GUIDE

STORMSHIELD MANAGEMENT CENTER

GUIDE D'INSTALLATION

Version 3.5.4

Dernière mise à jour du document : 19 mars 2024

Référence : sns-fr-SMC-guide_d_installation-v3.5.4

Table des matières

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 3.5.4, 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 3.5.4 est compatible avec la version 3.7.0 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 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.

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 VMware, Microsoft Hyper-V ou KVM.

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

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

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

Déployez le fichier *.OVA* sur l'un des environnements virtuels suivants :

- VMware ESXi versions 6.5, 6.7 ou 7.0

La machine virtuelle SMC nécessite :

- Deux processeurs,
- Une interface réseau Ethernet,
- RAM : 4 Go,
- Espace disque minimum nécessaire sur l'environnement VMware : 130 Go.

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.

Déployez les fichiers *.VHD* sur l'un des environnements virtuels suivants :

- Microsoft Hyper-V pour Windows Server 2016,
- Microsoft Hyper-V pour Windows Server 2019,
- Microsoft Hyper-V pour Windows Server 2022.

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.

Déployez les fichiers *.qcow2* sur l'environnement virtuel suivant :

- Red Hat 7.9.

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. Terminez la création de la nouvelle machine virtuelle.
4. Ouvrez les paramètres de cette machine et rendez-vous dans le menu **Ajouter un matériel**.
5. Cliquez sur **Stockage**, puis sélectionnez **Sélectionner ou créer un stockage personnalisé**. Sélectionnez le fichier *product-data.qcow2*.
6. 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.

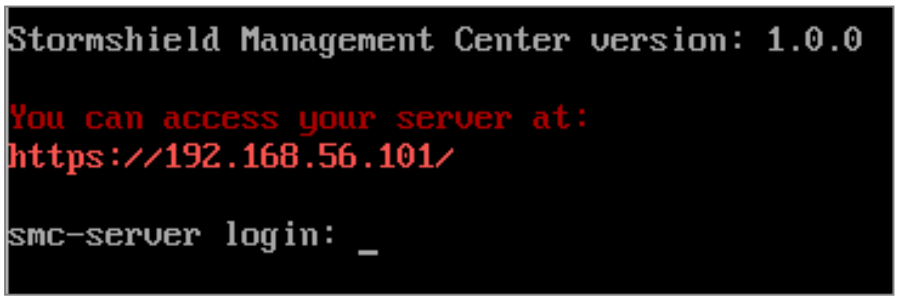
A la fin de la procédure, vous vous connecterez à l'interface web du serveur depuis l'un des navigateurs supportés :

- 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.

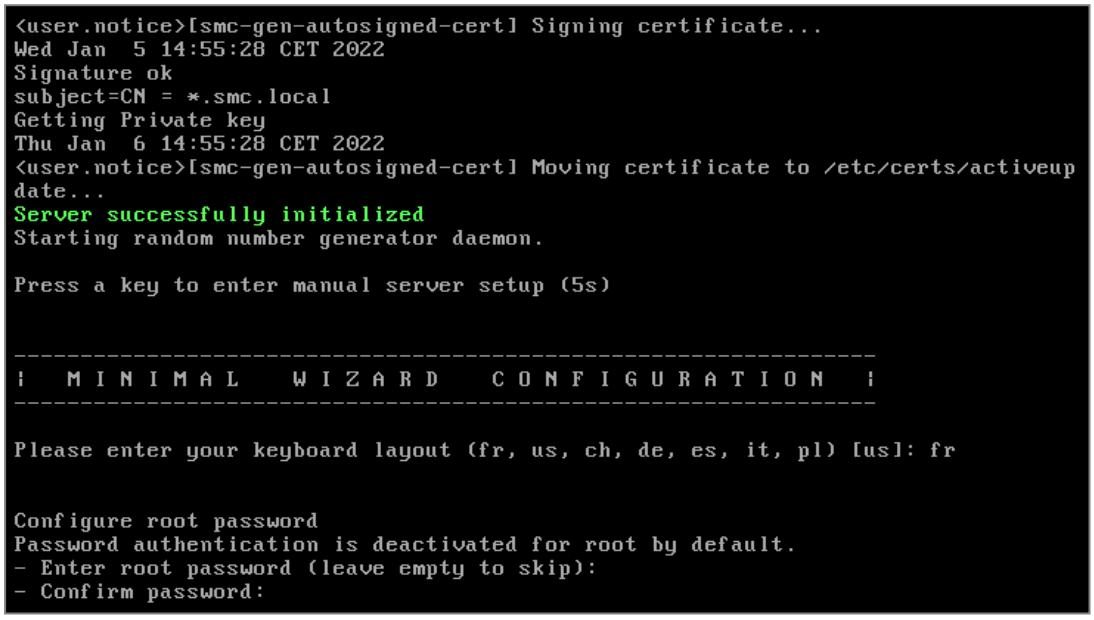
3.1 Initialiser automatiquement le serveur SMC

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.



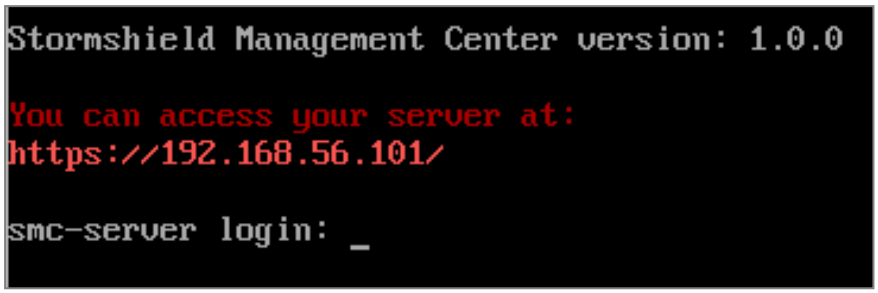
3.2 Initialiser manuellement le serveur SMC

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.

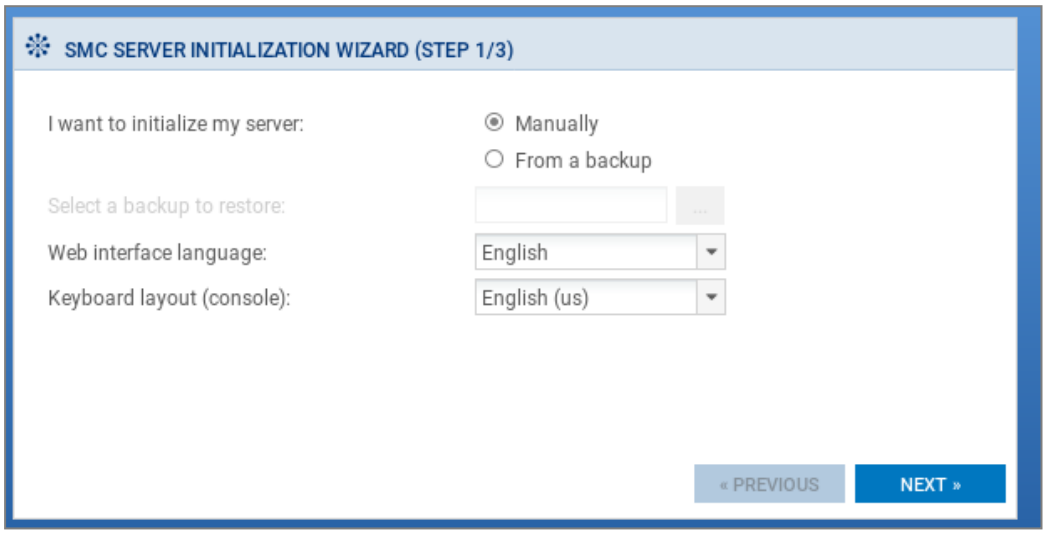


NOTE
L'assistant d'initialisation manuelle est accessible à tout moment à chaque redémarrage du serveur SMC.

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. 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.

5.1 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.

5.1.1 Obtenir votre licence SMC

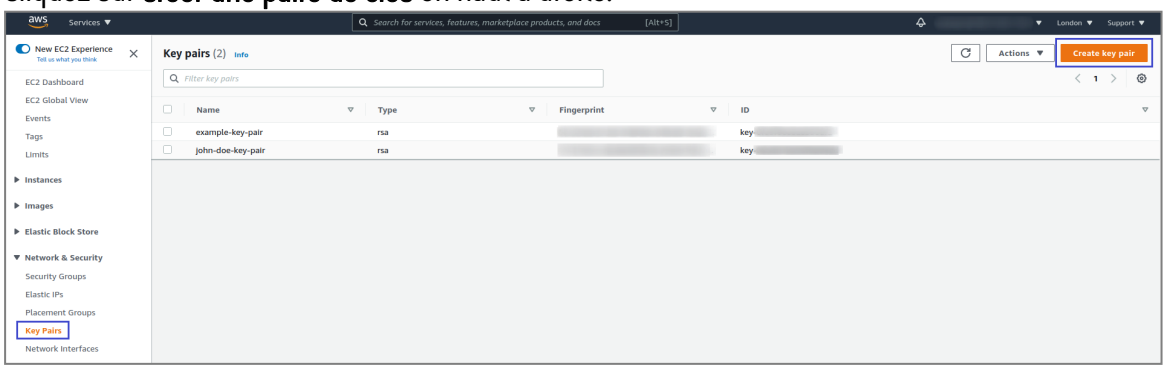
Le serveur SMC nécessite une licence logicielle pour fonctionner. La licence dépend du nombre de firewalls administrés par SMC.

Veuillez contacter votre distributeur Stormshield pour obtenir une licence.

5.1.2 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`.

5.2 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.

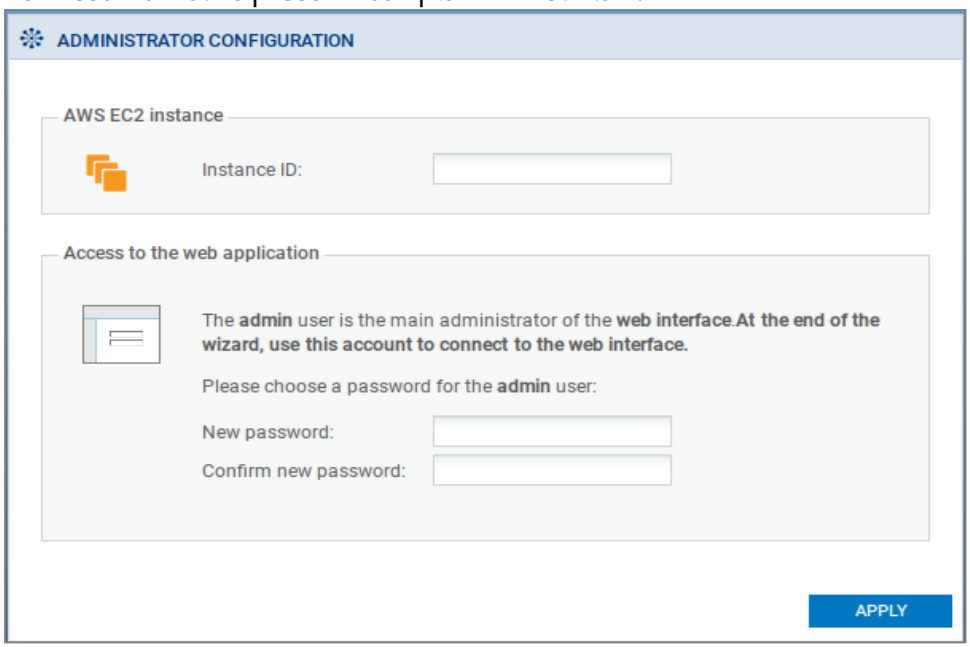
IMPORTANT
Le stockage EBS n'est pas inclus dans les frais. SMC nécessite 130 Go de stockage EBS.

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.

6. 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.

6.1 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.

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 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`.

6.1.3 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**.

6.1.4 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**.

6.1.5 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).

6.1.6 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			

6.2 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.

6.2.1 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**.

6.2.2 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

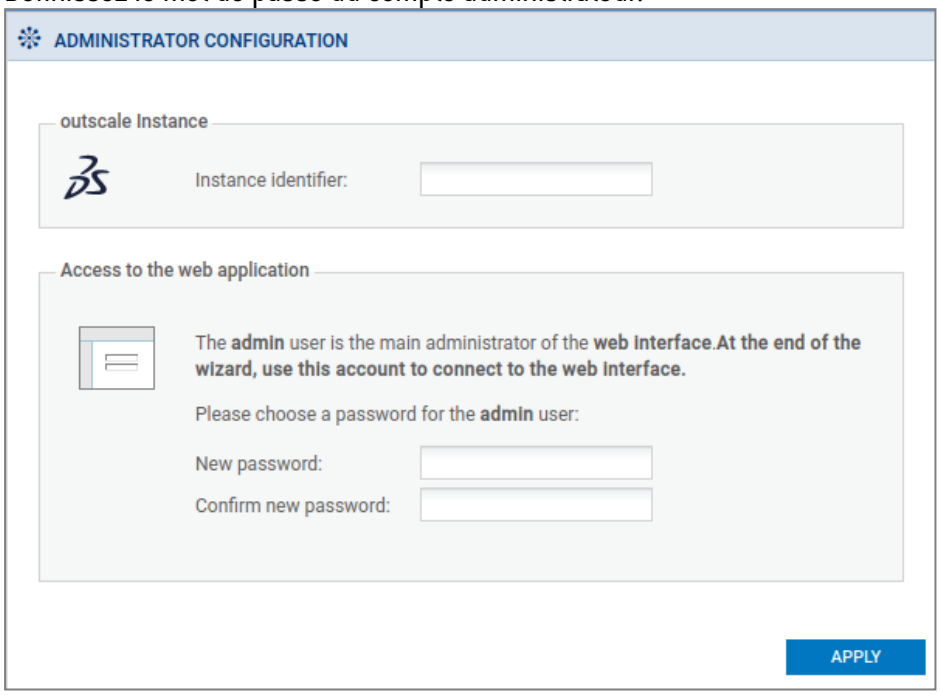
1. Sélectionnez l'adresse IP externe précédemment créée.
2. Cliquez sur **Associer instance**.
3. Sélectionnez votre instance SMC.
4. Validez en cliquant sur **Associer**.

6.2.3 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.

7. 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.

7.1 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

7.2 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, 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
    ```

7.3 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
    ```

8. 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