GUIDE

STORMSHIELD ENDPOINT SECURITY EVOLUTION

PRÉCONISATIONS SQL SERVER

Version 2.4.1

Dernière mise à jour du document : 25 mai 2023

Référence : ses-fr-préconisations_sql_server-v2.4.1

Table des matières

1. Avant de commencer 3
2. Pré-requis 3
2.1 Réseau 3
2.2 Comptes Active Directory 4
2.3 Serveurs ou machines virtuelles 4
2.4 Ressources CPU et RAM 4
2.5 Stockage 4
3. Installer SQL Server 6
4. Installer SQL Server Management Studio 10
5. Configurer les serveurs et les instances 10
5.1 Activer la compression automatique des sauvegardes 10
5.2 Activer la connexion administrateur distante 10
5.3 Autoriser le service SQL Server à verrouiller les pages en mémoire 10
5.4 Changer le port d'écoute 11
5.5 Ouvrir les ports sur le firewall 11
5.6 Tester la connexion distante 12
6. Assurer la maintenance des bases de données 13
6.1 Sauvegarder les bases de données 14
6.2 Contrôler l'intégrité de la base de données 14
6.3 Nettoyer la table CommandLog 15
6.4 Réduire la taille de la base de données 15
6.4.1 Niveau 1 15
6.4.2 Niveau 2 15
7. Pour aller plus loin 16

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

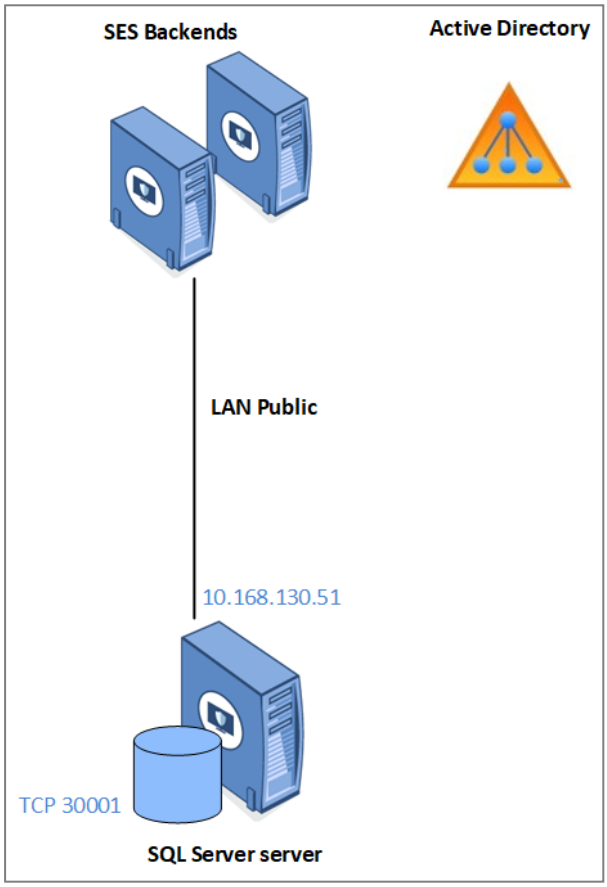
1. Avant de commencer

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. Pré-requis

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 (e.g., 150 000 agent = 500 Go)
Disque F:	Journaux SQL Server	50% du disque E:

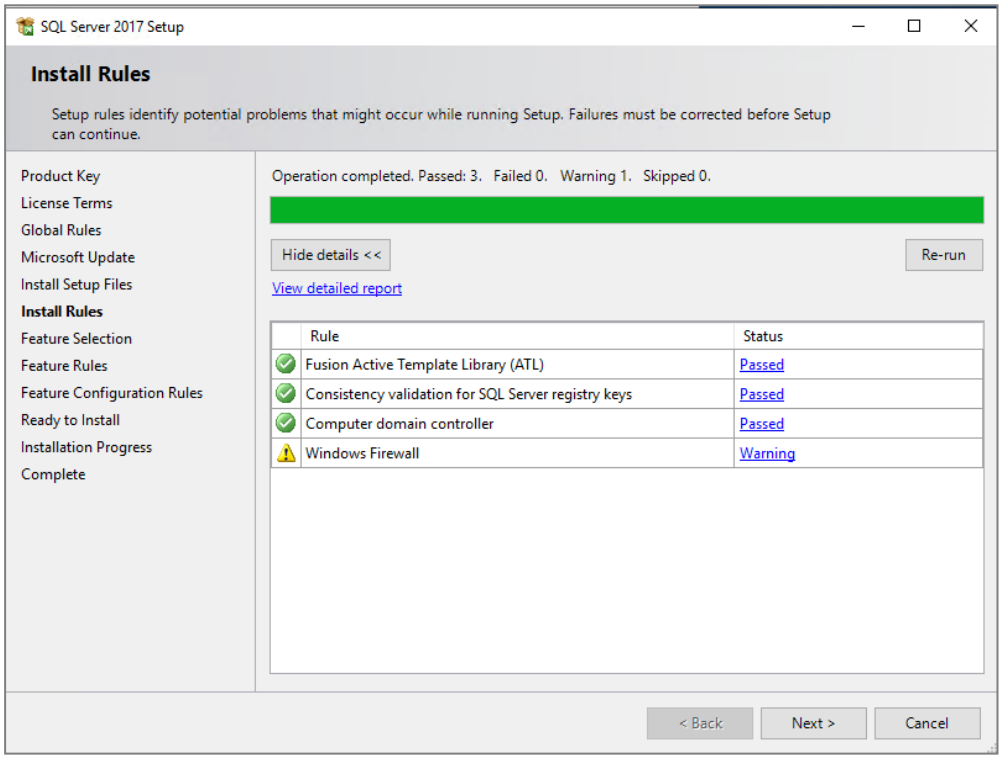
Disque	Contenu	Volume attribué
Disque G:	Sauvegardes SQL Server	Même volume que le disque E:
Disque H:	Données TempDB SQL Server	20% du disque E:

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

3. Installer SQL Server

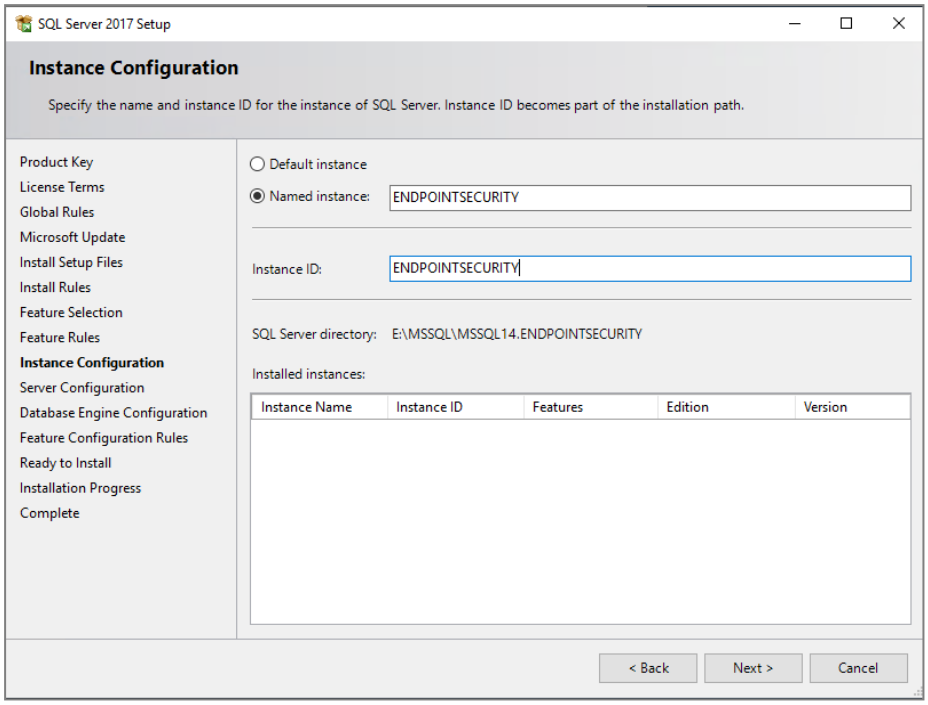
Le serveur SQL Server doit être membre du domaine Active Directory.

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.

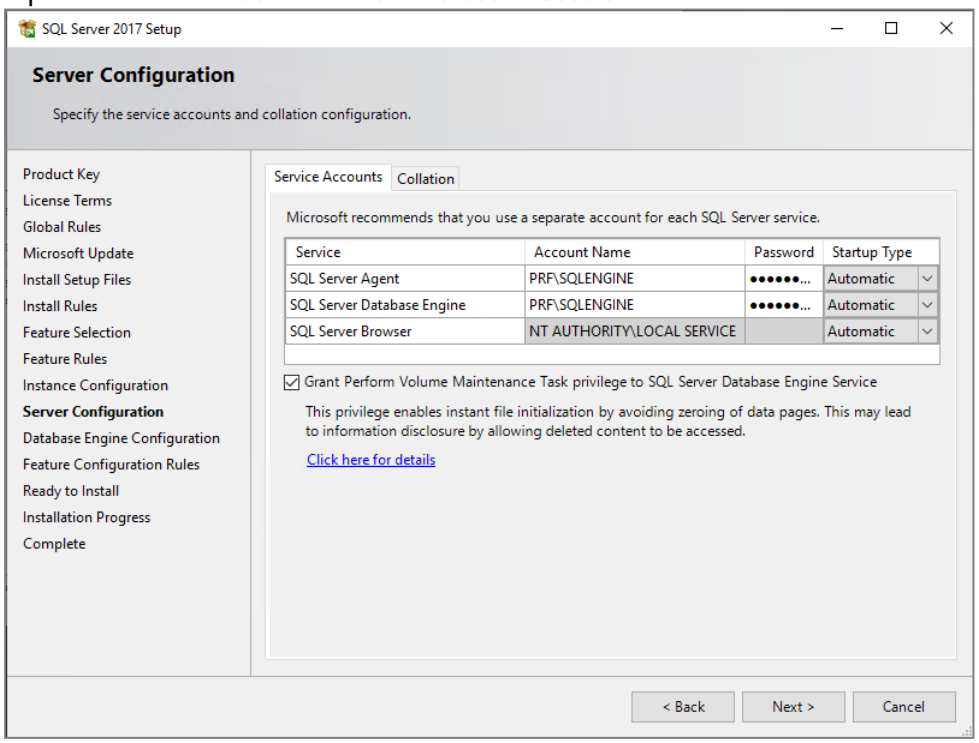


6. Sur l'écran de sélection des fonctionnalités, cochez **Services moteur de base de données**, et dans le champ **Répertoire racine de l'instance**, saisissez E:\MSSQL.

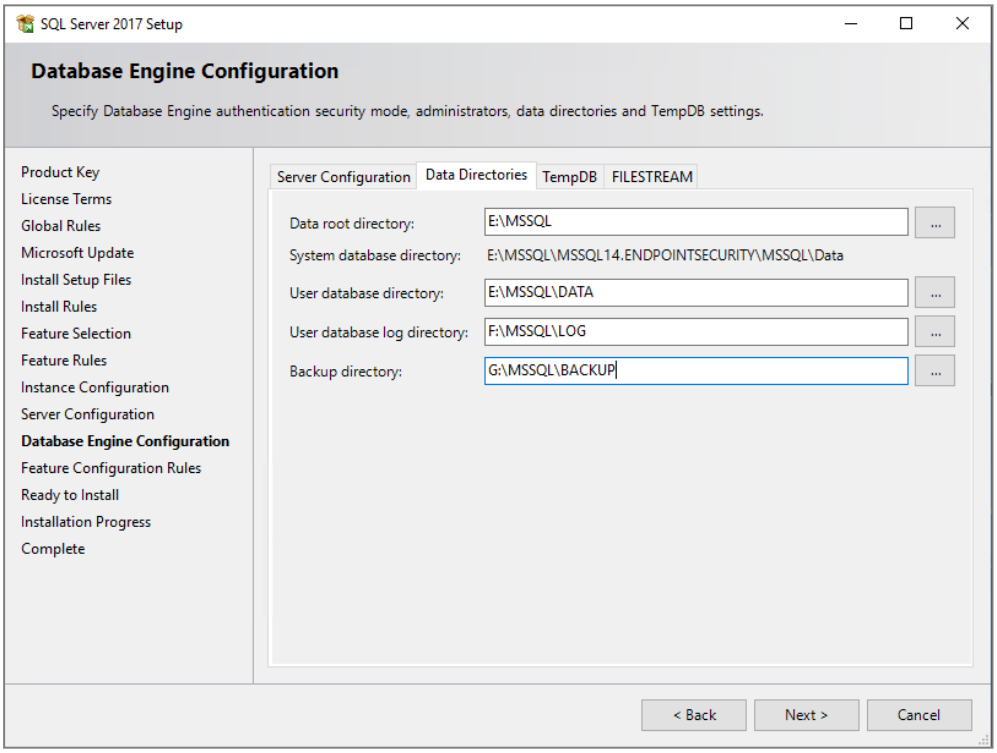
7. Sur l'écran de configuration de l'instance, saisissez les paramètres suivants :
Instance nommée: ENDPOINTSECURITY
ID d'instance : ENDPOINTSECURITY



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.



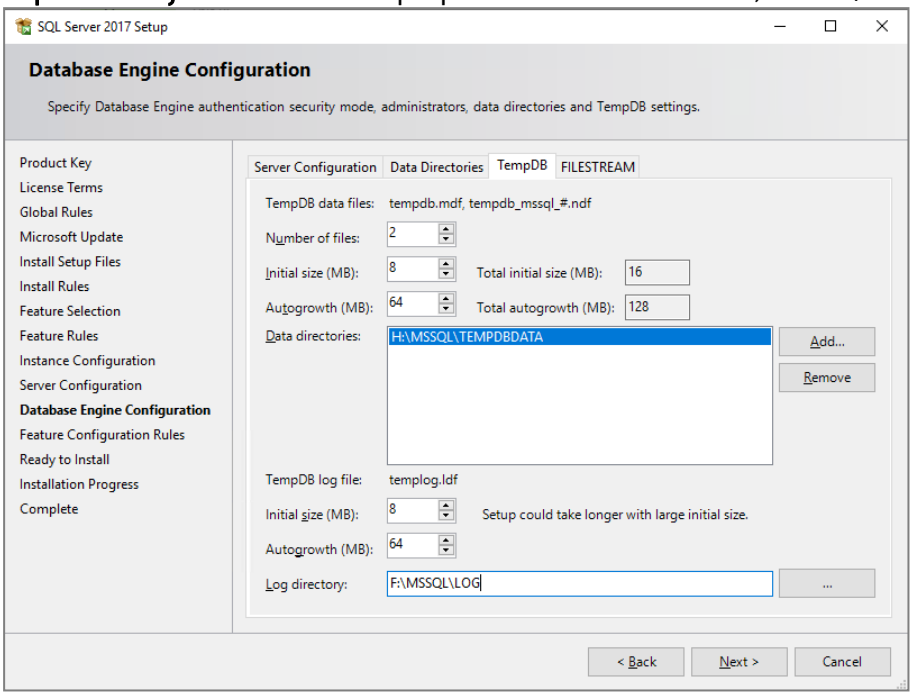
10. Dans l'onglet **Classement**, choisissez *French_CI_AS*. Pour plus d'informations, reportez-vous à la documentation Microsoft associée.
11. Sur l'écran **Configuration du moteur de base de données**, onglet **Configuration du serveur**, choisissez **Mode mixte**, et spécifiez un mot de passe pour 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
```

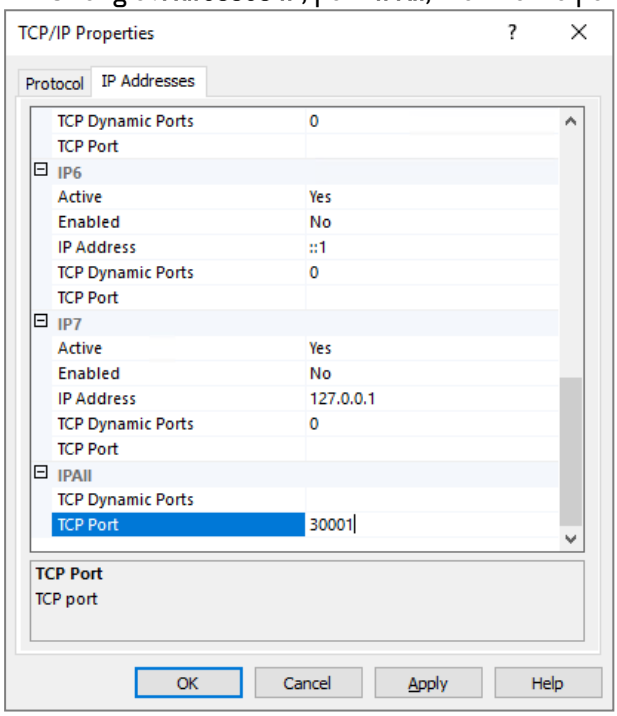
5.3 Autoriser le service SQL Server à verrouiller les pages en mémoire

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.

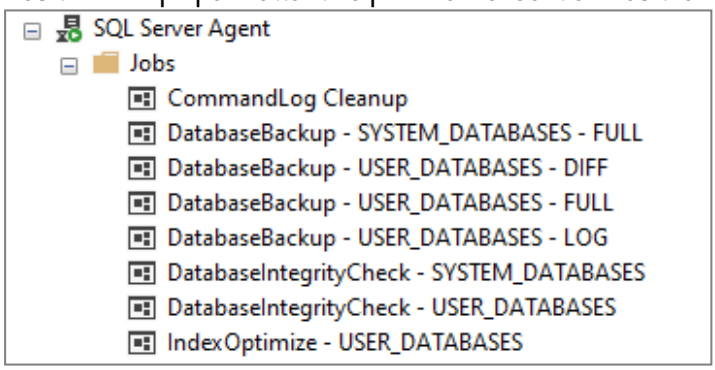
6. Assurer la maintenance des bases de données

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

- Sauvegarde périodique des bases,
- Contrôle d'intégrité.

Avec SES Evolution, il est préférable d'effectuer les travaux de maintenance à l'aide de scripts et procédures stockées SQL Server. Vous pouvez utiliser le jeu de scripts gratuit fourni par Ola Hallengren qui permet la mise en place d'une solution de maintenance complète. Le script *MaintenanceSolution.sql* installe les éléments suivants :

- Plusieurs procédures stockées :
  - *DatabaseBackup* : Sauvegarde de SQL Server
  - *DatabaseIntegrityCheck* : Contrôle d'intégrité SQL Server
  - *IndexOptimize* : Maintenance des statistiques et index SQL Server. Cet élément ne sera pas utilisé car cette étape est prise en charge par SES Evolution. Pour plus d'informations, reportez-vous au Guide d'administration.
- Une table *CommandLog* contenant les logs des opérations réalisées.
- Des travaux qui permettent de planifier l'exécution des tâches.



NOTE
Avec SQLServer Express, utilisez le planificateur de tâche Windows ou un planificateur externe car SQLAgent n'est pas disponible.

6.1 Sauvegarder les bases de données

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

Utilisez le script *DatabaseBackup* pour effectuer les sauvegardes suivantes :

- Une sauvegarde complète des bases de données SYSTEM_DATABASES à planifier **une fois par jour**.

```
EXECUTE [dbo].[DatabaseBackup]
@Databases = 'SYSTEM_DATABASES',
@Directory = NULL,
@BackupType = 'FULL',
@Verify = 'Y',
@CleanupTime = NULL,
@CheckSum = 'Y',
@LogToTable = 'Y'
```

- Une sauvegarde complète des bases de données USER_DATABASES à planifier **une fois par jour**.

```
EXECUTE [dbo].[DatabaseBackup]
@Databases = 'USER_DATABASES',
@Directory = NULL,
@BackupType = 'FULL',
@Verify = 'Y',
@CleanupTime = NULL,
@CheckSum = 'Y',
@LogToTable = 'Y'
```

- Une sauvegarde des journaux des bases de données USER_DATABASES à planifier **plusieurs fois par jour à fréquence élevée** : toutes les 15 minutes, 30 minutes ou une heure.

```
EXECUTE [dbo].[DatabaseBackup]
@Databases = 'USER_DATABASES',
@Directory = NULL,
@BackupType = 'LOG',
@Verify = 'Y',
@CleanupTime = NULL,
@CheckSum = 'Y',
@LogToTable = 'Y'
```

6.2 Contrôler l'intégrité de la base de données

Le contrôle d'intégrité doit être effectué régulièrement pour détecter les éventuelles corruptions de la base de données.

Utilisez le script *DatabaseIntegrityCheck* pour effectuer les contrôles d'intégrité suivants :

- Contrôle des bases SYSTEM_DATABASES à planifier une fois par semaine à un horaire différent des autres travaux.

```
EXECUTE [dbo].[DatabaseIntegrityCheck]
@Databases = 'SYSTEM_DATABASES',
@LogToTable = 'Y'
```

- Contrôle des bases USER_DATABASES à planifier une fois par semaine à un horaire différent des autres travaux.

```
EXECUTE [dbo].[DatabaseIntegrityCheck]
@Databases = 'USER_DATABASES',
@LogToTable = 'Y'
```

6.3 Nettoyer la table CommandLog

La table *CommandLog* contenant les logs des opérations réalisées doit être nettoyée quotidiennement.

Utilisez la commande suivante pour supprimer les logs de plus de 30 jours :

```
DELETE FROM master.dbo.CommandLog
WHERE StartTime < DATEADD(day, -30, GETDATE())
```

6.4 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.

6.4.1 Niveau 1

- Exécutez le script suivant :

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

6.4.2 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