IT-Network DocuScanner

Guide d’installation et d’utilisation

Version 2.08.14

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

1. Aperçu

L’IT-Network DocuScanner est un outil d’inventaire et de documentation automatisés des infrastructures IT. Il collecte les hôtes, les logiciels installés, les clés de licence, les objets Active Directory, les partages réseau et les caractéristiques de sécurité IT (BSI Grundschutz) et les présente dans une interface web.

Fonctions principales

- Scan réseau via Ping/ARP, résolution de nom d’hôte et capture MAC
- Inventaire logiciel via CIM/WMI avec repli DCOM
- Audit de licences (clés de produit Windows, Office, WMI SoftwareLicensingProduct)
- Interrogation Active Directory via Go-LDAP/LDAPS natif
- Partages SMB avec ACL (CIM + repli net-view) et détection NFS
- Heuristiques BSI Grundschutz issues des données de scan
- API REST pour outils externes, vérification automatique des mises à jour via les releases GitHub

Architecture

Le scanner se compose de deux composants :

Composant	Rôle	Plateforme
itscanner-server	Interface web, API REST, base SQLite, client AD-LDAP	Windows + Linux
Invoke-Scan.ps1	Scan réseau / logiciel / licence / partages / NFS via CIM-WMI	Windows uniquement

Note : le worker de scan (Invoke-Scan.ps1) est spécifique à Windows. Sous Linux, le serveur fournit l’interface web et l’interrogation AD ; le scan proprement dit doit partir d’un nœud Windows.

2. Prérequis système

Serveur (interface web / API)

Plateforme	Exigence minimale
Windows	Windows 10 / Windows Server 2016 ou plus récent, 64 bits
Linux	Distribution avec systemd (Debian 11+, Ubuntu 20.04+, RHEL 8+, openSUSE Leap 15+), 64 bits
RAM	512 Mo minimum, 2 Go recommandés pour les grands réseaux
Disque	200 Mo programme + croissance de la base SQLite (typiquement 50–500 Mo)
Réseau	TCP/8585 accessible pour l’interface web

Nœud de scan (worker Windows)

- Windows 10 / Server 2016 ou plus récent avec PowerShell 5.1
- Appartenance à un domaine recommandée ; droits Domain Admin ou équivalents pour les requêtes AD
- Module ActiveDirectory PowerShell (RSAT) optionnel — repli ADSI/LDAP intégré
- Services for NFS (fonctionnalité Windows) optionnel, permet la liste des montages NFS via showmount.exe

Exigences réseau pour les hôtes cibles

Port	Protocole	Rôle
135 / TCP	DCOM/RPC	Repli inventaire logiciel
445 / TCP	SMB	Partages, net-view
5985 / TCP	WinRM	Sessions CIM (recommandé)
389 / TCP	LDAP	Interrogation Active Directory
636 / TCP	LDAPS	AD chiffré (recommandé)
2049 / TCP	NFS	Détection NFS Linux

3. Installation sous Windows

L’installeur Windows est un setup NSIS qui enregistre le serveur en tant que service Windows. Le service démarre automatiquement au boot.

3.1 Pas à pas

1. Télécharger ITScanner-Server-Setup-2.08.14.exe en tant qu’administrateur
2. Téléchargement depuis la page GitHub Releases ou via la fonction d’auto-update
3. Exécuter l’installeur en tant qu’administrateur (clic droit → « Exécuter en tant qu’administrateur »)
4. Confirmer le chemin d’installation (par défaut : C:\Program Files\ITScanner-Server)
5. Terminer l’installation — le service « IT-Network DocuScanner Server » démarre automatiquement
6. Ouvrir le navigateur : http://localhost:8585

3.2 Gestion du service

```
# Vérifier le statut
sc query "IT-Network DocuScanner Server"

# Arrêter / démarrer le service
net stop "IT-Network DocuScanner Server"
net start "IT-Network DocuScanner Server"

# Supprimer le service (réinstallation propre)
itscanner-server.exe --uninstall
```

3.3 Répertoires

Chemin	Contenu
C:\Program Files\ITScanner-Server\	Programme + scripts
C:\ProgramData\ITScanner-Server\	Base, configuration, logs
C:\ProgramData\ITScanner-Server\itscanner.db	Base SQLite principale
C:\ProgramData\ITScanner-Server\scripts\	Invoke-Scan.ps1, ad_settings.json

4. Installation sous Linux

Le serveur fonctionne sur toute distribution Linux avec systemd. Deux paquets sont disponibles : un tar.gz universel avec script d'installation, et un .deb natif pour Debian/Ubuntu.

4.1 Debian / Ubuntu (.deb)

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

# Si des dépendances manquent :
sudo apt-get install -f
```

Le hook postinst crée automatiquement l'utilisateur système itscanner, prépare /var/lib/itscanner-server, enregistre l'unité systemd et démarre le service.

4.2 Universel (tar.gz)

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

4.3 Répertoires sous Linux

Chemin	Contenu
/opt/itscanner-server/	Binaires du programme
/var/lib/itscanner-server/	Base SQLite, configuration
/var/log/itscanner-server/	Logs supplémentaires (sinon journalctl)
/etc/systemd/system/itscanner-server.service	Unité systemd

4.4 Gestion du service

```
sudo systemctl status itscanner-server
sudo systemctl restart itscanner-server
sudo systemctl stop itscanner-server
sudo journalctl -u itscanner-server -f   # log en direct
```

Important : sous Linux, le worker de scan PowerShell n'est pas actif. Sont fonctionnels : interface web complète, API REST, requête AD en direct via LDAP, dérivation des sous-réseaux, heuristiques BSI, affichage des données issues de scans antérieurs. Un nœud Windows est nécessaire pour les scans actifs.

5. Configuration initiale

Après l'installation, les réglages suivants doivent être effectués pour que le scanner exploite tout son potentiel.

5.1 Connecter Active Directory

7. Aller dans Paramètres → AD / LDAP dans l'interface web
8. Saisir le FQDN du contrôleur de domaine, par ex. dc01.entreprise.local
9. Nom de domaine (forme DNS), par ex. entreprise.local
10. Compte de service : de préférence un compte dédié avec droits read-only sur l'ensemble de l'annuaire
11. Saisir le mot de passe — il est stocké chiffré dans la base
12. Lancer le test de connexion — il doit retourner un compteur de résultats

5.2 Identifiants de scan pour CIM/WMI

Pour l'inventaire logiciel et la collecte de partages sur les hôtes distants, des identifiants avec des droits d'administrateur local ou de domaine sont nécessaires.

13. Paramètres → Identifiants de scan
14. Saisir Domaine\\Administrateur (ou équivalent) comme nom d'utilisateur
15. Mot de passe : utilisé exclusivement pour les appels de scan

Astuce : activer WinRM sur les hôtes cibles (Enable-PSRemoting) pour des scans bien plus rapides et stables. Sans WinRM, le scanner tente DCOM en repli (plus lent, moins fiable).

5.3 Serveur de mise à jour

Par défaut, le serveur consulte github.com/satitec/itscanner pour de nouvelles releases. Pour utiliser un miroir interne :

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

6. Utilisation de l’interface web

L’interface web est accessible sur http://server:8585 et est divisée en onglets suivants :

6.1 Tableau de bord

Tuiles de synthèse avec les indicateurs clés : nombre d’hôtes, entrées logiciel, objets AD, statut BSI. La version courante du serveur et l’état du watchdog sont visibles en haut à droite.

6.2 Hôtes

Liste de tous les équipements détectés sur le réseau avec hostname, IP, MAC, OS, domaine et type (Server, Workstation, Switch, Firewall, NAS, Printer, Other). Filtres déroulants pour le type et le statut. Cliquer sur un hôte ouvre la vue détaillée avec liste des logiciels, clés de licence, ports ouverts et rôles serveur.

6.3 Logiciels

Inventaire logiciel groupé par nom de produit. Pour chaque entrée, on voit sur combien et quels hôtes le logiciel est installé. Recherche, filtre, export.

6.4 Partages

Partages réseau SMB groupés par hôte. Pour chaque partage, le nom, le chemin, la description et l’ACL sont affichés. Si l’accès CIM n’a pas été possible, le repli net-view est utilisé (sans détails ACL). Au-dessus du tableau, une ligne de diagnostic affiche les valeurs DB / API / Hôtes. Ainsi, lorsque l’onglet est vide, on voit immédiatement si des données sont en base ou si le scan n’a pas encore tourné. Les hôtes Linux avec un serveur NFS (port 2049) apparaissent comme entrée serveur NFS avec les montages disponibles, à condition que showmount.exe soit présent.

6.5 Licences

Vue d’ensemble de toutes les clés de licence collectées avec source (Registry, WMI), statut (activated, grace, unlicensed) et canal d’activation (Volume, OEM, Retail, KMS).

6.6 Active Directory

Tableau de tous les objets AD (utilisateurs, groupes, ordinateurs, OU, GPO). Filtre déroulant en haut à droite pour limiter à un type d’objet. Recherche plein-texte sur nom, sAMAccountName et Distinguished Name. Au-dessus du tableau : bouton « Charger depuis l’AD » (déclenche une requête LDAP en direct), « Actualiser » et une ligne de diagnostic DB / API / Affichés avec filtre actif.

6.7 Sous-réseaux

Sous-réseaux détectés avec gateway, ID VLAN et nombre d’hôtes. Si aucun sous-réseau n’a été enregistré par un scan, le serveur les dérive automatiquement à partir des adresses IP des hôtes (groupement par /24).

6.8 Rôles serveur

Aperçu de tous les rôles serveur Windows installés et fonctionnalités optionnelles par hôte. Sur les systèmes serveur, les rôles sont lus via Win32_ServerFeature (par ex. Active Directory Domain Services, DNS Server, DHCP Server, File Server, Web Server IIS, Hyper-V). Sur les postes de travail, le tableau affiche Win32_OptionalFeatures comme Hyper-V

Client, Telnet Client, Internet Information Services Express. Le tableau présente cinq colonnes : hôte, OS, rôle / fonctionnalité (identifiant interne), nom d'affichage et statut. Le filtre de recherche cherche en temps réel dans hostname, rôle et nom d'affichage ; le filtre déroulant des hôtes en haut à droite restreint l'affichage à un seul serveur. Prérequis : accès CIM à l'hôte cible (WinRM port 5985 ou DCOM port 135), plus droits admin pour les classes WMI Win32_ServerFeature et Win32_OptionalFeature. Les hôtes sans accès CIM n'apparaissent pas dans ce tableau.

6.9 Contrôles BSI

Heuristiques conformes à l'IT-Grundschutz basées sur les données de scan. L'onglet affiche en haut le nombre de contrôles passés, en avertissement et critiques dans trois cartes. Le tableau ci-dessous liste chaque contrôle avec catégorie, statut, constat et recommandation.

Exemples d'heuristiques :

- OS en fin de vie (Windows XP/7/8, Server 2003/2008/2012) → critique
- Plus de deux hôtes avec RDP ouvert (port 3389) → critique
- Telnet (port 23) sur un hôte quelconque → critique
- Redondance des contrôleurs de domaine (≥ 2 DC) → ok
- Logiciel de sauvegarde détecté (Veeam, Acronis, Commvault, Nakivo, Macrium) → ok
- Comptes AD désactivés → avertissement

6.10 Rapports

Rapports prêts à télécharger en PDF ou DOCX, notamment : aperçu serveurs/clients, inventaire matériel, conformité logicielle, audit de licences, rapport BSI Grundschutz, topologie réseau.

6.11 Gestion des scans

Gestion des jobs de scan avec nom, type, sous-réseaux cibles et planification. Boutons pour créer, éditer, déclencher et supprimer. Les jobs par défaut sont « Scan réseau complet » (hebdomadaire), « Statut réseau quotidien », « Inventaire logiciel » et « Audit AD ».

6.12 Historique des scans

Liste chronologique de tous les scans avec début, fin, durée, nombre d'hôtes trouvés et statut. Cliquer sur une entrée ouvre le log détaillé du scan.

6.13 Log

Vue de log en direct avec tous les événements serveur et scan. Bascule auto-refresh en haut à droite. Filtre déroulant pour le niveau de log (info / warning / error).

Astuce : pour le diagnostic, l'onglet Log est la source la plus importante. Recherchez « Share-Scan », « AD-Frueh-Import » ou « NFS-/Linux-Scan » pour suivre les sous-phases respectives.

6.14 Paramètres

Sous-menu avec connexion AD/LDAP, identifiants de scan, serveur de mise à jour, préférences de rapports et activation de licence.

7. Lancer un scan

7.1 Types de scan

Type	Activité
full	Réseau + logiciel + licence + AD + partages + NFS
network	Ping/ARP/résolution de hostname uniquement
software	CIM/WMI + licence sur les hôtes existants
ad	Requête AD en direct via LDAP uniquement
shares	Capture de partages SMB et NFS uniquement

7.2 Flux recommandé pour la mise en service initiale

16. Effectuer les réglages (connexion AD, identifiants de scan)
17. Gestion des scans → « Scan réseau complet » → vérifier les cibles → déclencher
18. Suivre la progression dans l'onglet Log — l'import AD anticipé apparaît après 10–30 secondes avec « AD-Frueh-Import : X de Y objets en base »
19. Pendant que le scan logiciel/partages tourne (plusieurs minutes), ouvrir déjà l'onglet AD — les données y sont déjà visibles
20. À la fin : vérifier l'historique des scans, générer les rapports

7.3 Séquence de log attendue

```
Scan 'Default' démarré : type=full
N hôtes connus de la base passés au scan
Scan AD terminé : 66 objets (ou=2, user=7, ...)
AD-Frueh-Import : 66 sur 66 objets en base
Hôtes connus chargés depuis la base : 36 total, 2 nouveaux
Inventaire logiciel v2.08 : CIM+StdRegProv...
Share-Scan : 36 hôtes vérifiés, 4 atteints, 32 sans CIM
NFS-/Linux-Scan : 36 hôtes vérifiés, NFS=N, marqueur SMB=M
Partages totaux : 7 SMB + N NFS/marqueur = X
Import partages : X sur X en base
Scan 'Default' réussi : 36 hôtes, 374 logiciels, ...
```

8. Mécanisme de mise à jour

En option, le serveur interroge l’endpoint des releases GitHub de satitec/itscanner et détecte automatiquement une nouvelle version. Le bon lien de téléchargement est fourni selon la plateforme (.exe pour Windows, .deb pour Debian/Ubuntu, .tar.gz universel).

8.1 Vérification manuelle

21. Paramètres → Mises à jour
22. Cliquer sur « Vérifier les mises à jour maintenant »
23. Si une mise à jour est disponible : le lien de téléchargement s’affiche
24. Télécharger le fichier, exécuter l’installeur — la base et la configuration sont préservées

8.2 Comportement automatique

Par défaut, le serveur n’interroge pas régulièrement les mises à jour. Une vérification planifiée peut être configurée via Gestion des scans en tant que tâche, ou via cron / Planificateur de tâches contre l’endpoint /api/update/check.

8.3 Comparaison de versions (Semver)

Le serveur compare les chaînes de version selon les règles Semver : 2.08.10 vs. 2.04.00 retourne 1 (a > b), le préfixe v est ignoré, les suffixes tels que -rc1 sont supprimés.

9. Dépannage

9.1 L’onglet AD reste vide malgré un scan réussi

Causes possibles :

- Le cache du navigateur conserve une vieille réponse → Ctrl+F5 force le rechargement
- Vérifier la ligne de diagnostic : « DB : 66 | API : 0 » → cache navigateur, « DB : 0 | API : 0 » → scan infructueux
- Chercher dans le log « AD-Frueh-Import » ou « AD-Partial : fichier impossible à écrire »

9.2 Onglet Partages vide

- Ligne de diagnostic : « API : 0 partages | N hôtes » → scan sans résultat
- Chercher dans le log « Share-Scan : X atteints, Y sans CIM » — si tous sans CIM, droits manquants
- Solution : activer WinRM sur les hôtes cibles (Enable-PSRemoting sur la cible)
- Sinon : vérifier les identifiants de scan — le compte doit avoir les droits admin sur l’hôte cible

9.3 « Pas d’accès CIM » sur de nombreux hôtes

- Fréquent avec les hôtes en workgroup ou dans des domaines tiers
- Activer la règle de pare-feu « Windows Management Instrumentation (WMI-In) » sur les hôtes cibles
- Sur les serveurs Linux, « Pas de CIM » apparaît → repli SMB-probe sur le port 445 les marque comme « SMB server »
- Sur les serveurs NFS : le port TCP 2049 est sondé — s’il est ouvert, une entrée serveur NFS apparaît

9.4 Avertissement Telnet dans l’onglet BSI alors qu’aucun Telnet n’est connu

Certains équipements embarqués (imprimantes, switches anciens) ont le port 23 ouvert. Vérifier la table ports de la base, fermer le port sur l’équipement ou documenter l’exception.

9.5 Le service ne démarre pas (Linux)

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

Causes fréquentes : port 8585 occupé (arrêter l’autre service ou ajuster --port dans l’unité systemd), permissions de fichier incorrectes (chown -R itscanner:itscanner /var/lib/itscanner-server).

9.6 Le service ne démarre pas (Windows)

```
# Ouvrir l’Observateur d’événements
eventvwr.msc

# Filtrer le log Application sur « IT-Network DocuScanner »
# Fréquent : chemin de base non inscriptible
# ou port 8585 occupé
```

10. Annexe

10.1 Endpoints API REST

Endpoint	Méthode	Rôle
/api/health	GET	Statut + version
/api/dashboard	GET	Indicateurs de synthèse
/api/hosts	GET	Liste des hôtes
/api/software	GET	Liste des logiciels
/api/shares	GET	Liste des partages
/api/licenses	GET	Clés de licence
/api/ad	GET	Objets AD (filtre : ?type, ?search)
/api/ad/stats	GET	Compteurs AD
/api/ad/query	POST	Déclencher requête LDAP en direct
/api/subnets	GET	Sous-réseaux (avec auto-derive)
/api/server-roles	GET	Rôles serveur (filtre : ?host, ?status)
/api/bsi	GET	Contrôles BSI (avec auto-derive)
/api/scans	GET	Historique de scans
/api/jobs	GET/POST	Jobs de scan
/api/jobs/{id}/trigger	POST	Démarrer un scan
/api/update/check	GET/POST	Vérification de mise à jour (GitHub)
/api/logs	GET	Entrées de log

10.2 Schéma de version

Sat-iTec utilise un schéma de version en trois parties X.YY.ZZ :

- X = Majeur (rare, changements d’architecture importants)
- YY = Mineur (nouvelles fonctionnalités, Y sur deux chiffres)
- ZZ = Patch (corrections, Z sur deux chiffres)

Exemple : 2.08.14 = Majeur 2, Mineur 8, Patch 14. Une nouvelle fonctionnalité incrémente YY (par ex. 2.09.00), une correction incrémente ZZ (par ex. 2.08.15).

10.3 Contact support

Sat-iTec Systemhaus GmbH

E-mail : support@sat-itec.se
Web : https://www.sat-itec.se
Releases GitHub : https://github.com/satitec/itscanner/releases