GUIDE

STORMSHIELD MANAGEMENT CENTER

GUIDE D'INSTALLATION

Version 3.9.2

Dernière mise à jour du document : 29 juin 2026

Référence : sns-fr-SMC-guide_d_installation-v3.9.2

Table des matières

1. Avant de commencer 4
1.1 Dimensionner l'environnement virtuel selon le nombre de firewalls SNS 4
1.2 Recommandations de mise en œuvre 4
2. Déployer le serveur SMC sur l'environnement virtuel 5
2.1 Déployer le fichier .OVA sur l'environnement virtuel VMware 5
2.2 Déployer les fichiers .VHD sur l'environnement virtuel Microsoft Hyper-V 5
2.3 Déployer les fichiers .qcow2 sur l'environnement virtuel KVM 5
2.4 Déployer les fichiers .qcow2 sur l'environnement virtuel Proxmox VE 6
3. Initialiser le serveur SMC depuis l'environnement virtuel 7
3.1 Initialiser automatiquement le serveur SMC 7
3.2 Initialiser manuellement le serveur SMC 8
4. Terminer l'initialisation du serveur SMC 10
5. Mettre en place la redondance de serveurs SMC 11
5.1 Comprendre la synchronisation entre les deux nœuds 11
5.2 Connaître les prérequis et recommandations 12
5.3 Activer la communication SSH entre les nœuds 13
5.4 Activer la redondance 13
5.5 Paramétrer les firewalls SNS pour la redondance 13
5.6 Désactiver et réactiver la redondance 14
5.6.1 Désactiver la synchronisation 14
5.6.2 Modifier les packages de rattachement 14
5.6.3 Réactiver la synchronisation 15
5.7 Mettre à jour SMC 15
5.8 Gérer les sauvegardes de SMC et des firewalls SNS 15
5.9 Utiliser le serveur Active Update de SMC lorsque la redondance est activée 15
6. Héberger le serveur SMC dans le cloud d'Amazon Web Services 17
6.1 Prérequis pour le déploiement du serveur SMC 17
6.1.1 Obtenir votre licence SMC 17
6.1.2 Créer une paire de clés dans la console de gestion AWS pour l'accès SSH 17
6.2 Déployer le serveur SMC depuis AWS Marketplace 18
7. Héberger le serveur SMC dans le cloud de 3DS Outscale 21
7.1 Prérequis pour le déploiement du serveur SMC 21
7.1.1 Obtenir votre licence SMC 21
7.1.2 Créer une paire de clés depuis 3DS Outscale pour l'accès SSH 21
7.1.3 Créer un Cloud privé virtuel (VPC - Virtual Private Cloud) 22
7.1.4 Créer une passerelle Internet (Internet Gateway) 22
7.1.5 Créer une route par défaut 23
7.1.6 Créer un groupe de sécurité pour les flux depuis et vers l'extérieur 23
7.2 Déployer le serveur SMC depuis 3DS Outscale Marketplace 24
7.2.1 Créer l'instance SMC 24
7.2.2 Allouer une adresse IP externe (EIP) à l'instance SMC 25
7.2.3 Initialiser l'instance SMC 25
8. Migrer un serveur SMC local vers un serveur SMC hébergé dans le cloud 27

8.1 Prérequis 27
8.2 Migrer vers le cloud d'Amazon Web Services 27
8.3 Migrer vers le cloud de 3DS Outscale 28

9. Pour aller plus loin 30

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

1. Avant de commencer

Le serveur SMC permet d'administrer de façon centralisée des firewalls SNS.

Depuis l'interface web du serveur SMC 3.9.2, vous pouvez :

- Administrer vos firewalls,
- Visualiser l'ensemble de vos firewalls,
- Garantir la cohérence des configurations,
- Accéder à l'interface d'administration web des firewalls,
- Créer des clés API pour l'utilisation de l'API publique de SMC.

Le serveur SMC est une machine virtuelle fournie sous la forme d'un fichier d'archive *.OVA* (Open Virtualization Archive) pour VMware, *.VHD* (Virtual Hard Disk) pour Microsoft Hyper-V ou *.qcow2* pour KVM.

Le serveur SMC 3.9.2 est compatible avec la version 4.3 minimum de Stormshield Network Security.

Pour installer le serveur SMC, téléchargez le fichier *smc-x.x.x.ova*, l'archive *smc-x.x.x-hyperv.zip* ou l'archive *smc-x.x.x-kvm.tar.gz* depuis votre espace personnel MyStormshield.

1.1 Dimensionner l'environnement virtuel selon le nombre de firewalls SNS

Le tableau suivant fournit une estimation des ressources minimum nécessaires pour votre machine virtuelle SMC par rapport au nombre de firewalls SNS administrés.

Le nombre de vCPU et la taille de la RAM peuvent varier en fonction du nombre d'objets, de règles, de topologies, etc. dans votre configuration.

Par ailleurs, le disque de données pour le stockage mesure 120 Go par défaut. Un espace supplémentaire peut être nécessaire en fonction de la fréquence des déploiements et des sauvegardes de configurations des firewalls SNS.

Nombre de firewalls SNS administrés	Nombre de vCPU minimal recommandé	RAM minimale recommandée
1 - 50	2	4 Go
51 - 400	4	8 Go
401 - 600	8	16 Go

1.2 Recommandations de mise en œuvre

- Nous recommandons d'installer le serveur SMC derrière un pare-feu n'autorisant que les flux nécessaires :
  - accès aux interfaces utilisateurs (SSH pour la console et HTTPS pour l'interface Web) du serveur SMC seulement pour les adresses IP des postes d'administration autorisées,
  - trafic permettant la connexion des firewalls SNS au serveur SMC sur le port TCP/1754 (port par défaut).
- Les mots de passe de l'utilisateur "root" (permettant l'accès au serveur en ligne de commande), de l'utilisateur "admin" (administrateur principal de l'interface Web) et de tout autre administrateur doivent être choisis conformément à la recommandation stipulée dans le *Guide d'administration* de SMC.

2. Déployer le serveur SMC sur l'environnement virtuel

Commencez par déployer le serveur SMC sur un environnement virtuel.

Pour connaître les versions des environnements virtuels compatibles avec SMC, veuillez consulter le document Cycle de vie produits Network Security and Tools.

Le serveur SMC utilise le modèle d'interface réseau virtuelle e1000.

Nous vous recommandons d'installer le serveur SMC dans une DMZ.

Consultez la section Dimensionner l'environnement virtuel selon le nombre de firewalls SNS pour dimensionner correctement votre environnement.

2.1 Déployer le fichier *.OVA* sur l'environnement virtuel VMware

Pour déployer le fichier :

1. Ouvrez le client VMware vSphere sur votre station d'administration.
2. Indiquez les paramètres de connexion au serveur VMware ESXi sur lequel vous souhaitez installer le serveur SMC.
3. Dans le menu **Fichier**, sélectionnez **Déployer un modèle OVF**.
4. Dans l'assistant de déploiement VMware, complétez les étapes de déploiement du fichier *.OVA*.

2.2 Déployer les fichiers *.VHD* sur l'environnement virtuel Microsoft Hyper-V

L'archive *smc-x.x.x-hyperv.zip* contient deux fichiers *.vhd* :

- smc-system.vhd,
- product-data.vhd.

1. Depuis l'outil Hyper-V Manager, sélectionnez un hyperviseur.
2. Créez une nouvelle machine virtuelle et suivez les étapes de l'assistant.
   - Dans le menu **Affecter la mémoire**, allouez 4 Go de mémoire,
   - Dans le menu **Connecter un disque dur virtuel**, cochez **Utiliser un disque dur virtuel existant** et sélectionnez le fichier *smc-system.vhd*.
3. Terminez la création de la nouvelle machine virtuelle.
4. Ouvrez les paramètres de cette machine et rendez-vous dans le menu **Contrôleur IDE 0**.
5. Cliquez sur **Ajouter** puis cochez **Disque dur virtuel** dans la partie **Support**, et sélectionnez le fichier *product-data.vhd*.
6. Validez puis connectez-vous à la machine.

2.3 Déployer les fichiers *.qcow2* sur l'environnement virtuel KVM

L'archive *smc-x.x.x-kvm.tar.gz* contient deux fichiers *.qcow* :

- smc-system.qcow2,
- product-data.qcow2.

1. Depuis l'outil virt-manager, sélectionnez l'hyperviseur KVM.
2. Créez une nouvelle machine virtuelle et suivez les étapes de l'assistant.
   - Choisissez **Importer une image disque existante** et sélectionnez le fichier *smc-system.qcow2*.
   - Allouez au moins 4 Go de mémoire et choisissez le nombre de CPU (2 minimum).
3. Cochez la case **Personnaliser la configuration avant l'installation**.
4. Terminez la création de la nouvelle machine virtuelle.
5. Ouvrez les paramètres de cette machine.
6. Rendez-vous dans le menu des paramètres du disque virtuel. Sélectionnez **SATA**.
7. Rendez-vous dans le menu **Ajouter un matériel**.
8. Cliquez sur **Stockage**, puis sélectionnez **Sélectionner ou créer un stockage personnalisé**. Sélectionnez le fichier *product-data.qcow2*.
9. Validez puis connectez-vous à la machine.

2.4 Déployer les fichiers *.qcow2* sur l'environnement virtuel Proxmox VE

L'archive *smc-x.x.x-kvm.tar.gz* contient deux fichiers *.qcow* :

- smc-system.qcow2,
- product-data.qcow2.

1. Ouvrez l'hyperviseur Proxmox VE et créez une nouvelle machine virtuelle.
2. Choisissez le fichier smc-system.qcow2 en partition principale.
3. Choisissez le fichier product-data.qcow2 en partition secondaire.
4. Complétez les étapes de déploiement.
5. Validez puis connectez-vous à la machine.

3. Initialiser le serveur SMC depuis l'environnement virtuel

La machine virtuelle SMC est déployée. À présent, vous devez initialiser le serveur manuellement ou automatiquement depuis l'environnement virtuel.

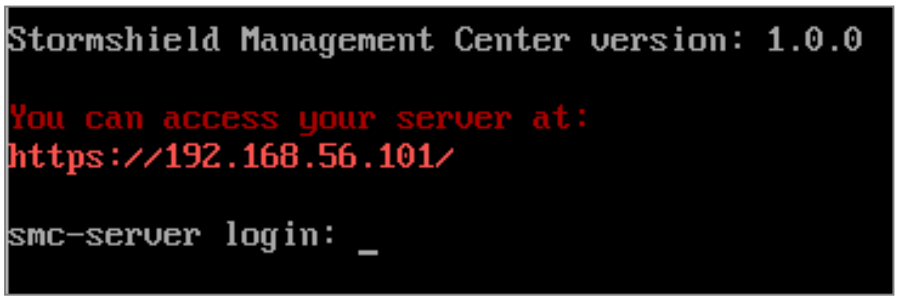
A la fin de la procédure, vous vous connecterez à l'interface web du serveur depuis l'un des navigateurs supportés :

- Microsoft Edge, dernière version stable,
- Google Chrome, dernière version stable,
- Mozilla Firefox, dernière version stable.

ASTUCE
A l'initialisation du serveur SMC, il est possible de lui attribuer manuellement une adresse IP temporaire ou de lui en attribuer une par serveur DHCP. Pour que l'attribution par DHCP fonctionne, connectez la première interface virtuelle (eth0) du serveur au bon réseau de l'infrastructure virtuelle. L'adresse IP statique définitive sera assignée dans l'assistant d'initialisation du serveur SMC décrit à la section Terminer l'initialisation du serveur SMC.

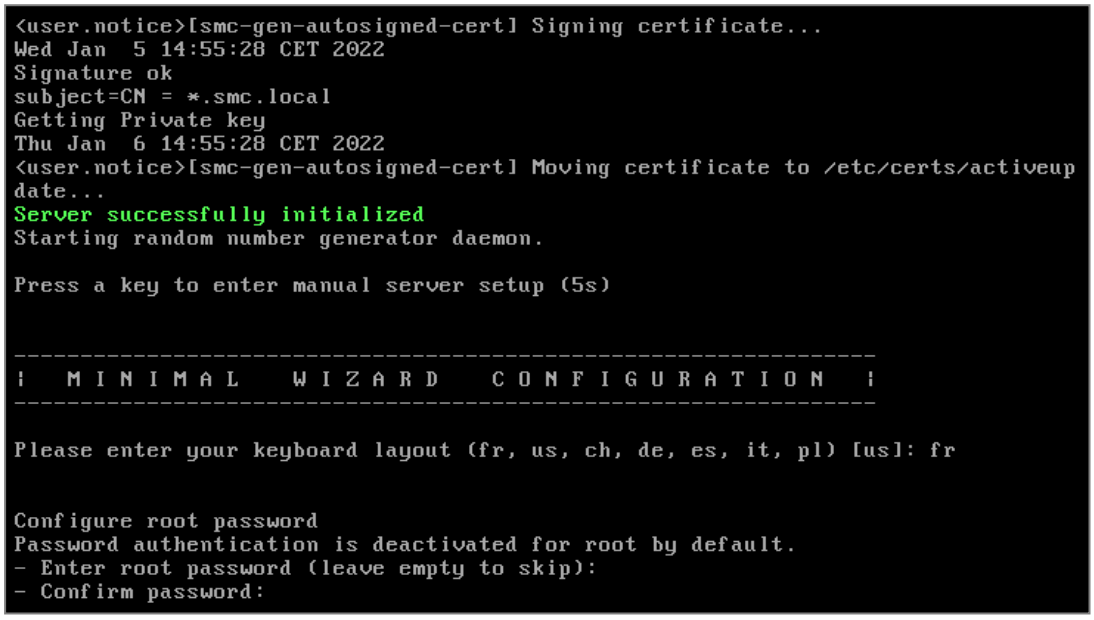
3.1 Initialiser automatiquement le serveur SMC

1. Démarrez la machine virtuelle SMC.
2. Par défaut, si la première interface du serveur est configurée pour obtenir une adresse IP par DHCP, aucune action n'est nécessaire pour initialiser le serveur.
3. A la fin de l'initialisation du serveur SMC, connectez-vous à l'adresse affichée en rouge avec un navigateur web afin de poursuivre l'initialisation.



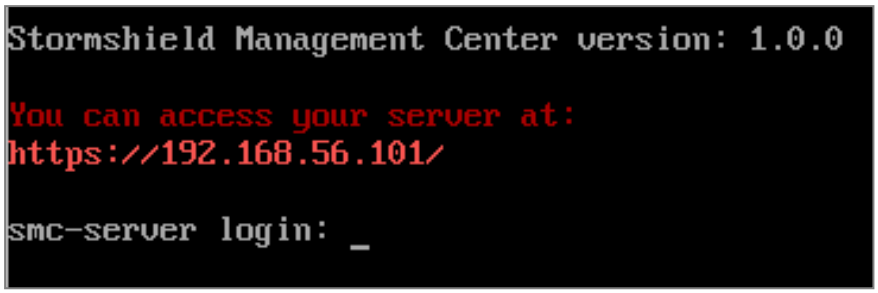
3.2 Initialiser manuellement le serveur SMC

1. Démarrez la machine virtuelle SMC.
2. Vous avez cinq secondes pour entrer dans un mode d'initialisation manuel. Si vous laissez passer les cinq secondes, une tentative d'attribution automatique d'adresse IP par DHCP est réalisée. Si cette dernière échoue, le mode d'initialisation manuel est proposé automatiquement.



3. Définissez les paramètres suivants :
   - La langue du clavier utilisée lorsque vous êtes connecté au serveur SMC en ligne de commande,
   - Le mot de passe de l'utilisateur "root" pour accéder au serveur en ligne de commande. Ce mot de passe est optionnel et par défaut l'utilisateur "root" ne possède pas de mot de passe.
   - Les paramètres de l'interface eth0 : adresse IP, masque de sous-réseau, passerelle par défaut,
   - Le fuseau horaire pour le réglage de la date,
   - La configuration de la date manuelle ou via un serveur NTP :
     - Configuration manuelle : entrez une date,
     - Via un serveur NTP : entrez un ou plusieurs serveurs NTP (adresses IP ou noms DNS séparés par une virgule). Le serveur NTP peut également être configuré après l'initialisation du serveur. Consultez le *Guide d'administration*SMC pour plus d'informations.

4. A la fin de l'initialisation du serveur SMC, connectez-vous à l'adresse affichée en rouge avec un navigateur web afin de poursuivre l'initialisation.

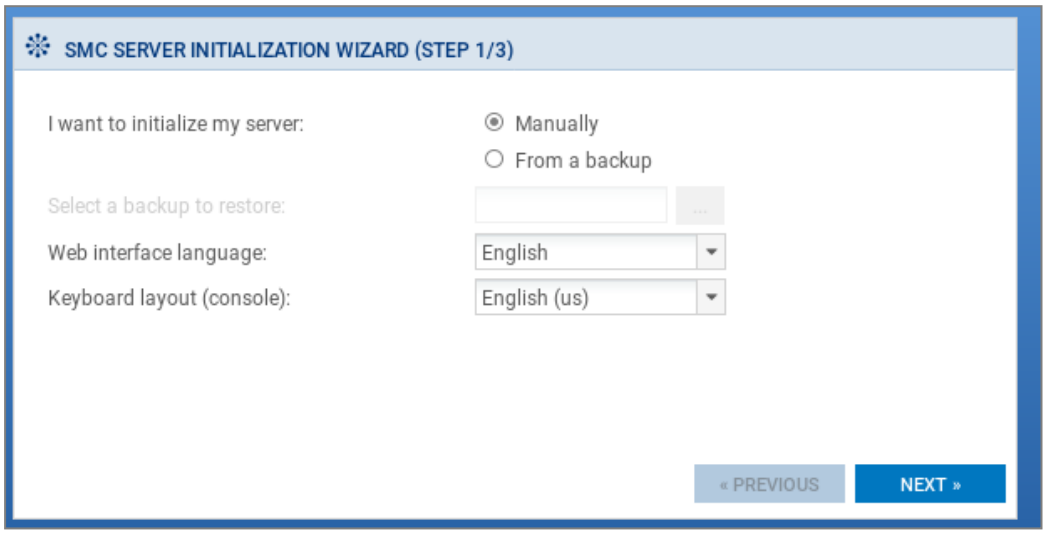


NOTE
L'assistant d'initialisation manuelle est accessible à tout moment à chaque redémarrage du serveur SMC.

4. Terminer l'initialisation du serveur SMC

Vous êtes maintenant connecté au serveur SMC depuis votre navigateur pour la première fois. L'assistant d'initialisation de SMC vous guide à travers les dernières étapes d'initialisation du serveur SMC.

1. Sélectionnez le mode d'initialisation manuel du serveur.



2. Sélectionnez la langue de l'interface web. Par défaut l'interface est dans la langue de votre navigateur. Si votre navigateur est configuré dans une autre langue que le français ou l'anglais, la langue par défaut est l'anglais.
3. Sélectionnez la langue du clavier utilisée lorsque vous êtes connecté au serveur SMC en ligne de commande.
4. Choisissez une adresse IP statique ou dynamique pour le serveur SMC.
5. Définissez le mot de passe de l'utilisateur "admin", l'administrateur principal de l'interface Web. Le mot de passe doit comporter huit caractères au minimum.
6. Cliquez sur **Appliquer**. L'initialisation est terminée.
7. Connectez-vous à l'interface web du serveur SMC avec l'utilisateur "admin" et le mot de passe définis à l'étape 5. Votre serveur SMC est à présent initialisé. Reportez-vous au *Guide d'administration Stormshield Management Center* pour savoir comment administrer les firewalls et opérer la maintenance du serveur.

5. Mettre en place la redondance de serveurs SMC

La redondance de serveurs SMC permet d'assurer la continuité de service en cas de panne du serveur SMC. Elle met en œuvre deux serveurs SMC sur lesquels la configuration est synchronisée :

- le nœud primaire
- le nœud secondaire

Lorsque la redondance est mise en place, la connexion avec les firewalls SNS est maintenue si l'un des cas suivants se produit :

- le nœud primaire rencontre un problème et les firewalls ne peuvent plus accéder à SMC,
- vous arrêtez le nœud primaire volontairement, pour une action de maintenance par exemple.

Les firewalls se connectent alors automatiquement au nœud secondaire. Vous devez vous connecter au nœud secondaire pour les administrer et les superviser.

Lorsque le nœud primaire redevient fonctionnel ou accessible, les firewalls s'y reconnectent, sans action de votre part.

ATTENTION
Nous vous recommandons de toujours utiliser **le nœud primaire** lorsqu'il est joignable afin de ne pas perdre des éléments de la configuration.

Pour en savoir plus sur le fonctionnement de la synchronisation entre les deux nœuds et le retour à la normale en cas de bascule, reportez-vous à la section Comprendre la synchronisation entre les deux nœuds.

5.1 Comprendre la synchronisation entre les deux nœuds

Les configurations des nœuds primaire et secondaire sont synchronisées toutes les heures selon les deux phases suivantes :

- le nœud primaire sauvegarde sa configuration à chaque heure passée de cinq minutes (par exemple 9h05),
- le nœud secondaire télécharge la sauvegarde de configuration depuis le nœud primaire à chaque heure passée de quinze minutes (par exemple 9h15). Les configurations sont alors synchronisées.

Cette fréquence n'est pas paramétrable.

Lors de la synchronisation, toutes les données nécessaires à la supervision et à l'administration des firewalls sont répliquées. La configuration synchronisée n'inclut pas les éléments suivants :

- La licence du serveur SMC. Vous devez installer une licence sur chaque nœud.
- Les configurations IP et DNS du serveur SMC.
- Le mot de passe de l'utilisateur "root".
- La configuration de la synchronisation NTP.
- Toute configuration système personnalisée réalisée par un administrateur.

La synchronisation n'a lieu que si vous avez réalisé une modification de configuration dans l'heure, via l'interface web d'administration, via l'API publique ou via une commande `smc-*`.

Ainsi, si vous modifiez directement un des fichiers du dossier `/data/config` (par exemple le fichier *cfgcheck.ini* ou le fichier *smc-webservices.local*), ils ne seront synchronisés que lors d'une prochaine modification de configuration via l'interface web d'administration, via l'API publique ou via une commande `smc-*`.

Les actions suivantes via l'interface web d'administration n'entraînent pas de synchronisation :

- La modification des paramètres réseau de SMC,
- L'ajout de nouveaux administrateurs,
- La modification du contrôle de cohérence du mode "Diffusion restreinte",
- L'exécution de scripts CLI SNS.

En conséquence, les trois premières actions doivent être réalisées manuellement sur les deux nœuds.

En cas de bascule de la connexion des firewalls sur le nœud secondaire, deux cas de figure sont possibles pour le retour à la normale :

- Le nœud primaire est éteint. Il n'y a donc plus de synchronisation entre les deux nœuds. Si vous effectuez des modifications de configuration depuis le nœud secondaire, lorsque le nœud primaire redémarre, il récupère la configuration du nœud secondaire.
- Les deux nœuds communiquent mais la connexion entre le nœud primaire et les firewalls rencontre un problème. Les firewalls se connectent automatiquement au nœud secondaire. La synchronisation du primaire vers le secondaire continue alors de fonctionner. Si vous administrez les firewalls depuis le nœud secondaire de façon temporaire, les modifications de configuration seront écrasées par la synchronisation entre les deux nœuds.

> **ATTENTION**
> Si vous êtes dans cette situation, nous vous recommandons de rétablir la connexion entre le nœud primaire et les firewalls plutôt que d'administrer depuis le nœud secondaire.

5.2 Connaître les prérequis et recommandations

Pour mettre en place la redondance, vous devez suivre les prérequis et recommandations suivants :

- Les deux nœuds doivent être installés et initialisés, selon la procédure indiquée dans le *Guide d'installation*.
- Nous recommandons d'installer les deux nœuds sur le même environnement virtuel pour un fonctionnement optimal.
- Ils doivent disposer de la même version de SMC. Si ce n'est pas le cas, la redondance ne peut pas fonctionner.
- Nous recommandons de dimensionner les machines virtuelles de façon identique (vCPU et RAM).
- Les deux nœuds doivent appliquer la même configuration NTP, pour être à la même heure et dans le même fuseau horaire. Pour plus d'informations, reportez-vous à la section Modifier la date via le protocole NTP du *Guide d'administration*.
- Chaque nœud doit disposer de sa propre licence supportant chacune le même nombre de firewalls. Si l'un des deux ne possède pas de licence, la redondance ne peut pas fonctionner.
- Les deux nœuds ne doivent avoir aucune adresse IP en commun.

- La communication SSH entre les deux nœuds doit être possible. Pour plus d'informations, reportez-vous à la section suivante.

5.3 Activer la communication SSH entre les nœuds

Le protocole SCP, utilisé pour la synchronisation des deux nœuds, nécessite une authentification par clés SSH pour fonctionner.

Vous devez générer une paire de clés pour chaque nœud, puis transférer la clé publique sur le nœud opposé.

Réalisez la procédure suivante en veillant bien à respecter les chemins et noms de fichiers indiqués :

1. Connectez-vous au premier nœud en SSH.
2. Exécutez la commande suivante pour générer la paire de clés :
   `ssh-keygen -t ecdsa -b 256 -f /data/redundancy/keys/redundancy -N ""`
3. Exécutez la commande suivante pour transférer la clé publique sur le nœud opposé :
   `scp /data/redundancy/keys/redundancy.pub root@<REMOTE_IP>:/data/ssh/authorized_keys.root`
4. Répétez l'action sur le second nœud.

5.4 Activer la redondance

Assurez-vous que les prérequis ci-dessus sont respectés puis activez la redondance :

1. Connectez-vous au nœud primaire en SSH.
2. Exécutez la commande suivante : `smc-redundancy --secondary <IP_NOEUD_SECONDAIRE>`.
   La redondance est alors active et la première synchronisation depuis le nœud primaire vers le nœud secondaire démarre immédiatement.
3. Pour vous assurer que la redondance fonctionne, consultez à tout moment le fichier */var/log/redundancy.log*.

NOTE
Le nœud primaire utilise l'adresse IP de sa première interface réseau pour communiquer avec le nœud secondaire. Le nœud secondaire utilise l'adresse IP indiquée dans la commande ci-dessus.
Si vous modifiez l'adresse IP de l'un des nœuds, la redondance ne fonctionne plus. Vous devez l'activer de nouveau avec la nouvelle adresse.

Dans le cas où vous utilisez des serveurs externes dans votre configuration, par exemple un serveur Syslog distant pour l'envoi des journaux de SMC ou bien un serveur LDAP ou Radius pour l'authentification des administrateurs, assurez-vous que les deux nœuds peuvent communiquer avec ces serveurs. L'adresse IP ou le nom de domaine du serveur externe doit être joignable par les deux nœuds.

5.5 Paramétrer les firewalls SNS pour la redondance

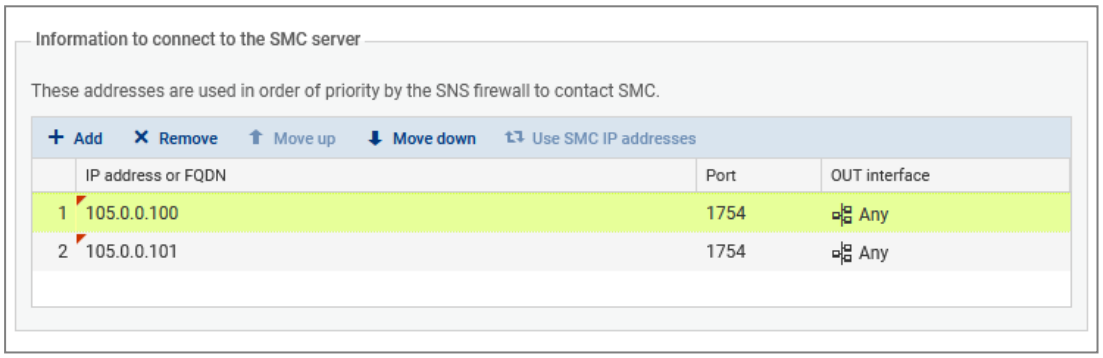
Une fois la redondance activée, vous devez indiquer aux firewalls les adresses IP des deux serveurs SMC à contacter. Ces informations sont données aux firewalls à travers le package de

rattachement à SMC :

- pour les firewalls qui étaient déjà connectés au nœud primaire avant la mise en place de la redondance, vous devez générer et installer des nouveaux packages de rattachement contenant les adresses des deux nœuds, comme indiqué dans la procédure ci-dessous.
- pour les nouveaux firewalls, suivez la procédure ci-dessous.

Pour indiquer les adresses IP des deux serveurs SMC dans le package de rattachement d'un firewall :

1. Suivez la procédure habituelle de rattachement d'un firewall. Pour plus d'informations, reportez-vous à la section Rattacher des firewalls SNS au serveur SMC du *Guide d'administration*.
2. Dans l'encart **Informations de connexion au serveur SMC**, indiquez les adresses IP des deux serveurs :



Dans l'exemple ci-dessus, le nœud primaire possède l'adresse 105.0.0.100 et le nœud secondaire possède l'adresse 105.0.0.101.

La commande `smc-import-firewalls` permet de générer plusieurs packages de rattachement à la fois. Pour plus d'informations, reportez-vous à la section Importer des firewalls en ligne de commande du *Guide d'administration*.

5.6 Désactiver et réactiver la redondance

Pour arrêter définitivement la redondance, vous devez désactiver la synchronisation entre les nœuds, puis modifier les packages de rattachement afin que les firewalls ne puissent plus se connecter au nœud secondaire.

Dans d'autres cas, par exemple lors d'une restauration de sauvegarde de configuration du serveur SMC, vous devez désactiver temporairement la synchronisation, puis la réactiver. Dans ce cas, vous n'avez pas besoin de modifier les packages de rattachement. Pour plus d'informations sur la restauration de sauvegarde, reportez-vous à la section Gérer les sauvegardes de SMC et des firewalls SNS du *Guide d'administration*.

5.6.1 Désactiver la synchronisation

1. Connectez-vous au nœud primaire en SSH.
2. Exécutez la commande suivante : `smc-redundancy --disable`.

5.6.2 Modifier les packages de rattachement

Une fois la synchronisation désactivée entre les deux nœuds, nous vous recommandons de générer de nouveaux packages de rattachement pour chaque firewall connecté à SMC, en

indiquant l'adresse IP de l'unique serveur SMC auquel ils doivent se connecter à présent.

Ainsi, ils n'essaieront plus de se connecter à l'ancien nœud secondaire dont la configuration ne serait plus synchronisée ou qui aurait été supprimé.

5.6.3 Réactiver la synchronisation

Pour réactiver la synchronisation entre les deux nœuds après une désactivation temporaire :

1. Connectez-vous au nœud primaire en SSH.
2. Exécutez la commande suivante : `smc-redundancy --enable`.

5.7 Mettre à jour SMC

Pour mettre à jour vos serveurs SMC lorsqu'une redondance est en place, procédez dans l'ordre suivant :

1. Éteignez le nœud secondaire.
2. Mettez à jour le nœud primaire comme indiqué à la section Mettre à jour le serveur SMC du *Guide d'administration*.
3. Attendez la fin de la mise à jour et la reconnexion des firewalls.
4. Démarrez le nœud secondaire puis mettez-le à jour.

Nous vous recommandons de réaliser les mises à jour en dehors des phases de synchronisation des deux nœuds. Pour plus d'informations, reportez-vous à la section Comprendre la synchronisation entre les deux nœuds.

Pendant le processus de mise à jour, aucune synchronisation ne peut avoir lieu entre les deux nœuds afin d'éviter toute perte de données.

5.8 Gérer les sauvegardes de SMC et des firewalls SNS

Si vous souhaitez restaurer une sauvegarde de configuration de SMC alors que la redondance est activée, vous devez suivre ces étapes :

1. Désactivez la synchronisation entre les deux nœuds selon la procédure correspondante.
2. Restaurez la sauvegarde sur chacun des nœuds. La sauvegarde doit provenir du nœud à restaurer. Pour plus d'informations, reportez-vous à la section Sauvegarder et restaurer la configuration du serveur SMC du *Guide d'administration*.
3. Lorsque les sauvegardes sont restaurées sur les deux nœuds, assurez-vous que les deux serveurs ont redémarré et possèdent bien la même configuration.
4. Après restauration de la sauvegarde, les deux nœuds ont le même adressage IP. Modifiez l'adressage pour revenir à la configuration IP initiale.
5. Activez de nouveau la synchronisation selon la procédure correspondante.

De plus, si vous avez activé la sauvegarde automatique de la configuration du serveur et des firewalls ainsi que la redondance, il n'est pas possible de récupérer sur un nœud les sauvegardes réalisées par l'autre nœud.

5.9 Utiliser le serveur Active Update de SMC lorsque la redondance est activée

SMC peut être utilisé en tant que point de distribution Active Update.

Si vous souhaitez utiliser cette fonctionnalité et que vous avez activé la redondance, vous devez réaliser sur les firewalls la procédure indiquée à la section Utiliser le serveur Active Update de SMC du *Guide d'administration* avec les informations de chaque nœud. Ainsi, les firewalls auront les adresses IP et certificats permettant d'utiliser les deux nœuds en tant que points de distribution Active Update.

Dans le cas où vous souhaitez mettre à jour les bases Active Update manuellement via le bouton **Mettre à jour les bases maintenant** de l'interface web d'administration ou via le script de téléchargement des bases, vous devez réaliser cette action sur les deux nœuds. Pour plus d'informations, reportez-vous à la section Télécharger les bases de données Active Update du *Guide d'administration*.

6. Héberger le serveur SMC dans le cloud d'Amazon Web Services

Le serveur SMC peut être hébergé dans le cloud d'Amazon Web Services (AWS) en mode Bring Your Own License (BYOL).

Un serveur SMC hébergé dans le cloud peut administrer des firewalls SNS hébergés également dans le cloud ou bien hébergés localement.

Suivez d'abord les prérequis ci-dessous. Choisissez ensuite sur AWS Marketplace une instance EC2 (Amazon Elastic Compute Cloud) adaptée à vos besoins pour héberger votre serveur SMC puis déployez le serveur avec le service CloudFormation.

6.1 Prérequis pour le déploiement du serveur SMC

Afin de déployer un serveur SMC dans le cloud d'AWS, vous devez :

- obtenir une licence SMC auprès de Stormshield,
- créer une paire de clés sur AWS pour sécuriser l'accès SSH à votre instance SMC.

Ces actions peuvent être réalisées avant ou pendant le déploiement de votre serveur SMC depuis AWS Marketplace.

6.1.1 Obtenir votre licence SMC

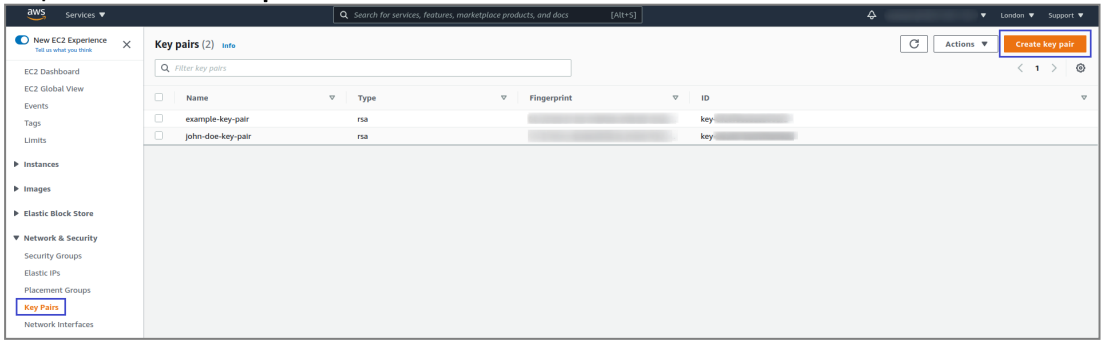
Le serveur SMC nécessite une licence logicielle pour fonctionner. La licence dépend du nombre de firewalls administrés par SMC.

Veuillez contacter votre distributeur Stormshield pour obtenir une licence.

6.1.2 Créer une paire de clés dans la console de gestion AWS pour l'accès SSH

Pour sécuriser l'accès SSH à votre serveur SMC, vous devez sélectionner une paire de clés existante lors de la création de la pile CloudFormation depuis AWS Marketplace, comme indiqué dans la section Déployer le serveur SMC depuis AWS Marketplace. Si une telle paire de clés n'existe pas ou si vous souhaitez en utiliser une nouvelle pour cette instance, vous pouvez la créer comme suit depuis le service EC2 de la console de gestion AWS :

1. Dans le menu **Services** du bandeau supérieur, sélectionnez **EC2** dans la section **Calcul**.
2. Sélectionnez le menu de gauche **Réseau et sécurité / Paires de clés**.
3. Cliquez sur **Créer une paire de clés** en haut à droite.



4. Indiquez le nom de la paire de clés.
5. Choisissez le type de la paire et le format de fichier *.pem*.

6. Cliquez sur **Créer une paire de clés**.
7. Téléchargez la paire de clés et stockez-là dans un endroit sûr sur votre ordinateur.

Lorsque vous vous connectez à votre serveur SMC en SSH, indiquez en argument de connexion le fichier d'identification correspondant à cette paire de clés. Par exemple :

```
ssh -i demo_keypair.pem ec2-user@<your_elastic_IP>
```

NOTE
Vous ne pouvez pas vous connecter à votre serveur SMC en SSH directement avec l'utilisateur `root`. Vous devez vous connecter avec l'utilisateur `ec2-user`.

6.2 Déployer le serveur SMC depuis AWS Marketplace

Depuis AWS Marketplace, déployez votre serveur SMC simplement avec le service AWS CloudFormation :

1. Accédez à AWS Marketplace.
2. Si ce n'est déjà fait, identifiez-vous en utilisant le compte Amazon.com.
3. Allez sur la page du produit SMC.
4. Sur la page de présentation, rendez-vous dans la section **Pricing Information** afin de voir le type d'instance EC2 dont vous avez besoin en fonction du nombre de firewalls administrés :

Instance AWS	Processeur virtuel	RAM (Go)	Dimensionnement SMC	Nombre de firewalls
t3.medium	2	4	Small	<50
t3.xlarge	4	16	Medium	<500
t3.2xlarge	8	32	Large	<1000

En fonction de l'instance sélectionnée, vous pouvez estimer le coût de votre serveur virtuel.

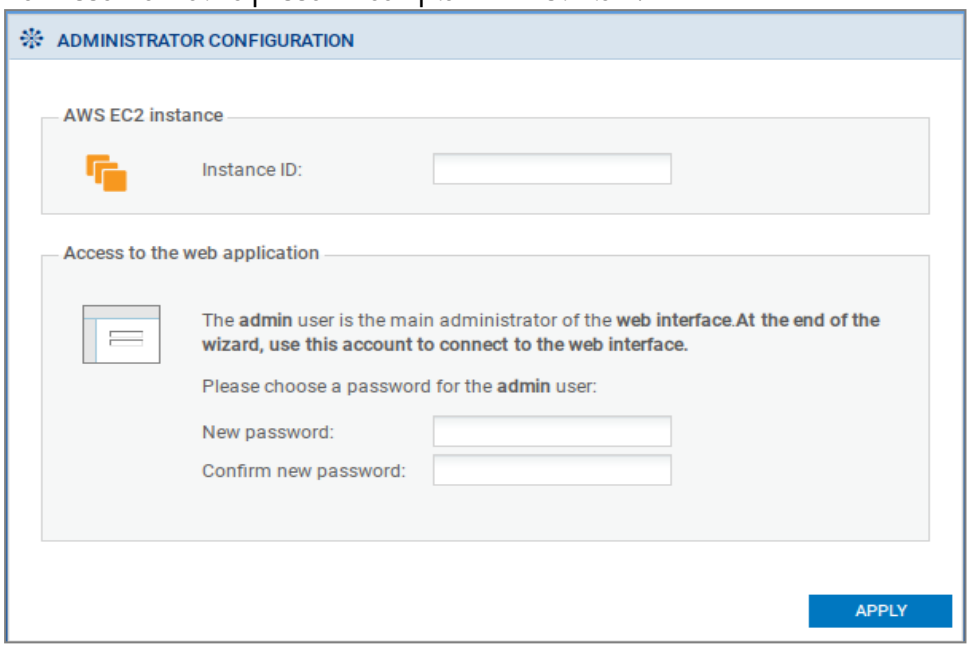
IMPORTANT
Le stockage EBS n'est pas inclus dans les frais. SMC nécessite 130 Go de stockage EBS.

IMPORTANT
Le montant comprend uniquement les frais AWS. La licence SMC n'est pas émise par AWS, car le serveur est fourni avec un modèle Bring Your Own License (BYOL). La licence du logiciel SMC doit être commandée auprès de votre distributeur. Consultez la section Obtenir votre licence SMC.

5. Cliquez sur **Continue to Subscribe** en haut de la page.
6. Lisez les conditions d'utilisation et cliquez sur **Accept Terms**.
7. Cliquez sur **Continue to Configuration**.
8. Si vous ne souhaitez pas déployer la dernière version disponible du serveur SMC, sélectionnez la version souhaitée.

9. Sélectionnez la région dans laquelle vous souhaitez déployer votre serveur SMC. Vous devez le déployer dans la région dans laquelle votre VPC est déjà déployé et éventuellement vos autres serveurs.
   La région dans laquelle vous allez déployer l'instance EC2 exécutant SMC peut avoir un impact sur plusieurs facteurs, notamment :
   - les frais AWS pour cette instance,
   - les performances du réseau,
   - la législation locale.
10. Cliquez sur **Continue to Launch**.
11. Laissez *Launch CloudFormation* dans la section **Choose Action**.
12. Sur la page **Créer une pile**, cliquez sur **Suivant** pour configurer votre pile CloudFormation. La pile comprend le serveur SMC et la configuration réseau permettant d'y accéder.
13. Complétez les paramètres :
    1. Sélectionnez l'instance dans le champ **InstanceType**.
    2. Dans le champ **KeyPairName**, sélectionnez la paire de clés que vous souhaitez installer sur votre instance, pour sécuriser l'accès en SSH au serveur SMC. Reportez-vous à la section Créer une paire de clés dans la console de gestion AWS pour l'accès SSH pour plus d'informations.
    3. Vous pouvez laisser les valeurs par défaut des champs **SMCSubnet** et **VirtualPrivateCloudNetwork** ou alors entrer vos valeurs souhaitées.
    4. Entrez une adresse dans le champ **SourceIPAddress**.
14. Cliquez sur **Suivant**.
15. Sur la page **Configurer les options de pile**, configurez les options proposées si besoin et cliquez sur **Suivant**.
16. Cliquez sur **Créer une pile**.
17. Attendez la fin de la création de la pile indiquée par le statut CREATE_COMPLETE sur la gauche de la page.
18. Accédez au service EC2 de votre console de gestion AWS pour visualiser l'instance créée par la pile CloudFormation.
19. Sélectionnez l'instance créée.
20. Cliquez sur le lien *https://EC2 Adresse IP Elastic>/admin* pour accéder à la console d'administration de SMC avec votre navigateur Web.
21. L'assistant d'initialisation du serveur SMC demande l'ID de l'instance EC2. Il est disponible dans le menu **Services / Calcul / EC2 / Instances / Instances** de la console de gestion AWS.

22. Définissez le mot de passe du compte administrateur.



23. Cliquez sur **Appliquer**. Votre serveur SMC est prêt à être utilisé.

NOTE
Le serveur SMC déployé depuis AWS est accessible depuis l'interface web d'administration et en SSH sur le port 22.
L'accès en console n'est pas possible.

7. Héberger le serveur SMC dans le cloud de 3DS Outscale

Le serveur SMC peut être hébergé dans le cloud de 3DS Outscale en mode Bring Your Own License (BYOL).

Un serveur SMC hébergé dans le cloud peut administrer des firewalls SNS hébergés également dans le cloud ou bien hébergés localement.

Suivez d'abord les prérequis ci-dessous. Choisissez ensuite sur 3DS Outscale Marketplace une instance adaptée à vos besoins pour héberger votre serveur SMC puis déployez le serveur.

7.1 Prérequis pour le déploiement du serveur SMC

Afin de déployer un serveur SMC dans le cloud de 3DS Outscale, vous devez :

- obtenir une licence SMC auprès de Stormshield,
- créer une paire de clés SSH (Keypair) pour sécuriser l'accès SSH à votre instance SMC,
- créer un Cloud privé virtuel (VPC - *Virtual Private Cloud*),
- créer une passerelle internet (*Internet Gateway*),
- créer une route par défaut,
- créer un groupe de sécurité pour les flux avec l'extérieur,
- créer l'instance SMC,
- allouer une adresse IP externe (EIP) à l'instance SMC,
- créer l'interface réseau privée de l'instance SMC,
- initialiser l'instance SMC.

Ces actions peuvent être réalisées avant ou pendant le déploiement de votre serveur SMC depuis 3DS Outscale Marketplace.

7.1.1 Obtenir votre licence SMC

Le serveur SMC nécessite une licence logicielle pour fonctionner. La licence dépend du nombre de firewalls administrés par SMC.

Veuillez contacter votre distributeur Stormshield pour obtenir une licence.

7.1.2 Créer une paire de clés depuis 3DS Outscale pour l'accès SSH

Pour sécuriser l'accès SSH à votre serveur SMC, vous devez sélectionner une paire de clés existante lors de la création de votre instance SMC depuis 3DS Outscale Marketplace, comme indiqué dans la section Déployer le serveur SMC depuis 3DS Outscale Marketplace.

Si une telle paire de clés n'existe pas ou si vous souhaitez en utiliser une nouvelle pour cette instance, vous pouvez la créer comme suit depuis la console COCKPIT 3DS Outscale :

1. Ouvrez le menu **Réseau / Sécurité**.
2. Sélectionnez **Keypairs**.
3. Cliquez sur **Créer**.
4. Entrez un nom pour la nouvelle clé SSH et cliquez sur **Créer**. Une clé est générée et une

boîte de dialogue s'ouvre pour la télécharger.

5. Téléchargez la paire de clés et stockez-là dans un endroit sûr sur votre ordinateur.

Lorsque vous vous connectez à votre serveur SMC en SSH, indiquez en argument de connexion le fichier d'identification correspondant à cette paire de clés. Par exemple :

```
ssh -i demo_keypair.pem outscale@<your_elastic_IP>
```

> **NOTE**
> Vous ne pouvez pas vous connecter à votre serveur SMC en SSH directement avec l'utilisateur `root`. Vous devez vous connecter avec l'utilisateur `outscale`.

7.1.3 Créer un Cloud privé virtuel (VPC - *Virtual Private Cloud*)

Le VPC est le réseau virtuel dans lequel sera déployé le serveur SMC. Il est constitué d'un sous-réseau auquel sera attachée l'interface de SMC.

Créer le VPC

Dans la console COCKPIT 3DS OUTSCALE, menu **VPC** :

1. Sélectionnez **VPC**.
2. Cliquez sur **Créer** puis sur **Mode expert**.
3. Entrez un nom pour le VPC, ainsi que le réseau associé en notation CIDR (exemple : *172.21.0.0/16*).
4. Validez en cliquant sur **Créer**.

Créer le sous-réseau du VPC

1. Sélectionnez le VPC créé précédemment. Le détail du VPC s'affiche dans la partie inférieure de l'écran de configuration.
2. Cliquez sur **Créer un subnet**.
3. Entrez un nom pour le VPC, ainsi que le réseau associé en notation CIDR (exemple : *172.21.0.0/24*).
   Ce sous-réseau doit obligatoirement être inclus dans le réseau du VPC.
4. Sélectionnez la zone géographique dans laquelle ce sous-réseau est disponible.
5. Validez en cliquant sur **Créer**.

7.1.4 Créer une passerelle Internet (*Internet Gateway*)

Il s'agit de la passerelle d'accès à Internet pour le serveur SMC.

Créer la passerelle Internet

Dans la console COCKPIT 3DS OUTSCALE, menu **VPC** :

1. Sélectionnez **Internet gateways**.
2. Cliquez sur **Créer.**
3. Validez en cliquant sur **Créer**.

Rattacher la passerelle Internet au VPC

1. Sélectionnez la passerelle créée à l'étape précédente.
2. Cliquez sur **Attacher**.
3. Sélectionnez le VPC créé précédemment.
4. Validez en cliquant sur **Attacher**.

7.1.5 Créer une route par défaut

L'objectif est de créer une route par défaut vers la passerelle internet pour tous les flux sortants.

Créer la route par défaut dans la table de routage du VPC

Dans la console COCKPIT 3DS OUTSCALE, menu **Réseau / Sécurité** :

1. Sélectionnez **Route tables**.
2. Sélectionnez la table de routage correspondant au VPC précédemment créé.
   Le détail de la table de routage s'affiche dans la partie inférieure de l'écran de configuration.
3. Dans le détail de la table de routage, cliquez sur **Créer une route**.
4. Dans le champ **Cible**, sélectionnez la passerelle Internet précédemment créée.
5. Cliquez sur le bouton **Toutes les IP**.
   Le champ **Destination** est automatiquement complété avec la valeur 0.0.0.0/0.
6. Validez en cliquant sur **Créer**.

Attacher cette table de routage au sous-réseau public du VPC

1. Sélectionnez la table de routage correspondant au VPC précédemment créé.
2. Cliquez sur **Attacher**.
3. Sélectionnez le sous réseau public du VPC.
4. Cliquez sur **Attacher** pour valider la configuration.
   La colonne **Associations** reflète ce nouvel état (passage de 0 à 1).

7.1.6 Créer un groupe de sécurité pour les flux depuis et vers l'extérieur

Ce groupe de sécurité rassemble les règles de flux autorisés depuis les réseaux externes vers SMC, et depuis les réseaux protégés vers l'extérieur.
Afin de pouvoir accéder à SMC, les flux entrants autorisés sont les suivants :

- SSH : accès en console au serveur SMC,
- HTTPS : accès à l'interface Web d'administration du serveur SMC,
- TCP/1754 : port par défaut pour la connexion des firewalls SNS.

Créer le groupe de sécurité

Dans la console COCKPIT 3DS OUTSCALE, menu **Réseau / Sécurité** :

1. Sélectionnez **Security groups**.
2. Cliquez sur **Créer**.
3. Nommez le groupe de sécurité.
4. Ajoutez une description.

5. Sélectionnez le VPC précédemment créé.
6. Cliquez sur **Créer**.

Créer les règles de sécurité correspondant aux flux autorisés avec l'extérieur

1. Sélectionnez le groupe de sécurité précédemment créé.
   La liste des règles attachées au groupe de sécurité s'affiche dans la partie inférieure de l'écran de configuration.
2. Dans la liste des règles, cliquez sur **Créer une règle**.
3. Sélectionnez le mode **Entrant**.
4. Sélectionnez le protocole **SSH**.
5. Cliquez sur **Toutes les IP**.
6. Cliquez sur le symbole "+".
7. Recommencez les étapes 3 à 6 avec le protocole **HTTPS**.
8. Recommencez les étapes 3 à 6 avec les valeurs **Entrant**, **Personnalisé, TCP**, **1754** et **Toutes les IP**.
9. Validez les règles en cliquant sur **Créer**.

IMPORTANT
Une règle autorisant des flux sortants est automatiquement créée.
Cette règle ne doit pas être supprimée car elle autorise, notamment, les flux sortants nécessaires pour les mises à jour de sécurité des instances déployées dans le VPC.

La liste des règles de flux autorisés pour le groupe de sécurité prend donc la forme suivante :

+ CREATE RULE | − DELETE RULE

Service	Type	Protocol	From Port	To Port	CIDR
SSH	inbound	tcp	22	22	0.0.0.0/0
HTTPS	inbound	tcp	443	443	0.0.0.0/0
Custom	inbound	tcp	1754	1754	0.0.0.0/0
Custom	outbound	-1			0.0.0.0/0
Custom	inbound	-1			

7.2 Déployer le serveur SMC depuis 3DS Outscale Marketplace

L'instance SMC déployée est rattachée aux VPC, groupe de sécurité pour les flux avec l'extérieur, clé SSH et sous-réseau précédemment créés.

7.2.1 Créer l'instance SMC

Dans la console COCKPIT 3DS OUTSCALE, menu **Calcul** :

1. Sélectionnez **Instances**.
2. Cliquez sur **Créer** puis **Mode expert**.
3. Nommez l'instance et cliquez sur **Suivant**.
4. Indiquez SMC dans le champ de recherche puis sélectionnez l'image SMC souhaitée.
5. Cliquez sur **Suivant**.

6. Sélectionnez les caractéristiques de votre instance, en fonction des recommandations matérielles minimum :
    - Le type de **CPU**,
    - Le niveau de **Performance** souhaité (paramètre 3DS OUTSCALE),
    - Le nombre de **Cœurs**,
    - La quantité de **Mémoire** (Go) allouée à la machine virtuelle.
7. Cliquez sur **Suivant**.
8. Sélectionnez le **VPC** créé précédemment.
9. Sélectionnez le sous-réseau du VPC créé précédemment.
10. Choisissez l'adresse IP à associer à l'interface publique du serveur SMC.
    Cette adresse doit appartenir au sous-réseau sélectionné à l'étape 9. Vous pouvez également laisser ce champ vide. 3DS Outscale assigne automatiquement une adresse disponible du sous-réseau.
11. Sélectionnez la zone géographique dans laquelle ce sous-réseau est disponible.
12. Cliquez sur **Suivant**.
13. Sélectionnez le groupe de sécurité pour les flux avec l'extérieur.
14. Cliquez sur **Suivant**.
15. Sélectionnez la clé SSH créée en tout début de procédure.
16. Cliquez deux fois sur **Suivant**.
    Un résumé de l'instance vous est proposé.
17. Validez la création de l'instance en cliquant sur **Créer**.

7.2.2 Allouer une adresse IP externe (EIP) à l'instance SMC

Créer l'adresse IP externe

Dans la console COCKPIT 3DS OUTSCALE, menu **Réseau / Sécurité** :

1. Sélectionnez **IP externes**.
2. Cliquez sur **Allouer**.
3. Nommez l'adresse IP externe.
4. Validez en cliquant sur **Allouer**.
   Une adresse IP externe est créée.

Allouer l'adresse à l'instance

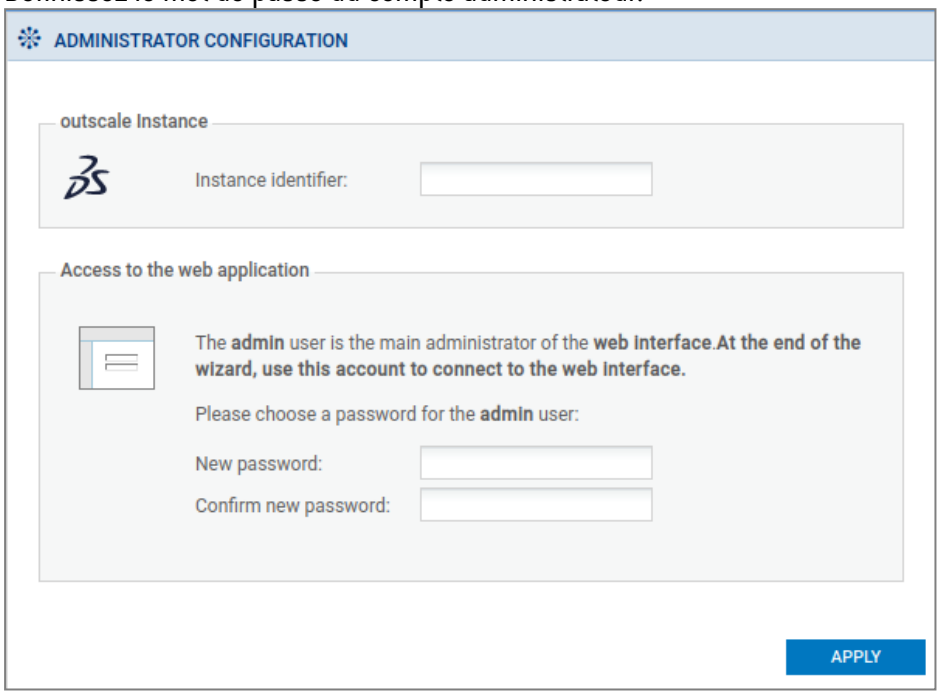
1. Sélectionnez l'adresse IP externe précédemment créée.
2. Cliquez sur **Associer instance**.
3. Sélectionnez votre instance SMC.
4. Validez en cliquant sur **Associer**.

7.2.3 Initialiser l'instance SMC

Dans la console COCKPIT 3DS OUTSCALE, menu **Calcul** :

1. Sélectionnez **Instances**.
2. Cliquez sur l'adresse IP de la colonne **IP externe** de votre instance SMC.
   Cette action va copier l'adresse IP externe de l'instance SMC.

3. Ouvrez une nouvelle page de navigateur web et collez l'adresse IP précédée de *https://* pour accéder à la console d'administration SMC.
4. Entrez l'identifiant de l'instance dans l'assistant d'initialisation du serveur SMC. Vous pouvez le trouver dans le menu **Calcul** > **Instances** > **Instances** de la console COCKPIT 3DS OUTSCALE.
5. Définissez le mot de passe du compte administrateur.



6. Cliquez sur **Appliquer**. Votre serveur SMC est prêt à être utilisé.

NOTE
Le serveur SMC déployé depuis 3DS Outscale est accessible depuis l'interface web d'administration et en SSH sur le port 22.
L'accès en console n'est pas possible.

8. Migrer un serveur SMC local vers un serveur SMC hébergé dans le cloud

Si vous souhaitez héberger dans le cloud votre serveur SMC local, vous avez la possibilité de le migrer de votre hyperviseur vers le cloud d'Amazon Web Services ou de 3DS Outscale tout en conservant sa configuration et la configuration des firewalls SNS.

8.1 Prérequis

Pour migrer un serveur SMC local existant dans le cloud, vous devez avoir installé au préalable un serveur SMC dans le cloud d'AWS ou de 3DS Outscale. Pour savoir comment faire, consultez les sections :

- Héberger le serveur SMC dans le cloud d'Amazon Web Services
- Héberger le serveur SMC dans le cloud de 3DS Outscale

8.2 Migrer vers le cloud d'Amazon Web Services

Afin de migrer un serveur SMC local existant dans le cloud d'AWS, les grandes étapes suivantes sont nécessaires :

- Modifier la configuration du serveur SMC local,
- Créer un utilisateur ec2-user sur le serveur SMC local,
- Migrer le serveur vers le serveur SMC hébergé dans le cloud d'AWS préalablement installé.

Veuillez suivre la procédure détaillée suivante pour migrer :

1. Connectez-vous au serveur SMC local en SSH avec l'utilisateur "root".
2. Exécutez les commandes suivantes pour modifier la configuration du serveur :
```
sed -i -E 's/^#*(PasswordAuthentication).*$/\1 no/g' /data/users/ssh/sshd_config
sed -i -E 's/^#*(PermitRootLogin).*$/\1 no/g' /data/users/ssh/sshd_config
sed -i -E 's/(\/data\/ssh)(.*)/\1\/\%u\2/' /data/users/ssh/sshd_config
```
3. Exécutez les commandes suivantes pour créer l'utilisateur ec2-user sur le serveur SMC local :
```
echo "ec2-user:x:99999:65534::/home/ec2-user:/bin/sh" >> /etc/passwd
echo "ec2-user:!:18908:0:99999:7:::" >> /etc/shadow
echo "ec2-user ALL=(ALL) NOPASSWD: ALL" > /etc/sudoers.d/ec2-user
echo "[[ \${USER} == "ec2-user" ]] && sudo -i" > /etc/profile.d/ec2-user.sh
```
4. Depuis le serveur SMC sur AWS, copiez le dossier *ec2-user* et son contenu situé sous `/data/ssh/` sur le serveur SMC local.
5. Vérifiez que le dossier *ec2-user* contient un fichier *authorized_keys.ec2-user*.
6. Exécutez la commande suivante pour accorder les droits nécessaires au dossier copié :
```
chown -R ec2-user:nogroup /data/ssh/ec2-user
```
7. Redémarrez le service sshd avec la commande `/etc/init.d/sshd restart`.
8. Vérifiez que vous pouvez vous connecter au serveur SMC local en SSH avec l'utilisateur ec2-user et la clé SSH AWS.

9. Adaptez le script suivant, puis exécutez-le depuis le serveur SMC local sur les firewalls SNS rattachés à votre serveur, afin de leur indiquer l'adresse de contact du serveur SMC sur AWS :

```
CONFIG FWADMIN CONTACT ADD address=<adresse de contact du SMC AWS> port=<port du
SMC AWS>
CONFIG FWADMIN ACTIVATE
```

10. Vérifiez sur l'un des firewalls SNS que la nouvelle adresse IP a été prise en compte avec la commande CLI `CONFIG FWADMIN CONTACT LIST`.
11. Votre serveur SMC local doit posséder une seule interface réseau. Configurez cette interface en DHCP le cas échéant.
12. Vous allez maintenant migrer le serveur local vers le serveur AWS. Sauvegardez la configuration du serveur SMC local comme indiqué dans la section ***Sauvegarder et restaurer la configuration du serveur SMC*** du *Guide d'administration* de SMC, puis éteignez la machine virtuelle.
13. Restaurez la sauvegarde sur le serveur SMC AWS.
14. Vérifiez que vous pouvez vous connecter au serveur SMC AWS en SSH avec l'utilisateur ec2-user et la clé SSH AWS.
15. Supprimez l'adresse de contact du serveur SMC local sur les firewalls SNS rattachés en effectuant les actions suivantes :
    a. Exécutez la commande CLI suivante sur les firewalls connectés au serveur SMC AWS afin d'identifier la position de l'adresse de contact du serveur SMC local :

```
CONFIG FWADMIN CONTACT LIST
```

    Le retour de la commande doit ressembler à ceci :

```
pos=1 address=<adresse de contact du SMC local> port=<port du SMC
local> bindaddr=
pos=2 address=<adresse de contact du SMC AWS> port=<port du SMC AWS>
bindaddr=
```

    b. Depuis le serveur SMC AWS, exécutez le script suivant sur les firewalls SNS rattachés à votre serveur :

```
CONFIG FWADMIN CONTACT REMOVE pos=<position de l'adresse de contact du
SMC local>
CONFIG FWADMIN ACTIVATE
```

8.3 Migrer vers le cloud de 3DS Outscale

Afin de migrer un serveur SMC local existant dans le cloud de 3DS Outscale, les grandes étapes suivantes sont nécessaires :

- Modifier la configuration du serveur SMC local,
- Créer un utilisateur Outscale sur le serveur SMC local,
- Migrer le serveur vers le serveur SMC hébergé dans le cloud de 3DS Outscale préalablement installé.

Veuillez suivre la procédure détaillée suivante pour migrer :

1. Connectez-vous au serveur SMC local en SSH avec l'utilisateur "root".
2. Exécutez les commandes suivantes pour modifier la configuration du serveur :

```
sed -i -E 's/^#*(PasswordAuthentication).*$/\1 no/g' /data/users/ssh/sshd_config
sed -i -E 's/^#*(PermitRootLogin).*$/\1 no/g' /data/users/ssh/sshd_config
sed -i -E 's/(\/data\/ssh)(.*)/\1\/\%u\2/' /data/users/ssh/sshd_config
```

3. Exécutez les commandes suivantes pour créer l'utilisateur Outscale sur le serveur SMC local :

```
echo "outscale:x:99999:65534::/home/outscale:/bin/sh" >> /etc/passwd
echo "outscale:!:18908:0:99999:7:::" >> /etc/shadow
echo "outscale ALL=(ALL) NOPASSWD: ALL" > /etc/sudoers.d/outscale
echo "[[ \${USER} == "outscale" ]] && sudo -i" > /etc/profile.d/outscale.sh
```

4. Depuis le serveur SMC sur 3DS Outscale, copiez le dossier *outscale* et son contenu situé sous `/data/ssh/` sur le serveur SMC local.
5. Vérifiez que le dossier *outscale* contient un fichier *authorized_keys.outscale*.
6. Exécutez la commande suivante pour accorder les droits nécessaires au dossier copié :

```
chown -R outscale:nogroup /data/ssh/outscale
```

7. Redémarrez le service sshd avec la commande `/etc/init.d/sshd restart`.
8. Vérifiez que vous pouvez vous connecter au serveur SMC local en SSH avec l'utilisateur Outscale et la clé SSH 3DS Outscale.
9. Adaptez le script suivant, puis exécutez-le depuis le serveur SMC local sur les firewalls SNS rattachés à votre serveur, afin de leur indiquer l'adresse de contact du serveur SMC sur 3DS Outscale :

```
CONFIG FWADMIN CONTACT ADD address=<adresse de contact du SMC 3DS Outscale>
port=<port du SMC 3DS Outscale>
CONFIG FWADMIN ACTIVATE
```

10. Vérifiez sur l'un des firewalls SNS que la nouvelle adresse IP a été prise en compte avec la commande CLI `CONFIG FWADMIN CONTACT LIST`.
11. Votre serveur SMC local doit posséder une seule interface réseau. Configurez cette interface en DHCP le cas échéant.
12. Vous allez maintenant migrer le serveur local vers le serveur 3DS Outscale. Sauvegardez la configuration du serveur SMC local, puis éteignez la machine virtuelle.
13. Restaurez la sauvegarde sur le serveur SMC 3DS Outscale.
14. Vérifiez que vous pouvez vous connecter au serveur SMC 3DS Outscale en SSH avec l'utilisateur Outscale et la clé SSH 3DS Outscale.
15. Supprimez l'adresse de contact du serveur SMC local sur les firewalls SNS rattachés en effectuant les actions suivantes :
    a. Exécutez la commande CLI suivante sur les firewalls connectés au serveur SMC 3DS Outscale afin d'identifier la position de l'adresse de contact du serveur SMC local :

    ```
    CONFIG FWADMIN CONTACT LIST
    ```

    Le retour de la commande doit ressembler à ceci :

    ```
    pos=1 address=<adresse de contact du SMC local> port=<port du SMC
    local> bindaddr=
    pos=2 address=<adresse de contact du SMC 3DS Outscale> port=<port du
    SMC 3DS Outscale> bindaddr=
    ```

    b. Depuis le serveur SMC 3DS Outscale, exécutez le script suivant sur les firewalls SNS rattachés à votre serveur :

    ```
    CONFIG FWADMIN CONTACT REMOVE pos=<position de l'adresse de contact du
    SMC local>
    CONFIG FWADMIN ACTIVATE
    ```

9. Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu