GUIDE

STORMSHIELD MANAGEMENT CENTER

INSTALLATION GUIDE

Version 3.9.3

Document last updated: October 20, 2026

Reference: sns-en-SMC-installation_guide-v3.9.3

Table of contents

1. Getting started ... 4
1.1 Adapting the size of the virtual environment according to the number of SNS firewalls ... 4
1.2 Setup recommendations ... 4
2. Deploying the SMC server on the virtual environment ... 5
2.1 Deploying the .OVA file on the virtual VMware environment ... 5
2.2 Deploying .VHD files in the Microsoft Hyper-V virtual environment ... 5
2.3 Deploying .qcow2 files in the KVM virtual environment ... 5
2.4 Deploying .qcow2 files in the Proxmox virtual environment ... 6
3. Initializing the SMC server from the virtual environment ... 7
3.1 Initializing the SMC server automatically ... 7
3.2 Initializing the SMC server manually ... 8
4. Ending the SMC server initialization ... 10
5. Setting up SMC server redundancy ... 11
5.1 Understanding synchronization between two nodes ... 11
5.2 Requirements and recommendations ... 12
5.3 Enabling SSH communication between nodes ... 12
5.4 Enabling redundancy ... 13
5.5 Configuring SNS firewalls for redundancy ... 13
5.6 Disabling and enabling redundancy again ... 14
5.6.1 Disabling synchronization ... 14
5.6.2 Editing connecting packages ... 14
5.6.3 Enabling synchronization again ... 14
5.7 Upgrading SMC ... 14
5.8 Managing SMC and SNS firewall backups ... 15
5.9 Using the SMC Active Update server when redundancy is enabled ... 15
6. Hosting the SMC server in the Amazon Web Services cloud ... 16
6.1 Requirements for the deployment of the SMC server ... 16
6.1.1 Obtaining your SMC license ... 16
6.1.2 Creating a key pair in the AWS management console for SSH access ... 16
6.2 Deploying the SMC server from AWS Marketplace ... 17
7. Hosting the SMC server in the 3DS Outscale cloud ... 20
7.1 Requirements for the deployment of the SMC server ... 20
7.1.1 Obtaining your SMC license ... 20
7.1.2 Creating a key pair in 3DS Outscale for SSH access ... 20
7.1.3 Creating a virtual private cloud (VPC) ... 21
7.1.4 Creating an Internet gateway ... 21
7.1.5 Creating a default route ... 22
7.1.6 Creating a security group for traffic to and from external networks ... 22
7.2 Deploying the SMC server via the 3DS Outscale Marketplace ... 23
7.2.1 Creating the SMC instance ... 23
7.2.2 Allocating an external IP address (EIP) to the SMC instance ... 24
7.2.3 Initializing the SMC instance ... 24
8. Migrating a local SMC server to a cloud-based SMC server ... 26

8.1 Requirements 26
8.2 Migrating to the Amazon Web Services cloud 26
8.3 Migrating to the 3DS Outscale cloud 27

9. Further reading 29

In the documentation, Stormshield Management Center is referred to in its short form: SMC and Stormshield Network in its short form: SNS.

1. Getting started

SMC server allows you to perform a centralized administration of SNS firewalls.

From the SMC server 3.9.3 web interface, you can:

- Administer firewalls,
- Get a clear overview of all your firewalls,
- Ensure consistent configurations,
- Access the web administration interface of firewalls,
- Create API keys to use the SMC public API.

The SMC server is a virtual machine provided in the form of an *.OVA* archive file (Open Virtualization Archive) for VMware, *.VHD* (Virtual Hard Disk) for Microsoft Hyper-V or *.qcow2* for KVM.

The SMC server 3.9.3 is compatible with Stormshield Network Security from version 4.3.

In order to install the SMC server, download the file *smc-x.x.x.ova*, the archive *smc-x.x.x-hyperv.zip* or the archive *smc-x.x.x-kvm.tar.gz* from your MyStormshield personal area.

1.1 Adapting the size of the virtual environment according to the number of SNS firewalls

The table below gives an estimate of the minimum resources that your SMC virtual machine needs in relation to the number of SNS firewalls managed.

The number of vCPUs and the size of the RAM may vary depending on the number of objects, rules, topologies, etc. in your configuration.

Moreover, the data disk for storage is 120 GB by default. Additional space may be required depending on the frequency of SNS firewall configuration deployments and backups.

Number of SNS firewalls managed	Minimum recommended number of vCPUs	Minimum recommended RAM
1- 50	2	4 GB
51- 400	4	8 GB
401- 600	8	16 GB

1.2 Setup recommendations

- We recommend to install the SMC server after a firewall which authorizes only necessary traffic:
  - access to user interfaces (SSH for the console and HTTPS for the Web interface) of the SMC server only for the IP addresses of authorized administration hosts,
  - traffic allowing the connection of SNS firewalls to the SMC server on the port TCP/1754 (default port).
- The passwords of the “root" account (allowing access to the server in command line), of the “admin” user (Web interface main administrator) and of any other administrator must be compliant with the recommendation written in the SMC*Administration guide* .

2. Deploying the SMC server on the virtual environment

Start by deploying the SMC server on a virtual environment.

To find out which versions of the virtual environments are compatible with SMC, please refer to the document Product life cycle Network Security and Tools.

The SMC server uses the e1000 virtual network interface.

We recommend that you install the SMC server in a DMZ.

Refer to the section Adapting the size of the virtual environment according to the number of SNS firewalls in order to properly size your environment.

2.1 Deploying the *.OVA* file on the virtual VMware environment

To deploy the file:

1. Open the VMware vSphere client on your administration workstation.
2. Indicate the parameters for connecting to the VMware ESXi server on which you wish to install the SMC server.
3. In the **File** menu, select **Deploy an OVF template**.
4. In the VMware deployment wizard, complete the steps to deploy the *.OVA* file.

2.2 Deploying *.VHD* files in the Microsoft Hyper-V virtual environment

The *smc-x.x.x-hyperv.zip* archive contains two *.vhd* files:

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

1. In the Hyper-V Manager tool, select a hypervisor.
2. Create a new virtual machine and follow the steps shown in the wizard.
   - In the **Assign Memory** menu, allocate 4 GB of memory.
   - In the **Connect Virtual Hard Disk** menu, select **Use an existing virtual hard disk** and select the *smc-system.vhd* file.
3. Finish the creation of the new virtual machine.
4. Open the parameters of this machine and go to the **IDE 0 Controller** menu.
5. Click on **Add** then select **Virtual hard disk** in the **Media** section, and select the *product-data.vhd* file.
6. Confirm, then log on to the machine.

2.3 Deploying *.qcow2* files in the KVM virtual environment

The *smc-x.x.x-kvm.tar.gz* archive contains two *.qcow* files:

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

1. In the virt-manager tool, select the KVM hypervisor.
2. Create a new virtual machine and follow the steps shown in the wizard.
   - Select **Import existing disk image** and select the *smc-system.qcow2* file.
   - Allocate at least 4 GB of memory and select the number of CPU (2 minimum).
3. Check **Customize configuration before install**.
4. Finish the creation of the new virtual machine.
5. Open the settings window of this machine.
6. Go to the virtual disk settings. Select **SATA**.
7. Go to the **Add hardware** menu.
8. Click on **Storage**, and select **Select or create custom storage**. Select the *product-data.qcow2* file.
9. Confirm, then log on to the machine.

2.4 Deploying *.qcow2* files in the Proxmox virtual environment

The *smc-x.x.x-kvm.tar.gz* archive contains two *.qcow* files:

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

1. Open the Proxmox VE hypervisor and create a new virtual machine.
2. Select the file smc-system.qcow2 as the main partition.
3. Select the file product-data.qcow2 as the backup partition.
4. Complete the deployment process.
5. Confirm, then connect to the machine.

3. Initializing the SMC server from the virtual environment

The SMC virtual machine is deployed. You will now need to initialize the server either manually or automatically from the virtual environment.

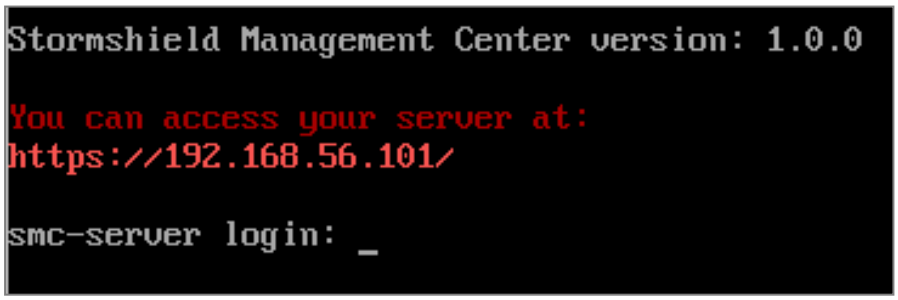
At the end of this procedure, you can connect to the server web interface from one of the supported web browsers:

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

TIP
When initializing the SMC server, a temporary IP address can be assigned either manually or by a DHCP server. In order for the DHCP assignment to work, connect the server's first virtual interface (eth0) to the right network in the virtual infrastructure. The definitive static IP address will be assigned in the SMC server initialization wizard described in section Ending the SMC server initialization.

3.1 Initializing the SMC server automatically

1. Start the SMC virtual machine.
2. By default, if the server first interface is configured to get an IP address from the DHCP server, no action is required from you to initialize the server.
3. When the SMC server is initialized, connect to the address displayed in red from a web browser to carry on initialization.



3.2 Initializing the SMC server manually

1. Start the SMC virtual machine.
2. You have five seconds to go into manual initialization mode. If you let these five seconds lapse, an attempt will be made to automatically assign an IP address via DHCP. If this attempt is unsuccessful, the manual initialization mode will then be suggested automatically.

```
<user.notice>[smc-gen-autosigned-cert] Signing certificate...
Wed Jan  5 14:55:28 CET 2022
Signature ok
subject=CN = *.smc.local
Getting Private key
Thu Jan  6 14:55:28 CET 2022
<user.notice>[smc-gen-autosigned-cert] Moving certificate to /etc/certs/activeup
date...
Server successfully initialized
Starting random number generator daemon.

Press a key to enter manual server setup (5s)


-----------------------------------------------------------------
|   M I N I M A L   W I Z A R D   C O N F I G U R A T I O N   |
-----------------------------------------------------------------

Please enter your keyboard layout (fr, us, ch, de, es, it, pl) [us]: fr


Configure root password
Password authentication is deactivated for root by default.
- Enter root password (leave empty to skip):
- Confirm password:
```

3. Define the following parameters:
   - The keyboard language used when you connect to the SMC server in command line,
   - The “root” user password allowing to connect to the server in command line. This password is optional. By default the “root” user does not have a password.
   - The parameters of the eth0 interface: IP address, subnet mask and default gateway,
   - The time zone for setting the date,
   - Whether the date will be configured manually or via an NTP server:
     - If manual configuration: enter a date,
     - If via an NTP server: enter one or several NTP servers (IP addresses or DNS names separated by commas). The NTP server can also be configured after the server has been initialized. Refer to the SMC *Administration guide* for more information.
4. When the SMC server is initialized, connect to the address displayed in red from a web browser to carry on initialization.

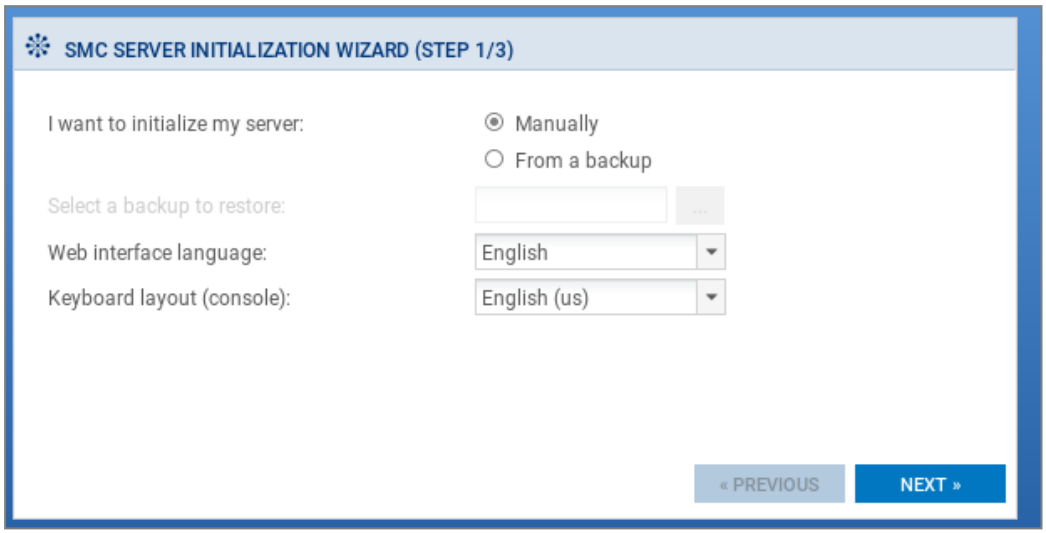
```
Stormshield Management Center version: 1.0.0

You can access your server at:
https://192.168.56.101/

smc-server login: _
```

NOTE
The manual initialization wizard can be accessed at any time each time the SMC server restarts.

4. Ending the SMC server initialization

You are now connected to the SMC server from a web browser for the first time. To complete the last steps of the SMC server initialization, use the SMC server initialization wizard.

1. Select the manual initialization mode.



2. Select the web interface language. The default language is your browser's language. If the browser's language is other than English or French, the default language is English.
3. Select the keyboard language used when you connect to the SMC server in command line,
4. Select a static or dynamic IP address for the SMC server.
5. Specify the password of the “admin” user, the main administrator of the web interface. The password must be at least eight characters long.
6. Click on **Apply**. This completes initialization.
7. Connect to the SMC server web interface with the "admin" user and password specified at step 5 of this procedure. Your SMC server is now initialized. Learn how to administer firewalls and maintain the server in the *Stormshield Management Center Administration guide*.

5. Setting up SMC server redundancy

With SMC server redundancy, service continuity can be guaranteed during a failure of the SMC server. Redundancy involves the use of two SMC servers, on which the configuration is synchronized:

- The main node,
- The backup node.

When redundancy has been set up, the connection with SNSfirewalls will continue in any of the following cases:

- The main node encounters an issue and firewalls can no longer access SMC,
- When you voluntarily shut down the main node, to conduct maintenance operations, for example.

The firewalls will then automatically connect to the backup node. You must then connect to the backup node to manage and monitor the firewalls.

When the main node resumes operation or is accessible again, the firewalls will connect to it again without the need for any action.

WARNING
We recommend always using the **main node** when it is reachable, to avoid losing configuration components.

For more information on synchronization between two nodes, and the resumption of the normal operational mode following a switch, refer to the section Understanding synchronization between two nodes.

5.1 Understanding synchronization between two nodes

The configurations on the main and backup nodes are synchronized every hour in two phases:

- The main node saves its configuration five minutes past every hour (e.g., 9:05 a.m.),
- The backup node downloads the configuration backup from the main node fifteen minutes past every hour (e.g., 9:15 a.m.). The configurations will then be synchronized.

The frequency of synchronizations cannot be configured.

During synchronization, all data required for firewall monitoring and management will be replicated. The synchronized configuration does not include the following elements:

- The SMC server license. You must install a license on each node.
- The IP and DNS configurations of the SMC server.
- The "root" account password.
- The configuration of the NTP synchronization.
- Any custom system configuration created by an administrator.

Configurations will be synchronized only if changes have been made to the configuration within the hour, either via the web administration interface, the public API or an `smc-*` command.

As such, if you make changes directly to any of the files in the `/data/config` folder (e.g., the file *cfgcheck.ini* or *smc-webservices.local*), they will only be synchronized the next time changes are made to the configuration either via the web administration interface, the public API or an `smc-*` command.

When the following operations are performed via the web administration interface, they will not warrant a synchronization:

- Changes to the SMC network settings,
- When new administrators are added,
- Changes to the consistency checker for the "*Diffusion Restreinte*" mode
- execution of SNS CLI scripts.

As a result, the first three operations must be performed manually on both nodes.

When the firewall connection switches to the backup node, there are two possible ways to resume the normal operational mode:

- If the main node is powered off, this means that the nodes are no longer being synchronized. If you make changes to the configuration from the backup node, when the main node restarts, it will retrieve the configuration from the backup node.
- Both nodes are communicating but the connection between the main node and the firewalls encounters an issue. The firewalls will automatically connect to the backup node. Synchronization from the main node to the backup node will then continue. If you are temporarily managing the firewalls from the backup node, changes to the configuration will be overwritten when both nodes are synchronized.

> **WARNING**
> If you are in this situation, we recommend that you set up the connection again between the main node and the firewalls, instead of managing them from the backup node.

5.2 Requirements and recommendations

To set up redundancy, follow the requirements and recommendations below:

- Both nodes must be installed and initialized in line with the procedure indicated in the *Installation guide*.
- We recommend installing both nodes in the same virtual environment for optimal operation.
- They must both be equipped with the same version of SMC, otherwise redundancy will not function.
- We recommend that you scale virtual machines with the exact same settings (vCPU and RAM).
- Both nodes must apply the same NTP configuration to function on the same time and in the same time zone. For more information, refer to the section Changing the date via NTP in the *Administration guide*.
- Each node needs to have its own license, with both supporting the same number of firewalls. If either node does not have a license, redundancy will not function.
- There must not be any common IP addresses between both nodes.
- SSH communication must be enabled between both nodes. For more information, see the next section.

5.3 Enabling SSH communication between nodes

The SCP protocol, which is used for synchronizing both nodes, requires authentication via SSH key in order to function.

You must generate a key pair for each node, then forward the public key to the opposite node.

Follow the procedure below, and ensure that you use the paths and file names indicated:

1. Connect to the first node in SSH.
2. Run the following command to generate the key pair:
   `ssh-keygen -t ecdsa -b 256 -f /data/redundancy/keys/redundancy -N ""`
3. Run the following command to forward the public key to the opposite node:
   `scp /data/redundancy/keys/redundancy.pub root@<REMOTE_IP>:/data/ssh/authorized_keys.root`
4. Repeat the operation on the second node.

5.4 Enabling redundancy

Ensure that you have met the above requirements before enabling redundancy:

1. Connect to the main node in SSH.
2. Run the following command: `smc-redundancy --secondary <BACKUP_NODE_IP>`. Redundancy is now enabled and the first synchronization from the main node to the backup node will immediately start.
3. To confirm that redundancy functions, refer to the file */var/log/redundancy.log* at any time.

> **NOTE**
> The main node uses the IP address of its first network interface to communicate with the backup node. The backup node uses the IP address indicated in the command above.
> If the IP address of either node is changed, redundancy will no longer function, and must be enabled again with the new address.

If you are using external severs in your configuration, such as a remote syslog server to send SMC logs, or an LDAP or Radius server to authenticate administrators, ensure that both nodes can communicate with these servers. Both nodes must be able to reach the IP address or the domain name of the external server.

5.5 Configuring SNS firewalls for redundancy

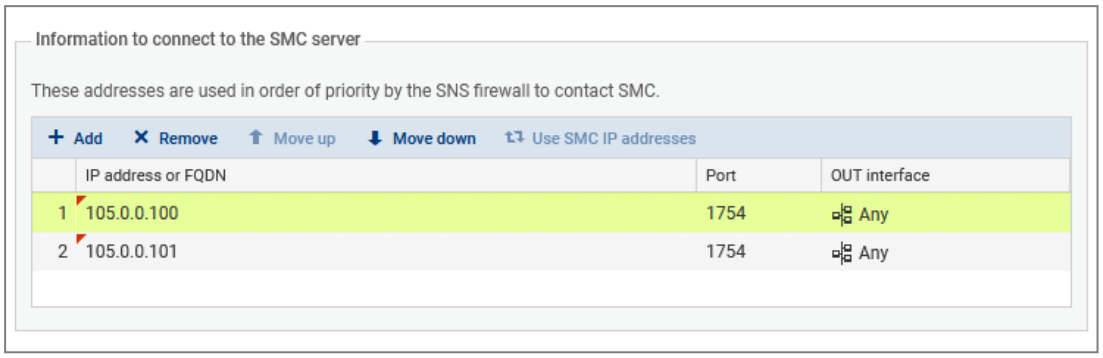
Once redundancy has been enabled, the IP addresses of both SMC servers to contact must be indicated to the firewalls. This information is sent to firewalls through the SMC connecting package:

- On firewalls that were already connected to the main node before redundancy was set up, you must generate and install new connecting package containing the addresses of both nodes, as indicated in the procedure below.
- On new firewalls, follow the steps below.

To indicate the IP addresses of both SMC servers in a firewall's connecting package:

1. Follow the usual procedure for connecting a firewall. For more information, refer to the section Connecting SNS firewalls to the SMC server in the *Administration guide*.

2. In the section **Information to connect to the SMC** server, indicate the IP addresses of both servers:



In the example above, the main node has the address 105.0.0.100 and the backup node has the address 105.0.0.101.

The command `smc-import-firewalls` makes it possible to generate several connecting packages simultaneously. For more information, refer to the section Importing firewalls in command line in the *Administration guide*.

5.6 Disabling and enabling redundancy again

To permanently stop redundancy, disable synchronization between both nodes, then modify the connecting packages so that the firewalls can no longer connect to the backup node.

In other cases, such as when a backup of the SMC server's configuration is being restored, you must temporarily disable synchronization, then enable it again. In this case, the connecting packages do not need to be modified. For more information on restoring backups, refer to the section Managing SMC backups and SNS firewalls in the *Administration guide*.

5.6.1 Disabling synchronization

1. Connect to the main node in SSH.
2. Run the following command: `smc-redundancy --disable`.

5.6.2 Editing connecting packages

Once synchronization has been disabled between both nodes, we recommend that you generate new connecting packages for each firewall connected to SMC, by indicating the IP address of the only SMC server to which they must now connect.

In this way, the firewalls will no longer attempt to connect to the former backup node with a configuration that is no longer synchronized or which may have been deleted.

5.6.3 Enabling synchronization again

To enable synchronization between two nodes again after it has been temporarily disabled:

1. Connect to the main node in SSH.
2. Run the following command: `smc-redundancy --enable`.

5.7 Upgrading SMC

To update your SMC servers when redundancy has been set up, follow the steps below in this order:

1. Shut down the backup node.
2. Update the main node as explained in the section Updating the SMC server in the *Administration guide*.
3. Wait for the update to end and for firewalls to reconnect.
4. Start the backup node and update it.

We recommend that you perform updates in time slots that do not coincide with the synchronization of both nodes. For more information, refer to the section Understanding synchronization between two nodes.

During updates, nodes cannot be synchronized in order to avoid data loss.

5.8 Managing SMC and SNS firewall backups

If you wish to restore the backup of an SMC configuration while redundancy is enabled, follow the steps below:

1. Disable synchronization between both nodes according to the relevant procedure.
2. Restore the backup on each node. The backup must originate from the node that is to be restored. For more information, refer to the section Saving and restoring the SMC server configuration in the *Administration guide*.
3. Once the backups have been restored on both nodes, ensure that both servers have restarted and have the same configuration.
4. After the backup has been restored, both nodes will have the same IP address. Change the address range to restore the initial IP configuration.
5. Enable synchronization again by following the relevant procedure.

If you have enabled redundancy and automatic backups of the server's and firewalls' configurations, backups made by one node cannot be retrieved on the other node.

5.9 Using the SMC Active Update server when redundancy is enabled

SMC can be used as an Active Update distribution point.

If you wish to use this feature and redundancy has been enabled, follow the procedure indicated in Using the SMC Active Update server on each firewall cluster by indicating the information of each node. Firewalls will then have the IP addresses and certificates with which they can use both nodes as Active Update distribution points.

If you wish to manually update the Active Update databases using the **Update bases now** button in the web administration interface, or via the databases' download script, this operation must be performed on both nodes. For more information, see the section Downloading Active Update databases in the *Administration guide*.

6. Hosting the SMC server in the Amazon Web Services cloud

The SMC server can be hosted in the Amazon Web Services (AWS) cloud in Bring Your Own License (BYOL) mode.

SMC servers hosted in the cloud can manage SNS firewalls that are either hosted locally or in the cloud.

Begin by following the instructions below. Next, in AWS Marketplace, select an EC2 (Amazon Elastic Compute Cloud) instance that fits your needs to host your SMC server, then deploy the server with the CloudFormation service.

6.1 Requirements for the deployment of the SMC server

To deploy an SMC server in the AWS cloud, you must:

- obtain a SMC license from Stormshield,
- create a key pair on AWS to secure SSH access to your SMC instance.

These operations can be performed before or during the deployment of your SMC server in AWS Marketplace.

6.1.1 Obtaining your SMC license

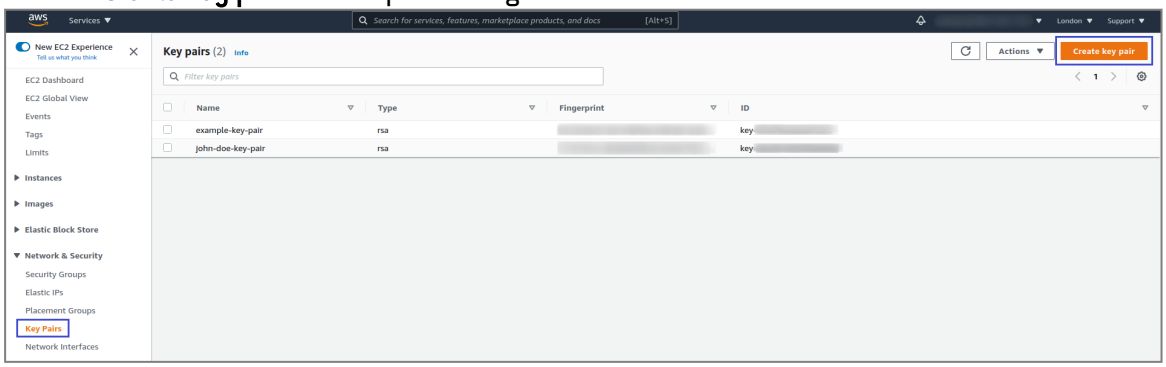
The SMC server requires a software license in order to run. The license required depends on the number of firewalls that SMC manages.

Contact your Stormshield distributor to obtain a license.

6.1.2 Creating a key pair in the AWS management console for SSH access

To secure SSH access to your SMC server, you must select an existing key pair when you create the CloudFormation stack in AWS marketplace, as shown in the section Deploying the SMC server from AWS Marketplace. If there is no such key pair, or if you wish to use a new key pair for this instance, you can create it as follows from the EC2 service in the AWS management console:

1. In the **Services** menu in the upper banner, select **EC2** under the section **Compute**.
2. In the menu on the left, select **Network & Security/Key pairs**.
3. Click on **Create key pair** at the top on the right.



4. Enter a name for the key pair.

5. Select the type of key pair and *.pem* as the file format.
6. Click on **Create key pair**.
7. Download the key pair and save it in a safe location on your computer.

When you sign in to your SMC server in SSH, enter as a connection argument the identification file corresponding to this key pair. For example:

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

> **NOTE**
> You cannot connect to your SMC server in SSH directly with the `root` user. You have to connect with the `ec2-user` user.

6.2 Deploying the SMC server from AWS Marketplace

Deploy your SMC server easily in AWS Marketplace with the CloudFomation service:

1. Go to AWS Marketplace.
2. If you have not already done so, sign in using your Amazon.com account.
3. Go to the SMC product page.
4. On the product presentation page, go to **Pricing Information** to see the type of EC2 instance that you need according to the number of firewalls managed:

AWS instance	Virtual processor	RAM (GB)	SMC size SMC	Number of firewalls
t3.medium	2	4	Small	<50
t3.xlarge	4	16	Medium	<500
t3.2xlarge	8	32	Large	<1000

You can estimate the cost of your virtual server based on the instance selected.

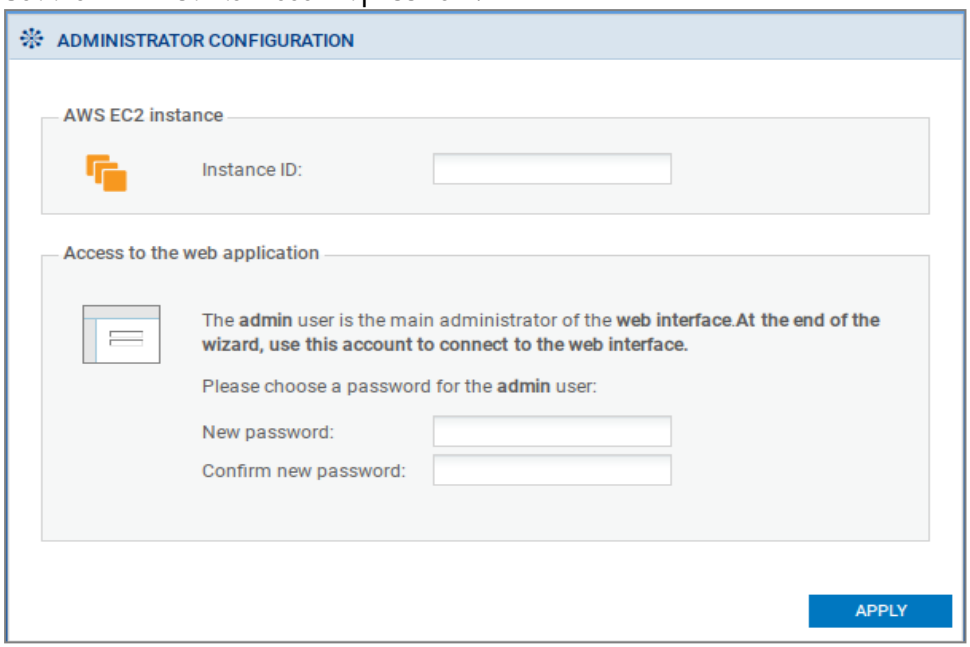
> **IMPORTANT**
> EBS storage is not included in the calculation of the cost. SMC requires 130 GB of EBS storage.

> **IMPORTANT**
> The price includes only AWS expenses. The SMC license is not issued by AWS, as the server comes with a Bring Your Own License (BYOL) model. The SMC software license must be ordered from your distributor. Refer to Obtaining your SMC license.

5. Click on **Continue to Subscribe** at the top of the page.
6. Read the conditions of use, then click on **Accept Terms**.
7. Click on **Continue to Configuration**.
8. If you do not wish to deploy the latest available version of the SMC server, select the desired version.

9. Select the region in which you wish to deploy your SMC server. You must deploy it in a region in which your VPC and other servers, if any, have already been deployed.
   The region in which you are going to deploy the EC2 instance that runs SMC may determine several factors, in particular:
   - AWS expenses for the instance in question,
   - network performance,
   - local legislation.
10. Click on **Continue to Launch**.
11. Leave *Launch CloudFormation* in the **Choose Action** section.
12. On the **Create stack** page, click on **Next** to configure your CloudFormation stack. The stack includes the SMC server and the network configuration that enables access to it.
13. Set the various parameters:
    1. Select the instance in the **InstanceType** field.
    2. In the **KeyPairName** field, select the key pair that you wish to install on your instance to secure SSH access to the SMC server. Refer to the section Creating a key pair in the AWS management console for SSH access for more information.
    3. You can either leave the default values in the **SMCSubnet** and **VirtualPrivateCloudNetwork** fields or enter your custom values.
    4. Enter an address in the **SourceIPAddress** field.
14. Click on **Next**.
15. On the **Configure StackSet options** page, configure the various options if necessary, and click on **Next**.
16. Click on **Create stack**.
17. Wait until the end of the stack creation process, when the status CREATE_COMPLETE appears on the left side of the page.
18. Go to your AWS Management Console's EC2 service to view the instance that the CloudFormation stack created.
19. Select the created instance.
20. Click on the link *https://EC2 Elastic IP address>/admin* to access the SMC administration console with your web browser.
21. The SMC server initialization wizard will ask you to enter the ID of the EC2 instance. This ID can be found in **Services/ Compute/ EC2/ Instances/ Instances** in the AWS management console.

22. Set the administrator account password.



23. Click on **Apply**. Your SMC server is ready to use.

> **NOTE**
> When deployed from AWS, the SMC server can be accessed from the web administration interface and in SSH over port 22.
> Console access is not possible.

7. Hosting the SMC server in the 3DS Outscale cloud

The SMC server can be hosted in the 3DS Outscale cloud in Bring Your Own License (BYOL) mode.

SMC servers hosted in the cloud can manage SNS firewalls that are either hosted locally or in the cloud.

Begin by following the instructions below. Next, in the 3DS Outscale Marketplace, select an instance that fits your needs to host your SMC server, then deploy it.

7.1 Requirements for the deployment of the SMC server

To deploy an SMC server in the 3DS Outscale cloud, you must:

- obtain a SMC license from Stormshield,
- create an SSH keypair to secure SSH access to your SMC instance,
- create a virtual private cloud (VPC),
- create an Internet gateway,
- create a default route,
- create a security group for traffic with external networks,
- create the SMC instance,
- allocate an external IP address (EIP) to the SMC instance,
- create the private network interface for the SMC instance,
- initialize the SMC instance.

These operations can be performed before or while your SMC server is deployed via the 3DS Outscale Marketplace.

7.1.1 Obtaining your SMC license

The SMC server requires a software license in order to run. The license required depends on the number of firewalls that SMC manages.

Contact your Stormshield distributor to obtain a license.

7.1.2 Creating a key pair in 3DS Outscale for SSH access

To secure SSH access to your SMC server, you must select an existing key pair when you create your SMC instance in 3DS Outscale, as shown in the section Deploying the SMC server via the 3DS Outscale Marketplace.

If there is no such key pair, or if you wish to use a new key pair for this instance, you can create it as follows from the 3DS Outscale Cockpit console:

1. Open the **Network/Security** menu.
2. Select **Keypairs**.
3. Click on **Create**.
4. Enter a name for the new SSH key and click on **Create**. A key will then be generated; you

can download it from the dialog box that opens.

5. Download the key pair and save it in a safe location on your computer.

When you sign in to your SMC server in SSH, enter as a connection argument the identification file corresponding to this key pair. For example:

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

> **NOTE**
> You cannot connect to your SMC server in SSH directly with the `root` user. You must log in with the `outscale` user account.

7.1.3 Creating a virtual private cloud (VPC)

The VPC is the virtual network in which the SMC server will be deployed. It is made up of a subnet to which the SMC interface will be attached.

Creating the VPC

In the **VPC** menu in the 3DS Outscale Cockpit console:

1. Select **VPC**.
2. Click on **Create**, then on **Expert mode**.
3. Enter a name for the VPC, and the associated network in CIDR notation (e.g., *172.21.0.0/16*).
4. Confirm by clicking on **Create**.

Creating the subnet of the VPC

1. Select the VPC created earlier. Details of the VPC appear in the lower section of the configuration screen.
2. Click on **Create subnet**.
3. Enter a name for the VPC, and the associated network in CIDR notation (e.g., *172.21.0.0/24*).
   This subnet must be included in the network of the VPC.
4. Select the geographical zone in which this subnet is available.
5. Confirm by clicking on **Create**.

7.1.4 Creating an Internet gateway

This refers to the gateway through which the SMC server accesses the Internet.

Creating the Internet gateway

In the **VPC** menu in the 3DS Outscale Cockpit console:

1. Select **Internet gateways**.
2. Click on **Create**.
3. Confirm by clicking on **Create**.

Attaching the Internet gateway to the VPC

1. Select the gateway created in the previous step.
2. Click on **Attach**.
3. Select the VPC created earlier.
4. Confirm by clicking on **Attach**.

7.1.5 Creating a default route

The aim of this step is to create a default route to the Internet gateway for all outbound traffic.

Creating the default route in the route table of the VPC

In the **Network/Security** menu in the 3DS Outscale Cockpit console:

1. Select **Route tables**.
2. Select the route table corresponding to the VPC created earlier.
   Details of the route table appear in the lower section of the configuration screen.
3. In the details of the route table, click on **Create route**.
4. In the **Target** field, select the Internet gateway created earlier.
5. Click on **All IP**s.
   The **Destination** field will automatically be filled in with the value 0.0.0.0/0.
6. Confirm by clicking on **Create**.

Attaching this route table to the public subnet of the VPC

1. Select the route table corresponding to the VPC created earlier.
2. Click on **Attach**.
3. Select the public subnet of the VPC.
4. Click on **Attach** to confirm the configuration.
   The **Associations** column reflects the change in status (switch from 0 to 1).

7.1.6 Creating a security group for traffic to and from external networks

In this security group, you will find the rules allowing traffic from external networks to SMC, and from protected networks to external networks.
To enable access to SMC, the following inbound traffic is allowed:

- SSH: access to the SMC server in console mode,
- HTTPS: access to the SMC server web administration interface,
- TCP/1754: default port through which SNS firewalls connect.

Creating the security group

In the **Network/Security** menu in the 3DS Outscale Cockpit console:

1. Select **Security groups**.
2. Click on **Create**.
3. Give the security group a name.
4. Add a description.
5. Select the VPC created earlier.
6. Click on **Create**.

Creating the security rules corresponding to traffic allowed with external networks

1. Select the security group created earlier.
   The list of rules attached to the security group appears in the lower section of the configuration screen.
2. In the list of rules, click on **Create rule**.
3. Select **Inbound** mode.
4. Select **SSH** as the protocol.
5. Click on **All IPs**.
6. Click on the "+" symbol.
7. Repeat steps 3 to 6 with **HTTPS** as the protocol.
8. Repeat steps 3 to 6 with the values **Inbound**, **Custom, TCP**, **1754** and **All IPs**.
9. Confirm the rules by clicking on **Create**.

> **IMPORTANT**
> A rule allowing outbound traffic will be automatically created.
> This rule must not be deleted as it allows, in particular, the necessary outbound traffic to retrieve security updates for instances deployed in the VPC.

The list of rules describing traffic allowed for the security group will therefore look like this:

+ 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 Deploying the SMC server via the 3DS Outscale Marketplace

The SMC instance deployed is attached to the VPC, security group for traffic with external networks, SSH key and subnet created earlier.

7.2.1 Creating the SMC instance

In the **Compute** menu in the 3DS Outscale Cockpit console:

1. Select **Instances**.
2. Click on **Create,** then **Expert mode**.
3. Give the instance a name, then click on **Next**.
4. Enter SMC in the search field, then select the desired SMC image.
5. Click on **Next**.
6. Select the attributes for your instance, based on the minimum hardware recommendations:
   - **CPU** type,
   - Desired **Performance** (3DS Outscale parameter),

- Number of **Cores**,
- Amount of **Memory** (GB) allocated to the virtual machine.

7. Click on **Next**.
8. Select the **VPC** created earlier.
9. Select the subnet of the VPC created earlier.
10. Choose the IP address to associate with the SMC server's public interface.
    This address must belong to the subnet selected in step 9. You can also leave this field empty. 3DS Outscale automatically assigns an available address from the subnet.
11. Select the geographical zone in which this subnet is available.
12. Click on **Next**.
13. Select the security group for traffic with external networks.
14. Click on **Next**.
15. Select the SSH key created right at the beginning of the process.
16. Click twice on **Next**.
    You will be shown a summary of the instance.
17. Confirm that you want to create the instance by clicking on **Create**.

7.2.2 Allocating an external IP address (EIP) to the SMC instance

Creating the external IP address

In the **Network/Security** menu in the 3DS Outscale Cockpit console:

1. Select **External IPs**.
2. Click on **Allocate**.
3. Give the external IP address a name.
4. Confirm by clicking on **Allocate**.
   An external IP address is then created.

Allocating the address to the instance

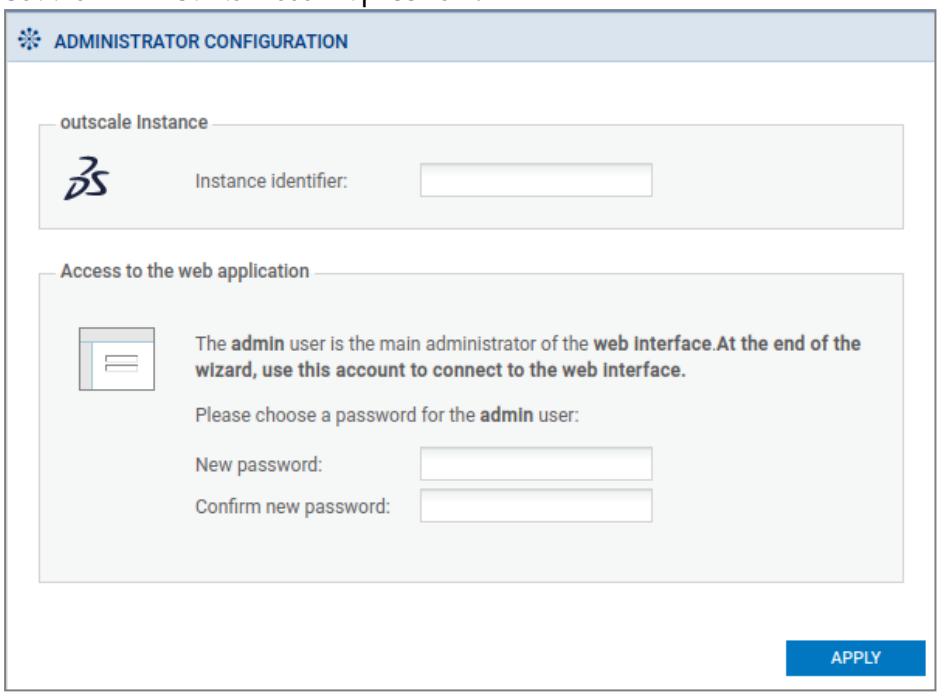
1. Select the external IP address created earlier.
2. Click on **Associateinstance**.
3. Select your SMC instance.
4. Confirm by clicking on **Associate**.

7.2.3 Initializing the SMC instance

In the **Compute** menu in the 3DS Outscale Cockpit console:

1. Select **Instances**.
2. Click on the IP address in the **External IP** column of your SMC instance.
   This will copy the external IP address of the SMC instance.
3. Open a new page in your web browser, type *https://* and paste the IP address to access the SMC administration console.
4. Enter the ID of the instance in the SMC server initialization wizard. You can find this ID in the **Compute** > **Instances** > **Instances** menu of the 3DS Outscale Cockpit console.

5. Set the administrator account password.



6. Click on **Apply**. Your SMC server is ready to use.

> **NOTE**
> When deployed from 3DS Outscale, the SMC server can be accessed from the web administration interface and in SSH over port 22.
> Console access is not possible.

8. Migrating a local SMC server to a cloud-based SMC server

If you wish to host your local SMC server in the cloud, you can migrate it from your hypervisor to the Amazon Web Services or 3DS Outscale cloud, while keeping its configuration and the configuration on your SNS firewalls.

8.1 Requirements

To migrate an existing local SMC server to the cloud, you must first install an SMC server in the AWS or 3DS Outscale cloud. Refer to these sections to find out how to do so:

- Hosting the SMC server in the Amazon Web Services cloud
- Hosting the SMC server in the 3DS Outscale cloud

8.2 Migrating to the Amazon Web Services cloud

To migrate an existing local SMC server to the AWS cloud, follow the major steps below:

- Edit the configuration of local SMC server,
- Create a user ec2-user on the local SMC server,
- Migrate the server to the SMC server hosted in the AWS cloud installed earlier.

Follow the detailed procedure below to proceed with the migration:

1. Log in to the local SMC server in SSH using the “root” user account.
2. Run the following commands to edit the configuration of the server:
```
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. Run the following commands to create the user ec2-user on the local SMC server:
```
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. On the SMC server on AWS, copy the folder *ec2-user* and its contents found in `/data/ssh/` on the local SMC server.
5. Ensure that the folder *ec2-user* contains a file named *authorized_keys.ec2-user*.
6. Run the following command to grant the necessary privileges to the copied folder:
```
chown -R ec2-user:nogroup /data/ssh/ec2-user
```
7. Restart the sshd service by using the command `/etc/init.d/sshd restart`.
8. Ensure that you are able to connect to the local SMC server in SSH as the user ec2-user and with the AWS SSH key.
9. Adapt the following script, then run it from the local SMC server on the SNS firewalls connected to your server, so that you can provide them with the contact address of the SMC server on AWS:
```
CONFIG FWADMIN CONTACT ADD address=<contact address of the AWS-based SMC>
port=<port of the AWS-based SMC>
CONFIG FWADMIN ACTIVATE
```

10. Check on one of the SNS firewalls whether the new IP address has been applied, by using the CLI command `CONFIG FWADMIN CONTACT LIST`.
11. Your local SMC server must have only one network interface. Configure it as a DHCP interface where necessary.
12. You are now about to migrate the local server to the AWS server. Back up the configuration of the local SMC server as indicated in the section Saving and restoring the *SMC* server configuration in the SMC *Administration guide*, then shut down the virtual machine.
13. Restore the backup on the AWS SMC server.
14. Ensure that you are able to connect to the AWS SMC server in SSH as the user ec2-user and with the AWS SSH key.
15. Delete the contact address of the local SMC server on the attached SNS firewalls with the following operations:
    a. Run the following CLI command on the firewalls connected to the AWS SMC server to identify the position of the local SMC server's contact address:
    ```
    CONFIG FWADMIN CONTACT LIST
    ```
    The command output should look like this:
    ```
    pos=1 address=<contact address of the local SMC> port=<port of the
    local SMC> bindaddr=
    pos=2 address=<contact address of the AWS-based SMC> port=<port of the
    AWS-based SMC> bindaddr=
    ```
    b. On the AWS-based SMC server, run the following script on the SNS firewalls attached to your server:
    ```
    CONFIG FWADMIN CONTACT REMOVE pos=<position of the local SMC's contact address>
    CONFIG FWADMIN ACTIVATE
    ```

8.3 Migrating to the 3DS Outscale cloud

To migrate an existing local SMC server to the 3DS Outscale cloud, follow the major steps below:

- Edit the configuration of local SMC server,
- Create an Outscale user on the local SMC server,
- Migrate the server to the SMC server hosted in the 3DS Outscale cloud installed earlier.

Follow the detailed procedure below to proceed with the migration:

1. Log in to the local SMC server in SSH using the “root” user account.
2. Run the following commands to edit the configuration of the server:
```
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. Run the following commands to create the Outscale user on the local SMC server:
```
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. On the SMC server on 3DS Outscale, copy the folder *outscale* and its contents found in `/data/ssh/` on the local SMC server.
5. Ensure that the folder *outscale* contains a file named *authorized_keys.outscale*.
6. Run the following command to grant the necessary privileges to the copied folder:
```
chown -R outscale:nogroup /data/ssh/outscale
```

7. Restart the sshd service by using the command `/etc/init.d/sshd restart`.
8. Ensure that you are able to connect to the local SMC server in SSH as the Outscale user and with the 3DS Outscale SSH key.
9. Adapt the following script, then run it from the local SMC server on the SNS firewalls connected to your server, so that you can provide them with the contact address of the SMC server on 3DS Outscale:

```
CONFIG FWADMIN CONTACT ADD address=<contact address of the 3DS Outscale SMC>
port=<port of the 3DS Outscale SMC>
CONFIG FWADMIN ACTIVATE
```

10. Check on one of the SNS firewalls whether the new IP address has been applied, by using the CLI command `CONFIG FWADMIN CONTACT LIST`.
11. Your local SMC server must have only one network interface. Configure it as a DHCP interface where necessary.
12. You are now about to migrate the local server to the 3DS Outscale server. Back up the configuration of the local SMC server, then shut down the virtual machine.
13. Restore the backup on the 3DS Outscale SMC server.
14. Ensure that you are able to connect to the 3DS Outscale SMC server in SSH as the Outscale user and with the 3DS Outscale SSH key.
15. Delete the contact address of the local SMC server on the attached SNS firewalls with the following operations:
    a. Run the following CLI command on the firewalls connected to the 3DS Outscale SMC server to identify the position of the local SMC server's contact address:

    ```
    CONFIG FWADMIN CONTACT LIST
    ```

    The command output should look like this:

    ```
    pos=1 address=<contact address of the local SMC> port=<port of the
    local SMC> bindaddr=
    pos=2 address=<contact address of the 3DS Outscale SMC> port=<port of
    the 3DS Outscale SMC> bindaddr=
    ```

    b. On the 3DS Outscale SMC server, run the following script on the SNS firewalls attached to your server:

    ```
    CONFIG FWADMIN CONTACT REMOVE pos=<position of the local SMC's contact address>
    CONFIG FWADMIN ACTIVATE
    ```

9. Further reading

Additional information and responses to questions you may have are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2026. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.