White Paper Docusnap Inventory

Technical overview and suggested solutions to inventory problems

TITLE	White Paper Docusnap Inventory
AUTHOR	Docusnap Consulting
DATE	07/16/2026
VERSION	6.0 | valid from July 08, 2026

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.

TABLE OF CONTENTS

1. Introduction

Problems often occur during the initial inventory due to missing user authorizations or blocked ports of a firewall. To help you resolve these problems, the following chapters explain the necessary requirements in more detail using ports, authorizations and an FAQ section.

The document is divided into a tabular overview, a detailed description of the individual inventories and a FAQ section.

Further information and HowTos can be found in our Docusnap Knowledge Base. These can be found at www.docusnap.com/en/ in the Support tab.

If a script-based inventory is possible, this is mentioned in the network requirements for the particular inventory.

All information in this White Paper is updated regularly. They may be incomplete.

2. Tabular overview

INVENTORY	PROTOCOL	PORT	LAYER
WINDOWS	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	Procedure Call (RPC), NetBIOS Session Service SMB / CIFS over TCP	135, 139, 445	TCP
	RPC Dynamic Ports	49152 - 65535	TCP/UDP
WINDOWS – AD IN ADDITION	LDAP	389	TCP/UDP
	LDAPS	636	TCP/UDP
SNMP	SNMP - Simple Network Management Protocol	161	UDP
CIFS	SNMP - Simple Network Management Protocol	161	UDP
	SMB / CIFS over TCP	445	TCP
LINUX	Secure Shell (SSH)	22	TCP/UDP
	SSH File Transfer Protocol (SFTP)	115	TCP
MACOS	Secure Shell (SSH)	22	TCP/UDP
VMWARE	https - Hypertext Transfer Protocol Secure	443	TCP
HYPER-V	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	NetBIOS Session Service, SMB / CIFS over TCP	139, 445	TCP
	RPC Dynamic Ports	49152 - 65535	TCP/UDP
HP-UX	Secure Shell (SSH)	22	TCP/UDP
CITRIX HYPERVISOR	https – Hypertext Transfer Protocol Secure	variable	TCP
NUTANIX	https – Hypertext Transfer Protocol Secure	9440	TCP
PROXMOX	https – Hypertext Transfer Protocol Secure	9440	TCP
IIS	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	Procedure Call (RPC), NetBIOS Session Service SMB / CIFS over TCP	135, 139 445	TCP
	RPC Dynamic Ports	49152 - 65535	TCP/UDP
IGEL	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	Procedure Call (RPC), SMB / CIFS over TCP	135, 445	TCP
EXCHANGE	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	Procedure Call (RPC), NetBIOS Session Service SMB / CIFS over TCP	135, 139 445	TCP
	RPC Dynamic Ports	49152 - 65535	TCP/UDP
SQLSERVER / 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	Oracle database listening for unsecure client connections to listener, replaces port 1521	2483	TCP/UDP

	Oracle database listening for SSL client connections to listener	2484	TCP/UDP
DELL EMC ISILON	http Hypertext Transfer Protocol	8080	TCP
ACTIVE DIRECTORY / ADDS SYNCHRONIZATION	LDAP	389	TCP/UDP
	LDAPS	636	TCP/UDP
ACTIVE DIRECTORY – GROUP POLICIES	Procedure Call (RPC), SMB / CIFS over TCP	135, 445	TCP
DFS	NetBIOS Name Service, NETBIOS Datagram Service	137, 138	UDP
	NetBIOS Session Service, SMB / CIFS over TCP	139, 445	TCP
	RPC Dynamic Ports	49152 - 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, SMB / CIFS over TCP	139, 445	TCP
	RPC Dynamic Ports	49152 - 65535	TCP/UDP
AZURE / MICROSOFT 365 / EXCHANGE ONLINE / AWS	https – Hypertext Transfer Protocol Secure	443	TCP
VEEAM BACKUP & REPLICATION	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	NetBIOS Session Service, SMB / CIFS over TCP	139, 445	TCP
	RPC Dynamic Ports	49152 - 65535	TCP/UDP
NTFS ANALYSE	NetBIOS Session Service, SMB / CIFS over TCP	139, 445	TCP
HPE-STORAGES	https – Hypertext Transfer Protocol Secure	8080 / 443	TCP
WARRANTY ENQUIRIES	https – Hypertext Transfer Protocol Secure	443	TCP
MERAKI	https – Hypertext Transfer Protocol Secure	443	TCP

3. Inventories

In the following chapters the different inventories are described.

3.1 Windows

3.1.1 Protocols and Authorizations

Protocols used Windows WMI:

DESIGNATION	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
PROCEDURE CALL (RPC), NETBIOS SESSION SERVICE SMB / CIFS OVER TCP	135, 139, 445	TCP
RPC DYNAMIC PORTS	49152 - 65535	TCP/UDP
ZUSÄTZLICH BEI WINDOWS AD		
LDAP	389	TCP/UDP
LDAPS	636	TCP/UDP

Required rights Windows general:

- Local administrator on Windows clients and servers. A domain administrator is required for domain controllers.
  - NetBIOS notation
  - UPN notation
- When using local administrator rights with Windows (IP), observe UAC.
  - Syntax: .\user
- Active WMI services on the target system
  - Windows Management Instrumentation
  - Remote Procedure Call (RPC)

3.1.2 Network infrastructure requirements

- Inventory via script is possible
- Windows system is member of Active Directory (Windows (AD) only)
- Unique name resolution must be given (Forward Lookup & Reverse Lookup)
- Transparent firewall configuration
- During the Windows (IP) scan, the system must be accessible via ping if IP address ranges are used
- For a complete inventory, it must be possible to execute PowerShell

3.1.3 FAQs

Q1 Despite authentication with a sufficiently authorized user, the error message "Connection could not be established" appears. What's the problem?

A1 When authenticating against the domain, please use a user specification with domain suffix.

- *User principal name* *UserName@Example.intern*
- *Down-level logon name* *Example\UserName*

Q2 Despite using a user with local administrator membership, the "Access denied" error message occurs.

A2 *The reason for the problem is the User Account Control (UAC). The user connects with "normal permissions" and the so-called auto-elevation mechanism, which should increase permissions if necessary, does not work with remote access. With the following command a corresponding registry entry can be set which solves the problem.*

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

Q3 Some systems are connected via a slow line. An inventory results in a timeout error. How can it be fixed?

A3 *You can increase the timeout in the inventory options. Navigate to the menu Docusnap - Inventory - General*

Q4 Do I need to be able to execute PowerShell in order to successfully inventory my clients?

A4 *No. PowerShell is used to inventory additional information such as certificates. If the execution of PowerShell is blocked, only this information is not collected.*

3.2 IP-Scan

3.2.1 Protocols and Authorizations

A detailed overview of the ports used during the IP Scan cannot be given. Depending on how the IP Scan is configured, different ports are scanned. A distinction can be made between individual ports up to a complete range. In theory, it is possible for the IP Scan to check all possible ports.

Note: Due to a high number of ICMP requests, an IP Scan can cause the network monitoring to generate warning messages. Monitoring tools can also issue a warning message that invalid packets are being sent. This behavior is normal for an IP Scan. These packets are sent so that, for example, the operating system can be recognized.

Required rights:

- Enable the call of Npcap. In some cases, antivirus vendors block Npcap from being called from another software.
- Local administrator rights to install the Npcap driver. This is required for an extended IP Scan.
- If the extended IP Scan is not used, no Npcap driver is required. Additional functions such as operating system recognition are therefore not possible.

3.2.2 Network infrastructure requirements

- Installation of the current Npcap driver on the running system. Can be selected in the setup routine or installed subsequently.
- Various third-party software can influence the execution of the IP-Scan, e.g. Wireshark.

3.2.3 FAQs

Q1 If a complete IP range is specified, not all systems in this range will be found. However, it is possible to scan the systems individually. What is the mistake?

A1 *If the systems are found individually during the scan, a scan should also be possible by specifying an IP range. If necessary, please check your firewall settings regarding ICMP Flooding Protection.*

Q2 How do I know if the current Npcap driver is installed?

A2 *As soon as the extended mode is activated in the wizard, Docusnap checks if the additional network driver is available. If this is not installed, the extended mode is not possible.*

Q3 My IP systems have either no or an incorrect MAC address. What is the reason for this?

A3 *As NMAP uses ARP queries to determine MAC addresses, this only works for devices in the same subnet. ARP queries are not sent across routers. Therefore, NMAP cannot see the MAC addresses of devices in other subnets as it does not have direct layer 2 access to these devices.*

3.3 SNMP

3.3.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
SNMP - SIMPLE NETWORK MANAGEMENT PROTOCOL	161	UDP

Note: Due to a high number of ICMP requests, an SNMP inventory can cause the network monitoring system to generate warning messages.

Required rights:

- Read community string - in standard public
- Authentication credentials for SNMP v3
- SNMP manager (querying system, e.g. Docusnap Server) must be authorized for SNMP polling on the SNMP agent (**whitelisting**).

3.3.2 Network infrastructure requirements

- SNMP protocol is enabled. V1, V2 or V3
- Transparent firewall configuration
- System must be reachable via ping. Can optionally be deactivated in the Scan Assistant.

3.3.3 FAQs

Q1 If a complete IP range is specified, not all systems in this range are found. However, an inventory of the systems is possible individually. What is the mistake?

A1 *If the systems are inventoried individually, an inventory should also be possible by specifying an IP range. If necessary, please check your firewall settings regarding ICMP Flooding Protection.*

3.4 CIFS

With the help of the CIFS inventory, releases of systems (e.g. NAS, etc.) can be recorded. Thus, the CIFS inventory forms the basis for an authorization analysis in Docusnap.

The system to be inventoried via CIFS must not already be registered via Linux or Windows wizards.

3.4.1 Protocols and Authorizations

Protocols used:

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

Required rights:

- Read community string
- Domain administrator or comparable - depending on system
- Authorization to start SNMP queries on the target system

3.4.2 Network infrastructure requirements

- Transparent firewall configuration
- If a user other than the currently logged in user is used for the CIFS inventory, the currently logged in user must not establish a connection to the CIFS system (e.g. connection via a network drive).
    - These can be checked using the *net use* command.
- Special case: NAS system groups must be considered (readout of SMB permissions)

3.5 Linux

3.5.1 Protocols and Authorizations

Protocols used:

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

Required rights:

- root user
- remote login as root allowed
- SUDO user with corresponding SUDO configuration. See FAQ for more information.

3.5.2 Network infrastructure requirements

- Inventory via script is possible
- Transparent firewall configuration
- supported Linux derivative
  - An overview of the supported derivatives can be found in the Docusnap system requirements.

3.5.3 FAQs

Q1 The system was successfully inventoried, but only part of the information is visible.

A1 To ensure that the collected information is complete, you must use the root user. Only with the root user a complete inventory is possible if no SUDO configuration is used.

Q2 Is authentication via RSA key possible?

A2 Yes, you can find more detailed information about the inventory by RSA key in the corresponding HowTo in the Docusnap Knowledge Base.

Q3 How can an inventory be configured using SUDO?

A3 To enable an inventory with SUDO users Docusnap and the Linux system must be configured accordingly. For more information please refer to the corresponding HowTo in the Docusnap Knowledge Base.

Q4 Despite successful SUDO configuration and successful inventory, not all data is inventoried.

A4 Check if a login shell is available to the user doing the inventory. If this is not available, the inventory is incomplete.

3.6 macOS

3.6.1 Protocols and Authorizations

Protocols used:

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

Required rights:

- remote login with a password-protected user
- Activate the "Remote login" service for the user used.

3.6.2 Network infrastructure requirements

- Inventory via script is possible
- Transparent firewall configuration

3.7 VMware

3.7.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

Required rights:

- Member of the ReadOnly role

3.7.2 Network infrastructure requirements

- Transparent firewall configuration
- Set proxy exceptions if necessary

3.7.3 FAQs

Q1 You cannot connect to the ESXi Host or vCenter in the Inventory Wizard.

A1 *Please perform a connection test of the Web API and activate it or set proxy exceptions if necessary.*

https://hostname-vCenter/mob

3.8 Hyper-V

3.8.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
NETBIOS SESSION SERVICE, SMB / CIFS OVER TCP	139, 445	TCP
RPC DYNAMIC PORTS	49152 - 65535	TCP/UDP

Required rights:

- Local administrator
  - NetBIOS notation
  - UPN notation

3.8.2 Network infrastructure requirements

- Inventory via script is possible
- Transparent firewall configuration
- .NET Framework version 4.6.1 or later
- Execute PowerShell
- PowerShell version 3 or later
- Access to the directory C:\Windows\Temp
- Access to the share IPC$

3.8.3 FAQs

Q1 I own a Hyper-V environment / IIS server, but no domain. Nevertheless, an authentication against the domain is assumed in the inventory dialog.

A1 *In the Docusnap menu - Inventory - Inventory tab – section Other a domain authentication for the Hyper-V and IIS wizard can be deactivated. Authentication with a local user is then possible.*

3.9 HP-UX

3.9.1 Protocols and Authorizations

Protocols used in the standard system:

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

Required rights:

- Users with administrative authorizations on the HP-UX Server

Required commands / tools:

- bdf - Free Memory Information
- cprop - System Information: Disk/Memory/Network Information/Processors/Firmware/System Summary
- cstm - Can execute scripts
- swlist - Software Information
- grep - Used to parse log files
- uname - Operating system/kernel info
- machinfo - Additional system information

3.9.2 Network infrastructure requirements

- Transparent firewall configuration

3.10 Citrix Hypervisor

3.10.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE	variable	TCP

Required rights:

- Administrator rights on Citrix Hypervisor Server

3.10.2 Network infrastructure requirements

- Transparent firewall configuration
- Set proxy exceptions if necessary

3.11 Nutanix

3.11.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS – HYPERTEXT TRANSFER PROTOCOL SECURE	9440	TCP

Required rights

- View-permission

3.11.2 Network requirements

- Inventory via script is possible
- Transparent firewall configuration
- If necessary, proxy exceptions must be set.

3.11.3 FAQs

Q1 You cannot connect to the Nutanix Cluster in the Inventory Wizard.

A1 *Please perform a connection test of the Web API and activate it or set appropriate proxy exceptions if necessary.*

➔ *https://NutanixCluster:9440*

Q2 How can the user be created with view permissions? The selection only allows User Admin, Cluster Admin and Backup Admin.

A2 *Only the user has to be created, without role assignment. In this way, the user receives the view permissions.*

3.12 Proxmox

3.12.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS – HYPERTEXT TRANSFER PROTOCOL SECURE	9440	TCP

Required rights

- Users, including realms (e.g., docusnap@pam), with read permissions on the cluster

3.12.2 Network requirements

- Inventory via script is possible
- Transparent firewall configuration
- If necessary, proxy exceptions must be set
- A cluster node must be reachable.

3.13 IIS

3.13.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
PROCEDURE CALL (RPC), NETBIOS SESSION SERVICE SMB / CIFS OVER TCP	135, 139 445	TCP
RPC DYNAMIC PORTS	49152 - 65535	TCP/UDP

Required rights:

- Local administrator
  - NetBIOS notation
  - UPN notation
- Administration rights Hyper-V manager
- SharePoint Farmadmin permissions on a SharePoint IIS
  - Enter the authentication with NetBIOS name

3.13.2 Network infrastructure requirements

- Transparent firewall configuration
- Unique name resolution must be given (forward lookup & reverse lookup).

3.13.3 FAQs

Q1 I own a Hyper-V environment / IIS server, but no domain. Nevertheless, an authentication against the domain is assumed in the inventory dialog.

A1 In the Docusnap menu - Inventory - Inventory tab – section Other a domain authentication for the Hyper-V and IIS wizard can be deactivated. Authentication with a local user is then possible.

3.14 Igel

3.14.1 Protocols and Authorizations

Protocols used:

DESIGNATION	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

Required rights:

- Users with at least read permissions on the Igel database (**db_reader**).

3.14.2 Network infrastructure requirements

- Transparent firewall configuration
- Database and server must allow remote connections

3.14.3 FAQs

Q1 There is only an Igel embedded Database available. How can Docusnap connect to it?

A1 *Docusnap only supports Microsoft SQL databases when inventorying Linux systems using the Igel wizard. An Igel embedded database is not supported. However, this can be migrated to a Microsoft SQL environment. The exact procedure is described in the Igel manual.*

Q2 Is it possible to inventory the Igel thin clients using a script?

A2 *Yes, you can inventory Igel thin clients with a Linux operating system using the Linux script. You can find the script in the Docusnap installation directory, subfolder Tools. A possible method of automated execution of the script is to use the Igel UMS.*

Note: The thin client is stored in the database as a Linux system and not as a thin client.

3.15 SharePoint

3.15.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
PROCEDURE CALL (RPC), SMB / CIFS OVER TCP	135, 445	TCP

Required rights:

- Full access to the SharePoint system. Corresponds to the FarmAdmin used during the installation. It is necessary to add the domain suffix to the username.
  - NetBIOS notation
  - UPN notation
- Db_owner rights in every SharePoint database
- Administration rights for all website collections
- Starting with Windows Server 2008 R2 and the separation of SharePoint and SQL Server, authentication problems may occur due to "multi-hop".
  - In this case, the inventory user must be included in the group of local administrators on the SharePoint server.
  - FarmAdmin must be stored in the authentication dialog. No user may be stored for server authentication.

3.15.2 Network infrastructure requirements

- Inventory via script is possible
- Transparent firewall configuration
- Execution of PsExec.exe (Microsoft Sysinternals Tool) possible
- PsExec can be blocked by virus scanner

3.15.3 FAQs

Q1 Despite the use of the specified FarmAdmin, the inventory is erroneous or incomplete.

A1 *If, for example, a domain administrator is used during the SharePoint installation, this is the "real" FarmAdmin. Check an inventory with this user.*

3.16 Exchange

3.16.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
PROCEDURE CALL (RPC), NETBIOS SESSION SERVICE SMB / CIFS OVER TCP	135, 139 445	TCP
RPC DYNAMIC PORTS	49152 - 65535	TCP/UDP

Required rights:

- Local administrator on the Exchange server(s) (PSExec connection)
- View-Only Organization Management / Organization Management
    - NetBIOS notation
    - UPN notation

Required Active Directory rights:

- Read access to the configuration partition
- Only the domain administrators have this by default
- ADSI Edit
    - Configuration
    - CN=Configuration…
        - CN=Services
        - CN=Microsoft Exchange
        - CN=Domain
        - CN=Administrative Groups
        - CN=Exchange Administrative Group
        - CN=Servers

3.16.2 Network infrastructure requirements

- Inventory via script is possible
- Transparent firewall configuration
- Execution of PsExec.exe (Microsoft Sysinternals Tool) possible
- PsExec can be blocked by virus scanner

3.16.3 FAQs

Q1 An inventory was successful, but no mailboxes were evaluated.

A1 Please check whether the inventory user is a member of the View-Only Organization Management / Organization Management group.

3.17 SQL-Server / BackupExec

3.17.1 Protocols and Authorizations

Protocols used:

DESIGNATION	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

Required rights:

- SysAdmin authorization for SQL Server inventory
- If a user without SysAdmin role is used, a "limited inventory" is possible. Only parts of the SQL Server or the instance are inventoried.
- For BackupExec inventory a user with read permissions on the BackupExec database is required (db_reader).
- SQL user or Domain user
  - Domain user is integrated in the inventory dialog. This cannot be changed. The session user or the deposited user account of the Docusnap Server service is used.
  - SQL user can be stored separately for each instance found

3.17.2 Network infrastructure requirements

- Transparent firewall configuration
- Database and server must allow remote connections
- TCP/IP protocol activated for SQL server or instance.

3.17.3 FAQs

Q1 In an automatic SQL server search, not all SQL servers are found.

A1 *Please check whether the SQL server browser is active on the SQL server to be inventoried. This is necessary for automatic determination. SQL server instances are determined using broadcast. No systems are found across a router (broadcast domain).*

3.18 Oracle

3.18.1 Protocols and Authorizations

Protocols used in the standard system:

DESIGNATION	PORT	TRANSPORT
ORACLE DATABASE LISTENING FOR UNSECURE CLIENT CONNECTIONS TO LISTENER, REPLACES PORT 1521	2483	TCP/UDP
ORACLE DATABASE LISTENING FOR SSL CLIENT CONNECTIONS TO LISTENER	2484	TCP/UDP

Required rights:

- Correspondingly authorized user (DBA). Inventory user can be created with the help of a script.
  - This can be found in the Docusnap manual in the chapter "Oracle" Inventory.
- Specify host name, service name, and port.
  - Data can be read out in the configuration
- Authorized user
  - Create session
  - Select any dictionary

3.18.2 Network infrastructure requirements

- Transparent firewall configuration

3.19 Dell EMC Isilon

3.19.1 Protocols and Authorizations

Protocols used in the standard system:

DESIGNATION	PORT	TRANSPORT
HTTP. HYPERTEXT TRANSFER PROTOCOL	8080	TCP

Required rights:

- Read access via membership of the AuditAdmin role
- New user must be activated

3.19.2 Network infrastructure requirements

- Transparent firewall configuration
- If necessary, proxy exceptions must be set.
- Standard port may be different

3.20 Active Directory / ADDS Synchronization

3.20.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
LDAP - LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL UNGESICHERT (LDAP) TLS-GESICHERT (LDAPS)	 389 636	TCP/UDP
GROUP POLICIES ONLY: PROCEDURE CALL (RPC), SMB / CIFS OVER TCP	135, 445	TCP

Required rights:

- A full ADS scan requires a domain administrator login.
  - Specification in NetBIOS or UPN notation
- As a domain user, a query is also possible - if the default configuration has not been changed.
  - It is not possible to read the configuration partition here.
  - Bitlocker recovery key cannot be captured. The AD class msFVE_RecoveryInformation is only accessible for domain administrators.
- Optional GPO inventory requires access to the domain controller via PsExec.exe.

3.20.2 Network infrastructure requirements

- Inventory via script is possible
- Transparent firewall configuration
- PsExec can be blocked by virus scanner

3.20.3 FAQs

Q1 The Active Directory was successfully inventoried. However, no users and groups were read out.

A1 Please check whether your domain is stored in Docusnap with the FQDN; e.g. "docusnap.internal".

Q2 How can it be avoided that the ADS reconciliation deletes inventoried systems that are not members of the domain?

A2 Set the OU filter to the uppermost level during ADS adjustment. Subsequently, the wizard compares the workgroup domains to membership domains. Only systems that no longer exist and were part of the domain are now removed.

Q3 Is there a way to capture the Bitlocker recovery keys without a domain administrator?

A3 Alternatively, it is possible to configure a delegation. In this case, a Bitlocker security group is created, for example. This group is then authorized to the "msFVE-RecoveryInformation"

objects via the object management. The inventory user is then added to the group. Further information about this can be found e.g. at Microsoft.

3.21 DFS

3.21.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
NETBIOS SESSION SERVICE, SMB / CIFS OVER TCP	139, 445	TCP
RPC DYNAMIC PORTS	49152 - 65535	TCP/UDP
LDAP - LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL	389	TCP/UDP

Required rights:

- Domain User
  - Member of the local administrators on the Namespace Servers
  - Member of the local administrators on the servers that provide resources for the DFS system
  - NetBIOS negation
  - UPN negation

3.21.2 Network infrastructure requirements

- Inventory via script is possible
- Transparent firewall configuration
- Execute PowerShell
- UAC must be configured correctly
- Only Windows DFS servers can be inventoried. If, for example, a NAS provides resources, an inventory of the SMB share permissions is not possible.

3.21.3 FAQs

Q1 Even though I have full administrator rights, I receive the message that the inventory is incomplete and SMB access rights could not be inventoried.

A1 *If resources are not only provided on the DFS namespace servers, but also on other systems, a double hop occurs. Windows then blocks authentication on the second remote system. In this case, the inventory must be executed by script. Alternatively, a discovery service can be deployed on the DFS namespace servers.*

3.22 DNS / DHCP

3.22.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
NETBIOS SESSION SERVICE, SMB / CIFS OVER TCP	139, 445	TCP
RPC DYNAMIC PORTS	49152 - 65535	TCP/UDP

Required rights:

- Domain administrator for DNS servers. A local administrator is adequate for DHCP servers and Hyper-V hosts.
    - NetBIOS notation
    - UPN notation

3.22.2 Network infrastructure requirements

- Inventory via script is possible
- Transparent firewall configuration
- .NET Framework version 4.6.1 or later
- Execute PowerShell
- PowerShell version 3 or later
- DNS and DHCP PowerShell modules must be installed on the servers to be inventoried
    - DNS – Microsoft Documentation
    - DHCP – Microsoft Documentation
- Access to the directory C:\Windows\Temp
- Access to the share IPC$

3.23 Azure / Microsoft 365

3.23.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

Required rights:

- A global administrator is required to create the necessary applications.
  - Azure: registered application with read access to Azure information
  - Microsoft 365: Registered application with read access to Microsoft 365 information

3.23.2 Network infrastructure requirements

- Transparent firewall configuration
- Discovery service must reach the Internet
- If necessary, set proxy exceptions.
- Disable the option "Microsoft 365 reports show anonymous user names instead of actual user names". You can find instructions on setting this option in the Microsoft Knowledge Base.
- The following URLs must be accessible
  - https://login.microsoftonline.com/
  - https://graph.microsoft.com/

3.23.3 FAQs

Q1 Is authentication via MFA (multi-factor authentication) possible?

A1 Yes. This is automatically requested.

Q2 Neither email mailbox information nor SharePoint and OneDrive data is inventoried.

A2 The reason for this is that Microsoft 365 has the option " Display concealed user, group, and site names in all reports" enabled by default.

Q3 Can multiple Docusnap instances use the same app for inventory?

A3 No. Only one app can be used per instance.

3.24 Exchange Online

3.24.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

Required rights:

- Active Scripting enabled in Internet Options
- Docusnap starting user must be Local Administrator
- Azure Administrator used must be Global Administrator

3.24.2 Network infrastructure requirements

- Transparent firewall configuration
- Discovery service must reach the internet
- If necessary, set proxy exceptions.
- 64-bit operating system
- .Net Framework 4.8 or later
- PowerShell 5.0 or later
- The following URLs must be accessible
  - https://login.microsoftonline.com/
  - https://graph.microsoft.com/

3.24.3 FAQs

Q1 Is authentication via MFA (multi-factor authentication) possible?

A1 Yes. This will be requested automatically.

Q2 Is the app created by Docusnap Global Administrator in my Azure environment?

A2 No, the app is not a Global Administrator. The permissions of the app is Exchange.ManageAsApp, full_Access_as_app and Global Reader. Because only the Global Reader role is assigned to the app, the inventory app can access mailboxes, etc. in read-only mode.

Q3 Can more than one Docusnap instance use the same app for inventory?

A3 No. Only one app can be used per instance.

3.25 Amazon Web Services - AWS

3.25.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

Required rights:

- User needs at least the following permissions
  - Creating policies
  - Create a user and assign the created policies
- By policy, the permissions list and read are required for the areas service, actions and resources

A detailed description of the inventory can be found in the HowTos of the Docusnap Knowledge Base.

- Inventory of Amazon Web Services (AWS)

3.25.2 Network infrastructure requirements

- Transparent firewall configuration
- Discovery service must reach the Internet
- If necessary, set proxy exceptions.

3.26 Veeam backup & Replication

3.26.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
NETBIOS SESSION SERVICE, SMB / CIFS OVER TCP	139, 445	TCP
RPC DYNAMIC PORTS	49152 - 65535	TCP/UDP

Required rights:

- Local administrator on the Veeam server
- Member of the Role Veeam Backup Admistrators

Network infrastructure requirements

- Inventory via script is possible
- Transparent firewall configuration
- Veeam Backup & Replication from version 11
- Execute PowerShell
- MFA must be disabled for the inventory user (service account).
    - User manual

3.26.2 FAQs

Q1 Is it possible to inventory older Veeam Backup and Replication versions?

A1 *Yes. You can use the Veeam Legacy scan.*

Q2 The Veeam server is not part of the domain. Therefore, a local administrator is used for the inventory. The error message "Access denied" occurs during the inventory.

A2 *The reason for the problem is the User Account Control (UAC). The user connects with "normal permissions" and the so-called auto-elevation mechanism, which should increase permissions, if necessary, does not work with remote access. With the following command a corresponding registry entry can be set which solves the problem.*

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

Q3 Disabling MFA (multi-factor authentication) is not an option. Do I have an alternative solution?

A3 *Yes, you can schedule a task to run Discovery-Veeam.exe using the local system account.*

3.27 NTFS Analysis

3.27.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
NETBIOS SESSION SERVICE, SMB / CIFS OVER TCP	139, 445	TCP

Required rights

- Domain users with read permission to the entire file structure

3.27.2 Network infrastructure requirements

- Filesystem based on NTFS or ReFS
- The file system is not allowed to be available as a mapped drive on the system making the inventory.

3.28 HPE-Storages

3.28.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS – HYPERTEXT TRANSFER PROTOCOL SECURE	8080 / 443	TCP

Required rights

- View permission / Browse Role

3.28.2 Network requirements

- WSAPI server (command: cli% startwsapi) started
- Inventory via script is possible
- Transparent firewall configuration
- If necessary, proxy exceptions must be set.

3.28.3 FAQs

Q1 Which HPE Storages can be inventoried?

A1 Following HPE Storages can be inventoried.

- *3PAR (Port 8080)*
- *Alletra (Port 443)*
- *Primera (Port 443)*

3.29 Warranty enquiries

3.29.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS – HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

3.29.2 Network requirements

- Transparent firewall configuration.
- If necessary, proxy exceptions must be set.
- The following URLs must be accessible
  - https://docusnap365.com/api/ds-dispatcher/

3.29.3 FAQs

Q1 For which system types in Docusnap are the warranty queries performed?

A1 *Windows, Linux and VMware ESXi-Server*

Q3 How are the warranty enquiries carried out / "Who" performs them?

A3 *Warranty queries are triggered when system information is stored in Docusnap. No matter if it is a remote or script inventory. The query is performed by the Docusnap Server service during a scheduled execution. In the case of an inventory with the Docusnap Client, the client performs the query.*

Q3 For which manufacturers can the warranty inquiries be done?

A3 *A current overview is documented in the manual.*

3.30 Meraki

3.30.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS – HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

3.30.2 Network requirements

- An API key belonging to a dashboard administrator with read access to the organization
- Organization-wide read permissions are sufficient

3.30.3 FAQs

Q1 Are multiple API keys required?

A1 No. A single API key centrally manages the entire organization—including all networks and devices—through the Meraki cloud.

VERSION HISTORY

Date	Description
03/20/2019	Version 1.0 - Documentation created
07/01/2019	Version 1.1 - IP Scan module was added
03/02/2020	Version 1.2 - Linux inventory using SUDO user was added; AWS added; Added encrypted LDAP connection
06/20/2020	Version 2.0 - Revision of the HowTos for Docusnap 11
03/24/2021	Version 2.1 – Exchange Online inventory has been revised
07/25.2022	Version 2.2 - DNS, DHCP and Exchange Online has been revised
12/08/2023	Version 2.3 – Removed fallback method for Windows inventory
08/17/2023	Version 3.1 - Added Bitlocker - Active Directory Inventory
11/21/2023	Version 4.0 - Revision of the HowTos for Docusnap 13
06/12/2024	Version 4.1 - Revise the required authorisations
11/28/2024	Version 5.0 - Revision of the HowTos for Docusnap 14
04/10/2025	Version 5.1 – Revise the ports and descriptions
06/10/2025	Version 5.2 - Legacy wizards removed and warranty queries extended
08/27/2025	Version 5.3 – Veeam B&R – inventory has been revised
11/11/2025	Version 5.4 – Network requirements extended
08/07/2026	Version 6.0 - Revision of the HowTos for Docusnap 15

© Docusnap GmbH - www.docusnap.com