STORMSHIELD

STORMSHIELD MANAGEMENT CENTER

NOTES DE VERSION

Version 3

Dernière mise à jour du document : 17 juin 2021

Référence : sns-fr-SMC-notes_de_version-v3.0

Table des matières

Dans la documentation, Stormshield Management Center est désigné sous la forme abrégée : SMC et Stormshield Network sous la forme abrégée : SN.

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

Nouvelles fonctionnalités de SMC 3.0

Authentification

Groupes imbriqués

Un administrateur faisant partie d'un groupe LDAP imbriqué dans un autre peut maintenant se connecter au serveur SMC.

Configuration des firewalls SN

Gestion des interfaces réseau

Vous pouvez désormais gérer les interfaces réseau des firewalls SN de manière centralisée sur le serveur SMC. Pour les firewalls SN en version 3.7 minimum, les interfaces réseau sont affichées sur SMC en lecture seule. Pour les firewalls SN à partir de la version 4.2.3, vous pouvez activer la configuration des interfaces réseau en écriture dans les paramètres SMC.

Les interfaces Ethernet, les bridges, les VLAN et les agrégats en IPv4 des firewalls compatibles seront donc affichés sur le serveur SMC et leur configuration peut être gérée sans avoir à se connecter sur chaque firewall individuellement. Pour les interfaces supportées, SMC vérifie leur configuration et remonte des erreurs grâce au contrôleur de cohérence.

En savoir plus

Maintien de la connexion lors d'un déploiement

Le déploiement d'une configuration erronée par inadvertance peut provoquer la perte de connexion entre le serveur et le firewall. À partir de la version 4.2.3 des firewalls SN, la configuration précédente sera restaurée si la connexion a été perdue. Ceci permet de garantir que le firewall reste toujours joignable depuis le serveur SMC.

En savoir plus

Redémarrage après un déploiement

Un firewall SN peut parfois nécessiter un redémarrage après le déploiement d'une configuration réseau pour appliquer les modifications. Dans un tel cas l'information est remontée par SMC grâce au nouvel état de santé "Redémarrage nécessaire", et il est possible de redémarrer les firewalls concernés directement depuis le serveur SMC. Cette fonctionnalité est supportée sur les firewalls seuls en version 4.2.3.

En savoir plus

Détection de modifications locales

Après un premier déploiement sur un firewall SN rattaché, SMC détecte désormais si la configuration des éléments gérés par SMC a été modifiée localement. Vous pouvez alors décider de déployer la configuration actuellement présente sur le serveur SMC, écrasant ainsi les modifications locales. Vous pouvez aussi restaurer la dernière configuration qui avait été déployée sur le firewall en question.

En savoir plus

Import des firewalls depuis un fichier CSV

La commande permettant d'importer des firewalls SN depuis un fichier CSV en ligne de commande a été renommée en `smc-import-firewalls`. L'ancienne commande `smc-firewalls-and-packages` n'est plus supportée.

En savoir plus

Règles de filtrage et de translation

Création de jeux de règles

Vous pouvez désormais créer des jeux de règles pour regrouper les règles de filtrage ou de translation que vous souhaitez déployer sur un ou plusieurs firewalls. Cela vous permet de réutiliser un ensemble de règles correspondant à une application particulière dans la configuration de différents firewalls, indépendamment de leur emplacement dans l'arborescence de dossiers.

En savoir plus

Correctifs de SMC 3.0

Configuration des firewalls SN

Journaux d'audit inaccessibles

Références support 79393 et 80772

En cas de connexion au firewall via le serveur SMC, l'accès aux journaux d'audit pouvait échouer pour certaines versions de firewalls SN. Ce problème a été corrigé.

Configuration réseau par clé USB impossible

Référence support 79258

En raison d'une section manquante dans le package de rattachement il était impossible d'utiliser une clé USB pour renseigner la configuration réseau pour un firewall en configuration d'usine. La section a été rajoutée et l'utilisation des clés USB est désormais possible.

Initialisation du serveur SMC

Paramètre ambigu

Référence support 82014

Le paramètre `DNS configuration (leave blank if no DNS)` demandé lors de l'initialisation manuelle du serveur SMC a été modifiée en `DNS server IPs (comma separator or leave blank if no DNS)` pour éliminer des ambiguïtés.

Mise à jour

Fuseau horaire non conservé

Référence support : 80779

Le fuseau horaire défini est désormais conservé après une mise à jour de SMC.

Perte de scripts

Référence support : 71885

Les scripts exécutés automatiquement lors de l'activation d'une interface réseau du système hôte de SMC sont désormais conservés après une mise à jour.

Message d'erreur ambigu

Référence support : 0081991

Un message d'erreur ambigu affiché lors d'un problème de restauration du serveur à partir d'une sauvegarde a été modifiée pour indiquer clairement la cause de l'erreur.

Règles de filtrage et de translation

Import de règles

Référence support : 79314

Lors d'un import de règles de filtrage à partir d'un fichier CSV, l'opérateur "!" (différent de) était ignoré. Ce problème a été corrigé et les champs sont désormais importés en tenant compte de cet opérateur.

Références support : 78561 et 79308

Un import de règles contenant la valeur "any" dans un champ `#nat_to_target` du fichier CSV échouait parce que cette valeur est interdite. La valeur pour ce champ est désormais paramétrée automatiquement à "none" et l'import n'échoue plus.

Référence support : 80828

Il est désormais possible d'importer des règles de filtrage et de translation contenant des noms de domaine.

Référence support : 80590

Il est désormais possible d'importer des règles via un fichier CSV contenant certaines catégories IPRep qui manquaient auparavant.

Adaptation du nom de protocole

Référence support 82222

Dans les règles de filtrage le nom du protocole "ldap" a été modifié en "ldap_tcp" afin d'assurer la cohérence entre SMC et SMC.

Erreur de copier-coller

Référence support : 78373

Lors du copier-coller d'une règle vers l'écran des règles de filtrage ou de translation, le nom de la règle et son contenu sont désormais collés correctement.

Système

Erreurs fréquentes

Référence support : 81714

Des erreurs de connexion au port série s'affichaient toutes les cinq minutes. Ce problème a été corrigé.

Compatibilité

Les plates-formes suivantes sont compatibles avec SMC 3.0.

Environnements virtuels

VMware ESXi	6.5 et 6.7
Microsoft Hyper-V	Windows Server 2012 R2 et 2016
KVM	Red Hat 7.6

Navigateurs web

Pour un fonctionnement optimal de l'interface d'administration des firewalls, il est recommandé d'utiliser la dernière version des navigateurs Microsoft Edge, Google Chrome et Mozilla Firefox (version ESR - Extended Support Release). Pour de plus amples renseignements sur ces versions, nous vous invitons à consulter le Cycle de Vie des Produits des éditeurs concernés.

Annuaires Active Directory

Active Directory	Windows Server 2012 R2 et 2016

Compatibilité SMC/firewalls SN

Le serveur SMC permet d'administrer les firewalls SN à partir de la version 2.5.

Ce tableau récapitule les versions minimum des firewalls SN requises pour être compatibles avec les fonctionnalités suivantes de SMC :

Fonctionnalité/Objet	Version de SMC	Version minimum du firewall SN requise
Scripts CLI SNS	1.1	2.5
Règles de filtrage/translation	2.0	3.0
Topologies VPN par politique	2.0	3.0
Objets Routeur et Temps	2.1.0	3.1
Modification de l'interface de sortie des firewalls	2.2.0	3.3
Multiples adresses de contact de SMC dans le package de rattachement	2.2.1	3.3
SMC en tant que point de distribution de CRL	2.2.1	3.3
Indicateurs de santé	2.5	3.6
Mode "Responder-only" dans les topologies VPN en étoile	2.5	3.6
Algorithme de chiffrement AES GCM 16	2.5	3.6
Import de règles de filtrage et de translation depuis l'interface web	2.5	3.3

Délai de clôture des SA (VPN Peer Inactivity)	2.6.1	3.7.2
Paramètre CRLRequired	2.6.1	3.8
Déclaration d'un serveur SCEP associé à une autorité de certification/renouvellement automatique des certificats SCEP	2.6.1	3.9
Interfaces de sortie multiples dans le package de rattachement	2.6.1	3.9
Sécurisation des certificats par TPM (Trusted Platform Module)	2.6.1	3.10
Paramètre DSCP dans les topologies VPN	2.6.1	3.10
Déclaration d'un serveur EST associé à une autorité de certification/renouvellement automatique des certificats EST	2.7	3.10 et 4.1
Exclusion des clés privées de la sauvegarde automatique de firewalls	2.7	3.10 et 4.1
Topologies VPN par route	2.8	3.3
Gestion des interfaces réseau (en lecture seule)	3.0	3.7

NOTE
Pour pouvoir superviser l'état des topologies VPN contenant des firewalls SN de la version 4.2. ou supérieure, vous devez utiliser un serveur SMC de la version 2.8.1 ou supérieure.

Préconisations

Informations sur les mises à jour ultérieures

Suite à la mise à jour du serveur SMC en version 3.0.x, les disques virtuels manqueront d'espace et ne permettront pas l'installation des mises à jour ultérieures. Après la mise à jour en version 3.0.x, réalisez la procédure suivante afin d'augmenter l'espace disque du serveur :

1. Effectuez une sauvegarde de la configuration du serveur SMC 3.0.x.
2. Éteignez le serveur SMC.
3. Déployez un nouveau serveur SMC dans la même version 3.0.x.
4. Restaurez la configuration sauvegardée sur la nouvelle machine virtuelle.

Vous devez passer par la version 3.0 pour pouvoir bénéficier des mises à jour ultérieures.

Informations avant la mise à jour

Recommandations matérielles minimum

Afin d'assurer la bonne performance du serveur SMC, nous recommandons de l'installer sur une machine virtuelle disposant d'au moins de 2 vCPU et 4 Go de RAM.

Accès au serveur SMC pendant une mise à jour

Lorsque vous mettez à jour votre serveur SMC, nous vous recommandons de rendre l'accès à SMC indisponible pour les autres administrateurs le temps de la mise à jour. Dans le cas contraire, s'ils sont en train de travailler sur la configuration, ils ne sont pas prévenus qu'une mise à jour est en cours et pourraient perdre leur travail.

Serveur Syslog

Si vous utilisez un serveur distant au format Syslog pour collecter les traces de SMC, vous devez reconfigurer votre serveur distant après une mise à jour du serveur SMC via la commande `smc-syslog-ng`. Cette manipulation n'est plus nécessaire à partir de la version 2.6 du serveur SMC.

Avant la mise à jour d'une version 2.0

À partir de la version 2.1.0 du serveur SMC, des changements ont été apportés dans le système d'exploitation afin de pouvoir gérer un plus grand nombre de données, notamment dans le cadre de la nouvelle fonctionnalité de sauvegarde automatique de la configuration du serveur et des firewalls SN.

Nous vous recommandons de déployer un nouvel *.OVA*, *.VHD* ou *.qcow2* afin d'exploiter au mieux les modifications suivantes :

- interface virtuelle plus performante,
- disque de taille plus importante pour supporter la fonctionnalité de sauvegarde automatique.

Nous vous conseillons également de ne pas activer la fonctionnalité de sauvegarde automatique avant d'avoir déployé une nouvelle machine.

Pour déployer un nouvel *.OVA*, *.VHD* ou *.qcow2*, veuillez appliquer la procédure suivante :

1. Commencez par mettre à jour votre machine en version 2.1.0 ou supérieure à partir d'une archive de mise à jour.
2. Réalisez une sauvegarde de la configuration du serveur et éventuellement des traces.
3. Déployez un nouvel *.OVA*, *.VHD* ou *.qcow2* version 2.1.0 ou supérieure.
4. À partir de l'assistant d'initialisation de SMC, restaurez la configuration sauvegardée sur la nouvelle machine.

Pour plus d'informations sur ces procédures ou pour obtenir de l'aide, consultez le *Guide d'administration* de SMC ou contactez le Technical Assistance Center.

Consultez également la base de connaissances SNS accessible depuis votre espace personnel MyStormshield. Celle-ci fournit une procédure manuelle pour augmenter la taille du disque et modifier l'interface virtuelle.

Avertissement avant de rattacher des firewalls SN au serveur SMC

Veuillez prendre connaissance de ces informations si vous souhaitez rattacher au serveur SMC un parc de firewalls SN déjà en production et qui contient des éléments de configuration globaux.

Lorsque SMC déploie une configuration sur un firewall, tous les éléments de configuration globaux existant sur ce firewall sont supprimés, et remplacés par les éventuels éléments de configuration définis dans la configuration SMC.

Ceci comprend :

- Les objets globaux définis sur le firewall,
- Les règles de filtrage globales définies sur le firewall,
- Les tunnels VPN globaux définis sur le firewall.

Ces éléments ne sont pas visibles par défaut dans l'interface web de configuration SNS. Pour les afficher, vous devez aller dans les **Préférences** de votre firewall, section **Paramètres de l'application** et activer l'option **Afficher les politiques globales (Filtrage, NAT, IPsec et Objets)**.

En rattachant un firewall SN à SMC, vous acceptez donc que ces éléments globaux que vous auriez pu mettre en place sur ce firewall soient écrasés dès le premier déploiement de configuration par SMC.

En revanche les objets, règles et tunnels VPN locaux (que vous manipulez par défaut dans l'interface Web d'administration des firewalls) ne seront jamais modifiés ou supprimés par un déploiement de configuration par SMC.

Nous vous préconisons donc de recréer ces éléments globaux sous forme d'éléments locaux sur le firewall ou bien de récrire les règles dans SMC avant de rattacher le firewall à SMC, pour éviter toute perte d'éléments de configuration et ne pas perturber la production.

Dans les cas les plus fréquents, où le firewall à rattacher ne dispose pas d'éléments de configuration globaux, son rattachement à SMC ne nécessite pas de précaution particulière et se fera sans impact sur la production.

Dans tous les cas, nous préconisons de réaliser une sauvegarde de la configuration de votre firewall avant de le rattacher à SMC.

Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version de SMC est consultable sur la Base de connaissance Stormshield (anglais uniquement). Pour vous connecter à la Base de connaissance, utilisez les mêmes identifiants que sur votre espace client MyStormshield.

Précisions sur les cas d'utilisation

Utilisation des objets VTI générés par les topologies VPN par route

Lorsque vous modifiez ou supprimez une topologie VPN par route sur SMC, les objets VTI de type Machine générés automatiquement par cette topologie pour représenter les correspondants distants sont également modifiés ou supprimés. Si vous utilisez ces objets dans la configuration locale de vos firewalls SN, veillez à d'abord les supprimer avant de modifier ou supprimer une topologie dans SMC.

Déploiement de topologie VPN

Il n'est pas possible de déployer une topologie VPN depuis le serveur SMC si le nom d'un firewall SN est trop long. Les noms des topologies VPN sur les firewalls ne peuvent pas comporter plus de 127 caractères.

Configuration du routage sur SMC

Plusieurs interfaces pour joindre le serveur SMC sont configurables mais une seule passerelle par défaut sur une seule interface peut être déclarée. Vous devrez configurer manuellement le routage pour les autres interfaces. Un article de la Base de connaissance Stormshield indique la procédure à suivre (anglais uniquement).

Utilisation d'un objet réseau global dans une configuration locale

Sur un firewall SN, des objets globaux peuvent être utilisés dans une configuration locale. Or lorsque SMC déploie une configuration sur un firewall, les objets globaux existant sur le firewall sont supprimés et remplacés par les objets définis dans la configuration de SMC. Afin que la configuration locale ne cesse pas de fonctionner, vous devez forcer le déploiement des objets globaux nécessaires sur les firewalls concernés.

Pour plus d'informations, reportez-vous à la section Avertissement avant de rattacher des firewalls SN au serveur SMC.

Migration d'un firewall virtuel modèle V vers un modèle EVA

La mise à jour d'un firewall virtuel V-50, V-100 ou V-200 vers un modèle EVA via la variable %FW_UPD_SUFFIX% dans un script CLI SNS exécuté depuis le serveur SMC n'est pas supportée.

Pour contourner le problème, remplacez la variable %FW_SIZE% par la valeur XL-VM dans le script de mise à jour.

Ressources documentaires

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

Guides

- Guide d'installation Stormshield Management Center
- Guide d'administration Stormshield Management Center
- Manuel d'utilisation et de configuration des firewalls Stormshield Network Security

Vidéos

- CLI Commands and Scripts, disponible sur Institute.

Télécharger cette version

Se rendre sur votre espace personnel MyStormshield

Vous devez vous rendre sur votre espace personnel MyStormshield afin de télécharger la version 3.0 de Stormshield Management Center :

1. Connectez-vous à votre espace MyStormshield avec vos identifiants personnels.
2. Dans le panneau de gauche, sélectionnez la rubrique **Téléchargements**.
3. Dans le panneau de droite, sélectionnez le produit qui vous intéresse puis la version souhaitée.

Vérifier l'intégrité des binaires

Afin de vérifier l'intégrité des binaires Stormshield Management Center :

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 votre espace client MyStormshield, rubrique **Téléchargements**.

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/.

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