GUIDE

STORMSHIELD ENDPOINT SECURITY EVOLUTION

PRÉCONISATIONS SQL SERVER

Version 2.7.1

Dernière mise à jour du document : 30 juin 2025

Référence : ses-fr-préconisations_sql_server-v2.7.1

Table des matières

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

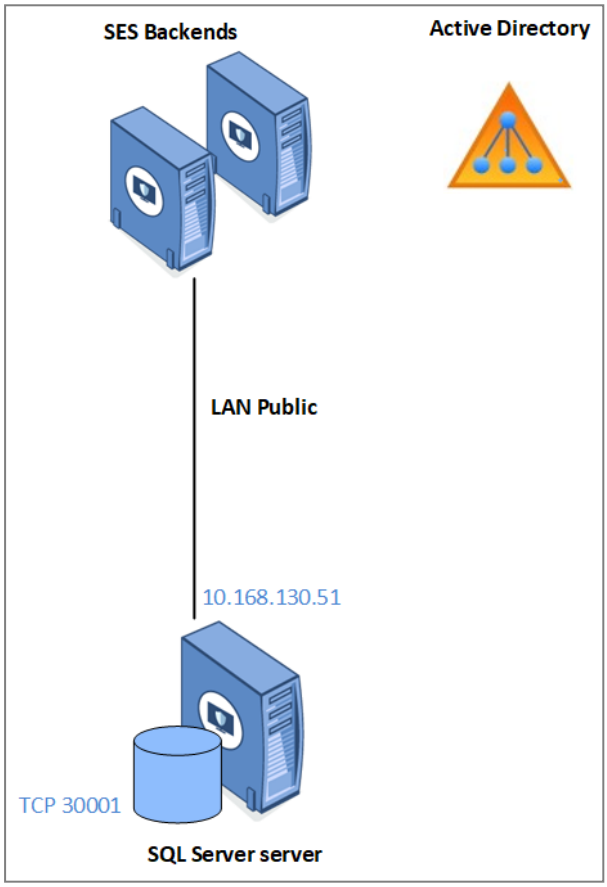
1. Avant de commencer

Bienvenue dans le guide des préconisations SQL Server pour Stormshield Endpoint Security Evolution.

Ce document fournit tous les éléments nécessaires à l'installation, la configuration et la maintenance d'une instance SQL Server utilisée avec Stormshield Endpoint Security Evolution.

2. Prérequis

Les éléments ci-dessous sont nécessaires à la construction de l'architecture finale.



L'adresse IP est un exemple. L'adresse IP réelle est définie par votre propre plan d'adressage.

2.1 Réseau

- L'architecture s'appuie sur Active Directory.
- Le LAN public est réservé à la connexion à la base de données.

IP	192.168.130.x
Masque de sous réseau	255.255.252.0
Passerelle	192.168.128.254
DNS	192.168.130.50

Les ports suivants doivent être ouverts sur les firewalls :

- TCP SQL SERVER : 30001 - Port TCP de communication avec l'instance SQL Server,
- UDP (optionnel) : 1434 - Port d'écoute du SQL Server Browser (pour les connexions *Serveur\Instance*).

Pour plus d'informations, reportez-vous à la section Configurer les serveurs et les instances.

2.2 Comptes Active Directory

- Compte d'installation :
  Le compte utilisé pour l'installation des instances SQL Server doit avoir les droits suivants :
  - CREATE OBJECT sur Active Directory.
  - CONTRÔLE TOTAL sur l'OU cible.
  - ADMIN LOCAL des serveurs SQL Server.
- Compte de service SQL Server :
  Ce compte de service est utilisé pour l'exécution des services SQL Server. Il dispose des autorisations ADMIN LOCAL des serveurs SQL Server. Le mot de passe ne doit pas expirer.

2.3 Serveurs ou machines virtuelles

La gestion de l'alimentation des serveurs doit être configurée en mode **Performances élevées**. Si le serveur est une machine virtuelle HyperV ou VMWare, cette étape s'effectue côté machine physique (host).

Sur Windows, modifiez le mode **Performances élevées** dans le **Panneau de configuration > Système et sécurité > Options d'alimentation**.

2.4 Ressources CPU et RAM

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 *SQL Server Management Studio* après installation des bases de données.

Veuillez consulter les préconisations sur les ressources de CPU et RAM nécessaires dans la section Dimensionner le serveur SES Evolution selon le nombre d'agents du *Guide d'installation SES*.

2.5 Stockage

Les données stockées sur le serveur SQL Server sont réparties comme suit :

Disque	Contenu	Volume attribué
Disque C:	Système d'exploitation	130 Go (fixe)
Disque E:	Données SQL Server	Dépend du nombre d'agents. Voir le *Guide d'installation* .
Disque F:	Journaux SQL Server	50% du disque E:

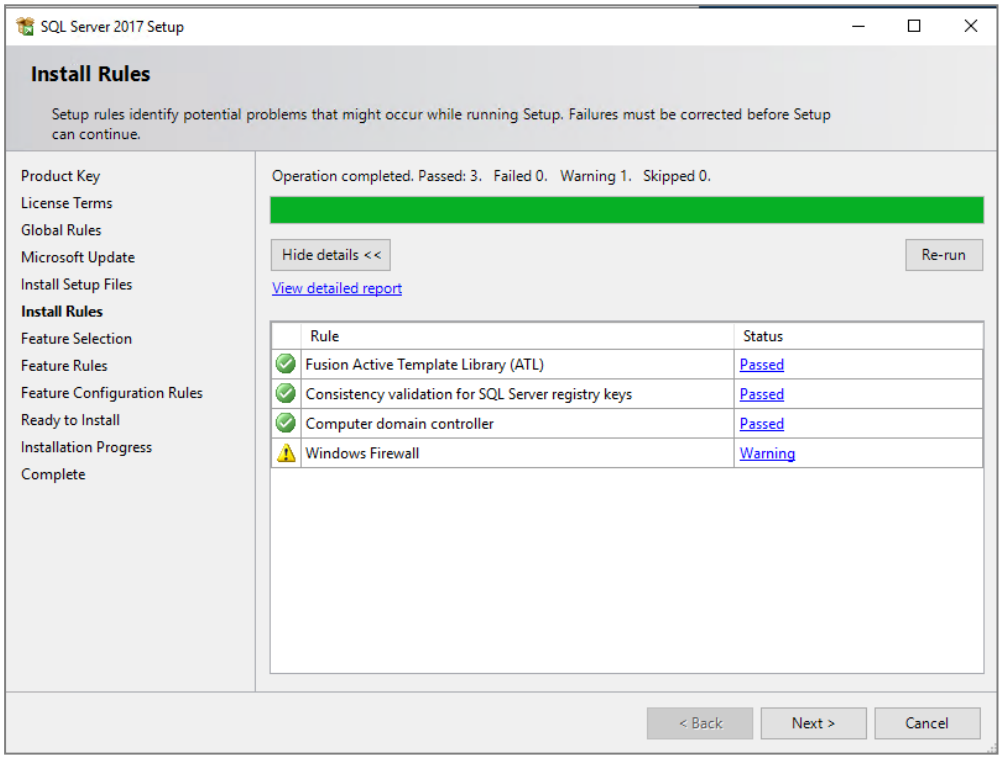
Disque	Contenu	Volume attribué
Disque G:	Sauvegardes SQL Server	Même volume que le disque E:
Disque H:	Données TempDB SQL Server	20% du disque E:

Les volumes dédiés à SQL Server (E:,F:,G: et H:) doivent être exclus des analyses ANTIVIRUS.

3. Installer SQL Server

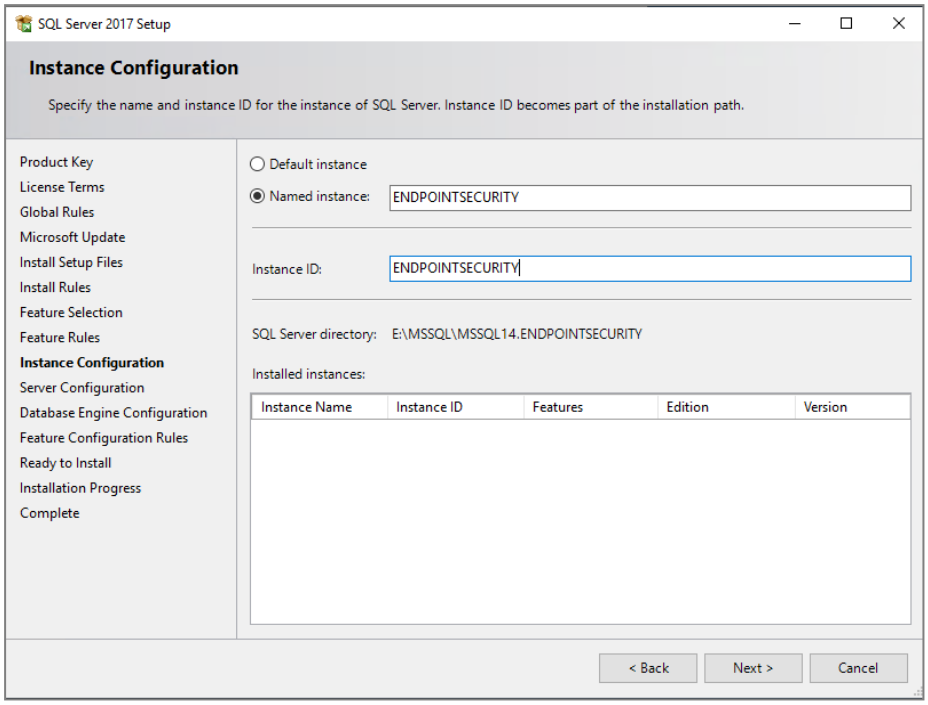
Le serveur SQL Server doit être membre du domaine Active Directory.

1. Lancez le Centre d'installation SQL Server.
2. Choisissez l'option **Nouvelle installation autonome SQL Server**.
3. Saisissez la clé produit, puis acceptez les termes de la licence.
4. Si besoin, téléchargez automatiquement les dernières mises à jour Windows et SQL Server.
5. Après vérification des règles d'installation, vous êtes informé d'un avertissement sur le firewall Windows. Vous devrez le configurer ultérieurement pour autoriser tout le trafic réseau SQL Server. Pour plus d'informations, reportez-vous à la section Ouvrir les ports sur le firewall.

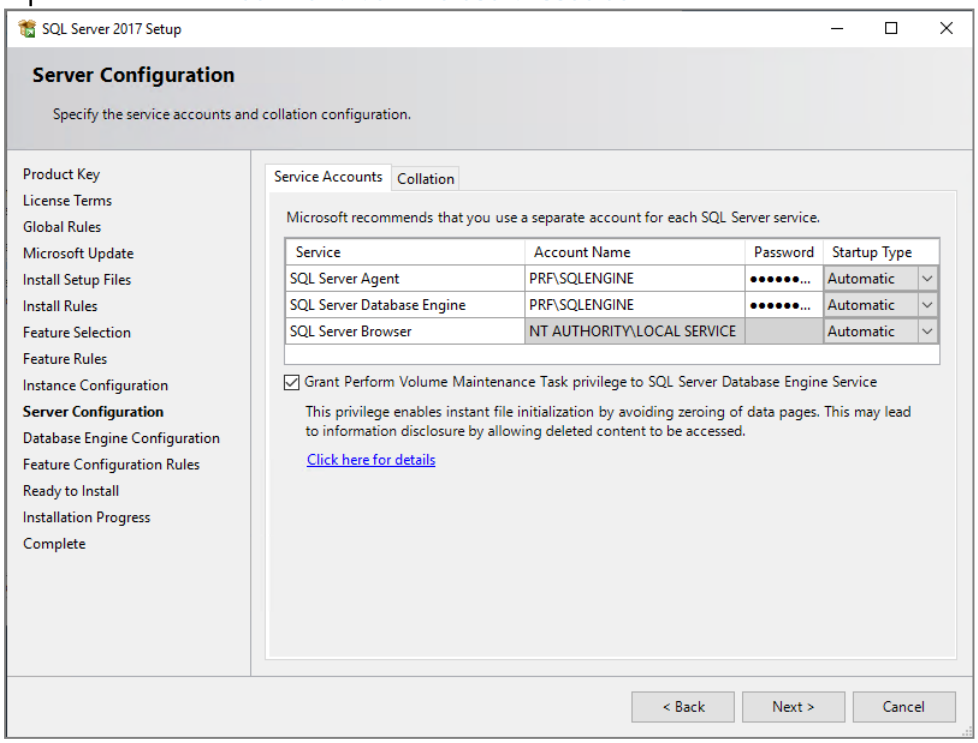


6. Sur l'écran de sélection des fonctionnalités, cochez **Services moteur de base de données**, et dans le champ **Répertoire racine de l'instance**, saisissez E:\MSSQL.

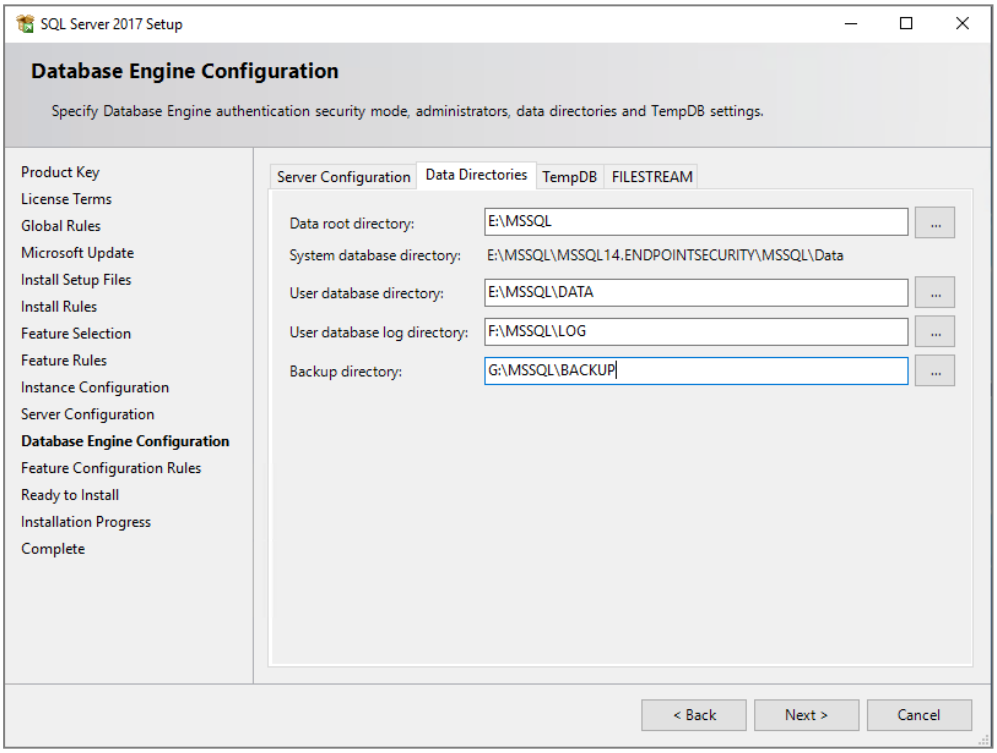
7. Sur l'écran de configuration de l'instance, saisissez les paramètres suivants :
Instance nommée: ENDPOINTSECURITY
ID d'instance : ENDPOINTSECURITY



8. Sur l'écran **Configuration du serveur**, onglet **Comptes de service**, remplissez le nom du compte et le mot de passe pour les services **SQL Server Agent** et **Moteur de base de données SQL Server**. Ici pour simplifier, le même compte est utilisé pour les deux mais vous pouvez les dissocier.
9. Cochez impérativement l'option **Accorder le privilège Effectuer une tâche de maintenance en volume au service Moteur de base de données SQL Server**. Pour plus d'informations, reportez-vous à la documentation Microsoft associée.



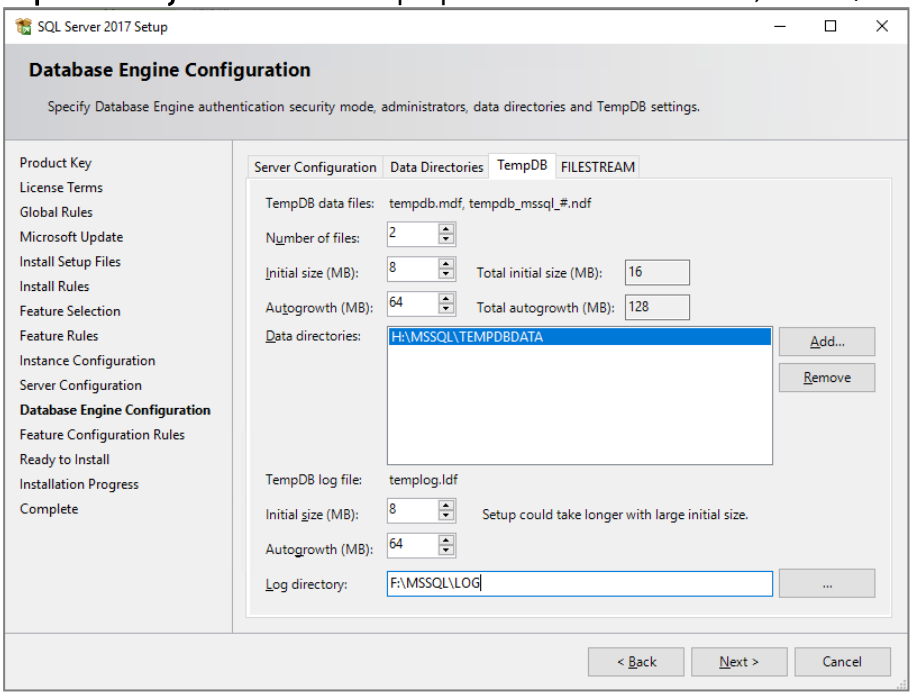
10. Dans l'onglet **Classement**, choisissez *French_CI_AS*. Pour plus d'informations, reportez-vous à la documentation Microsoft associée.
11. Sur l'écran **Configuration du moteur de base de données**, onglet **Configuration du serveur**, choisissez **Mode mixte**, et spécifiez un mot de passe pour le compte *sa*.
Le compte nécessaire à l'installation est automatiquement ajouté à l'instance.
12. Dans l'onglet **Répertoires de données**, répartissez les fichiers de bases de données de la manière suivante :
    - **Répertoire racine de données** : E:\MSSQL
      Binaires et bibliothèques spécifiques à l'instance.
    - **Répertoire de la base de données utilisateur** : E:\MSSQL\DATA
      Fichiers de données (.mdf ou ndf) pour les bases utilisateurs.
    - **Répertoire de journal de la base de données utilisateur** : F:\MSSQL\LOG
      Fichiers journaux (.ldf) pour les bases utilisateurs.
    - **Répertoire de sauvegarde** : G:\MSSQL\BACKUP
      Fichiers de sauvegarde



En matière de stockage, vous devez respecter les recommandations suivantes :

- N'installez pas SQL Server sur le disque C:\ avec le système d'exploitation.
- Ne faites pas cohabiter les fichiers de données et les fichiers journaux sur le même disque.
- Isoler les sauvegardes des autres fichiers.

13. Dans l'onglet **tempDB**, par défaut, la base tempDB est configurée avec un fichier DATA par processeur virtuel. Ne dépassez pas 8 fichiers.
    - **Répertoire de données** : H:\MSSQL\TEMPDBDATA
    - **Répertoire du journal** : Le même que pour les bases utilisateurs, F:\MSSQL\LOG



Pour tempDB, vous devez respecter les recommandations suivantes :

- Pour des raisons de performances et d'administration, isolez les fichiers de données de la tempDB sur un volume dédié.
- Ne faites pas cohabiter les fichiers de données et les fichiers journaux sur le même volume.

14. Dans l'écran **Prêt pour l'installation**, cliquez sur **Installer**. L'installation de l'instance SQL Server s'effectue.

4. Installer SQL Server Management Studio

SQL Server Management Studio (SSMS) est l'utilitaire officiel pour la gestion des instances et des bases de données SQL Server. Il est recommandé de l'installer sur un poste client et de gérer les instances à distance afin de réduire l'impact sur les performances du serveur.

SSMS peut être installé sur le serveur hébergeant l'instance, mais seulement pour une utilisation ponctuelle à des fins de dépannage.

1. Téléchargez la dernière version du programme d'installation.
2. Lancez le programme d'installation.
3. À l'issue de l'installation, redémarrez le poste de travail.
4. Ouvrez SSMS et vérifiez que vous pouvez vous connecter à l'instance en local.

5. Configurer les serveurs et les instances

Effectuez les modifications de configuration avec un compte d'installation qui dispose des droits suivants :

- SysAdmin sur l'instance SQL Server,
- Admin Local du serveur Windows.

5.1 Activer la compression automatique des sauvegardes

- Dans SQL Server Management Studio, exécutez le script TSQL suivant sur les deux instances :

```
exec sp_configure 'backup compression default',1
reconfigure
```

5.2 Activer la connexion administrateur distante

- Dans SQL Server Management Studio, exécutez le script TSQL suivant sur les deux instances :

```
exec sp_configure 'show advanced options',1
reconfigure
exec sp_configure 'remote admin connections',1
reconfigure
```

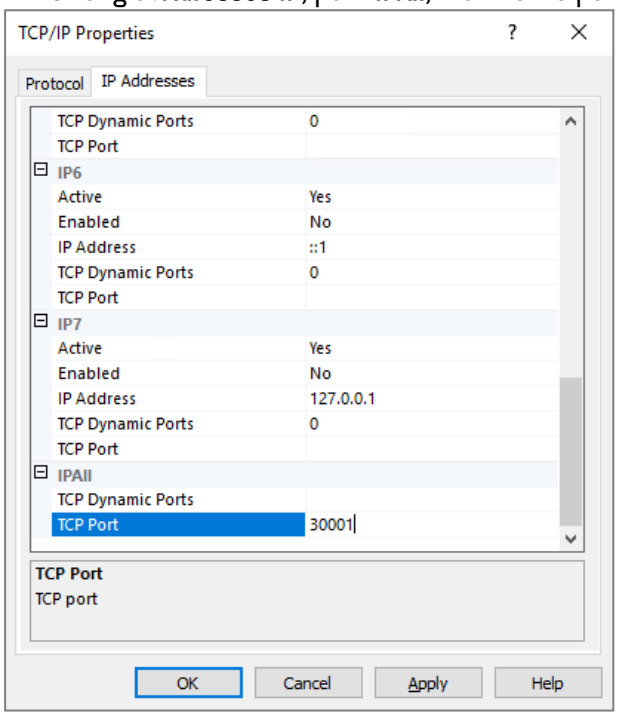
5.3 Autoriser le service SQL Server à verrouiller les pages en mémoire

1. Ouvrez le gestionnaire Windows de Stratégie de sécurité locale.
2. Rendez-vous dans **Stratégies locales > Attribution des droits utilisateur**.
3. Dans le paramètre **Verrouiller les pages en mémoire**, ajoutez le compte de service SQL Server, *PRF\SQLENGINE* dans notre exemple.

5.4 Changer le port d'écoute

Pour des raisons de sécurité, vous devez modifier le port d'écoute de SQL Server sur vos deux instances.

1. Ouvrez l'utilitaire SQL Server Configuration Manager.
2. Rendez-vous dans **Configuration du réseau SQL Server > Protocoles pour ENDPOINTSECURITY**.
3. Faites un clic droit sur **TCP/IP** et choisissez **Propriétés**.
4. Dans l'onglet **Adresses IP**, pour **IPAll**, modifiez le port TCP. Saisissez le port 30001.



5. Sélectionnez **Services SQL Server**.
6. Dans le panneau de droite, faites un clic droit sur SQL Server (ENDPOINTSECURITY) et sélectionnez **Redémarrer**.

5.5 Ouvrir les ports sur le firewall

Sur les nouveaux serveurs Windows, le firewall est activé et les ports TCP sont fermés par défaut. Vous devez ouvrir tous les flux nécessaires à SQL Server sur vos deux instances :

- SQL TCP : TCP 30001 (SQL Engine)
- SQL UDP : UDP 1434 (SQL Browser)
- EndPoint : TCP 5022 (EndPoint Always On)
- LISTENER : TCP 1433 (Listener Always On)

1. Ouvrez l'application Pare-feu Windows Defender avec fonctions avancées de sécurité.
2. Dans **Règles de trafic entrant**, créez une règle de type **Port** avec les paramètres suivants :
   - **Protocole** TCP et **Port** 30001,
   - **Action** : Autoriser la connexion,
   - **Profil** : Domaine, Privé et Public
   - **Nom** : SQL TCP.
3. Créez une deuxième règle de type **Port** pour UDP 1434 avec les mêmes paramètres, et que vous nommerez "SQL UDP".

ASTUCE
Vous pouvez aussi créer les règles à l'aide de Powershell :

```
New-NetFirewallRule -Name "Listener Always On" -DisplayName "Listener
Always On" -Profile Any -Enabled True -Protocol TCP -LocalPort 1433 -
Action Allow

New-NetFirewallRule -Name "Endpoint Always On" -DisplayName "ENDPOINT
ALWAYS ON" -Profile Any -Enabled True -Protocol TCP -LocalPort 5022 -
Action Allow

New-NetFirewallRule -Name "SQL TCP" -DisplayName "SQL TCP" -Profile Any
-Enabled True -Protocol TCP -LocalPort 30001 -Action Allow

New-NetFirewallRule -Name "SQL UDP" -DisplayName "SQL UDP" -Profile Any
-Enabled True -Protocol UDP -LocalPort 1434 -Action Allow
```

5.6 Tester la connexion distante

- Dans SQL Server Management Studio, testez les connexions avec une Authentification Windows, puis une Authentification SQL Server.

6. Assurer la maintenance des bases de données

Pour assurer le maintien en condition opérationnelle de vos bases de données SQL Server, vous devez effectuer les actions suivantes :

- Sauvegarder régulièrement les bases de données,
- Contrôler l'intégrité des bases de données.

Stormshield fournit le script SQL *Stormshield_Database_Maintenance_Procedures.sql*, qui installe des procédures stockées SQL Server pour faciliter la mise en place d'une solution de maintenance pour vos bases de données.

Ces procédures sont utilisables avec toutes les versions de SES Evolution supérieures à 2.5.0.

6.1 Mettre en place le script fourni par Stormshield

1. Sur votre espace client Mystormshield, choisissez le menu **Téléchargements > Stormshield Endpoint Security > Evolution > Tools** et cliquez sur le lien *Stormshield_Database_Maintenance_Procedures.sql* pour le télécharger.
2. Dans SQL Server Management Studio, exécutez le script sur chaque instance SQL Server qui héberge au moins une base de données SES Evolution. Ce script crée les procédures stockées dans la base master.

6.2 Sauvegarder les bases de données

La sauvegarde est la tâche la plus importante dans l'administration d'une base de données. Elle vous permet de récupérer vos données en cas de perte de serveur, configuration, fichiers de données, etc.

Il est recommandé de planifier la sauvegarde automatique de vos bases pour qu'elle soit effectuée régulièrement. Pour plus d'informations sur la mise en place de la planification, reportez-vous à la section Planifier la maintenance via SQL Agent.

Afin de réduire les risques, vous pouvez aussi sauvegarder les bases ponctuellement avant des opérations importantes, notamment :

- Avant la mise à jour de SES Evolution : Si vous ne pouvez pas sauvegarder entièrement la machine physique ou virtuelle, vous pouvez effectuer une sauvegarde des deux bases de données afin de pouvoir réinstaller le produit puis restaurer les bases en cas d'incident grave lors de la mise à jour.
- Après la mise à jour de SES Evolution : Effectuer une sauvegarde juste après la mise à jour du produit permet la restauration en cas d'incident survenant entre la fin de la mise à jour et la sauvegarde planifiée suivante. Cela vous évite d'avoir à réinstaller la version précédente de SES Evolution, puis restaurer la sauvegarde précédente, et enfin de refaire la mise à jour.

Pour sauvegarder les bases de données :

1. Créez les répertoires de destination des sauvegardes des bases de logs et d'administration, par exemple *E:\Backups\EsAdministration* et *E:\Backups\EsLogs*.
2. Assurez-vous que *SQL Server* ait les droits d'écriture dans ces répertoires. Le compte d'exécution de SQL Server est de la forme *MSSQL$ENDPOINTSECURITY* si votre instance se nomme ENDPOINTSECURITY.

3. Dans SQL Server Management Studio, appelez la procédure stockée *Stormshield_BackupDatabase* et fournissez les paramètres suivants, spécifiques à votre environnement :

Paramètre	Description
DatabaseName	Nom de la base de données à sauvegarder. La valeur peut être `EsAdministration` ou `EsLogs`.
BackupDirectory	Chemin absolu du répertoire dans lequel le fichier de sauvegarde est créé. Ce répertoire doit exister. Les chemins réseau sont acceptés, par exemple : *\\storage\backups\EsAdministration*. Le fichier créé est au format *DATABASENAME_YYYY-MM-DD_HH-MM-SS_TYPE.bak*. Par exemple : *EsAdministration_2024-07-14_22-30-42_full.bak* ou *EsLogs_2024-07-14_22-30-42_diff.bak*.
BackupType	Type de sauvegarde à effectuer. La valeur peut être : • `'full'` pour effectuer une sauvegarde complète de la base de données dans le fichier de sauvegarde, • `'diff'` pour effectuer une sauvegarde différentielle. Le fichier de sauvegarde contient uniquement les données qui ont changé depuis la dernière sauvegarde complète. La taille du fichier dépend de l'utilisation de la base. Un fichier de sauvegarde différentielle est généralement beaucoup plus petit qu'un fichier de sauvegarde complète. Les sauvegardes différentielles peuvent être effectuées plus fréquemment puisqu'elles sont plus rapides et génèrent un fichier plus petit. La restauration est cependant plus complexe.
Compress	Active ou désactive la compression lors de la sauvegarde. La compression permet d'obtenir un fichier plus petit au prix d'une consommation CPU légèrement plus élevée. La valeur peut être : • 1 : Compression activée (valeur par défaut et recommandée), • 0 : Compression désactivée.
CheckSum	Active ou désactive la création de sommes de contrôle (checksums) d'intégrité des données. Ces contrôles permettent d'augmenter la résilience des fichiers de sauvegarde face aux corruptions. La valeur peut être : • 1 : Création activée (valeur par défaut et recommandée), • 0 : Création désactivée.
Verify	Active ou désactive la vérification du fichier de sauvegarde une fois que l'opération de sauvegarde est terminée. Si la vérification est activée, SQL Server vérifie le fichier de sauvegarde (e.g., structure, intégrité, checksum si activé). Cette vérification allonge la durée de l'opération mais permet de détecter les erreurs du fichier de sauvegarde au plus tôt. • 1 : Vérification activée (valeur par défaut et recommandée), • 0 : Vérification désactivée.
DryRun	Active ou désactive l'exécution de la procédure en mode test. Lorsque la valeur est 1, la procédure n'exécute pas réellement les commandes et ne fait que les afficher. Cela permet de tester la procédure avant de l'exécuter en situation réelle. • 1 : Mode test activé, • 0 : Mode test désactivé (valeur par défaut).

Paramètre	Description
CopyOnly	Active ou désactive la possibilité de faire une sauvegarde qui ne sera pas enregistrée dans l'historique des sauvegardes de la base. Cela peut être utile pour faire un export de la base. • 1 : Sauvegarde absente de l'historique activée, • 0 : Sauvegarde absente de l'historique désactivée (valeur par défaut).

Exemple de commandes pour effectuer une sauvegarde ponctuelle complète des deux bases :

```
EXECUTE master.dbo.Stormshield_BackupDatabase
@DatabaseName = 'EsAdministration',
@BackupDirectory = 'E:\Backups\EsAdministration',
@BackupType = 'full';
```

```
EXECUTE master.dbo.Stormshield_BackupDatabase
@DatabaseName = 'EsLogs',
@BackupDirectory = 'E:\Backups\EsLogs',
@BackupType = 'full';
```

NOTE
Pour respecter les bonnes pratiques et éviter les potentielles erreurs de suppression, la procédure ne supprime pas les fichiers de sauvegarde existants. Pour faire de la place sur votre support de sauvegarde, mettez en place une politique de suppression des fichiers de sauvegarde obsolètes adaptée à votre besoin de rétention des données.

6.3 Contrôler l'intégrité de la base de données

Effectuez régulièrement le contrôle d'intégrité des bases de données pour détecter d'éventuelles corruptions.

- Dans SQL Server Management Studio, appelez la procédure stockée *Stormshield_CheckDatabases* pour effectuer une vérification des bases de données SES Evolution et optionnellement des bases de données système. Fournissez les paramètres suivants, spécifiques à votre environnement :

Paramètre	Description
FullCheck	Active ou désactive la vérification complète des bases de données. Cette opération est plus longue mais permet de détecter plus d'erreurs qu'une vérification simple. Par exemple, pour une base de données d'environ 200 GB, une vérification complète dure environ 30 minutes contre 10 minutes pour une vérification simple. La durée dépend des capacités de la machine, ainsi que de la charge CPU et disque au moment de la vérification. La valeur peut être : 1 : Vérification complète activée (Valeur par défaut, recommandée pour une fréquence hebdomadaire ou mensuelle). 0 : Vérification complète désactivée (Valeur recommandée pour une fréquence quotidienne).

Paramètre	Description
IncludeSystemDatabases	Inclut ou exclut la vérification des bases de données système de SQL Server. Ces bases de données ne sont pas liées à SES Evolution mais sont indispensables au bon fonctionnement de SQL Server lui-même. • 1 : Vérification des bases de données système activée (valeur par défaut et recommandée), • 0 : Vérification des bases de données système désactivée. Si cette vérification est déjà effectuée par un autre produit ou un autre plan de maintenance sur le même serveur, il est inutile de la refaire.

Exemple de contrôle d'intégrité de la base de données :

Dans SQL Server Management Studio, exécutez la procédure de vérification une seule fois :

- Vérification complète en utilisant les paramètres par défaut :

```
EXECUTE master.dbo.Stormshield_CheckDatabases;
```

- Vérification simple et plus rapide :

```
EXECUTE master.dbo.Stormshield_CheckDatabases @FullCheck = 0;
```

Si la commande échoue, vous devez aviser en fonction des messages d'erreur ou d'avertissement retournés par SQL Server. Dans la plupart des cas, Stormshield recommande de restaurer une sauvegarde de la base de données plutôt que de tenter une réparation des données par SQL Server. En effet, la réparation est susceptible de supprimer des données.

Voici un exemple de messages renvoyés par SQL Server dans un cas de corruption du fichier de données de la base d'administration :

```
[2024-07-14T22:30:45.7482429+02:00] Checking master...
[2024-07-14T22:30:46.0763424+02:00] Checking msdb...
[2024-07-14T22:30:46.5159005+02:00] Checking model...
[2024-07-14T22:30:46.6096237+02:00] Checking EsAdministration...
Msg 8939, Level 16, State 98, Line 3
Table error: Object ID 1483152329, index ID 1, partition ID 72057594055557120, alloc unit ID 72057594066436096 (type In-row data), page (1:7501). Test (IS_OFF (BUF_IOERR, pBUF->bstat)) failed. Values are 133129 and -4.
Msg 8928, Level 16, State 1, Line 3
Object ID 1483152329, index ID 1, partition ID 72057594055557120, alloc unit ID 72057594066436096 (type In-row data): Page (1:7501) could not be processed. See other errors for details.
Msg 8978, Level 16, State 1, Line 3
Table error: Object ID 1483152329, index ID 1, partition ID 72057594055557120, alloc unit ID 72057594066436096 (type In-row data). Page (1:7249) is missing a reference from previous page (1:7501). Possible chain linkage problem.
Msg 8976, Level 16, State 1, Line 3
Table error: Object ID 1483152329, index ID 1, partition ID 72057594055557120, alloc unit ID 72057594066436096 (type In-row data). Page (1:7501) was not seen in the scan although its parent (1:7073) and previous (1:7665) refer to it. Check any previous errors.
CHECKDB found 0 allocation errors and 4 consistency errors in table 'IdentifierVersion' (object ID 1483152329).
CHECKDB found 0 allocation errors and 4 consistency errors in database 'EsAdministration'.
repair_allow_data_loss is the minimum repair level for the errors found by DBCC CHECKDB (EsAdministration).
[2024-07-14T22:30:51.8276754+02:00] Checking EsLogs...
```

6.4 Planifier la maintenance via SQL Agent

Vous pouvez planifier des travaux de sauvegarde et de vérification d'intégrité avec SQL Agent.

Assurez-vous de planifier les opérations de sauvegarde après la fin de la maintenance quotidienne de SES Evolution. Cette dernière est configurable dans la console d'administration de SES Evolution. Pour plus d'informations, reportez-vous à la section Configurer la tâche de maintenance quotidienne du *Guide d'administration*.

6.4.1 Connaître les prérequis

- Vous devez disposer d'une édition de SQL Server Standard ou Enterprise qui inclut SQL Agent.
  Avec SQL Server Express, utilisez le planificateur de tâches Windows ou un planificateur externe car SQL Agent n'est pas disponible.
- Le service Windows *SQL Server Agent* doit être démarré et configuré en démarrage automatique pour que les travaux SQL s'exécutent correctement.

6.4.2 Créer les travaux de maintenance

Vous pouvez créer des travaux de maintenance simples en exécutant dans SQL Server Management Studio la procédure *Stormshield_CreateBasicDailySqlAgentJobs* avec les paramètres suivants adaptés à votre environnement :

Paramètre	Description
EsAdministrationBackupDirectory	Chemin absolu du répertoire dans lequel le fichier de sauvegarde de la base *EsAdministration* est créé.
EsLogsBackupDirectory	Chemin absolu du répertoire dans lequel le fichier de sauvegarde de la base *EsLogs* est créé.
CheckDatabaseStartTime	Heure de démarrage de la vérification d'intégrité, au format HHMMSS. La valeur par défaut est 030000, qui correspond à 3:00 du matin.
BackupDatabasesStartTime	Heure de démarrage des sauvegardes, au format HHMMSS. La valeur par défaut est 050000, qui correspond à 5:00 du matin.

Si les bases de données *EsAdministration* et *EsLogs* sont hébergées sur deux serveurs SQL Server différents, vous devez effectuer l'opération deux fois : une fois sur chaque serveur.

Par exemple, la commande suivante :

```
EXECUTE master.dbo.Stormshield_CreateBasicDailySqlAgentJobs
@EsAdministrationBackupDirectory = 'E:\Backups\EsAdministration',
@EsLogsBackupDirectory = 'E:\Backups\EsLogs',
@CheckDatabaseStartTime = 020000,
@BackupDatabasesStartTime = 040000
```

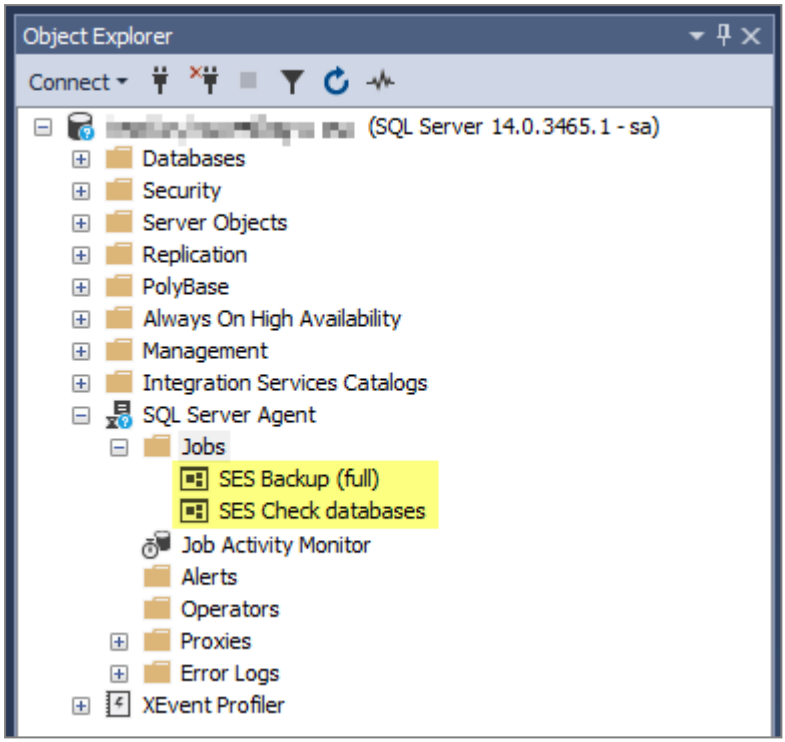
Va créer deux travaux SQL Agent :

- *SES Check databases* : Contrôle l'intégrité des bases système et SES Evolution, tous les dimanches à 2 heures du matin (heure locale du serveur SQL Server),
- *SES Backup (full)* : Effectue une sauvegarde complète des deux bases de données SES Evolution (administration et logs), tous les jours à 4 heures du matin (heure locale du serveur SQL Server).

Si les deux travaux ci-dessus existent déjà, la procédure les écrase avec les nouveaux travaux qui correspondent aux paramètres fournis.

6.4.3 Personnaliser la planification des travaux de maintenance

Dans SQL Server Management Studio, vous pouvez personnaliser les paramètres de planification ainsi que les paramètres des procédures exécutées dans chaque travail. L'image ci-dessous liste les travaux SQL Agent :



Pour personnaliser la planification des travaux de maintenance :

1. Faites un clic droit sur le travail à personnaliser, et sélectionnez **Properties**.
   La fenêtre **Job Properties** s'affiche.
2. Dans la page **Schedules**, sélectionnez le travail, puis cliquez sur **Edit** pour modifier les paramètres de planification à votre convenance.
3. Dans la page **Steps**, sélectionnez le travail, puis cliquez sur **Edit** pour visualiser et modifier les commandes SQL exécutées par le script.

6.5 Restaurer une base de données SES Evolution

En cas de défaillance ou corruption d'une base de données, vous pouvez restaurer une sauvegarde.

6.5.1 Connaître les prérequis

- Le compte Windows utilisé pour l'identité du backend au moment de l'installation de SES Evolution doit être un compte de domaine.
- La sauvegarde à restaurer doit avoir été effectuée sur la même version que la version de SES Evolution en production. Par exemple, restaurer une sauvegarde de base SES Evolution 2.6.1 sur une version 2.6.3 empêchera le démarrage de SES Evolution. D'où l'importance de sauvegarder les bases après chaque mise à jour de SES Evolution. Pour plus d'informations, reportez-vous à la section Sauvegarder ponctuellement les bases de données.
- La console d'administration, les gestionnaires d'agents, et le backend SES Evolution doivent être arrêtés dans cet ordre avant d'effectuer une restauration.

6.5.2 Restaurer une base de données sur le même environnement

- Dans SQL Server Management Studio, utilisez la procédure *Stormshield_RestoreDatabase* avec les paramètres suivants adaptés à votre environnement :

Paramètre	Description
DatabaseName	Nom de la base de données dans laquelle le fichier sera restauré. La valeur peut être *EsAdministration* ou *EsLogs*. **ATTENTION** Toutes les données de cette base seront écrasées par les données provenant du fichier.
BackupFilePath	Chemin absolu du fichier de sauvegarde à restaurer. Ce fichier doit exister pour que la procédure fonctionne correctement. Les chemins réseau sont acceptés, comme par exemple *\\storage\backups\EsAdministration_2024-07-14_22-30-42_full.bak*.
DestinationDataDirectory (optionnel)	Chemin absolu du répertoire dans lequel les fichiers de données SQL Server sont restaurés. Si ce paramètre est utilisé, le répertoire doit exister pour que la procédure fonctionne correctement.
DestinationLogDirectory (optionnel)	Chemin absolu du répertoire dans lequel les fichiers de log de transaction SQL Server sont restaurés. Si le paramètre est utilisé, le répertoire doit exister pour que la procédure fonctionne correctement.

Par exemple, exécutez la commande suivante :

```
EXECUTE master.dbo.Stormshield_RestoreDatabase
@DatabaseName = 'EsAdministration',
@BackupFilePath = 'E:\Backups\EsAdministration\EsAdministration_2024-07-
14_22-30-42_full.bak';
```

6.5.3 Restaurer une base de données sur un autre serveur ou instance

Pour restaurer une base de données SES Evolution sur un autre serveur ou instance SQL Server, l'instance de destination doit être en version supérieure ou égale de SQL Server.

Suivez cette procédure pour chaque base de données en commençant par la base d'administration :

1. Sur l'instance SQL Server cible, exécutez le script *Stormshield_Database_Maintenance_Procedures.sql*.

2. Restaurez la base sur l'instance SQL Server cible :
   - Si l'instance cible est sur une machine différente, exécutez cette commande SQL :
     ```
     EXECUTE master.dbo.Stormshield_RestoreDatabase
     @DatabaseName = 'EsXxx',
     @BackupFilePath = 'E:\Backups\EsXxx\EsXxx_2024-07-14_22-30-42_
     full.bak';
     ```
     où `Xxx` doit être remplacé par `Administration` ou `Logs`.
   - Pour personnaliser les répertoires de destination pour les fichiers SQL, spécifiez-les manuellement dans la commande :
     ```
     EXECUTE master.dbo.Stormshield_RestoreDatabase
     @DatabaseName = 'EsXxx',
     @BackupFilePath = 'C:\backups\EsXxx_2024-07-14_22-30-42_
     full.bak',
     @DestinationDataDirectory = 'F:\Data',
     @DestinationLogDirectory = 'G:\Logs';
     ```
   - Si la machine cible contient plusieurs autres instances, spécifiez explicitement le répertoire de destination afin que les fichiers soient restaurés dans les répertoires correspondant à la bonne instance. Par exemple, pour une instance nommée *DESTINATION* :
     ```
     EXECUTE master.dbo.Stormshield_RestoreDatabase
     @DatabaseName = 'EsXxx',
     @BackupFilePath = 'C:\backups\EsXxx_2024-07-14_22-30-42_
     full.bak',
     @DestinationDataDirectory = 'C:\Program Files\Microsoft SQL
     Server\MSSQL15.DESTINATION\MSSQL\DATA',
     @DestinationLogDirectory = 'C:\Program Files\Microsoft SQL
     Server\MSSQL15.DESTINATION\MSSQL\DATA';
     ```
3. Exécutez la commande suivante sur la base restaurée afin de recréer automatiquement les identifiants nécessaires au fonctionnement de SES Evolution :
   ```
   EXECUTE master.dbo.Stormshield_RestoreLoginUserMappings;
   ```
4. Si vous êtes en train de restaurer la base de logs, mettez à jour la référence à son instance dans la base d'administration SES Evolution que vous avez préalablement restaurée. Pour cela, exécutez la commande suivante sur l'instance qui héberge la base d'administration :
   ```
   EXECUTE master.dbo.Stormshield_ChangeLogsDatabaseInstance
   @NewInstanceName = 'LOGS_SERVER_ADDRESS\LOGS_INSTANCE_NAME';
   ```
   où `LOGS_SERVER_ADDRESS` et `LOGS_INSTANCE_NAME` sont l'adresse et l'instance SQL de la base de logs. Pour les instances par défaut (qui ne sont pas nommées), l'adresse seule sans backslash suffit : `LOGS_SERVER_ADDRESS`.

5. Mettez à jour l'adresse de la nouvelle instance SQL Server dans les fichiers de configuration de SES Evolution :
   1. Sur chaque backend, faites une sauvegarde des fichiers :
      C:\Program Files\Stormshield\SES Evolution\Backend\Api\web.config
      C:\Program Files\Stormshield\SES Evolution\Backend\PublicApi\web.config
   2. Dans chacun de ces fichiers, modifiez les lignes :
      `<add name="Administration" connectionString="Data Source=`**`ADM_SERVER_ADDRESS\ADM_INSTANCE_NAME;`**`Initial Catalog=EsAdministration;..." ... />`
      `<add name="Logs" connectionString="Data Source=`**`LOGS_SERVER_ADDRESS\LOGS_INSTANCE_NAME;`**`Initial Catalog=EsLogs;..." ... />`
      afin que les valeurs `ADM_SERVER_ADDRESS`, `ADM_INSTANCE_NAME`, `LOGS_SERVER_ADDRESS`, et `LOGS_INSTANCE_NAME` correspondent aux adresses et instances SQL des bases d'administration et de logs.
      Pour les instances par défaut (qui ne sont pas nommées), l'adresse seule sans backslash suffit : `ADM_SERVER_ADDRESS` et `LOGS_SERVER_ADDRESS`.

6.6 Déplacer les bases de données SES Evolution

Vous pouvez déplacer les bases de données SES Evolution vers un autre serveur SQL ou une autre instance SQL Server. Cela permet par exemple de migrer les bases d'une édition de SQL Server vers une autre édition sans risquer une mise à jour sur l'instance en production.

6.6.1 Connaître les prérequis

- Le compte Windows utilisé pour l'identité du backend au moment de l'installation de SES Evolution doit être un compte de domaine.
- Vous devez arrêter la console d'administration, les gestionnaires d'agents, et le backend SES Evolution dans cet ordre avant de déplacer une base de données. Pendant l'opération, la console d'administration n'est pas disponible mais les agents continuent de protéger les postes et stockent les logs générés en local. Ces logs sont envoyés vers la base de données et/ou à Syslog une fois la procédure terminée, lorsque les agents se reconnectent.

6.6.2 Déplacer les bases de données sur un autre serveur ou instance

Si vous déplacez les deux bases, vous devez d'abord déplacer *EsAdministration* puis *EsLogs*.

1. Fermez toutes les consoles d'administration pour vous assurer qu'il n'y ait plus de données en cours de modification.
2. Sur chaque machine où un gestionnaire d'agents est installé, arrêtez le service Windows "Stormshield Endpoint Security Server" :
   - Soit via les services Windows,
   - Soit via la commande `net stop EsrCoreSvc`.
3. Sur chaque machine où un backend est installé, arrêtez le serveur IIS :
   - Soit via le "Internet Information Services (IIS) Manager",
   - Soit via la commande `iisreset /stop`.

4. Pour chaque base de données à déplacer :
   a. Assurez-vous que le script *Stormshield_Database_Maintenance_Procedures.sql* ait été exécuté sur l'instance source.
   b. Effectuez une sauvegarde complète de la base à déplacer :
   ```
   EXECUTE master.dbo.Stormshield_BackupDatabase
   @DatabaseName = 'EsXxx',
   @BackupDirectory = 'E:\Backups\EsXxx',
   @BackupType = 'full',
   @CopyOnly = 1;
   ```
   où Xxx est soit *Administration* soit *Logs*.
   c. Effectuez la procédure Restaurer une base de données sur un autre serveur ou instance.
5. Sur chaque machine où un backend est installé, redémarrez le serveur IIS :
   - Soit via le "Internet Information Services (IIS) Manager"
   - Soit via la commande `iisreset /start`.
6. Sur chaque machine où un gestionnaire d'agents est installé, redémarrez le service Windows "Stormshield Endpoint Security Server" :
   - Soit via les services Windows,
   - Soit via la commande `net start EsrCoreSvc`.
7. Supprimez les bases de données source une fois que vous avez confirmé que SES Evolution est opérationnel.

En cas d'échec de la procédure, revenez à l'état initial :

1. Restaurez les fichiers *web.config* que vous avez sauvegardés dans la procédure de restauration.
2. Redémarrez les backends et les gestionnaires d'agents.

6.7 Recréer la base de données de logs

Si vous n'avez pas sauvegardé la base de données de logs SES Evolution et qu'un incident grave se produit sur le serveur hébergeant cette base, les backends SES Evolution ne démarrent plus car aucune base de logs n'est joignable.

Vous devez donc recréer la base de logs *EsLogs*. Pour cela, vous devez disposer d'un Centre d'installation SES Evolution *EsInstaller.exe* de la même version que votre installation courante.

> **NOTE**
> Si vous ne sauvegardez pas la base *EsAdministration* et que cette base est perdue, seule une réinstallation du produit permet de la recréer.

6.7.1 Mettre en place une instance cible temporaire pour la création des bases

La création de la base de logs doit se faire sur une instance SQL Server existante.

Les bases *EsAdministration* et *EsLogs* étaient hébergées dans la même instance SQL Server :

- Si la base *EsAdministration* est encore opérationnelle :
  1. Utilisez ou créez une instance SQL Server temporaire afin de créer une nouvelle base *EsLogs*.
  2. Restaurez cette base sur l'instance cible.

- Si la base *EsAdministration* n'est plus opérationnelle :
  1. Restaurez la base *EsAdministration*.
  2. Utilisez ou créez une instance SQL Server temporaire afin de créer une nouvelle base *EsLogs*.
  3. Restaurez cette base sur l'instance cible.

Si la base *EsLogs* était hébergée dans une instance SQL Server séparée

1. Mettez en place un nouveau serveur et une nouvelle instance SQL Server en utilisant le même nom de machine, la même adresse IP, le même nom DNS que l'instance qui hébergeait la base *EsLogs* perdue.

6.7.2 Créer une nouvelle base de logs

La création d'une nouvelle base *EsLogs* doit être effectuée avec un Centre d'installation SES Evolution *EsInstaller.exe* de la même version que votre installation courante.

Cette base est créée sur l'instance "destination" qui est soit une instance temporaire, soit directement l'instance cible définitive.

1. Lancez le Centre d'installation SES Evolution.
2. Choisissez d'effectuer une nouvelle installation.
3. Décochez le maximum de composants afin qu'il ne reste que les composants obligatoires.
4. Paramétrez l'installation :
   a. Pour la base d'administration et de logs, choisissez l'instance "destination" comme instance cible.
   b. Configurez tous les autres paramètres de la même manière que pour l'installation d'origine. Les mots de passe saisis dans la section **Certificats** ne sont pas utiles.
5. Lancez l'installation.
6. Exécutez le script *Stormshield_Database_Maintenance_Procedures.sql* sur l'instance "destination".
7. Exécutez la commande suivante sur l'instance "destination" pour supprimer la base de données *EsAdministration* qui vient d'être créée par l'installation :
   ```
   EXECUTE master.dbo.Stormshield_DropDatabase @DatabaseName =
   'EsAdministration';
   ```

   ATTENTION
   Veillez à ne pas supprimer la vraie base *EsAdministration*.
8. Exécutez la commande suivante sur l'instance "destination" afin de créer les accès pour le compte Windows utilisé par les backends :
   ```
   EXECUTE master.dbo.Stormshield_CreateBackendAccess
   @BackendAccountName = 'DOMAIN_NAME\BACKEND_USER_NAME'
   ```
   où DOMAIN_NAME\BACKEND_USER_NAME correspond au compte de domaine Windows qui a été renseigné lors de l'installation des backends SES.
9. Si l'instance "destination" est une instance temporaire, déplacez la nouvelle base *EsLogs* qui vient d'être créée vers l'instance cible définitive en effectuant la procédure Déplacer les bases de données SES Evolution.

6.8 Réduire la taille de la base de données

Par défaut, SES Evolution supprime les logs lorsqu'ils ont plus de 12 mois, ou 2 mois pour SQL Server Express. Ce paramètre est configurable dans le panneau **Système**, comme indiqué dans la section Gérer la suppression des logs du *Guide d'administration* SES Evolution. Néanmoins, SQL Server ne libère pas l'espace disque alloué et le conserve pour le réutiliser plus tard.

Si vous estimez que votre base de données SQL Server prend trop de place sur le disque, vous pouvez manuellement procéder à une réduction de celle-ci. Cette opération n'est pas indispensable au bon fonctionnement de la base de données.

Deux niveaux de réduction sont possibles :

- Le niveau 1 est rapide et n'a pas d'effet indésirable sur le fonctionnement de SES Evolution, mais la réduction de la base de données n'est pas maximale.
- Le niveau 2 est beaucoup plus long car il dépend de la taille de la base de données. Il peut entraîner une indisponibilité de SES Evolution.

6.8.1 Niveau 1

- Exécutez le script suivant :

```
DBCC SHRINKDATABASE (EsAdministration, 10, TRUNCATEONLY);
GO
DBCC SHRINKDATABASE (EsLogs, 10, TRUNCATEONLY);
GO
```

6.8.2 Niveau 2

Cette procédure peut conduire à une indisponibilité temporaire de SES Evolution et avoir un impact sur ses performances futures. Elle n'est donc pas recommandée. Si vous souhaitez l'exécuter malgré tout, faites-le sur une période de faible charge.

1. Arrêtez tous les gestionnaires d'agents.
2. Exécutez le script suivant :

```
USE EsLogs;
GO
DBCC SHRINKFILE (N'EsLogs_Events');
GO
DBCC SHRINKFILE (N'EsLogs');
GO
CHECKPOINT;
GO
DBCC SHRINKDATABASE (EsLogs, 5, TRUNCATEONLY);
GO
```

3. Redémarrez les gestionnaires d'agents.

7. 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).

documentation@stormshield.eu