

PROCÉDURE DE MIGRATION

Procédure de migration de la console ESET PROTECT

On-Premise sur Virtual Appliance vers un serveur Windows

12/03/2024 | v.1.0

Introduction

Ce document explique succinctement et simplement comment migrer votre console ESET PROTECT On-Premise sur Virtual Appliance vers un serveur Windows.

Recommandations

• Les machines que vous souhaitez migrer doivent communiquer avec la console ESET PROTECT On-Premise.

• Nous conseillons de déchiffrer les appareils administrés chiffrés par ESET Full Disk Encryption (EFDE) avant la migration. Après la migration, vous pourrez chiffrer à nouveau les appareils nouvellement administrés à partir de la nouvelle console Cloud.

• Nous conseillons d'effectuer la migration sur un échantillon de postes dans un premier temps. Une fois cet échantillon remonté sur la nouvelle console, vous pouvez effectuer la procédure sur le reste des postes.

Liens utiles

• La procédure de migration d'ESET PROTECT On-Premise est détaillée sur notre site : <u>https://support.eset.com/en/kb7732-migrate-eset-protect-from-virtual-appliance-to-windows-server</u>

Migrer ESET PROTECT Virtual Appliance vers ESET PROTECT Server (Windows)

1. Création d'un certificat homologue

Ouvrez la console Web de l'Appliance virtuelle ESET PROTECT et connectez-vous.

Il vous faut ensuite créer un certificat homologue, pour se faire, rendez-vous dans « Plus » \rightarrow « Certificat Homologue » \rightarrow « Nouveau » \rightarrow « Certificat » :

eser	PROTECT			দ্বিত ব	Computer Name		QUICK LINKS 🗢	③ HELP マ	A ADMINISTRATO	R ⊡ LOG	3OUT nin
		Peer Certificates	ACCESS	GROUP Select 🗊	Tags	~	ADD FILTER			PRESETS 🗢] ၀
교		Tags 🔎		DESCRIPTION		STATUS	VALID FROM		VALID TO		٥
A	Quaranune			Server certificate			2020 Nov 28 00:00	00	2030 Nov 30 00:00:00		
	COMPUTERS Computer Users			Agent certificate			2020 Nov 28 00:00	00	2030 Nov 30 00:00:00		
Þ	Dynamic Group Templates			Proxy certificate			2020 Nov 28 00:00	00	2030 Nov 30 00:00:00		
≞	icinplaces			Agent certificate for s	erver assisted i		2020 Nov 28 00:00	00	2030 Nov 30 00:00:00		
۲	LICENSES										
φ											
۶											
>											
	Peer Certificates	\sim									
		This is where you can see the list of your applied tags and quickly filter them.									
	Server Server Settings										
				+ Certificate	-						
				ФРИ/АВМ С							
			ACTIO	NS 🗢 NEW 1	EDIT	SHO	W REVOKED			K © 1 ©	

Dans L'onglet **« Général »**, saisissez le titre du certificat. Sélectionnez **« Serveur »** dans le menu déroulant Produit. Laissez le champ Hôte défini sur la valeur par défaut et laissez les champs Phrase de passe et Confirmer la phrase de passe vide.

ese) protect		تع م ح	Computer Name	QUICK LINKS 🗢	⊘ HELP ∀	A ADMINISTRATOR	LOGOUT S9 min
		Create Certificate						
돠		$\underbrace{ \text{Peer Certificates}}_{\text{Peer Certificate}} > \text{New Server Certificate}$						
						1		*
		0 Basic	Description					
~		A Sign	New Server Certificate					
Þ		Summary	Tags					
			Select tags					
٢			Product ③					
Φ			Server		~			
∿								
			Host (2)					
			•					
			🕴 Passphrase 💿					
			Confirm passphrase					
			Show passphrase					
						1		
			Attributes (Subject))				
			Common name					-
E			BACK CONTINUE	FINISH CANCEL				

Accédez ensuite à l'onglet **« Signature »**. Sélectionnez **« Autorité de certification »** sous **« Méthode de signature »**. Dans les options d'**« Autorité de certification »**, cliquez sur **« Sélectionner l'autorité de certification >**. Une nouvelle fenêtre s'ouvre. Sélectionnez l'autorité de certification que vous souhaitez utiliser pour signer un nouveau certificat. Cliquez sur **« OK »** pour confirmer et revenir à la fenêtre précédente.

er Certificates > New Serve	r Certificate	
n de		
Basic	Basic	
Sign	Signing method	
Summary	Certification authority	
	Custom pix the	
	A Certification authority	
	<select authority="" certification=""></select>	
	Create Certification Authority	
	Custom pfx file	
	Choose File No file chosen	
	UPLOAD	
	Certification Authority passphrase	

Saisissez la « **phrase de passe de l'autorité de certification** ». Il s'agit du même mot de passe que celui que vous utilisez pour vous connecter à la console Web de l'Appliance virtuelle ESET PROTECT. Cliquez sur « **Terminer** » pour appliquer.

Create Certificate Peer Certificate New Server Certificate		
Basic Sign Summary	Signing method Certification authority Custom pfx file Certification authority CN=MSP Synchronization CA; Create Certification Authority Custom pfx file Cnosse File No file chosen UPLOAD	
	Certification Authority passphrase	
	BACK CONTINUE FINISH CANCEL	

2. Définir une nouvelle adresse IP du serveur ESET PROTECT et créer une politique de migration.

<u>Ouvrez la console Web de l'Appliance virtuelle ESET PROTECT</u> et connectez-vous.

Accédez à « Politique » → « Nouvelle politique » :

eset	PROTECT		G ▼ Computer Name QUICK LINKS マ ③ HELP マ	A ADMINISTRATOR ☐ LOGOUT >9 min
		Policies :	ACCESS GROUP Select 👔 SHOW UNASSIGNED 💟 🔯 All (86) Tags 🤝	
돠		Policies ,O	ADD FILTER	PRESEIS
		^ All	NAME POLICY PRODUCT TAGS	DESCRIPTION
₩ L I 📀 🔶 ÷	Reports Tasks Installers Policies Notifications Status Overview More	Cuttom Policies Cuttom Policies Discrete Control Co	Application reporting - Report ESET Management Agent Connection - Connect every 6 ESET Management Agent Connection - Connect every 2 ESET Management Agent Connection - Connect every 6 ESET Management Agent Connection - Connect every 6 ESET Management Agent General - Maximum protection ESET Virtualization Security General - Recommended setti ESET Virtualization Security - S Antivirus - Balanced ESET Endpoint for macOS (OS Antivirus - Maximum security ESET Endpoint for macOS (OS	ESET Management Agent will Agent default replication inter Replication interval for up to 1 Replication interval recommen The most secure configuration Recommended settings for ES ESET Security Product for OS Taking advantage of advanced
		Tags P	Device control - Maximum sec ESET Endpoint for Windows Device control - Read only ESET Endpoint for Windows	All devices are blocked. When All devices can only be read
			Firewall - Block all traffic exce ESET Endpoint for Windows	Block all traffic except connect
			Logging - Full diagnostic logg ESET Endpoint for Windows	This template will ensure that
			Logging - Log important even ESET Endpoint for Windows	Policy ensures that warnings,
			Antivirus - Balanced ESET Endpoint for Windows	Security configuration recom
		This is where you can see the list of your	Antivirus - Maximum security ESET Endpoint for Windows	Taking advantage of machine I
		applied tags and quickly filter them.	Visibility - Balanced ESET Endpoint for Windows	Default setting for visibility. St
			Visibility - Invisible mode ESET Endpoint for Windows	Disabled notifications, alerts,
Ð	COLLAPSE		ACTIONS 🗢 NEW POLICY	K © 1 🛛 📚

Nommez votre politique :

es	PROTECT ON-PREM	(¢) \checkmark Type to searc	:h	QUICK LINKS 🗢 💿 HELP 🗢	⊟ LOGOUT ×23 h
==		New Policy			
G		Policies > New Policy			
▲				News	
1		Basic		Name	
Đ		A Settings		New Policy	
÷		Assign		Description	
۲	Policies	Summary			
φ				Tags	
8-				Select tags	
		>			
E	COLLAPSE			BACK CONTINUE FINISH CANCEL	

Cliquez sur l'onglet **« Paramètres »**, sélectionnez **« ESET Management Agent »** dans le menu déroulant, puis cliquez sur **« Modifier la liste des serveurs »**.

asic	COT Management Associ		2
ettings	Q Type to search		
ssign			0 • 4
ummary	○ ●	Edit server list	
	○ ● 🗲 Data limit	1	MB 🗸 🕄
	O • 4 Connection interval	Change interval	0
	○ ● ≁ Certificate	Change certificate	0

Dans la fenêtre Serveurs, cliquez sur **« Ajouter »**. Dans le champ Hôte, saisissez l'adresse IP de votre nouveau serveur ESET PROTECT (sous Windows) au format xxx.xxx.xxx. Si vous utilisez un port autre que le port 2222 par défaut du serveur ESET PROTECT, indiquez votre numéro de port personnalisé. Cliquez sur **« OK »**. Assurez-vous que l'adresse de votre nouveau serveur ESET PROTECT figure en premier dans la liste et cliquez sur **« Enregistrer »**.



Cliquez sur « **Attribuer** » dans le menu de gauche puis sur « **Attribuer** » pour afficher une nouvelle fenêtre contextuelle avec tous les groupes statiques et dynamiques.

New Policy					
Basic Settings	\frown	ASSIGN UNASSIGN			
Assign		TARGET NAME	TARGET DESCRIPTION	TARGET TYPE	٥
Summary			NO DATA AVAILABLE		
		BACK CONTINUE	FINISH CANCEL		

Sélectionnez le groupe statique test que vous souhaitez migrer pour affecter la politique à tous les agents connectés et cliquez sur **« OK »**.

es	et PROTE	ECT ON-PREM	D Type to search	O II QUICK LINKS 🗢 💿 HELP 🗢	& ADMINISTRATOR 🖂 LOGOUT
- 22	DASHBOARD	Select targets			×
G	COMPUTERS	Groups ,P ⊗ ♠	A 0 V O SHOW SUBGROUPS Tags	ADD FILTER PRESETS 👻	
▲	DETECTIONS	All (3)	□ △2 COMPUTER NAME TAGS	ST M M LAST CONNECTED	A (3)
	Reports	Test group (1)		V Updated January 4, 2024 14:	0 0
Đ	Tasks	V Windows computers			
	Installers	🗌 🗸 🖿 Linux computer			٢
0	Policies	Mac computers			
~	Notification	Devices with outdated modules			
	Nouncation	Devices with an outdated operation			
T V	Status Over	Problematic devices			
.	More	Unactivated security product			
		Mobile devices			
		1/26			4 © 1 ⊙ ♀
		TARGET NAME	TARGET DESCRIPTION	TARGET TYPE	0
		Test group		setic Group	
				N	
		REMOVE REMOVE ALL			OK CANCEL
Ð	COLLAPSE		BACK CONTINUE	CANCEL	

Passez en revue les paramètres de cette politique et cliquez sur **« Terminer »** pour l'appliquer. Le délai d'application de la politique varie en fonction de la configuration d'ESET PROTECT Server.

Une fois la politique appliquée, ouvrez ESET PROTECT Virtual Appliance et créez une sauvegarde de la base de données.

3. Activer l'interface Webmin

Dans le menu de gestion de l'Appliance serveur ESET PROTECT, sélectionnez « Activer/Désactiver l'interface Webmin » pour activer l'interface Webmin.

Connectez-vous à l'interface Webmin à l'aide d'un navigateur Web avec l'adresse IP de l'Appliance virtuelle ESET PROTECT et le port 10000. Par exemple, https://xxx.xxx.xxx:10000. Connectez-vous à l'interface Webmin à l'aide des informations d'identification de l'Appliance virtuelle ESET PROTECT, où root est l'identifiant de connexion.

You	SWebmin must enter a username and sword to login to the server on
å r	oot
• •	
Rem	ember me
	♣) Sign in

Dans le menu principal de l'interface Webmin, développez le menu « **Tools** » et cliquez sur « **File Manager** ». Cliquez sur le dossier « **root** ». Cliquez avec le bouton droit de la souris sur le fichier era-backup.sql et sélectionnez « **Download** » dans le menu contextuel. Enregistrez le fichier sur un lecteur local et copiez-le à un emplacement accessible depuis la machine Windows cible.



Retournez à la fenêtre ESET PROTECT Virtual Appliance, connectez-vous au mode de gestion et sélectionnez « **Arrêter le système** ».

Sur le serveur Windows cible, <u>préparez une installation propre de MySQL Server</u>. Lorsque le programme d'installation de MySQL vous demande de créer un mot de passe de compte racine, nous vous recommandons d'utiliser le même que celui que vous avez utilisé dans l'Appliance ESET PROTECT Server.

Avant de poursuivre, vous devez importer la sauvegarde de la base de données ESET PROTECT Virtual Appliance dans une base de données vide nommée era_db sur le serveur MySQL cible. Ouvrez l'invite de commande et accédez au dossier des fichiers binaires du serveur MySQL (l'emplacement par défaut est C:\NProgram Files\NMySQL\NMySQL Server x.x\Nbin). Tapez les commandes suivantes, et remplacez "TARGETHOST" par l'adresse du serveur de base de données cible.

mysql --host TARGETHOST -u root -p "--execute=CREATE DATABASE era_db /*!40100
DEFAULT CHARACTER SET utf8 */;"â€

Restaurez la base de données de sauvegarde d'ESET PROTECT Virtual Appliance sur la base de données vide préparée précédemment. Remplacer "PATHTOBACKUPFILE" par l'emplacement où vous avez stocké la sauvegarde de la base de données ESET PROTECT Virtual Appliance :

mysql --host TARGETHOST -u root -p era_db < PATHTOBACKUPFILE</pre>

Créez un utilisateur de base de données ESET PROTECT On-Prem nommé root sur le serveur MySQL cible. Remplacez "TARGETERAPASSWD" par le mot de passe que vous avez utilisé pour vous connecter à ESET PROTECT Virtual Appliance Web Console :

mysql --host TARGETHOST -u root -p "--execute=CREATE USER root@'%' IDENTIFIED BY
'TARGETERAPASSWD';"

Accordez les droits d'accès appropriés à l'utilisateur de la base de données ESET PROTECT On-Prem - root, sur le serveur MySQL cible :

mysql --host TARGETHOST -u root -p "--execute=GRANT ALL ON eradb.* TO root;"â€<

4. Configuration du serveur ESET PROTECT

<u>Téléchargez le composant ESET PROTECT Server</u>. Exécutez le fichier d'installation et suivez l'assistant d'installation.

	Téléch	arger ESET I	Prot	ect
Insta	llers tout-en-un	Appliance Virtuelles	Ins	tallers standalone
	Install	ers standalone ESET I	Protect	
	Configurer le té	léchargement		Documentation
Component	Server	•		Online help guide Find more documentation
Operating system Bitness	Windows Server 2022, Storage Server 2016, 14 2012, Storage Server 2	Server 2019, Server 2016, 9, Server 2012 Core, Server – 012R2 (64-bit)		
	TÉ	LÉCHARGER		
	Nom de fichier: server_ Vers	x64.msi Taille du fichier: 113 MB sion: 11.0.199.0		
	Voir tou:	s les changelogs		

Dans l'écran de configuration de la connexion au serveur de base de données, assurez-vous que le serveur MySQL et le pilote ODBC MySQL sont correctement détectés. La base de données doit être nommée era_db. Dans la section Compte de base de données, saisissez le nom d'utilisateur "root" et le mot de passe que vous avez créés dans le chapitre précédent.

Please enter database serve	r connection.	es
Database:	MySQL Server	~
ODBC driver:	MySQL ODBC 5.3 Unicode Driver	~
Database name:	era_db	
Hostname:	localhost	
Port:	3306	
Database account		
Username:		
Decemend		

Cliquez sur « **Next** » pour continuer. Le programme d'installation vous demande si vous souhaitez utiliser l'utilisateur root fourni comme utilisateur de base de données pour ESET PROTECT On-Prem.

Cochez la case **« Use Administrator password already stored in the database »**. Modifiez le port de l'agent et de la console si nécessaire pour qu'ils correspondent aux paramètres de l'Appliance ESET PROTECT Server. La valeur par défaut du port de l'agent est 2222 et celle du port de la console est 2223. Cliquez sur **« Next »**.



Dans la fenêtre suivante, sélectionnez « **Keep currently used certificate** » et cliquez sur « **Next** ». Suivez l'assistant d'installation pour terminer l'installation du composant serveur.

🔀 ESET PROTECT Server Setup	_		×
Certificates Please specify whether certificates will be generated or not.		(езет
 Keep currently used certificates Load certificates from file Generate new certificates 			
Back Next	t	Cano	el

Installez ESET PROTECT Web Console.

<u>Ouvrez ESET PROTECT On-Prem dans votre navigateur Web</u> et connectez-vous.

Utilisez votre mot de passe ESET PROTECT Server Appliance. Vérifiez que les agents ont migré avec succès et qu'ils se connectent au nouveau serveur. Ne désinstallez pas votre ancien serveur ESET PROTECT Server Appliance avant d'avoir vérifié que la migration s'est déroulée correctement.

5. Créer une nouvelle politique et définir un nom d'hôte pour un nouveau serveur ESET PROTECT

Une fois que la migration test s'est effectuée correctement, il faut migrer le reste du parc vers la nouvelle console.

Cliquez sur « Politiques » \rightarrow « Nouvelle politique ».

Dans la section « Base », saisissez un nom pour votre politique.

Cliquez sur « Paramètres », sélectionnez « ESET Management Agent » dans le menu déroulant, puis cliquez sur Modifier la liste des serveurs.

Dans la fenêtre Serveurs, cliquez sur **« Ajouter »**. Dans le champ **« hôte »**, saisissez le nom d'hôte de votre nouveau serveur ESET PROTECT. Si vous utilisez un port autre que le port 2222 par défaut du serveur ESET PROTECT, indiquez votre numéro de port personnalisé. Cliquez sur **« OK »**. Assurez-vous que le nom d'hôte de votre nouveau serveur ESET PROTECT est répertorié en premier, puis cliquez sur **« Enregistrer »**.

Cliquez sur **« Attribuer »** puis **« Attribuer »** pour afficher une nouvelle fenêtre contextuelle avec tous les groupes statiques et dynamiques.

Cochez les groupes d'ordinateurs auxquels vous souhaitez attribuer la stratégie et cliquez sur OK. Nous vous recommandons d'appliquer la politique par lots à différents groupes d'ordinateurs.

Passez en revue les paramètres de cette stratégie et cliquez sur **« Terminer »** pour l'appliquer. Le temps nécessaire à l'application de la politique varie en fonction de l'intervalle de réplication de l'Appliance virtuelle ESET PROTECT.

Lorsque la nouvelle politique est appliquée et qu'il n'y a pas de problème avec le nouveau serveur ESET PROTECT, supprimez l'ancienne politique avec les deux noms d'hôte que vous avez créés dans la section 2.