HOW TO

STORMSHIELD ENDPOINT SECURITY

RENOUVELER L'AUTORITÉ DE CERTIFICATION RACINE DE SES

Produits concernés : SES

Date : 7 juin 2019

Référence : ses-fr-how_to-renouveler_l_autorité_de_certification_racine

Table des matières

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

Renouveler l'autorité de certification racine de SES

Ce document s'applique aux versions 7.2.26 et supérieures de Stormshield Endpoint Security.

Des certificats numériques permettent d'authentifier les serveurs, consoles et agents d'un parc SES lors de leurs communications. Les certificats spécifiques de chaque composant sont tous issus de la même autorité de certification racine de confiance.

Le certificat de l'autorité racine a une durée de vie de 10 ans environ. Passé cette période, le certificat est considéré comme expiré et toute communication entre composants utilisant des certificats issus de cette autorité racine est impossible. Il est donc obligatoire de renouveler l'autorité racine de confiance AVANT l'expiration de son certificat.

Ce document décrit la procédure de renouvellement de ce certificat et les différentes phases à respecter pour garantir une continuité de service de la communication entre composants du parc.

Avant de commencer

La procédure de renouvellement des certificats doit être effectuée en plusieurs phases, espacées de plusieurs mois. Il est important de respecter au mieux les durées conseillées par Stormshield afin d'éviter une surcharge des serveurs ou une perte de connexion des agents.

Trois phases sont à respecter durant cette procédure :

Phase 1 : Préparation	Six mois avant l'expiration (indiquée par la console d'administration lors du déploiement de configuration)	Cette phase vise à préparer les serveurs SES au changement d'autorité racine afin qu'ils préparent les nouveaux certificats pour les agents en lissant cette charge sur six mois. La durée de cette phase permet également de s'assurer qu'un maximum d'agents fréquemment déconnectés pourront récupérer leur nouveau certificat.
Phase 2 : Déploiement de la nouvelle autorité de certification racine	Un mois avant l'expiration (indiquée par la console d'administration lors du déploiement de configuration)	Cette phase correspond au changement effectif d'autorité racine et à l'utilisation des nouveaux certificats par tous les constituants. Elle doit être déclenchée le plus tard possible afin de s'assurer qu'un maximum d'agents ont récupéré leur nouveau certificat.
Phase 3 : Nettoyage des anciens certificats	Quelques mois après le changement de l'autorité racine (étape optionnelle)	Cette phase doit être effectuée lorsque l'ensemble des agents du parc se sont bien reconnectés aux serveur et ont récupéré leur certificat.

Phase 1 - Préparation

Environ six mois avant l'expiration du certificat de l'autorité racine, une nouvelle autorité racine doit être générée afin de commencer l'émission des nouveaux certificats Agent.

Sur le serveur principal SES, vous devez générer la nouvelle autorité racine :

1. Lancez en mode administrateur le fichier SES *gen_root.bat*. Ce fichier est situé dans le dossier principal du serveur SES (par défaut *C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Server*).

2. Déplacez le curseur de la souris afin de générer des nombres aléatoires permettant d'émettre des clés symétriques de manière sécurisée.
   Deux fichiers sont générés dans le dossier principal du serveur :
   - *new_root.pem* (environ 6 Ko)
   - *new_rootcert.pem* (environ 2 Ko)

     Ces deux fichiers constituent la nouvelle autorité racine.
3. Si le parc comporte plusieurs serveurs, copiez ces deux fichiers dans le répertoire principal de chaque serveur.

Les serveurs du parc commencent la génération de nouveaux certificats Agent et leur diffusion lorsque les deux conditions suivantes sont réunies :

- Le serveur dispose des nouveaux certificats racine
- Il reste moins de 182 jours avant l'expiration de la racine (six mois)

La diffusion des nouveaux certificats peut générer un surcroît de charge pour les serveurs. Afin de limiter ce problème, chaque serveur ne génère qu'un nouveau certificat agent à la fois. Si plusieurs agents demandent en même temps une mise à jour de certificat, un seul est servi. Les autres reçoivent une réponse négative et recommencent plus tard.

Après avoir effectué les opérations de la phase 1, le message dans la console indiquant de suivre la procédure de renouvellement des certificats ne s'affiche plus lors du déploiement sur l'environnement.

Phase 2 - Déploiement de la nouvelle autorité de certification racine

Veillez à respecter les préconisations suivantes :

- Cette phase ne doit pas être entreprise plus d'un mois avant l'expiration du certificat de l'autorité racine : si cette opération est effectuée trop tôt, la communication entre agents et serveurs sera interrompue jusqu'à l'entrée dans cette période.
- L'opération de changement de certificats occasionne un surcroît de charge sur les serveurs SES, il est donc conseillé de l'effectuer en dehors des périodes de forte charge des serveurs.
- Cette opération est à effectuer sur tous les serveurs du parc en même temps.

Changer l'autorité racine sur tous les serveurs SES

Pour effectuer le changement d'autorité racine :

1. Lancez en mode administrateur le fichier : *switch_cert.bat*. Ce fichier est situé dans le dossier principal du serveur SES (par défaut *C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Server*).
2. Le fichier de commande demande confirmation. Tapez Yes pour confirmer. Toute autre saisie sera vue comme un abandon de la commande.

Mettre à jour les certificats Console

ATTENTION
Les nouveaux certificats Console doivent être importés pour chaque utilisateur de la console.

Une fois le changement d'autorité racine effectué, le certificat Console doit être généré à partir de la nouvelle autorité.

Pour effectuer cette opération :

1. Lancez en mode administrateur le fichier *gen_console.bat*. Ce fichier est situé dans le dossier principal du serveur SES (par défaut *C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Server*).
2. Suivez la procédure. Un nouveau mot de passe est demandé deux fois. Il est formellement déconseillé d'utiliser des caractères non ASCII dans le mot de passe.
3. Une fois la procédure terminée, récupérez le fichier *new_console.sr12* et transférez-le sur la machine où la console est installée. Si la console est sur le serveur, le transfert est inutile.
4. Ouvrez la console et importez le nouveau certificat dans le menu **Configuration** > **Connexions sécurisées**.
5. Renseignez le mot de passe dans le champ **Passphrase**.

Le déploiement sur l'environnement est alors de nouveau possible.

Mettre à jour la base de données de clés

Cette opération n'est à effectuer que si les fonctionnalités de chiffrement de fichier, chiffrement total du disque ou chiffrement de périphériques amovibles sont utilisées ou ont été utilisées sur le parc.

La base de données de clés utilise l'autorité racine pour chiffrer les données qu'elle contient. Une mise à jour de ce certificat est donc également nécessaire.

1. Récupérez depuis un serveur les deux fichiers *old_root.pem* et *root.pem* situés dans le dossier principal du serveur (par défaut *C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Server*).
2. Lancez l'assistant d'installation DBInstaller depuis un poste sur lequel une console est installée.
3. Choisissez le menu **Maintenance des tables de clés de chiffrement**.
4. Entrez les informations de connexion à l'instance sur laquelle est installée la base de données de clés (srkey).
5. Choisissez l'option **Changer d'autorité de certification**.
6. Placez le fichier *old_root.pem* dans **Ancienne valeur**.
7. Placez le fichier *root.pem* dans **Nouvelle valeur**.

Reconnexion des agents

Les agents ayant précédemment récupéré un certificat issu de la nouvelle autorité basculeront automatiquement sur le nouveau certificat lors de leur prochaine connexion au serveur.

Un surcroît de charge sera observable sur les serveurs car chaque agent va tenter de se connecter une première fois en utilisant son ancien certificat, se faire refuser la connexion puis établir une nouvelle connexion avec le nouveau certificat.

Si un agent ne parvient pas à obtenir son nouveau certificat pendant la phase 1, il récupèrera un nouveau certificat depuis le serveur de certificats SES de la même manière qu'un agent nouvellement installé.

ATTENTION
La récupération de certificat via le serveur de certificats SES est une opération consommatrice de ressources sur les serveurs et seul un certificat peut être généré à la fois. Si de nombreux agents sont dans ce cas, des erreurs de connexion peuvent apparaître car le serveur de certificats refusera les demandes concurrentes de certificat. L'agent retentera régulièrement cette opération jusqu'à récupérer un certificat lui permettant de communiquer avec son serveur.

Après avoir effectué les opérations de la phase 2, le message dans la console indiquant de suivre la procédure de renouvellement des certificats ne s'affiche plus lors du déploiement sur l'environnement.

Phase 3 – Nettoyage des anciens certificats

Cette phase ne doit pas être effectuée tant que certains agents n'ont pas de nouveau certificat. Toute communication entre les serveurs et les agents isolés non mis à jour est définitivement coupée, sans aucune possibilité de revenir en arrière sans opérations manuelles incluant l'arrêt des agents concernés.

Cette phase permet de supprimer les anciens certificats racine des serveurs du parc.

Pour effectuer cette opération :

1. Lancez en mode administrateur le fichier *cleanup_cert.bat*. Ce fichier est situé dans le dossier principal du serveur SES (par défaut *C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Server*).
2. Le fichier de commande demande confirmation. Tapez Yes pour confirmer. Toute autre saisie sera vue comme un abandon de la commande.

Ce nettoyage supprime définitivement toute trace des précédents certificats.

documentation@stormshield.eu