IT-Network DocuScanner

Installations- och användarhandbok

Version 2.08.14

Sat-iTec Systemhaus GmbH
https://www.sat-itec.se

1. Översikt

IT-Network DocuScanner är ett verktyg för automatiserad inventering och dokumentation av IT-infrastruktur. Det fångar värdar, installerad programvara, licensnycklar, Active Directory-objekt, nätverksdelningar och IT-säkerhetsegenskaper (BSI Grundschutz) och presenterar dem i ett webbgränssnitt.

Huvudfunktioner

- Nätverksskanning via Ping/ARP, värdnamnsuppslagning och MAC-insamling
- Programvaruinventering via CIM/WMI med DCOM-fallback
- Licensgranskning (Windows-produktnycklar, Office, WMI SoftwareLicensingProduct)
- Active Directory-fråga via inbyggd Go-LDAP/LDAPS
- SMB-delningar med ACL (CIM + net-view-fallback) och NFS-detektering
- BSI Grundschutz-heuristik baserad på skanningsdata
- REST-API för externa verktyg, automatisk uppdateringskontroll via GitHub-releaser

Arkitektur

Skannern består av två komponenter:

Komponent	Uppgift	Plattform
itscanner-server	Webbgränssnitt, REST-API, SQLite-databas, AD-LDAP-klient	Windows + Linux
Invoke-Scan.ps1	Nätverk/programvara/licens/delningar/NFS-skanning via CIM-WMI	Endast Windows

Notera: Skanningsworkern (Invoke-Scan.ps1) är Windows-specifik. Under Linux levererar servern webbgränssnittet och AD-frågan; själva skanningen måste utgå från en Windows-nod.

2. Systemkrav

Server (webbgränssnitt / API)

Plattform	Minimikrav
Windows	Windows 10 / Windows Server 2016 eller senare, 64-bit
Linux	Distribution med systemd (Debian 11+, Ubuntu 20.04+, RHEL 8+, openSUSE Leap 15+), 64-bit
RAM	Minst 512 MB, rekommenderat 2 GB för stora nät
Disk	200 MB program + tillväxt av SQLite-databas (typiskt 50–500 MB)
Nätverk	TCP/8585 nåbar för webbgränssnittet

Skanningsnod (Windows-worker)

- Windows 10 / Server 2016 eller senare med PowerShell 5.1
- Domänmedlemskap rekommenderas; Domain Admin eller motsvarande rättigheter för AD-frågor
- ActiveDirectory PowerShell-modul (RSAT) valfritt — ADSI/LDAP-fallback inbyggd
- Services for NFS (Windows-funktion) valfritt, möjliggör NFS-monteringslista via showmount.exe

Nätverkskrav för målvärdar

Port	Protokoll	Syfte
135 / TCP	DCOM/RPC	Programvaruinventering (fallback)
445 / TCP	SMB	Delningar, net-view
5985 / TCP	WinRM	CIM-sessioner (rekommenderas)
389 / TCP	LDAP	Active Directory-fråga
636 / TCP	LDAPS	AD krypterat (rekommenderas)
2049 / TCP	NFS	Linux-NFS-detektering

3. Installation under Windows

Windows-installeraren är ett NSIS-setup som registrerar servern som en Windows-tjänst. Tjänsten startar automatiskt vid systemstart.

3.1 Steg för steg

1. Ladda ner ITScanner-Server-Setup-2.08.14.exe som administratör
2. Hämtning från GitHub releases-sidan eller via auto-update-funktionen
3. Kör installeraren som administratör (högerklick → ”Kör som administratör”)
4. Bekräfta installationssökväg (standard: C:\Program Files\ITScanner-Server)
5. Slutför installationen — tjänsten ”IT-Network DocuScanner Server” startar automatiskt
6. Öppna webbläsare: http://localhost:8585

3.2 Tjänstehantering

```
# Kontrollera status
sc query "IT-Network DocuScanner Server"

# Stoppa / starta tjänsten
net stop "IT-Network DocuScanner Server"
net start "IT-Network DocuScanner Server"

# Ta bort tjänsten (ren ominstallation)
itscanner-server.exe --uninstall
```

3.3 Kataloger

Sökväg	Innehåll
C:\Program Files\ITScanner-Server\	Program + skript
C:\ProgramData\ITScanner-Server\	Databas, konfiguration, loggar
C:\ProgramData\ITScanner-Server\itscanner.db	SQLite-huvuddatabas
C:\ProgramData\ITScanner-Server\scripts\	Invoke-Scan.ps1, ad_settings.json

4. Installation under Linux

Servern körs på alla Linux-distributioner med systemd. Två installationspaket finns: en universell tar.gz med installationsskript och ett nativt .deb för Debian/Ubuntu.

4.1 Debian / Ubuntu (.deb)

```
sudo dpkg -i itscanner-server_2.08.14_amd64.deb
sudo systemctl status itscanner-server

# Om beroenden saknas:
sudo apt-get install -f
```

Postinst-hooken skapar automatiskt systemanvändaren itscanner, lägger upp /var/lib/itscanner-server, registrerar systemd-enheten och startar tjänsten.

4.2 Universell (tar.gz)

```
tar -xzf itscanner-server-linux-2.08.14.tar.gz
cd itscanner-server-linux-2.08.14
sudo ./install.sh
```

4.3 Kataloger under Linux

Sökväg	Innehåll
/opt/itscanner-server/	Programbinärer
/var/lib/itscanner-server/	SQLite-DB, konfiguration
/var/log/itscanner-server/	Ytterligare loggar (annars journalctl)
/etc/systemd/system/itscanner-server.service	systemd-enhet

4.4 Tjänstehantering

```
sudo systemctl status itscanner-server
sudo systemctl restart itscanner-server
sudo systemctl stop itscanner-server
sudo journalctl -u itscanner-server -f   # live-logg
```

Viktigt: Under Linux är PowerShell-skanningsworkern inte aktiv. Funktionellt: webbgränssnitt med alla flikar, REST-API, AD-livefråga via LDAP, subnätshärledning, BSI-heuristik, datavisning från tidigare skanningar. För aktiva skanningar krävs en Windows-nod.

5. Förstagångskonfiguration

Efter installationen bör följande inställningar göras så att skannern kan visa sin fulla potential.

5.1 Anslut Active Directory

7. Gå till Inställningar → AD / LDAP i webbgränssnittet
8. Ange Domain Controller-FQDN, t.ex. dc01.foretag.local
9. Domännamn (DNS-form), t.ex. foretag.local
10. Servicekonto: helst ett dedikerat konto med read-only-rättigheter på hela katalogen
11. Ange lösenord — lagras krypterat i databasen
12. Trigga anslutningstestet — ska ge en träffräknare

5.2 Skanningsuppgifter för CIM/WMI

För programvaruinventering och delningsinsamling på fjärrvärdar krävs autentiseringsuppgifter med lokala eller Domain Admin-rättigheter.

13. Inställningar → Skanningsuppgifter
14. Ange Domän\\Administratör (eller motsvarande) som användarnamn
15. Lösenord: används enbart för skanningsanrop

Tips: Aktivera WinRM på målvärdar (Enable-PSRemoting) för betydligt snabbare och stabilare skanningar. Utan WinRM försöker skannern DCOM som fallback (långsammare, mindre tillförlitligt).

5.3 Uppdateringsserver

Som standard kontrollerar servern github.com/satitec/itscanner för nya releaser. För att använda en intern spegel:

```
# Annan repo
curl -X PUT -H "Content-Type: application/json" \
  -d '{"github_repo":"foretag/itscanner-internal"}' \
  http://server:8585/api/settings/updates
```

6. Använda webbgränssnittet

Webbgränssnittet nås på http://server:8585 och är uppdelat i följande flikar:

6.1 Översikt

Översiktskakel med de viktigaste nyckeltalen: antal värdar, programvarupos, AD-objekt, BSI-status. Aktuell serverversion och watchdog-status visas uppe till höger.

6.2 Värdar

Lista över alla enheter som upptäckts i nätet med hostname, IP, MAC, OS, domän och typ (Server, Workstation, Switch, Firewall, NAS, Printer, Other). Filterrullgardiner för typ och status. Klick på en värd öppnar detaljvyn med programvarulista, licensnycklar, öppna portar och serverroller.

6.3 Programvara

Programvaruinventering grupperad efter produktnamn. Per post visas på hur många och vilka värdar programvaran är installerad. Sök, filtrera, exportera.

6.4 Delningar

SMB-nätverksdelningar grupperade efter värd. Per delning visas namn, sökväg, beskrivning och ACL. Om CIM-åtkomst inte var möjlig används net-view-fallback (utan ACL-detaljer). Ovanför tabellen visas en diagnosrad med värdena DB / API / Värdar. Vid tom flik syns direkt om data finns i databasen eller om skanningen ännu inte gått. Linux-värdar med NFS-server (port 2049) visas som NFS-server-post med tillgängliga monteringspunkter, förutsatt att showmount.exe finns.

6.5 Licenser

Översikt över alla insamlade licensnycklar med källa (Registry, WMI), status (activated, grace, unlicensed) och aktiveringskanal (Volume, OEM, Retail, KMS).

6.6 Active Directory

Tabell med alla AD-objekt (användare, grupper, datorer, OU:er, GPO:er). Filterrullgardin uppe till höger för att begränsa till objekttyp. Fritextsökning över namn, sAMAccountName och Distinguished Name. Ovanför tabellen: knappar ”Ladda från AD” (utlöser en LDAP-livefråga) och ”Uppdatera” samt en diagnosrad DB / API / Visade med aktivt filter.

6.7 Subnät

Identifierade subnät med gateway, VLAN-ID och antal värdar. Om inga subnät registrerats av en skanning härleder servern dem automatiskt från värdarnas IP-adresser (gruppering efter /24).

6.8 Serverroller

Översikt över alla installerade Windows-serverroller och valfria funktioner per värd. På server-OS läses rollerna via Win32_ServerFeature (t.ex. Active Directory Domain Services, DNS Server, DHCP Server, File Server, Web Server IIS, Hyper-V). På arbetsstationer visar tabellen Win32_OptionalFeatures som Hyper-V Client, Telnet Client, Internet Information Services Express. Tabellen har fem kolumner: värd, OS, roll/funktion (intern beteckning), visningsnamn och status. Sökfiltret söker i hostname, roll och visningsnamn i realtid; värdfilter-rullgardinen uppe till höger begränsar visningen till en enskild server. Förutsättning:

CIM-åtkomst till målvärden (WinRM port 5985 eller DCOM port 135) plus admin-rättigheter för WMI-klasserna Win32_ServerFeature och Win32_OptionalFeature. Värdar utan CIM-åtkomst visas inte i denna tabell.

6.9 BSI-kontroller

IT-Grundschutz-konforma heuristiker baserade på skanningsdata. Fliken visar antalet godkända, varnande och kritiska kontroller överst i tre kort. Tabellen nedanför listar varje kontroll med kategori, status, fynd och rekommendation.

Exempel på heuristiker:

- End-of-life-operativsystem (Windows XP/7/8, Server 2003/2008/2012) → kritiskt
- Mer än två värdar med öppen RDP (port 3389) → kritiskt
- Telnet (port 23) på någon värd → kritiskt
- Domain Controller-redundans (≥ 2 DC:er) → ok
- Backupprogramvara upptäckt (Veeam, Acronis, Commvault, Nakivo, Macrium) → ok
- Inaktiverade AD-konton → varning

6.10 Rapporter

Förgenererade rapporter att hämta som PDF eller DOCX, bland annat: server-/klientöversikt, hårdvaruinventering, programvarukonformitet, licensgranskning, BSI Grundschutz-rapport, nätverkstopologi.

6.11 Skanningshantering

Hantering av skanningsjobb med namn, typ, målsubnät och schemaläggning. Knappar för att skapa, redigera, trigga och radera. Standardjobb är ”Fullständig nätverksskanning” (veckovis), ”Daglig nätverksstatus”, ”Programvaruinventering” och ”AD-granskning”.

6.12 Skanningshistorik

Kronologisk lista över alla skanningar med start- och sluttid, varaktighet, antal hittade värdar och status. Klick på en post öppnar detaljloggen för den körningen.

6.13 Logg

Live-loggvy med alla server- och skanningsevent. Auto-refresh-växel uppe till höger. Filter-rullgardin för loggnivå (info / warning / error).

Tips: Vid problem är Logg-fliken den viktigaste diagnoskällan. Sök efter ”Share-Scan”, ”AD-Frueh-Import” eller ”NFS-/Linux-Scan” för att följa respektive delfaser.

6.14 Inställningar

Undermeny med AD/LDAP-anslutning, skanningsuppgifter, uppdateringsserver, rapportförval och licensaktivering.

7. Köra en skanning

7.1 Skanningstyper

Typ	Aktivitet
full	Nätverk + programvara + licens + AD + delningar + NFS
network	Endast Ping/ARP/hostname-uppslagning
software	CIM/WMI + licens på befintliga värdar
ad	Endast AD-livefråga via LDAP
shares	Endast SMB- och NFS-delningsinsamling

7.2 Rekommenderat flöde vid första driftsättning

16. Gör inställningar (AD-anslutning, skanningsuppgifter)
17. Skanningshantering → ”Fullständig nätverksskanning” → kontrollera mål → trigga
18. Följ förloppet i Logg-fliken — AD-tidigimporten rapporterar efter 10–30 sekunder med ”AD-Frueh-Import: X av Y objekt i DB”
19. Medan programvaru-/delningsskanningen körs (kan ta flera minuter) öppna redan AD-fliken — datan är redan synlig där
20. När klart: kontrollera skanningshistoriken, generera rapporter

7.3 Förväntad loggsekvens

```
Skanning 'Default' startad: typ=full
N kända värdar från DB skickade till skanning
AD-skanning klar: 66 objekt (ou=2, user=7, ...)
AD-Frueh-Import: 66 av 66 objekt i DB
Kända värdar laddade från DB: 36 totalt, 2 nya
Programvaruinventering v2.08: CIM+StdRegProv...
Share-Scan: 36 värdar kontrollerade, 4 nådda, 32 utan CIM
NFS-/Linux-Scan: 36 värdar kontrollerade, NFS=N, SMB-markör=M
Delningar totalt: 7 SMB + N NFS/markör = X
Delningsimport: X av X i DB
Skanning 'Default' lyckad: 36 värdar, 374 programvara, ...
```

8. Uppdateringsmekanism

På begäran kontrollerar servern GitHub releases-endpunkten för satitec/itscanner och upptäcker automatiskt en nyare version. Rätt nedladdningslänk levereras per plattform (.exe för Windows, .deb för Debian/Ubuntu, .tar.gz universellt).

8.1 Manuell kontroll

21. Inställningar → Uppdateringar
22. Klicka på ”Sök efter uppdateringar nu”
23. Vid tillgänglig uppdatering: nedladdningslänk visas
24. Ladda ner filen, kör installeraren — databas och konfiguration bevaras

8.2 Automatikbeteende

Som standard frågar servern inte efter uppdateringar regelbundet. En schemalagd kontroll kan konfigureras via Skanningshantering som jobb, eller via cron / Aktivitetsschemaläggaren mot endpunkten /api/update/check.

8.3 Versionsjämförelse (Semver)

Servern jämför versionssträngar enligt Semver-regler: 2.08.10 mot 2.04.00 ger 1 (a > b), v-prefixet ignoreras, suffix som -rc1 trimmas bort.

9. Felsökning

9.1 AD-fliken förblir tom trots lyckad skanning

Möjliga orsaker:

- Webbläsarcache håller gammal respons → Ctrl+F5 tvingar omladdning
- Kontrollera diagnosrad: ”DB: 66 | API: 0” → webbläsarcache, ”DB: 0 | API: 0” → skanningen var resultatlös
- Sök i loggen efter ”AD-Frueh-Import” eller ”AD-Partial-fil kunde inte skrivas”

9.2 Delningsfliken tom

- Diagnosrad: ”API: 0 delningar | N värdar” → skanning gav inget
- Sök i loggen efter ”Share-Scan: X nådda, Y utan CIM” — om alla utan CIM saknas behörigheter
- Lösning: Aktivera WinRM på målvärdar (Enable-PSRemoting på målet)
- Alternativt: kontrollera skanningsuppgifter — kontot måste ha admin-rättigheter på målvärden

9.3 ”Ingen CIM-åtkomst” för många värdar

- Vanligt vid workgroup-värdar eller värdar i främmande domäner
- Aktivera brandväggsregeln ”Windows Management Instrumentation (WMI-In)” på målvärdarna
- På Linux-servrar visas ”Ingen CIM” → SMB-probe-fallback på port 445 markerar dem som ”SMB-server”
- På NFS-servrar: TCP-port 2049 sondas — om öppen visas en NFS-serverpost

9.4 Telnet-varning i BSI-fliken trots att ingen Telnet är känd

Vissa inbyggda enheter (skrivare, äldre switchar) har port 23 öppen. Kontrollera ports-tabellen i databasen, stäng porten på enheten eller dokumentera undantaget.

9.5 Tjänsten startar inte (Linux)

```
sudo journalctl -u itscanner-server -n 50 --no-pager
```

Vanliga orsaker: port 8585 upptagen (stoppa annan tjänst eller justera --port-flagga i systemd-enheten), felaktiga filrättigheter (chown -R itscanner:itscanner /var/lib/itscanner-server).

9.6 Tjänsten startar inte (Windows)

```
# Öppna Loggboken
eventvwr.msc

# Filtrera applikationsloggen på ”IT-Network DocuScanner”
# Vanligt: databassökväg ej skrivbar
# eller port 8585 upptagen
```

10. Appendix

10.1 REST-API-endpunkter

Endpunkt	Metod	Syfte
/api/health	GET	Status + version
/api/dashboard	GET	Översiktsmetrik
/api/hosts	GET	Värdlista
/api/software	GET	Programvarulista
/api/shares	GET	Delningslista
/api/licenses	GET	Licensnycklar
/api/ad	GET	AD-objekt (filter: ?type, ?search)
/api/ad/stats	GET	AD-räknare
/api/ad/query	POST	Trigga LDAP-livefråga
/api/subnets	GET	Subnät (med auto-derive)
/api/server-roles	GET	Serverroller (filter: ?host, ?status)
/api/bsi	GET	BSI-kontroller (med auto-derive)
/api/scans	GET	Skanningshistorik
/api/jobs	GET/POST	Skanningsjobb
/api/jobs/{id}/trigger	POST	Starta skanning
/api/update/check	GET/POST	Uppdateringskontroll (GitHub)
/api/logs	GET	Loggposter

10.2 Versionsschema

Sat-iTec använder ett tredelat versionsschema X.YY.ZZ:

- X = Major (sällan, större arkitekturändringar)
- YY = Minor (nya funktioner, Y skrivs tvåsiffrigt)
- ZZ = Patch (felrättningar, Z skrivs tvåsiffrigt)

Exempel: 2.08.14 = Major 2, Minor 8, Patch 14. En ny funktion ökar YY (t.ex. 2.09.00), en felrättning ökar ZZ (t.ex. 2.08.15).

10.3 Supportkontakt

Sat-iTec Systemhaus GmbH

E-post: support@sat-itec.se

Webb: https://www.sat-itec.se

GitHub-releaser: https://github.com/satitec/itscanner/releases