Whitepaper Docusnap Inventarisierung

Technischer Überblick und Lösungsvorschläge zu Problemen bei der Inventarisierung

TITEL	Whitepaper Docusnap Inventarisierung
AUTOR	Docusnap Consulting
DATUM	02.03.2020
VERSION	1.2 | gültig ab 02.03.2020

INHALTSVERZEICHNIS

1. Einleitung

Oftmals treten bei der Erstinventarisierung Probleme durch fehlende Berechtigungen eines Benutzers, oder durch geblockte Ports einer Firewall auf. Um Sie bei der Behebung dieser Probleme zu unterstützen werden die notwendigen Voraussetzungen in den nachfolgenden Kapiteln mittels Ports, Rechten und eines FAQ Teils genauer erläutert.

Das Dokument untergliedert sich in eine tabellarische Übersicht und eine detaillierte Beschreibung der einzelnen Inventarisierungen.

Weiterführende Informationen und HowTos können Sie unserer Docusnap Knowledge Base entnehmen. Diese Finden Sie unter www.docusnap.com im Register Support.

Sämtliche 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 – 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
WINDOWS PSEXEC	DCE Endpoint-Solution bei PsExec, Microsoft-DS Active Directory, Windows-Freigaben (CIFS)	135, 445	TCP
	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

XENCENTER	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 / 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 SQL Net Listener and Data Guard	1521	TCP
DELL EMC² ISILON	http - Hypertext Transfer Protocol	8080	TCP
ACTIVE DIRECTORY / ADS 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	DCE Endpoint-Solution, Microsoft-DS Active Directory, Windows-Freigaben (CIFS)	135, 445	TCP
AZURE / OFFICE 365 / AWS	https - Hypertext Transfer Protocol Secure	443	TCP

3. Inventarisierungen

In den nachfolgenden Kapiteln werden die verschiedenen Inventarisierungen beschrieben.

3.1 Windows – WMI / PsExec (Fallback Methode)

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

Verwendete Protokolle Windows – PsExec:

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

Benötigte Rechte Windows allgemein:

- Domänen Administrator
  - NetBIOS Schreibweise
  - UPN Schreibweise
- Alternativ ist bei Clients und Servern ein Domänen-Benutzer mit lokaler Administrator-Berechtigung möglich
- Bei Verwendung von lokalen Administrator-Rechten bei Windows (IP) UAC beachten. Siehe FAQ für weitere Informationen.
  - Bei einzelner Anmeldung Rechnername\User
  - Bei Sammelinventarisierung .\User

Zusätzliche Rechte – WMI:

- Aktive WMI Dienste auf dem Zielsystem
  - Windows Verwaltungsinstrumentation
  - Remoteprozeduraufruf (RPC)

Zusätzliche Rechte – PsExec:

- Ausführung von PsExec.exe (Microsoft Sysinternals Tool) möglich
  - Testen der Ausführung:
    - C:\Program Files\Docusnap X\bin\PsExec.exe \\Hostname/IP-Adresse -u domäne\benutzer cmd
  - PsExec kann vom Virenscanner geblockt werden:
    - C:\Windows\PSEXESVC.EXE - auf dem Zielsystem freigeben
    - C:\Program Files\Docusnap X\bin\PsExec.exe - auf dem Quellsystem freigeben

3.1.2 Netzwerktechnische Voraussetzungen

- Windows System ist Mitglied des Active Directorys (nur Windows (AD))
- Eindeutige Namensauflösung muss gegeben sein (Forward Lookup & Reverse Lookup)
- Transparente Firewall Konfiguration
- System muss per Ping erreichbar sein
- Bei Verwendung der Fallback Methode muss Ausführung von PsExec erlaubt 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 Wo können weiterführende Informationen zur Inventarisierung gefunden werden?

A3 *Weitere Informationen zur Windows Inventarisierung finden Sie in der Docusnap Knowledge Base.*

- *WMI Zugriffsprobleme*
- *Windows Firewall Ausnahmen*

Q4 Ist eine Windows Inventarisierung mittels Script möglich?

A4 *Ja. Genauere Informationen zur Inventarisierung mit Hilfe eines Scripts finden Sie im zugehörigen HowTo in der Docusnap Knowledge Base.*

- *Docusnap Script Windows*

Q5 Einige Systeme sind über eine langsame Leitung angebunden. Eine Inventarisierung resultiert in einem Timeout Fehler. Wie kann dieser behoben werden?

A5 *Sie können den Timeout in den Inventarisierungsoptionen erhöhen. Navigieren Sie dazu in das Menü Docusnap – Inventarisierung – Allgemein*

Q6 Warum wird PsExec von einem Virenscanner als bedrohlich eingestuft?

A6 *Einige Antivirus-Scanner melden, dass eines oder mehrere der Tools mit einem "remote admin"-Virus infiziert sind. PsTools enthalten keine Viren, sie wurden jedoch von Viren verwendet. Aus diesem Grund tritt unter Umständen eine Virenmeldung auf und PsExec muss aus der Quarantäne freigegeben werden.*

Q7 Wie kann eine Inventarisierung mittels PsExec Verbindung (Fallback Methode) aktiviert werden?

A7 *Sie finden die Option unter Docusnap – Inventarisierung – Tab Inventarisierung. Aktivieren Sie anschließend die Checkbox „Fallbackmethode Windowsinventarisierung" und bestätigen Sie Ihre Änderung mit „OK". Anschließend haben Sie die Inventarisierung mittels PsExec erfolgreich aktiviert.*

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 WinPcap Treibers. Dieser wird für einen „erweiterten IP-Scan" benötigt.
- Wird der „erweiterte IP-Scan" nicht verwendet, wird kein WinPcap Treiber vorausgesetzt. Zusätzliche Funktionen wie z. B. Betriebssystemerkennung sind dadurch nicht möglich.

3.2.2 Netzwerktechnische Voraussetzungen

- Installation des aktuellen WinPcap Treibers auf dem ausführenden System. Kann 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 WinPcap 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

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. Siehe FAQ für weitere Informationen.

3.5.2 Netzwerktechnische Voraussetzungen

- 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 es möglich Linux Systeme per Script zu inventarisieren?

A2 Ja. Genauere Informationen zur Inventarisierung mit Hilfe eines Scripts finden Sie im zugehörigen HowTo in der Docusnap Knowledge Base.

- *Docusnap Script Linux*

Q3 Ist eine Authentifizierung mittels RSA Schlüssel möglich?

A3 Ja. Genauere Informationen zur Inventarisierung per RSA Schlüssel finden Sie im zugehörigen HowTo in der Docusnap Knowledge Base.

- *Linux Inventarisierung mit Authentifizierung per RSA Schlüssel*

Q4 Wie kann eine Inventarisierung mittels SUDO konfiguriert werden?

A4 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.

- *Linux Inventarisierung mit Authentifizierung per RSA Schlüssel*

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

- Transparente Firewall Konfiguration

3.6.3 FAQs

Q1 Ist es möglich Mac Systeme per Script zu inventarisieren?

A1 Ja. Die entsprechende Script Datei finden Sie im Installationsverzeichnis von Docusnap, Unterordner „Bin“.

3.7 VMware

3.7.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
HTTPS – HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

Benötigte Rechte:

- Root User bzw. AD Benutzer mit durchgängigen Administrator-Rechten
- Alternativ besteht die Möglichkeit einen „Read Only" User zu erstellen. Dieser besitzt auf die komplette Umgebung nur Lese-Berechtigungen.

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 oder Domänen-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 XenCenter

3.10.1 Protokolle und Berechtigungen

Verwendete Protokolle:

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

Benötigte Rechte:

- Administrator Rechte auf Xen 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 mindestens 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 Scripts?

A2 *Ja. Igel Thin Clients mit einem Linux Betriebssystem können Sie mittels des Linux Scripts inventarisieren. Die entsprechende Script Datei finden Sie im Installationsverzeichnis von Docusnap, im Verzeichnis „Bin". Eine mögliche Methode der automatisierten Ausführung des Scripts ist die Verwendung der Igel UMS.*

Hinweis: Der Thin Client wird dadurch als Linux System und nicht als Thin Client 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

- 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.*

Q2 Ist eine Inventarisierung mittels Script möglich?

*A2 Ja. Im Docusnap Installationsverzeichnis, Unterordner „Bin" finden Sie ein DocusnapSP** Script. Wählen Sie das entsprechende Script für Ihre SharePoint Version aus. Per CMD oder Power Shell können Sie das Script auf dem SharePoint Server starten. Die Ergebnisse werden in ein Zip Archiv gepackt. Dieses können Sie anschließend per Script Import in Docusnap importieren.*

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:

- Domänen-Administrator sowie Mitgliedschaft in der Gruppe Exchange Organisation-Administrator (Organization Management). Angabe des Benutzers mit Domänenzusatz.
    - NetBIOS Schreibweise
    - UPN Schreibweise

3.13.2 Netzwerktechnische Voraussetzungen

- 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 der Exchange Organisation-Administratoren ist.*

Q2 Ist eine Inventarisierung mittels Script möglich?

A2 *Ja. Genauere Informationen zur Inventarisierung mit Hilfe eines Scripts finden Sie im zugehörigen HowTo in der Docusnap Knowledge Base.*

- *Inventarisierung von Exchange*

Q3 Gibt es weiterführende Informationen zur Exchange Inventarisierung?

A3 Ja. Eine detaillierte Beschreibung der Inventarisierung können Sie dem zugehörigen HowTo in der Docusnap Knowldege Base entnehmen.

- *Inventarisierung von Exchange*

3.14 SQL Server / Veeam / 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 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 gefundener 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 SQL NET LISTENER AND DATA GUARD	1521	TCP

Benötigte Rechte:

- Entsprechend berechtigter Benutzer (DBA). Inventarisierungsbenutzer kann mit Hilfe eines Scripts 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:

- Root Rechte in EMC² Isilon Umgebung.

3.16.2 Netzwerktechnische Voraussetzungen

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

3.17 Active Directory / ADS 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
    - Hierbei ist kein Auslesen der Konfigurationspartition möglich
- Für die optionale GPO Inventarisierung ist der Zugriff auf den Domänencontroller per PsExec.exe erforderlich.

3.17.2 Netzwerktechnische Voraussetzungen

- 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“.*

Q1 Wie kann vermieden werden, dass der ADS Abgleich inventarisierte Systeme löscht, die kein Mitglied der Domäne sind.

A1 *Setzen Sie beim ADS 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.*

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-Administrator
  - NetBIOS Schreibweise
  - UPN Schreibweise

3.18.2 Netzwerktechnische Voraussetzungen

- Transparente Firewall Konfiguration
- DNS (Auflösung und rekursive Auflösung)

3.19 DNS / DHCP

3.19.1 Protokolle und Berechtigungen

Verwendete Protokolle:

BEZEICHNUNG	PORT	TRANSPORT
DCE ENDPOINT-SOLUTION, NETBIOS SESSION SERVICE, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS-FREIGABEN (CIFS)	135, 139, 445	TCP

Benötigte Rechte:

- Domänen-Administrator
  - NetBIOS Schreibweise
  - UPN Schreibweise

3.19.2 Netzwerktechnische Voraussetzungen

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

3.20 Azure / Office365 / AWS

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
    - Office365: Registrierte Anwendung mit lesendem Zugriff auf Office365 Informationen
    - AWS: Per Richtlinie werden die Berechtigungen Auflisten sowie Lesen für die Bereiche Service, Aktionen, Ressourcen benötigt

- Eine detaillierte Beschreibung der Inventarisierung finden Sie in den HowTos der Docusnap Knowledge Base.
    - Inventarisierung von Microsoft Azure
    - Inventarisierung von Microsoft Office 365
    - Inventarisierung von Amazon Web Services (AWS)

3.20.2 Netzwerktechnische Voraussetzungen

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

VERSIONSHISTORIE

Datum	Beschreibung
20.03.2019	Dokumentation erstellt
01.07.2019	IP-Scan Modul wurde ergänzt
02.03.2020	Linux Inventarisierung mittels SUDO Benutzer wurde ergänzt; AWS hinzugefügt; Verschlüsselte LDAP Verbindung hinzugefügt