Whitepaper Docusnap Inventarisierung

Technischer Überblick und Lösungsvorschläge zu Problemen bei der Inventarisierung

TITEL	Whitepaper Docusnap Inventarisierung
AUTOR	Docusnap Consulting
DATUM	13.06.2024
VERSION	4.1 | gültig ab 12.06.2024

INHALTSVERZEICHNIS

1. Einleitung

Häufig treten bei der Erstinventarisierung Probleme auf, die auf fehlende Berechtigungen eines Benutzers oder auf geblockte Ports einer Firewall zurückzuführen sind. Um Sie bei der Behebung dieser Probleme zu unterstützen, werden in den folgenden Kapiteln die notwendigen Voraussetzungen anhand von Ports, Rechten und einem FAQ-Teil näher erläutert.

Das Dokument gliedert sich in eine tabellarische Übersicht, eine detaillierte Beschreibung der einzelnen Bestandsaufnahmen und einen FAQ-Teil.

Weitere Informationen und HowTos finden Sie in unserer Docusnap Knowledge Base. Diese finden Sie unter www.docusnap.com im Bereich Support.

Wenn eine Inventarisierung per Skript möglich ist, wird dies bei den netzwerktechnischen Voraussetzungen der jeweiligen Inventarisierung vermerkt.

Alle Informationen in diesem Whitepaper werden regelmäßig aktualisiert. Unter Umständen sind diese unvollständig.

2. Tabellarische Übersicht

INVENTARISIERUNG	PROTOKOLL	PORT	TRANSPORT LAYER
WINDOWS – WMI	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	NetBIOS Session Service, Microsoft-DS Active Directory, Windows-Freigaben (CIFS)	139, 445	TCP
	dynamic High Range Port	1024 - 65535	TCP/UDP
	Nur bei Windows (AD) LDAP – Lightweight Directory Access Protocol Ungesichert (LDAP) TLS-Gesichert (LDAPS)	 389 636	TCP/UDP
SNMP SYSTEME	SNMP - Simple Network Management Protocol	161	UDP
CIFS SYSTEME	SNMP - Simple Network Management Protocol	161	UDP
	Microsoft-DS Active Directory - Windows-Freigaben (CIFS)	445	TCP
LINUX SYSTEME	Secure Shell (SSH)	22	TCP/UDP
	SSH File Transfer Protocol (SFTP)	115	TCP
MAC SYSTEME	Secure Shell (SSH)	22	TCP/UDP
VMWARE	https – Hypertext Transfer Protocol Secure	443	TCP
HP-UX	Secure Shell (SSH)	22	TCP/UDP
HYPER-V / IIS SERVER	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	DCE Endpoint-Solution, NetBIOS Session Service, Microsoft-DS Active Directory, Windows-Freigaben (CIFS)	135, 139, 445	TCP
	dynamic High Range Port	1024 - 65535	TCP/UDP
CITRIX HYPERVISOR	https – Hypertext Transfer Protocol Secure	Port kann angepasst werden	TCP
IGEL SYSTEME	SQL Database – MSSQL (Microsoft SQL Server)	1433	TCP
	SQL Database – MSSQL (Microsoft SQL Server) Monitor	1434	TCP/UDP

	dynamic High Range Port	1024 - 65535	TCP/UDP
SHAREPOINT	DCE Endpoint-Solution, Windows-Freigaben (CIFS)	135, 445	TCP
EXCHANGE	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	DCE Endpoint-Solution, NetBIOS Session Service, Microsoft-DS Active Directory, Windows-Freigaben (CIFS)	135, 139, 445	TCP
	dynamic High Range Port – WMI	1024 - 65535	TCP/UDP
SQL-SERVER / VEEAM LEGACY / BACKUP EXEC	SQL Database – MSSQL (Microsoft SQL Server)	1433	TCP
	SQL Database – MSSQL (Microsoft SQL Server) Monitor	1434	TCP/UDP
	dynamic High Range Port	1024 - 65535	TCP/UDP
ORACLE DATENBANK	Oracle Datenbank listening für unsichere Client-Verbindungen zum Listener, ersetzt Port 1521	2483	TCP/UDP
	Oracle Datenbank listening für SSL Client-Verbindungen zum Listener	2484	TCP/UDP
DELL EMC² ISILON	http - Hypertext Transfer Protocol	8080	TCP
ACTIVE DIRECTORY / ADDS ABGLEICH	LDAP - Lightweight Directory Access Protocol Ungesichert (LDAP) TLS-Gesichert (LDAPS)	 389 636	TCP/UDP
	DCE Endpoint-Solution, Microsoft-DS Active Directory, Windows-Freigaben (CIFS) – nur bei Gruppenrichtlinien	135, 445	TCP
DFS	NetBIOS Name Service, NETBIOS Datagram Service	137, 138	UDP
	NetBIOS Session Service, Microsoft-DS Active Directory - Windows-Freigaben (CIFS)	139, 445	TCP
	dynamic High Range Port	1024 - 65535	TCP/UDP
	LDAP - Lightweight Directory Access Protocol	389	TCP/UDP
DNS / DHCP	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	NetBIOS Session Service, Microsoft-DS Active Directory, Windows-Freigaben (CIFS)	139, 445	TCP

	dynamic High Range Port	1024 - 65535	TCP/UDP
AZURE / MICROSOFT 365 / AWS / EXCHANGE ONLINE	https - Hypertext Transfer Protocol Secure	443	TCP
VEEAM BACKUP & REPLICATION	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	NetBIOS Session Service, Microsoft-DS Active Directory, Windows-Freigaben (CIFS)	139, 445	TCP
	dynamic High Range Port	1024 - 65535	TCP/UDP
NTFS ANALYSE	NetBIOS Session Service, Microsoft-DS Active Directory - Windows-Freigaben (CIFS)	139, 445	TCP

3. Inventarisierungen

In den nachfolgenden Kapiteln werden die verschiedenen Inventarisierungen beschrieben.

3.1 Windows

3.1.1 Protokolle und Berechtigungen

Verwendete Protokolle Windows WMI:

BEZEICHNUNG	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE – NUR BEI WMI	137, 138	UDP
NETBIOS SESSION SERVICE, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS-FREIGABEN (CIFS)	139, 445	TCP
DYNAMIC HIGH RANGE PORT – NUR BEI WMI	1024 – 65535	TCP/UDP
NUR BEI WINDOWS (AD) LDAP – LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL UNGESICHERT (LDAP) TLS-GESICHERT (LDAPS)	 389 636	TCP/UDP

Benötigte Rechte

- Lokaler Administrator auf Windows Clients und Servern. Für Domänen Controller wird ein Domänen Administrator benötigt.
  - NetBIOS Schreibweise
  - UPN Schreibweise
- Bei Verwendung von lokalen Administrator-Rechten bei Windows (IP) UAC beachten.
  - Bei einzelner Anmeldung Rechnername\User
  - Bei Sammelinventarisierung .\User
- Aktive WMI Dienste auf dem Zielsystem
  - Windows Verwaltungsinstrumentation
  - Remoteprozeduraufruf (RPC)

3.1.2 Netzwerktechnische Voraussetzungen

- Inventarisierung via Skript ist möglich
- Windows System ist Mitglied des Active Directorys (nur Windows (AD))
- Eindeutige Namensauflösung muss gegeben sein (Forward Lookup & Reverse Lookup)
- Transparente Firewall Konfiguration
- Beim Windows (IP) Scan muss das System via Ping erreichbar sein, wenn IP-Adressbereiche verwendet werden
- Für eine Vollständige Inventarisierung muss das Ausführen der PowerShell möglich sein

3.1.3 FAQs

Q1 Trotz der Authentifizierung mit einem ausreichend berechtigten Benutzer tritt die Fehlermeldung „Verbindung konnte nicht hergestellt werden“ auf. Wo liegt das Problem?

A1 Verwenden Sie bitte bei der Authentifizierung gegenüber der Domäne eine Benutzerangabe mit Domänenzusatz.

- *User Principal Name* *UserName@Example.intern*
- *Down-Level Logon Name* *Example\UserName*

Q2 Trotz der Verwendung eines Benutzers mit lokaler Administrator-Mitgliedschaft tritt die Fehlermeldung „Zugriff verweigert“ auf.

A2 Der Grund für das Problem ist die User Account Control (UAC). Der Benutzer verbindet mit „normalen Berechtigungen" und der sogenannte Auto-Elevation-Mechanismus, der die Rechte bei Bedarf erhöhen sollte, greift beim Remote Zugriff nicht. Mit Hilfe des folgenden Befehls kann ein entsprechender Registry Eintrag gesetzt werden, der das Problem behebt.

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

Q3 Einige Systeme sind über eine langsame Leitung angebunden. Eine Inventarisierung resultiert in einem Timeout Fehler. Wie kann dieser behoben werden?

A3 Sie können das Timeout in den Inventarisierungsoptionen erhöhen. Navigieren Sie dazu in die allgemeinen Optionen – Inventarisierung.

Q4 Muss das Ausführen der PowerShell möglich sein, damit ich meine Clients erfolgreich inventarisieren kann?

A4 Nein. Die PowerShell wird verwendet, um zusätzliche Informationen wie z.B. Zertifikate zu inventarisieren. Ist das Ausführen der PowerShell geblockt werden nur diese Informationen nicht erfasst.

3.2 IP-Scan

3.2.1 Protokolle und Berechtigungen

Eine detaillierte Übersicht der verwendeten Ports kann beim IP-Scan nicht gegeben werden. Je nachdem wie der IP-Scan konfiguriert wird, werden unterschiedliche Ports gescannt. Hierbei kann zwischen einzelnen Ports bis hin zu einer kompletten Range unterschieden werden. In der Theorie ist es möglich, dass der IP-Scan alle möglichen Ports prüft.

Hinweis: Durch eine hohe Anzahl an ICMP Requests kann ein IP-Scan dazu führen, dass das Netzwerk Monitoring Warnmeldungen erzeugt. Ebenfalls können Monitoring Tools eine Warnmeldung ausgeben, dass invalide Pakete versendet werden. Dieses Verhalten ist bei einem IP-Scan normal. Diese Pakete werden versendet, damit z. B. das Betriebssystem erkannt werden kann.

Benötigte Rechte:

- Freischalten des Aufrufs von NMAP. In manchen Fällen blocken Antivirus Hersteller den Aufruf von NMAP aus einer anderen Software.
- Lokale Administrator Rechte zwecks der Installation des Npcap Treibers. Dieser wird für den erweiterten IP-Scan benötigt.
- Wird der erweiterte IP-Scan nicht verwendet, wird kein Npcap Treiber vorausgesetzt. Zusätzliche Funktionen wie z. B. Betriebssystemerkennung sind dadurch nicht möglich.

3.2.2 Netzwerktechnische Voraussetzungen

- Installation des aktuellen Npcap Treibers auf dem ausführenden System. Das kann optional in der Setup Routine ausgewählt, oder nachträglich installiert werden.
- Diverse Drittsoftware kann eine Ausführung des IP-Scans beeinflussen; z. B. Wireshark.

3.2.3 FAQs

Q1 Wird eine komplette IP-Range angegeben, so werden nicht alle Systeme in diesem Bereich gefunden. Einzeln ist ein Scan der Systeme jedoch möglich. Wo liegt der Fehler?

A1 Wenn die Systeme einzeln beim Scan gefunden werden, sollte ein Scan mittels der Angabe einer IP-Range ebenfalls möglich sein. Prüfen Sie bitte ggf. die Einstellung Ihrer Firewall in Bezug auf ICMP Flooding Protection.

Q2 Wie erkennt man, ob der aktuelle Npcap Treiber installiert ist?

A2 Sobald der erweiterte Modus im Assistenten aktiviert wird, prüft Docusnap, ob der zusätzliche Netzwerktreiber vorhanden ist. Ist dieser nicht installiert, ist ein erweiterter Modus nicht möglich.

3.3 SNMP Systeme

3.3.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
SNMP - SIMPLE NETWORK MANAGEMENT PROTOCOL	161	UDP

Hinweis: Durch eine hohe Anzahl an ICMP Requests kann eine SNMP-Inventarisierung dazu führen, dass das Netzwerk Monitoring Warnmeldungen erzeugt.

Benötigte Rechte:

- Read Community String – im Standard public
- Authentifizierungsdaten bei SNMP v3
- SNMP Manager (Abfragendes System, z. B. Docusnap Server) muss für SNMP Polling auf den SNMP Agenten berechtigt sein (**Whitelisting**).

3.3.2 Netzwerktechnische Voraussetzungen

- SNMP Protokoll ist aktiviert. V1, V2 oder V3
- Transparente Firewall Konfiguration
- Systemerreichbarkeit via Ping. Kann optional im Scan Assistenten deaktiviert werden.

3.3.3 FAQs

Q1 Wird eine komplette IP-Range angegeben, so werden nicht alle Systeme in diesem Bereich gefunden. Einzeln ist eine Inventarisierung der Systeme jedoch möglich. Wo liegt der Fehler?

A1 Wenn die Systeme einzeln inventarisiert werden, sollte eine Inventarisierung mittels der Angabe einer IP-Range ebenfalls möglich sein. Prüfen Sie bitte ggf. die Einstellung Ihrer Firewall in Bezug auf ICMP Flooding Protection.

3.4 CIFS Systeme

Mit Hilfe der CIFS Inventarisierung können Freigaben von Systemen (z. B. NAS, etc.) erfasst werden. Somit bildet die CIFS Inventarisierung die Grundlage für eine Berechtigungsanalyse in Docusnap.

Das per CIFS zu inventarisierende System darf nicht bereits per Linux oder Windows Assistenten erfasst sein.

3.4.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
SNMP - SIMPLE NETWORK MANAGEMENT PROTOCOL	161	UDP
MICROSOFT-DS ACTIVE DIRECTORY - WINDOWS-FREIGABEN (CIFS)	445	TCP

Benötigte Rechte:

- Read Community String
- Domänen Administrator oder vergleichbar – je nach System
- Berechtigung zum Starten von SNMP Abfragen auf dem Zielsystem

3.4.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration
- Wird bei der CIFS Inventarisierung ein anderer Benutzer als der aktuell angemeldete Benutzer verwendet, so darf der aktuell angemeldete Benutzer keine Verbindung zu dem CIFS System herstellen (z. B. Anbindung durch ein Netzlaufwerk).
    - Diese können mit Hilfe des Befehls *net use* geprüft werden.
- Sonderfall: NAS Systemgruppen sind zu beachten (Auslesen von SMB Berechtigungen)

3.5 Linux Systeme

3.5.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
SECURE SHELL (SSH)	22	TCP/UDP
SSH FILE TRANSFER PROTOCOL (SFTP)	115	TCP

Benötigte Rechte:

- root User
- remote Login als root erlaubt
- SUDO Benutzer mit entsprechender SUDO Konfiguration.

3.5.2 Netzwerktechnische Voraussetzungen

- Inventarisierung via Skript ist möglich
- Transparente Firewall Konfiguration
- unterstütztes Linux Derivat
    - Eine Übersicht der unterstützten Derivate finden Sie in den Docusnap Systemvoraussetzungen.

3.5.3 FAQs

Q1 Das System konnte erfolgreich inventarisiert werden, aber nur ein Teil der Informationen sind ersichtlich.

A1 Um sicherzustellen, dass die gesammelten Informationen vollständig sind, müssen Sie zwingend den root User verwenden. Nur mit dem root User ist eine vollständige Inventarisierung, sofern keine SUDO Konfiguration verwendet wird, möglich.

Q2 Ist eine Authentifizierung mittels RSA Schlüssel möglich?

A2 Ja. Genauere Informationen zur Inventarisierung per RSA Schlüssel finden Sie im zugehörigen HowTo in der Docusnap Knowledge Base.

Q3 Wie kann eine Inventarisierung mittels SUDO konfiguriert werden?

A3 Damit die Inventarisierung mit einem SUDO Benutzer möglich ist, muss sowohl Docusnap als auch das Linux System entsprechend konfiguriert werden. Weitere Informationen dazu finden Sie im zugehörigen HowTo in der Docusnap Knowledge Base.

Q4 Trotz erfolgreicher SUDO Konfiguration und erfolgreicher Inventarisierung werden nicht alle Daten inventarisiert.

A4 Prüfen Sie, ob dem inventarisierenden Benutzer eine Login Shell zur Verfügung steht. Ist diese nicht vorhanden, ist die Inventarisierung unvollständig.

3.6 Mac Systeme

3.6.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
SECURE SHELL (SSH)	22	TCP/UDP

Benötigte Rechte:

- remote Login mit einem kennwortgeschützten Benutzer
- aktivieren des Dienstes „Entfernte Anmeldung“ für den verwendeten Benutzer

3.6.2 Netzwerktechnische Voraussetzungen

- Inventarisierung via Skript ist möglich
- Transparente Firewall Konfiguration

3.7 VMware

3.7.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
HTTPS – HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

Benötigte Rechte:

- Mitglied in der Rolle ReadOnly.

3.7.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration
- Ggf. Proxy Ausnahmen setzen

3.7.3 FAQs

Q1 Eine Verbindung zum ESXi Host bzw. zum vCenter ist im Inventarisierungsassistenten nicht möglich.

A1 Führen Sie bitte einen Verbindungstest der Web API durch und aktivieren Sie diese bzw. setzen Sie ggf. entsprechende Proxy Ausnahmen.

https://Hostname-vCenter/mob

3.8 HP-UX

3.8.1 Protokolle und Berechtigungen

Verwendete Protokolle im Standard:

BEZEICHNUNG	PORT	TRANSPORT
SECURE SHELL (SSH)	22	TCP/UDP

Benötigte Rechte:

- Benutzer mit administrativen Berechtigungen auf dem HP-UX Server

Benötigte Kommandos / Tools:

- bdf - Freier Speicher Informationen
- cprop - System Informationen: Disk/Memory/Network Information/Processors/Firmware/System Summary
- cstm - Kann Skripte ausführen
- swlist - Software Informationen
- grep - Wird zum Parsen von Logdateien genutzt
- uname - Betriebssystem/Kernel infos
- machinfo - Zusätzliche Systeminformationen

3.8.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration

3.9 Hyper-V / IIS Server

3.9.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
DCE ENDPOINT-SOLUTION, NETBIOS SESSION SERVICE, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS-FREIGABEN (CIFS)	135, 139, 445	TCP
DYNAMIC HIGH RANGE PORT	1024 - 65535	TCP/UDP

Benötigte Rechte:

- Lokaler Administrator
  - NetBIOS Schreibweise
  - UPN Schreibweise
- Administrationsrechte Hyper-V Manager
- SharePoint Farmadmin Berechtigungen bei einem SharePoint IIS
  - Eingabe der Authentifizierung mit NetBIOS Name

3.9.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration
- Eindeutige Namensauflösung muss gegeben sein (Forward Lookup & Reverse Lookup).

3.9.3 FAQs

Q1 Ich besitze eine Hyper-V Umgebung / IIS Server, aber keine Domäne. Trotzdem wird im Inventarisierungsdialog eine Authentifizierung gegenüber der Domäne vorausgesetzt.

A1 Im Docusnap Menü – Inventarisierung kann unter Sonstiges eine Domänenauthentifizierung für den Hyper-V und IIS-Assistenten deaktiviert werden. Anschließend ist eine Authentifizierung mit einem lokalen Benutzer möglich.

3.10 Citrix Hypervisor

3.10.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
HTTPS – HYPERTEXT TRANSFER PROTOCOL SECURE	Port kann angepasst werden	TCP

Benötigte Rechte:

- Administrator Berechtigungen auf dem Citrix Hypervisor Server

3.10.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration
- Ggf. Proxy Ausnahmen setzen

3.11 Igel Systeme

3.11.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
SQL DATABASE – MSSQL (MICROSOFT SQL SERVER)	1433	TCP
SQL DATABASE – MSSQL (MICROSOFT SQL SERVER) MONITOR	1434	TCP/UDP
DYNAMIC HIGH RANGE PORT	1024 - 65535	TCP/UDP

Benötigte Rechte:

- Benutzer mit Lese-Berechtigungen auf der Igel Datenbank (db_reader).

3.11.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration
- Datenbank und Server müssen Remote Verbindungen zulassen

3.11.3 FAQs

Q1 Es steht nur eine Igel Embedded Database zur Verfügung. Wie kann Docusnap eine Verbindung zu dieser herstellen?

A1 Docusnap unterstütz bei der Inventarisierung von Linux Systemen mittels dem Igel Assistenten lediglich Microsoft SQL-Datenbanken. Eine Igel Embedded Database wird nicht unterstützt. Diese kann jedoch in eine Microsoft SQL-Umgebung migriert werden. Die genaue Vorgehensweise ist im Igel Handbuch beschrieben.

Q2 Besteht die Möglichkeit einer Inventarisierung der Igel Thin Clients mittels eines Skripts?

A2 Ja. Igel Thin Clients mit einem Linux Betriebssystem können Sie mittels des Linux Skripts inventarisieren. Das Skript finden Sie im Docusnap Installationsverzeichnis, Unterordner Tools. Eine mögliche Methode der automatisierten Ausführung des Skripts ist die Verwendung der Igel UMS.

Hinweis: Der Thin Client wird dadurch als Linux System und nicht als ThinClient in der Datenbank gespeichert.

3.12 SharePoint

3.12.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
DCE ENDPOINT-SOLUTION, WINDOWS-FREIGABEN (CIFS)	135, 445	TCP

Benötigte Rechte:

- Vollständiger Zugriff auf das SharePoint System. Entspricht dem bei der Installation verwendeten FarmAdmin. Angabe des Benutzers mit Domänenzusatz.
    - NetBIOS Schreibweise
    - UPN Schreibweise
- Db_owner Rechte in jeder SharePoint Datenbank
- Administrationsrechte für alle Websitesammlungen
- Ab Windows Server 2008 R2 und der Trennung von SharePoint und SQL-Server kann es zu Authentifizierungsproblemen aufgrund von „Multi-Hop" kommen.
    - In diesem Fall muss der Inventarisierungsbenutzer in die Gruppe der lokalen Administratoren auf dem SharePoint Server aufgenommen werden.
    - FarmAdmin muss im Authentifizierungsdialog hinterlegt werden. Bei der Server Authentifizierung darf kein User hinterlegt sein.

3.12.2 Netzwerktechnische Voraussetzungen

- Inventarisierung via Skript ist möglich
- Transparente Firewall Konfiguration
- Ausführung von PsExec.exe (Microsoft Sysinternals Tool) möglich
- PsExec kann vom Virenscanner geblockt werden

3.12.3 FAQs

Q1 Trotz der Verwendung des vorgegebenen FarmAdmins ist die Inventarisierung fehlerhaft oder nicht vollständig.

A1 Wird bei der SharePoint Installation z. B. ein Domänen-Administrator verwendet, so ist dieser der „echte" FarmAdmin. Prüfen Sie eine Inventarisierung mit diesem User.

3.13 Exchange

3.13.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
DCE ENDPOINT-SOLUTION, NETBIOS SESSION SERVICE, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS-FREIGABEN (CIFS)	135, 139, 445	TCP
DYNAMIC HIGH RANGE PORT – WMI VERBINDUNG	1024 - 65535	TCP/UDP

Benötigte Rechte Exchange Server:

- Lokaler Administrator auf dem/den Exchange Server (PSExec Verbindung)
- View-Only Organization Management / Organization Management
    - NetBIOS Schreibweise
    - UPN Schreibweise

Benötigte Rechte Active Directory:

- Lesenden Zugriff auf die Configuration Partition
- Dies besitzen im Standard nur die Domänen Administratoren
- ADSI Editor
    - Configuration
    - CN=Configuration…
        - CN=Services
        - CN=Microsoft Exchange
        - CN=Domäne
        - CN=Administrative Groups
        - CN=Exchange Administrative Group…
        - CN=Servers

3.13.2 Netzwerktechnische Voraussetzungen

- Inventarisierung via Skript ist möglich
- Transparente Firewall Konfiguration
- Ausführung von PsExec.exe (Microsoft Sysinternals Tool) möglich
- PsExec kann vom Virenscanner geblockt werden

3.13.3 FAQs

Q1 Eine Inventarisierung war erfolgreich, jedoch wurden keine Postfächer ausgewertet

A1 Prüfen Sie bitte, ob der Inventarisierungsuser Mitglied View-Only Organization Management / Organization Management Gruppe ist

3.14 SQL-Server / Veeam Legacy / BackupExec

3.14.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
SQL DATABASE – MSSQL (MICROSOFT SQL SERVER)	1433	TCP
SQL DATABASE – MSSQL (MICROSOFT SQL SERVER) MONITOR	1434	TCP/UDP
DYNAMIC HIGH RANGE PORT	1024 - 65535	TCP/UDP

Benötigte Rechte:

- SysAdmin Berechtigung bei der SQL-Server Inventarisierung
- Wird ein User ohne SysAdmin Rolle verwendet, so ist eine Eingeschränkte Inventarisierung möglich. Es werden nur Teile des SQL-Servers bzw. der Instanz inventarisiert.
- Bei Veeam Legacy und BackupExec Inventarisierung wird ein Benutzer mit Lese-Berechtigungen auf der Veeam bzw. BackupExec Datenbank benötigt (db_reader).
- SQL-User oder Domänen-Benutzer
    - Domänen-Benutzer ist im Inventarisierungsdialog integriert. Dieser kann nicht geändert werden. Sitzungsbenutzer bzw. das hinterlegte Benutzerkonto vom Docusnap Server Dienst wird verwendet.
    - SQL-Benutzer kann pro gefundene Instanz separat hinterlegt werden

3.14.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration
- Datenbank und Server müssen Remote Verbindungen zulassen
- TCP/IP Protokoll bei SQL-Server bzw. Instanz aktiviert.

3.14.3 FAQs

Q1 Bei einer automatischen SQL-Server Suche werden nicht alle SQL-Server gefunden.

A1 Prüfen Sie bitte ob der SQL-Server Browser auf dem zu inventarisierenden SQL-Server aktiv ist. Dieser ist für eine automatische Ermittlung notwendig. SQL-Server Instanzen werden mittels Broadcast ermittelt. Über einen Router hinweg werden keine Systeme gefunden (Broadcast Domäne).

3.15 Oracle Datenbank

3.15.1 Protokolle und Berechtigungen

Verwendete Protokolle im Standard:

BEZEICHNUNG	PORT	TRANSPORT
ORACLE DATENBANK LISTENING FÜR UNSICHERE CLIENT-VERBINDUNGEN ZUM LISTENER, ERSETZT PORT 1521	2483	TCP/UDP
ORACLE DATENBANK LISTENING FÜR SSL CLIENT-VERBINDUNGEN ZUM LISTENER	2484	TCP/UDP

Benötigte Rechte:

- Entsprechend berechtigten Benutzer (DBA). Inventarisierungsbenutzer kann mit Hilfe eines Skripts erzeugt werden.
    - Dieses finden Sie im Docusnap Handbuch im Kapitel „Oracle“ Inventarisierung.
- Angabe von Hostname, Servicename und Port
    - Angaben können in der Konfiguration ausgelesen werden
- Berechtigter User
    - Create Session
    - Select any dictionary

3.15.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration

3.16 Dell EMC² Isilon

3.16.1 Protokolle und Berechtigungen

Verwendete Protokolle im Standard:

BEZEICHNUNG	PORT	TRANSPORT
HTTP. HYPERTEXT TRANSFER PROTOCOL	8080	TCP

Benötigte Rechte:

- Lesender Zugriff mittels Mitgliedschaft der Rolle AuditAdmin
- Neu angelegter Benutzer muss aktiviert werden

3.16.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration
- Ggf. müssen Proxy Ausnahmen gesetzt werden
- Standard-Port kann abweichen

3.17 Active Directory / ADDS Abgleich

3.17.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
LDAP - LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL UNGESICHERT (LDAP) TLS-GESICHERT (LDAPS)	 389 636	TCP/UDP
DCE ENDPOINT-SOLUTION, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS-FREIGABEN (CIFS) – NUR BEI GRUPPENRICHTLINIEN	135, 445	TCP

Benötigte Rechte:

- Für einen vollständigen ADS-Scan ist die Anmeldung als Domänen-Administrator erforderlich.
    - Angabe in NetBIOS oder UPN Schreibweise
- Als Domänen-Benutzer ist eine Abfrage auch möglich – sofern die Standardkonfiguration nicht verändert, wurde
    - Das Auslesen der Konfigurationspartition ist nicht möglich
    - Erfassen von Bitlocker Wiederherstellungsschlüssel ist nicht möglich. Die AD Klasse msFVE_RecoveryInformation ist den Domänen Administratoren vorbehalten
- Für die optionale Inventarisierung der GPOs ist der Zugriff auf den Domänencontroller per PsExec.exe erforderlich
- Für den ADDS Abgleich wird nur ein Domänen Benutzer benötigt.

3.17.2 Netzwerktechnische Voraussetzungen

- Inventarisierung via Skript ist möglich
- Transparente Firewall Konfiguration
- PsExec kann vom Virenscanner geblockt werden

3.17.3 FAQs

Q1 Das Active Directory wurde erfolgreich inventarisiert. Es wurden jedoch keine Benutzer und Gruppen ausgelesen.

A1 Prüfen Sie bitte, ob Ihre Domäne in Docusnap mit dem FQDN hinterlegt wurde; z. B. „docusnap.intern".

Q2 Wie kann vermieden werden, dass der ADDS Abgleich inventarisierte Systeme löscht, die kein Mitglied der Domäne sind?

A2 Setzen Sie beim ADDS Abgleich den OU Filter auf die oberste Ebene. Anschießend vergleicht der Assistent auf die Arbeitsgruppen Domänen Mitgliedschaft. Es werden jetzt nur Systeme entfernt, die nicht mehr existieren und Teil der Domäne waren.

Q3 Gibt es eine Möglichkeit die Bitlocker Recovery Schlüssel auch ohne einen Domänen Administrator zu erfassen?

A3 Alternativ ist es möglich, eine Delegierung zu konfigurieren. Hierbei wird z.B. eine Sicherheitsgruppe Bitlocker erstellt. Diese Gruppe wird über die Objektverwaltung auf die "msFVE-RecoveryInformation" -Objekte berechtigt. Der Inventarisierungsuser wird dann der Gruppe hinzugefügt.
Weitere Informationen dazu finden Sie z.B. bei Microsoft.

3.18 DFS

3.18.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
NETBIOS SESSION SERVICE, MICROSOFT-DS ACTIVE DIRECTORY - WINDOWS-FREIGABEN (CIFS)	139, 445	TCP
DYNAMIC HIGH RANGE PORT	1024 - 65535	TCP/UDP
LDAP - LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL	389	TCP/UDP

Benötigte Rechte:

- Domänen-Benutzer
  - Mitglied der lokalen Administratoren auf den Namespace Servern
  - Mitglied der lokalen Administratoren auf den Servern die Ressourcen für das DFS System bereitstellen
  - NetBIOS Schreibweise
  - UPN-Schreibweise

3.18.2 Netzwerktechnische Voraussetzungen

- Inventarisierung via Skript ist möglich
- Transparente Firewall Konfiguration
- Ausführen der PowerShell
- UAC muss entsprechend konfiguriert sein
- Es können nur Windows DFS-Server inventarisiert werden. Stellt z.B. eine NAS Ressourcen bereit, ist eine Inventarisierung der SMB Share Berechtigungen nicht möglich.

3.18.3 FAQs

Q1 Trotz voller Administrator Berechtigungen erhalte ich die Meldung, dass die Inventarisierung unvollständig ist, und SMB-Zugriffsrechte nicht erfasst werden konnten.

A1 Werden Ressourcen nicht nur auf den DFS Namespace Servern, sondern auch auf anderen Systemen bereitgestellt entsteht ein sog. Double Hop. Windows unterbindet dann die Authentifizierung auf dem zweiten remote System. In diesem Fall muss die Inventarisierung via Skript durchgeführt werden. Alternativ kann ein Discovery Service auf dem DFS Namespace Servern verwendet werden.

3.19 DNS / DHCP

3.19.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
NETBIOS SESSION SERVICE, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS-FREIGABEN (CIFS)	139, 445	TCP
DYNAMIC HIGH RANGE PORT	1024 – 65535	TCP/UDP

Benötigte Rechte:

- Domänen-Administrator bei DNS Servern. Bei DHCP Servern ist ein lokaler Administrator ausreichend
    - NetBIOS Schreibweise
    - UPN Schreibweise

3.19.2 Netzwerktechnische Voraussetzungen

- Inventarisierung via Skript ist möglich
- Transparente Firewall Konfiguration
- .NET Framework Version 4.6.1 oder aktueller
- Ausführen der PowerShell
- PowerShell Version 3 oder aktueller
- DNS & DHCP PowerShell Module müssen auf den zu inventarisierenden Servern vorhanden sein
    - DNS – Microsoft Dokumentation
    - DHCP – Microsoft Dokumentation
- Zugriff auf das Verzeichnis C:\Windows\Temp
- Zugriff auf die Freigabe IPC$

3.20 Azure / Microsoft 365

3.20.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

Benötigte Rechte:

- Um die nötigen Anwendungen zu erstellen, wird ein Global Administrator benötigt.
  - Azure: Registrierte Anwendung mit lesendem Zugriff auf Azure Informationen
  - Microsoft 365: Registrierte Anwendung mit lesendem Zugriff auf Microsoft 365 Informationen

3.20.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration
- Discovery Service muss das Internet erreichen
- Ggf. Proxy Ausnahmen setzten
- Deaktivieren der Option **Microsoft 365-Berichte zeigen anonyme Benutzernamen anstelle von tatsächlichen Benutzernamen an**. Eine Anleitung dazu finden Sie in der Microsoft Knowledge Base.
- Erreichbarkeit folgenden URLs
  - https://login.microsoftonline.com/
  - https://graph.microsoft.com/

3.20.3 FAQs

Q1 Ist eine Authentifizierung via MFA (Multi-Faktor-Authentifizierung) möglich?

A1 Ja. Diese wird automatisch verlangt.

Q2 Es werden weder E-Mail-Postfachinformationen noch SharePoint und OneDrive Daten inventarisiert.

A2 Die Ursache hierfür ist, dass Microsoft 365 im Standard die Option "Ausgeblendete Benutzer-, Gruppen- und Websitenamen in allen Berichten anzeigen" aktiviert hat.

Q3 Können mehrere Docusnap Instanzen dieselbe App zur Inventarisierung verwenden?

A3 Nein. Pro Instanz kann nur eine App verwendet werden.

3.21 Exchange Online

3.21.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

Benötigte Rechte:

- Aktiviertes Active Scripting in den Internetoptionen
- Docusnap startender Benutzer muss Lokaler Administrator sein
- Verwendeter Azure Administrator muss Global Administrator sein

3.21.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration
- Discovery Service muss das Internet erreichen
- Ggf. Proxy Ausnahmen setzten
- 64-Bit Betriebssystem
- .Net Framework 4.8 oder höher
- PowerShell 5.0 oder höher
- Erreichbarkeit folgenden URLs
    - https://login.microsoftonline.com/
    - https://graph.microsoft.com/

3.21.3 FAQs

Q1 Ist eine Authentifizierung via MFA (Multi-Faktor-Authentifizierung) möglich?

A1 Ja. Diese wird automatisch verlangt.

Q2 Ist die von Docusnap erstellte App in meiner Azure Umgebung Global Administrator?

A2 Nein, die App ist kein Global Administrator. Die Berechtigungen der App sind Exchange.ManageAsApp, full_Access_as_app und Global Reader. Da nur die Rolle Global Reader der App zugewiesen ist, kann die Inventarisierungsapp auf Postfächer etc. nur lesend zugreifen.

Q3 Können mehrere Docusnap Instanzen dieselbe App zur Inventarisierung verwenden?

A3 Nein. Pro Instanz kann nur eine App verwendet werden.

3.22 Amazon Web Services - AWS

3.22.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

Benötigte Rechte:

- Benutzer benötigt mindestens folgende Berechtigungen
  - Erstellen von Richtlinien
  - Erstellen eines Benutzers sowie Vergabe der erstellten Richtlinien
- Per Richtlinie werden die Berechtigungen Auflisten sowie Lesen für die Bereiche Service, Aktionen und Ressourcen benötigt

3.22.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration
- Discovery Service muss das Internet erreichen
- Ggf. Proxy Ausnahmen setzten

3.23 Veeam Backup & Replication

3.23.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
NETBIOS SESSION SERVICE, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS-FREIGABEN (CIFS)	139, 445	TCP
DYNAMIC HIGH RANGE PORT	1024 – 65535	TCP/UDP

Benötigte Rechte:

- Lokale Administrationsrechte auf dem Veeam Server
- Mitglied in der Rolle **Veeam Backup Administrators**

3.23.2 Netzwerktechnische Voraussetzungen

- Inventarisierung via Skript ist möglich
- Transparente Firewall Konfiguration
- Veeam Backup & Replication ab Version 11
- Ausführen der PowerShell

3.23.3 FAQs

Q1 Können ältere Veeam Backup and Replication Versionen inventarisiert werden?

A1 Ja, dafür steht der Veeam Legacy Scan zur Verfügung.

Q2 Der Veeam Server ist nicht Teil der Domäne. Deshalb wird für die Inventarisierung ein lokaler Administrator verwendet. Bei der Inventarisierung tritt die Fehlermeldung „Zugriff verweigert" auf.

A2 Der Grund für das Problem ist die User Account Control (UAC). Der Benutzer verbindet mit „normalen Berechtigungen" und der sogenannte Auto-Elevation-Mechanismus, der die Rechte bei Bedarf erhöhen sollte, greift beim Remote Zugriff nicht. Mit Hilfe des folgenden Befehls kann ein Registry Eintrag gesetzt werden, der das Problem umgeht.

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

3.24 NTFS Analyse

3.24.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
NETBIOS SESSION SERVICE, MICROSOFT-DS ACTIVE DIRECTORY - WINDOWS-FREIGABEN (CIFS)	139, 445	TCP

Benötigte Rechte:

- Domänen Benutzer mit Lesen Berechtigung auf die vollständige Ordnerstruktur

3.24.2 Netzwerktechnische Voraussetzungen

- Filesystem auf Basis von NTFS oder ReFS
- Das Filesystem darf nicht als gemapptes Laufwerk auf dem inventarisierenden System vorhanden sein.

VERSIONSHISTORIE

Datum	Beschreibung
20.03.2019	Version 1.0 - Dokumentation erstellt
01.07.2019	Version 1.1 - IP-Scan Modul wurde ergänzt
02.03.2020	Version 1.2 - Linux Inventarisierung mittels SUDO Benutzer wurde ergänzt; AWS hinzugefügt; Verschlüsselte LDAP Verbindung hinzugefügt
10.06.2020	Version 2.0 - Überarbeitung des HowTos für Docusnap 11
24.03.2021	Version 2.1 – Exchange Online Inventarisierung wurde überarbeitet
25.07.2022	Version 2.2 – DNS, DHCP und Exchange Online überarbeitet
08.12.2022	Version 2.3 – Fallback Methode bei Windows Inventarisierung entfernt
26.01.2023	Version 3.0 – Überarbeitete Version für Docusnap 12
17.08.2023	Version 3.1 – Erweiterung Bitlocker – Active Directory Inventarisierung
21.11.2023	Version 4.0 – Überarbeitung des HowTos für Docusnap 13
12.06.2024	Version 4.1 – Überarbeiten der benötigen Berechtigungen