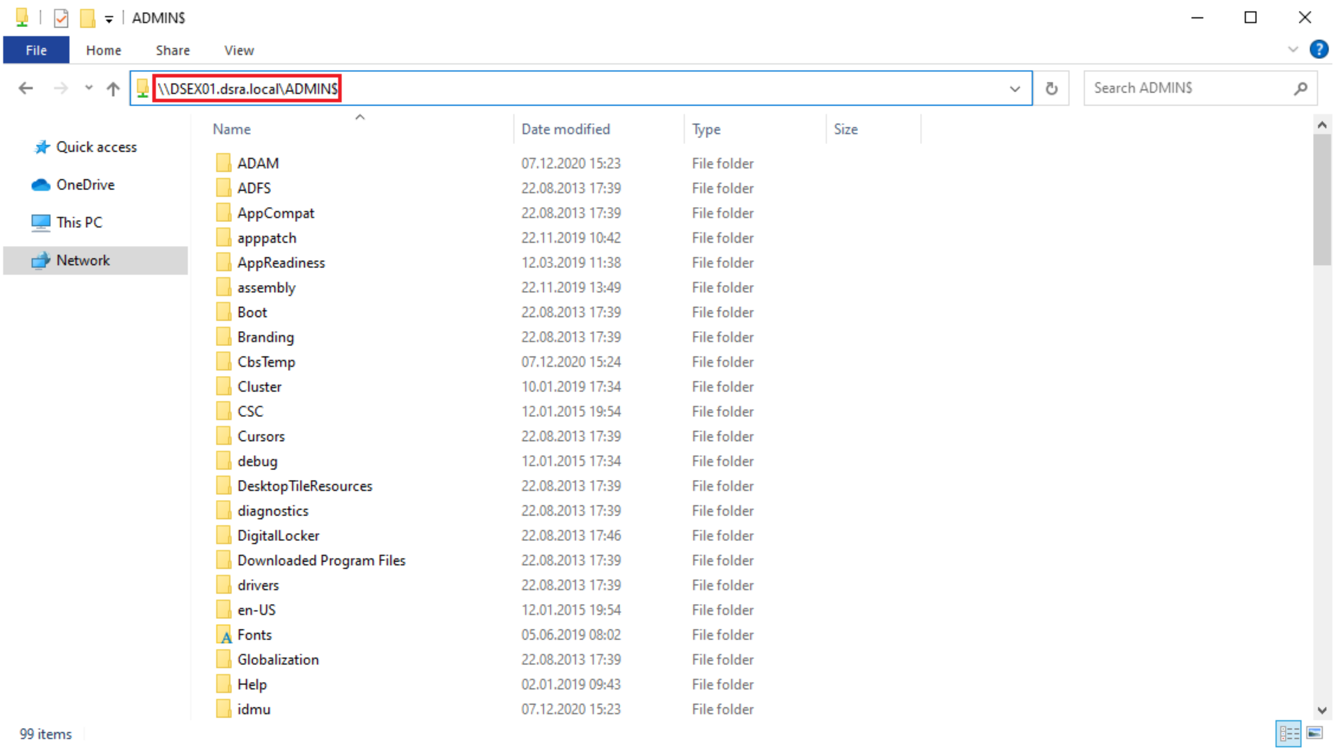
Name	Description	Status	Startup Type	Log On As
Remote Procedure Call (RPC)	The RPCSS service is the Servic...	Running	Automatic	Network Service
Remote Procedure Call (RPC) Locator	In Windows 2003 and earlier ve...		Manual	Network Service
Remote Registry	Enables remote users to modif...	Running	Automatic (Trigger ...	Local Service
Resultant Set of Policy Provider	Provides a network service that...		Manual	Local System
Routing and Remote Access	Offers routing services to busin...		Disabled	Local System
RPC Endpoint Mapper	Resolves RPC interfaces identifi...	Running	Automatic	Network Service
RPC/HTTP Load Balancing Service	Coordinates and routes the net...		Manual	Network Service
Secondary Logon	Enables starting processes und...		Manual	Local System
Secure Socket Tunneling Protocol Serv...	Provides support for the Secur...		Manual	Local Service
Security Accounts Manager	The startup of this service sign...	Running	Automatic	Local System
Server	Supports file, print, and named...	Running	Automatic	Local System
Shell Hardware Detection	Provides notifications for Auto...	Running	Automatic	Local System
Smart Card	Manages access to smart cards...		Disabled	Local Service
Smart Card Device Enumeration Service	Creates software device nodes ...	Running	Manual (Trigger Sta...	Local System
Smart Card Removal Policy	Allows the system to be config...		Manual	Local System
SNMP Trap	Receives trap messages genera...		Manual	Local Service
Software Protection	Enables the download, installat...		Automatic (Delayed...	Network Service
Special Administration Console Helper	Allows administrators to remot...		Manual	Local System
Spot Verifier	Verifies potential file system co...		Manual (Trigger Sta...	Local System
SSDP Discovery	Discovers networked devices a...		Disabled	Local Service
Still Image Acquisition Events	Launches applications associat...		Manual	Local System

Figure 9 - Server Service

Share

The ADMIN$ share must be available on the target system.

This can be tested via Windows Explorer.



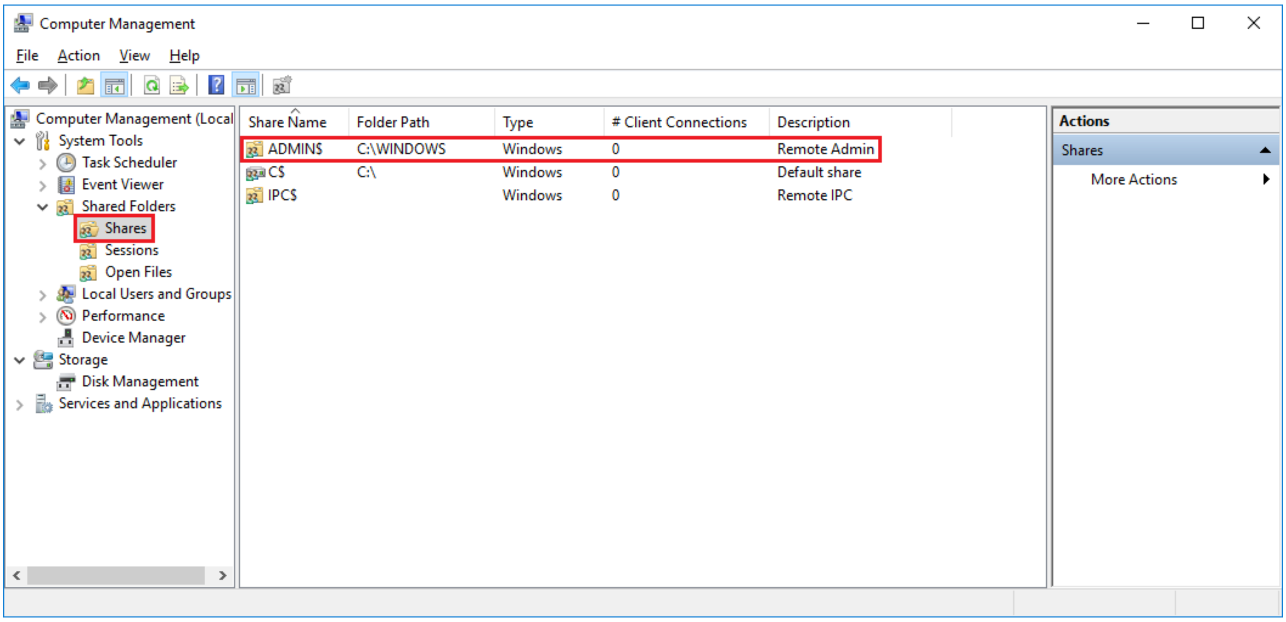
\\DSEX01.dsra.local\ADMIN$

Name	Date modified	Type	Size
ADAM	07.12.2020 15:23	File folder	
ADFS	22.08.2013 17:39	File folder	
AppCompat	22.08.2013 17:39	File folder	
apppatch	22.11.2019 10:42	File folder	
AppReadiness	12.03.2019 11:38	File folder	
assembly	22.11.2019 13:49	File folder	
Boot	22.08.2013 17:39	File folder	
Branding	22.08.2013 17:39	File folder	
CbsTemp	07.12.2020 15:24	File folder	
Cluster	10.01.2019 17:34	File folder	
CSC	12.01.2015 19:54	File folder	
Cursors	22.08.2013 17:39	File folder	
debug	12.01.2015 17:34	File folder	
DesktopTileResources	22.08.2013 17:39	File folder	
diagnostics	22.08.2013 17:39	File folder	
DigitalLocker	22.08.2013 17:46	File folder	
Downloaded Program Files	22.08.2013 17:39	File folder	
drivers	22.08.2013 17:39	File folder	
en-US	12.01.2015 19:54	File folder	
Fonts	05.06.2019 08:02	File folder	
Globalization	22.08.2013 17:39	File folder	
Help	02.01.2019 09:43	File folder	
idmu	07.12.2020 15:23	File folder	

99 items

Figure 10 - Windows Explorer

The share can also be checked directly on the target system via the Computer Management.



Computer Management

Computer Management (Local
- System Tools
  - Task Scheduler
  - Event Viewer
  - Shared Folders
    - Shares
    - Sessions
    - Open Files
  - Local Users and Groups
  - Performance
  - Device Manager
- Storage
  - Disk Management
- Services and Applications

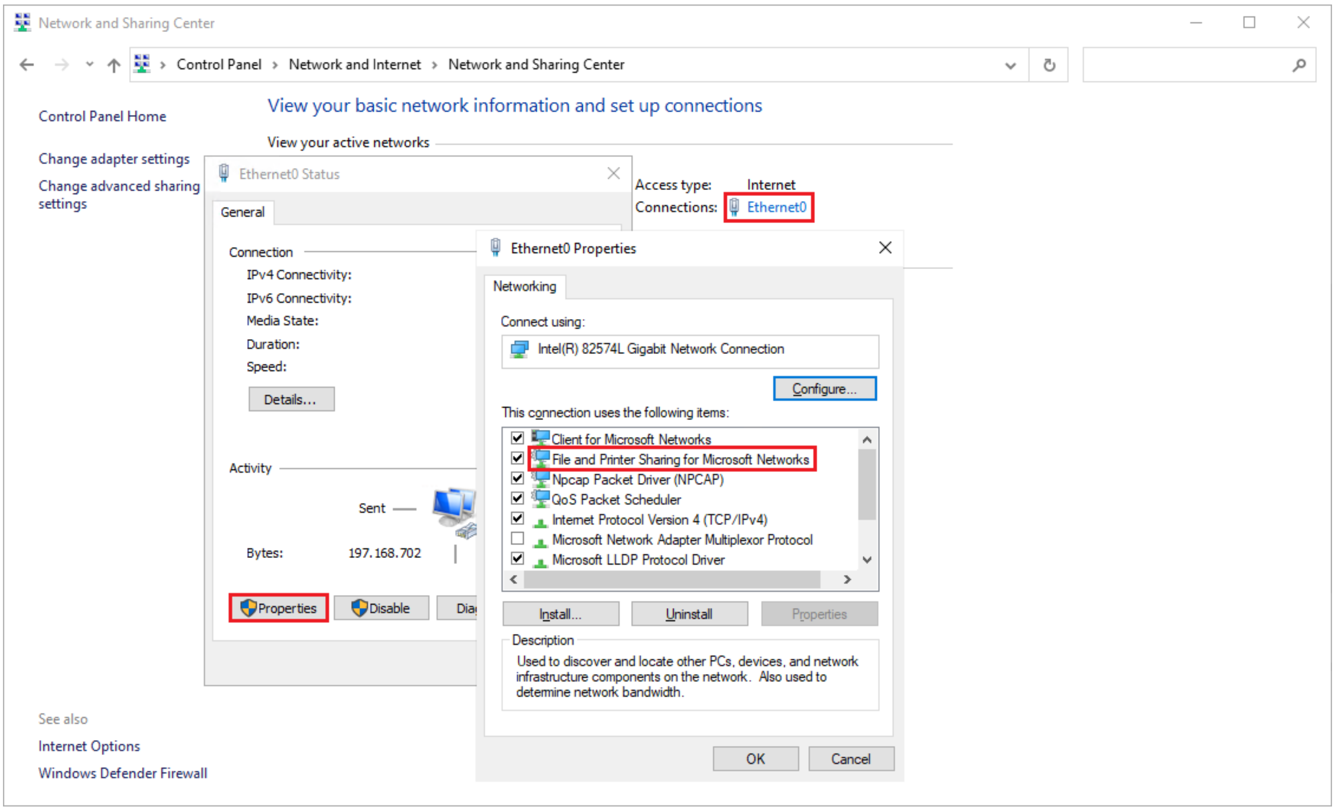
Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\WINDOWS	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC

Figure 11 - Computer Management

Windows Network

File and printer sharing must be enabled on the target system.

This can be checked on the target system via the Network and Sharing Center. To do this, open the Control Panel and select the Network and Sharing Center.



Network and Sharing Center

Control Panel > Network and Internet > Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
Internet Options
Windows Defender Firewall

View your basic network information and set up connections

View your active networks

Access type: Internet
Connections: Ethernet0

Ethernet0 Status

Connection
IPv4 Connectivity:
IPv6 Connectivity:
Media State:
Duration:
Speed:

Activity
Sent
Bytes: 197.168.702

Ethernet0 Properties

Connect using:
Intel(R) 82574L Gigabit Network Connection

This connection uses the following items:
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Description
Used to discover and locate other PCs, devices, and network infrastructure components on the network. Also used to determine network bandwidth.

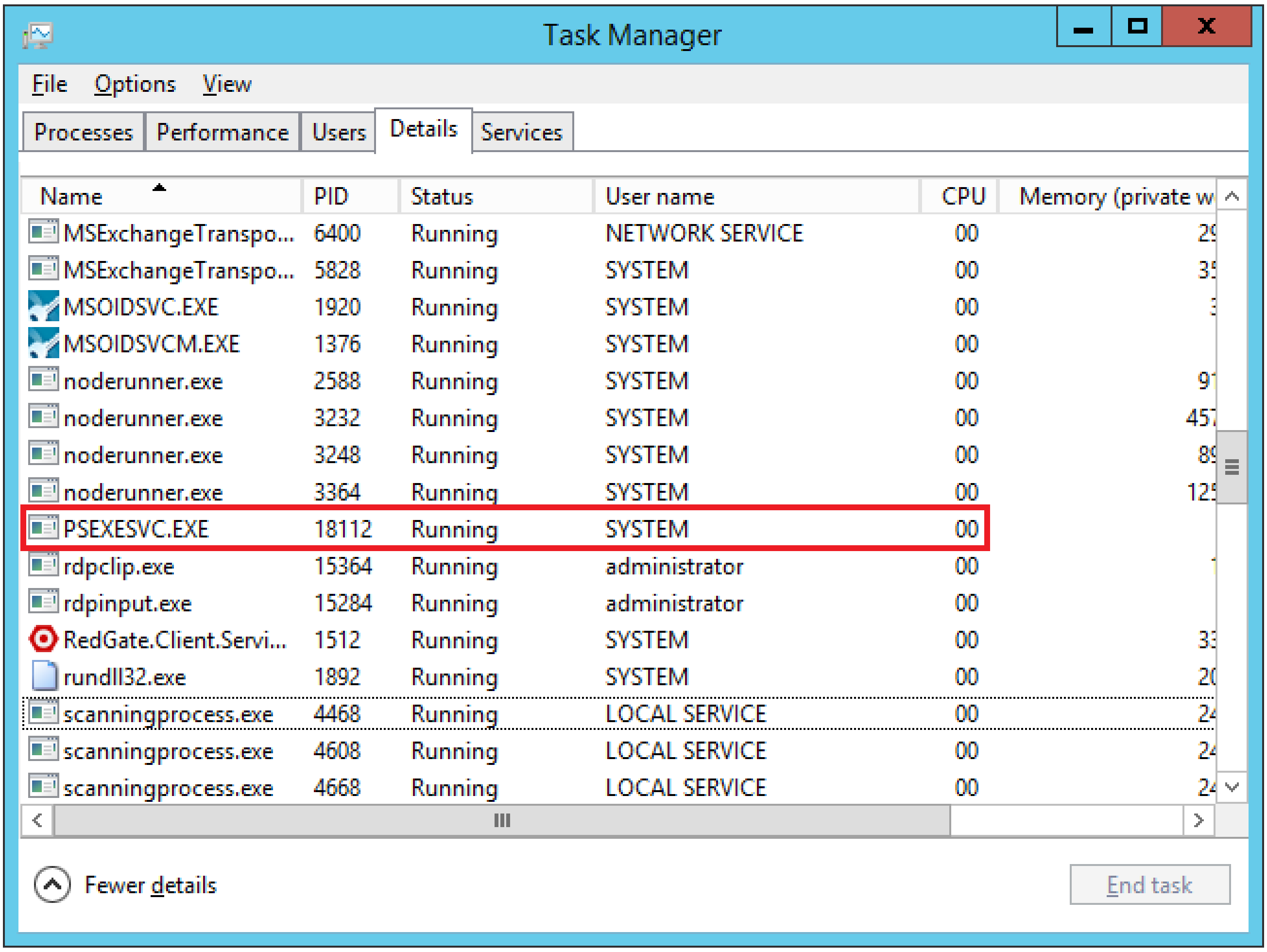
Figure 12 - File and Printer Sharing

Process is already running

Only one PSExec process can be executed per system simultaneously.

On the target system, it should be checked whether the *PSExecSVC.exe* process or a Docusnap process is running - for example, the Exchange scan runs the *DocusnapEX13.exe* process.

If one of the two processes is still active, it should be terminated manually and the connection test repeated.



Name	PID	Status	User name	CPU	Memory (private w
MSExchangeTranspo...	6400	Running	NETWORK SERVICE	00	29
MSExchangeTranspo...	5828	Running	SYSTEM	00	35
MSOIDSVC.EXE	1920	Running	SYSTEM	00	3
MSOIDSVCM.EXE	1376	Running	SYSTEM	00	
noderunner.exe	2588	Running	SYSTEM	00	91
noderunner.exe	3232	Running	SYSTEM	00	457
noderunner.exe	3248	Running	SYSTEM	00	89
noderunner.exe	3364	Running	SYSTEM	00	125
PSEXESVC.EXE	18112	Running	SYSTEM	00	
rdpclip.exe	15364	Running	administrator	00	1
rdpinput.exe	15284	Running	administrator	00	
RedGate.Client.Servi...	1512	Running	SYSTEM	00	33
rundll32.exe	1892	Running	SYSTEM	00	20
scanningprocess.exe	4468	Running	LOCAL SERVICE	00	24
scanningprocess.exe	4608	Running	LOCAL SERVICE	00	24
scanningprocess.exe	4668	Running	LOCAL SERVICE	00	24

Figure 13 - PSExec Service

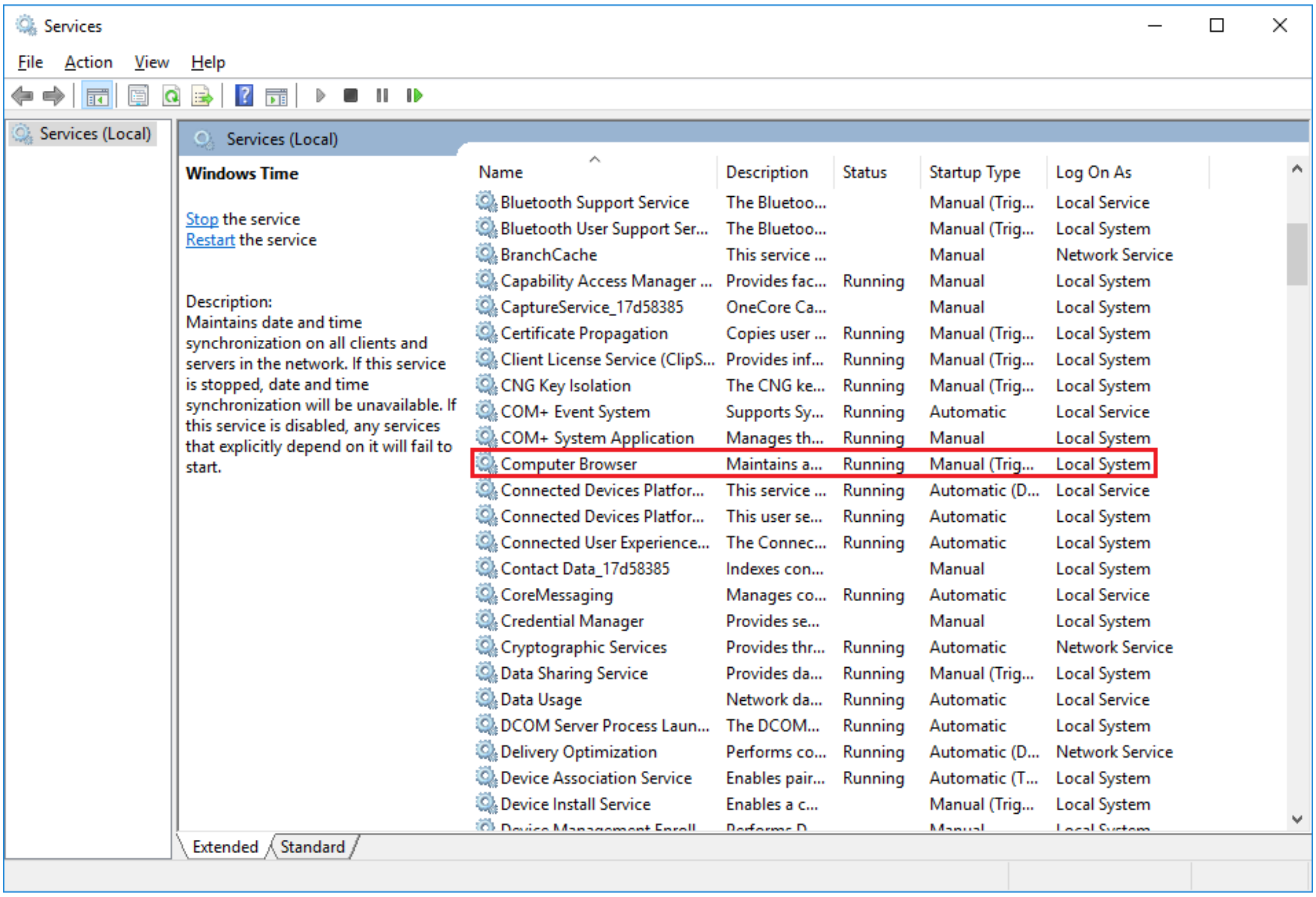
Windows Updates

If all steps have been checked successfully and the inventory still fails, you should check whether Windows updates are still pending on the target system.

3. Mount of remote share failed

In some cases, the message **Mount of remote share failed** is displayed.

On the system that performs the inventory, it should be checked whether the *Computer Browser* service is active.



Windows Time

Stop the service
Restart the service

Description:
Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

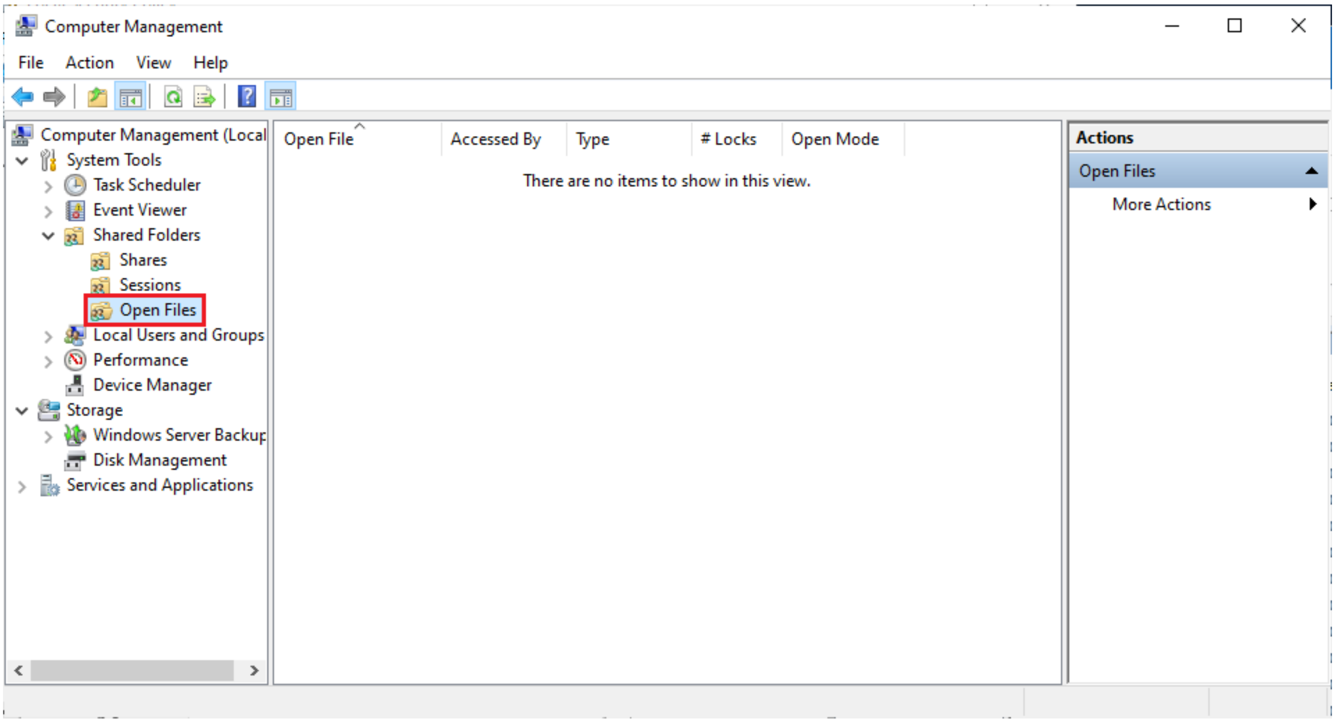
Name	Description	Status	Startup Type	Log On As
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Local Service
Bluetooth User Support Ser...	The Bluetoo...		Manual (Trig...	Local System
BranchCache	This service ...		Manual	Network Service
Capability Access Manager ...	Provides fac...	Running	Manual	Local System
CaptureService_17d58385	OneCore Ca...		Manual	Local System
Certificate Propagation	Copies user ...	Running	Manual (Trig...	Local System
Client License Service (ClipS...	Provides inf...	Running	Manual (Trig...	Local System
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local System
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Running	Manual	Local System
Computer Browser	Maintains a...	Running	Manual (Trig...	Local System
Connected Devices Platfor...	This service ...	Running	Automatic (D...	Local Service
Connected Devices Platfor...	This user se...	Running	Automatic	Local System
Connected User Experience...	The Connec...	Running	Automatic	Local System
Contact Data_17d58385	Indexes con...		Manual	Local System
CoreMessaging	Manages co...	Running	Automatic	Local Service
Credential Manager	Provides se...		Manual	Local System
Cryptographic Services	Provides thr...	Running	Automatic	Network Service
Data Sharing Service	Provides da...	Running	Manual (Trig...	Local System
Data Usage	Network da...	Running	Automatic	Local Service
DCOM Server Process Laun...	The DCOM...	Running	Automatic	Local System
Delivery Optimization	Performs co...	Running	Automatic (D...	Network Service
Device Association Service	Enables pair...	Running	Automatic (T...	Local System
Device Install Service	Enables a c...		Manual (Trig...	Local System
Device Management Enroll...	Performs D...		Manual	Local System

Figure 14 - Computer Browser Service

4. Access Denied

The **Access Denied** error may occur if files are still open in the path \\Server\Admin$\Temp\Docusnap\scan on the target system.

This can be checked via Computer Management on the target system.



There are no items to show in this view.

Figure 15 - Computer Management - Open Files

If files are still open here, they should be closed and the inventory repeated.

LIST OF FIGURES

Version history

Date	Description
08/27/2021	Document created
07/12/2022	Version 1.1 - Deleted DNS and DHCP Inventory

Docusnap