



Inventarisierung - PSExec

Inventarisierungen per PSExec – Analyse und Fehlerbehebungen

TITEL Inventarisierung - PSExec
AUTOR Docusnap Consulting
DATUM 30.08.2021
VERSION 1.0 | gültig ab 28.08.2021

Die Weitergabe, sowie Vervielfältigung dieser Unterlage, auch von Teilen, Verwertung und Mitteilung ihres Inhaltes ist nicht gestattet, soweit nicht ausdrücklich durch die Docusnap GmbH zugestanden. Zuwiderhandlung verpflichtet zu Schadenersatz. Alle Rechte vorbehalten.

This document contains proprietary information and may not be reproduced in any form or parts whatsoever, nor may be used by or its contents divulged to third parties without written permission of Docusnap GmbH. All rights reserved.

INHALTSVERZEICHNIS

1.	Einleitung	4
2.	Datei konnte nicht gefunden werden	5
2.1	Verbindungstest	6
2.1.1	Verbindungstest erfolgreich	8
2.1.2	Verbindungstest fehlerhaft	10
3.	Einbinden der Freigabe fehlgeschlagen	14
4.	Zugriff verweigert	15

1. Einleitung

Für folgende Inventarisierungen wird PSEXec verwendet:

- Exchange
- SharePoint
- DNS
- DHCP
- GPO
- Windows Fallback Inventarisierung

Im Standard liegt PSEXec in einem der folgenden Pfade:

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

Wurde Docusnap in einem anderen Verzeichnis installiert, kann dieser Pfad abweichen.

PSEXec baut eine Verbindung zu dem Inventarisierungssystem auf und kopiert die Inventarisierungsdatei auf das System. Nach der Inventarisierung wird die Ergebnisdatei wieder zum Docusnap Server kopiert und dort importiert. Dementsprechend muss eine PSEXec Verbindung zu dem Inventarisierungssystem hergestellt werden können. In diesem HowTo wird die Analyse einer fehlerhaften PSEXec Verbindung, sowie Fehlerbehebungen beschrieben.

- In [Kapitel 2](#) wird die Fehlermeldung *Datei konnte nicht gefunden werden* behandelt
- [Kapitel 3](#) beschreibt einen Lösungsansatz für die Meldung *Einbinden der Freigabe fehlgeschlagen*

2. Datei konnte nicht gefunden werden

Wenn keine PSEXec Verbindung möglich ist, wird in den meisten Fällen die Fehlermeldung Datei konnte nicht gefunden werden angezeigt. Dieser Fehler kann verschiedene Auslöser haben

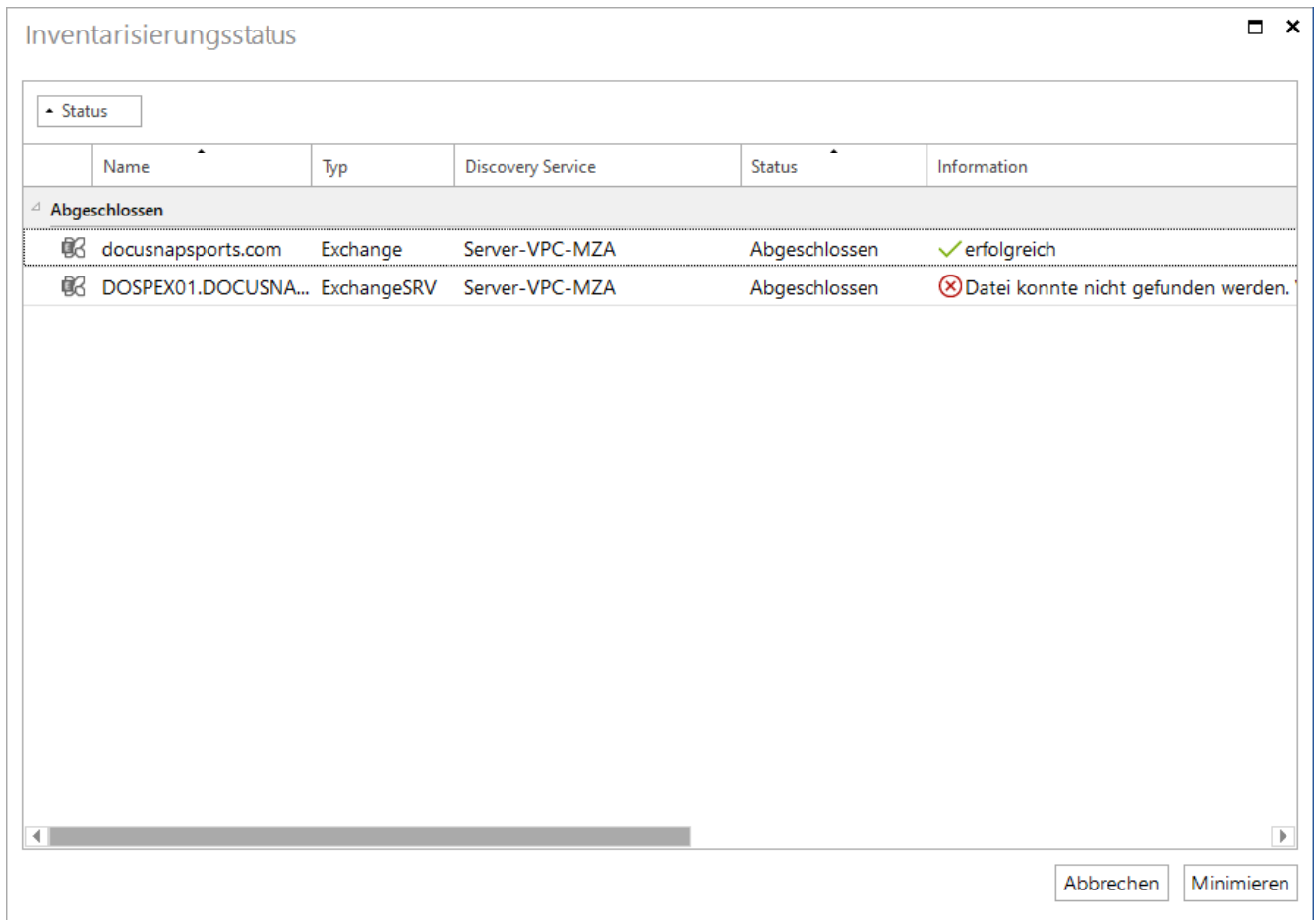


Abbildung 1 - Datei konnte nicht gefunden werden

2.1 Verbindungstest

Wenn dieser Fehler ausgegeben wird, sollte zunächst ein manueller PSEXec Verbindungstest zu dem Zielsystem durchgeführt werden.

Wichtig ist, dass der Test mit demselben Benutzer durchgeführt wird, der auch bei der Inventarisierung verwendet wird.

Hierfür zuallererst CMD oder PowerShell in dem entsprechenden Benutzerkontext ausführen. Alternativ kann auch der Benutzer, mit dem die PSEXec Verbindung aufgebaut werden soll, mittels Parametern übergeben werden.

PSEXec befindet sich in dem Installationsverzeichnis von Docusnap in dem Ordner Bin – z. B. C:\Program Files\Docusnap 11\Bin.

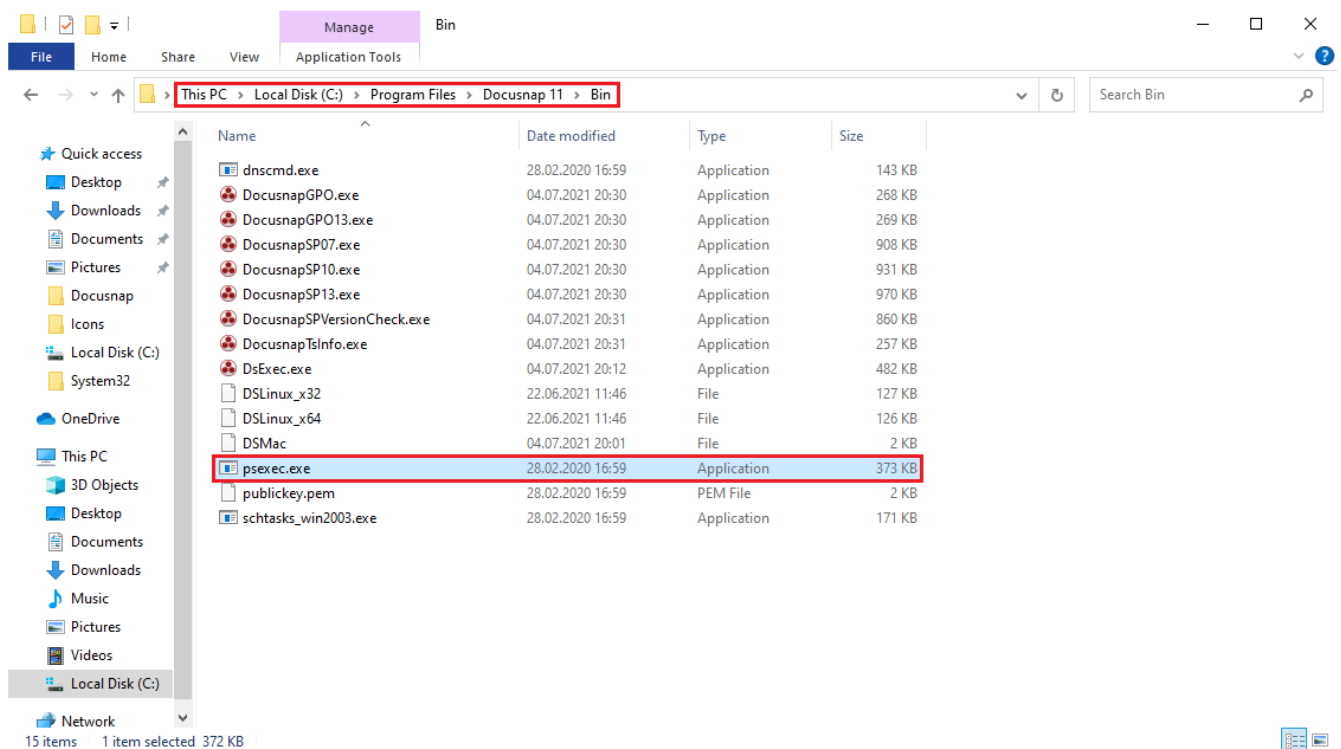
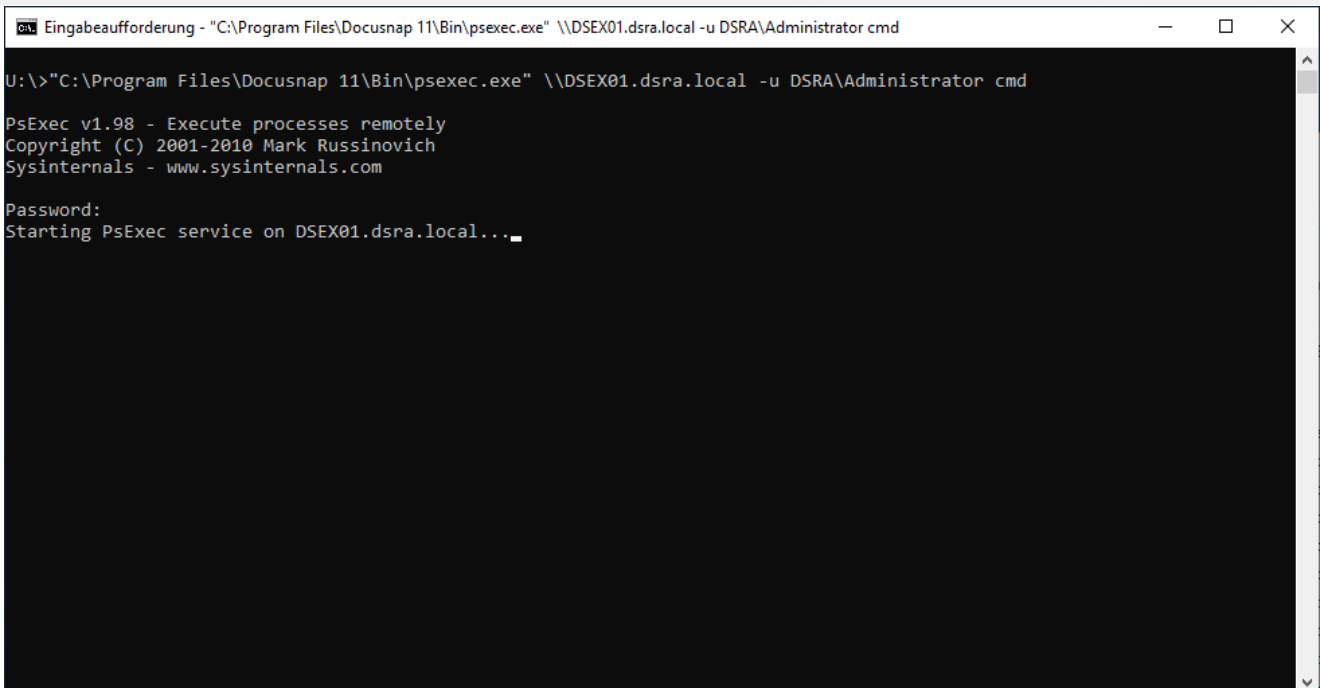


Abbildung 2 - PSEXec Pfad

Der Verbindungstest erfolgt über folgenden Aufruf:

```
psexec.exe \\Zielsystem -u Domäne\Benutzer cmd
```



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

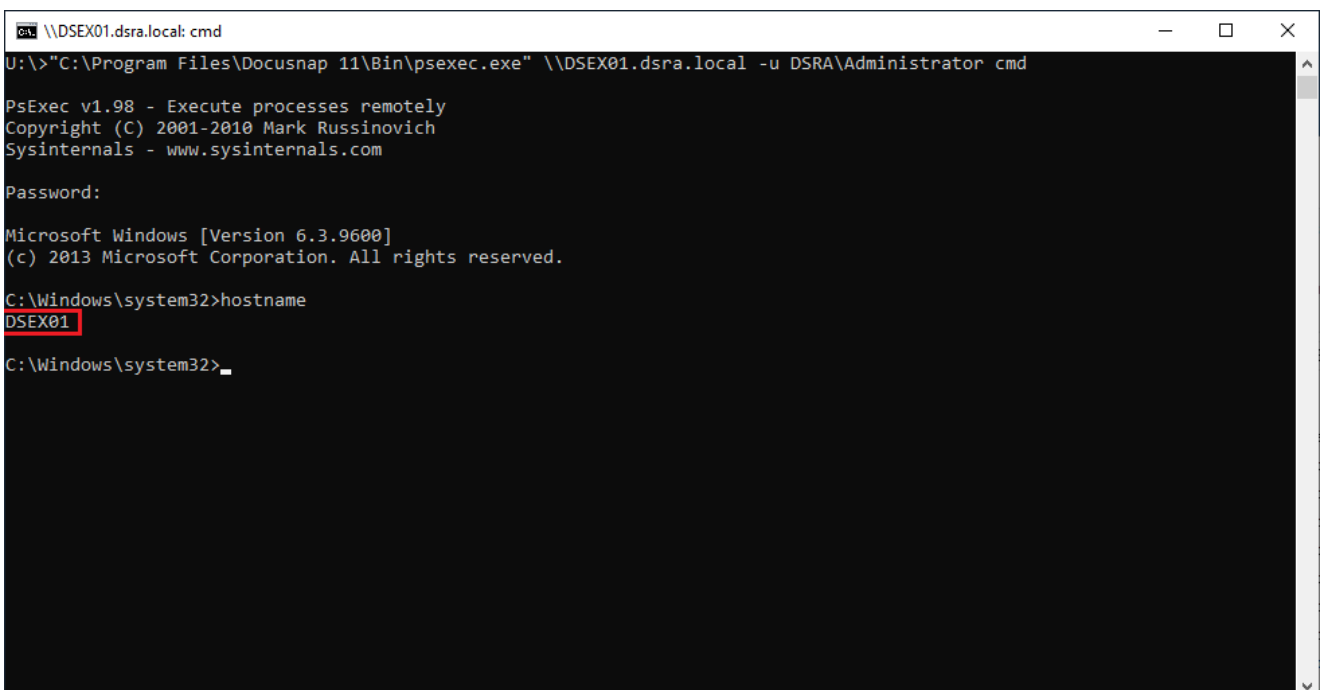
PSEXec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:
Starting PSEXec service on DSEX01.dsra.local...
```

Abbildung 3 - PSEXec Verbindungstest

Während der Passwordeingabe erfolgt keine Rückmeldung.

Ist die Verbindung erfolgreich kann noch der Befehl `hostname` ausgeführt werden. Als Ergebnis sollte der Hostname des entfernten Systems ausgegeben werden.



```
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

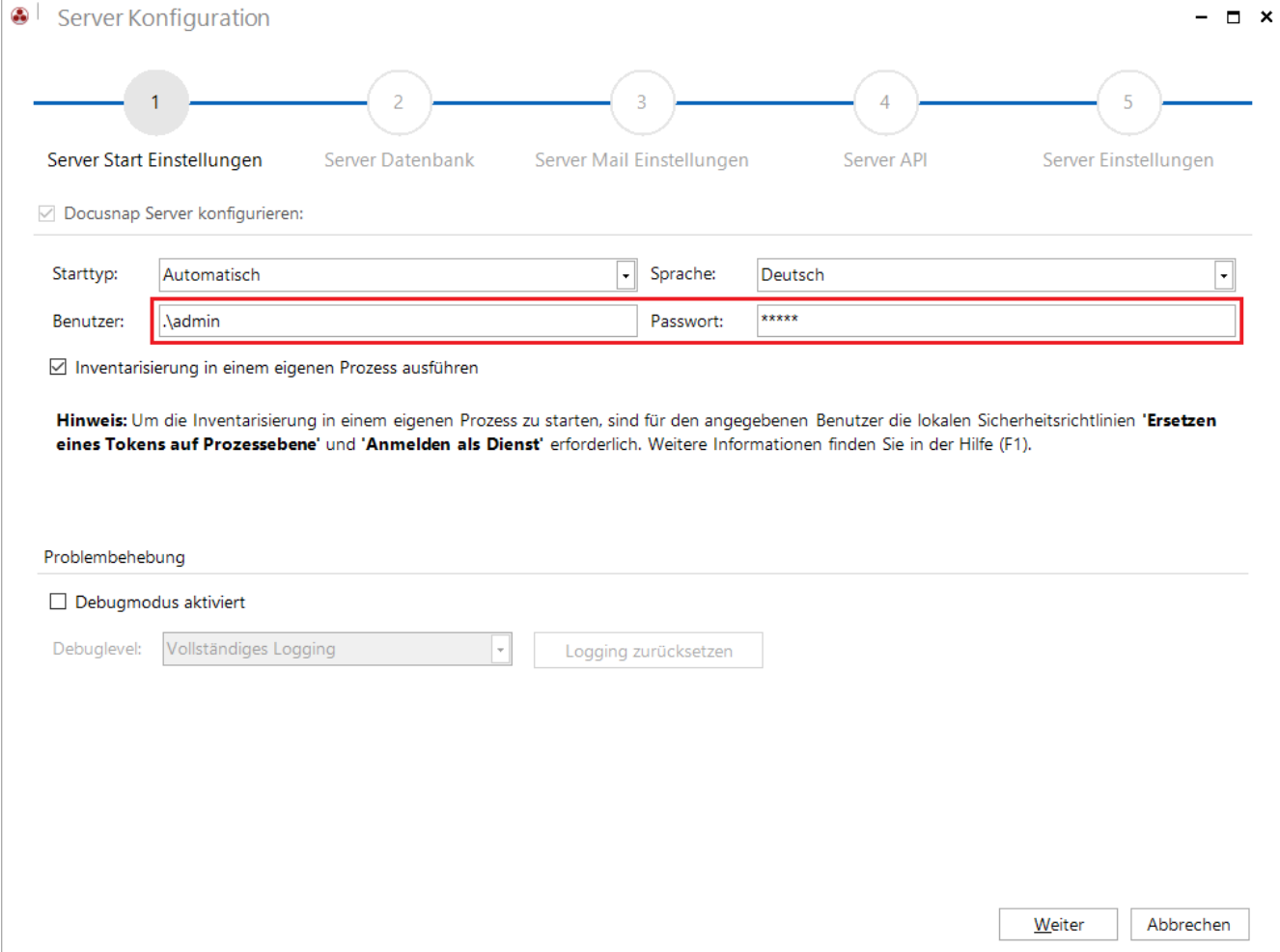
C:\Windows\system32>
```

Abbildung 4 - PSEXec Hostname

2.1.1 Verbindungstest erfolgreich

Ist der Verbindungstest erfolgreich, können Probleme seitens PSEXec ausgeschlossen werden.

In diesem Fall sollte die Docusnap Server Konfiguration überprüft werden. Im ersten Schritt der Konfiguration besteht die Möglichkeit einen Benutzer zu hinterlegen.



Server Konfiguration

1 2 3 4 5

Server Start Einstellungen Server Datenbank Server Mail Einstellungen Server API Server Einstellungen

Docusnap Server konfigurieren:

Starttyp: Automatisch Sprache: Deutsch

Benutzer: .\admin Passwort: *****

Inventarisierung in einem eigenen Prozess ausführen

Hinweis: Um die Inventarisierung in einem eigenen Prozess zu starten, sind für den angegebenen Benutzer die lokalen Sicherheitsrichtlinien **'Ersetzen eines Tokens auf Prozessebene'** und **'Anmelden als Dienst'** erforderlich. Weitere Informationen finden Sie in der Hilfe (F1).

Problemebehebung

Debugmodus aktiviert

Debuglevel: Vollständiges Logging Logging zurücksetzen

Weiter Abbrechen

Abbildung 5 - Docusnap Server Konfiguration

Ist hier ein Benutzer hinterlegt, sollte überprüft werden, ob dieser bei den benötigten lokalen Sicherheitsrichtlinien Anmelden als Dienst und Ersetzen eines Tokens auf Prozessebene hinterlegt ist.

1. Lokale Sicherheitsrichtlinien über die Windows Suche mit **secpol.msc** öffnen
2. Lokale Richtlinien
3. Zuweisen von Benutzerrechten
4. **Anmelden als Dienst** öffnen und prüfen, ob der Serverdienst Benutzer hinterlegt ist
5. **Ersetzen eines Tokens auf Prozessebene** öffnen und prüfen, ob der Serverdienst Benutzer hinterlegt ist

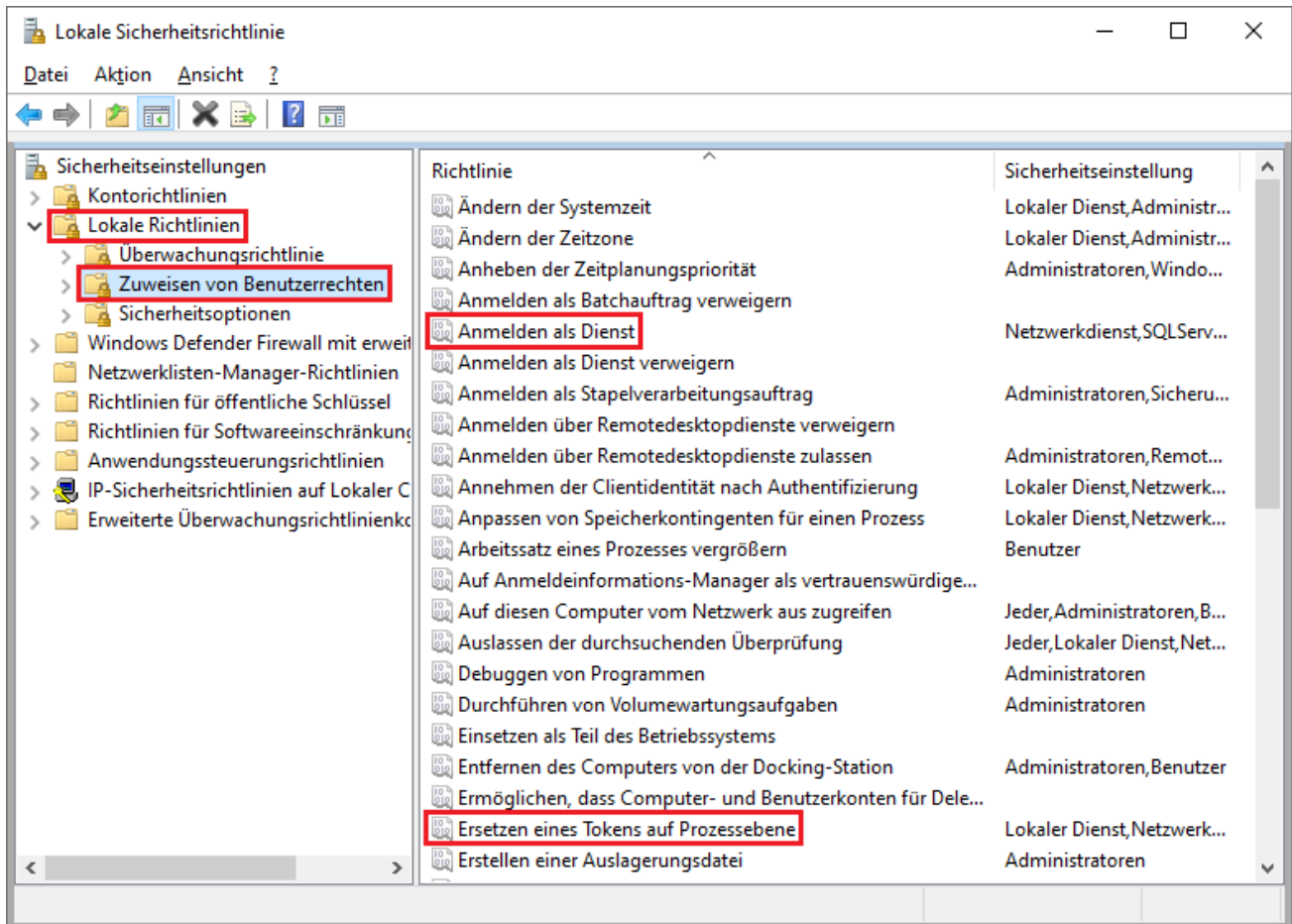


Abbildung 6 - Lokale Sicherheitsrichtlinien

Wenn alle Sicherheitsrichtlinien bereits gesetzt sind, kann in der Docusnap Server Konfiguration noch überprüft werden, ob die Option Inventarisierung in einem eigenen Prozess ausführen aktiviert ist. Diese sollte gesetzt sein.

Starttyp: Sprache:

Benutzer: Passwort:

Inventarisierung in einem eigenen Prozess ausführen

Hinweis: Um die Inventarisierung in einem eigenen Prozess zu starten, sind für den angegebenen Benutzer die lokalen Sicherheitsrichtlinien **'Ersetzen eines Tokens auf Prozessebene'** und **'Anmelden als Dienst'** erforderlich. Weitere Informationen finden Sie in der Hilfe (F1).

Abbildung 7 - Inventarisierung in einem eigenen Prozess ausführen

2.1.2 Verbindungstest fehlerhaft

Schlägt der Verbindungstest fehl, sollten die nachstehenden Punkte überprüft werden.

Berechtigungen

Für die Verbindung muss ein Benutzer verwendet werden, der auf dem Zielsystem lokaler Administrator ist.

Antivirus

Oftmals schlägt die Verbindung fehl, da PSEXec durch die installierte Antiviren Lösung blockiert wird. In der Regel erscheint in der Antiviren Konsole auf dem System ein Warnhinweis, dass die Ausführung von PSEXec blockiert wurde.

Es kann auch dazu kommen, dass die PSEXec.exe auf dem Docusnap System gelöscht wird. In diesem Fall wird sich PSEXec in überhaupt nicht mehr in dem entsprechenden Pfad befinden.

Um diesen Fehler in Zukunft zu unterbinden, muss eine Ausnahme für PSEXec in der Antiviren Lösung eingerichtet werden.

Dienste

Wird eine Arbeitsstation inventarisiert, muss der Arbeitsstationsdienst ausgeführt werden.

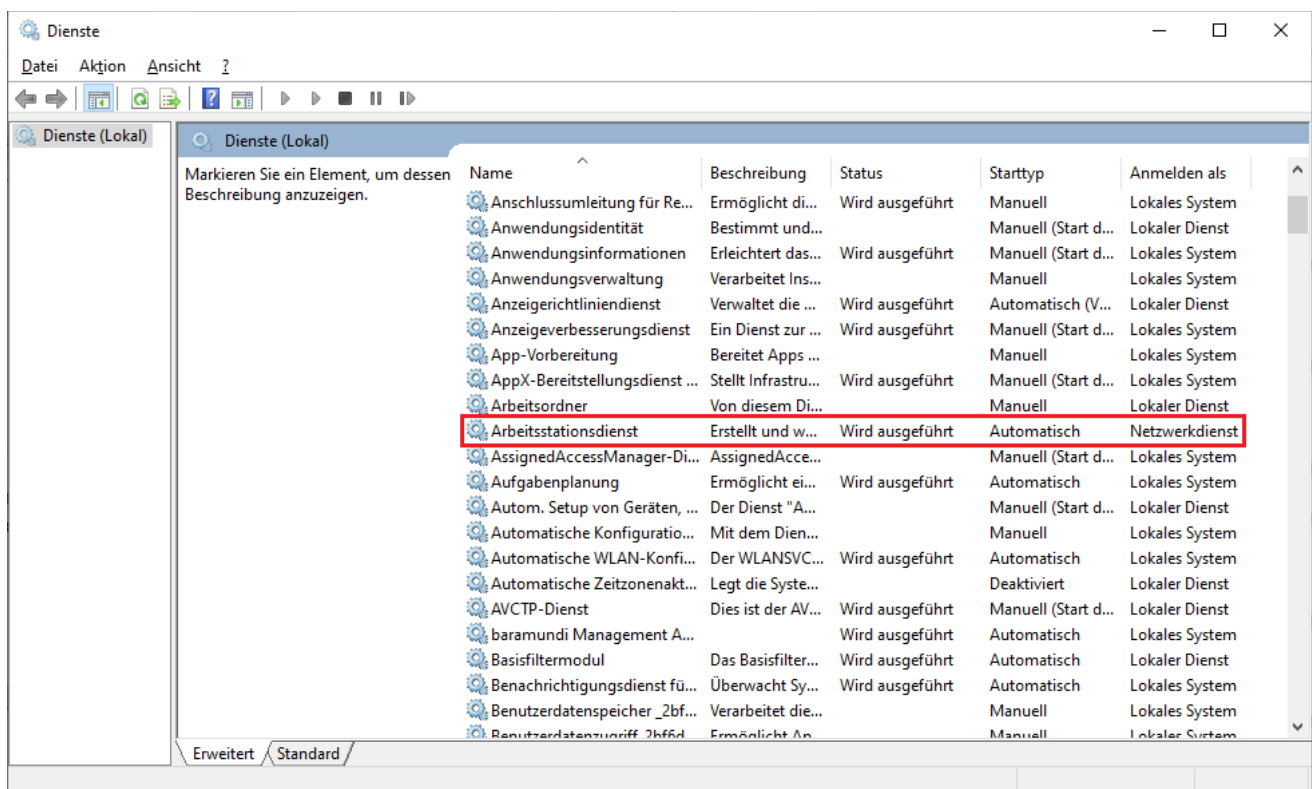


Abbildung 8 – Arbeitsstationsdienst

Bei einem Server ist dies der Serverdienst

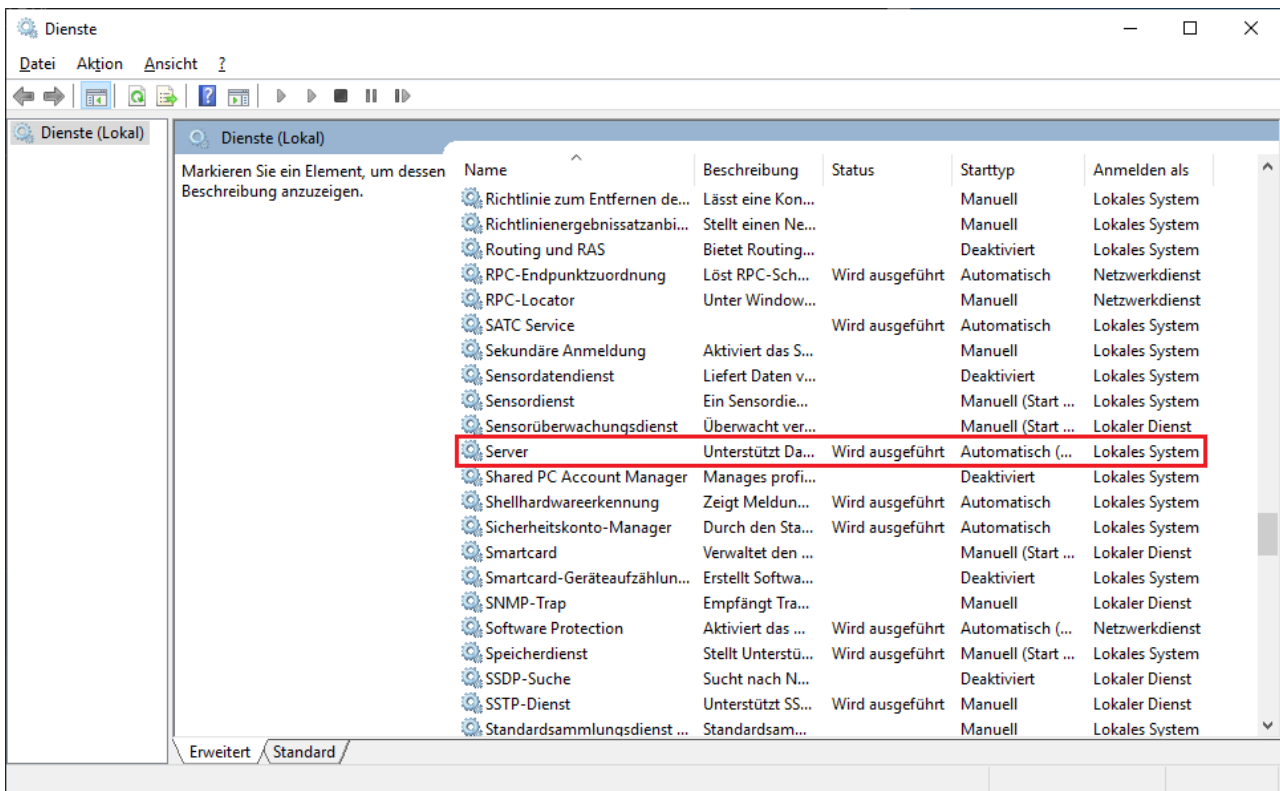


Abbildung 9 - Serverdienst

Freigabe

Die Freigabe ADMIN\$ muss auf dem Zielsystem erreichbar sein.

Dies kann über den Windows Explorer getestet werden.

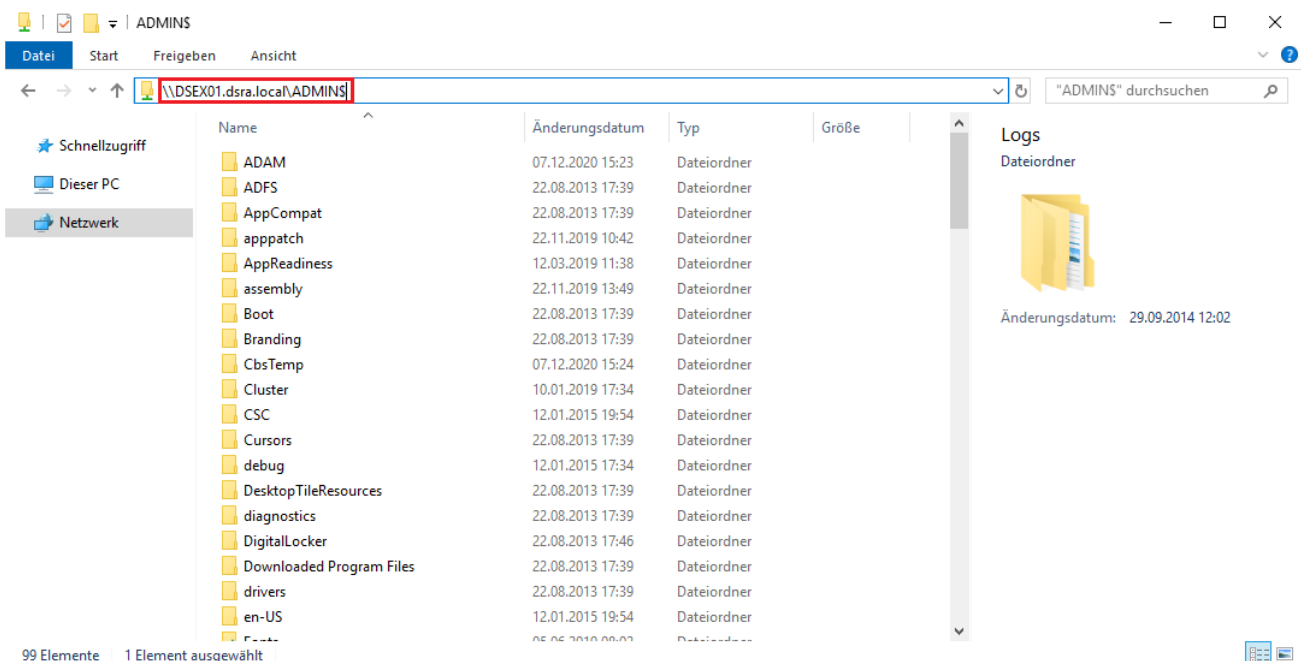


Abbildung 10 - Windows Explorer

Über die Computerverwaltung kann auf dem Zielsystem die Freigabe auch direkt überprüft werden.

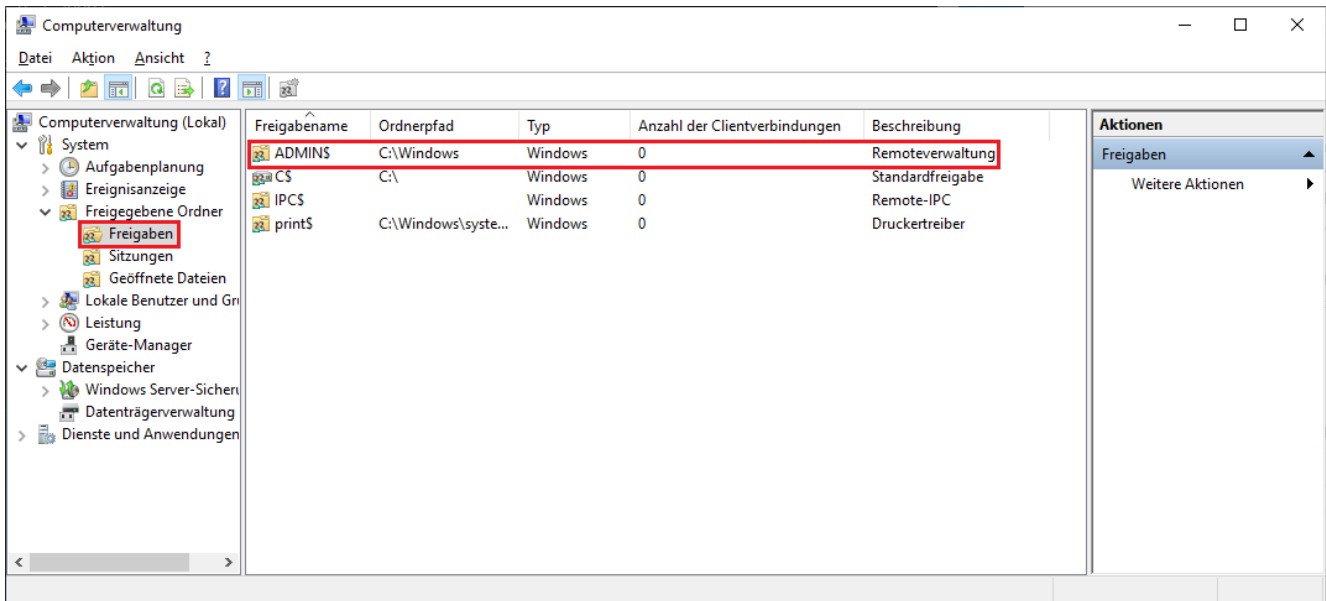


Abbildung 11 – Computerverwaltung - Freigabe

Windows Netzwerk

Die Datei- und Druckerfreigabe muss auf dem Zielsystem aktiviert sein.

Dies kann auf dem Zielsystem über das Netzwerk- und Freigabecenter überprüft werden. Hierfür die Systemsteuerung öffnen und dort das Netzwerk- und Freigabecenter auswählen.

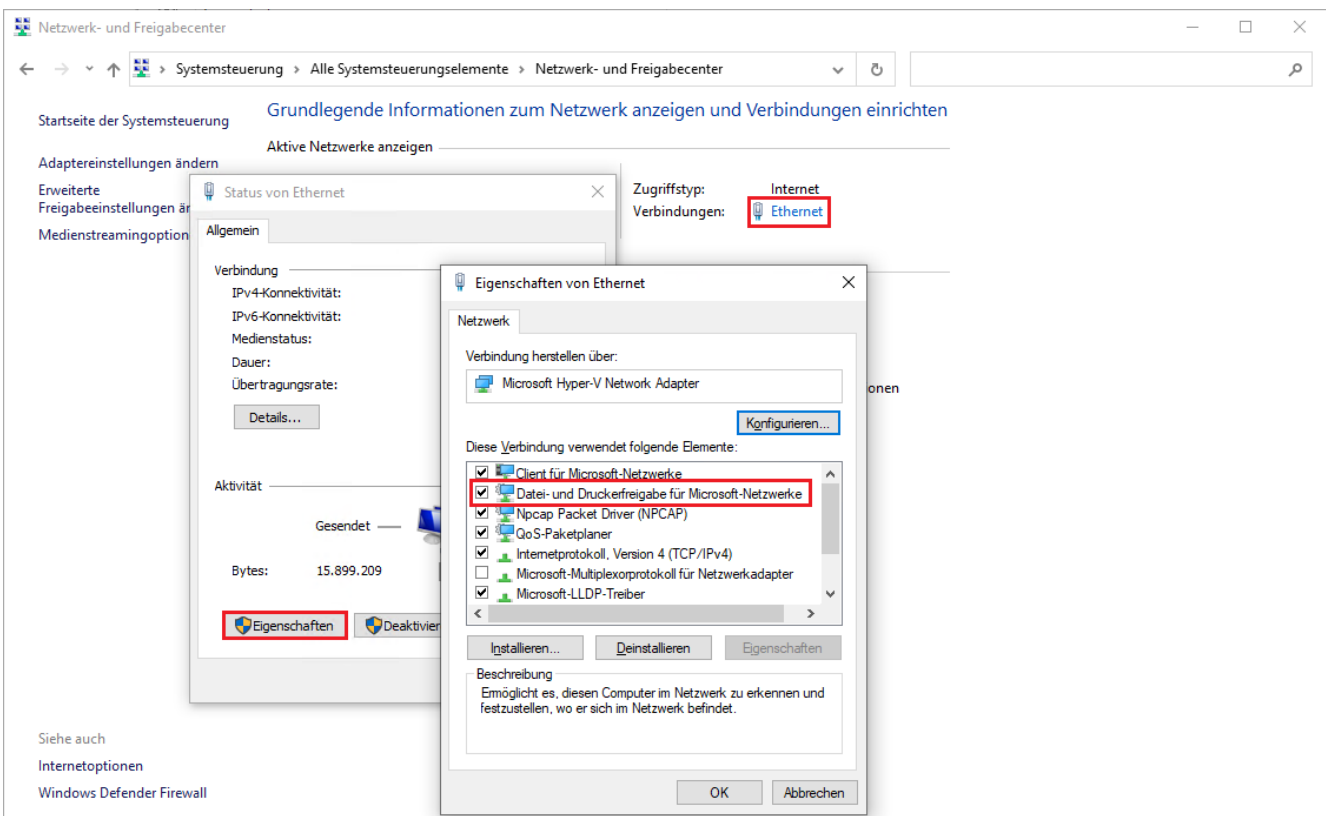


Abbildung 12 - Datei und Druckerfreigabe

Prozess wird bereits ausgeführt

Pro System kann nur ein PSEXec Prozess gleichzeitig ausgeführt werden.

Auf dem Zielsystem sollte überprüft werden, ob der Prozess *PSEXecSVC.exe* oder ein Docusnap Prozess ausgeführt wird – z. B. wird bei der Exchange Inventarisierung der Prozess *DocusnapEX13.exe* ausgeführt.

Ist noch einer der beiden Prozesse aktiv, sollte dieser manuell beendet und der Verbindungstest wiederholt werden.

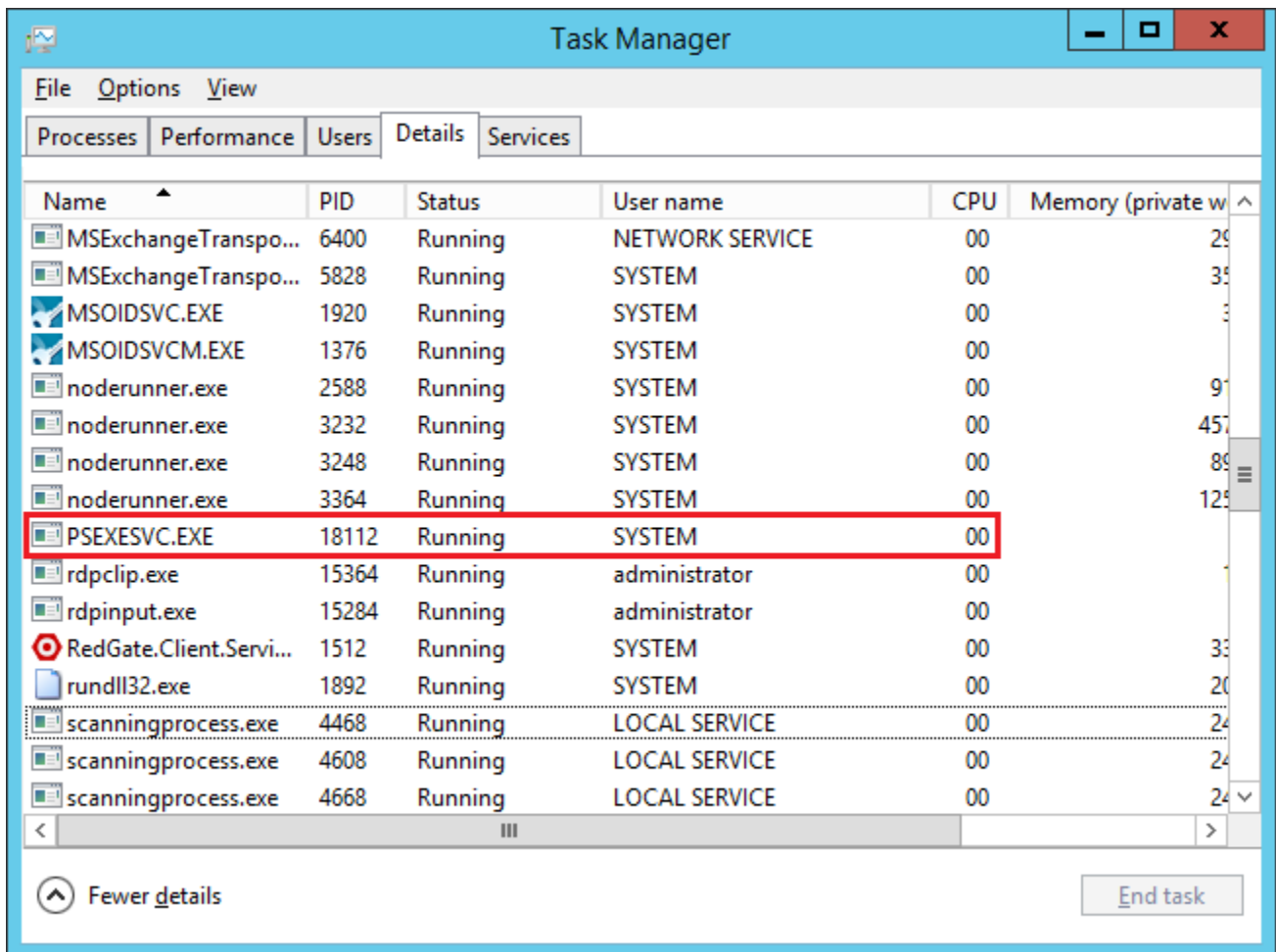


Abbildung 13 - PSEXec Dienst

Windows Updates

Wurden alle Punkte erfolgreich überprüft und die Inventarisierung schlägt weiterhin fehl, sollte noch überprüft werden, ob auf dem Zielsystem die Installation von Windows Updates aussteht.

3. Einbinden der Freigabe fehlgeschlagen

In seltenen Fällen wird die Meldung Einbinden der Freigabe fehlgeschlagen ausgegeben.

Hier sollte auf dem System, welches die Inventarisierung durchführt, überprüft werden, ob der Dienst Computerbrowser aktiv ist.

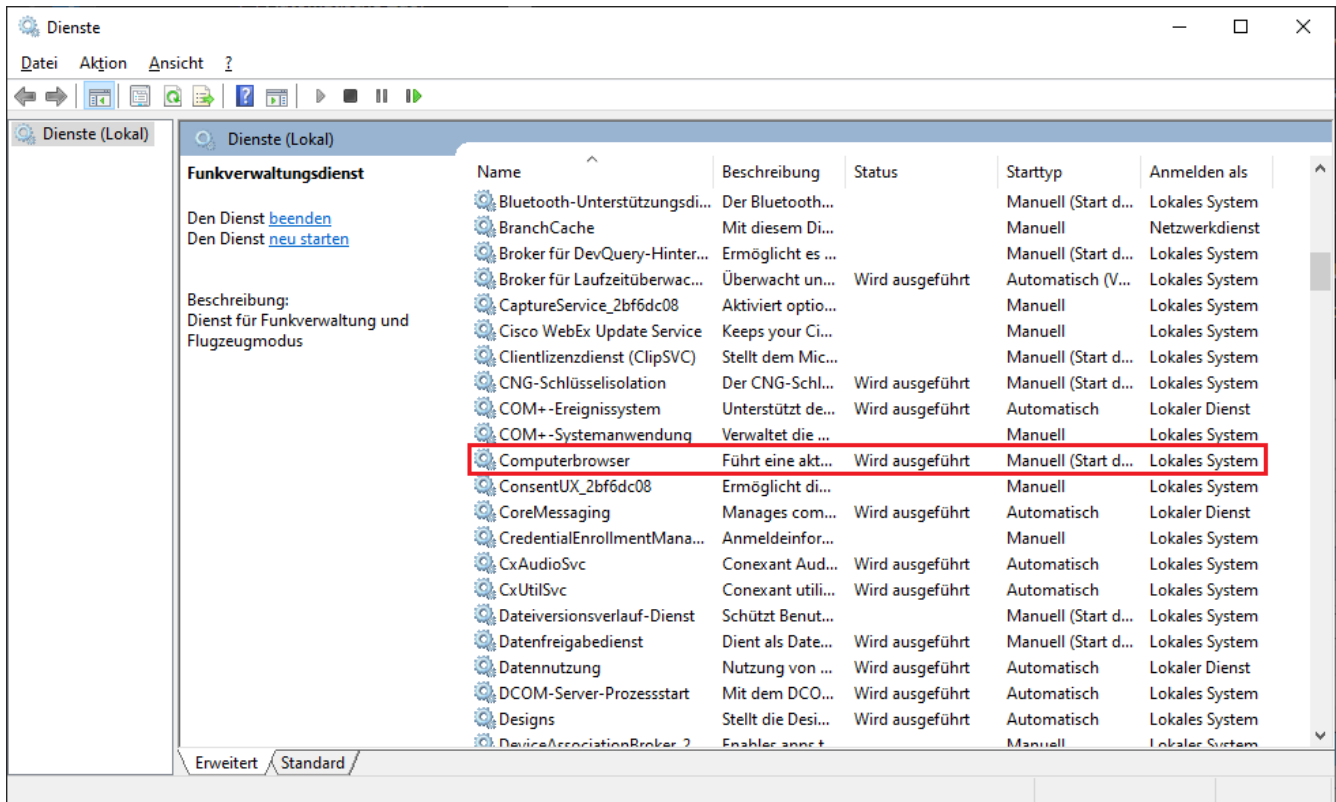


Abbildung 14 - Computerbrowser

4. Zugriff verweigert

Die Meldung **Zugriff verweigert** kann auftreten, wenn auf dem Zielsystem noch Dateien in dem Pfad \\Server\Admin\$\Temp\Docusnap\scan geöffnet sind.

Dies kann über die Computerverwaltung auf dem Zielsystem überprüft werden.

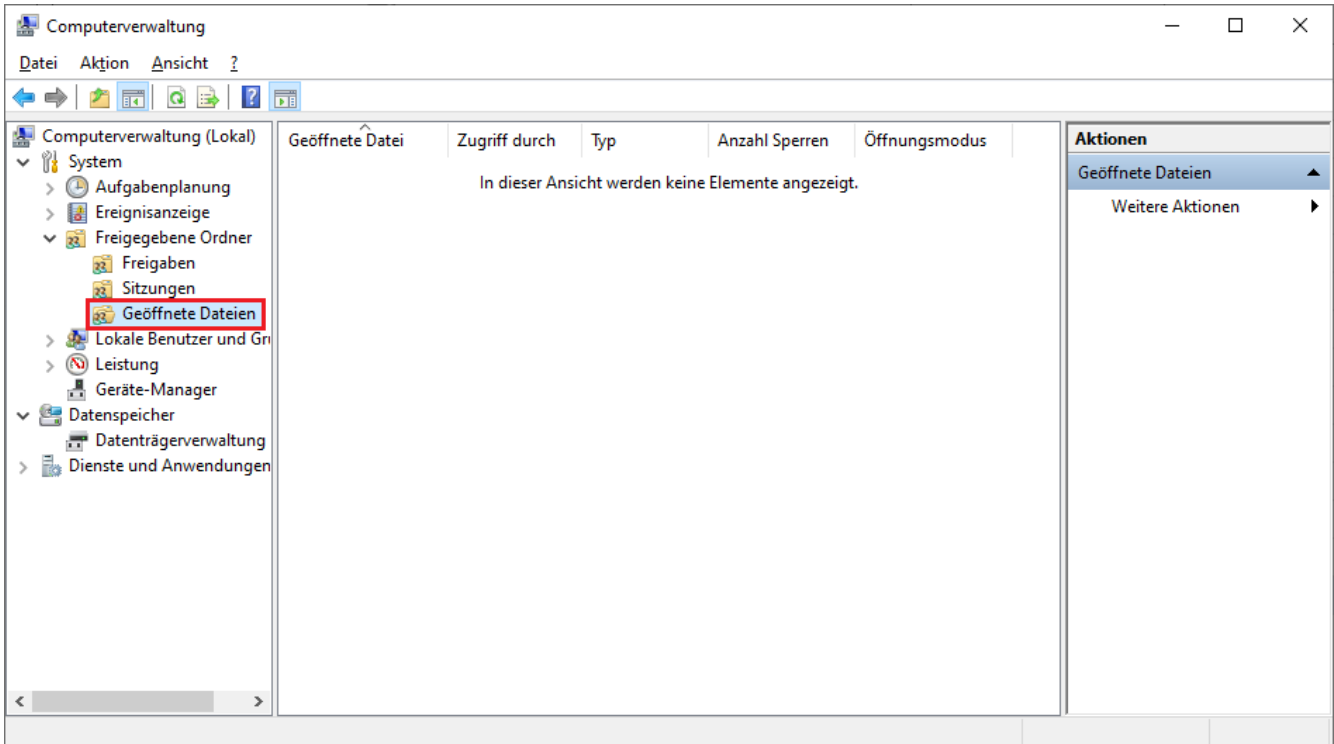


Abbildung 15 - Computerverwaltung - Geöffnete Dateien

Sind hier noch Dateien geöffnet, sollten diese geschlossen und die Inventarisierung wiederholt werden.

ABBILDUNGSVERZEICHNIS

ABBILDUNG 1 - DATEI KONNTE NICHT GEFUNDEN WERDEN	5
ABBILDUNG 2 - PSEXEC PFAD	6
ABBILDUNG 3 - PSEXEC VERBINDUNGSTEST	7
ABBILDUNG 4 - PSEXEC HOSTNAME	7
ABBILDUNG 5 - DOCUSNAP SERVER KONFIGURATION	8
ABBILDUNG 6 - LOKALE SICHERHEITSRICHTLINIEN	9
ABBILDUNG 7 - INVENTARISIERUNG IN EINEM EIGENEN PROZESS AUSFÜHREN	9
ABBILDUNG 8 – ARBEITSSTATIONSDIENST	10
ABBILDUNG 9 - SERVERDIENST	11
ABBILDUNG 10 - WINDOWS EXPLORER	11
ABBILDUNG 11 – COMPUTERVERWALTUNG - FREIGABEN	12
ABBILDUNG 12 - DATEI UND DRUCKERFREIGABE	12
ABBILDUNG 13 - PSEXEC DIENST	13
ABBILDUNG 14 - COMPUTERBROWSER	14
ABBILDUNG 15 - COMPUTERVERWALTUNG - GEÖFFNETE DATEIEN	15

VERSIONSHISTORIE

Datum	Beschreibung
27.08.2021	Dokument erstellt
