



STORMSHIELD



GUIDE

**STORMSHIELD ENDPOINT SECURITY
EVOLUTION**

GUIDE D'INSTALLATION

Version 2.6.2

Dernière mise à jour du document : 22 août 2024

Référence : ses-fr-guide_d_installation-v2.6.2



Table des matières

1. Avant de commencer	4
2. Prérequis système pour SES Evolution	6
2.1 Backend	6
2.2 Console d'administration	7
2.3 Gestionnaires d'agents	8
2.4 Bases de données SQL Server	8
2.5 Agents	9
2.5.1 Prérequis	9
2.5.2 Utiliser l'agent sur les systèmes d'exploitation Microsoft Windows Server Core	10
2.6 Dimensionner le serveur SES Evolution selon le nombre d'agents	11
3. Préconisations de sécurité pour SES Evolution	13
3.1 Appliquer les recommandations de sécurité de Microsoft	13
3.2 Configurer le pare-feu Windows	13
3.3 Désactiver l'accès au mode sans échec pour les utilisateurs standard	14
4. Récupérer la licence SES Evolution	15
5. Installer SES Evolution	16
5.1 Réaliser une installation de démonstration	16
5.1.1 Résoudre les problèmes	18
5.2 Réaliser une installation standard	18
5.2.1 Préparer une installation standard	18
5.2.2 Effectuer une installation standard	19
5.3 Installer les serveurs SES Evolution sur des domaines Active Directory différents	22
6. Ajouter une console, un composant backend ou un gestionnaire d'agents	23
7. Mettre à jour SES Evolution	24
7.1 Gérer la mise à jour de SES Evolution depuis des systèmes d'exploitation non compatibles	24
7.1.1 Backend	24
7.1.2 Console d'administration	25
7.1.3 Gestionnaires d'agents	25
7.1.4 Agents	25
7.2 Résoudre les problèmes	26
7.2.1 Failed to extract files from patch (0xa0050005)	26
8. Désinstaller SES Evolution	27
8.1 Désinstaller les consoles, gestionnaires d'agents et backends	27
8.2 Désinstaller les bases de données	27
9. Configurer les connexions TLS entre les composants	28
9.1 Configurer les connexions TLS par stratégie de groupe (GPO)	28
9.2 Configurer les connexions TLS par script PowerShell	28
10. Assurer la continuité de service	30
10.1 Recommandations pour les gestionnaires d'agents	30
10.1.1 Assurer la redondance des gestionnaires d'agents	30
10.1.2 Gérer la défaillance d'un gestionnaire d'agents	30



- 10.2 Recommandations pour les serveurs backend 31
 - 10.2.1 Assurer la redondance des serveurs backend 31
 - 10.2.2 Gérer la défaillance d'un serveur backend 31
- 10.3 Recommandations pour les bases de données 31
 - 10.3.1 Assurer la redondance des bases de données 31
 - 10.3.2 Gérer la défaillance d'une base de données 32
- 11. Compatibilité entre SES Evolution et les autres solutions de sécurité 33
 - 11.1 Agent SES Evolution 33
 - 11.2 Console 36
 - 11.3 Serveur backend 36
 - 11.4 Gestionnaire d'agents 36
- 12. Pour aller plus loin 38

Dans la documentation, Stormshield Endpoint Security Evolution est désigné sous la forme abrégée : SES Evolution.



1. Avant de commencer

Bienvenue dans le guide d'installation de Stormshield Endpoint Security Evolution version 2.6.2.

La solution de sécurité globale SES Evolution offre aux organisations de toutes tailles une protection complète des postes de travail des collaborateurs.

L'agent SES Evolution est installé sur les postes et les protège des attaques connues et inconnues, ainsi que des intrusions, de façon transparente pour les collaborateurs. Indépendant de bases de signatures, il peut fonctionner aussi bien en mode connecté que déconnecté des gestionnaires d'agents SES Evolution, tout en conservant le même niveau de sécurité.

La console d'administration permet d'organiser, paramétrer et surveiller l'ensemble des agents d'un parc. Elle permet de définir des politiques de sécurité entièrement configurables et de segmenter les agents en groupes afin de faciliter leur administration. Les outils avancés de suivi de logs et d'analyse d'attaque permettent à l'administrateur de surveiller l'état de son parc et de remonter à la source des attaques détectées et bloquées par les agents SES Evolution.

La solution SES Evolution s'intègre également à vos autres solutions de sécurité en remontant directement ses événements dans votre SIEM.

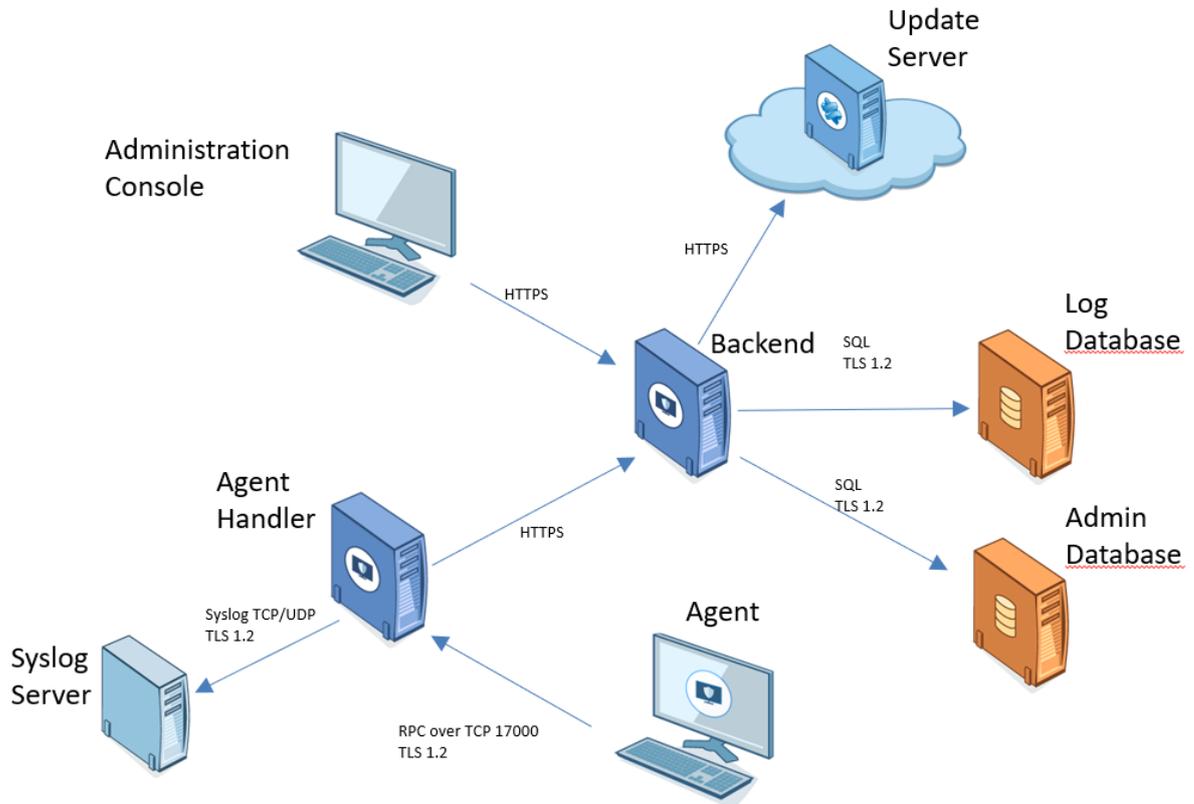
Le Centre d'installation de SES Evolution, *SES_Evolution_Installation_Center.exe*, permet d'effectuer les opérations suivantes :

- Réaliser une nouvelle installation,
- Modifier une installation existante,
- Mettre à jour une installation existante,
- Supprimer les bases de données.

Le Centre d'installation s'affiche dans la langue du système d'exploitation.

La solution SES Evolution comprend un ensemble de composants qui communiquent entre eux de façon sécurisée :

- Des bases de données d'administration et de logs,
- Un ou plusieurs gestionnaires d'agents qui reçoivent directement les informations des agents et leurs logs, demandent la mise à jour de la base de données d'administration et renvoient les logs vers un serveur Syslog,
- Un ou plusieurs serveurs applicatifs backend, qui centralisent les opérations effectuées sur l'environnement SES Evolution et qui mettent à disposition une API REST publique. Pour plus d'informations sur l'API publique, reportez-vous à la section [Activer et gérer l'API publique de SES Evolution](#) du *Guide d'administration*.
- Une ou plusieurs consoles d'administration,
- Le serveur de mise à jour Stormshield, qui permet de télécharger les ressources les plus récentes, e.g., nouvelles politiques de sécurité intégrées, mises à jour des jeux de règles intégrés.
- Les agents déployés sur les postes de travail ou sur les serveurs.



Pour plus d'informations sur la protection des connexions réseau utilisant TLS, reportez-vous à la section [Configurer les connexions TLS entre les composants](#).

Le déploiement des agents SES Evolution sur les postes de travail est géré depuis la console d'administration. Pour plus d'informations, reportez-vous à la section [Installer les agents sur les postes de travail](#) du *Guide d'administration*.

Pour obtenir le Centre d'installation SES Evolution dans la version souhaitée, rendez-vous dans votre espace client [MyStormshield](#), section **Téléchargements**.



2. Prérequis système pour SES Evolution

Pour installer et utiliser Stormshield Endpoint Security Evolution version 2.6.2 sous Microsoft Windows, vous devez disposer au minimum des prérequis ci-dessous.

Certains des composants requis se trouvent dans le dossier *resources_x64* livré dans la distribution.

2.1 Backend

i NOTES

- Le clonage de machines virtuelles avec un composant backend installé n'est pas supporté. Il en résulterait un comportement instable de SES Evolution et la désinstallation du composant serait impossible.
- Le composant backend ne doit pas être installé sur un contrôleur de domaine.

Systèmes d'exploitation	Consultez le document Cycle de vie produits pour connaître les informations de compatibilité avec les versions de Microsoft Windows.
Processeurs pour machines physiques	Processeur 64 bits de 2 GHz avec au minimum deux cœurs ou équivalent. Les processeurs Itanium ne sont pas supportés.
	i NOTE Plus la machine possède de cœurs, plus le déploiement de l'environnement sur les agents du parc est rapide.
Processeurs pour machines virtuelles	Au minimum une socket virtuelle et deux cœurs de 2 GHz par socket.
Mémoire physique	Au minimum 2 Go ou davantage si le système d'exploitation le nécessite.
Espace disque	<ul style="list-style-type: none">• Au minimum 100 Mo pour l'installation• Au minimum 1 Go pour le stockage des données Il s'agit du prérequis d'espace disque pour le système de fichiers NTFS. De l'espace supplémentaire est aussi nécessaire pour les mises à jour et le stockage des logs.
Configuration réseau	<ul style="list-style-type: none">• Pas de prérequis d'adresse IP statique• Communications entrantes :<ul style="list-style-type: none">◦ TCP 443◦ TCP 10443 (API publique)• Communications sortantes (ports SQL par défaut, mais peuvent dépendre des paramètres de l'instance SQL Server) :<ul style="list-style-type: none">◦ TCP 1433 (SQL)◦ TCP 1434 (SQL)◦ UDP 1434 (SQL)



Logiciel	<ul style="list-style-type: none">• Serveur IIS, à installer avant SES Evolution. Le rôle IIS doit être activé.• Framework .NET 4.6.2
Certificat	<ul style="list-style-type: none">• Présence du certificat <i>VeriSign Universal Root Certification Authority</i> pour vérifier l'authenticité des mises à jour SES Evolution. Il doit se trouver dans le magasin de certificats Autorités de certification racines de confiance ou Autorités de certification racines tierce-partie.

2.2 Console d'administration

i NOTE

Le clonage de machines virtuelles avec une console d'administration SES Evolution installée n'est pas supporté. Il en résulterait un comportement instable de SES Evolution et la désinstallation du composant serait impossible.

Systèmes d'exploitation	Consultez le document Cycle de vie produits pour connaître les informations de compatibilité avec les versions de Microsoft Windows.
Processeurs pour machines physiques	Processeurs 64 bits avec au minimum 2 GHz Intel Pentium 4 ou équivalent. Les processeurs Itanium ne sont pas supportés.
Processeurs pour machines virtuelles	Au minimum une socket virtuelle et deux cœurs de 1 GHz par socket. Stormshield recommande une socket virtuelle et deux cœurs de 2 GHz par socket.
Mémoire physique	Au minimum 1 Go. Stormshield recommande 2 Go.
Espace disque	<ul style="list-style-type: none">• Au minimum 100 Mo pour l'installation• Au minimum 100 Mo pour le stockage des données Il s'agit du prérequis d'espace disque pour le système de fichiers NTFS.
Configuration réseau	<ul style="list-style-type: none">• Communications sortantes :<ul style="list-style-type: none">◦ TCP 443 (HTTPS)
Logiciel	Framework .NET 4.6.2
Affichage	Au minimum 1680x1050.
Certificat	<ul style="list-style-type: none">• Présence du certificat <i>VeriSign Universal Root Certification Authority</i> pour vérifier l'authenticité des mises à jour SES Evolution. Il doit se trouver dans le magasin de certificats Autorités de certification racines de confiance ou Autorités de certification racines tierce-partie.



2.3 Gestionnaires d'agents

i NOTES

- Le clonage de machines virtuelles avec un gestionnaire d'agents installé n'est pas supporté. Il en résulterait un comportement instable de SES Evolution et la désinstallation du composant serait impossible.
- Le gestionnaire d'agents ne doit pas être installé sur un contrôleur de domaine.

Systèmes d'exploitation	Consultez le document Cycle de vie produits pour connaître les informations de compatibilité avec les versions de Microsoft Windows.
Processeurs pour machines physiques	Processeur 64 bits de 2 GHz avec au minimum deux cœurs ou équivalent. Les processeurs Itanium ne sont pas supportés.
Processeurs pour machines virtuelles	Au minimum une socket virtuelle et deux cœurs de 2 GHz par socket.
Mémoire physique	Au minimum 2 Go ou davantage si le système d'exploitation le nécessite.
Espace disque	<ul style="list-style-type: none">• Au minimum 100 Mo pour l'installation• Au minimum 1 Go pour le stockage des données <p>Il s'agit du prérequis d'espace disque pour le système de fichiers NTFS. De l'espace supplémentaire est aussi nécessaire pour les mises à jour et le stockage des logs.</p>
Configuration réseau	<ul style="list-style-type: none">• Pas de prérequis d'adresse IP statique• Communications entrantes :<ul style="list-style-type: none">◦ TCP 17000• Communications sortantes :<ul style="list-style-type: none">◦ TCP 443 (HTTPS)◦ Port TCP pour Syslog◦ Port UDP pour Syslog
Logiciel	Framework .NET 4.6.2
Certificat	<ul style="list-style-type: none">• Présence du certificat <i>VeriSign Universal Root Certification Authority</i> pour vérifier l'authenticité des mises à jour SES Evolution. Il doit se trouver dans le magasin de certificats Autorités de certification racines de confiance ou Autorités de certification racines tierce-partie.

2.4 Bases de données SQL Server

Systèmes d'exploitation	<ul style="list-style-type: none">• Windows Server 2016• Windows Server 2019• Windows Server 2022
-------------------------	---



Processeurs	Processeur 64 bits de 2 GHz minimum. Les processeurs Itanium ne sont pas supportés. L'exécution de SQL Server sur une machine virtuelle est plus lente que son exécution en mode natif en raison de la surcharge liée à la virtualisation.
Mémoire physique	SQL Server Express : au minimum 1 Go et au maximum 1,41 Go SQL Server : au minimum 4 Go Vous devez définir le quota de RAM correspondant à la quantité de mémoire à allouer à SQL Server pour ne pas qu'il utilise toute la mémoire du serveur. Cette valeur est configurée via l'outil <i>SQL Server Management Studio</i> après installation des bases de données. Veuillez consulter les préconisations dans la colonne RAM du tableau Dimensionner le serveur SES Evolution selon le nombre d'agents .
Espace disque	<ul style="list-style-type: none">• Au minimum 6 Mo pour l'installation.• L'espace pour le stockage des données dépend de l'environnement. Stormshield recommande le système de fichiers NTFS.
Configuration réseau	<ul style="list-style-type: none">• Pas de prérequis d'adresse IP statique.• Communications entrantes (ports SQL par défaut, mais peuvent dépendre des paramètres de l'instance SQL Server) :<ul style="list-style-type: none">◦ TCP 1433 (SQL)◦ TCP 1434 (SQL)◦ UDP 1434 (SQL)
Logiciel	Consultez le document Cycle de vie produits pour connaître les informations de compatibilité avec les versions de Microsoft SQL Server.

Pour plus d'informations sur le dimensionnement et l'installation de SQL Server, reportez-vous au *Guide des préconisations SQL Server*.

2.5 Agents

2.5.1 Prérequis

Systèmes d'exploitation	Consultez le document Cycle de vie produits pour connaître les informations de compatibilité avec les versions de Microsoft Windows.
Processeurs pour machines physiques	Processeurs 64 bits avec au minimum 2 GHz Intel Pentium 4 ou équivalent. Les processeurs Itanium ne sont pas supportés.
Processeurs pour machines virtuelles	Au minimum une socket virtuelle et un cœur de 1 GHz par socket. Stormshield recommande une socket virtuelle et deux cœurs de 2 GHz par socket.
Mémoire physique	Au minimum 1 Go. Davantage si le système d'exploitation le nécessite. Stormshield recommande 2 Go.



Espace disque	<ul style="list-style-type: none">• Au minimum 100 Mo pour l'installation,• Au minimum 200 Mo pour le stockage des données. <p>Il s'agit du prérequis d'espace disque pour le système de fichiers NTFS. De l'espace supplémentaire est aussi nécessaire pour les mises à jour et les logs.</p>
Configuration réseau	<ul style="list-style-type: none">• Communications sortantes :<ul style="list-style-type: none">◦ TCP 17000 (RPC)
Bande passante réseau	Au minimum 12 Kbit/s. Une bande passante plus faible peut empêcher les échanges entre l'agent et le gestionnaire d'agents.
Logiciel	Framework .NET 4.6.2 ou supérieur.
Affichage	Au minimum 1024X768.
Certificat	<p>Présence du certificat <i>VeriSign Universal Root Certification Authority</i> pour vérifier l'authenticité des mises à jour SES Evolution.</p> <p>Il doit se trouver dans le magasin de certificats Autorités de certification racines de confiance ou Autorités de certification racines tierce-partie. Vous pouvez le télécharger directement sur votre espace client MyStormshield, dans la section Téléchargements > Stormshield Endpoint Security > Evolution > Resources. Dans l'archive, le fichier <i>.bat</i> permet d'installer automatiquement le certificat dans le magasin de certificats avec un compte administrateur.</p>

2.5.2 Utiliser l'agent sur les systèmes d'exploitation Microsoft Windows Server Core

Consultez le document [Cycle de vie produits](#) pour connaître les informations de compatibilité avec les versions de Microsoft Windows Server Core.

Ces systèmes d'exploitation possèdent une interface graphique réduite. L'interface de l'agent n'est donc pas démarrée automatiquement lors de l'ouverture de session d'un utilisateur (icône  dans la barre des tâches sur un système d'exploitation "classique"). Pour afficher l'interface graphique de l'agent :

- Utilisez la commande **EsGui.exe**.

De plus, si une demande de confirmation par l'utilisateur est paramétrée dans une règle de sécurité, l'agent n'affiche pas de fenêtre et considère automatiquement que la réponse à la confirmation est "non". L'utilisateur n'a pas la possibilité de répondre "oui".



2.6 Dimensionner le serveur SES Evolution selon le nombre d'agents

Le tableau ci-dessous fournit une estimation des besoins matériels **minimum** pour votre environnement SES Evolution par rapport au nombre d'agents installés. Jusqu'à 5 000 agents environ, tous les composants serveur peuvent être installés sur une seule machine. Au-delà, nous vous recommandons de répartir les composants sur plusieurs machines.

Un gestionnaire d'agents peut supporter jusqu'à 30 000 agents.

Il est fortement recommandé d'utiliser des disques durs de type SSD pour optimiser les performances et les temps de réponse.

! IMPORTANT

Le quota de RAM correspond à la quantité de mémoire que vous devez allouer à SQL Server pour ne pas qu'il utilise toute la mémoire du serveur. Cette valeur est configurée via l'outil *SQL Server Management Studio* après installation des bases de données. Référez-vous à la colonne RAM du tableau ci-dessous.

Nombre d'agents	CPU	RAM	Disque
< 200 agents (1 serveur)	2 cœurs / 2 threads - 3 GHz	4 Go Quota SQL : 1,5 Go	170 Go pour 1 an de rétention de logs, 155 Go pour 6 mois, 150 Go pour 3 mois.
< 500 agents (1 serveur)	4 cœurs / 4 threads - 3 GHz	6 Go Quota SQL : 3 Go	250 Go pour 1 an de rétention de logs, 175 Go pour 6 mois, 150 Go pour 3 mois.
< 1 000 agents (1 serveur)	4 cœurs / 4 threads - 3 GHz	6 Go Quota SQL : 3 Go	300 Go pour 1 an de rétention de logs, 250 Go pour 6 mois, 200 Go pour 3 mois.
< 2 500 agents (1 serveur)	4 cœurs / 4 threads - 3 GHz	8 Go Quota SQL : 4 Go	600 Go pour 1 an de rétention de log, 350 Go pour 6 mois, 250 Go pour 3 mois.
< 5 000 agents (1 serveur)	6 cœurs / 6 threads - 3 GHz	12 Go Quota SQL : 6 Go	1 To pour 1 an de rétention de log, 600 Go pour 6 mois, 350 Go pour 3 mois.
< 10 000 agents (2 serveurs)	Base de données : 2 cœurs / 2 threads -3 GHz Backend + Gestionnaire d'agents : 4 cœurs / 4 threads -3 GHz	Base de données : 8 Go Backend + Gestionnaire d'agents : 8 Go	Base de données : 2 To pour 1 an de rétention de log, 1 To pour 6 mois, 600 Go pour 3 mois. Backend + Gestionnaire d'agents : 50 Go
< 30 000 agents (3 serveurs)	Base de données : 4 cœurs / 4 threads -3 GHz Backend + Gestionnaire d'agents : 4 cœurs / 4 threads -3 GHz Gestionnaire d'agents supplémentaire : 4 cœurs / 4 threads -3 GHz	Base de données : 16 Go Backend + Gestionnaire d'agents : 16 Go Gestionnaire d'agents supplémentaire : 16 Go	Base de données : 8 To pour 1 an de rétention de log, 4 To pour 6 mois, 2 To pour 3 mois. Backend + Gestionnaire d'agents : 100 Go Gestionnaire d'agents supplémentaire : 100 Go



< 60 000 agents (4 serveurs)	Base de données : 4 cœurs / 4 threads -3 GHz Backend + Gestionnaire d'agents : 4 cœurs / 4 threads -3 GHz 2 Gestionnaires d'agents supplémentaires : 4 cœurs / 4 threads -3 GHz	Base de données : 16 Go Backend + Gestionnaire d'agents : 16 Go 2 Gestionnaires d'agents supplémentaires : 16 Go	Base de données : 12 To pour 1 an de rétention de log, 6 To pour 6 mois, 5 To pour 3 mois. Backend + Gestionnaire d'agents : 100 Go 2 Gestionnaires d'agents supplémentaires : 100 Go
< 90 000 agents (5 serveurs)	Base de données : 4 cœurs / 4 threads -3 GHz Backend + Gestionnaire d'agents : 4 cœurs / 4 threads -3 GHz 3 Gestionnaires d'agents supplémentaires : 4 cœurs / 4 threads -3 GHz	Base de données : 16 Go Backend + Gestionnaire d'agents : 16 Go 3 Gestionnaires d'agents supplémentaires : 16 Go	Base de données : 16 To pour 1 an de rétention de log, 8 To pour 6 mois, 5 To pour 3 mois. Backend + Gestionnaire d'agents : 100 Go 3 Gestionnaires d'agents supplémentaires : 100 Go
< 120 000 agents (6 serveurs)	Base de données : 4 cœurs / 4 threads -3 GHz Backend + Gestionnaire d'agents : 4 cœurs / 4 threads -3 GHz 4 Gestionnaires d'agents supplémentaires : 4 cœurs / 4 threads -3 GHz	Base de données : 16 Go Backend + Gestionnaire d'agents : 16 Go 4 Gestionnaires d'agents supplémentaires : 16 Go	Base de données : 16 To pour 1 an de rétention de log, 8 To pour 6 mois, 5 To pour 3 mois. Backend + Gestionnaire d'agents : 100 Go 4 Gestionnaires d'agents supplémentaires : 100 Go
< 150 000 agents (7 serveurs)	Base de données : 4 cœurs / 4 threads -3 GHz Backend + Gestionnaire d'agents : 4 cœurs / 4 threads -3 GHz 5 Gestionnaires d'agents supplémentaires : 4 cœurs / 4 threads -3 GHz	Base de données : 16 Go Backend + Gestionnaire d'agents : 16 Go 5 Gestionnaires d'agents supplémentaires : 16 Go	Base de données : 24 To pour 1 an de rétention de log, 12 To pour 6 mois, 6 To pour 3 mois. Backend + Gestionnaire d'agents : 100 Go 5 Gestionnaires d'agents supplémentaires : 100 Go



3. Préconisations de sécurité pour SES Evolution

Pour la sécurité et le bon fonctionnement de SES Evolution, nous vous recommandons de respecter les préconisations suivantes.

3.1 Appliquer les recommandations de sécurité de Microsoft

Les systèmes d'exploitation Microsoft disposent de mécanisme de sécurité. Nous préconisons d'appliquer sur votre parc les recommandations de Microsoft sur les sujets suivants :

- Système de fichiers NTFS recommandé,
- Configuration par défaut des répertoires d'installation recommandée,
- À partir de Windows 10, utilisation vigilante de l'assistant Cortana,
- Utilisation modérée du clonage des postes de travail et serveurs,
- Configuration du fichier de vidage du système (fichier dump ou full dump). Nous préconisons de configurer le système d'exploitation pour générer un fichier de vidage contenant l'image mémoire complète lors d'un arrêt de la machine.
- À partir de Windows 8, utilisation recommandée de la protection Secure Boot,
- Activation permanente de la fonctionnalité Hyper-V sur Windows 10 recommandée,
- Chiffrement de partition système avec BitLocker recommandé,
- À partir de Windows 10, utilisation recommandée de Credential Guard,
- À partir de Windows 8.1, activation de la protection LSA renforcée recommandée,
- Activation du chiffrement TLS 1.2 et désactivation des chiffrements TLS 1.0 et 1.1 pour les communications vers les serveurs backend.

Pour plus d'informations sur ces sujets, veuillez vous reporter à la documentation Microsoft en vigueur.

3.2 Configurer le pare-feu Windows

Assurez-vous que les numéros de ports suivants sont autorisés sur les pare-feu des machines hébergeant les composants de SES Evolution et également sur tous les équipements réseau situés entre les machines hébergeant les composants de SES Evolution.

Agents

Protocoles	Sens	Port	Commentaires
TCP	Sortant	17000	Communication avec les gestionnaires d'agents SES Evolution
UDP	Sortant	53	Requêtes DNS
TCP	Sortant	80	Accès aux listes de révocation de certificats
TCP	Sortant	88	Authentification Kerberos
TCP/UDP	Sortant	389	Authentification LDAP
TCP	Sortant	3268	Authentification GC (Global Catalog) LDAP

Gestionnaire d'agents



Protocoles	Sens	Port	Commentaires
TCP	Entrant	17000	Communication avec les agents SES Evolution
TCP	Sortant	433	Connexions HTTPS avec le serveur backend
TCP	Sortant	1468	Communication avec un serveur Syslog
TCP/TLS	Sortant	6514	Communication avec un serveur Syslog
UDP	Sortant	514	Communication avec un serveur Syslog

Serveur backend

Protocoles	Sens	Port	Commentaires
TCP	Entrant	443	Connexions HTTPS provenant de la console d'administration ou du gestionnaire d'agents
TCP	Sortant	443	Connexions HTTPS vers le serveur public de mise à jour Stormshield
TCP/UDP	Sortant	Variable	Connexions vers le moteur de base de données. Le port dépend de sa configuration.
TCP	Entrant	10443	Connexions HTTPS provenant des systèmes externes qui utilisent les API publiques (SIEM/SOAR)

Console d'administration

Protocoles	Sens	Port	Commentaires
TCP	Sortant	433	Connexions HTTPS vers le serveur backend

3.3 Désactiver l'accès au mode sans échec pour les utilisateurs standard

Le mode sans échec permet de diagnostiquer des problèmes qui empêchent d'utiliser un poste de travail lorsqu'il est démarré normalement. Par défaut la configuration Windows permet à tous les utilisateurs de démarrer leur poste avec ce mode.

Or, en mode sans échec, l'auto-protection de l'agent SES Evolution est désactivée. Vous devez donc autoriser l'utilisation de ce mode aux seuls administrateurs.

Pour désactiver l'accès au mode sans échec aux utilisateurs non administrateurs, dans la base de registre Windows, positionnez la valeur *SafeModeBlockNonAdmins* de la clé *HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System* à « 1 ».



4. Récupérer la licence SES Evolution

Vous devez récupérer votre licence sur votre espace client MyStormshield et l'enregistrer au cours de l'installation de la solution.

Les licences définissent le nombre d'agents SES Evolution actifs que vous pouvez gérer avec la solution, ainsi qu'une date de fin de validité. Vous pouvez cumuler plusieurs licences pour un même environnement. En revanche, une licence est valable pour l'installation d'un seul environnement SES Evolution. Si vous installez un autre environnement, vous devez disposer d'une licence supplémentaire.

Pour récupérer votre licence :

1. Munissez-vous de votre bon de livraison Stormshield (delivery document au format PDF) et connectez-vous sur votre espace client [MyStormshield](#).
2. Dans le menu de gauche, choisissez **Produit > Enregistrer un produit > Enregistrer un logiciel SES**, et acceptez les conditions d'utilisation.
3. Entrez les informations suivantes :
 - **Société cible** : Nom de la société sous lequel vous êtes enregistré chez Stormshield.
 - **Clé de licence** : Suite de caractères qui se trouve dans la colonne Numéro de série du bon de livraison.
 - **Revendeur** : Nom de votre revendeur SES Evolution.
4. Cliquez sur **Enregistrer**.
5. Dans la zone **Liste des produits** sur le tableau de bord de votre espace client, cliquez sur votre numéro de série.
6. Cliquez sur **Télécharger toutes les licences** et décompressez le fichier zip reçu.



5. Installer SES Evolution



Pour installer la solution SES Evolution, le Centre d'installation vous guide à travers les différentes étapes d'une installation standard ou de démonstration.

Les composants de la solution peuvent être installés sur la même machine ou sur des machines différentes.

Avant d'installer SES Evolution, veuillez prendre connaissance des préconisations suivantes :

- La console, le composant backend et les bases de données doivent être installés sur des machines appartenant au même domaine Active Directory, ou sur deux domaines possédant une relation de confiance.
- L'installation des bases de données nécessite SQL Server.
- Il est recommandé d'installer le composant backend et les bases de données dans une zone de confiance.
- N'installez pas le composant backend ou le gestionnaire d'agents sur un contrôleur de domaine.
- Vous devez disposer des droits d'administration pour installer la solution.
- Avant une installation complète ou une installation du composant backend, il est recommandé de désactiver les mises à jour Windows et de les réactiver ensuite.
- Sur un composant backend ou un gestionnaire d'agents, il est recommandé d'exclure le répertoire "%ProgramData%\Stormshield\SES Evolution" dans les antivirus présents sur le poste afin d'optimiser les performances. En effet SES Evolution utilise de nombreux fichiers au format compressé *cab* qui déclenchent l'analyse antivirus.
- Vous pouvez installer un agent SES Evolution sur un composant backend ou sur un gestionnaire d'agents : une politique de sécurité adéquate est fournie par défaut pour les protéger.

En cas de problème lors de l'installation de SES Evolution, consultez les fichiers de logs qui se trouvent dans le répertoire *AppData/Local/Temp* de l'administrateur.

5.1 Réaliser une installation de démonstration

L'installation de démonstration consiste à installer l'ensemble des composants de la solution sur une même machine avec une configuration simplifiée des mots de passe et comptes d'accès.

ATTENTION

Une installation de démonstration ne permet pas d'ajouter des composants supplémentaires. Elle est uniquement recommandée à des fins de test ou de démonstration. Ne l'installez pas dans un environnement de production.

De plus, il n'est pas possible de migrer d'une installation de démonstration vers une installation standard. Une désinstallation complète de la solution serait nécessaire avant de procéder à une installation standard.

Pour installer SES Evolution, procédez de la façon suivante :



1. Connectez-vous à la machine avec un compte Windows ayant les caractéristiques suivantes :
 - Si la machine appartient à un domaine, ce doit être un compte de domaine,
 - Il doit avoir les droits d'administration sur la machine locale,
 - Si la base de données existe avant l'installation, le compte doit avoir accès à l'instance de base de données avec le rôle serveur "sysadmin".
2. Double-cliquez sur le fichier *SES_Evolution_Installation_Center.exe*.
3. Cliquez sur **Nouvelle installation**.
4. Sélectionnez **Installation de démonstration**.
5. Dans la section **Bases de données**, les options d'installation sont automatiquement sélectionnées en fonction de votre configuration :
 - Si aucune instance SQL Server n'est déjà installée sur le poste, SES Evolution propose d'installer SQL Server Express. La première option est alors automatiquement sélectionnée. Si un fichier d'installation SQL Server Express et le cas échéant un fichier de mise à jour SQL Server Express sont présents dans le même répertoire que le Centre d'installation, le Centre d'installation les détecte automatiquement. Complétez les informations de connexion à l'instance SQL Server Express.
 - Si une instance SQL Server est déjà existante sur le poste, la deuxième option est automatiquement sélectionnée. L'instance SQL Server doit être vide de données. Le nom de l'instance de la base de données s'affiche automatiquement.
 - Que vous choisissiez un compte Windows ou SQL Server, le rôle "sysadmin" est nécessaire pour créer les bases de données.
6. Configurez le **Stockage de la base de données de logs**. Les paramètres diffèrent selon que vous disposez de SQL Server Enterprise ou de SQL Server Express.
 - **Chemin de stockage des logs** : Utilisez le chemin de stockage par défaut de SQL Server ou entrez un chemin personnalisé. Ce champ n'est disponible que pour SQL Server Enterprise.
 - **Rétention des événements agents et Rétention des logs système** : Par défaut, les logs SES Evolution sont conservés 12 mois avant d'être automatiquement supprimés, et seulement deux mois si vous utilisez SQL Server Express. Entrez une durée de rétention supérieure ou égale à 1 mois. Pour SQL Server Express, la durée maximale autorisée est de 12 mois.
Avec SQL Server Enterprise, vous pouvez choisir de conserver les logs indéfiniment. Dans ce cas, assurez-vous d'avoir toujours suffisamment d'espace disque pour contenir tous les logs.
Les valeurs de rétention peuvent être modifiées ultérieurement via la console d'administration. Pour plus d'informations, reportez-vous à la section [Gérer la suppression des logs](#) du *Guide d'administration*.
7. Dans la section **Mot de passe unique général**, saisissez un mot de passe qui sera utilisé à la fois pour chiffrer les autorités de certification et les connexions du composant backend aux bases de données. Choisissez un mot de passe respectant les contraintes de l'instance de base de données.
Le compte "super administrateur" est le compte de domaine avec lequel vous êtes connecté. Il doit appartenir au même domaine Active Directory que le serveur SQL et les différentes instances de bases de données SES Evolution, ainsi que la console d'administration. Sinon une relation de confiance doit exister entre les domaines.
8. Enregistrez votre fichier de licence. Pour récupérer votre licence, reportez-vous à la section [Récupérer la licence SES Evolution](#).
9. Cliquez sur **Installer**.



10. À l'étape suivante, déplacez la souris de manière aléatoire. Les mouvements permettent de produire des nombres aléatoires à partir desquels sont générés les certificats nécessaires au fonctionnement et à la sécurité de SES Evolution.
11. Lorsque l'installation est terminée, quittez le Centre d'installation. La solution est prête à l'emploi.

Nous vous recommandons de mettre en place une redondance des composants backoffice. Pour plus d'informations, reportez-vous à la section [Assurer la continuité de service](#).

5.1.1 Résoudre les problèmes

Installation failed. The network path was not found

Situation : Lors d'une installation de démonstration, le Centre d'installation affiche l'erreur : *Installation failed. The network path was not found.*

Cause : Vous avez lancé le Centre d'installation en étant connecté avec un compte local alors que votre machine est liée à un Active Directory.

Solution : Installez SES Evolution en étant connecté avec un compte Active Directory.

5.2 Réaliser une installation standard

L'installation standard permet d'utiliser SES Evolution dans un environnement de production. Vous pouvez soit installer tous les composants sur une même machine, soit les répartir sur plusieurs machines.

Lors d'une première installation de SES Evolution sur une première machine, l'installation des bases de données, des certificats et la création du super administrateur sont obligatoires et vous ne pouvez pas les décocher. Vous pouvez ajouter d'autres composants sur cette même machine.

Pour ajouter ensuite un ou plusieurs composants backend, des consoles d'administration et des gestionnaires d'agents sur d'autres machines, vous devez exécuter le Centre d'installation sur chaque machine et modifier une installation existante. Les machines sur lesquelles vous installez des consoles et des gestionnaires d'agents doivent pouvoir communiquer avec le backend. Et le backend doit pouvoir communiquer avec les bases de données.

5.2.1 Préparer une installation standard

Lors d'une installation standard de votre environnement SES Evolution, suivez les recommandations ci-dessous :

- Les configurations Active Directory, DNS et réseau doivent être préparées en amont, avant l'installation de SES Evolution.
- Il est possible d'installer le composant backend et les gestionnaires d'agents sur des machines membres de domaines Active Directory différents. Pour plus d'informations, reportez-vous à la section [Installer les serveurs SES Evolution sur des domaines Active Directory différents](#).
- Les serveurs backend et gestionnaires d'agents ne doivent pas être installés sur un contrôleur de domaine.



- Sur les parcs dépassant les 50 000 agents, nous vous recommandons de mettre en place le mécanisme de load-balancing de Windows (fonctionnalité NLB) sur les machines hébergeant les serveurs backend afin de former un cluster permettant d'assurer la redondance et la répartition de charge. Pour plus d'informations, reportez-vous à la section [Assurer la continuité de service](#).
- Nous préconisons d'exécuter le Centre d'installation successivement sur les machines dans l'ordre suivant :
 1. Serveur(s) hébergeant les bases de données d'administration et de logs,
 2. Serveur(s) hébergeant le composant backend,
 3. Serveur(s) hébergeant le gestionnaire d'agents,
 4. Serveur(s) ou poste(s) de travail hébergeant la console d'administration.
- Nous vous recommandons de mettre en place une redondance de tous les composants backoffice. Pour plus d'informations, reportez-vous à la section [Assurer la continuité de service](#).

5.2.2 Effectuer une installation standard

Pour une première installation de SES Evolution, procédez de la façon suivante :

1. Connectez-vous à la machine avec un compte Windows ayant les caractéristiques suivantes :
 - Si la machine appartient à un domaine, ce doit être un compte de domaine,
 - Il doit avoir les droits d'administration sur la machine locale,
 - Si la base de données existe avant l'installation, le compte doit avoir accès à l'instance de base de données avec le rôle serveur "sysadmin".
2. Double-cliquez sur le fichier *SES_Evolution_Installation_Center.exe*.
3. Cliquez sur **Nouvelle installation**.
4. Sélectionnez **Installation standard**.
5. Indiquez l'adresse des instances des bases de données d'administration et de logs. Les deux bases peuvent se trouver sur la même instance. Quel que soit le type d'authentification choisi, le rôle "sysadmin" est nécessaire pour créer les bases de données.

i NOTE

Les instances de bases de données ne doivent pas contenir de données et doivent être accessibles à partir du système d'exploitation où est exécuté le Centre d'installation.



6. Configurez le **Stockage de la base de données de logs**. Les paramètres diffèrent selon que vous disposez de SQL Server Enterprise ou de SQL Server Express.
 - **Chemin de stockage des logs** : Utilisez le chemin de stockage par défaut de SQL Server ou entrez un chemin personnalisé. Ce champ n'est disponible que pour SQL Server Enterprise.
 - **Rétention des événements agents et Rétention des logs système** : Par défaut, les logs SES Evolution sont conservés 12 mois avant d'être automatiquement supprimés, et seulement deux mois si vous utilisez SQL Server Express. Entrez une durée de rétention supérieure ou égale à 1 mois. Pour SQL Server Express, la durée maximale autorisée est de 12 mois.
Avec SQL Server Enterprise, vous pouvez choisir de conserver les logs indéfiniment. Dans ce cas, assurez-vous d'avoir toujours suffisamment d'espace disque pour contenir tous les logs.
Les valeurs de rétention peuvent être modifiées ultérieurement via la console d'administration. Pour plus d'informations, reportez-vous à la section [Gérer la suppression des logs](#) du *Guide d'administration*.
7. Indiquez les mots de passe à utiliser pour chiffrer les clés privées pour les autorités de certification racine et intermédiaires.
8. Le compte super administrateur est pré-rempli avec le compte de domaine avec lequel vous êtes connecté. Le super administrateur est l'utilisateur de la console qui permet de créer les autres utilisateurs. Il doit appartenir au même domaine Active Directory que le serveur SQL et les différentes instances de bases de données SES Evolution, ainsi que la console d'administration. Sinon une relation de confiance doit exister entre les domaines.

i NOTE

Si vous renommez le compte de domaine qui est super administrateur SES Evolution, assurez-vous d'avoir créé au préalable un utilisateur portant le nouveau nom dans la console d'administration SES Evolution. Sinon vous ne pourrez plus vous connecter à la console. Pour plus d'informations, reportez-vous au *Guide d'administration*.



9. Cochez **Backend** si vous souhaitez installer un composant backend sur cette machine. Le backend centralise toutes les opérations effectuées sur l'environnement. Il est le cœur de l'installation. Remplissez les paramètres suivants :
- Le nom DNS de l'hôte qui sera utilisé pour accéder au backend en HTTPS. Il est pré-rempli avec le nom de la machine sur laquelle vous êtes connecté et le domaine. Ce nom ne peut pas être changé par la suite.
 - Le nom d'hôte du cluster doit obligatoirement être renseigné. Si vous souhaitez faire de la répartition de charge ou de la redondance (fonctionnalité NLB) sur plusieurs backends (recommandé au-delà de 50 000 agents), c'est cette adresse que les gestionnaires d'agents et la console utiliseront pour se connecter au backend. Il doit être différent du premier nom d'hôte. Cette information ne peut être remplie que lors d'une première installation du backend. Ces deux noms DNS ne peuvent pas être changés par la suite. Si vous ne souhaitez pas mettre en place un cluster de backend, vous devez néanmoins déclarer une entrée DNS (CNAME) avec un nom spécifique (e.g., SESBACKCLUSTER.SES.local). Son adresse IP pointera sur l'adresse de la machine où est installé le backend. Par la suite, vous n'aurez pas besoin de réinstaller des composants SES Evolution en cas de mise en oeuvre d'une architecture avec cluster NLB. Vous devrez simplement modifier l'alias DNS créé afin qu'il pointe sur l'adresse IP virtuelle du cluster NLB.
 - Sélectionnez un type de compte qui sera utilisé comme identité des processus de travail du serveur IIS :

Compte de domaine	Compte de domaine, idéalement créé uniquement pour être utilisé comme identité des services et programmes SES Evolution, avec un mot de passe qui n'expire jamais. Il est aussi utilisé par le service de mise à jour du backend, installé sur chaque serveur backend.
Compte local	Compte local à la machine. Cette option peut être utilisée pour faire une installation de SES Evolution hors d'un domaine Windows et utilisant plusieurs machines différentes. Cela implique de créer des comptes locaux avec un nom et mot de passe identiques sur toutes les machines. Il est aussi utilisé par le service de mise à jour du backend, installé sur chaque serveur backend.
Compte IIS prédéfini	Compte virtuel, valable uniquement sur la machine locale, à n'utiliser qu'en cas d'installation locale d'un backend sur la même machine que la base de données. Dans ce cas, le service de mise à jour du backend est installé en tant que SYSTEM.

- Entrez le nom et le mot de passe du compte.
10. Cochez ensuite **Gestionnaire d'agents** et **Console d'administration** si vous souhaitez les installer sur cette machine. Indiquez l'adresse de contact du gestionnaire d'agents qui sera utilisée par les agents pour le contacter.
11. Enregistrez votre fichier de licence. Pour récupérer votre licence, reportez-vous à la section [Récupérer la licence SES Evolution](#).
12. Cliquez sur **Installer**.
13. À l'étape suivante, déplacez la souris de manière aléatoire. Les mouvements permettent de produire des nombres aléatoires à partir desquels sont générés les certificats nécessaires au fonctionnement de SES Evolution.
Si le rôle IIS n'est pas activé, le Centre d'installation l'active automatiquement à l'installation du composant backend. Cette opération peut être assez longue.
14. Lorsque l'installation est terminée, quittez le Centre d'installation.



Pour installer les autres composants sur d'autres machines, exécutez le Centre d'installation sur chaque machine et choisissez le menu **Modifier une installation existante**. Pour plus d'informations, reportez-vous à la section [Ajouter une console, un composant backend ou un gestionnaire d'agents](#).

Nous vous recommandons de mettre en place une redondance des composants backoffice. Pour plus d'informations, reportez-vous à la section [Assurer la continuité de service](#).

5.3 Installer les serveurs SES Evolution sur des domaines Active Directory différents

Si vous possédez plusieurs domaines Active Directory dans votre infrastructure, vous avez la possibilité d'installer les gestionnaires d'agents sur des machines membres de domaines différents de celui du composant backend. La sécurisation des communications entre le composant backend et les gestionnaires d'agents s'effectue par une authentification mutuelle à l'aide des certificats.

Les différents domaines Active Directory doivent donc pouvoir communiquer entre eux.

Pour installer un gestionnaire d'agents sur un domaine différent de celui du composant backend, suivez la procédure suivante :

1. Depuis un serveur membre du domaine Active Directory 1, dans le Centre d'installation réalisez une **installation standard** et cochez l'installation du composant backend.
2. Depuis un serveur membre du domaine Active Directory 2, dans le Centre d'installation cliquez sur **Modifier une installation existante** et cliquez sur **Gestionnaire d'agents Stormshield Endpoint Security Evolution**.
3. Remplissez les paramètres et cliquez sur **Installer**.

Si vous installez plusieurs gestionnaires d'agents, répétez l'opération sur chaque machine hébergeant les gestionnaires.



6. Ajouter une console, un composant backend ou un gestionnaire d'agents

Le menu **Ajouter un nouveau composant à une installation existante** dans le Centre d'installation vous permet d'installer des consoles, des serveurs backend ou des gestionnaires d'agents sur des machines différentes de celle sur laquelle vous avez fait la première installation. Vous ne pouvez pas ajouter de composant si vous avez réalisé une installation de démonstration.

Dans le cas des gestionnaires d'agents, vous pouvez les installer sur des machines membres de domaines Active Directory différents de celui du composant backend. Pour plus d'informations, reportez-vous à la section [Installer les serveurs SES Evolution sur des domaines Active Directory différents](#).

L'ajout de ces composants au sein d'un même environnement ne nécessite pas de licence supplémentaire.

Pour ajouter une console, un composant backend ou un gestionnaire d'agents, effectuez les actions suivantes :

1. Connectez-vous à la machine avec un compte Windows ayant les caractéristiques suivantes :
 - Si la machine appartient à un domaine, ce doit être un compte de domaine,
 - Il doit avoir les droits d'administration et l'autorisation d'ouvrir une session interactive sur la machine locale,
 - Uniquement pour le composant backend, il doit avoir accès à l'instance de base de données avec le rôle serveur "sysadmin".
2. Exécutez le fichier *SES_Evolution_Installation_Center.exe*.
3. Cliquez sur **Ajouter un nouveau composant à une installation existante**.
4. Sélectionnez le composant à installer.
5. Dans le cas de l'ajout d'un composant backend, indiquez l'adresse de l'instance de la base de données d'administration et les informations de connexion du compte "super administrateur" sur la base de données. Dans le cas de l'ajout d'une console ou d'un gestionnaire d'agents, indiquez l'adresse du composant backend.
6. Complétez les paramètres. Pour plus d'informations sur les paramètres à remplir, reportez-vous à la section [Réaliser une installation standard](#). Concernant le mot de passe de l'autorité de certification intermédiaire du composant backend ou du gestionnaire d'agents, ce paramètre n'est pas visible lors de la toute première installation puisque l'information est déjà renseignée dans la section **Certificats** de l'installation standard.
7. Appliquez les changements pour terminer la procédure.



7. Mettre à jour SES Evolution

Pour mettre à jour les composants de la solution SES Evolution, procurez-vous un Centre d'installation dans la version souhaitée sur votre espace client [MyStormshield](#), section **Téléchargements** et exécutez-le depuis une des machines hébergeant un composant de la solution. Tous les composants seront automatiquement mis à jour.

Avant la mise à jour, nous vous recommandons d'effectuer une sauvegarde complète de vos machines.

Nous préconisons :

- un instantané (snapshot) complet pour une machine virtuelle,
- une image disque pour une machine physique.

Pour appliquer la mise à jour :

1. Connectez-vous à la machine avec votre compte de domaine.
2. Double-cliquez sur le fichier *SES_Evolution_Installation_Center.exe*.
3. Cliquez sur **Mettre à jour une installation existante**.
4. Indiquez l'adresse de l'instance de la base de données d'administration et les informations de connexion du compte "super administrateur" sur la base de données.
5. Sur la fenêtre suivante, le Centre d'installation détecte automatiquement les composants à mettre à jour. Cliquez sur **Démarrer la mise à jour**.

Si la console d'administration nécessite une mise à jour, le Centre d'installation affiche la liste des utilisateurs connectés à la console et le nom du poste de travail. Un bandeau rouge sur toutes les consoles ouvertes demande aux utilisateurs d'enregistrer leurs modifications et de fermer la console. Lorsque toutes les consoles sont fermées, la mise à jour s'effectue.

6. Si certains utilisateurs ne ferment pas leur console :
 - a. Cliquez sur **Forcer la mise à jour** pour fermer les consoles à distance et continuer la mise à jour. Utilisez cette option uniquement si vous êtes certain qu'aucune modification n'est en cours, par exemple si l'utilisateur de la console est absent.
 - b. Cliquez sur **Annuler la mise à jour** si vous préférez reporter la mise à jour.

Pour mettre à jour les agents, reportez-vous à la section [Mettre à jour les agents](#) du *Guide d'administration*.

7.1 Gérer la mise à jour de SES Evolution depuis des systèmes d'exploitation non compatibles

Si vous disposez de composants backoffice ou d'agents SES Evolution installés sur des systèmes d'exploitation non compatibles avec la solution, Stormshield recommande fortement de mettre à jour tous les serveurs et postes de travail concernés avant la mise à jour de SES Evolution. Pour plus d'informations, reportez-vous à la [Documentation Microsoft](#).

Pour connaître la liste des systèmes d'exploitation supportés par SES Evolution, reportez-vous au document [Cycle de vie produits](#) [Prérequis système pour SES Evolution](#)

7.1.1 Backend

Vous devez impérativement mettre à jour le système d'exploitation du serveur backend SES Evolution vers une version compatible.



Dans le cas contraire, si vous devez absolument déplacer le backend vers un autre serveur ayant un système d'exploitation supporté, il faudra désinstaller et réinstaller tous les composants backoffice SES Evolution : backend, gestionnaire d'agents et console d'administration.

7.1.2 Console d'administration

Si la mise à jour du système d'exploitation n'est pas possible, vous devez désinstaller la console d'administration du système d'exploitation obsolète et la réinstaller sur un système compatible.

7.1.3 Gestionnaires d'agents

Si la mise à jour du système d'exploitation n'est pas possible, suivez la procédure ci-dessous pour effectuer la migration vers un nouveau serveur compatible :

1. Installez un gestionnaire d'agents de remplacement en version 2.5.x sur un système d'exploitation compatible. Pour plus d'informations, reportez-vous à la section [Ajouter une console, un composant backend ou un gestionnaire d'agents](#) du guide d'installation.
2. Dans le menu **Backoffice > Gestionnaires d'agents** de la console d'administration, vérifiez que le nouveau gestionnaire d'agents s'affiche.
3. Dans le menu **Environnement > Agents > Paramètres > Gestionnaires d'agents**, modifiez le **Groupe de gestionnaires d'agents par défaut** pour chaque groupe d'agents ayant un gestionnaire d'agents obsolète. Remplacez-le par le nouveau gestionnaire d'agents installé à l'étape 1 sur un système d'exploitation compatible.
4. **Dans le menu Sécurité > Déploiement**, déployez cette modification sur tous les agents.
5. Dans l'interface d'un agent obsolète, vérifiez qu'il ait bien reçu la **Dernière mise à jour de la politique**.
6. Désinstallez le gestionnaire d'agents du serveur non compatible avec SES Evolution. Pour plus d'informations, reportez-vous à la section [Désinstaller SES Evolution](#) du guide d'installation.
Les agents sont désormais connectés au nouveau gestionnaire d'agents installé sur un système d'exploitation compatible.
7. Répétez ces étapes pour tous les gestionnaires d'agents installés sur un système d'exploitation non compatible.
8. Mettez à jour le backoffice SES Evolution en version 2.6 ou supérieure. Pour plus d'informations, reportez-vous à la section [Mettre à jour SES Evolution](#) du guide d'installation.

7.1.4 Agents

Si vous ne pouvez pas mettre à jour le système d'exploitation de certains agents SES Evolution, suivez les recommandations ci-dessous :

1. Mettez à jour les agents concernés en version 2.5.x la plus élevée afin de bénéficier des correctifs et fonctionnalités les plus récents.
2. Déplacez ces agents vers un ou plusieurs groupes d'agents dédiés dont la version logicielle cible reste en 2.5.x. Pour plus d'informations, reportez-vous à la section [Créer et configurer les groupes d'agents](#) du guide d'administration.

La dernière version 2.5.x continuera d'assurer la protection des postes de travail équipés de systèmes obsolètes avec les politiques de sécurités compatibles.

**! ATTENTION**

Si vous conservez des agents SES Evolution sur des systèmes d'exploitation 32 bits, vous devez impérativement garder un installateur 32 bits dans un emplacement sûr. Sinon, vous ne pourrez plus installer ce type d'agent.

7.2 Résoudre les problèmes

7.2.1 Failed to extract files from patch (0xa0050005)

Situation : Lors d'une mise à jour, le Centre d'installation affiche l'erreur :
Failed to extract files from patch (0xa0050005).

Cause : Le certificat nécessaire à la vérification de l'authenticité de la mise à jour SES Evolution n'est pas présent sur la machine.

Solution : Ajoutez le certificat **VeriSign Universal Root Certification Authority** au magasin de certificats *Autorités de certification racines de confiance* ou *Autorités de certification racines tierce-partie*.

- ou -

Connectez la machine à Internet afin que le certificat soit téléchargé automatiquement.



8. Désinstaller SES Evolution

Pour effectuer une désinstallation complète de SES Evolution, vous devez désinstaller les différents composants SES Evolution dans l'ordre suivant :

1. Agents SES Evolution,
2. Consoles d'administration,
3. Gestionnaires d'agents,
4. Serveurs backend,
5. Bases de données.

Vous devez pour cela disposer des droits d'administration.

8.1 Désinstaller les consoles, gestionnaires d'agents et backends

1. Connectez-vous à la machine hébergeant le composant SES Evolution avec votre compte de domaine.
2. Dans les **Programmes et fonctionnalités** du Panneau de configuration de Windows, sélectionnez le composant souhaité et cliquez sur **Désinstaller**.
3. Dans le désinstalleur SES Evolution qui s'ouvre, saisissez les informations demandées : **Nom du backend** pour la console et le gestionnaire d'agents, et **Instance de base de données** pour le backend.
4. Cliquez sur **Désinstaller**.
5. Lorsque la désinstallation terminée, redémarrez la machine.

8.2 Désinstaller les bases de données

1. Connectez-vous à la machine avec votre compte de domaine.
2. Double-cliquez sur le fichier *SES_Evolution_Installation_Center.exe*.
3. Cliquez sur **Désinstaller les bases de données**.
4. Complétez les informations de connexion à l'instance de base de données et cliquez sur **Se connecter**.
5. Dans l'écran suivant, cliquez sur **Désinstaller les bases de données**.
6. Lorsque la désinstallation est terminée, quittez le Centre d'installation.

Pour des informations sur la désinstallation des agents, reportez-vous à la section [Désinstaller les agents](#) du *Guide d'administration*.



9. Configurer les connexions TLS entre les composants

Les connexions réseau entre les composants de la solution SES Evolution sont protégées par le protocole TLS. Les composants s'appuient sur la configuration du système d'exploitation des serveurs backend et des gestionnaires d'agents pour le paramétrage des connexions réseau utilisant TLS.

Afin d'améliorer la sécurité des connexions utilisant TLS, nous vous recommandons de désactiver les algorithmes de chiffrement les plus faibles.

Vous pouvez choisir entre l'une des deux méthodes suivantes pour effectuer cette opération.

i NOTE

Si d'autres applications installées sur le serveur utilisent également le protocole TLS, elles seront impactées par cette modification.

9.1 Configurer les connexions TLS par stratégie de groupe (GPO)

1. Ouvrez l'éditeur de stratégie de groupe (*gpedit.msc*),
2. Sélectionnez **Configuration ordinateur > Politiques > Modèles d'administration > Réseau > Paramètres de configuration SSL**,
3. Dans le panneau de droite, double-cliquez sur **Ordre des suites de chiffrement SSL**,
4. La fenêtre **Ordre des suites de chiffrement SSL** s'ouvre. Sélectionnez l'option **Activé**,
5. Dans le champ **Suites de chiffrement SSL**, collez la valeur suivante sur une seule ligne et sans espace :
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384
6. Déployez cette configuration sur les serveurs sur lesquels sont installés les backend et gestionnaires d'agents SES Evolution.

9.2 Configurer les connexions TLS par script PowerShell



1. Exécutez le script PowerShell suivant sur les serveurs sur lesquels sont installés les backend et gestionnaires d'agents SES Evolution avec les droits d'administration :

```
$AllowedSuites = `
'TLS_DHE_RSA_WITH_AES_128_GCM_SHA256', `
'TLS_DHE_RSA_WITH_AES_256_GCM_SHA384', `
'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256', `
'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256', `
'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384', `
'TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384', `
'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256', `
'TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256', `
'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384', `
'TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384', `
'TLS_RSA_WITH_AES_128_CBC_SHA256', `
'TLS_RSA_WITH_AES_128_GCM_SHA256', `
'TLS_RSA_WITH_AES_256_CBC_SHA256', `
'TLS_RSA_WITH_AES_256_GCM_SHA384'

Get-TlsCipherSuite | foreach { $_.Name } | where { $AllowedSuites
-notcontains $_ } | Disable-TlsCipherSuite
```

2. Redémarrez les serveurs pour prendre en compte le nouveau paramétrage.



10. Assurer la continuité de service

Pour assurer la continuité de service en cas de panne d'un composant SES Evolution, nous vous recommandons de mettre en place une redondance des composants backoffice.

Nous vous recommandons d'installer :

- Au moins deux gestionnaires d'agents par groupe de gestionnaires, installés sur deux serveurs distincts,
- Au moins deux serveurs backend, installés sur des serveurs distincts,
- Les bases de données d'administration et de logs sur des machines distinctes et dédiées uniquement à cet usage.

Consultez les sections suivantes pour plus d'informations.

Si toutefois, il n'est pas possible de mettre en place une redondance des composants backoffice, nous vous recommandons d'effectuer régulièrement une sauvegarde complète de vos machines et de stocker les sauvegardes en sécurité.

Nous préconisons :

- un instantané (snapshot) complet pour une machine virtuelle,
- une image disque pour une machine physique.

10.1 Recommandations pour les gestionnaires d'agents

10.1.1 Assurer la redondance des gestionnaires d'agents

Chaque agent SES Evolution se connecte à un groupe de gestionnaires d'agents.

Nous vous recommandons d'installer au moins deux gestionnaires d'agents par groupe de gestionnaires pour assurer la continuité de service en cas de défaillance.

Installez chaque gestionnaire sur des serveurs différents, virtuels ou physiques.

Comptez un gestionnaire d'agents pour 25000 agents.

10.1.2 Gérer la défaillance d'un gestionnaire d'agents

Avec redondance

En cas de défaillance, la charge supportée normalement par le serveur défaillant est automatiquement récupérée par l'autre serveur. Le basculement est effectif dès la première connexion des agents à leur groupe de gestionnaires d'agents suivant la panne.

Nous vous recommandons alors d'en installer un autre pour maintenir la redondance.

Pour installer un nouveau gestionnaire d'agents, utilisez le centre d'installation sur la machine souhaitée.

Après l'installation, depuis la console d'administration, vous devez :

- ajouter le nouveau gestionnaire d'agents au groupe concerné,
- déployer l'environnement pour que le nouveau gestionnaire soit connu des agents.

En cas de défaillance de tous les gestionnaires, reportez-vous à la section suivante.



Sans redondance

Si vous n'aviez qu'un seul gestionnaire d'agents dans un groupe, vous devez restaurer la machine à partir d'une sauvegarde (instantané de machine virtuelle ou image disque de machine physique). Ainsi, l'opération est transparente pour les agents, qui se reconnectent alors au même gestionnaire.

Lorsque la machine redémarre, le gestionnaire d'agents se connecte au serveur backend pour récupérer les dernières politiques de sécurité et les applique aux agents.

10.2 Recommandations pour les serveurs backend

10.2.1 Assurer la redondance des serveurs backend

Nous vous recommandons d'installer au moins deux serveurs backend pour assurer la continuité de service en cas de défaillance.

Installez chaque serveur sur des machines différentes, virtuelles ou physiques.

Activez le mécanisme Microsoft Network Load Balancing (cluster NLB) sur chaque machine hébergeant un serveur backend, pour assurer la redondance et la répartition de charge.

Pour plus d'informations sur le mécanisme NLB, reportez-vous à la section [Effectuer une installation standard](#).

10.2.2 Gérer la défaillance d'un serveur backend

Avec redondance

En cas de défaillance d'un serveur backend, nous vous recommandons d'en installer un autre pour maintenir la redondance.

Pour installer un nouveau serveur backend, utilisez le centre d'installation sur la machine souhaitée.

Assurez-vous d'ajouter au préalable la nouvelle machine au cluster NLB et de retirer l'ancienne.

Sans redondance

Si vous n'aviez qu'un seul serveur backend, vous devez restaurer la machine à partir d'une sauvegarde (instantané de machine virtuelle ou image disque de machine physique).

Nous vous recommandons de vérifier l'état du cluster après la restauration de la machine. La machine restaurée doit être visible dans le cluster.

Lorsque la machine redémarre, le serveur backend se connecte aux bases de données d'administration et de logs. Les gestionnaires d'agents et consoles d'administration se connectent normalement au serveur backend.

10.3 Recommandations pour les bases de données

10.3.1 Assurer la redondance des bases de données

Nous vous recommandons de disposer de deux serveurs pour chacune des bases de données d'administration et de logs, et d'activer la fonctionnalité Groupe de disponibilité Always On (AG)



de SQL Server. La fonctionnalité permet d'assurer un basculement automatique ou manuel entre des bases de données en cas d'indisponibilité.

La fonctionnalité Always On n'est pas disponible sur les versions Express de SQL Server.

10.3.2 Gérer la défaillance d'une base de données

Avec redondance

En cas de défaillance d'une base de données lorsque vous utilisez la fonctionnalité Always On, reportez-vous à la documentation de Microsoft SQL Server.

Sans redondance

Si vous n'aviez qu'une seule base de données d'administration ou de logs, vous devez restaurer la machine hébergeant la base à partir d'une sauvegarde (instantané de machine virtuelle ou image disque de machine physique).



11. Compatibilité entre SES Evolution et les autres solutions de sécurité

Le cumul de plusieurs solutions de sécurité peut avoir un impact sur les performances et entraîner des incompatibilités.

Pour fonctionner correctement, les composants de SES Evolution doivent pouvoir accéder aux ressources listées ci-dessous.

Veuillez vous assurer qu'aucune autre solution de sécurité n'empêche l'accès à ces ressources sur les différentes machines sur lesquelles sont installés les composants.

11.1 Agent SES Evolution

Dossiers

%PROGRAMDATA%\Stormshield Endpoint Security Evolution Agent Diagnostic Result\

%PROGRAMDATA%\Stormshield\SES Evolution\Agent

%SYSTEMROOT%\System32\Drivers\SES Evolution

%PROGRAMFILES%\Stormshield\SES Evolution\Agent

Clés de registre

HKEY_CURRENT_USER\Software\Stormshield

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Minimal\EsaGuardSvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Minimal\EsaGuiSrvSvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Minimal\EsaUpdateSvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Network\EsaGuardSvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Network\EsaGuiSrvSvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Network\EsaUpdateSvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaAccountCtrlDrv

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaAnalyzerSvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaAppldSvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaCollectorSvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaCommSvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaCoreDrv

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaDeviceCtrlDrv

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaDiagSrvSvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaExecCtrlDrv



HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaGuardDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaGuardSvc
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaGuiSrvSvc
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaInjectDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaInjectSvc
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaKeylogGuardDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaKrnCtrlDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaLogSvc
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaMemProtectDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaNetworkCtrlDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaPolicySvc
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaProbeDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaRulesEngDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaResponseSvc
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaScriptSvc
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaUpdateDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaUpdateSvc
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaUsbCtrlDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaUsbCtrlSvc
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaWirelessCtrlDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EsaWirelessCtrlSvc
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\Confgurable\System
HKEY_LOCAL_MACHINE\Software\Classes\Software\Stormshield\SES Evolution\Agent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib_V2Providers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Stormshield Endpoint Security Evolution Agent



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\ExcludedApplications
Sous cette clé, les valeurs suivantes sont relatives à l'agent SES Evolution :

- EsAnalyzer.exe
- EsAppld.exe
- EsCollector.exe
- EsComm.exe
- EsDiagSrv.exe
- EsGuard.exe
- EsGui.exe
- EsGuiSrv.exe
- EsInject.exe
- EsInjectWow64Host.exe
- EsLog.exe
- EsNotificationHost.exe
- EsNotify.exe
- EsPolicy.exe
- EsScript.exe
- EsScriptHost.exe
- EsSetup.exe
- EsSetupWorker.exe
- EsUpdate.exe
- EsUpdateHost.exe
- EsUsbCtrl.exe
- EsWirelessCtrl.exe

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug\AutoExclusionList
Voir la listes des valeurs relatives à l'agent SES Evolution ci-dessus.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps
Voir la listes des valeurs relatives à l'agent SES Evolution ci-dessus.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{36fc9e60-c465-11cf-8056-444553540000}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e965-e325-11ce-bfc1-08002be10318}

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment

HKEY_LOCAL_MACHINE\SOFTWARE\Stormshield\SES Evolution

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WlanSvc\Parameters\WlanAPIPermissions

HKEY_USERS\Environment

HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders



11.2 Console

Dossiers

%PROGRAMDATA%\Stormshield\SES Evolution\Console\

%PROGRAMFILES%\Stormshield\SES Evolution\Console\

%APPDATA%\EsConsole\

%TEMP%\EsInstaller\

Clés de registre

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EscConsoleUpdateSvc

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SOFTWARE\Stormshield\SES Evolution\Console

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Stormshield Endpoint Security Evolution Console

11.3 Serveur backend

Dossiers

%PROGRAMDATA%\Stormshield\SES Evolution\Backend\

%PROGRAMFILES%\Stormshield\SES Evolution\Backend\

%SYSTEMROOT%\System32\inet_srv\Config\

%TEMP%\EsInstaller\

Clés de registre

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EsrBackendUpdateSvc

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SOFTWARE\Stormshield\SES Evolution\Backend

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Stormshield Endpoint Security Evolution Backend

11.4 Gestionnaire d'agents

Dossiers

%PROGRAMDATA%\Stormshield\SES Evolution\Server\log

%PROGRAMDATA%\Stormshield\SES Evolution\Server\AgentLogs

%PROGRAMFILES%\Stormshield\SES Evolution\Server\

%SYSTEMROOT%\ServiceProfiles\LocalService\AppData\Local\Temp\Esserver\

%TEMP%\EsInstaller\

Clés de registre



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Endpoint Security Server Performance

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EsrCoreSvc

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EsrServerUpdateSvc

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SOFTWARE\Stormshield\SES Evolution\Server

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Stormshield Endpoint Security Evolution Server



12. Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sur SES Evolution sont disponibles sur le site web [Documentation](#) et dans la [base de connaissances Stormshield](#) [authentification nécessaire].



STORMSHIELD

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2024. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.