Docusnap 15

Neuerungen, Veränderungen und Upgrade auf Docusnap 15

TITEL	Docusnap 15
AUTOR	Kevin Reidelbach
DATUM	07.09.2026
VERSION	1.1 | gültig ab 07.09.2026

INHALTSVERZEICHNIS

1. Einleitung

Mit dem Release von Docusnap 15 werden einige Neuerungen und Änderungen in Docusnap eingeführt. Dieses Dokument soll Ihnen einen Überblick über die Neuerungen und Änderungen geben. Außerdem wird beschrieben, wie Sie ein Upgrade auf Docusnap 15 durchführen können.

Neue Systemvoraussetzungen

- **Ab Docusnap 15 wird mindestens ein Microsoft SQL Server 2017 (Express) benötigt!**
- **Zudem muss der Kompatibilitätsgrad der Docusnap Datenbank auf mindestens „SQL Server 2017 (140)“ gesetzt sein.**
  Dieser lässt sich mit Hilfe des SQL Management Studios konfigurieren:

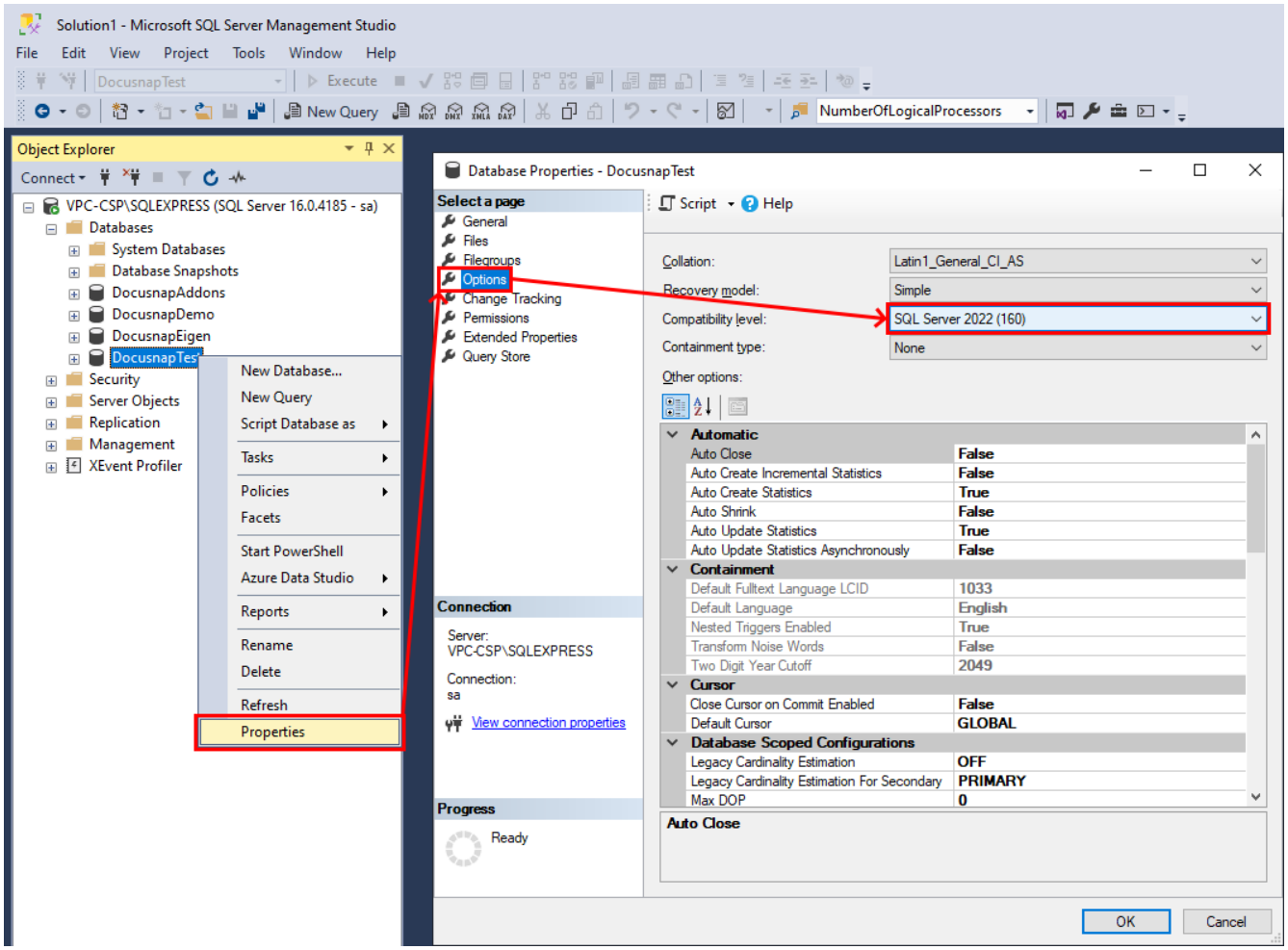

Abbildung 1 - Datenbank Kompatibilitätsgrad

Neue Funktionen

- Proxmox Inventarisierung
- Meraki Inventarisierung
- Erweiterter Schutz

Änderungen

- Hyper-V
  - **Anpassung erforderlich!**
- Gruppenrichtlinien (GPO)
  - **Keine Anpassung erforderlich!**
- Neuerungen und Änderungen bei den Discovery Services
  - **Anpassung erforderlich!**
- Linux – Docker Informationen
  - **Keine Anpassung erforderlich!**
- Discovery Services – Komponenten und Sicherheitsfeatures
  - **Anpassung empfohlen (manuelle Neuinstallation)!**
- Entfernung von Legacy-Assistenten
  - Office 365
  - DFS-Legacy

Upgrade durchführen

1. Docusnap 13 oder 14 ist installiert
2. Aktiver Servicevertrag / Miete vorhanden
3. Upgrade auf dem Docusnap Server starten
   Installations-Datei herunterladen – ausführen – Installation durchführen
4. Verknüpfungen mit zentraler Konfigurationsdatei anpassen bei Verwendung des Startparameters -UseConfig
5. Standardprogrammpfad zur Docusnap.exe lautet nun …\Docusnap\…
6. Datenbank-Update durchführen
   Vorher prüfen, wann die letzte Datenbanksicherung durchgeführt wurde!
7. Verwendete Skriptdateien austauschen / Freigabepfad anpassen
8. DDS-Installationen manuell aktualisieren!
   Aktualisierung der Komponenten und neue Sicherheitsmaßnahmen.
9. Docusnap Clientsysteme aktualisieren

2. Upgrade durchführen

Für das kostenlose Upgrade auf Docusnap 15 ist ein aktiver Service- oder Mietvertrag erforderlich! Vorhandene Aktivierungsschlüssel behalten ihre Gültigkeit. Hier können Sie Docusnap 15 herunterladen.

Ein Upgrade auf Docusnap 15 ist ab Docusnap 13 möglich.

1. Upgrade am Server starten

Im ersten Schritt starten Sie das Upgrade auf dem Docusnap Server. Laden Sie dazu die Setup-Datei von der Homepage herunter und führen Sie die Installation durch.

2. Zentrale Konfigurationsdatei anpassen (-UseConfig)

Wenn Sie eine zentrale Konfigurationsdatei verwenden, bei der die Variante mit dem Parameter -UseConfig in der Desktopverknüpfung verwendet wird, muss diese angepasst werden. Passen Sie in der Verknüpfung die Pfade für Ziel und Ausführen in an – aus dem Installationsverzeichnis ...\Docusnap 14 wird ...\Docusnap.

3. Datenbank-Backup prüfen / durchführen

Bevor Sie das Datenbank-Upgrade durchführen, sollten Sie, falls noch nicht geschehen, ein Datenbank-Backup durchführen.

4. Datenbank-Upgrade durchführen

Wenn Sie Docusnap nach dem Upgrade starten, fordert Sie Docusnap auf, die Datenbank zu aktualisieren. Falls noch eine aktive Verbindung zur Docusnap Datenbank besteht, wird diese angezeigt. Schließen Sie alle Docusnap Client-Anwendungen und führen Sie anschließend das Datenbank-Upgrade durch. Das Upgrade auf dem Docusnap Server ist beendet.

5. Verwendete Skriptdateien austauschen / Freigabepfad anpassen

Wenn Sie Inventarisierungen mit einer der Skriptvarianten durchführen, müssen Sie diese jetzt unbedingt an ihrem Ablageort austauschen. Dieser Austausch sollte nach jedem Update / Upgrade von Docusnap erfolgen.

Wir empfehlen bei der Verwendung einer / der Skriptvarianten grundsätzlich die Installation eines Docusnap Discovery Services (DDS) mindestens auf dem System, auf dem auch der Docusnap Server konfiguriert wurde.

In den Einstellungen des DDS können Sie ein zusätzliches Verzeichnis für die Ablage der Inventarisierungsmodule (Skriptdateien) angeben. Dies bewirkt, dass die Skriptdateien bei einem Update von Docusnap automatisch ausgetauscht werden und somit immer aktuell sind.

Wenn Sie die Variante mit der Bereitstellung über den DDS verwenden, muss nichts angepasst werden!

Installieren und konfigurieren Sie den DDS – HowTo.
Hier finden Sie ein HowTo, was die Einrichtung der skriptbasierten Inventarisierung am Beispiel Windows zeigt.

6. DDS-Installationen aktualisieren

Die Docusnap Plugin Dateien werden bei einem Update / Upgrade von Docusnap automatisch aktualisiert. Nicht jedoch die Komponenten wie NMAP oder der NPCAP Treiber. Aus diesem Grund empfehlen wir eine vollständige Aktualisierung aller Docusnap Discovery Services.

Für die vollständige Aktualisierung muss das DDS-Setup nochmal auf den jeweiligen Systemen ausgeführt werden. Die Verbindungen der DDS werden nach Abschluss der Installation wieder aufgebaut.

Das Setup finden Sie im Installationsverzeichnis von Docusnap 15, im Ordner Setup. Einfach das Setup erneut ausführen. Die vorhandene Installation wird daraufhin aktualisiert. Mit dem Parameter -q kann die Installation im Silent Modus durchgeführt werden.

7. Update der Docusnap Client-Systeme

Nun können Sie das Upgrade auch auf den übrigen Client-Systemen durchführen. Wenn dort Docusnap gestartet wird, erscheint automatisch die Meldung, dass ein Update verfügbar ist. -> Wie beschrieben vorgehen!

Im Zuge eines Updates von Docusnap 14 wurde auch die Installation auf einer Netzwerkfreigabe von Docusnap unterstützt. Bei Clientinstallationen empfiehlt es sich, die Installation zukünftig über das Netzwerk freizugeben. Bei Updates / Upgrades müssen daraufhin keine Client Updates mehr durchgeführt werden.

Die Vorgehensweise wird im Installations- und Konfigurations HowTo – Kapitel 3 beschrieben!

3. Proxmox Inventarisierung

Der Proxmox-Inventarisierungsassistent erwartet die Angabe eines beliebigen Cluster-Nodes oder eines Standalone-Nodes mit einem Benutzer inklusive Realm (z. B. root@pam), der über Leseberechtigungen auf dem Cluster oder Node verfügt.

Wird ein Cluster betrieben, reicht die Angabe eines Nodes aus. Docusnap ermittelt daraus den gesamten Cluster mit allen Nodes.

Die Inventarisierung erfolgt über die Hersteller-API, verwendet HTTPS mit dem Port 8006 und liefert die folgenden Daten:

- Cluster - Knoten, Quorum, Hochverfügbarkeit (HA-Gruppen)
- Nodes - PVE-Version, Hardware, Datenträger, Netzwerk
- VMs & Linux-Container - CPU, RAM, Netzwerk, Snapshots
- Speicher - Storages sowie Ceph mit OSDs & Pools
- Sicherheit - Firewall-Regeln (Cluster / Node / VM)
- Benutzer & Rechte - Authentifizierungsquellen, Gruppen, Rollen, Berechtigungen
- Datensicherung - Backup-Jobs & Replikationen zwischen Nodes

Auf Cluster-, Node-, VM- und Container-Ebene stehen Berichte bereit:

- Cluster – Cluster Übersicht: ganzer Cluster mit seinen Nodes und Gästen
- Nodes – Node Details (ein Node), „Node Gesamtbericht" (alle Nodes)
- Virtuelle Maschinen – VM-Details (eine VM), „VM Gesamtbericht" (alle VMs)
- Linux-Container – Linux-Container Details (ein Container), Linux-Container Gesamtbericht (alle)

Um die Dokumentation zu vervollständigen, sollten die Proxmox-Nodes noch als Linux-Systeme inventarisiert werden!

4. Meraki

Der Meraki-Inventarisierungsassistent erwartet die Angabe eines gültigen Meraki-Cloud-API-Schlüssels mit entsprechenden Leserechten für die Meraki-Organisation.

Die Inventarisierung erfolgt über die Meraki-Cloud-API (api.meraki.com), nutzt HTTPS mit dem Port 443 und liefert die folgenden Daten:

- Meraki-Cloud-API-Schlüssel (lesend) - Zugang zur Organisation
- Geräte - Produkttyp, Modell, Netzwerkzuordnung
- Netzwerke - VLANs, WLAN-SSIDs, Group Policies (inkl. Content-Filtering)
- Sicherheit - Firewall-/Access-Regeln, SNMP, RADIUS, Smartports
- Verwaltung - Administratoren & Rechte, SSO-Rollen, API-IP-Bereiche
- Lizenzierung - Co-Termination, Per-Device, Subscription

Auf Ebene der Meraki-Organisation stehen Berichte bereit:

- Übersicht – Org-Steckbrief: Organisation, Lizenz, Administration, Sicherheit, Netzwerke und Geräte.
- Geräte-Inventar – Alle Geräte nach Produkttyp und Modell: Tags, Serial, MAC, Netzwerk, IP, Status, Firmware.
- Netzwerke – Je Netzwerk die VLANs (Subnetz/Gateway) und die aktiven SSIDs mit Authentifizierung.
- Lizenzierung – Lizenzstatus und -umfang sowie die aktiven Lizenzpositionen mit Ablaufdatum.
- Sicherheit – Login-/Passwortregeln, Administratoren (MFA), RADIUS, Gruppenrichtlinien, Content-Filter.
- Switch-Ports – Port-Profile (Smartports) und die Port-Belegung je Switch.
- Mobilfunk-Gateways – Cellular Gateways mit Status, Carrier, SIM und Tarif.

5. Hyper-V

Die Hyper-V-Inventarisierung wurde in Docusnap 15 neu entwickelt. Der bisherige Inventarisierungsassistent bleibt vorerst als „Hyper-V Legacy" erhalten.

Der Hyper-V-Inventarisierungsassistent erwartet die Angabe der jeweiligen Hyper-V-Hosts (nicht Cluster!) und des jeweiligen Administrators auf dem Hyper-V-Host.

An den sonstigen Voraussetzungen hat sich im Vergleich zur Legacy-Inventarisierung nichts geändert.

Neu ist die rollenbasierte Erkennung von Hyper-V-Hosts auf Basis der Windows-Inventarisierung. Das heißt, wenn Windows-Systeme mit installierter Hyper-V-Rolle inventarisiert wurden, können diese im Assistenten angezeigt werden.

Ebenfalls neu ist die Möglichkeit, eine skriptbasierte Inventarisierung durchzuführen.

Die Inventarisierung liefert die folgenden Daten:

- Neuentwicklung - mehr Detailtiefe zur Hyper-V-Infrastruktur
- Hosts - Einstellungen, OS, Migration, NUMA, Fibre Channel
- VMs - Konfiguration, Ressourcen, virtuelle Switches & Netzwerkadapter
- Failover-Cluster - Knoten, Netzwerke, hochverfügbare VMs
- VM-Sicherheitseinstellungen (Shielded VMs, Verschlüsselung, TPM, Secure Boot)
- Replikationen - Host- & VM-Ebene
- Prüfpunkte / Checkpoints - deckt vergessene/verkettete Checkpoints auf

6. Gruppenrichtlinien (GPO)

In Docusnap 15 werden nun auch die technischen Einstellungen jeder Gruppenrichtlinie erfasst. Dazu gehören

- Status
- Computerkonfiguration aktiv
- Benutzerkonfiguration aktiv
- WMI-Filterpfad
- Erstelldatum
- Änderungsdatum
- Besitzer

Weiterhin werden die Richtlinien nun auch in der Docusnap-Baumstruktur dargestellt. Dadurch können die gesetzen Richtlinien im Detail ausgewertet und in Berichten aufgelistet werden.

Auf Ebene der Active-Directory-Inventarisierung und der Domäne (AD-DS-Sicherheit) finden sich folgende GPO-Berichte:

- Übersicht – alle GPOs – kuratierte Tabelle, eine Zeile je Richtlinie: Herkunft, Status, Reichweite.
- Details – alle GPOs – jede Richtlinie der Domäne vollständig, je Richtlinie eine Seite.
- Übersicht – verknüpfte GPOs – dieselbe Tabelle, beschränkt auf die an der Domäne verknüpften.
- Details – verknüpfte GPOs – dieselbe Volltiefe, beschränkt auf die verknüpften Richtlinien.
- Details – eine einzelne Richtlinie vollständig: Verknüpfungen, Delegation, Einstellungen.
- GPO-Sicherheit – untersucht alle GPOs und zeigt GPOs mit erfasster sicherheitsrelevanter Konfiguration
- Delegationsabweichungen vom Microsoft-Standard; abgelegt unter „AD DS Sicherheit"

7. Linux – Docker Informationen

Der Linux-Scan erfasst in Docusnap 15 zusätzlich Docker-Container-Hosts. Wird ein Linux-System als Docker-Host erkannt, werden die Docker-Engine und die vollständige Container-Landschaft mit inventarisiert. Abgelegt unter dem jeweiligen Linux-System im Zweig Docker sind die folgenden Informationen zu finden:

- Überblick & Engine
  - Docker-, API- und Go-Version, Build-Time und OS/Architektur sowie Kennzahlen: Container gesamt/laufend/pausiert/gestoppt, Images, Compose-Stacks und Netzwerke.
- Container
  - Name, Image, Status und Health-Status, Erstellzeitpunkt, Restart-Policy und Container-ID; je Container zusätzlich Ports, Netzwerke und Labels.
- Images
  - die auf dem Host vorhandenen Container-Images.
- Netzwerke
  - Treiber (bridge, macvlan, host), Scope, Internal-Flag, IPv6 und Netzwerk-ID.
- Volumes
  - Name, Treiber, Mountpoint, Scope, Erstellzeitpunkt und Größe.
- Compose-Stacks
  - Projektname, Arbeitsverzeichnis, Config-Dateien und Health-Status.
- Komponenten
  - Engine, containerd, runc und docker-init mit Version und Git-Commit.

8. Erweiterter Schutz

Der erweiterte Schutz in Docusnap 15 verschlüsselt sensible Daten in Docusnap noch einmal zusätzlich. Dazu gehören:

- Docusnap-Datenbankverbindung
  - Bei SQL-Authentifizierung der Benutzername und das Passwort
- Inventarisierungsinformationen
  - Benutzernamen und Passwörter aller Inventarisierungsassistenten
  - Private Schlüssel für die Linux-Inventarisierung
  - Entra-ID-App-Registrierungsdaten
- Eingabemasken

Der erweiterte Schutz wird im Konfigurationsdialog des Docusnap Server Dienstes aktiviert.

Er basiert auf einer Zertifikatsverschlüsselung und erweitert somit die bisherige Verschlüsselung. Nach der Aktivierung im Konfigurationsdialog des Docusnap Server Dienstes wird ein Zertifikat auf dem System installiert (Lokaler Computer).

Wird Docusnap auch außerhalb des Docusnap Servers benutzt, muss das Zertifikat anschließend exportiert und auf jedem System installiert sein, auf dem Docusnap genutzt wird. Dies gilt auch beim Starten von Docusnap über die Netzwerkfreigabe.

Dabei müssen die Berechtigungen für den Zugriff auf das Zertifikat / Privater Schlüssel berücksichtigt werden. Bei Zertifikaten im Computer Store können nur SYSTEM und Administratoren auf den privaten Schlüssel zugreifen und somit die Daten entschlüsseln und nutzen! Hierfür gibt es zwei Möglichkeiten:

a) Private Key-Berechtigung für einen ausgewählten Benutzerkreis setzen (empfohlen: über AD-Gruppe), jeweils auf den Systemen, auf denen Docusnap genutzt wird.

b) Zuvor exportiertes Zertifikat inkl. privatem Schlüssel gezielt in die Benutzer-Zertifikatsspeicher (Aktueller Benutzer) der jeweiligen Docusnap-Anwender importieren.

Wenn das Zertifikat verloren geht, muss der Schutz zurückgesetzt werden. Dabei gehen alle geschützten Daten verloren und müssen neu angelegt werden. Dies betrifft auch alle eingerichteten, zeitgesteuerten Aufträge.

Ohne Zertifikat ist kein Zugriff auf Docusnap möglich!

Vor der Aktivierung des Schutzes ist ein Datenbank-Backup durchzuführen!

Das Zertifikat ist zu sichern! Geht es verloren, kann Docusnap nicht mehr gestartet werden.

Der erweiterte Schutz lässt sich nur mit Datenverlust deaktivieren!

Customizings, die Eingabemasken ändern oder hinzufügen, können nicht in andere Docusnap-Umgebungen übertragen werden, wenn der erweiterte Schutz aktiviert ist.

9. Neuerungen und Änderungen bei den Discovery Services

Wird mit Docusnap 15 ein Discovery Service (DDS) installiert, werden nicht mehr die zur Inventarisierung benötigten Komponenten mitinstalliert. Diese Komponenten lädt der Docusnap Server erst nach der Registrierung nach.

Das bringt zwei Vorteile:

- Die Größe des Installationspakets sinkt deutlich – von 400 MB auf 75 MB.
- Die Komponenten lassen sich einfacher aktualisieren.

Bei der bisherigen Installation wurde im Installationsverzeichnis der Discovery Services auch NMAP abgelegt, aber nicht aktualisiert. NMAP und die weiteren Inventarisierungs-Plugins liegen jetzt ausschließlich unter C:\ProgramData\Docusnap\Discovery\discovery – und werden dort bei jeder Aktualisierung vollständig erneuert.

Zusätzlich wurde die Kommunikation zwischen DDS und Docusnap Server gehärtet.

Wir empfehlen daher, die Discovery Services manuell zu aktualisieren, damit die Komponenten auf dem neuesten Stand sind und von der verbesserten Sicherheit profitieren.

Das Setup finden Sie im Installationsverzeichnis von Docusnap 15 im Ordner Setup. Führen Sie es einfach erneut aus – die vorhandene Installation wird dabei aktualisiert. Mit dem Parameter -q lässt sich die Installation im Silent-Modus durchführen.

10. Entfernung von Legacy-Assistenten

Mit Docusnap 15 entfallen die veralteten Module:

- DFS – Legacy
- Office 365 – Legacy

Wenn Sie diese Inventarisierungen noch zeitgesteuert durchführen, sollten Sie diese Aufträge löschen und auch die dazugehörigen Daten in der Baumstruktur.

Im Nachgang sollten die aktuellen Inventarisierungen eingeplant werden: M365 und DFS.

ABBILDUNGSVERZEICHNIS

VERSIONSHISTORIE

Datum	Beschreibung
10.08.2026	Erstellung des HowTos
07.09.2026	Anpassung des erweiterten Schutzes – Hinweis auf die Eingabemasken hinzugefügt