STORMSHIELD

STORMSHIELD ENDPOINT SECURITY

NOTES DE VERSION

Version 7.2

Date : 13 septembre 2018

Référence : ses-fr-notes_de_version-v7.2.23

Table des matières

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

Ce document n'est pas exhaustif et d'autres modifications mineures ont pu être incluses dans cette version.

Nouvelle fonctionnalité de Stormshield Endpoint Security 7.2.23

À partir de la version 7.2.20, SES ne permet plus d'administrer la solution antivirus Avira. Si vous possédez cette option, veuillez consulter la section **Préconisations** avant d'effectuer la mise à jour.

Arrêt de l'agent depuis un poste de travail

Lorsque la configuration dynamique de l'agent l'autorise, l'utilisateur peut désormais arrêter l'agent en cliquant sur le lien **Désactiver** depuis l'interface de l'agent sur son poste de travail. Si la configuration n'autorise pas l'arrêt de l'agent, cliquer sur ce lien ouvre la fenêtre de challenge.

Correctifs de Stormshield Endpoint Security 7.2.23

Correctifs agent

Incompatibilité avec ArcGIS Explorer Desktop

Références support CF88610 - 158672CW

La protection RCP de l'agent SES ne provoque plus un blocage du logiciel ArcGIS Explorer Desktop lors de son démarrage.

Configuration de l'accès temporaire au web rapide depuis l'agent

Références support CF88593 - 158463CW

Dans le cas où l'utilisateur possède un raccourci sur son poste de travail pour demander l'accès temporaire au web, les options «/GrantWebAccess» et «/NoConfirm» à rajouter dans la cible du raccourci de l'exécutable *ssmon.exe* ont été corrigées. La première était devenue sensible à la casse et la seconde provoquait l'effet inverse.

Incompatibilité avec la fonctionnalité "Verrouillage système" de Symantec Endpoint Protection

Références support CF88327 - 154855CW

La cohabitation des agents SES et des agents Symantec Endpoint Protection dont la fonctionnalité "Verrouillage système" est activée (ou "System lockdown") ne provoque plus de message d'erreur interne dans les logs de protection système de SES.

Correctifs console

Déploiement des changements de configuration sur l'environnement

Le libellé du bouton **Appliquer les changements à l'environnement** a été modifié. Le bouton s'appelle désormais **Déployer sur l'environnement**.

Numéro de version de politique et de configuration dans le panneau de surveillance des agents

Références support CF88585 - 158368CW

Dans le panneau de surveillance des agents, les colonnes **Politique** et **Configuration** indiquent désormais les numéros de version en plus des noms.

Mise à jour du panneau de surveillance des agents

Références support CF88260 - 154383CW

Dans le panneau de surveillance des agents, lorsque des nouvelles politiques ou configurations étaient déployées sur l'environnement, la colonne **État de la conf.** pouvait indiquer pendant un certain temps un état "valide" alors que les nouvelles politiques ou configurations appliquées n'étaient pas encore visibles dans les colonnes **Politique** et **Configuration**. Désormais ce délai est réduit à 30 secondes. Dès lors que l'état redevient valide, les noms et numéros de politiques et configurations sont donc mis à jour dans la console au bout de 30 secondes.

Suppression de la fonctionnalité d'apprentissage

La fonctionnalité d'apprentissage dans la politique de configuration dynamique de l'agent a été supprimée. De ce fait, la partie **Contrôle du comportement des applications** dans la politique de sécurité a été modifiée. La protection **Accès au registre** a été supprimée, et les protections **Accès aux fichiers** et **Contrôle des exécutions** n'ont plus que deux réglages possibles : activées et désactivées.

Format du hash d'identifiant d'applications

Lors de la création d'un identifiant d'applications par hash, celui-ci peut contenir des espaces ou des tirets. Ils sont supprimés lors de la validation de l'identifiant.

Adaptation des menus et boutons selon le rôle de l'utilisateur

Les boutons de modification de politique ainsi que le menu **Ajouter un annuaire interne** ne sont désormais plus disponibles pour un utilisateur n'ayant pas le droit de réaliser ces actions.

Rapports de la console

Les rapports **Temps réel** sont désormais cohérents avec les valeurs indiquées dans le panneau **Surveillance** > **Agents**.

Libellés de colonnes permutés dans la politique de sécurité

Les libellés des colonnes **Accès à cette application** et **Accès aux applications** dans la politique de sécurité, onglet **Contrôle applicatif**, menu **Applications de confiance** avaient été permutés. Cette erreur est corrigée.

Versions de Windows compatibles avec Stormshield Endpoint Security 7.2.23

Stormshield Endpoint Security 7.2.23 est compatible avec les versions de Windows suivantes :

Windows	Professional Edition	Secure Edition	Server-Side Edition
XP SP3 - 32 bits	✓	✓	-
Vista SP2 - 32 bits	✓	✓	-
7 SP1 - 32/64 bits	✓	✓	-
8.1 Update 1 - 32/64 bits	✓	✓	-
Windows 10 Enterprise 2015 LTSB - 32/64 bits	✓	✓	-
Windows 10 Enterprise 2016 LTSB - 32/64 bits	✓	✓	
Windows 10 1703 Creators Update - 32/64 bits	✓	✓	-
Windows 10 1709 Fall Creators Update - 32/64 bits	✓	✓	-
Windows 10 1803 April Update - 32/64 bits	✓	✓	
Server 2003 SP2 - 32 bits	-	-	✓
Server 2003 R2 SP2 - 32 bits	-	-	✓
Server 2008 R2 - 64 bits	-	-	✓
Server 2012 R2 - 64 bits	-	-	✓

Préconisations

Avertissement avant la mise à jour en version 7.2.20 ou version supérieure

A partir de la version 7.2.20 ou supérieure, SES ne permet plus d'administrer l'antivirus **Avira**. Veuillez prendre connaissance ci-dessous des recommandations et des conséquences que ce changement implique :

- Dans la politique Antivirus, assurez-vous de connaître le mot de passe défini dans la section **Paramètres de la protection par mot de passe**.
- Dans la politique Antivirus, assurez-vous d'avoir coché la case **Installer/Désinstaller** dans la fenêtre qui s'ouvre lorsque vous cliquez sur les ... du paramètre **Zones à protéger par mot de passe**.

Conséquences côté serveur

- Les mentions et fonctionnalités de l'antivirus Avira sont supprimées,
- Les fichiers de mise à jour appliqués sur le serveur ne contiennent plus l'antivirus.

Conséquences côté console d'administration

- Si vous avez des politiques Antivirus, elles sont automatiquement supprimées à la mise à jour en 7.2.20, ainsi que les liens dans l'environnement. Vous n'avez aucune action à faire.
- Si vous avez des scripts ou ressources de scripts contenant des éléments relatifs à l'antivirus Avira : vous devez les supprimer manuellement. Tant qu'il restera des éléments le mentionnant, un message s'affichera à l'ouverture de la console.
- Si vous importez des politiques Antivirus, vous obtiendrez un message et un log d'erreur. La politique ne sera pas importée.
- Si vous importez des scripts ou ressources de scripts mentionnant l'antivirus Avira, ils seront importés mais vous obtiendrez des messages d'erreur et vous ne pourrez pas les valider tant que vous n'aurez pas supprimé ces mentions.

Conséquences côté agent

La mise à jour vers la version 7.2.20 ou supérieure ne déclenche pas la suppression de l'antivirus Avira des postes de travail possédant un agent avec option Antivirus. Il est donc possible de :

- Conserver les agents avec l'option Antivirus. Cependant il ne sera plus possible d'administrer Avira depuis la console SES.
- Désinstaller Avira sur les postes de travail. Reportez-vous à la section suivante.

Désinstaller l'antivirus Avira sur un poste de travail (optionnel)

Vous pouvez désinstaller Avira avant ou après la mise à jour de l'agent.

Pour désinstaller Avira, suivez les trois étapes suivantes en exécutant les commandes en tant qu'administrateur directement sur les postes de travail ou sur plusieurs postes à la fois via un outil d'administration de parc informatique.

1. Désinstallez Avira avec la commande suivante :
   ```
   "<répertoire_agent>\av\tmp\presetup.exe" /REMSILENTNOREBOOT /PASSWORD="<mot_de_passe_avira>" /unsetuplog="<chemin_fichier_log>"
   ```
   Avec :

- <répertoire_agent> : chemin vers le répertoire d'installation de l'agent. Par défaut : *C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Agent*,
- <mot_de_passe_avira> : mot de passe d'administration de la console Avira défini dans la politique Antivirus,
- <chemin_fichier_log> : chemin vers un fichier dans lequel seront écrits les logs de désinstallation d'Avira. Exemple : *C:\Tmp\fichier_log.txt*

2. Supprimez le répertoire "av" de l'agent. Exécutez la commande suivante après avoir redémarré les postes de travail sur lesquels Avira a été désinstallé et après la mise à jour complète vers la version 7.2.20 ou supérieure :
```
rd /q /s "<répertoire_agent>\av"
```
3. Désinstallez Avira Launcher (à partir de la version 15.0.19.164 de l'antivirus Avira) :
```
for /f "usebackq tokens=* delims=" %%G IN (`dir /s /B "C:\ProgramData\Package Cache" ^| find "Avira.OE.Setup.Bundle.exe"`) do ("%%G" /uninstall /quiet /log <chemin_fichier_log>)
```
Ce script recherche toutes les instances d'installeur de Avira Launcher et exécute leur désinstallation silencieuse.
Avec :
   - <chemin_fichier_log> : chemin vers un fichier dans lequel seront écrits les logs de désinstallation d'Avira. Exemple : *C:\Tmp\fichier_log.txt*

   Avira Launcher peut également être désinstallé via le **Panneau de configuration** Windows dans les **Programmes et fonctionnalités**.

Problèmes connus

Les problèmes connus sont les suivants :

ID	Incompatibilité	Solution
	Description : Incompatibilité entre BitLocker To Go et la fonctionnalité de contrôle des périphériques amovibles de l'agent.	Vous devez désactiver le paramètre **Gestion des groupes** dans les paramètres généraux du contrôle des périphériques, pour utiliser BitLocker To Go.
	Description : La protection contre le redémarrage forcé n'est pas compatible avec Windows 10 1703.	Le problème est corrigé dans la version 1709 de Windows 10.
	Description : Incompatibilité avec IBM Trusteer Rapport sous Windows 7 64 bits.	Aucune solution pour le moment.
87979 - 152138CW	**Description** : Un écran bleu apparaît quand on utilise SES et Avast Endpoint 8.01609.	Vous devez désactiver le pilote Avast Virtualization driver (aswSnx.sys). **Procédure** : 1. Démarrer le poste de travail en mode sans échec. 2. Désactiver le pilote Avast présent dans *C:\Windows\system32\drivers\aswsnx.sys* en le renommant par exemple *C:\Windows\system32\drivers\aswsnx.sys.old*. 3. Redémarrer le poste de travail et vérifier qu'il ne présente plus d'écran bleu.
87998 - 152269PW	**Description** : Lors de l'installation de Avast Business version 17.2.2517 et de SES, les processus Windows ne démarrent pas. L'erreur suivante apparaît : *L'application n'a pas réussi à démarrer correctement (0xc0000142). Cliquez sur OK pour fermer l'application.*	Aucune solution pour le moment.

ID	Incompatibilité	Solution
1645	**Description** : Impossible de créer un périphérique bootable avec le logiciel HP USB Disk Storage Format Tool. Le message d'erreur suivant apparaît entre la fin du formatage et le début de la copie des fichiers sur le périphérique : "FAILED TO MAKE THE DEVICE DOS-BOOTABLE". **Cause** : Quand un périphérique de stockage amovible est branché sur l'ordinateur, Stormshield Endpoint Security le passe en accès interdit le temps de contrôler si le périphérique est chiffré ou non. Ceci pose problème au logiciel HP qui monte et démonte le périphérique à plusieurs reprises pendant le traitement.	Aucune solution pour le moment. (#FKX-94147-408)
1846	**Description** : Incompatibilité avec le système d'authentification par carte à puce Digital Persona. Impossibilité d'accéder aux fichiers chiffrés par Stormshield Endpoint Security lorsqu'on utilise l'authentification Windows. **Cause** : Si Digital Persona est installé après Stormshield Endpoint Security, celui-ci supprime la GINA dll de Stormshield Endpoint Security et donc le système d'authentification.	Installer Stormshield Endpoint Security après Digital Persona. (#DNX-52479-415)

ID	Incompatibilité	Solution
2137	**Description** : Incompatibilité avec l'outil de chiffrement Sophos SafeGuard Enterprise. Les clés USB apparaissent dans le poste de travail mais leur contenu n'est pas accessible. Les disques durs USB sont accessibles uniquement en lecture seule. **Cause** : Incompatibilité de l'outil avec le contrôle de périphériques. SafeGuard détecte si un autre driver tente de mettre en place un filtre et dans ce cas bloque l'accès aux périphériques.	Modifier la base de registre pour que le driver de Stormshield Endpoint Security `odin-sys.sra` soit chargé avant le driver de SafeGuard Enterprise. **Procédure** : 1. Arrêter l'agent Stormshield Endpoint Security avec `stopagent.exe`. 2. Accéder à la clé de registre `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet \Control\ServiceGroupOrder`. 3. Éditer la valeur `List` et ajouter une ligne **Odin** au dessus de la ligne **Primary Disk** (driver de Safeguard Enterprise). 4. Accéder à la clé de registre `HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services \odin`. 5. Ajouter la valeur `Group` (de type chaîne) et entrer `Odin` dans le champs **Données de valeur**. 6. Redémarrer la machine. (#BSX-16078-335)
5180	**Description** : Incompatibilité avec BitLocker To Go (chiffrement de fichiers Stormshield Endpoint Security). **Cause** : Concurrence sur les opérations réalisées par BitLocker To Go et Stormshield Endpoint Security.	Aucune solution pour le moment. Le chiffrement de fichiers Stormshield Endpoint Security doit être désactivé pour les périphériques amovibles.
	Description : Incompatibilité avec l'application F-Secure sur les systèmes d'exploitation 64 bits. **Cause** : Incompatibilité avec l'auto-protection de Stormshield Endpoint Security.	Désactiver l'option **Utiliser la surveillance avancée des processus** dans les paramètres de DeepGuard de l'application F-Secure.
	Description : Un écran bleu apparaît quand on utilise Stormshield Endpoint Security et une solution embarquant le(s) driver(s) Safenet aksfridge.sys, Aksdf.sys ou encore Hardlock.sys.	La version 6.62 ou supérieure des drivers Safenet (Sentinel HASP/LDK) intègre une correction pour ce problème.
	Description : Impossibilité de bloquer les périphériques USB de type MTP.	Aucune solution pour le moment.
	Description : Impossibilité de bloquer les périphériques de type carte SD et eSata.	Aucune solution pour le moment.

ID	Incompatibilité	Solution
9525	**Description** : Un écran bleu apparaît lorsque FortiClient Endpoint Protection est installé avec Stormshield Endpoint Security.	Modifier la base de registre pour que le driver SES *heimdall-sys.sra* soit chargé après le driver de FortiClient Endpoint Protection. **Procédure** : 1. Démarrer la machine en mode sans échec ou arrêter l'agent SES avec stopagent ou un challenge réponse **Arrêt total de l'agent**. 2. Accéder à la clé de registre `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\heimdall`. 3. Éditer la valeur `Group` et remplacer la valeur actuelle par `FSFilter Content Screener`. 4. Ajouter la valeur `Tag` de type DWORD, puis éditer la valeur afin de remplacer 0 par 1. 5. Redémarrer la machine. Effets de bord : la protection des périphériques (Bluetooth, Com, USB, etc.) n'est plus fonctionnelle et ne doit pas être utilisée.
	Description : Un écran bleu apparaît lorsque 360 Total Security Protection est installé avec SES. **Cause** : Incompatibilité avec le driver 360Box64.	Aucune solution pour le moment.
9418	**Description** : Incompatibilité avec l'extension "Éditeur Office pour Docs, Sheets et Slides" pour Google Chrome. L'ouverture d'un document avec cette extension échoue et affiche soit une erreur, soit une page blanche.	Aucune solution pour le moment.
8397	**Description** : Lorsqu'un fichier compressé NTFS est chiffré, des données peuvent être perdues et il n'y a pas de gain d'espace.	Désactiver la compression des fichiers NTFS avant de les chiffrer.
9257	**Description** : Incompatibilité avec la sécurité EAF/EAF+ d'EMET (Enhanced Mitigation Experience Toolkit).	Aucune solution pour le moment pour être compatible avec ce module d'EMET.
	Description : Impossible de mettre à jour les postes de travail de Microsoft Windows 10 CBB 1511 vers Windows 10 CBB 1607 avec le chiffrement total du disque SES activé.	**Contournement** : Désactiver le chiffrement, opérer la migration et rechiffrer le poste de travail après la mise à jour.

Précisions sur les cas d'utilisation

Les matériels et logiciels suivants ne sont pas supportés lors du chiffrement de disque :

- Le RAID logiciel et les disques dynamiques.
- Les outils de partitionnement et de création d'image disque.
- Les disques durs ayant une taille de secteur différente de 512 octets.
- Les partitions étendues (ou partitions secondaires) ne sont pas supportées pour le chiffrement de disque complet ; seuls les disques ne contenant que des partitions primaires peuvent être chiffrés avec cette option.
- Le multiboot (plusieurs systèmes d'exploitation sur la même partition ou sur deux partitions) n'est pas supporté par le chiffrement de disque.
- La présence d'un boot loader autre que celui de Windows n'est pas supportée par l'option de chiffrement de disque.

Ressources documentaires

Les ressources documentaires techniques suivantes sont disponibles sur le site de **Documentation Technique Stormshield**. Nous vous invitons à vous appuyer sur ces ressources pour exploiter au mieux l'ensemble des fonctionnalités de cette version.

Guides

- Guide d'administration Stormshield Endpoint Security
- Guide de prise en main Stormshield Endpoint Security

How to

- Comment appliquer une politique de sécurité à votre Active Directory
- Comment débloquer un utilisateur
- Comment mettre à jour un parc sous Windows 10
- Comment isoler un poste de travail avec le firewall SES
- Comment adapter la politique de sécurité SES d'un poste selon sa réputation SNS

Vérifier l'intégrité des binaires

Afin de vérifier l'intégrité des binaires Stormshield Endpoint Security :

1. Entrez l'une des commandes suivantes en remplaçant `filename` par le nom du fichier à vérifier :
   - Système d'exploitation Linux : `sha256sum filename`
   - Système d'exploitation Windows : `CertUtil -hashfile filename SHA256`
2. Comparez le résultat avec les empreintes (hash) indiquées sur l'espace client MyStormshield, rubrique Téléchargements.

Récapitulatif des versions de Stormshield Endpoint Security 7.2

Le tableau suivant récapitule le détail des versions de Stormshield Endpoint Security 7.2 :

Version	Date de sortie	Build
7.2.01	11/05/2015	24884
7.2.03	31/07/2015	25366
7.2.04	30/10/2015	25798
7.2.05	22/01/2016	26324
7.2.07	09/05/2016	26972
7.2.08	27/05/2016	27072
7.2.09	10/06/2016	27184
7.2.10	29/07/2016	27616
7.2.11	22/09/2016	28114
7.2.12	29/09/2016	28180
7.2.13	21/10/2016	28446
7.2.14	30/11/2016	28738
7.2.15	09/02/2017	29261
7.2.16	18/05/2017	29988
7.2.17	19/06/2017	30056
7.2.18	28/08/2017	30367
7.2.19	30/11/2017	30808
7.2.20	28/02/2018	32002
7.2.21	20/03/2018	3
7.2.22	18/05/2018	b6
7.2.23	13/09/2018	4

Versions précédentes de Stormshield Endpoint Security 7.2

Retrouvez dans cette section les nouvelles fonctionnalités, les vulnérabilités résolues et correctifs des versions précédentes de Stormshield Endpoint Security 7.2.

7.2.22	Nouvelles fonctionnalités		Correctifs
7.2.21			Correctifs
7.2.20	Nouvelles fonctionnalités		Correctifs
7.2.19	Nouvelles fonctionnalités		Correctifs
7.2.18	Nouvelles fonctionnalités		Correctifs
7.2.17	Nouvelles fonctionnalités		
7.2.16	Nouvelles fonctionnalités		Correctifs
7.2.15	Nouvelles fonctionnalités		Correctifs
7.2.14	Nouvelles fonctionnalités		Correctifs
7.2.13	Nouvelles fonctionnalités		Correctifs
7.2.12		Vulnérabilités résolues	
7.2.11	Nouvelles fonctionnalités		Correctifs
7.2.10	Nouvelles fonctionnalités		Correctifs
7.2.09			Correctifs
7.2.08		Mises à jour	Correctifs
7.2.07	Nouvelles fonctionnalités	Mises à jour	Correctifs
7.2.06	Nouvelles fonctionnalités	Mises à jour	Correctifs
7.2.05	Nouvelles fonctionnalités	Mises à jour	Correctifs
7.2.04	Nouvelles fonctionnalités	Mises à jour	Correctifs
7.2.03			Correctifs
7.2.02		Mises à jour	Correctifs
7.2.01			Correctifs
7.2	Nouvelles fonctionnalités	Fonctionnalités retirées	Correctifs

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.22

À partir de la version 7.2.20, SES ne permet plus d'administrer la solution antivirus Avira. Si vous possédez cette option, veuillez consulter la section Préconisations avant d'effectuer la mise à jour.

Modernisation de l'interface graphique de la console SES

L'interface de la console SES a été modernisée et simplifiée. Des changements graphiques et de noms de menus améliorent l'ergonomie de l'interface et facilitent la prise en main et l'utilisation de la console.

De même, le menu **Licences** de la partie **Surveillance**, qui présente un rapport indiquant des informations sur vos licences, a été déplacé dans le menu **Rapports** pour figurer parmi les autres types de rapports.

Support de SQL Server 2017

SES supporte désormais SQL Server 2017.

Compatibilité avec Windows 10 1803

Le système d'exploitation Windows 10 1803 April 2018 Update est compatible avec SES 7.2.22.

Modification des informations affichées dans le panneau de surveillance des agents

La colonne **Identifiant de l'agent** a été ajoutée au panneau de surveillance des agents. Elle est cachée par défaut. Il est maintenant possible de trier et filtrer les agents selon leur identifiant.

La colonne **Dernière synchronisation** a été ajoutée et placée après la colonne **Configuration**. Elle est affichée par défaut. Elle indique la date et l'heure auxquelles l'agent a reçu et appliqué le dernier fichier de politiques et de configurations.

La colonne **Dernière config.** a été supprimée.

Affichage de l'icône SES sur les postes de travail

Référence support CF 88063, T1534, 152698PW

La nouvelle option **Affichage de l'icône dans la barre d'état**, dans la configuration dynamique de l'agent, permet de choisir le mode d'affichage de l'icône du moniteur d'agent sur les postes de travail. Cette option est cochée par défaut. Si l'option est décochée, l'icône du moniteur n'est pas visible dans la barre d'état. De plus, l'option concernant l'affichage des notifications est automatiquement décochée et grisée.

Activation du moniteur d'agent dans le menu Démarrer

Il est désormais possible d'activer le moniteur d'agent dans le menu **Démarrer** des postes de travail.

Désinstallation de l'agent SES via le panneau de configuration Windows

Sur les postes de travail, l'entrée Stormshield Endpoint Security Agent est désormais visible dans le panneau de configuration Windows permettant de désinstaller un programme. Il est donc possible de désinstaller l'agent via ce panneau si l'arrêt de ce dernier est autorisé dans sa politique.

Intégration des politiques dans le programme d'installation des agents

Référence support T1639

Il est désormais possible d'intégrer les politiques courantes dans le programme d'installation des agents. Il suffit pour cela de copier le fichier *sync/Agent.srz* dans le dossier *Apache/cgi-bin*, puis de re-générer les programmes d'installation. Lors de l'installation de l'agent, vous devrez récupérer un certificat de l'agent afin que l'agent soit opérationnel, comme indiqué dans la section *Compte et mot de passe pour le téléchargement de certificats* du *Guide d'administration*. Il est ainsi possible de déployer des agents fonctionnels même s'ils n'ont pas accès au serveur SES au moment de l'installation.

Correctifs de Stormshield Endpoint Security 7.2.22

Correctifs agent

Prise en main à distance d'une session Terminal Server (TSE)

Références support CF 88448, T1515, 155784CW

Depuis un agent SES Server-Side Edition, il n'était pas possible de prendre en main à distance une session TSE. Une notification indiquait que l'accès était refusé après la confirmation de la prise en main. Ce problème est résolu.

Déchiffrement du disque dur via un média de recouvrement

Références support CF 88413, T1578, 154773PW

Lors de l'utilisation de *NepRecovery.exe* à partir d'un média de recouvrement et dans le cas de fichiers *.srr* volumineux, le message d'erreur qui indiquait parfois que le mot de passe était erroné ou que le fichier *.srr* était corrompu ne s'affiche plus.

Gel de la machine lors du lancement d'un fichier exécutable sur un serveur DFS

Références support CF 88133, T1388, 153165CW

Le lancement d'un fichier exécutable depuis un serveur DFS figeait systématiquement le poste de travail équipé de l'agent SES pendant deux minutes. Ce problème est résolu.

Évolution du format des fichiers de log

Référence support T492

Les fichiers de log contiennent désormais l'identifiant du processus (PID) qui a généré la ligne de log.

Nouveau fichier de log après désinstallation de l'agent

Référence support T1477

Après la désinstallation d'un agent SES, le nouveau fichier de log *framework.log* est copié dans le répertoire *%WINDIR%\Temp\Stormshield*.

Incompatibilité entre Sophos Endpoint Protection et SES

Références support T1694, CF 88315, 154850CW

Dans certains cas, notamment lorsque d'autres logiciels de sécurité comme Sophos Endpoint Protection v10.7 étaient installés sur le poste de travail, un écran bleu pouvait survenir lorsque la protection contre le débordement de mémoire était active. Ce problème est résolu.

Application d'une configuration corrompue

Références support CF 88524, T1702, 155827CW

Lorsque l'agent recevait une configuration corrompue, celui-ci tentait en vain de l'interpréter. Désormais l'agent attend de recevoir une nouvelle configuration.

Application des politiques

Références support CF 88515, T1641, 157247CW

Lorsqu'une politique ou un script était appliqué sur une condition en rapport avec l'utilisateur Active Directory et lorsque le contrôleur de domaine mettait du temps à répondre, le temps d'application de la politique était très long. Ce problème est résolu.

Ordre d'application des règles de points d'accès Wifi

Référence support T1465

Jusqu'à présent, les règles de points d'accès Wifi étaient appliquées dans l'ordre de leur groupe alors que toutes les autres règles sont appliquées dans l'ordre de leur rang, indépendamment de leur groupe. Les règles Wifi se comportent désormais comme les autres.

Journalisation circulaire dans le gestionnaire de traces

Références support T1769, CF 88306, 153218PW

Dans le gestionnaire de traces, il est désormais possible de choisir la journalisation circulaire pour stocker les traces et donc de limiter en taille le fichier de logs.

Correctifs serveur

Évolution du format des fichiers de logs

Référence support T492

Les fichiers de logs contiennent désormais l'identifiant du processus (PID) qui a généré la ligne de log.

Nouveau fichier de logs après désinstallation du serveur

Référence support T1477

Après la désinstallation du serveur SES, le nouveau fichier de logs *framework.log* est copié dans le répertoire *%WINDIR%\Temp\Stormshield*.

Gestion de la migration

Références support T1073, CF 88528, 155829PW

Désormais, lorsqu'un serveur reçoit une configuration et des politiques de la part d'une console SES, il ignore le contenu s'il possède déjà une configuration et des politiques provenant d'une console plus récente.

Correctifs console

Modification du mot de passe de la console

Références support T1715, CF 88546, 157780CW

Le formulaire de modification du mot de passe de la console limitait sa taille à 20 caractères. Désormais la limite est de 128 caractères.

Affichage de l'état de connexion des agents

Références support T1704, CF 88261, 154426CW

La console pouvait afficher des agents comme étant connectés alors qu'ils ne l'étaient plus. Ce problème arrivait lorsqu'un agent était déconnecté du serveur (ou hors réseau) et que le serveur était relancé avant d'avoir connaissance de la déconnexion de l'agent.

Affichage de la version du serveur et des agents SES

Références support T1627, T1477

Dans la console, la version du serveur et des agents est désormais affichée sous la forme 7.2.22 à la place de 7.222. Ce changement s'applique également aux agents listés dans le panneau de surveillance et qui ont une version antérieure. Il est aussi visible dans le fichier XML exporté depuis le panneau de surveillance des agents.

Import et export des filtres de log

Référence support T1488

L'état activé/désactivé de chaque filtre de log dans le gestionnaire des logs est maintenant correctement exporté et importé dans le fichier *lfxml*.

Sauvegarde du premier opérateur d'un filtre avancé dans l'affichage des logs

Référence support T1490

Dans les filtres avancés de la surveillance des logs, le premier opérateur n'était pas sauvegardé. Il était remplacé par un IF AND actif lors de l'import d'un filtre avancé ou après la fermeture et réouverture de la console. Le premier opérateur est maintenant bien sauvegardé.

A noter également que lors de la désactivation des filtres avancés, le filtre est recalculé en fonction des opérateurs disponibles en mode non avancé.

Logs d'administration de la console

Référence support T1599, CF 88501, 157144CW

Lorsqu'un administrateur changeait la politique appliquée à un environnement ou à un groupe d'utilisateurs via la liste déroulante et non par le bouton  , la modification du lien de la politique à l'environnement n'était pas journalisée. Ce problème est résolu.

Copier-coller de règles

Référence support T1120

Lorsqu'une règle applicative était copiée-collée depuis une autre politique de sécurité, aucun log n'était remonté par les agents vers le serveur pour signaler l'application de cette règle. Ce problème est résolu.

Fusion d'agents

Références support T1760, CF 88415, 153940PW

Lorsque la base de données de logs contenait un historique de logs de connexion d'agents important (de plusieurs années), l'opération de fusion d'agents dans la console pouvait dépasser deux minutes et finalement échouer. Afin de donner la possibilité de réduire cet historique, une option de nettoyage d'historique d'agents a été ajoutée dans le menu **Maintenance des tables de journaux et surveillance** de l'assistant d'installation DbInstaller.

Cependant, il faut noter que dans le cas d'un historique de logs de connexion d'agents important, la mise à jour de la base de données des tables de journaux et surveillance peut prendre plusieurs minutes.

Correctif de Stormshield Endpoint Security 7.2.21

Correctif agent

Incompatibilité avec le correctif Spectre/Meltdown pour Windows 7 et 8.1 32 bits

Références support T1643, T1644

Le correctif de Microsoft contre les vulnérabilités Spectre et Meltdown provoquait une incompatibilité avec SES sur Windows 7 et 8.1 32 bits. Ce problème est résolu. À l'avenir, si une autre incompatibilité de ce type apparaissait, les protections SES impactées seraient automatiquement désactivées. Un message d'erreur "Internal Error 17" apparaîtrait alors.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.20

A partir de la version 7.2.20, SES ne permet plus d'administrer la solution antivirus Avira. Si vous possédez cette option, veuillez consulter la section Préconisations avant d'effectuer la mise à jour.

Installation de SES

Un seul fichier est désormais nécessaire à l'installation de SES (*setup.exe*). Le répertoire *bin* contenant les fichiers *server.exe* et *console.exe* n'existe plus. Le programme d'installation dédié au serveur uniquement reste cependant disponible.

Chiffrement et enrôlement des périphériques amovibles

Référence support T1322

Il est désormais possible de chiffrer un périphérique amovible enrôlé ou d'enrôler un périphérique chiffré. Attention, lorsqu'un périphérique est déchiffré via la console SES sur un poste de travail sans agent SES, son contenu n'est plus considéré comme étant de confiance.

Support des versions de Microsoft SQL Server

Référence support T1309

Il est maintenant possible d'installer un serveur SES avec une version de SQL Server qui n'est pas reconnue par SES. Un message d'avertissement s'affiche alors.

Guide de prise en main

Un nouveau *Guide de prise en main* est disponible sur votre espace sécurisé MyStormshield. Il fournit de l'aide et des recommandations pour le déploiement et la mise en route de SES 7.2.

Correctifs de Stormshield Endpoint Security 7.2.20

Correctifs agent

Incompatibilité avec le correctif Spectre/Meltdown pour Windows 10 32 bits

Référence support T1550

Le correctif de Microsoft contre les vulnérabilités Spectre et Meltdown provoquait une incompatibilité avec SES sur Windows 10 32 bits. Ce problème est résolu. À l'avenir, si une autre incompatibilité de ce type apparaissait, les protections SES impactées seraient automatiquement désactivées. Un message d'erreur "Internal Error 17" apparaîtrait alors.

Outil de réparation de disque Windows

Référence support CF 88404

SES n'empêche plus l'outil de réparation de disque Windows *chkdsk* de réparer un disque au démarrage du poste de travail.

Amélioration de la stabilité

Référence support T1281

Il n'est désormais plus possible de perdre le fichier de configuration de l'agent *conf.srx*. Il est généré à nouveau à chaque redémarrage du poste de travail et ré-évaluation des politiques à appliquer.

Désinstallation de l'agent sur Windows 10

Référence support T1424

La désinstallation d'un agent sur un système d'exploitation Windows 10 version 1709 ou supérieure ne provoque plus de perte de réseau lorsque l'opération est terminée.

Nouveaux logs après désinstallation de l'agent

Référence support T1424

Le fichier de log *\log\updater.sro* est désormais divisé en trois fichiers :

- *\log\installer.sro* : logs concernant l'installation
- *\log\updater.sro* : logs concernant la mise à jour
- *\log\uninstaller.sro* : logs concernant la désinstallation

Après la désinstallation d'un agent, le répertoire *%WINDIR%\Temp\Stormshield* est créé et les fichiers de logs suivants y sont copiés :

- install.log
- SRService.log
- installer.sro
- updater.sro
- uninstaller.sro

Correctifs console

Mot de passe des utilisateurs

Référence support T1274

Il est désormais possible de saisir un mot de passe de plus de 20 caractères lorsqu'un utilisateur se connecte à une console SES. Il n'y a plus de limite maximale du nombre de caractères.

Nombre de connexions à un serveur

Référence support CF 88335 / 154830CW

Le nombre de connexions simultanées à un serveur SES a été augmenté de 1000 à 2000 et le nombre d'agents assignés à un serveur n'est désormais plus limité.

Export des agents

Référence support T1282

Dans le panneau de surveillance des agents, il est désormais possible de choisir les agents à exporter dans un fichier *.xml*. Trois options sont proposées : la liste de tous les agents, la liste des agents sélectionnés ou la liste des agents affichés.

Amélioration des performances

Référence support T1316 / CF 88157

Le panneau **Gestionnaire des utilisateurs** s'affiche plus rapidement qu'auparavant, même si le nombre d'utilisateurs configurés est important.

L'étape d'application des changements à l'environnement est plus rapide lorsque plusieurs serveurs SES sont configurés.

Politiques dans le panneau de surveillance des agents

Référence support T862

La politique affichée par agent dans le panneau de **Surveillance des agents** pouvait être incorrecte. Elle s'affiche désormais correctement.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.19

Nouveau gestionnaire de traces

SES propose un nouvel outil de prise de traces sur les postes de travail équipés de l'agent. Le gestionnaire de traces permet de relever différentes traces liées au déroulement du fonctionnement de l'agent, au système d'exploitation et au réseau. La prise de traces peut-être lancée directement depuis l'agent, en ligne de commande ou depuis un fichier de configuration.

Le gestionnaire peut récupérer les informations suivantes :

- Les journaux de l'agent,
- Les traces de l'agent,
- Les informations rassemblées par l'outil Msinfo32,
- L'enregistreur d'actions utilisateur (PSR),
- Le suivi des périphériques,
- Les journaux d'événements Windows,
- La configuration IP,
- La table de routage,
- Les traces du réseau.

Ce nouvel outil offre un meilleur diagnostic en cas de comportement inattendu de l'agent SES. Pour plus d'informations sur l'utilisation du gestionnaire, veuillez consulter le *Guide d'administration* de SES.

Compatibilité avec les versions Windows 10 1709 32 et 64 bits

Référence support T1083

SES fonctionne désormais sur les systèmes d'exploitation Windows 10 1709 32 et 64 bits. Vous pouvez mettre à jour votre système Windows 10 1703 vers Windows 10 1709 sans désinstaller SES.

Gestion du parcours des règles sur les applications de confiance

Référence support T948 (153682CW)

Dans une politique de sécurité, vous pouvez désormais choisir le mode d'évaluation des règles portant sur les applications de confiance. Disponible en mode avancé, la nouvelle colonne **Évaluation des règles** offre deux possibilités pour chaque règle :

- **Parcourir suivante** : la règle suivante portant sur la même application est évaluée et appliquée le cas échéant.
- **Ignorer suivantes** : dès lors que la règle s'applique, les règles suivantes portant sur la même application sont ignorées.

Les versions précédentes de SES n'offraient pas ce choix. Jusqu'en version 7.2.11, seule la première règle concernant une application s'appliquait, les suivantes étaient ignorées. De la version 7.2.12 à 7.2.18, toutes les règles concernant une application s'appliquaient. A partir de la version 7.2.19, le choix par défaut est **Parcourir suivante**.

Pré-enrôlement manuel d'un périphérique

Référence support T1155

Il est désormais possible de pré-enrôler un périphérique amovible grâce à son numéro de série, sans que celui-ci soit branché au poste de travail hébergeant la console d'administration. Lorsque le périphérique sera branché sur un poste de travail équipé d'un agent SES, l'enrôlement sera automatique.

Révocation de périphériques enrôlés

Référence support T1017

Il est désormais possible de révoquer un périphérique amovible enrôlé ou pré-enrôlé sans que celui-ci soit branché au poste de travail hébergeant la console d'administration. Lorsqu'un périphérique révoqué est branché sur un poste hébergeant un agent SES, toutes les traces d'enrôlement par SES sont supprimées et celui-ci devient inaccessible. Un périphérique révoqué peut être à nouveau enrôlé dans une console d'administration.

Copier-coller de numéros de série de périphériques

Référence support T1133

Il est désormais possible de copier-coller les numéros de série des périphériques enrôlés, pré-enrôlés ou révoqués depuis le panneau d'enrôlement vers une politique de sécurité.

Correctifs de Stormshield Endpoint Security 7.2.19

Correctifs agent

Utilisation d'Internet Explorer 11

Références support : CF88112, 153057CW, T1054

Internet Explorer 11 s'exécute désormais correctement avec SES et Sophos Endpoint Security and Control (version 10.7).

Application d'une politique de sécurité comportant des identifiants par hash

Référence support : T620

Lorsqu'un agent avec une politique ne comportant pas d'identifiant d'application par hash reçoit une nouvelle politique comportant des identifiants par hash (la politique "modèle de base par exemple), le poste de travail ne reste plus bloqué comme précédemment.

Perte de noms de périphériques USB

Références support : 153143PW, T1115

Désormais lorsqu'une politique avec enrôlement de périphériques amovibles est appliquée sur un agent, le nom des volumes sur périphériques USB s'affiche dans l'explorateur Windows et la boite de dialogue d'exécution automatique s'affiche au branchement de ces périphériques.

Enrôlement des périphériques USB sous Windows 8.1 et 10

Références support : T845, 153084PW

Désormais lorsqu'une clé USB formatée sous Windows 8.1 ou 10 est enrôlée, elle possède le statut de confiance.

Correctifs console

Fusion des agents dans le panneau de surveillance

Références support 153940PW

La fusion d'agents par nom NetBIOS ou AD dans le panneau de surveillance des agents n'échoue plus dans certains cas.

Mise à jour du groupe de règles dédié à McAfee

Références support 151571CW, CF87829, T1075

De nouvelles règles de confiance ont été ajoutées au groupe de règles McAfee afin de permettre l'installation et la mise à jour du module HIPS de McAfee lorsque SES est déjà installé sur le poste.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.18

Mise à jour du modèle de base des politiques de sécurité

Une nouvelle règle de confiance pour le contrôle de compte utilisateur (consent.exe) a été ajoutée dans le modèle de base afin d'autoriser ce contrôle à accéder aux applications.

De même, les règles sur Microsoft Office ont été enrichies afin d'inclure les règles sur Microsoft Office 365.

Prise en charge de la signature multiple des applications

Une application peut être signée par plusieurs certificats. Lors de la création d'un identifiant d'application à utiliser dans les politiques de sécurité, vous pouvez désormais choisir le certificat qui permettra d'identifier l'application.

Référence support 152719CW

Ajout d'un nouveau domaine de confiance dans les règles applicatives

Le nouveau domaine de confiance **Attachement désactivé** a été ajouté dans les règles sur les applications de confiance, en mode avancé. Si ce domaine de confiance est coché dans la règle, SES ne s'attache pas à l'application concernée et ne modifie pas directement la mémoire de cette application. Cela permet notamment de définir des règles afin de faire cohabiter SES avec d'autres applications qui ne tolèrent pas ce genre d'attachement et provoquent des incompatibilités. Ce domaine de confiance ne s'applique qu'aux systèmes 64 bits.

Configuration des messages Syslog pour Stormshield Visibility Center (SVC) dans l'assistant d'installation

Dans la maintenance des tables de configuration de l'assistant d'installation de SES, une nouvelle fonction permet de lancer un script qui configure les messages de logs afin qu'ils soient exploités par le produit Stormshield Visibility Center.

Référence support 152307PW

Prévention de la corruption de fichiers SES

Sur l'agent et le serveur SES, un nouveau mécanisme permet de prévenir la corruption de fichiers de configuration SES ainsi que la récupération de ces derniers à partir d'un état corrompu.

Ajout de la variable %HOSTID% dans les logs envoyés à un serveur tiers

Il est désormais possible d'utiliser la variable %HOSTID% dans les logs envoyés à un serveur tiers via les protocoles SMTP et Syslog. Cette variable est remplacée par l'identifiant du certificat de l'agent ou par une chaîne vide si le log est émis par le serveur SES.

Protection Débordements mémoire

Sur les systèmes d'exploitation 64 bits, un log est désormais émis lorsque l'agent SES bloque un comportement de type Stack Pivot effectué par une application 32 bits.

Protection Accès à la mémoire physique

Un log est désormais émis par l'agent SES lorsqu'il bloque une tentative d'accès direct à la mémoire physique.

Référence support 153478CW

Protection des périphériques

Dans les paramètres des groupes de périphériques, le nouveau niveau d'audit **Accès en lecture** a été ajouté.

Correctifs de Stormshield Endpoint Security 7.2.18

Correctifs agent

Référence support 153143PW

Affichage des périphériques USB dans l'explorateur

Sous Windows Vista et les versions ultérieures du système d'exploitation, le nom des volumes FAT ou NTFS sur périphériques USB ne s'affichait pas dans l'explorateur Windows en présence d'un agent SES. La boîte de dialogue d'exécution automatique ne s'affichait pas non plus au branchement de ces mêmes périphériques. Ces deux problèmes sont résolus.

Référence support 152066CW

Incompatibilité avec IBM Trusteer Rapport

L'utilisation du logiciel de protection de sites web bancaires Rapport conjointement avec SES sur les systèmes d'exploitation 64 bits provoquait des arrêts d'Internet Explorer et Google Chrome. Le problème est résolu sous Microsoft Windows 8.1 et 10.

Référence support 152215CW

Chiffrement total du disque

Certains protocoles de communication entre le système d'exploitation et les disques durs n'étaient pas supportés par SES. Il était donc impossible de chiffrer certains disques. Ce problème est résolu.

Référence support 152886CW

Applications de confiance

Lorsqu'un identifiant d'application utilisait un certificat, une application pouvait ne pas être considérée comme une application de confiance durant les premiers instants après son lancement. Ce problème est résolu.

Incompatibilité avec Atempo Live Backup

Une incompatibilité avec le logiciel de sauvegarde Atempo Live Backup a été corrigée. Cette incompatibilité laissait les postes bloqués sur l'écran de démarrage Windows.

Référence support 153466CW - 153963CW - 153903CW

Incompatibilité avec Microsoft Edge

Une incompatibilité entre la protection HPP (HoneyPot) et Microsoft Edge sous Windows 10 version 1703 a été corrigée. Cette incompatibilité bloquait Edge pendant plusieurs secondes lors de son lancement, puis provoquait sa fermeture.

Correctifs serveur

Absence de la session de recouvrement dans la base de données de clés

Auparavant il n'était pas possible de recréer une session de chiffrement d'un agent si celle-ci avait été supprimée de la base de données de clés. A présent, si la base n'est plus présente en base de données, elle est recréée lors du démarrage du poste de travail suivant.

Mise à jour du composant serveur Apache en version 2.4.27

Le serveur web Apache a été mis à jour en version 2.4.27.

Correctifs console

Référence support 152977CW

Gel de l'interface de la console

Dans certains cas, lorsque le thème du système d'exploitation, la résolution ou les préférences utilisateur changeaient, l'interface graphique de la console se figeait et ne répondait plus. Ce problème est résolu.

Utilisation de TLS 1.2 pour les échanges entre la console et le serveur

Dans certains cas, la console d'administration utilisait TLS 1.0 pour échanger des informations avec le serveur SES. Désormais la version 1.2 de TLS est systématiquement utilisée.

Référence support 153321CW

Ordre des règles dans les politiques de sécurité

Dans certains cas comme le copier-coller de règles, deux règles pouvaient se trouver au même rang. Ce problème est résolu.

Référence support 151939PW

Corruption du fichier du média de recouvrement

Lors de la création d'un média de recouvrement avec un grand nombre de clés, la génération du fichier de clés pouvait échouer. Ce problème est résolu.

Référence support 152719CW

Ajout d'un groupe de règles McAfee ETP à importer

Le nouveau groupe de règles McAfee ETP à importer permet de rendre l'utilisation des produits McAfee Endpoint Security Platform et Threat Prevention compatible avec SES.

Nouvelle fonctionnalité de Stormshield Endpoint Security 7.2.17

Pré-enrôlement des périphériques amovibles

Il est désormais possible de pré-enrôler des périphériques amovibles en grande quantité depuis la console SES en important un fichier *.csv* listant tous les périphériques à enrôler. Lorsqu'un périphérique pré-enrôlé est branché sur un agent SES, il est automatiquement enrôlé.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.16

Nouveau mode d'enrôlement automatique

Un nouveau mode d'enrôlement automatique permet d'enrôler un périphérique amovible pour un utilisateur Windows différent de l'utilisateur connecté. Ce mode est activé dans l'onglet **Contrôle des périphériques** d'une politique de sécurité.

Après branchement du périphérique amovible, une fenêtre apparaît qui permet d'entrer les identifiants Windows de l'utilisateur pour lequel l'enrôler.

Masquage du menu "Périphériques amovibles" sur les agents SES

Le menu de gestion des périphériques amovibles n'apparaît plus sur l'agent SES si le chiffrement des périphériques amovibles est désactivé dans la politique de sécurité de l'agent.

Ordre d'affichage des groupes de règles dans la console

Dans la console d'administration, les groupes de règles des onglets **Contrôle des périphériques**, **Contrôle de la sécurité réseau**, et **Contrôle applicatif** sont désormais affichés dans l'ordre alpha-numérique et non plus dans l'ordre de leur création.

Copier-coller des entrées d'identifiants d'applications

Dans la console d'administration, un menu contextuel a été ajouté dans la liste des identifiants d'applications, et dans les entrées d'un identifiant. Il permet notamment de copier-coller des entrées d'un identifiant à un autre, ou de copier les entrées de plusieurs identifiants à la fois.

Possibilité d'accéder au registre 64 bits dans les tests de script

Un nouveau paramètre, **Redirection du registre (sur systèmes 64 bits)**, a été ajouté dans les tests de scripts vérifiant l'existence d'une clé ou la valeur d'une clé de registre. Ce paramètre permet de désactiver la redirection de registre vers la vue 32 bits pour les applications 32 bits sur les systèmes 64 bits. Il n'a aucun effet sur les systèmes 32 bits. Tous les tests de registre qui existaient avant la mise à jour vers la version 7.2.16 se verront affecter la valeur *Activée* pour ce nouveau paramètre, ce qui correspond au comportement des versions antérieures à 7.2.16.

Modification des niveaux de force des mots de passe

Les niveaux de force des mots de passe dans les politiques de chiffrement ont été modifiés. Ils sont désormais de force **Élevée**, **Standard** et **Faible** et la valeur appliquée par défaut est **Standard**.

Les critères de force du mot de passe changent également :

- **Élevée** : le mot de passe doit être composé d'au moins 16 caractères, et d'au moins trois des quatre types de caractères suivants : lettre minuscule, lettre majuscule, caractère spécial et chiffre.
- **Standard** : le mot de passe doit être composé d'au moins 12 caractères, et d'au moins trois des quatre types de caractères suivants : lettre minuscule, lettre majuscule, caractère spécial et chiffre.
- **Faible** : le mot de passe ne respecte pas les critères de force Élevée ou Standard.

Un contrôle sur la force du mot de passe a été ajouté lors de la création d'un média de recouvrement. Ce mot de passe doit désormais avoir une force Élevée.

NepRecovery

Un message a été ajouté à la fermeture de l'outil de recouvrement NepRecovery qui rappelle à l'utilisateur de penser à retirer le média de recouvrement.

Un contrôle sur la force du mot de passe a été ajouté lors de la modification du mot de passe utilisateur : celui-ci doit désormais avoir une force Standard au minimum.

Refonte des fenêtres de création et d'import de politique

Dans la console d'administration, les fenêtres de création et d'import ont fait l'objet des modifications suivantes :

- Il est désormais possible d'importer un fichier de politique sans avoir à créer une politique vide en premier lieu,
- L'import de fichiers de politique permet désormais d'importer plusieurs fichiers à la fois,
- La création de politique permet désormais de choisir des modèles de politiques pré-existants,
- L'import de politique permet désormais d'importer des modèles de groupes de règles pré-existants.

Affichage des clés enrôlées automatiquement dans la console

Les clés enrôlées automatiquement sont désormais affichées dans la console au même titre que les clés enrôlées manuellement par les administrateurs. Cet affichage se base sur les logs émis par les agents lorsque les utilisateurs effectuent l'enrôlement automatique.

Certificats de signature

Les certificats de signature de type SHA-256 sont désormais reconnus par SES à partir de Windows 7.

Changement des libellés des droits sur les fichiers dans les règles applicatives

Dans les règles applicatives, onglet **Contrôle applicatif**, colonne **Fichiers**, les droits ont été renommés. Les droits suivants, du plus restrictifs au moins restrictifs, sont désormais disponibles :

- Accès refusé
- Lecture seule - RX (exécution autorisée)
- Lecture/écriture - RW (exécution refusée)
- Lecture/écriture - RWX (création refusée)
- Accès total - RWX

Nouveau certificat de signature

Dans le cadre du renouvellement du certificat de signature du code des produits Stormshield, un nouveau certificat a été déployé. Conformément au nouveau nom de la société, ce certificat est désormais au nom de Stormshield à la place de SkyRecon.

Correctifs de Stormshield Endpoint Security 7.2.16

Correctifs agent

Référence support #CF 87791

Compatibilité Veeam Backup

La procédure de restauration de la solution Veeam Backup restait bloquée sur l'action *Démonter la partition*, et l'option proposée par Veeam (*Annuler*) ne permettait pas de restaurer la base de données. Ce problème est résolu.

Référence support #CF 87920

Corrections dans la protection heap spray

La présence de faux-positifs avec la protection heap spray empêchait parfois l'utilisateur d'ouvrir certains fichiers légitimes. Ces faux-positifs ont été corrigés et la protection heap spray est désormais plus précise.

Suppression des logs DRIVER_ERROR lors d'une nouvelle installation

Les messages de type *DRIVER_ERROR* ne sont désormais plus affichés lors d'une nouvelle installation de SES car ils ne sont pas pertinents dans ce cas.

Référence support #CF 87797

Mise à jour du pilote de chiffrement dans l'image de restauration Windows

Lors d'une mise à jour de l'agent, le pilote de chiffrement n'était pas mis à jour dans l'image de restauration Windows. Il était alors impossible d'accéder aux données du disque lors d'une tentative de restauration du système.

Pour corriger ce problème, ce pilote est désormais mis à jour en même temps que l'agent.

Référence support #CF 87829

Compatibilité avec McAfee FRP

Une incompatibilité entre SES et McAfee FRP (File and Removable media Protection) pouvait provoquer un blocage du poste de travail et l'impossibilité de brancher des clés USB. Ce problème est résolu.

Échec lors la mise à jour de l'agent

Il était possible qu'une mise à jour d'un agent échoue lorsque la politique de sécurité contenait des règles bloquant la création de fichiers système. Désormais, le processus de mise à jour gère correctement ce cas de figure.

Référence support #CF 87934

Compatibilité avec Bromium

La présence d'un agent SES 7.2.15 empêchait l'initialisation de Bromium. Ce problème est résolu.

Référence support #CF 87839

Blocage de flux normalement autorisés par la politique de sécurité

Des flux sortants normalement autorisés par la politique de sécurité étaient bloqués par le firewall de SES. Le comportement de celui-ci, qui pouvait refuser une connexion en mode stateful sous certaines conditions, a été corrigé.

Correctifs console

Incompatibilité du chiffrement total du disque avec un serveur de bases de données antérieur à la version 7.2.15

Désormais il est possible de chiffrer un agent dont la version est antérieure à la 7.2.15 en utilisant des bases de données 7.2.15.

Erreur lors de l'enrôlement d'une clé USB

Lors de l'enrôlement d'une clé USB par un utilisateur Active Directory, le champ **Enrôlé par** de la fenêtre d'enrôlement était vide si certains attributs LDAP manquaient pour l'utilisateur connecté. La console récupère désormais correctement l'utilisateur courant dans l'annuaire LDAP.

Avertissement avant d'écraser une sauvegarde de base de données

Lors de la sauvegarde d'une base de données avec l'utilitaire de maintenance des bases de données (DbInstaller), le logiciel demande désormais confirmation à l'utilisateur avant d'écraser le fichier si ce dernier existe déjà.

Audit de la console

Dans une démarche d'amélioration de l'ergonomie de l'interface de la console, le menu **Observateur d'événements** se nomme désormais **Audit de la console**.

Correction du lancement de NepRecovery

L'outil de recouvrement NepRecovery ne se lançait plus correctement sur le système d'exploitation Windows PE depuis la version 7.2.15 de SES. Ce problème est résolu.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.15

Détection et réparation automatique de la désynchronisation des mots de passe de recouvrement

L'agent SES vérifie désormais la validité des informations de recouvrement avec le serveur à chaque démarrage d'un poste de travail chiffré. Dans le cas où les informations de recouvrement de l'agent et du serveur ne sont pas synchronisées, un processus de réparation automatique est lancé. Cela permet de s'assurer que l'utilisation du mot de passe de recouvrement sera toujours possible sans erreur.

Pour bénéficier de cette fonctionnalité, il faudra effectuer une mise à jour de la table des clés de chiffrement avec l'utilitaire de maintenance des bases de données (DbInstaller).

Passage au .NET Framework 4.6.1 pour la console d'administration et les outils liés

La console d'administration et les outils liés utilisaient la version 4.0 du .NET Framework. Cette version n'étant plus maintenue par Microsoft, SES utilise désormais la version 4.6.1. Par conséquent, il n'est plus possible d'installer et d'utiliser ces composants sur les systèmes Windows XP et Windows Server 2003.

Gestion des groupes de périphériques dans la politique de sécurité

Dans l'onglet **Contrôle des périphériques** de la politique de sécurité, le paramètre **Gestion des groupes** a été ajouté. Ce paramètre permet d'activer ou désactiver l'ensemble des fonctionnalités relatives aux groupes de périphériques amovibles dans la politique de sécurité : audit, chiffrement de périphériques, enrôlement etc.

Si le paramètre **Gestion des groupes** est modifié dans la politique, nous vous recommandons de redémarrer les postes de travail pour que les agents SES prennent correctement en compte la nouvelle politique de sécurité.

Pour plus d'informations, reportez-vous au *Guide d'administration* Stormshield Endpoint Security.

Informations sur la configuration de l'agent SES dans la base de registre

Des informations sur les configurations et politiques courantes de l'agent SES sont désormais stockées dans la base de registre des postes des utilisateurs. Les clés contiennent les noms, versions et dates d'application des configurations statique et dynamique, des politiques de sécurité, de chiffrement et d'antivirus. Elles contiennent également la limite de version de mise à jour de l'agent, le mode de l'agent (Normal, Warning, Standby) ainsi que les éventuels challenges Désactivation des protections et Contrôle antivirus en cours.

Pour plus d'informations, reportez-vous au *Guide d'administration* Stormshield Endpoint Security.

Affichage des logs de la session courante sur l'agent SES

Désormais, l'agent SES affiche par défaut les logs de la session courante uniquement, c'est à dire depuis le dernier redémarrage de Windows ou depuis la dernière reconnexion de l'agent après un arrêt.

Les autres options d'affichage (tous les logs, 20, 50, 100 et 200) sont toujours accessibles dans la liste déroulante en bas à droite de la fenêtre des logs.

Amélioration de l'auto-protection de SES

L'auto-protection SES, chargée de protéger certains fichiers utiles pour le bon fonctionnement de l'agent et pour la sécurité du poste, a été améliorée. Elle s'appliquait à tous les fichiers possédant

une certaine extension (de manière générale, les fichiers *.sr*) quel que soit leur emplacement sur le disque. Désormais, elle s'applique uniquement aux fichiers spécifiques de SES.

Correctifs de Stormshield Endpoint Security 7.2.15

Correctifs agent

Application de politiques

Dans les versions précédentes de SES, il y avait une latence entre l'affichage d'un log d'application de politique et l'application fonctionnelle de la politique. Le log indique désormais l'application effective d'une nouvelle politique. Dans le cas des règles du contrôle des applications, les règles d'apprentissage ont été désactivées par souci de performance. Les exceptions devront dorénavant être explicitement indiquées dans les règles applicatives.

Référence support 11877

Blocage lors de la mise à jour de la licence de l'antivirus Avira

L'application des politiques par un agent SES installé avec l'antivirus Avira pouvait être bloquée lors de la mise à jour de la licence Avira. Désormais, la mise à jour de la licence Avira ne bloque plus le fonctionnement de l'agent SES. Ce dernier applique toujours les changements de politiques envoyés par le serveur. De plus, dans les logs système des journaux d'événements, un log indique que la licence Avira est expirée.

Référence support #CF 87633

Installation du VPN de Stormshield sur Windows 10 1607 CBB

Sur les postes de travail équipés de l'agent SES et sous système d'exploitation Windows 10 1607 CBB, le VPN de Stormshield s'installait mal et sa carte réseau virtuelle n'apparaissait pas dans le panneau de configuration. Désormais, l'installation de cette carte réseau fonctionne.

Log VOLUME_DENIED intempestif

Un log VOLUME_DENIED apparaissait dans le fichier *device.sro* à chaque fois qu'un périphérique était branché à un poste de travail, et ce même si aucun blocage n'était effectivement appliqué. Ce log n'apparaît désormais que lorsque l'accès au périphérique est réellement interdit.

Référence support #CF 87626

Incompatibilité entre SEP 14 et la protection RCP

Lorsque l'antivirus Symantec Endpoint Protection 14 était installé sur un poste de travail, et que la protection RCP de SES était activée, certaines applications cessaient de fonctionner, notamment Mozilla Firefox, Internet Explorer, et le service Symantec Endpoint Protection lui-même. Ce problème est résolu.

Logs d'auto-protection superflus

Sur l'agent SES, de très nombreux logs [AUTO-PROTECTION] [OPEN-PROCESS] pouvaient apparaître dans le fichier *heimdall.sro* présent dans le dossier log de l'agent SES. Ces logs étaient affichés à chaque fois qu'un processus tentait d'accéder aux informations des processus SES. Ces logs ont été retirés car empêcher l'accès aux processus SES constitue le fonctionnement normal du produit.

Référence support 151256CW (#CF 87724)

Compatibilité avec Microsoft Office 2013 et 2016 64 bits

SES n'était pas compatible avec la version 64 bits des produits Microsoft Office 2013 et 2016. L'ensemble de ces produits fonctionnent maintenant correctement sur les systèmes d'exploitation supportés.

Applications consoles de Microsoft Windows 10

Lorsqu'une règle applicative interdisait la création de fichier à une application de type "console" sous Windows 10, l'application ne pouvait pas se lancer (même en mode Warning). Ce problème est résolu.

Incompatibilité entre le contrôle d'exécution sur périphériques de SES et le chiffrement de périphériques de McAfee

La fonction de contrôle d'exécution sur périphériques amovibles est maintenant fonctionnelle pour les périphériques chiffrés avec la fonctionnalité FRP de McAfee : la fenêtre d'avertissement est affichée et l'exécutable est bloqué le cas échéant.

Référence support #CF 87789

Ouverture de session Windows après mise à jour de l'agent

Après une mise à jour de l'agent SES sur un poste de travail, lors du redémarrage du poste, la session Windows de l'utilisateur pouvait ne plus s'ouvrir. Ceci se produisait lorsque l'agent appliquait au moins une politique de sécurité contenant un ou des certificats. Ce problème est résolu.

Correctifs serveur

Simplification du mode de mise à jour du serveur

Le paramètre pour changer le mode de mise à jour du serveur par la console a été supprimé. Désormais, le mode de mise à jour du serveur par défaut est le mode automatique. Le serveur vérifie toujours la présence de nouvelles mises à jour au démarrage du service SES. Attention, si des serveurs sont configurés en mode de mise à jour manuel, il est important de les mettre à jour en version 7.2.15 avant la console, afin qu'ils ne restent pas bloqués en mise à jour manuelle, ou bien de les passer en mise à jour automatique avant la mise à jour en version 7.2.15.

Simplification de la récupération des mises à jour par le serveur

La possibilité pour un serveur SES de récupérer ses mises à jour sur un serveur distant est désormais limitée aux répertoires locaux et aux partages Windows. Un serveur SES ne peut plus récupérer des mises à jour sur un serveur FTP ou HTTP. Dans la politique serveur, dans la section **Mises à jour du logiciel**, les paramètres **Type de source**, **Port**, **Nom de l'utilisateur**, **Mot de passe**, et **Chemin d'accès à distance** ont été supprimés. Le paramètre **URL/Chemin local** a été renommé en **Dossier de téléchargement des mises à jour**.

Pour plus d'informations, reportez-vous au *Guide d'administration* Stormshield Endpoint Security.

Correctifs console

Amélioration de la recherche des ports

Dans les règles firewall réseau et les sous-règles applicatives réseau, le seul critère de recherche des ports était leur nom. Désormais, il est possible de rechercher un port par son numéro, son nom ou sa description. De plus, la fenêtre peut être redimensionnée par l'utilisateur.

Référence support 9542

Fonctions de sauvegarde et restauration de l'utilitaire de maintenance des bases de données (DbInstaller)

Des erreurs empêchaient la restauration de bases de données de s'effectuer. Ce problème est résolu.

Configuration des logs

Dans une démarche d'amélioration de l'ergonomie de l'interface de la console, le menu **Éditeur de logs** se nomme désormais **Configuration des logs**.

Erreur dans le rapport "Modifications de la configuration de Stormshield Endpoint Security"

Dans la console, lors de l'ouverture du rapport sur les modifications de la configuration de SES, celui-ci affichait une erreur liée à la base de données de stockage des politiques. Ce problème est résolu.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.14

Référence support 075589CW

Chemins App-V 4.6 : gestion de l'antislash

Il est maintenant possible de spécifier des chemins qui commencent par un antislash unique « \ » (en plus des lettres de lecteurs « X:\ » et des chemins UNC « \\ ») dans les chemins des identifiants d'application, dans les règles applicatives. Cela permet notamment de spécifier des chemins pour les applications virtualisées avec App-V 4.6.

Mise à jour de la version Windows 10 CBB 1511 vers la version "Anniversary Update" 1607

La mise à jour d'un parc de postes de travail vers la version 1607 de Windows 10 est possible mais nécessite une manipulation particulière dans les politiques de sécurité. Une procédure pour vous aider est disponible sur MyStormshield dans la base documentaire.

Correctifs de Stormshield Endpoint Security 7.2.14

Correctifs agent

Référence support 11508

Suppression du filtrage ICMP des règles applicatives sur le réseau

Dans la colonne **Réseau** du panneau des règles applicatives dans la politique de sécurité, le paramètre **Par défaut** agissait sur les protocoles ICMP, TCP et UDP, alors qu'il n'était pas possible d'écrire des règles réseau concernant le protocole ICMP dans cette fenêtre. Désormais, les règles applicatives réseau ne concernent plus le protocole ICMP.

Référence support 11639 (#CF 87512)

Gestion du slash ("/") dans les unités organisationnelles (OU) LDAP

Lorsque le Distinguished Name (DN) complet d'une machine contenait au moins un slash (par exemple avec une OU qui contient elle-même un slash), l'agent installé sur cette machine ne pouvait pas récupérer une politique liée à cette OU. Désormais, l'agent fonctionne correctement dans ce cas.

Référence support 11578

Nouveau format de logs d'auto-protection

Désormais dans un souci de clarté, les logs concernant l'auto-protection de SES ont changé de format.

Référence support 11536 (#CF 87441 - 150724PW)

Lenteur d'application de politiques après un changement réseau

Lorsque le serveur SES était inaccessible, l'application des politiques conditionnées pouvait demander 20 secondes. Le fonctionnement a été modifié afin d'appliquer le changement de politique le plus rapidement possible, même en étant déconnecté du serveur SES. Certaines latences dans l'affichage des logs d'application de politique peuvent toujours avoir lieu. Ce point sera corrigé dans une prochaine version.

Référence support 11811 (#CF 85877)

Blocage des connexions TCP utilisant l'option FastOpen

Dans l'onglet **Contrôle de la sécurité réseau** de la politique de sécurité, lorsque le paramètre **Contrôle d'intégrité TCP** était activé, le firewall bloquait les connexions TCP utilisant l'option TCP FastOpen. Désormais, cette option est bien reconnue et n'est plus bloquée.

Référence support 11846 et 11920 (#CF 87614)

Utilisation des outils stopagent et ssusrlog avec le compte Système local Windows

Il est désormais possible de lancer les outils SES stopagent et ssusrlog avec le compte Système local. Ce compte est notamment utilisé pour les exécutions de processus dans les scripts SES.

Référence support 150843PW

Gel de l'interface de l'agent après une mise à jour

Après une mise à jour de l'agent, dans certains cas, l'interface de l'agent pouvait indiquer que celui-ci était désactivé tant que le poste de travail n'était pas redémarré. L'agent fonctionnait correctement malgré cela, seule l'interface ne répondait plus.

Correctif serveur

Référence support 11531

Mise à jour du numéro de version SES dans le Panneau de configuration Windows

Lors d'une mise à jour du serveur SES, le numéro de version visible dans le menu **Programmes et fonctionnalités** du **Panneau de configuration** Windows ne correspondait pas à la dernière version installée. Ce problème est résolu.

Correctif console

Référence support 11816

Export des politiques SES

Dans la console d'administration, seule la politique de sécurité est exportée au format SCZP. Ce format est une archive contenant le fichier de la politique de sécurité au format SCEP ainsi que les identifiants d'application associés. Tous les autres types de politiques s'exportent directement au format SCEP.

À partir de la version 7.2.11, toutes les politiques s'exportaient en SCZP. Afin d'importer une politique autre que de type sécurité dans les versions 7.2.11 à 7.2.13, il fallait au préalable extraire le fichier SCEP contenu dans l'archive SCZP.

À partir de la version 7.2.14, le problème est corrigé : toutes les politiques autres que de type sécurité s'exportent au format SCEP.

Référence support 11716 (#CF 87511)

Trafic entre la console d'administration et les bases de données

Le trafic entre la console et les bases de données pouvait être très important lorsqu'il y avait un grand nombre d'agents et/ou de bases de logs. Ce trafic a été optimisé pour réduire le volume de données échangées. Ce problème impactait surtout les parcs ayant plusieurs bases de données de logs.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.13

Mise à jour de l'antivirus Avira

La version d'Avira désormais déployée sur les agents SES 7.2.13 est la version Avira Antivirus Pro 2015. Si vous possédez un parc d'agents utilisant l'option Antivirus, vous devrez commencer par désinstaller la version précédente d'Avira (Avira Professional Security 2013) avant de procéder à la mise à jour de vos agents. La nouvelle version d'Avira sera automatiquement déployée avec la mise à jour des agents.

La procédure à suivre est indiquée dans le *Guide d'administration Stormshield Endpoint Security*, section *Migration vers Avira 2015*.

L'option Antivirus est désormais compatible avec Microsoft Windows 10.

Synchronisation des données de recouvrement du chiffrement total de disque

Lors de la mise à jour de SES depuis une version antérieure à la 7.2.06, désormais les données de recouvrement du chiffrement total du disque sont vérifiées et réparées si nécessaire. Cette procédure de vérification est initiée par l'agent lors de sa mise à jour. Ceci permet d'éviter que des données de recouvrement entre l'agent et le serveur SES soient désynchronisées en raison de mauvaises manipulations en base de données ou de l'instabilité des réseaux.

Correctifs de Stormshield Endpoint Security 7.2.13

Correctifs agent

Référence support 11372

Affichage des logs d'application des politiques et configurations

Lorsque l'agent appliquait une nouvelle politique ou configuration, le log d'application pouvait s'afficher plusieurs fois de suite dans la fenêtre des journaux d'événements. Ce problème est résolu.

Référence support 11080 (#CF 86971)

Problème de connexion au serveur par route directe

Lorsqu'une route directe était établie vers le serveur SES dans la configuration réseau, l'agent SES ne pouvait pas se connecter au serveur. Le problème survenait avec certains VPN et les politiques ne pouvaient pas être appliquées. Désormais si une route peut atteindre le serveur, l'agent ne perdra pas sa connexion.

Référence support 11444 (#CF 87417 et 87432)

Écran bleu lorsque le fichier *Ntdll.dll* était compressé

Sur Microsoft Windows 10 et Windows 8.1, les fichiers exécutables du système d'exploitation dont le fichier *Ntdll.dll* peuvent être compressés avec la commande `compact /compactos:always`. Lorsqu'on installait l'agent SES sur une machine sur laquelle cette commande avait été exécutée ou lorsqu'on exécutait cette commande après avoir installé l'agent, un écran bleu se produisait au redémarrage de la machine. Ce problème est résolu.

Référence support 11551 (#CF 87486)

Écran bleu aléatoire lors du contrôle des événements kernel

Certaines vérifications effectuées dans le cadre du contrôle des événements kernel dans la politique de sécurité pouvaient entraîner aléatoirement un écran bleu. Ces actions ont été revues et corrigées.

Référence support 11350 (#CF 87349)

Incompatibilité entre l'agent SES et certains drivers graphiques Intel

Sur Microsoft Windows XP ou 2003 Server, un écran bleu pouvait se produire lorsque l'agent SES et certains drivers graphiques Intel étaient installés sur le même poste de travail. Ce problème est résolu.

Référence support 11645 (#CF 87509)

Erreur avec le test intégré sur l'interface réseau active dans les scripts

Depuis la version 7.2.10, une erreur survenait lors d'un test réseau sur l'interface active et empêchait l'exécution de celui-ci. Ce problème est résolu.

Correctifs console

Référence support 11079

Permissions incorrectes sur la console

Dans certains cas, certaines fonctionnalités de la console (par exemple la duplication de script) n'étaient pas accessibles. Ce problème est résolu.

Référence support 11365 (#CF 87355)

Problème d'affichage dans les règles applicatives de la politique de sécurité

Dans les règles applicatives appliquées à l'accès à la base de registre, lorsque l'on ajoutait une ligne, si celle-ci était la dernière affichée, une barre de défilement apparaissait au milieu de la fenêtre. Ce problème est résolu.

Référence support 10666

Paramètres du comportement système dans la politique de sécurité

Dans l'onglet *Comportement système* de la politique de sécurité, le niveau "Bas" de certains paramètres signifiait qu'il n'y avait pas de blocage ou pas de protection. Le niveau "Bas" a été renommé en "Désactivé".

Référence support 9955

Listes et grilles

Le bouton d'édition "..." dans les listes et grilles n'était pas assez visible (aligné à droite) et n'était pas adapté aux listes déroulantes. Dorénavant, le bouton est affiché lors du survol d'une ligne et son apparence correspond à l'action qu'il déclenche (liste déroulante ou fenêtre d'édition).

Référence support 11440

Ajout de nouvelles actions dans les logs Périphérique

Dans l'éditeur de logs, les actions VOLUME_MOUNT, VOLUME_READWRITE, FILE_CREATE, FILE_READ et FILE_WRITE ont été ajoutées dans les logs Périphérique.

Référence support 11512 (#CF 87443)

Dysfonctionnement de l'assistant d'installation de la base de données

Lors d'une migration avec restauration de la base de données d'une version de StormShield 6.0.XX vers une version de SES 7.2.XX, l'assistant d'installation de la base de données pouvait cesser de fonctionner brutalement. Ce problème est résolu.

Référence support 9171

Activation des groupes de règles dans la politique de sécurité

Lorsqu'un groupe de règles était désactivé dans la politique de sécurité, les règles n'afffichaient pas un état "Désactivé". Désormais, toutes les règles du groupe affichent bien l'état "Désactivé".

Référence support 11219

Modification du nom d'un groupe de règles lors de la copie

Lorsqu'un groupe de règles était copié d'une politique de sécurité à une autre, il pouvait arriver que le nom soit tronqué. Ce problème est résolu.

Référence support 11541

Correction de l'erreur "Fichier invalide" lors de l'import d'une politique

Lors d'un import de politique, lorsque l'encodage était différent d'UTF-8, une erreur interrompait l'action. L'import se déroule désormais correctement, mais en cas d'encodage inconnu certains caractères pourront être remplacés.

Référence support 11216

Suppression de groupes de règles

Dans une politique de sécurité en mode édition, il est désormais possible de supprimer des groupes de règles concernant les périphériques amovibles ou le firewall réseau avec le bouton "Suppr" du clavier.

Référence support 11381

Amélioration de l'action "Restaurer" dans les scripts

L'action **Restaurer** (une politique/une configuration) proposée dans les scripts a été améliorée et une action **Réévaluer** a été ajoutée. Pour plus d'informations sur ces deux options, reportez-vous à la section *Scripts* du *Guide d'administration*.

Correctif serveur

Référence support 9035 (#CF 86831)

Droits manquants lors de la suppression d'un serveur

Lorsqu'un utilisateur possédait les permissions nécessaires pour la suppression d'un serveur SES, la suppression ne fonctionnait pas. Ce problème était dû à une erreur d'attribution des droits sur le serveur SQL lors de l'installation. Désormais la suppression de serveur s'effectue correctement si l'utilisateur a les permissions nécessaires.

Vulnérabilités résolues de Stormshield Endpoint Security 7.2.12

Références support 11522, 11524 et 11526

Mise à jour de OpenSSL en version 1.0.2j

Des vulnérabilités (CVE-2016-6304, CVE-2016-6306 et CVE-2016-2177) ont été corrigées par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.2j. Le détail de la vulnérabilité CVE-2016-6304 (OCSP Status Request extension unbounded memory growth) est disponible sur notre site https://advisories.stormshield.eu/.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.11

Nouveau challenge "Mise à jour de l'agent"

Le challenge **Mise à jour de l'agent** permet désormais de mettre à jour un agent SES sans tenir compte de la limite de version définie dans la configuration statique de l'agent. Il sera effectif pour les versions de l'agent supérieures à la version 7.2.11.

Déplacement des règles de groupes d'agents

Un nouveau bouton dans la barre d'outils des configurations IP et Netbios des groupes d'agents de l'annuaire interne permet désormais de déplacer des entrées d'un groupe vers un autre groupe en cours d'édition.

Modification des identifiants d'application pour les extensions et applications de confiance

Un ou plusieurs identifiants d'application peuvent être simultanément ajoutés ou supprimés de plusieurs règles sur les extensions et applications de confiance.

Fenêtre de création d'un utilisateur dans la console

Une boîte de dialogue complète permet désormais d'ajouter un nouvel utilisateur SQL ou Active Directory de la console. Elle permet de spécifier à la création différentes informations sur l'utilisateur (identifiant, mot de passe, rôle, environnement) ainsi que la configuration de la console pour ce nouvel utilisateur (initialisée par défaut comme la configuration de l'utilisateur courant).

Support de MS SQL Server 2014 et MS SQL Server 2016

SES supporte désormais les versions MS SQL Server 2014 et MS SQL Server 2016.

Nouveau log pour le test de script "Exécuter un programme" lorsque le programme n'a pas pu être créé

Lors de l'ajout d'un test intégré "Exécuter un programme" dans un script, le log créé dans le fichier *skybatch.sro* prend désormais la valeur [CHECK] [ERROR] lorsque le programme n'a pas pu être exécuté (faute de frappe ou commande inexistante par exemple).

Correctifs de Stormshield Endpoint Security 7.2.11

Correctifs agent

Référence support 11163 (#CF 87346)

Lenteur des processus sur systèmes d'exploitation 64 bits

Sur les systèmes d'exploitation 64 bits, des processus 32 bits utilisaient 100% d'un processeur (ou d'un cœur). Ce problème se produisait lorsque la protection contre les débordements mémoire était activée. Les processus étaient par conséquent très lents et semblaient bloqués. Ce problème est résolu.

Référence support 11020

Champ d'application des règles sur les applications de confiance dans la politique de sécurité

La propagation de la portée d'une règle de confiance pour une application (sélectionnable dans la colonne **Champ d'application**) ne fonctionnait pas pour le domaine de confiance **Exécution sur un périphérique amovible** : lorsque le champ d'application de la règle était défini sur **Application et enfants**, une fenêtre de notification demandant la confirmation de l'exécution d'un processus sur le périphérique amovible s'affichait quand même. Désormais la propagation de la portée de la règle pour ce domaine fonctionne.

Pour plus d'informations sur le champ d'application d'une règle de sécurité, reportez-vous au *Guide d'administration Stormshield Endpoint Security*.

Référence support 11203 (#CF 87173)

Blocage des flux liés à une détection de balayage de port

Dans certains cas, les trames ICMP (type 3, code 3) pouvaient être bloquées par l'agent SES après une détection de balayage de port avec l'IDS au niveau bas. Ces flux sont désormais bloqués uniquement avec un niveau d'IDS défini sur haut ou critique.

Référence support 11086 et 11087 (#CF 87246)

Logs concernant les règles d'extension dans la politique de sécurité

Les logs système concernant les règles d'extension en état Warning définies dans la politique de sécurité n'étaient plus générés. Ce problème est résolu.

De même, ces logs n'étaient pas générés si un identifiant d'application n'était pas renseigné dans la règle. Dorénavant, les logs seront générés même en l'absence d'identifiant.

Référence support 11185

Agrégation des règles de confiance

Lorsque plusieurs règles de confiance s'appliquaient à un même identifiant, seule la première règle de confiance était prise en compte. Désormais, toutes les règles de confiance sont prises en compte et agrégées.

Référence support 11370 (#CF 87350/87373/150043CW/150079CW)

Correction d'un BSOD sur système d'exploitation Microsoft Windows 64 bits

Un BSOD pouvait avoir lieu en version 7.2.10 sur des systèmes d'exploitation Windows 64 bits lors de l'utilisation de certaines applications comme GoToMeeting nécessitant des outils tels que webcam et micro USB. Ce problème est résolu.

Référence support 11127 (#CF 87200 et 86916)

Amélioration des performances

Les performances de SES ont été améliorées pour l'ensemble des versions de Windows, et notamment pour les versions 64 bits de Windows lorsque la protection RCP est activée.

Correctif serveur

Référence support 11035 (#CF 87237)

Mise à jour du serveur

Lorsque le répertoire d'installation du serveur SES n'avait pas de nom court Windows ou que les noms courts Windows étaient désactivés, la mise à jour du serveur échouait. Désormais, la mise à jour fonctionne même si les noms courts Windows sont absents ou désactivés.

Correctifs console

Référence support 10595

Suppression de l'option "Lecture seule" des règles applicatives

L'option **Lecture seule**, qui empêchait la modification du contenu d'un exécutable, a été supprimée du panneau des règles applicatives dans la politique de sécurité.

Référence support 11186

Export d'une politique de sécurité

Lors de l'export d'une politique de sécurité, par défaut la politique était exportée seule. Désormais, l'option par défaut est l'export de la politique avec ses ressources.

Référence support 10860 (#CF 87185 et 87227)

Affichage de groupes Active Directory dans un script

La fenêtre de sélection de groupes ou d'utilisateurs dans les ressources de script n'affichait pas l'ensemble des éléments présents. Cette fenêtre a été remplacée par une fenêtre de recherche permettant de filtrer les éléments recherchés.

Référence support 11241 (#CF 87044)

Affichage de l'icône de l'agent en mode Active Directory

Dans la vue Active Directory, les ordinateurs sur lesquels sont installés les agents affichent une icône spécifique. Dans certains cas, cette icône n'était pas affichée. Ce problème est résolu.

Référence support 11256 (#CF 86923)

Ordre des règles lors de l'import de politiques de sécurité

Lors de l'import de politiques de sécurité provenant d'une version 6.0 de SES, les règles de contrôle applicatif (règles applicatives, extensions et applications de confiance) perdaient leur rang. Désormais, le rang est bien conservé lors de l'import.

Référence support 8583

Mode d'affichage de "Composants kernel"

Dans l'onglet *Comportement système* de la politique de sécurité, l'élément **Composants kernel** était affiché en rouge lorsque la protection était désactivée et en vert lorsqu'elle était activée.

Désormais, lorsque la protection est désactivée, l'élément est grisé. Une info-bulle indique que la protection est désactivée et l'élément n'est plus sélectionnable.

Si la protection est activée, l'élément est affiché comme un élément normal.

Référence support 9553

Droits sur les règles d'extension CD/DVD/Blu-Ray

Dans l'onglet *Contrôle des périphériques* de la politique de sécurité, lors d'un copier-coller ou d'un import de règles d'extension dans un groupe CD/DVD/Blu-Ray, les droits possibles affichés dans la liste étaient incorrects. Désormais, les droits possibles tiennent compte du type de périphérique.

Référence support 11265

Exception lors de la fermeture de la console

Une exception pouvait avoir lieu à la fermeture de la console quand le tableau de bord était affiché. Ce problème est résolu.

Référence support 8824

Amélioration de l'éditeur de script

Lorsque l'on éditait une politique de script ou les ressources de scripts, le caractère ":" était remplacé par "::" dans l'affichage de l'arborescence du script. Ce problème est résolu.

Référence support 10398

Menu contextuel pour les logs en mode Test

Le menu contextuel (clic droit) de la surveillance des logs n'apparaissait pas dans le cas où le log remonté dans la console provenait d'une règle en mode Test.

Désormais, les logs remontés par les règles en mode Test peuvent être copiés et triés avec le menu contextuel.

Référence support 7248

Changement des messages courts pour les réseaux ARP

Les messages courts des logs réseau ARP affichaient le contenu des variables PORTDST et PORTSRC, alors que la notion de port n'existe pas dans une attaque ARP. Ce problème est résolu.

Référence support 10854

ssusrlog.exe

Lorsqu'un log est envoyé avec succès au serveur via ssusrlog.exe, aucun message d'erreur n'apparaît dorénavant et un message de confirmation s'affiche. De plus l'exécutable est désormais capable de gérer les paramètres incorrects.

Référence support 11162

Chargement des domaines dans un annuaire Active Directory

L'ouverture de la console pouvait être lente lorsque celle-ci fonctionnait en mode Active Directory. Plusieurs améliorations ont été apportées lors du chargement des domaines dans une forêt Active Directory. Par exemple, les sous-domaines se chargent maintenant en arrière-plan.

Référence support 11250

Uniformisation des recherches LDAP dans la console

Plusieurs fonctionnalités de la console nécessitent d'opérer des requêtes LDAP : ressources de script, recherche dans l'annuaire Active Directory, recherche d'utilisateurs pour l'enrôlement de périphériques, ajout d'utilisateurs de la console avec authentification Windows. Lorsque l'utilisateur saisissait une chaîne, dans certains cas, la console ajoutait automatiquement le caractère "*" avant et après la chaîne. Ce caractère incluait les éléments qui contenaient la chaîne recherchée au lieu d'effectuer une recherche exacte, ce qui augmentait significativement le temps de recherche.

Désormais la recherche s'opère sur la chaîne exacte. Il faudra ajouter le caractère "*" manuellement si nécessaire.

De plus la recherche d'utilisateurs s'opère maintenant sur plus d'attributs : le nom de connexion Windows ou le nom DNS.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.10

Support de Windows 10 CBB

Stormshield Endpoint Security supporte désormais les systèmes d'exploitation Microsoft Windows 10 CBB. L'ensemble des fonctionnalités et dispositifs de sécurité de Stormshield Endpoint Security sont disponibles sur ces nouvelles plate-formes.

> **ATTENTION**
> Aucune protection n'est appliquée par Stormshield Endpoint Security concernant les processus faisant partie de la fonctionnalité WSL (Windows Subsystem for Linux) disponible avec la mise à jour de Windows 10 de Juillet 2016. Ces processus pourraient donc compromettre l'intégrité du produit Stormshield Endpoint Security ainsi que du poste de travail s'ils étaient utilisés à mauvais escient. Il est donc recommandé de n'activer cette fonctionnalité qu'en cas de besoin et de manière ponctuelle.

Affichage du numéro de série des nouvelles licences dans la console SES

Dorénavant, pour les licences qui possèdent un numéro de série, celui-ci est affiché dans le gestionnaire des licences et dans le menu de mise à jour des licences.

Serveurs mutualisés

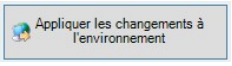
Un même serveur SES peut désormais gérer un annuaire interne et un annuaire Active Directory. L'installation du produit doit se faire au préalable en mode Active Directory. Dans le cas où un agent appartient aux deux annuaires, un nouveau paramètre permet de gérer la priorité des annuaires (menu **Environnement**, onglet *Paramètres*).

Protection contre l'élévation de privilèges

L'agent SES protège désormais le poste de travail contre l'usurpation et la modification frauduleuse du contexte de sécurité d'un processus. Ce nouveau mécanisme est intégré dans la protection contre l'élévation de privilèges. De plus, la console SES permet maintenant de choisir entre trois niveaux de protection contre l'élévation de privilèges : Désactivé/Haut/Critique. Si l'option était activée avant la mise à jour, le niveau Critique sera sélectionné en 7.2.10.

Pour le détail des niveaux, reportez-vous au chapitre 9 du *Guide d'administration* 7.2, section *Comportement Système*.

Synchronisation des environnements

Dans la console SES, l'ancien bouton **Synchroniser**  qui permettait de déployer les politiques et configurations du serveur vers les agents SES a été remplacé par un nouveau bouton **Appliquer les changements à l'environnement** 

de façon à être plus visible et plus explicite.

Ajout d'actions sur détection d'événement

Il est désormais possible de mettre en place des actions à exécuter lorsqu'un événement particulier se produit sur un agent SES, grâce à des scripts associés à des logs dans l'Éditeur de logs de la console SES. Dès lors qu'un log donné est remonté par un agent, le script associé est exécuté.

Ergonomie de la console

Dans la console SES, la zone éditable d'un champ est désormais de couleur blanche et entourée d'un cadre bleu, de façon à être plus visible.

Priorité des politiques appliquées par script

Dorénavant, les politiques de configuration dynamique de l'agent et les politiques de sécurité paramétrées dans des scripts seront appliquées selon un nouvel ordre en fonction de leur source d'application. Le nouvel ordre d'application est le suivant, du plus prioritaire au moins prioritaire : challenges (dans la configuration statique de l'agent), actions sur détection (dans l'éditeur de logs), scripts et politiques liées (dans un environnement).

Gestion des politiques de chiffrement

Dans la console SES, la suppression d'une politique de chiffrement appliquée à des agents pouvait accidentellement déchiffrer des postes de travail. Afin d'éviter ceci, dorénavant un agent conserve sa politique de chiffrement courante jusqu'à l'application explicite d'une nouvelle politique. Ainsi, pour déchiffrer une machine utilisant le chiffrement total du disque, il faut désormais lui appliquer une politique de chiffrement dont le chiffrement total du disque est désactivé.

Nouveau paramètre pour les applications de confiance

Dans la console SES, pour les applications de confiance d'une politique de sécurité, une nouvelle colonne **Champ d'application** permet désormais de choisir de propager la confiance à l'application seule ou à l'application et ses enfants. Ce paramètre est disponible en mode avancé uniquement.

Correctifs de Stormshield Endpoint Security 7.2.10

Correctifs agent

Référence support 10546

Compatibilité entre l'agent SES et le produit Stormshield Data Security for Cloud & Mobility

Lorsque l'on désinstallait un agent SES d'un poste également équipé de Stormshield Data Security for Cloud & Mobility, ce dernier pouvait devenir instable. Ce problème est résolu.

Référence support 10756 (#CF 87031)

Désinstallation de l'agent SES en mode sans échec avec prise en charge réseau

Le système pouvait cesser de fonctionner (écran bleu) lorsque l'on désinstallait l'agent SES en mode sans échec avec prise en charge réseau. Ce problème est résolu.

Référence support 10495 (#CF 86854)

Compatibilité entre l'agent SES et l'antivirus Sophos

Lorsque l'agent SES était installé sur le même poste que Sophos, certaines applications pouvaient arrêter de fonctionner. Ce phénomène aléatoire était provoqué par un accès concurrent entre Stormshield Endpoint Security et Sophos lors de l'installation des protections. Ce problème est résolu.

Référence support 10635

Validation automatique de l'accès temporaire au web

Lorsque vous créez un raccourci sur le bureau de l'utilisateur pour demander un accès temporaire au web (argument "/GrantWebAccess" ajouté dans la cible du raccourci de l'exécutable *ssmon.exe*), vous pouvez désormais ajouter l'option "/NoConfirm" afin de désactiver la fenêtre de confirmation de l'accès au web. L'accès est alors immédiatement effectif.

Référence support 10458

Faux positifs sur la protection (lecture seule) des clés de registre

Lorsqu'une clé de registre était en accès lecture seule dans les règles applicatives dans la console SES, un log était généré pour chaque accès à la clé sur le poste de travail. Désormais, un log ne sera généré que pour une tentative d'accès en écriture.

Référence support 10594

Suppression de la protection implicite contre le renommage

Lorsqu'un identifiant d'application par chemin était lié à une règle applicative, un fichier correspondant à l'identifiant d'application ne pouvait plus être ni renommé ni supprimé. Ce problème est résolu.

Référence support 10701 et 10862

Compatibilité avec le navigateur Firefox versions 47 et supérieures

Le navigateur Firefox en versions 47 et supérieures ne fonctionnait pas correctement sur un poste de travail équipé d'un agent SES. Ce problème est résolu.

Référence support 10863

Accès à une valeur d'une clé de registre protégée

Lorsque un programme tentait de modifier la valeur « UpperFilters » de la clé de registre "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E967-E325-11CE-BFC1-

08002BE10318}", l'accès lui était refusé. Désormais, il est possible d'y écrire des valeurs compatibles avec le fonctionnement de SES.

Référence support 10877 (#CF 87170)

Corruption du fichier main.srx sur le poste de travail

Sur un poste de travail équipé de l'agent SES, lorsque le fichier *main.srx* était corrompu, invalide ou inexistant, l'agent était incapable d'appliquer les politiques courantes. Ce problème est résolu. Si un fichier *srx* du dossier Batch est corrompu, invalide ou inexistant, l'agent téléchargera de nouveau l'ensemble des politiques.

Référence support 10724

Mise à jour de libxml2 en version 2.9.4

La version de libxml2 utilisée par Stormshield Endpoint Security pour la gestion des fichiers XML a été mise à jour en version 2.9.4. La version 2.9.3 présentait des failles de sécurité.

Correctifs serveur

Référence support 10740 et 10345

Temps de connexion agent/serveur

La communication entre les agents et le serveur SES a été améliorée et le temps de connexion ainsi réduit. En effet, la communication était lente lorsque de petites quantités de données étaient échangées. Le serveur pouvait également se trouver surchargé car des agents qui se déconnectaient et reconnectaient pouvaient être comptés plusieurs fois.

Référence support 10782 (#CF 86613)

Gestion des connexions du serveur

Lorsque beaucoup d'agents SES se connectaient simultanément au serveur, celui-ci ne parvenait pas à traiter toutes les demandes de connexion. Les agents ne pouvaient alors plus se connecter et le serveur était indisponible. Ce problème est résolu.

Référence support 10705 (#CF 87063)

Indisponibilité du serveur web HTTP

Selon l'environnement logiciel présent sur le poste qui hébergeait le serveur SES, la version 2.4 du serveur Web Apache fournie depuis la version 7.2.07 de SES pouvait connaître un état instable et refuser la quasi-totalité des connexions entrantes.

Correctifs console

Référence support 9062 et 10763

Choix de la langue de la console à l'installation

Lors du premier démarrage de la console SES, la langue par défaut était l'anglais même si une autre langue était choisie au moment de l'installation du produit (français, espagnol, portugais ou allemand). Ce problème est résolu.

Référence support 10698

Menu Aller à la règle dans les logs

Dans le panneau des logs de la console SES, le menu contextuel **Aller à la règle** accessible depuis un clic droit sur un log particulier pouvait ne pas fonctionner en mode de rafraîchissement automatique. Ce problème est résolu.

Référence support 10672

Copie d'un groupe dans la politique de sécurité

Dans les onglets *Contrôle des périphériques* et *Contrôle de la sécurité réseau* des politiques de sécurité dans la console SES, la copie d'un groupe ne fonctionnait plus. Ce problème est résolu.

Référence support 10400

Menu Copier la cellule dans les logs

Dans le panneau des logs de la console SES, le menu contextuel **Copier la cellule** accessible depuis un clic droit sur un log particulier ne fonctionnait pas correctement. Ce problème est résolu.

Référence support 10011

Affichage de la version du système d'exploitation d'un agent 7.1 dans une console 7.2

Dans le panneau **Surveillance des agents** d'une console SES 7.2, la version du système d'exploitation affichée pour chaque agent pouvait être incorrecte si la version de l'agent était antérieure à la version 7.2. Ce problème est résolu.

Référence support 10636

Utilisation des filtres dans les logs

Une erreur s'affichait lorsque de trop nombreux filtres simples étaient sélectionnés dans les panneaux de logs de la console SES. Désormais la zone d'affichage des filtres est limitée en taille et une barre de défilement apparaît en cas de besoin.

Référence support 10537

Panneau d'aide pour le format des dates

Dans le panneau de configuration de la console SES, lorsque vous saisissez un format d'affichage de date, une aide en bas du panneau traduit désormais la valeur du champ en date. Par exemple, "G" est égal à "15/06/2009 13:45:30 PM".

Référence support 10812

Test intégré sur un groupe Active Directory

Lors de la mise en place d'un test intégré sur un groupe Active Directory dans la console SES, il n'était plus possible de saisir un nom de domaine dans les propriétés du test. Ce problème est résolu.

Référence support 10202

Priorités des logs dans l'éditeur de logs

Le changement de priorité des logs dans l'éditeur de logs de la console SES n'était pas pris en compte lorsqu'un filtre sur l'affichage des logs était actif. Ce problème est résolu. Le changement de priorité ne tient compte que des logs affichés sur le moment.

Référence support 10896

Réorganisation du Gestionnaire des rôles

Le panneau des permissions dans le Gestionnaire des rôles de la console SES a été revu. Les permissions sont désormais triées dans le même ordre que les catégories de la console, et les permissions "Créer et modifier les certificats" et "Créer et modifier les politiques de sécurité" ont été fusionnées.

Correctifs de Stormshield Endpoint Security 7.2.09

Correctifs agent

Référence support 10805 (#CF 87125)

Blocage de l'installation de certaines mises à jour Windows

L'installation de mises à jour Windows pouvait être bloquée par l'agent SES lorsque ces mises à jour accédaient à des clés sensibles de la base de registre. Ce problème est résolu.

Référence support 10803

Compatibilité avec le client VPN TheGreenBow

Le pare-feu SES et le client VPN TheGreenBow pouvaient être incompatibles lorsque l'option du client VPN **Bloquer les flux non chiffrés** était activée. Ce problème est résolu.

Correctifs de Stormshield Endpoint Security 7.2.08

Correctif serveur

Référence support #CF 87063

Serveur Web HTTP indisponible

Selon l'environnement logiciel présent sur le poste qui héberge le serveur SES, la version 2.4 du serveur Web Apache livré depuis SES 7.2.07 pouvait refuser la quasi-totalité des connexions entrantes. Ce problème est résolu.

Mises à jour de Stormshield Endpoint Security 7.2.08

Référence support 10685

Mise à jour de OpenSSL

Une vulnérabilité (CVE-2016-2107 - Attack against an AES CBC session implemented with AES-NI) a été corrigée par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.2h.
Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.07

Support de Windows 10 LTSB

Stormshield Endpoint Security supporte désormais les systèmes d'exploitation Microsoft Windows 10 LTSB. L'ensemble des fonctionnalités et dispositifs de sécurité de Stormshield Endpoint Security sont disponibles sur ces nouvelles plate-formes.

Sélection des logs à envoyer sur un serveur SMTP ou Syslog

Auparavant, l'ensemble des logs était envoyé soit sur un serveur SMTP soit sur un serveur Syslog. Désormais, vous pouvez choisir d'utiliser les deux types de serveur simultanément et sélectionner les types de logs à envoyer sur l'un ou l'autre des serveurs. Ce choix s'effectue dans la politique de configuration dynamique de l'agent et dans l'éditeur de logs.

> **ATTENTION**
> Après la mise à jour de votre console en version 7.2.07, veillez à vérifier le paramètre **Activer les logs d'autoprotection** dans les configurations dynamiques des agents. La gestion désormais séparée des serveurs SMTP et Syslog peut modifier votre paramétrage. La configuration recommandée est "fpdlm" (toutes options désactivées). Pour plus d'informations, reportez-vous au *Guide d'administration 7.2*.

Notification de l'expiration proche du mot de passe de chiffrement total du disque

Des messages d'avertissement s'affichent désormais sur le poste de travail de l'utilisateur 20 jours, 10 jours, 5 jours et un jour avant l'expiration de son mot de passe de chiffrement. Ils permettent à l'utilisateur de modifier directement le mot de passe et d'être averti de sa prochaine expiration.

Raccourci pour accéder temporairement au web

Il est désormais possible de créer un raccourci sur le bureau de l'utilisateur pour demander rapidement un accès temporaire au web. Il faut créer un raccourci de l'exécutable de l'interface graphique de l'agent *ssmon.exe* sur le bureau, puis ajouter l'argument "/GrantWebAccess" dans la cible du raccourci. Ce raccourci permet de ne pas passer par le menu Stormshield Endpoint Security accessible depuis la barre d'état système. Pour plus d'informations, consultez le *Guide d'administration 7.2*.

Ajout d'un champ de recherche dans le panneau de surveillance des agents

Un champ de recherche dans le panneau **Surveillance des agents** de la console permet désormais de retrouver plus rapidement des agents. La recherche s'opère automatiquement sur les colonnes **Nom de machine**, **Nom AD**, **Adresse IP**, etc.

Ajout d'un panneau permettant de voir les emplacements d'assignation des serveurs

Un sous-panneau a été ajouté au panneau **Serveurs Stormshield Endpoint Security**. Lors de la sélection d'un serveur, il liste l'ensemble des emplacements auxquels est assigné le serveur sélectionné.

Ajout des paramètres Version d'agent minimale autorisée et Version d'agent maximale autorisée

Deux paramètres dans la configuration du serveur permettent désormais aux serveurs de bloquer la communication avec des agents de versions différentes de la leur. Reportez-vous au *Guide*

d'administration 7.2 pour plus d'informations.

Correctifs de Stormshield Endpoint Security 7.2.07

Correctifs agent

Référence support 9661

Logs de la protection HoneyPot en mode Warning

Lorsque le mode Warning était activé sur l'agent SES, les logs de blocage de la protection HPP n'apparaissaient pas. Ce problème est résolu.

Référence support 9836 (#CF 86559)

Erreur d'exécution de l'agent SES

Dans certaines circonstances, une corruption du fichier *Sigs.srn* pouvait entraîner une erreur d'exécution de l'agent SES (framework.exe). Ce problème est résolu. Un log système de type SIG_ERROR sera remonté dans ce cas.

Référence support 9127

Protection des fichiers SES en mode Warning et StandBy

Les fichiers SES (*.sra, *.srn, *.sro, *.srx, *.srxml) sont désormais protégés par extension en mode Warning et StandBy. La protection est effective dans les mêmes conditions qu'en mode Normal, c'est-à-dire tant que l'agent est activé et 20 secondes après sa désactivation.

Référence support 8903

Génération de log en cas d'échec de la première connexion au serveur Active Directory

Désormais, lorsqu'un agent SES en mode Active Directory se connecte pour la première fois au serveur AD et si la connexion échoue, un log est généré.

Référence support 8905

Application de politiques lorsque le serveur SES est injoignable

Lorsque l'agent SES est déconnecté du serveur, les conditions d'application de politiques au sein d'un groupe d'agents sont à présent évaluées à chaque tentative de reconnexion au serveur afin de savoir quelles politiques appliquer.

Référence support 9970

Suppression du fichier sr_footprint après révocation d'une clé USB

Lorsqu'une clé USB était révoquée depuis une console d'administration installée sur un poste de travail équipé d'un agent SES, le fichier *sr_footprint* n'était pas supprimé. Ce problème est résolu. Désormais, après une révocation de clé, celle-ci est également éjectée par la console.

De plus, un avertissement prévient maintenant lorsque la clé USB n'est pas détectée par la console lors de sa révocation.

Référence support 10118 (#CF 86724)

Compatibilité avec ESET

Le produit ESET Endpoint Antivirus ne pouvait pas être installé sur un poste de travail équipé d'un agent SES Professional Edition. Ce problème est résolu.

Référence support 10190 (#CF 86466)

Compatibilité avec le client VPN TheGreenBow

Le client VPN TheGreenBow (version 5.22 et supérieure) ne fonctionnait pas correctement quand la fonctionnalité Firewall de SES était activée sur l'agent. Ce problème est résolu.

Référence support 10324 (#CF 86833 et 86856)

Connexion à un serveur StormShield 6.0 lors d'une migration partielle

Lors d'une migration partielle de la version 6.0 vers la version 7.2, il pouvait arriver que les agents 7.2 se connectent de nouveau à l'ancien serveur 6.0. Ce problème est résolu.

Références support 10100 et 10103

Erreur d'exécution de l'agent SES lorsque la connexion réseau est instable

Lorsque la connexion entre l'agent et le serveur SES était instable en raison de perte de paquets réseau, latences, etc., l'exécution de l'agent (framework.exe) pouvait se terminer. Ce problème est résolu.

Correctifs serveur

Référence support 10346

Connexion impossible des agents au serveur SES

Les agents ne parvenaient plus à communiquer avec le serveur SES lorsque lui-même ne pouvait plus communiquer avec son serveur de base de données de logs et de surveillance. Ce problème est résolu.

Référence support 10505

Connexion des agents SES au serveur sans synchronisation

Après une installation de serveur et d'agents SES, il pouvait arriver que le serveur cesse de fonctionner lorsqu'un agent se connectait alors qu'il n'y avait jamais eu de synchronisation opérée depuis la console d'administration. Ce problème est résolu.

Correctifs console

Référence support 10137 (#CF 86753)

Impossibilité de synchroniser les serveurs SES depuis la console

La synchronisation des serveurs SES échouait lorsque le temps que mettait la console d'administration à récupérer les informations de configuration depuis la base de données et à générer les fichiers à envoyer aux serveurs était trop long. Ce problème est résolu.

Référence support 9894 (#CF 86233)

Gestion des espaces de noms disjoints pour l'ajout d'utilisateurs

Il est désormais possible d'ajouter un utilisateur Active Directory dont le nom DNS du domaine et le nom NetBIOS du domaine sont différents (espaces de noms disjoints) dans les utilisateurs de la console.

Référence support 5252

Classement des ressources de script par ordre alphabétique

Les tests et les actions dans les ressources de script sont désormais ordonnés par ordre alphabétique et non plus selon leur ordre de création.

Référence support 8394

Configurations et politiques non récupérées par l'agent défini par un nom NetBios

Un agent défini par un nom NetBios comportant des minuscules ne pouvait pas récupérer les configurations et politiques sur le serveur SES. Ce cas se produisait en mode annuaire interne uniquement, avec une configuration des groupes d'agents par nom NetBios. Ce problème est résolu.

Référence support 10323

Démarrage de la console d'administration impossible avec une licence expirée

En mode annuaire interne seulement, lorsque la licence SES arrivait à expiration, un message d'erreur s'affichait et la console d'administration ne démarrait pas. Ce problème est résolu.

Référence support 10354 (#CF 86759)

Lenteurs lors du chargement du Tableau de bord de la console d'administration

Le chargement du tableau de bord pouvait entrainer des lenteurs. La correction apportée améliore les performances de la console mais ne résout pas le problème sur des bases de données très volumineuses.

Mises à jour de Stormshield Endpoint Security 7.2.07

Référence support 9947

Ajout de variables dans les logs

Les variables %CERT%, %MD5% et %SHA1% ont été ajoutées dans les logs Système afin d'afficher des informations supplémentaires sur la source dans les messages. Reportez-vous au *Guide d'administration 7.2* pour consulter les exemples d'utilisation du gestionnaire de logs.

Référence support 10150

Mise à jour de OpenSSL

OpenSSL a été mis à jour en version 1.0.2g.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.06

AVERTISSEMENT
La version 7.2.06 est actuellement en cours de certification Critères Communs et n'est pas encore rendue publique.

Génération aléatoire des clés de chiffrement

Une nouvelle étape a été ajoutée dans la procédure d'installation d'un serveur Stormshield Endpoint Security. L'utilisateur doit déplacer aléatoirement la souris afin d'augmenter l'aléa pour la génération des clés de chiffrement servant au chiffrement total du disque.

Correctifs de Stormshield Endpoint Security 7.2.06

Correctifs agent

Référence support 9286

Remontée des logs agent au serveur pendant l'arrêt de la machine

Lors de l'arrêt d'une machine, des logs concernant des événements en cours pouvaient ne pas être envoyés au serveur. Le problème est corrigé : pendant la phase d'arrêt, tous les logs sont désormais stockés dans un fichier qui sera envoyé au serveur au cours du prochain démarrage de la machine.

Références support 9285, 9708

Chiffrement total de disque : problème de création du compte invité depuis l'agent

Le compte invité (GUEST) ne pouvait être créé depuis l'agent SES après le changement des mots de passe des comptes de chiffrement USER et ADMIN. Il ne pouvait pas non plus être créé par le compte USER si celui-ci avait une validité d'une heure seulement. La possibilité de créer le compte invité dépend désormais uniquement des droits donnés dans la politique de chiffrement.

Référence support 9543

Erreur lors du recouvrement des données

À la suite d'un recouvrement de données d'une machine chiffrée via le média de recouvrement, le poste pouvait devenir inutilisable. Ce problème pouvait arriver si l'option **Chiffrement des partitions** dans la politique de chiffrement avait été modifiée au fil du temps. Les informations sont maintenant correctement récupérées pour effectuer le déchiffrement du disque en utilisant le média de recouvrement.

Référence support 9883

Amélioration de la fenêtre d'expiration du mot de passe de chiffrement

La demande de renouvellement du mot de passe de chiffrement après son expiration est désormais plus explicite pour l'utilisateur. Le bouton **Annuler** de cette fenêtre a également été grisé afin d'obliger l'utilisateur à changer son mot de passe.

Références support 8938, 9366, 9222, 9224, 9367, 9654, 9223

Ajout de logs pour le suivi du chiffrement total de disque

Les logs logiciels suivants concernant le chiffrement total de disque ont été ajoutés :

- Partitions chiffrées : à la fin du chiffrement ou du déchiffrement total de disque, un log reporte les partitions qui viennent d'être chiffrées ou déchiffrées.
- Échecs et succès lors de l'identification au démarrage du poste dont le disque est chiffré.
- Création/suppression d'un compte invité : un log indique le type de compte de chiffrement (utilisateur, administrateur ou invité) connecté lors de la création ou suppression du compte invité.
- Report du chiffrement total de disque.
- Changement de mot de passe utilisateur via le média de recouvrement.
- Mise à jour des éléments de recouvrement.
- Remise en clair du disque : un log précise que l'opération de déchiffrement via le média de recouvrement est terminée.

Correctifs serveur

Référence support 9688

Mise à jour automatique de la configuration d'Apache

Lors de l'installation d'une nouvelle version du serveur SES, les fichiers de configuration d'Apache n'étaient pas regénérés ce qui empêchait le serveur Apache de démarrer proprement. Il fallait le faire manuellement avec l'outil *skyapache.exe*. La génération des fichiers de configuration d'Apache se fera automatiquement lors de la mise à jour du serveur SES 7.2.06 vers une version supérieure.

Référence support 8556

Page web de téléchargement de certificats

La page web de téléchargement de certificats était accessible en HTTPS (sécurisé) et HTTP (non sécurisé). Seul l'accès sécurisé est conservé.

Référence support 9601

Log indiquant l'envoi des politiques du serveur vers les agents

Un log apparaît désormais dans le fichier *output.sro* sur le serveur pour indiquer que le serveur SES vient d'envoyer les configurations et politiques à un agent.

Correctif console

Référence support 9599

Log indiquant la génération des éléments de recouvrement

Un log apparaît désormais lorsque les éléments de recouvrement sont générés par le serveur pour un agent. Ce log est par défaut visible dans la partie Logs logiciel de la console.

Mises à jour de Stormshield Endpoint Security 7.2.06

Références support 8556, 9857, 9895

Mise à jour de OpenSSL et Apache

Le composant OpenSSL a été mis à jour afin d'utiliser la version 1.0.2e et le composant Apache a été mis à jour en version 2.4.18.

La mise à jour du serveur SES depuis une version antérieure à la version 7.2.06 n'entraîne pas les mises à jour de configuration du serveur Apache. Vous devez appliquer manuellement cette mise à jour en exécutant la commande «skyapache.exe - - update» situé dans *Program Files\Stormshield\Stormshield Endpoint Security Server\Apache\conf* depuis une ligne de commande administrateur. Les anciens fichiers de configuration sont renommés en *httpd.conf.old* et *ssl.conf.old*. Le serveur SES doit être redémarré pour la prise en compte de ces modifications.

Par ailleurs, il n'est plus possible d'utiliser Internet Explorer 8 sur Windows XP pour télécharger un certificat (https://ip_du_serveur/ssl/cgi). Un navigateur plus récent est requis pour atteindre cette page.

Référence support 8889

Amélioration de la sécurité pour les informations de recouvrement

Les données de recouvrement pour le chiffrement total de disque sont désormais authentifiées avec l'algorithme PBKDF2-HMAC-SHA512 et chiffrées à l'aide d'une clé générée avec PBKDF2-HMAC-SHA512.

Référence support 8504

Suites de chiffrement

Le serveur SES supporte désormais les suites de chiffrement ECDHE-RSA-AES256-SHA et ECDHE-RSA-AES256-SHA384.

Référence support 9626

Amélioration de la sécurité lors de l'authentification sur un disque chiffré

Désormais, le protocole d'authentification utilise l'algorithme PBKDF2 afin d'améliorer la sécurité de l'étape d'authentification . Lors d'une mise à jour depuis une version n'utilisant pas ce protocole, le mot de passe USER devra être renouvelé afin de procéder à la mise en place de ce nouveau processus. Il n'y a pas de déchiffrement du disque pendant la mise à jour.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.05

Prise de traces d'exécution

Il est maintenant possible d'enregistrer des traces en cas de problèmes rencontrés lors de l'utilisation de l'agent SES et de fournir au support Stormshield Endpoint Security des informations utiles à l'analyse des problèmes via le Gestionnaire de traces.

Reportez-vous au *Guide d'administration* pour plus d'informations sur le Gestionnaire de traces.

Correctifs de Stormshield Endpoint Security 7.2.05

Correctifs agent

Référence support 9420

Demande de redémarrage répétitive

Lors de l'installation d'un agent Secure Edition, un redémarrage est obligatoire. Après le redémarrage, l'agent proposait continuellement de redémarrer le poste. Ce problème est résolu.

Référence support 8979

Filtrage réseau avec plusieurs adresses IP

Dans une configuration avec une interface réseau portant plusieurs adresses IPv4, le filtrage réseau pouvait mal fonctionner. Ce problème est résolu.

Référence support 6010

Date/Heure dans les logs émis via Syslog

Les logs externes émis via Syslog comprenaient une date et une heure (timestamp) correspondant aux date et heure d'émission par le serveur SES. Maintenant, elles correspondent aux date et heure auxquelles le log a été généré par l'agent.

Référence support 9097

Amélioration de l'autoprotection de l'agent en mode Warning

L'autoprotection des clés de registre de l'agent a été améliorée lorsque ce dernier est en mode Warning.

Référence support 9580

Écran bleu lors du renommage d'une clé de registre en mode Warning

Lorsque l'agent était en mode Warning, un écran bleu pouvait survenir lors du renommage de clés de registre. Ce problème est résolu.

Référence support 8827

Changement de la description de l'identifiant d'application de *ssmon.exe*

L'identifiant d'application de *ssmon.exe* avait pour description «StormShield Monitor ». La description a été modifiée en « Stormshield Endpoint Monitor ».

Référence support 9016

Suppression des latences LDAP avant l'application des politiques par l'agent

Lors du téléchargement de politiques par l'agent, celui-ci les applique directement puis met à jour ses informations LDAP. Ainsi, la latence de connexion au serveur LDAP est réduite.

Référence support 9571 (#CF 86480)

Ouverture de connexion RDP sur Windows XP et Windows Server 2003

L'activation de certaines protections contre le débordement de mémoire empêchait la prise en main à distance avec l'outil de Microsoft (*mstsc.exe*) sur Windows XP et Windows Server 2003. Ce problème est résolu.

Correctif serveur

Référence support 9329 (#CF 86052)

Mauvaise version du serveur dans le panneau Programmes et Fonctionnalités après une mise à jour

La version du serveur dans le panneau des **Programmes et Fonctionnalités** est désormais correcte après une mise à jour.

Correctifs console

Référence support 9329 (#CF 86052)

Mauvaise version de la console dans le panneau Programmes et Fonctionnalités après une mise à jour

La version de la console dans le panneau des **Programmes et Fonctionnalités** est désormais correcte après une mise à jour.

Référence support 9314

Modification de la valeur par défaut de la taille de clé de chiffrement

Lors de la création d'une nouvelle politique de chiffrement, la taille de la clé de chiffrement par défaut est maintenant 256, au lieu de 128 précédemment.

Référence support 9293

Affichage des modifications de politiques dans l'observateur d'événements

Dans l'observateur d'événements de la console, lorsqu'une politique était modifiée, seule l'icône s'affichait dans les colonnes des valeurs modifiées. Le texte accompagnant l'icône manquait.

Désormais, lorsqu'une modification dans une politique est validée, l'icône et le texte lié à cette icône s'affichent correctement dans l'observateur d'événements.

Référence support 9427

Édition d'un rôle dans la console

Lors de l'édition d'un rôle dans la console, si on validait le rôle sans avoir fait de modification ou si on quittait la console, une exception survenait. Ce problème est résolu.

Référence support 9237

Prise en compte après validation des modifications des informations sur les groupes d'agents en annuaire interne

La première validation ne prenait pas en compte les modifications apportées. La validation et la synchronisation des informations avec la base de données ont été corrigées.

Référence support 8962

Installation et mise à jour de la console sur un poste possédant un agent SES

Une erreur survenait lors de l'installation, la mise à jour ou la désinstallation d'une console lorsqu'un agent était présent sur le poste de travail. Ce problème est résolu.

Référence support 9199

Bouton de sélection d'un élément de l'Active Directory dans les ressources de scripts

Dans les ressources de scripts, il n'était plus possible de sélectionner un utilisateur ou un groupe de l'Active Directory à l'ajout d'un test intégré de type « Domaine ». Ce problème est résolu.

Référence support 9302

Logs d'erreurs SRService erronés

Lors de l'installation d'un agent, des logs d'erreurs SRService étaient générés au redémarrage de la machine. Ces erreurs apparaissaient même dans le cas où l'installation s'était bien passée et qu'aucune erreur n'avait été rencontrée. Ces logs d'erreurs ont été supprimés et n'apparaissent plus en cas d'installation réussie de l'agent.

Référence support 9465

Message d'erreur lors de la mise à jour de la console utilisée par plusieurs sessions Windows

Lorsque plusieurs utilisateurs sont connectés à la console sur un même poste, la mise à jour de la console est impossible. Un message d'erreur était généré mais ne précisait pas qu'il fallait vérifier si d'autres utilisateurs étaient connectés à la console. Le message d'erreur demande désormais de vérifier si d'autres sessions Windows utilisant la console ou l'installeur de base de données ne sont pas en cours sur le poste.

Référence support 9484

Graphique de configuration des agents

Le graphique de configuration des agents dans le tableau de bord ne prenait pas en charge l'échelle de tendance. Ce problème est résolu.

Référence support 9577

Sélection de la valeur pour l'interface réseau active dans les ressources de scripts

Depuis la version 7.2, certains éditeurs graphiques n'étaient plus disponibles dans les ressources de scripts. Ces éditeurs ont été réintégrés.

Référence support 9582

Installation de SES en annuaire interne avec une licence expirée

Lors de l'installation d'un environnement SES, si la licence d'évaluation utilisée avait expiré, l'installation échouait sans indiquer de raison. Ce problème est résolu.

Référence support 9585

Erreur de traduction du menu contextuel Afficher les logs dans l'annuaire AD

Dans une console en espagnol ou en portugais, le menu contextuel permettant d'afficher les logs d'un objet AD sélectionné affichait quatre fois la même option, sans indiquer le type de log à sélectionner. Ce problème est résolu.

Référence support 8753

Sélection du nœud dans les scripts et dans les ressources de scripts par clic droit

Le mauvais menu contextuel s'ouvrait via le clic droit de la souris lors de la sélection sur une condition, un test, un résultat (vrai/faux) ou une action. Ce problème est résolu.

Référence support 7294

Ajout de la variable d'environnement |programfilesnative|

Jusqu'à présent, il n'existait que la variable d'environnement |programfiles| pour faire référence à un identifiant d'application pour le contrôle applicatif.

|programfiles| ne permettait de pointer que les chemins de « Program Files » 32 bits. Désormais la variable |programfilesnative| permet de faire référence au chemin « Program Files » natif. Il s'agira toujours de « C:\Program Files » que ce soit sur système d'exploitation 32 ou 64 bits.

Référence support 9680

Exception dans la console lors d'une copie de cellule vide

Dans les logs système, la console renvoyait une exception lorsqu'on copiait une cellule vide. Ce problème est résolu.

Référence support 9696

Interprétation des expressions régulières définies dans l'éditeur de logs

Les expressions régulières permettant de choisir les messages de logs définies dans l'éditeur de logs n'étaient pas interprétées de la même manière par la console et l'agent. Ce problème est résolu.

Référence support 8410

Statuts de synchronisation dans un environnement multi-serveurs

Dans certains cas, lors d'une synchronisation avec plusieurs serveurs, la fenêtre **Serveurs** affichait pour tous les serveurs sauf un l'état « Synchronisation échouée », même dans le cas où les serveurs étaient correctement synchronisés.

Référence support 8826

Comportement de la recherche dans l'annuaire AD

Désormais, lorsqu'une recherche dans l'annuaire AD renvoie trop de résultats, seuls les 50 premiers sont affichés. De plus, une icône de statut est affichée à côté du nœud racine de la recherche et une info-bulle indique qu'il faut préciser la recherche.

Référence support 9705

Suivi des modifications des messages de log dans l'observateur d'événements

L'ajout et la suppression des messages de log dans l'éditeur de logs n'étaient pas correctement renseignés dans l'observateur d'événements. De plus, les nouveaux logs sont maintenant affichés en italique jusqu'à leur première validation afin de les repérer plus simplement lors de l'édition.

Référence support 9482

Réapparition de règles applicatives supprimées

Après la suppression de règles applicatives depuis le nœud principal, ces dernières pouvaient réapparaître lors de la sélection d'un groupe ou lors de la validation de la politique. Ce problème est résolu.

Référence support 9621

Ajout d'identifiants sur des règles applicatives dans une politique qui n'est pas en édition

Il était possible de lier un identifiant d'application à une règle applicative même si la politique n'était pas en édition, ce n'est désormais plus le cas.

Référence support 9502

Définition d'un identifiant d'application commençant par « *:\ »

Il est de nouveau possible de définir un identifiant d'application ne tenant pas compte de la lettre de lecteur (« *:\ »).

Référence support 8467

Ajout de règles applicatives ou de pare-feu sur le nœud principal des groupes

Il n'est désormais plus possible d'ajouter des règles sur les nœuds principaux des différentes règles de la politique de sécurité.

Référence support 9734

Glisser-déposer pour les ressources de scripts

Depuis la version 7.2, il n'était plus possible d'effectuer un glisser-déposer pour déplacer des éléments constituant un script (tests, actions, conditions). Les panneaux impactés étaient les ressources de scripts et les politiques de scripts. Ce problème est résolu.

Référence support 9651 (#CF 86289)

Écran bleu dû au contrôle applicatif

Un écran bleu pouvait subvenir sur le poste de travail lors du lancement d'un binaire si il y avait beaucoup de règles applicatives dans la politique de sécurité. Ce problème est résolu.

Mises à jour de Stormshield Endpoint Security 7.2.05

Référence support 9749

Intégration de nouvelles fonctions de configuration d'AVIRA

- Le paramètre **Afficher les messages d'avertissement** a été ajouté pour les composants 'Scanner', 'Protection Temps réel' et 'Protection Web' de la configuration Antivirus.
- Le paramètre **Répertoire de quarantaine** a été ajouté dans les paramètres généraux de la configuration Antivirus.
- Il n'est plus nécessaire d'être administrateur pour démarrer une procédure de scan par Avira.

Référence support 8237

Protection Stack Pivot pour les processus 64 bits

La protection contre les attaques dites de « stack pivot » a été renforcée afin de protéger également les processus 64 bits.

Référence support 9753

Mise à jour de libxml2 en version 2.9.3

La version de libxml2 utilisée précédemment (2.9.2) pour la gestion des fichiers XML présentait des failles de sécurité. La version utilisée par SES est la version la plus récente à ce jour (2.9.3).

Référence support 9710

Mise à jour d'OpenSSL en version 1.0.1q

La version d'OpenSSL utilisée précédemment (1.0.1p) contenait une vulnérabilité permettant potentiellement à un attaquant de provoquer un déni de service sur le serveur SES. La version utilisée par SES a été mise à jour en version 1.0.1q.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2.04

Tableau de bord

L'écran d'accueil de la console d'administration SES présente désormais un tableau de bord. Quatre graphiques permettant de surveiller l'état du parc d'agents composent le tableau de bord. Chaque graphique est détachable pour faciliter le suivi multi-écrans.

Le tableau de bord est également accessible depuis le menu **Gestionnaires** de la console.

Reportez-vous au *Guide d'administration* pour plus d'informations sur le tableau de bord.

Évolution de l'affichage des logs dans la console d'administration SES

L'ancien panneau **Surveillance des logs** a été remplacé par le menu principal **Tableau de bord** dans le panneau **Gestionnaires** de la console, et par les quatre sous-menus **Logs Logiciel**, **Logs Système**, **Logs Réseau** et **Logs Périphérique**.

Cette amélioration permet principalement de faire des recherches pertinentes sur les logs grâce aux filtres simples et avancés.

Reportez-vous au *Guide d'administration* pour plus d'informations sur l'affichage des logs.

Support de Windows Server 2003 SP2 et R2 SP2

Stormshield Endpoint Security supporte désormais les systèmes d'exploitation Microsoft Windows Server 2003 SP2 et R2 SP2. L'ensemble des fonctionnalités et dispositifs de sécurité de Stormshield Endpoint Security sont disponibles pour l'installation Stormshield Endpoint Security Server-Side Edition 32 bits sur ces nouvelles plate-formes.

Mise à jour des templates de whitelisting

Il est désormais possible de mettre à jour les templates (modèles) de whitelisting (liste blanche) utilisés par Stormshield Endpoint Security par le menu **Outils** > **Mettre à jour les modèles de liste blanche**.

Le fichier *Templates.scwt* se trouve par défaut dans le répertoire **Templates** de la console d'administration SES. Le support technique peut également fournir une version mise à jour du fichier sur demande.

ATTENTION

En raison des modifications importantes apportées aux bases de données de logs, la mise à jour des bases d'alertes par l'outil DBInstaller peut prendre du temps. Afin que la mise à jour se déroule correctement, l'espace disponible sur le disque sur lequel sont stockées les bases doit être au moins égal à la taille de la plus grosse table des bases de données des logs (db_SoftwareLog, db_systemLog, db_networkLog ou db_MediaLog).

Correctifs de Stormshield Endpoint Security 7.2.04

Problème connu

Référence support 8962

Problème lors de l'installation d'une console d'administration SES sur un poste avec un agent SES

Il est actuellement impossible d'installer ou de désinstaller une console d'administration SES sur un poste sur lequel un agent SES est déjà présent.

Le seul contournement possible dans cette version est de désactiver ou de mettre l'agent SES en mode Warning.

Correctifs agent

Référence support 9190 (#CF 85863)

Perte de la configuration de l'écran d'accueil lors du chiffrement de fichier

Sur le système d'exploitation Windows 8, lors du chiffrement de fichier sur l'ensemble du disque système, la configuration de l'écran d'accueil était perdue. Il en était de même si des pense-bêtes étaient configurés. Ces problèmes sont corrigés.

Référence support 9181 (#CF 85358)

L'agent ne s'installe pas sur Windows XP hongrois

Il n'était pas possible d'installer l'agent SES sur la version hongroise de Windows XP. Le problème pouvait également se présenter sur des versions du système d'exploitation dans d'autres langues. Ce problème est corrigé.

Référence support 8954

Message d'erreur lors de l'application d'une politique de chiffrement de fichier

Lors de l'application d'une politique de chiffrement de fichier, un log d'erreur remontait lorsqu'une partition ne possédait pas de lettre associée. Ce problème est corrigé.

Référence support 8907

Amélioration de la gestion des droits d'accès au dossier d'installation de SES

La protection contre un changement intempestif des droits d'accès au dossier de Stormshield Endpoint Security par un administrateur ou par un programme disposant des droits administrateur a été améliorée.

Référence support 8701

Installation de l'antivirus après un redémarrage

L'antivirus ne s'installait pas correctement juste après un redémarrage de la machine. Cela était dû à l'absence de certains éléments. Ces éléments sont maintenant correctement récupérés.

Référence support 8806 (#CF 84878)

Mauvaise application de politiques en cas de perte de connexion à l'Active Directory

En mode Active Directory, si une politique était appliquée sur une Unité Organisationnelle (OU) ou un groupe d'agents SES possédant un caractère spécial (accent, etc.), en cas de perte de connexion au serveur Active Directory, l'agent n'appliquait pas les politiques liées à cette OU.

Référence support 8715

Problème lors de l'installation de l'antivirus

Lors de l'installation de l'antivirus, un log d'erreur remontait à cause d'une erreur de copie de fichier. Ce problème est corrigé.

Référence support 9067 (#CF 85838)

Incompatibilité McAfee

Sur les systèmes d'exploitation 64 bits, un écran bleu se produisait dès lors que McAfee Viruscan 8.8 Patch 6 cohabitait avec Stormshield Endpoint Security. Ce problème est corrigé.

Sur les systèmes d'exploitation 32 bits, les applicatifs McAfee finissaient par s'arrêter de manière inattendue. Ce problème est corrigé.

Référence support 8976 (#CF 85826)

Utilisation du port LDAP pour récupérer le computer name

Jusqu'à présent le port utilisé pour récupérer le computer name côté agent était le port 135, or ce port n'est pas considéré comme un port LDAP valide. La récupération du computer name passe désormais par un port LDAP standard.

> **NOTE**
> En sortie, les ports distants TCP 88, TCP 389, UDP 389, UDP 53 et TCP 3268 doivent être ouverts entre le poste de travail et le server Active Directory.

Référence support 8974

Exception sur *ntdll.dll* lors de la perte de connexion à l'Active Directory sur Windows XP

Sur Windows XP, lorsque la connexion au serveur Active Directory était impossible et qu'une politique était modifiée depuis la console d'administration SES, une reconnexion au serveur depuis l'agent provoquait une exception dans *ntdll*. Ce problème est corrigé.

Référence support 9039

Changement des noms de fichiers de mise à jour SES

Lors d'une mise à jour de Stormshield Endpoint Security, les noms des fichiers de mise à jour téléchargés par l'agent sont maintenant en minuscules.

Référence support 8832

Logs Firewall avec filtrage au niveau Ethernet

Dans le module Firewall, dans le cas d'un blocage réseau au niveau Ethernet (via adresse MAC source ou destination), le type de log remonté était erroné. Maintenant dans ce cas, le log correspondant de type 'FW_MAC' est bien remonté.

Référence support 9111

Adresse MAC dans les logs Firewall

Dans le module Firewall, dans le cas d'un blocage réseau au niveau Ethernet, l'adresse MAC indiquée dans le log remonté était erronée. Ce problème est corrigé.

Référence support 9178 (#CF 85872)

Lenteur à l'ouverture de la session Windows

Une extrême lenteur de la machine pouvait survenir en raison du plantage d'un des processus de svchost.

Référence support 9289

Chemin d'installation de l'agent SES en minuscules

Depuis la version 7.2, le chemin d'installation des agents SES contenait des noms de dossiers commençant par une minuscule. Les chemins d'installation ont été normalisés et se nomment désormais «Stormshield» au lieu de «stormshield». Par conséquent, l'agent 7.2 s'installe dans le dossier **C:\Program Files\Stormshield\Stormshield Endpoint Security Agent**.

Référence support 9294

Écran bleu aléatoire

Lorsque l'agent SES bloquait l'ouverture d'une clé de registre, un écran bleu pouvait survenir. Ce problème est corrigé.

Référence support 8970 (#CF 85869)

Chrome 64 bits ne fonctionne pas avec Stormshield Endpoint Security

La version 64 bits de Chrome affichait un message d'erreur lorsqu'elle cohabitait avec l'agent SES, et ce sur toutes les plate-formes 64 bits supportées (Windows 7 64 bits et Windows 8.1 64 bits). Ce problème est corrigé.

Référence support 8211

Avast 64 bits ne fonctionne pas avec Stormshield Endpoint Security

La version 64 bits d'Avast provoquait un écran bleu lorsqu'elle cohabitait avec l'agent SES, et ce sur toutes les plate-formes 64 bits supportées (Windows 7 64 bits et Windows 8.1 64 bits). Ce problème est corrigé.

Correctifs serveur

Référence support 8930 (#CF 85501)

Mise en conformité de Syslog TCP avec la RFC 6587

Une non-conformité de l'émission Syslog sur TCP provoquait une mauvaise interprétation des logs par certains serveurs Syslog commerciaux dont le serveur RSA. Ce problème est corrigé.

Référence support 8503

Problème de fuite mémoire dans le moteur de conversion côté serveur

Une erreur lors de la synchronisation des politiques côté serveur provoquait une ligne de log ainsi qu'une fuite mémoire. Ce problème est corrigé.

Depuis ce correctif, la vérification de la version des politiques de sécurité est effectuée côté agent et coté serveur.

Référence support 9236

Génération d'un certificat depuis un serveur mis à jour

Le programme d'installation d'une version 7.2 de Stormshield Endpoint Security ne permettait plus de générer les certificats sur un serveur 7.2 qui avait été mis à jour depuis une version 7.1 ou 6.0.

Correctifs console

Référence support 9169

Accès à une règle depuis le tableau de bord

La fonctionnalité **Aller à la règle** du tableau de bord pointe désormais sur la règle correspondant au log concerné.

Référence support 8833

Redémarrage de la console d'administration SES et changement de licence

Il est maintenant possible d'ajouter une licence périmée, puis de la remplacer par une licence valide sans avoir besoin de redémarrer la console d'administration SES.

Référence support 8828

L'observateur d'événements liste tous les changements effectués sur les politiques de sécurité

Lors d'un ajout ou d'une modification effectués sur un identifiant d'application, le log dans l'observateur d'événements n'affichait pas suffisamment d'informations. De même, les modifications effectuées dans les paramètres généraux du contrôle applicatif de la politique de sécurité n'étaient pas toutes listées dans l'observateur d'événements. Désormais, ce dernier liste tous les changements effectués depuis la console d'administration SES sur les politiques de sécurité.

Référence support 8553

Doublons dans l'éditeur de logs

Lorsque des logs étaient importés plusieurs fois dans l'éditeur, ils étaient visibles en autant d'exemplaires qu'il y avait d'imports. Ce problème est corrigé. Chaque nouvel import d'un log donné remplace désormais sa version précédente.

Référence support 8946

Problème de synchronisation des tests et des actions après une migration

Lorsque des tests et des actions étaient migrés sur la version 7.2.03 de Stormshield Endpoint Security, ils n'étaient pas synchronisés si l'administrateur ne les avait pas visualisés avant de lancer la synchronisation de la console d'administration SES. Ce problème est corrigé.

Référence support 9119

Problème de détection des périphériques USB

Dans certains cas, le lancement de la détection de périphérique USB pouvait entraîner une fermeture inattendue de la console d'administration SES. Ces cas sont maintenant traités et n'interrompent plus l'utilisation de la console.

Référence support 9149 (#CF 85554)

Perte de paramètres dans une politique ou configuration

Après de nombreuses modifications dans une politique ou une configuration, des erreurs pouvaient apparaître lors d'un passage en mode édition dans la console d'administration SES. Ces erreurs provoquaient la perte de l'ensemble des paramètres de la politique ou de la configuration. Ce problème est corrigé.

Mises à jour de Stormshield Endpoint Security 7.2.04

Référence support 8857

Mise à jour de la librairie libxml2

La librairie libxml2 utilisée pour la gestion des fichiers XML (configuration, politiques, etc.) présentait une faille de sécurité. Elle a été mise à jour pour corriger ce problème.

Référence support 8304

Mise à jour du composant serveur Apache en version 2.2.31

Le composant serveur Apache installé avec le serveur SES a été mis à jour en version 2.2.31 afin de contrer la faille permettant à un attaquant de provoquer un déni de service.

Correctifs de Stormshield Endpoint Security 7.2.03

Correctif agent

Référence support 8897

Plantage Internet Explorer 11 avec la protection RCP activée

La protection RCP entraînait un plantage de certaines applications 32 bits exécutées sur le système d'exploitation Windows 7 64 bits. C'était le cas d'Internet Explorer 11 qui se lance en 32 bits. Ce problème est résolu.

Correctifs de Stormshield Endpoint Security 7.2.02

Correctifs agent

Référence support 8547 (#CF 85247)

Écran bleu lors de la mise en veille du poste de travail

Lorsque la politique Firewall réseau dans le contrôle de la sécurité réseau de la politique de sécurité contenait des règles de filtrage sur l'adresse MAC, certaines machines n'entraient pas normalement en état de veille. L'arrêt de ces machines pouvait aussi durer anormalement longtemps : un écran bleu survenait puis la machine s'arrêtait. Ce problème est corrigé.

Si vous utilisez des règles de filtrage sur adresse MAC, nous vous recommandons de procéder à la mise à jour de Stormshield Endpoint Security en version 7.2.02.

Sur les postes concernés par ce problème, suivez la procédure suivante :

1. Désactivez toutes les règles Firewall réseau avec filtrage MAC. Il est possible de créer une politique « temporaire » sans filtrage MAC pour les agents concernés.

   NOTE
   Si des règles d'autorisation Firewall réseau contiennent du filtrage sur adresse MAC , l'accès à certains services réseau peut être bloqué durant cette phase de mise à jour. Il est alors possible de choisir d'ajouter des règles "adresses IP" d'autorisation additionnelles.
2. Attendez que toutes les machines aient reçu la nouvelle politique.
3. Redémarrez les machines concernées.
4. Procédez à la mise à jour de Stormshield Endpoint Security.
5. Réactivez les règles désactivées.

Si cette procédure n'est pas suivie, l'écran bleu risque d'apparaître lors de la mise à jour. Dans ce cas, il suffit de redémarrer deux fois la machine. La mise à jour se fera tout de même et le problème sera définitivement corrigé. Si Microsoft Windows demande de choisir entre un redémarrage normal, un mode sans échec ou une récupération du système, choisissez le redémarrage normal.

NOTE
Les postes sous Windows XP ne sont pas concernés et leur mise à jour peut se faire normalement.

Référence support 8427 (#CF 84778)

Deadlock sur des mécanismes de synchronisation

Sur les applications utilisant des mécanismes de synchronisation sur le poste de travail, un deadlock pouvait survenir lors de l'arrêt des threads utilisant ces mécanismes (par exemple les applications utilisant Mono ou Unity3D). Ce problème est corrigé.

Référence support 7133

Écran bleu aléatoire lors de la sortie de veille

Un écran bleu pouvait survenir lors de la sortie de veille sur des systèmes d'exploitation 32 bits. Ce problème est corrigé.

Référence support 8478

Log de redémarrage en complément de la notification

Lors d'une mise à jour ou d'une installation de l'agent SES, un log de redémarrage a été ajouté dans le journal.

Référence support 8407

Exécution d'applications sur périphérique amovible

Lorsque l'agent était désactivé, l'exécution d'applications depuis un périphérique amovible n'était pas possible. Ce problème est corrigé.

Référence support 8338

Méthode de keylogging Directx

Le keylogging utilisant la méthode Directx n'était pas bloqué lorsque la protection était paramétrée sur le niveau critique. Ce problème est corrigé.

Référence support 8295

Configurations Firewall réseau et Points d'accès WiFi incohérentes entre console et agent

La désactivation des groupes Firewall réseau et Points d'accès Wifi dans l'onglet *Contrôle de la sécurité réseau* de la politique de sécurité pouvait ne pas être prise en compte par l'agent SES. Ce problème est corrigé.

Référence support 8434

Amélioration des logs liés à la circulation des jetons

Les logs d'erreurs lors de l'échange des jetons entre le serveur et les agents SES ont été améliorés.

Références support 6596 et 8494

Amélioration de l'auto-protection de l'agent

La protection des composants de l'agent SES sur le poste de travail a été renforcée afin d'interdire les changements de droits sur ces composants.

Référence support 8441

Compatibilité avec Oracle VM VirtualBox

La compatibilité avec Oracle VM VirtualBox a été améliorée.

Référence support 8535 (#CF 85050)

Apparition des règles No Execute dans ssmon

Lorsque la protection contre la création d'exécutables était activée, les messages relatifs au blocage n'apparaissaient plus dans le journal d'événements de l'agent SES mais uniquement dans les fichiers de log. Ce problème est corrigé.

Référence support 8521

Correction de l'affichage du log de blocage de création de fichiers exécutables

Désormais, lorsque la protection contre la création d'exécutables est activée, aucun log ne remonte si le contenu d'un fichier exécutable est simplement modifié.

Référence support 8581 (#CF 84542)

Installation de l'antivirus Avira sur un système d'exploitation en espagnol

Désormais, l'antivirus Avira s'installe par défaut en anglais, sur les postes de travail dont la langue système est autre que le français.

Référence support 8584

Protection contre la création d'exécutables

La protection contre la création de fichiers exécutables a été renforcée.

Référence support 8633 (#CF 85259)

Correction d'un écran bleu de type IRQL_NOT_LESS_OR_EQUAL au démarrage de la machine

Un écran bleu pouvait apparaître de manière aléatoire sur certains postes clients sous Windows XP.

Référence support 8678 (#CF 85675)

Correction de la gestion des clés registres Root

La gestion des clés registres Root a été améliorée. Un dysfonctionnement pouvait provoquer un arrêt inattendu des applications.

Référence support 8727 (#CF 85696)

Compatibilité entre client VPN IPSec et firewall SES sous Windows 7 64 bits

L'utilisation conjointe du firewall agent SES (driver « thor3 ») et d'un client VPN IPSec sur un même poste de travail sous Windows 7 en 64 bits pouvait ne pas fonctionner. Les paquets entrants du type UDPENCAP (encapsulation du protocole ESP dans des paquets UDP ports source / destination 4500) étaient mal filtrés par le firewall SES. En conséquence, les flux réseau routés via un tunnel VPN IPSec n'étaient pas fonctionnels. Ce problème est corrigé.

Correctifs serveur

Référence support 6596

Amélioration de l'auto-protection du serveur

La protection des composants du serveur SES a été renforcée afin d'interdire les changements de droits sur ces composants.

Référence support 8716 (#CF 85597)

Amélioration de la gestion des fichiers cache de logs

Les fichiers cache de logs mal formatés sont désormais correctement gérés sur le serveur SES.

Correctifs console

Référence support 8329

Recherche erronée dans un filtre de log

Lors d'un filtrage sur les logs logiciel, système, réseau ou périphérique dans le panneau **Surveillance des logs** avec la méthode « contient » dans le champ **Comparaison**, la recherche ne retournait pas les logs si la « Valeur » du filtre contenait le caractère [_]. Ce problème est corrigé.

Référence support 8428

Vérification de la parenté du certificat des serveurs

Lors de la synchronisation entre la console d'administration SES et les serveurs, la parenté du certificat des serveurs est désormais vérifiée en comparant leur autorité racine à celle du certificat de la console d'administration.

Référence support 8451

Erreur de la console lors du tri des certificats selon leur date de validité

Dans la politique de sécurité, désormais le tri des certificats par leur date de validité fonctionne correctement.

Référence support 8486

Erreur de la console lors du tri des politiques s'il n'y a aucune politique héritée

Désormais, dans le panneau **Politiques liées** accessible depuis le **Gestionnaire des environnements**, le tri fonctionne correctement pour les catégories de politiques ne contenant pas de politique héritée.

Référence support 8426

Incohérence des rangs après suppression de règles de sécurité

Dans la catégorie **Contrôle applicatif** de la politique de sécurité, lorsque le focus était positionné sur **Règles applicatives**, **Extensions** ou **Applications de confiance** et que l'utilisateur supprimait une ou plusieurs lignes, il y avait une incohérence dans la numérotation des rangs. Ce problème est corrigé.

Référence support 8327

Création des règles applicatives / sous-règles Réseau

Depuis l'introduction en version 7.2.00 du paramètre IP dans les sous-règles Réseau des règles applicatives de la politique de sécurité, il était impossible de créer deux règles avec les mêmes modes d'accès et ports. Ce problème est corrigé.

Référence support 8478

Log de redémarrage en complément de la notification

Un log de redémarrage a été ajouté dans le log de la console pour signaler une mise à jour ou une installation de Stormshield Endpoint Security.

Référence support 6910

Support des caractères spéciaux dans la politique antivirus

La politique antivirus supporte désormais les caractères spéciaux dans les champs **Chemin à analyser** et **Fichiers à analyser**.

Référence support 8549 (#CF 85629)

Validation impossible de l'éditeur de logs après l'import de fichier *.LFXML*

Dans l'éditeur de log, une erreur empêchait les éléments importés d'être enregistrés dans la base de données. Ce problème est corrigé.

Référence support 7298

Conservation de l'ordre des règles d'une politique de sécurité lors de leur copie

Les règles d'une politique de sécurité peuvent désormais être collées dans une autre politique de sécurité dans le même ordre.

Référence support 8625

Possibilité d'enrôler un périphérique amovible via un utilisateur Windows de l'Active Directory

Dans le gestionnaire d'enrôlement des périphériques, l'ajout d'une clé était impossible si l'utilisateur de la console provenait d'un compte Windows. Le champ **Enrôlé par** restait vide car l'utilisateur n'était pas retrouvé dans l'Active Directory. Ce problème est corrigé.

Mises à jour de Stormshield Endpoint Security 7.2.02

Référence support 8202

Ajout d'un menu contextuel sur les identifiants d'applications

Dans la console d'administration SES, un menu contextuel a été ajouté sur les identifiants d'applications dans la catégorie **Contrôle applicatif** de la politique de sécurité. Celui-ci permet d'assigner ou retirer des identifiants à la règle en cours ou d'aller directement sur l'identifiant sélectionné dans le panneau de gestion des identifiants d'applications.

Référence support 8448

Ajout du raccourci de l'outil Stormshield SignTool au menu Démarrer.

Un raccourci vers l'outil de signature Stormshield SignTool apparaît désormais dans le menu **Démarrer** de Windows lors d'une migration vers la version 7.2.02 de Stormshield Endpoint Security.

Référence support 8455

Filtrage sur les extensions de certificats à l'import de certificats

Lors de l'import de certificats dans la console d'administration SES, il est maintenant possible de filtrer l'import sur les extensions de certificats (**.cert*, **.crt*, **.der*, **.pem*, **.p7b* et **.p7c*).

Référence support 8666

Affichage multi-lignes dans la console d'administration SES

Dans la politique de sécurité, l'éditeur de règles est désormais personnalisable. On peut choisir un affichage sur plusieurs lignes pour les règles réseau, les règles applicatives, les règles d'extensions et les règles d'applications de confiance.

Référence support 8775

Mise à jour de OpenSSL

OpenSSL a été mis à jour en version 1.0.1p.

Référence support 8498

Mise à jour de cURL

cURL a été mis à jour en version 7.42.1.

Référence support 8309

Mise à jour de SQLite

Certaines failles de sécurité ont été découvertes dans SQLite. Pour pallier celles-ci, la mise à jour de SQLite vers la version 3.8.10.2 a été appliquée.

Correctifs de Stormshield Endpoint Security 7.2.01

Correctif agent

Référence support 8446

Échec de la migration des politiques 7.1 vers 7.2

Lors d'une mise à jour de la version 7.1 de StormShield vers la version 7.2 de Stormshield Endpoint Security, le nouvel agent 7.2 ne parvenait pas à appliquer les politiques 7.2 téléchargées depuis le serveur avant sa mise à jour. Il était nécessaire de resynchroniser les politiques sur le serveur depuis la console SES pour que l'agent 7.2 puisse les récupérer et les appliquer. Ce problème est désormais résolu et a fait l'objet du bulletin de sécurité STORM-2015-03.

Nouvelles fonctionnalités de Stormshield Endpoint Security 7.2

Moteur de détection de heap spray amélioré

Stormshield Endpoint Security inclut un nouvel algorithme de détection de heap spray. Désormais, ce nouveau moteur remplace l'ancien lorsque l'option **Protection contre les débordements mémoire** est paramétrée sur « Haut » ou « Critique » dans la politique de sécurité. Au niveau « Bas », le précèdent algorithme reste utilisé.

Ce nouveau moteur affiche une progression dans la détection des attaques de type heap spray.

Mise à jour de l'updater

Le processus de mise à jour d'une ancienne version de StormShield vers la nouvelle version Stormshield Endpoint Security 7.2 a évolué. Il ne présente pas de risque de dégrader la sécurité du poste de travail lors du prochain redémarrage de celui-ci une fois la nouvelle version installée.

Support de Windows 8.1 et Server 2012 R2

Stormshield Endpoint Security supporte désormais les systèmes d'exploitation Microsoft Windows 8.1 Update 1 et Windows Server 2012 R2 Update 1. L'ensemble des fonctionnalités et dispositifs de sécurité de Stormshield Endpoint Security sont disponibles sur ces nouvelles plate-formes.

Support de Windows Server 2003 SP2 et R2 SP2

Stormshield Endpoint Security supporte désormais les systèmes d'exploitation Microsoft Windows Server 2003 SP2 et R2 SP2. L'ensemble des fonctionnalités et dispositifs de sécurité de Stormshield Endpoint Security sont disponibles pour l'installation Stormshield Endpoint Security Server-Side Edition 32 et 64 bits sur ces nouvelles plate-formes.

Filtrage applicatif par hash ou certificat

Il est maintenant possible d'utiliser des certificats ou des hashes MD5 ou SHA-1 pour identifier des applications dans les règles applicatives de la console d'administration. De plus, il est désormais possible de configurer le filtrage applicatif en mode liste noire ou liste blanche. Enfin, l'import d'anciennes politiques de la version 7.1 est possible. L'utilisation de cette nouvelle fonctionnalité est documentée dans le *Guide d'administration* de Stormshield Endpoint Security.

Amélioration de la sécurité des allocations mémoire au niveau du noyau

Les droits d'exécution des allocations mémoire effectuées par les composants noyaux de Stormshield Endpoint Security ont été retirés. Cette amélioration est possible depuis Microsoft Windows 8 / Windows 2012 et les versions suivantes.

Annulation d'un verrou dans la console d'administration

Il est désormais possible de rompre un verrou dans la console d'administration de Stormshield Endpoint Security. En effet, un administrateur possédant le droit **Gestion des utilisateurs** peut forcer l'édition d'une politique. L'administrateur peut donc prendre la main sur l'utilisateur qui est en train d'éditer cette politique et qui ne l'a pas validée.

Renforcement de la protection contre les débordements mémoire

La protection contre les débordements mémoire vérifie désormais les attaques dites de « stack pivot ». L'agent Stormshield Endpoint Security bloque désormais ce type d'attaque.

Amélioration des traces des drivers de Stormshield Endpoint Security

Les traces de debug des modules noyaux de Stormshield Endpoint Security ont été améliorées.

Passage au framework .NET 4.0

Stormshield Endpoint Security utilise désormais le framework .NET 4.0 plutôt que la version 2.0. Ce nouveau prérequis sera automatiquement installé par Stormshield Endpoint Security si besoin.

Correctifs de Stormshield Endpoint Security 7.2

Correctifs agent

Référence support 7228

Blocage des périphériques USB lors d'un arrêt de l'agent

L'accès aux périphériques USB pouvait être bloqué par l'agent Stormshield Endpoint Security lorsque celui-ci était arrêté. Ce problème est désormais résolu.

Référence support 7035

Démarrage anticipé du service de l'agent

Le service de l'agent démarrera toujours en premier sur le poste de travail afin que l'état de l'agent soit actif plus rapidement.

Référence support 7523

Nouveau fichier de configuration des protections noyau

Un nouveau fichier *dumpconf.srn* est créé à la racine de la partition système. Ceci permet de séparer la configuration de la politique pour la protection de Stormshield Endpoint Security.

Référence support 7550

Intégrité des fichiers de configuration des protections noyau

Les fichiers *dumprules.srn* et *dumpconf.srn* stockés à la racine de la partition système sont désormais couverts par un test d'intégrité afin de détecter une éventuelle corruption.

Référence support 7643

Mauvaise initialisation de la protection RCP

La protection RCP pouvait ne pas fonctionner correctement sur certains processus à cause d'une mauvaise initialisation d'un mécanisme interne. Ce problème est désormais résolu.

Référence support 6454

La protection HPP pouvait ne pas fonctionner sans la protection RCP

Sous Windows 7 32 bits, la protection HPP n'était pas effective lorsque la protection RCP était désactivée. Ce problème est désormais résolu.

Référence support 7141

La protection HPP pouvait ne pas fonctionner sans la protection KRP

Sous Windows XP, la protection HPP n'était pas effective lorsque la protection KRP était désactivée. Ce problème est désormais résolu.

Référence support 7142

Mauvaise initialisation de la protection HPP

Sous les systèmes 32 bits, la protection HPP pouvait ne pas fonctionner correctement à cause d'une mauvaise initialisation d'un mécanisme interne. Ce problème est désormais résolu.

Référence support 7789

BSOD dans Thor3 et Meili

Un écran bleu impliquant les drivers de filtrage réseau (Thor3 et Meili) pouvait subvenir si le poste de travail manquait de mémoire physique. Ce problème est désormais résolu.

Correctifs console

Référence support 6861

Redimensionnement des colonnes du panneau Politiques liées

Il est désormais possible de redimensionner les colonnes du panneau **Politiques liées** dans la console d'administration.

Référence support 6829

Suppression de la catégorie « Configuration serveur »

Dans l'arborescence Active Directory de la console d'administration, lorsqu'un agent était sélectionné, la catégorie « Configuration serveur » s'affichait. Ce n'est plus le cas désormais. De même, si un serveur est sélectionné dans cette arborescence et que celui-ci est lié à une unité organisationnelle de l'AD, alors le panneau des serveurs Stormshield Endpoint Security s'affiche.

Référence support 7239

Amélioration des logs firewall

La lisibilité des logs du pare-feu de Stormshield Endpoint Security a été améliorée.

Référence support 7165

Mise à jour d'une console juste après son installation

Lorsque la console d'administration était mise à jour juste après avoir été installée, le programme d'installation des bases de données était exécuté plutôt que celui de mise à jour. Ce problème est désormais résolu.

Référence support 7065

Édition multiple de règles applicatives

Il est désormais possible d'éditer l'état d'une sélection de plusieurs règles applicatives dans la console d'administration.

Référence support 7306

Problème de sélection de panneau dans la console

Un mauvais onglet pouvait s'afficher dans la console d'administration lors d'un changement de sélection de politique, ce qui provoquait des comportements aléatoires. Ce problème est désormais résolu.

Référence support 7130

Menus contextuels dans la console d'administration

Des menus contextuels dans la console d'administration pouvaient apparaître sur des éléments qui n'auraient pas dû en avoir. Ce problème est désormais résolu.

Référence support 7412

Réorganisation des règles pare-feu par raccourcis clavier

Une erreur pouvait survenir lorsque les règles pare-feu étaient réorganisées en utilisant les raccourcis clavier prévus à cet effet. Ce problème est désormais résolu.

Référence support 7435

Validation des chemins

Des chemins invalides dans les règles applicatives ou d'extensions sur les périphériques amovibles pouvaient être acceptés dans la console d'administration. Ce problème est désormais résolu.

Référence support 7544

Corruption de pile

Une corruption de pile pouvait avoir lieu dans la console d'administration lors de la création d'un CD de recouvrement par exemple. Ce problème est désormais résolu.

Référence support 7422

Affichage aléatoire du DbInstaller

Un bug dans le DbInstaller a été corrigé. Celui-ci pouvait afficher son panneau principal après une migration de la base de données lors d'une mise à jour de la console d'administration. De même, le panneau résumant l'installation du produit pouvait rester affiché si l'import des anciennes politiques était sélectionné.

Corrections graphiques dans la console

L'aspect graphique de la console a été uniformisé. Des icônes ainsi que la taille de certaines colonnes ont été revues. L'option **Renommer** a été ajoutée dans certains menus contextuels.

Référence support 7622

Corrections dans la console

L'affichage des numéros de pages dans la surveillance des logs a été corrigé : la première page porte maintenant le numéro « 1 » et non « 0 ».

Référence support 7563

Changement des variables d'environnement

|systemroot| et |programfiles| ont été retirées de la liste des variables d'environnement autorisées pour le chiffrement de fichiers. En effet, ces emplacements ne sont jamais chiffrés par l'agent.

Référence support 8013

Génération des règles Firewall / Filtrage Réseau

Lors de la génération des règles « Firewall réseau » dans le fichier de la politique de sécurité, l'ordre des règles n'était pas correctement respecté. En effet, au lieu de générer les règles en suivant le paramètre Rang ('#' dans l'affichage de la console), on utilisait l'ordre des groupes des règles « Firewall réseau » de la politique de sécurité. Ce problème a été corrigé : l'ordre des règles respecte maintenant le paramètre « Rang ». Attention, cette correction peut avoir un impact fonctionnel important sur votre politique de filtrage réseau. Lors d'une migration depuis une version antérieure de Stormshield Endpoint Security, l'administrateur doit vérifier que l'ordre des règles de filtrage réseau respecte bien le filtrage souhaité.

Référence support 7533

Changement du système de lien des politiques

Un nouveau panneau d'édition des liens de politiques a remplacé l'existant. Il est désormais possible d'y créer des liens sans utiliser le glisser/déposer.

Référence support 8207

Rétrocompatibilité des politiques

Un mécanisme a été ajouté pour fiabiliser le comportement d'un agent mis à jour récemment et n'ayant pas encore reçu les politiques correspondant à sa version.

Référence support 8025

Gestion des séparateurs CSV

Un nouveau paramètre a été ajouté dans les options de la console d'administration pour gérer les différents séparateurs du format CSV. Ce paramètre impacte l'import du contenu des groupes d'agents ainsi que celui des fichiers de hash.

Référence support 8059

Modification de l'installeur SES

L'installeur Stormshield Endpoint Security a été modifié : l'étape facultative « Paramètres de la console » a été supprimée. Le nom de l'instance par défaut de la base de données est maintenant SES et non plus EDDAS. Quelques chaînes ont été modifiées pour les rendre plus claires.

Fonctionnalités retirées de Stormshield Endpoint Security 7.2

Retrait de la fonctionnalité « Protection contre la surcharge CPU »
Cette fonctionnalité a été retirée du produit car son taux de faux positifs était trop élevé.

Retrait de la fonctionnalité « Copier / Coller »
La fonctionnalité a été retirée à partir de la version 7.2 de Stormshield Endpoint Security.

Contact

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- https://mystormshield.eu/
  La soumission d'une requête auprès du TAC doit se faire par le biais du gestionnaire d'incidents dans l'espace privé https://mystormshield.eu/, menu **Support technique** > **Rapporter un incident/Suivre un incident**.
- +33 (0) 9 69 329 129
  Afin d'assurer un service de qualité, veuillez n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace https://mystormshield.eu/.