

Table des matières

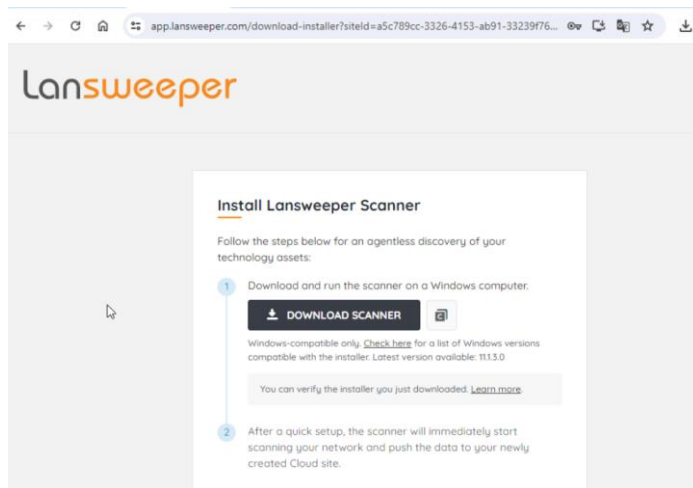
Introduction.....	2
Installation.....	2
Ajout de credential	5
Ajout d'une plage d'adresse.....	Erreur ! Signet non défini.
Meilleure version après fermeture et redémarrage	6
Mapper les credential	6
Lancement de scan.....	7

Introduction

Lansweeper est une solution pour gérer son parc informatique savoir les logiciels installés dessus etc cette solution est assez complète et dispose d'une solution de test pendant 14 jours.

Installation

Il faut d'abord que je m'enregistre sur lansweeper et que je tombe sur cette page



Ensuite je telecharge et j'exécute ça

Install Lansweeper Scanner

Follow the steps below for an agentless discovery of your technology assets:

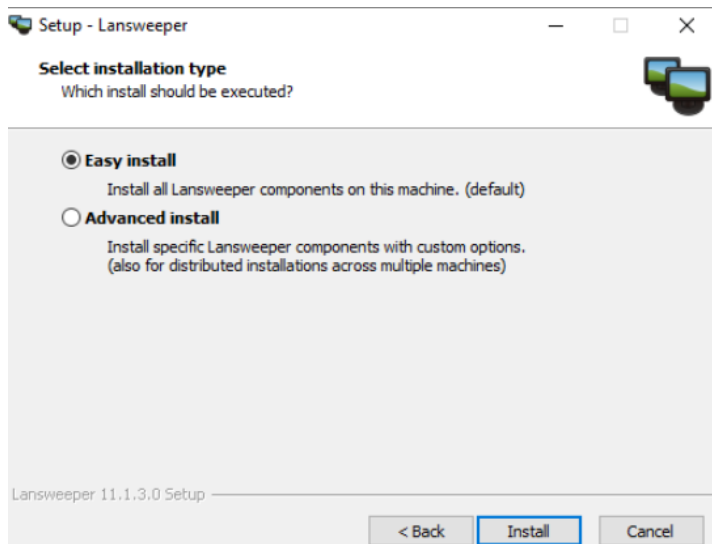
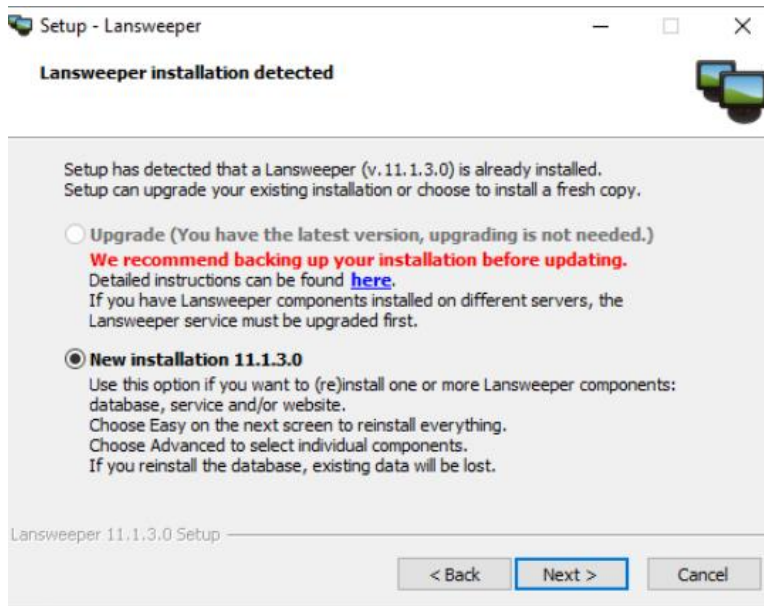
- 1 Download and run the scanner on a Windows computer.



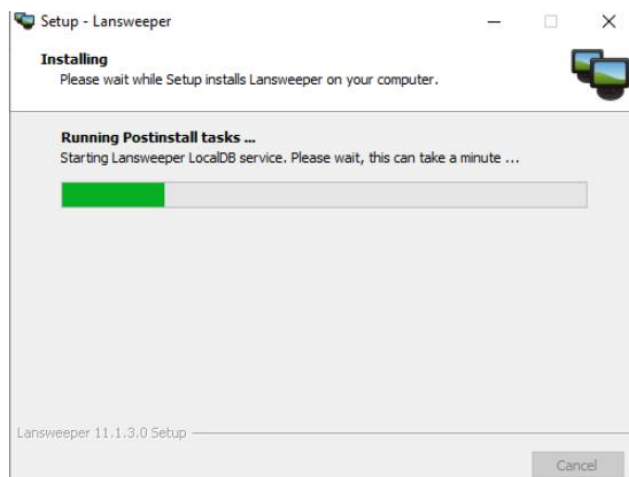
Windows-compatible only. [Check here](#) for a list of Windows versions compatible with the installer. Latest version available: 11.1.3.0

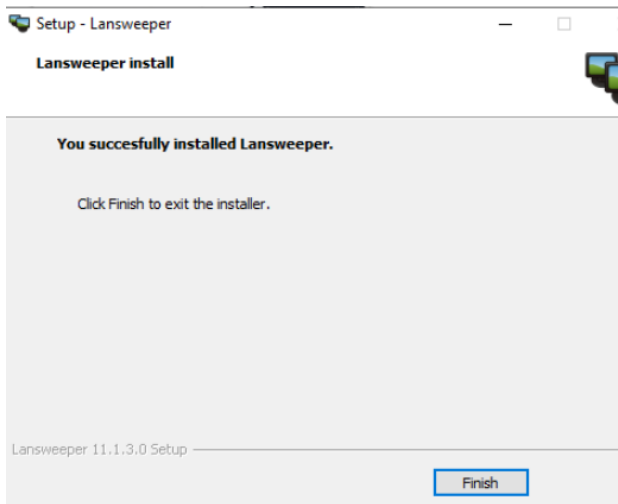
You can verify the installer you just downloaded. [Learn more](#).

- 2 After a quick setup, the scanner will immediately start scanning your network and push the data to your newly created Cloud site.



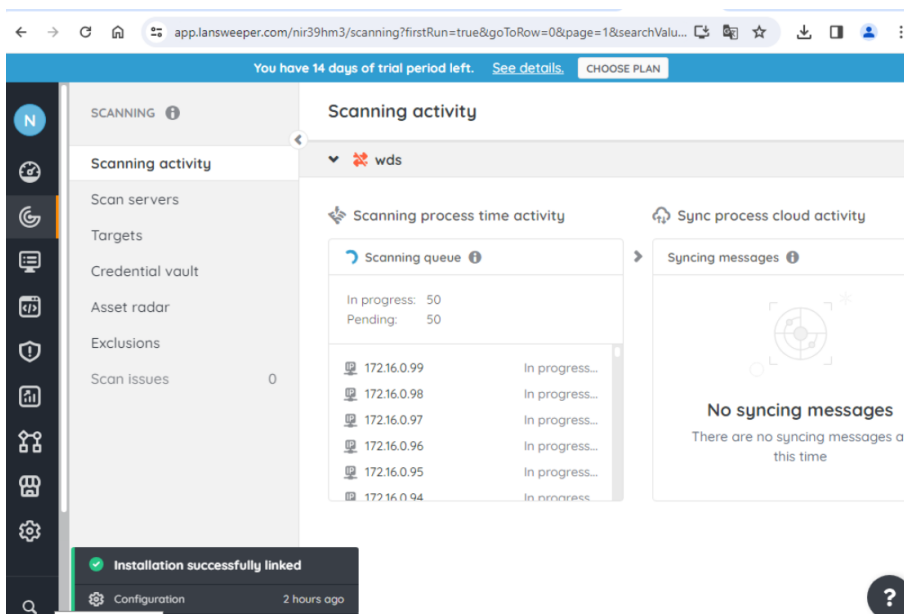
Ensuite l'installation se lance



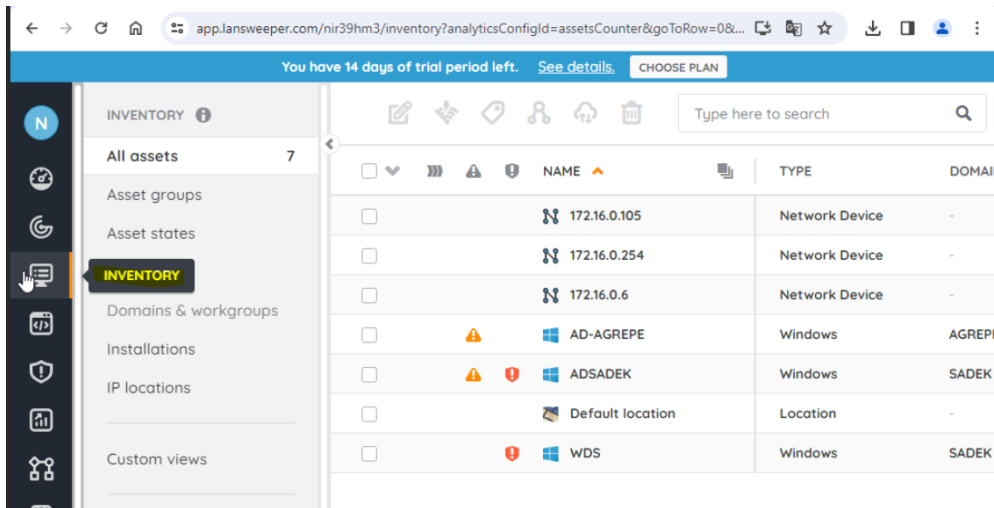


Ensuite pour accéder à la console c'est <http://localhost:83>

Dès le début un scan ce met en place sur mon réseau local



Je peux aussi voir les machines qu'il a analysé



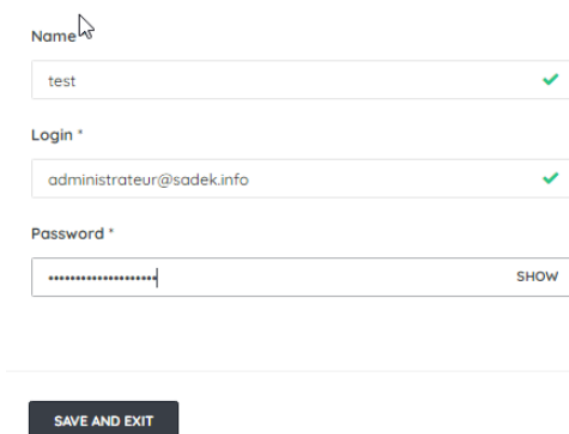
The screenshot shows the Lansweeper web interface. The top navigation bar includes a trial period notice and a 'CHOOSE PLAN' button. A sidebar on the left contains navigation options like 'All assets', 'Asset groups', 'Asset states', 'INVENTORY', 'Domains & workgroups', 'Installations', 'IP locations', and 'Custom views'. The main content area displays a table of assets with columns for NAME, TYPE, and DOMAIN.

	NAME	TYPE	DOMAIN
<input type="checkbox"/>	172.16.0.105	Network Device	-
<input type="checkbox"/>	172.16.0.254	Network Device	-
<input type="checkbox"/>	172.16.0.6	Network Device	-
<input type="checkbox"/>	AD-AGREPE	Windows	AGREPE
<input type="checkbox"/>	ADSADEK	Windows	SADEK
<input type="checkbox"/>	Default location	Location	-
<input type="checkbox"/>	WDS	Windows	SADEK

Ajout de credential

Pour pouvoir analyser les machines nous avons besoin d'un credential.

Il faut ce rendre dans scanning > Credential Vault > My Credential > Microsoft cloud credential



The screenshot shows a form for adding a credential. It has three input fields: 'Name' with the value 'test', 'Login' with the value 'administrateur@sadek.info', and 'Password' which is masked with dots. A 'SHOW' button is next to the password field. Below the form is a 'SAVE AND EXIT' button.

Name

Login *

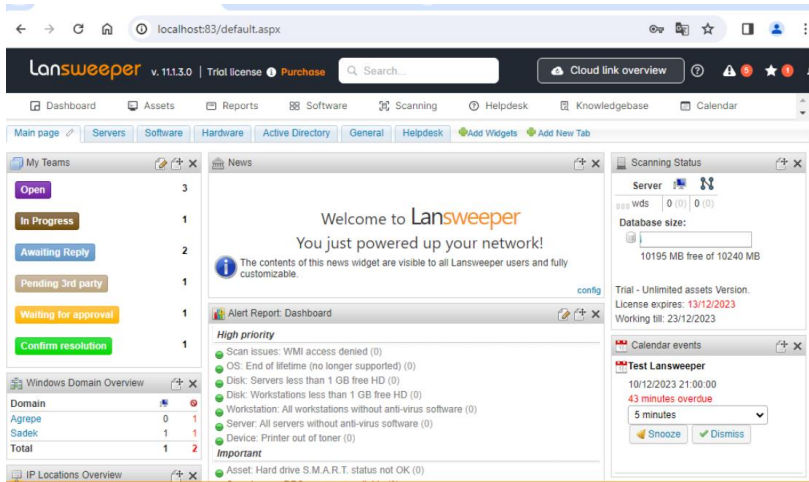
Password * SHOW

SAVE AND EXIT

Je n'ai pas trouvé comment le mapper aux machines mais d'après plusieurs tests tous les credentials sont essayés pour accéder aux machines windows si on a plusieurs configuré pour cette OS

Meilleure version après fermeture et redémarrage

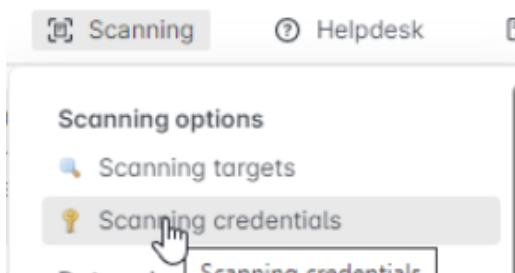
Si je ferme et retourne sur le port 83 avec mon navigateur et que je me logue avec mon user admin c'est beaucoup plus intéressant



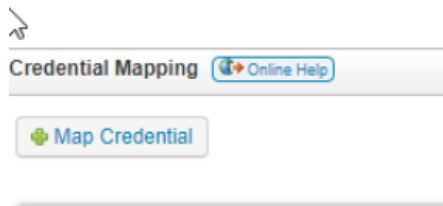
Mapper les credential

Toujours sur cette version on peut maintenant mapper les credential qu'on a fait sur l'ancienne page à des machines

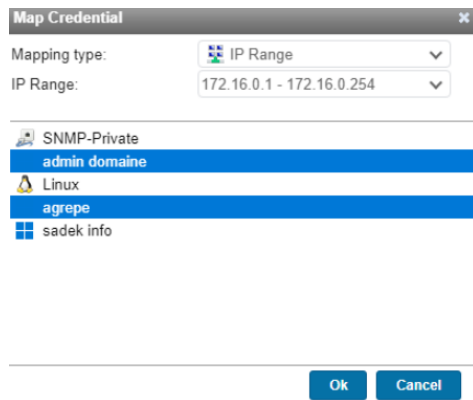
Il faut ce rendre ici



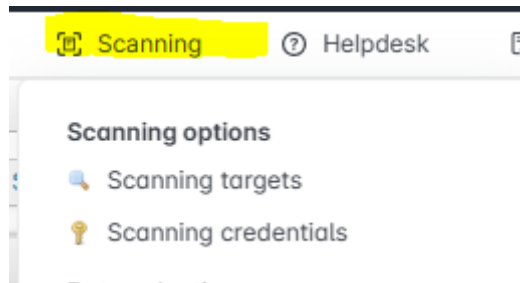
Ensuite pour mapper il faut cliquer ici



Je vais procéder par plage ip

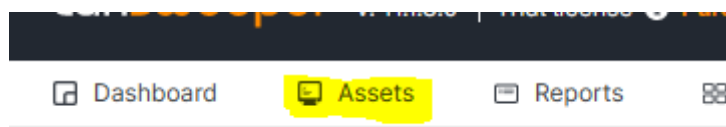


Lancement de scan



Quick scan	Enabled	Scan type	Target	Description	Schedule	Options	Last scan	Error
Scan now	<input checked="" type="checkbox"/>	Active Directory Computer Path	dc=sadek,dc=info (SADEK)		Show schedule			
Scan now	<input checked="" type="checkbox"/>	Active Directory Domain	sadek.info (SADEK)		Active scanning	Show options	10/12/2023 21:57	
Scan now	<input checked="" type="checkbox"/>	Active Directory User Path	dc=sadek,dc=info (SADEK)		Show schedule		10/12/2023 20:58	
Scan now	<input checked="" type="checkbox"/>	IP Range	172.16.0.1 - 172.16.0.254		Show schedule	Show options	10/12/2023 21:54	

Pour vérifier mes assets et voir le resultat du scan



Name	Type	Domain	Last User	OS	Model	Manufacturer	IP Address	IP Location	Mac Address	OU	State	Created at	Last successful scan	Last scan attempt
172.16.0.105	Network device						172.16.0.105	Local Subnet - Ethernet	52:4D:AF:10:73:E3		Active	10/12/2023 20:57:18	10/12/2023 21:56:11	10/12/2023 21:56:11
Accueil	Linux			Linux	Apache/2.4.53 (Debian)		172.16.0.6	Local Subnet - Ethernet	BA:A8:66:44:81:6D		Active	10/12/2023 20:57:28		10/12/2023 21:56:11
AD-AGREPE	Windows	AGREPE	AGREPE/Administrateur	Win 2019	Standard PC (i440FX + PIIX, 1996)	OEMU	172.16.0.230	Local Subnet - Ethernet	5E:6B:20:01:2B:BF		Active	10/12/2023 20:57:19	10/12/2023 21:59:50	10/12/2023 21:59:50
ADSARDEK	Windows	SADEK	Administrateur	Win 2019	Standard PC (i440FX + PIIX, 1996)	OEMU	172.16.0.250	Local Subnet - Ethernet	66:76:C7:82:EA:08		Active	10/12/2023 20:57:23	10/12/2023 21:59:57	10/12/2023 21:59:57
Default location	Location							Undefined			Active	10/12/2023 20:56:15	10/12/2023 20:56:15	
piSense - Login	Firewall				Firewall	piSense	172.16.0.254	Local Subnet - Ethernet	B2:40:D1:F7:F3:EB		Active	10/12/2023 20:58:03	10/12/2023 21:56:33	10/12/2023 21:56:33
WDS	Windows	SADEK	wds	Win 2019	Standard PC (i440FX + PIIX, 1996)	OEMU	172.16.0.104	Local Subnet - Ethernet	2A:93:54:98:79:ED		Active	10/12/2023 20:55:40	10/12/2023 21:59:34	10/12/2023 21:59:34

ADSARDEK - Windows Server 2019 Standard (64 bit)
 172.16.0.250 - SADEK - Uptime: 3day(s) 0 h 27 m
 Scan server: wds
 Last scan attempt: 10/12/2023 21:59:57

Summary Config Software Performance Uptime Location Event log Report History Docs Comments Scan time

Asset information

- Asset type: Windows
- Last user: Administrateur
- OS: Windows Server 2019 Standard (64 bit)
- Build: 10.0.17763S.107
- Version: 1809
- Domain: SADEK
- Manufacturer: OEMU
- Model: Standard PC (i440FX + PIIX, 1996)
- Memory: 9.8 GiB VRAM
- Processor: 3x Common KVM processor
- Graphics: Microsoft Basic Display Adapter 0 MB
- Optical: QEMU QEMU DVD-ROM ATA Device
- Antivirus: Windows Defender Enabled
- Network: Intel(R) PRO/1000 MT Network Connection - 66:76:C7:82:EA:08
192.168.1.250 - 172.16.0.250 - fe80::6105:ca5b:9e5d:faa3
- Harddisk: C: 77,3 GiB free of 149,5 GiB

Lifecycle information

- State: Active
- Purchased: unknown
- Warranty: unknown

Scan summary

- Scan status: ■■■
- Scan server: wds
- Created at: 10/12/2023 20:57:23
- Last successful scan: 10/12/2023 21:59:57
- Last scan attempt: 10/12/2023 21:59:57

Location

- IP location: Local Subnet - Ethernet
- Asset location: Undefined

Nous pouvons aussi voir toutes les applications installées

Summary Config Software Performance Uptime Location Event log Report History Docs Comments Scan time

Software Features License Keys Antivirus SQL Server Information

Show desktop apps

Installed software

Software	Version	Type	Publisher	Install Date
FileZilla	3.66.0	Desktop app	Tim Kosse	
Microsoft Command Line Utilities 13 for SQL Server	13.0.1601.5	Desktop app	Microsoft Corporation	01/12/2023
Microsoft Edge	120.0.2210.61	Desktop app	Microsoft Corporation	09/12/2023
Microsoft Edge Update	1.3.181.5	Desktop app		
Microsoft Exchange Server 2019 Cumulative Update 12	15.2.1118.7	Desktop app	Microsoft Corporation	
Microsoft Lync Server 2013, Bootstrapper Prerequisit...	5.0.8308.0	Desktop app	Microsoft Corporation	26/10/2023
Microsoft ODBC Driver 13 for SQL Server	13.0.811.168	Desktop app	Microsoft Corporation	01/12/2023
Microsoft Server Speech Platform Runtime (x64)	11.0.7400.345	Desktop app	Microsoft Corporation	26/10/2023