TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

HIGH AVAILABILITY ON SNS

Product concerned: SNS 4.x, SNS 5.x

Document last updated: September 29, 2025

Reference: sns-en-high_availability_technical_note

Table of contents

Change log 4
Getting started 5
Recommendations and best practices 6
Choosing a firewall model that supports HA 6
Obtaining compatible firewalls 6
Using the same firmware version 6
Closely following security rules and installation precautions 6
Recommendations regarding dedicated HA links 7
Network architecture - interconnections 7
Configuring HA 9
Preparing the firewalls 9
Creating the cluster 9
Adding the second firewall to the cluster 10
Checking the status of the cluster 10
Status LEDs on the firewall 12
Changing HA parameters 13
Changing the pre-shared key between members of the cluster 13
Selecting the active firewall when both are equal (firewall priority) 13
Enabling session synchronization according to duration 14
Changing the swap configuration 14
Changing the weight of an interface in the calculation of the quality factor 15
System components involved in high availability 16
Using CLI/Serverd commands in HA 16
Objects replicated in a cluster 18
Objects synchronized in real time 18
Objects synchronized periodically 18
Objects that are not replicated 18
Excluding TCP/UDP traffic from replication 19
Concept of synchronization 20
Synchronization in real time 20
Synchronization upon request 20
HA network traffic 21
Electing the active firewall 22
Understanding how the quality factor is calculated 22
Example of how the quality index of interfaces is calculated 23
HA control commands 24
Updating a cluster 27
Updating the passive firewall 27
If your firewall is equipped with a TPM (Trusted Platform Module) 27

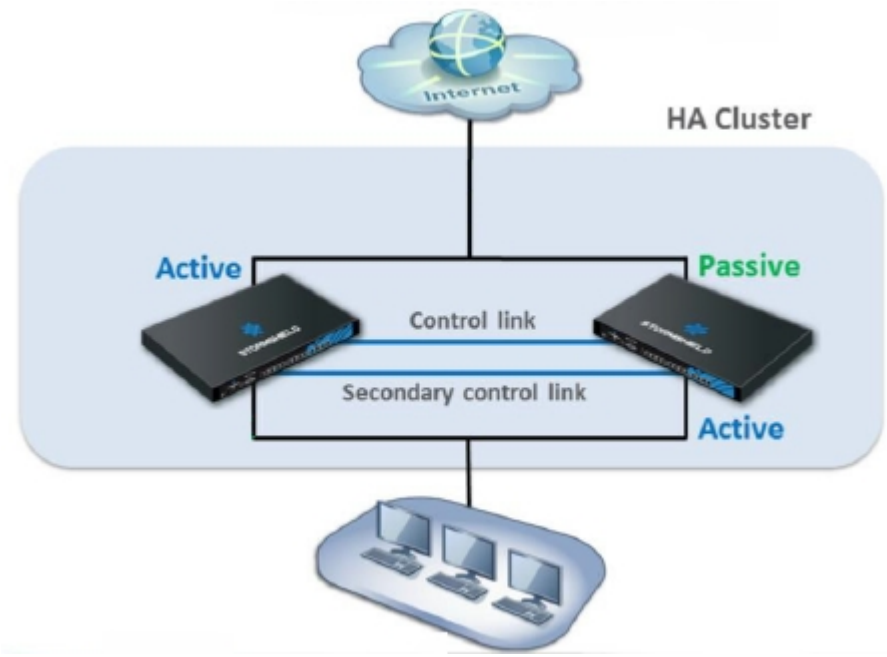
Updating the active firewall 27
If your firewall is equipped with a TPM (Trusted Platform Module) 27
Replacing the defective member of a cluster (Return Material Authorization - RMA) 29
Deleting the serial number of the older firewall from the configuration of the cluster 29
Adding the replacement firewall to the cluster 29
Troubleshooting 30
Further reading 32

Change log

Date	Description
December 13, 2024	Clarification on the use of the bypass
November 12, 2024	Clarification of latency definition (Recommendations and best practices section)
July 31, 2020	New document

Getting started

High availability (HA) is a feature that provides service continuity during a hardware or firewall failure, by deploying a cluster of firewalls. In this architecture, the links that interconnect the LAN and WAN must be duplicated, as shown below:



To form the high availability cluster, both firewalls are connected with one or two control links on dedicated interfaces. The second link is optional but strongly recommended.

Firewalls in a cluster have the same configuration, and operate in active/passive mode. This means that only one firewall is active or running at any given time, and is the same firewall that manages all traffic that goes through the networks connected to the cluster.

Recommendations and best practices

Several conditions must be met before firewalls can be interconnected to form an operational cluster.

Choosing a firewall model that supports HA

- HA is offered across the entire SNS range, except for SN160(W) and SN210(W) models.
- HA cannot be configured if the bypass mechanism has been enabled, as both mechanisms are incompatible. For more information, refer to the General configuration tab section in the *SNS user manual*.
- Clusters must consist of two firewalls of the same model.
- On firewalls that support extension modules, both members of the cluster must have the same number of network interfaces.
- HA is supported on VMWare, HyperV and KVM virtualization platforms. However, it is not supported on public virtualization platforms such as Microsoft Azure, Amazon Web Services and OpenStack.

Obtaining compatible firewalls

To set up a firewall cluster, your firewalls must be in one of the following configurations:

- A standard firewall (*master* license) and a backup firewall for high availability (*slave* license),
- Two standard firewalls (*master* license).

Clusters cannot be configured with two firewalls that have a *slave* HA license option.

If you choose the master and slave license, the backup firewall is designated with an “HA” label on its packaging (e.g., NA-SN6100 HA) and on its delivery slip.

When you order firewalls that will make up a cluster, the options subscribed for the standard firewall (Extended Web Control, Stormshield Network Vulnerability Manager, Advanced antivirus, etc.) will be automatically replicated on the backup firewall, except for the “Express exchange” option, which must be subscribed individually for each firewall.

Using the same firmware version

- To successfully set up HA, the same firmware version must be installed on both members of the cluster.
- If both firewalls have different firmware versions, the cluster will run in fail-soft mode so that the member with the older firmware version can be upgraded.

Closely following security rules and installation precautions

- Documentation is provided with every firewall, and sets out the security rules and installation precautions that you must follow to ensure that your firewalls are optimally set up.

- These documents are also available in PDF on the Stormshield technical documentation website (Installation guide, Security rules - SN range, Security rules - SN6100 and Security rules - SNi40).
- Refer to **Recommended connectors for high availability (HA) links** as well in the Product presentation and installation guide available on the Stormshield technical documentation website.

Recommendations regarding dedicated HA links

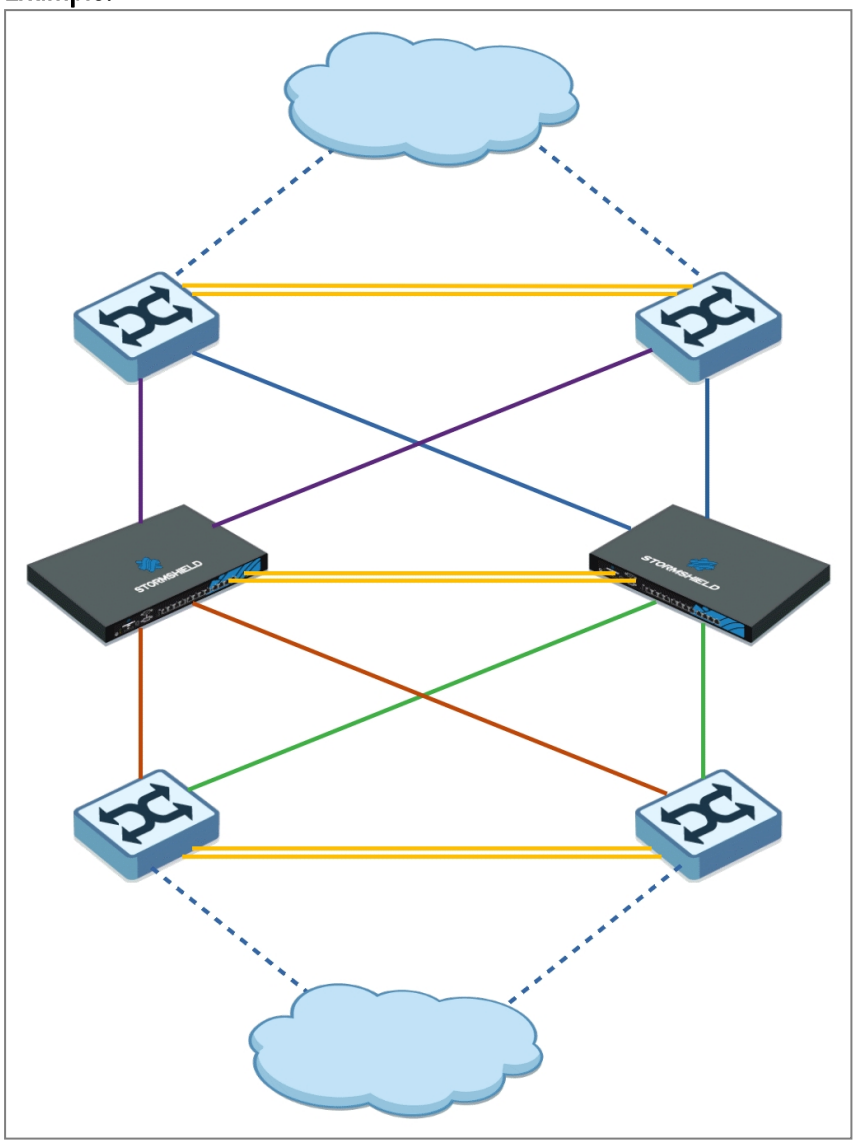
- HA control links can be set up between unaggregated network interfaces (LACP) or unaggregated VLAN interfaces (LACP).
- An HA control link must be connected to the same physical interface on both members of the cluster (e.g., *dmz1*).
- If the nodes communicate through an Ethernet interface, the interface has to be reserved solely for this purpose. It will not be supported as the parent interface of a virtual VLAN interface.
- The interface that is used for communications between the nodes of a cluster can be isolated in a VLAN. In this case, some of the advanced features relating to the communication of cluster members will not be available.
- The addresses of HA links must not be translated or routed.
- HA links can go through switches that are compatible with multicast routing. If this is the case, ensure that *IGMP snooping* features are disabled on the ports that host HA links. In any case, Stormshield recommends using a direct link between both members of the cluster.
- If there is only one HA control link and its connection is lost, both members of the cluster will attempt to manage network traffic, causing the network to be highly unstable. You are therefore strongly advised to define a secondary HA control link.
- Latency between two members of a cluster must be below 200 ms. This is the time it takes for a packet to make a return trip (i.e., 100 ms outbound and 100 ms inbound).

Network architecture - interconnections

To avoid creating a Single Point Of Failure (SPOF), you are strongly advised to:

- Duplicate interconnecting network devices (switches),
- Connect firewalls to each switch,
- Duplicate links between each switch.

Example:



Configuring HA

The setup of an HA firewall cluster involves two steps:

- Creating the cluster on the firewall that is already running,
- Adding the other firewall to the cluster.
  Do note that this operation will restart the firewall that was added to the cluster, but will not affect production (traffic will not be disrupted).

HA can be configured either via USB key (see the Technical Note Initial configuration via USB key), or via the firewall web administration interface, by following the procedure below.

Preparing the firewalls

- Both firewalls must be interconnected via their HA interfaces before you start to create the cluster.
- On the firewall to be added to the cluster, all network interfaces other than those dedicated to HA must not be connected before the cluster has been fully defined, to avoid disrupting the production network.

Creating the cluster

1. Log in to the web administration interface of the firewall on which you wish to create the cluster.
2. Click on **System** > **High availability**.
   The first step of the cluster creation wizard appears.
3. Select **Create a group of firewalls (cluster)**.
4. Click on **Next**.
5. In **Configure the main link**, select the **Interface** dedicated to high availability (*dmz1* in the example).
6. Give this interface a clear **name** (*HA-main* in the example).
7. Define the **IP address and network mask** for this interface (192.168.69.1/30 in the example).
   Do note that point-to-point links accept /31 network masks. In this case, for a 192.168.69.0/31 network, the respective addresses of the firewalls are 192.168.69.0 and 192.168.69.1 on the HA link.
8. If you wish to define a backup HA link, in the section **Secondary link (optional)**, select the checkbox **Use a second communication link**.
9. Give this interface a clear **name** (*HA-backup* in the example).
10. Define the **IP address and network mask** for this interface (192.168.70.1/30 in the example).
11. Click on **Next**.
12. Enter and confirm the **Pre-shared key** that secures communications between members of the cluster.
    For greater security, use passwords longer than 12 characters containing a combination of uppercase and lowercase letters, numbers and special characters. For more information on password security, refer to the recommendations given by the French National Cybersecurity Agency (ANSSI) (in French).

13. You can choose to **Encrypt communication between firewalls**, which is recommended if members of the cluster were interconnected through switches.
Do note that this option may impact performance in configurations that support many connections per second or many IPsec tunnels.
14. The **Enable link aggregation when the firewall is passive** option is selected by default. In a configuration that uses link aggregation (LACP), this option makes it possible to enable aggregates even on the passive member of the cluster. Disable it by unselecting the checkbox.
15. Click on **Next**.
16. Confirm the recap of the configuration by clicking on **Finish**.

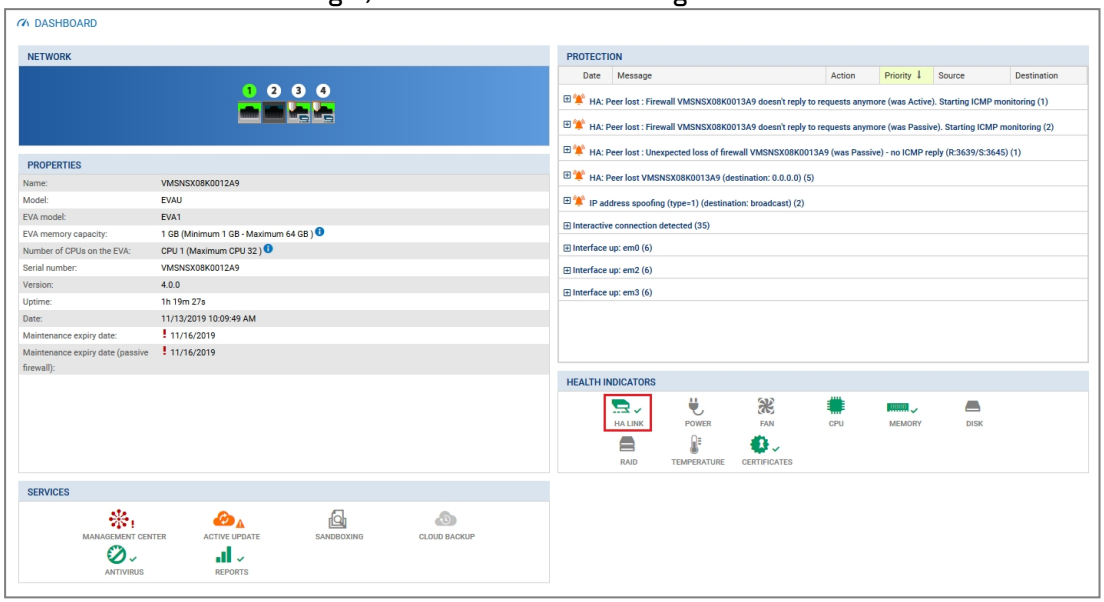
Adding the second firewall to the cluster

1. Log in to the web administration interface of the firewall that needs to join the cluster created earlier.
2. Click on **System** > **High availability**.
The first step of the cluster creation wizard appears.
3. Select **Join an existing firewall cluster**.
4. Click on **Next**.
5. In **Configure the main link**, select the **Interface** dedicated to high availability.
This interface must be the same as the one selected on the first firewall (*dmz1* in the example).
6. Define the **IP address and network mask** for this interface. This address must belong to the network chosen for the main link of the first firewall (192.168.69.2/30 in the example).
7. If you have defined a backup HA link, in the section **Secondary link (optional)**, select the checkbox **Use a second communication link**.
8. Select the **Interface** dedicated to high availability.
This interface must be the same as the one selected on the first firewall (*dmz2* in the example).
9. Define the **IP address and network mask** for this interface. This address must belong to the network chosen for the secondary link of the first firewall (192.168.70.2/30 in the example).
10. Click on **Next**.
11. Enter the IP address of the firewall to contact (address assigned to the HA link of the firewall on which the cluster was created).
12. Enter the pre-shared key defined during the creation of the cluster.
13. Click on **Next**.
14. Confirm the recap of the configuration by clicking on **Finish**.
A confirmation message will appear.
15. Confirm the operation by clicking on **Join the firewall cluster and reboot**.
After you have applied the new network configuration, the firewall that joined the cluster will restart.
16. Once this step is over, you can connect the interfaces other than those dedicated to HA.

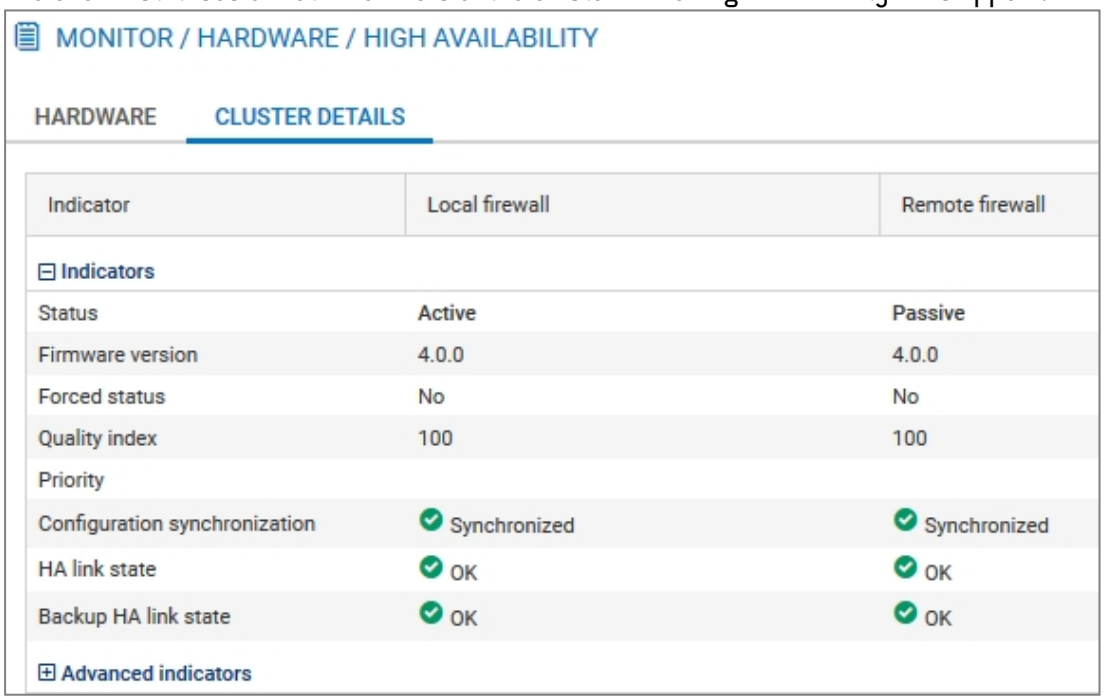
Checking the status of the cluster

In the web administration interface of the firewall on which you created the cluster:

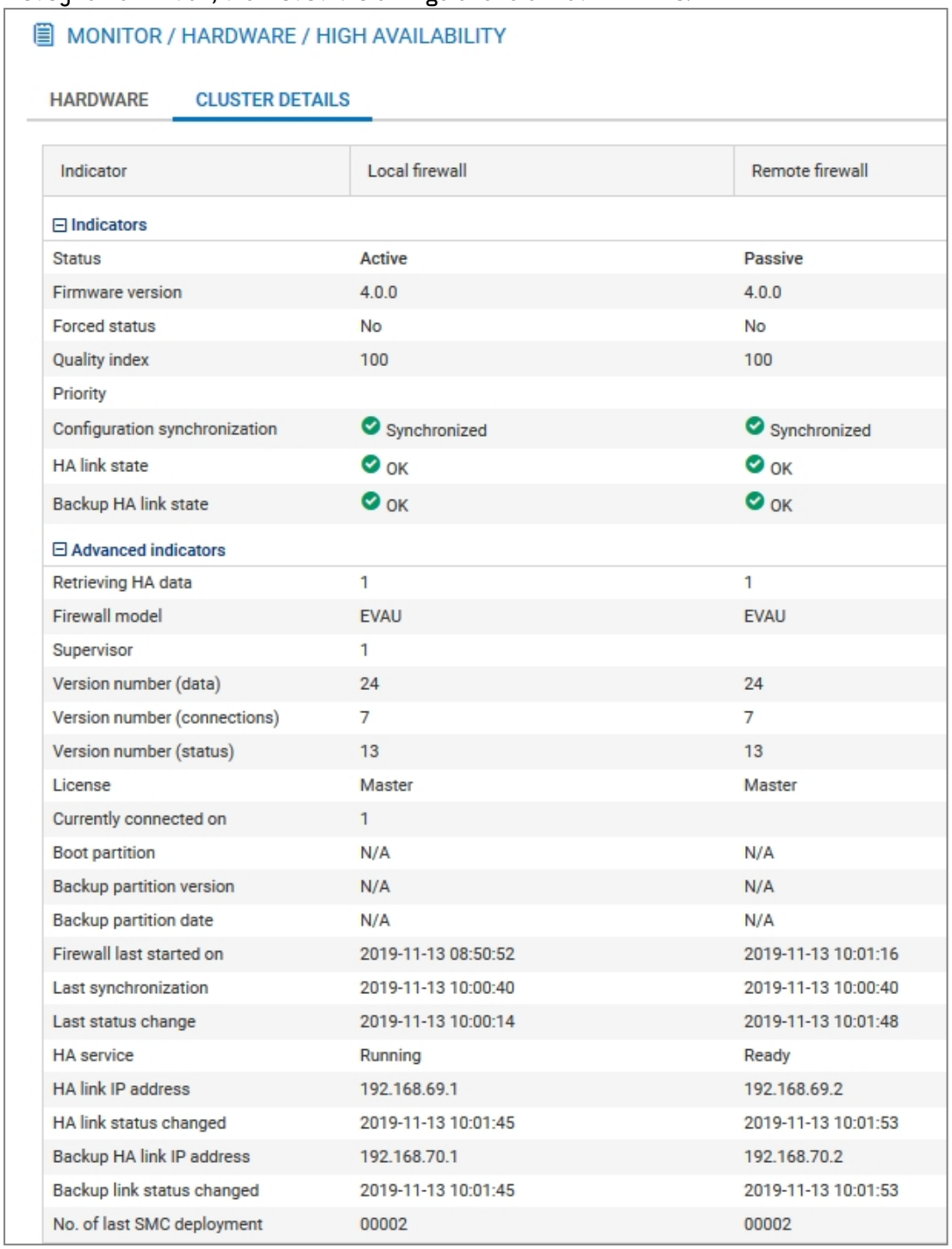
1. Click on the **Monitoring** tab.
2. In the **Health indicators** widget, the **HA link** icon must be green:



3. Click on this icon to go to **Monitoring** > **Hardware / High Availability**.
4. Click on the **Cluster details** tab.
   The overall statuses of both members of the cluster and of high availability links appear:



5. By clicking on **Advanced indicators**, you can show other information such as the date of the last synchronization, the last status change of one or both HA links:



MONITOR / HARDWARE / HIGH AVAILABILITY

HARDWARE | CLUSTER DETAILS

Indicator	Local firewall	Remote firewall
Indicators		
Status	Active	Passive
Firmware version	4.0.0	4.0.0
Forced status	No	No
Quality index	100	100
Priority		
Configuration synchronization	Synchronized	Synchronized
HA link state	OK	OK
Backup HA link state	OK	OK
Advanced indicators		
Retrieving HA data	1	1
Firewall model	EVAU	EVAU
Supervisor	1	
Version number (data)	24	24
Version number (connections)	7	7
Version number (status)	13	13
License	Master	Master
Currently connected on	1	
Boot partition	N/A	N/A
Backup partition version	N/A	N/A
Backup partition date	N/A	N/A
Firewall last started on	2019-11-13 08:50:52	2019-11-13 10:01:16
Last synchronization	2019-11-13 10:00:40	2019-11-13 10:00:40
Last status change	2019-11-13 10:00:14	2019-11-13 10:01:48
HA service	Running	Ready
HA link IP address	192.168.69.1	192.168.69.2
HA link status changed	2019-11-13 10:01:45	2019-11-13 10:01:53
Backup HA link IP address	192.168.70.1	192.168.70.2
Backup link status changed	2019-11-13 10:01:45	2019-11-13 10:01:53
No. of last SMC deployment	00002	00002

Status LEDs on the firewall

On the passive firewall, the *Online* LED (*Run* on SN6100 and SNi40 models) will blink (about 2 seconds off for every 1 second it is on). This LED is static on the active firewall.

Changing HA parameters

Some HA parameters can be changed and some options can be enabled in **Configuration** > **System** > **High availability** > **Advanced properties**.

Changing the pre-shared key between members of the cluster

1. Go to the section **Changing the pre-shared key between firewalls in the high availability cluster**.
2. Enter the **New pre-shared key**.
3. Confirm it.
   A gauge will indicate the security level of the chosen pre-shared key.
4. Click on **Apply**.
   A message will suggest that you **Save** changes to the configuration.
5. As these changes to the configuration must be synchronized in the cluster, confirm that you wish to **Apply changes**.
   The icon will then appear in the upper panel of the web administration interface, indicating that the configuration requires synchronization.
6. Click on this icon to start synchronizing.
   A message will inform you that this synchronization may restart the passive firewall.
7. Confirm by clicking on **Synchronize the configuration**.
   Both members of the cluster are now synchronized.

Selecting the active firewall when both are equal (firewall priority)

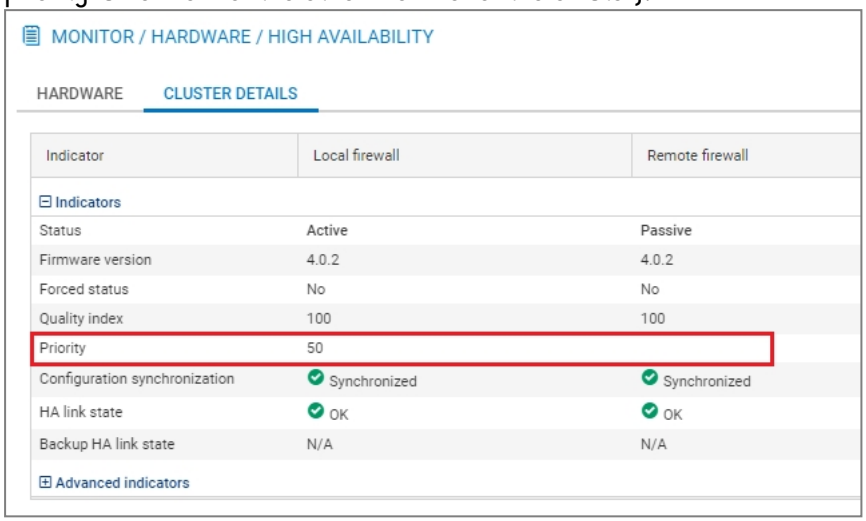
The quality factor is a parameter that is calculated from the firewall's health status (more details in the section Understanding how the quality factor is calculated).

If this quality factor is the same on both members of the cluster, you can force a member to be the active firewall (**Automatic** is selected by default).

Do note that this action applies only when the quality factor is the same on both members of the cluster: if the quality factor starts to fall on the selected member, it will still become passive.

1. Go to the section **Quality index**.
2. Select one of the members of the cluster for the **Active firewall if equal** field:
   - *This firewall (serial_number_of_this_firewall)*,
   - *The other firewall (remote) (serial_number_of_the_remote_firewall)*.
3. Click on **Apply**.
   A message will suggest that you **Save** changes to the configuration.
4. As these changes to the configuration must be synchronized in the cluster, confirm that you wish to **Apply changes**.
5. If you selected *The other firewall (remote) (serial_number_of_the_remote_firewall)*, a message will inform you that changing the priority may swap the statuses of the firewalls. Confirm by clicking on **Apply**.
   If the equality factor was the same on both members of the cluster, the firewalls will be swapped and you will be logged out of the web administration interface.

When a firewall is chosen as the default active firewall, its priority will then become 50 (no priority is defined for the other member of the cluster):



Enabling session synchronization according to duration

With this option, the number of synchronized connections can be restricted by prioritizing connections that last longer than the value indicated.

Very short and very frequent connections such as DNS requests will therefore not be synchronized.

1. Go to the section **Session synchronization**.
2. Select the checkbox **Enable synchronization based on connection duration**.
3. Indicate the minimum duration (in seconds) of connections that need to be synchronized.
4. Click on **Apply**.
   A message will suggest that you **Save** changes to the configuration.
5. As these changes to the configuration must be synchronized in the cluster, confirm that you wish to **Apply changes**.
   The icon will then appear in the upper panel of the web administration interface, indicating that the configuration requires synchronization.
6. Click on this icon to start synchronizing.
   A message will inform you that this synchronization may restart the passive firewall.
7. Confirm by clicking on **Synchronize the configuration**.
   Both members of the cluster are now synchronized.

Changing the swap configuration

Three options can be enabled or disabled:

- **Reboot all interfaces during switchover (except HA interfaces)**: when this option is enabled, bridge interfaces will be reinitialized during the swap to force the switches connected to the firewall to renew their ARP tables.
- **Enable link aggregation when the firewall is passive**: when this option is enabled, in configurations that use link aggregation (LACP), aggregates will be enabled even on the passive member of the cluster.

- **Periodically send gratuitous ARP requests**: if this option is selected, you will send ARP announcements at regular intervals so that the various devices on the network (switch, routers, etc) can update their own ARP tables.

1. Go to the section **Swap configuration**.
2. Enable or disable the relevant options.
3. Click on **Apply**.
   A message will suggest that you **Save** changes to the configuration.
4. As these changes to the configuration must be synchronized in the cluster, confirm that you wish to **Apply changes**.
   The icon will then appear in the upper panel of the web administration interface, indicating that the configuration requires synchronization.
5. Click on this icon to start synchronizing.
   A message will inform you that this synchronization may restart the passive firewall.
6. Confirm by clicking on **Synchronize the configuration**.
   Both members of the cluster are now synchronized.

Changing the weight of an interface in the calculation of the quality factor

The role and components of the quality factor are explained in Understanding how the quality factor is calculated.

To give an interface more importance in this calculation, simply increase its weight (set to 100 by default):

IMPACT OF THE UNAVAILABILITY OF AN INTERFACE IN A FIREWALL'S QUALITY INDICATOR

Interface	Weight [0-9999]
out	100
in	100
dmz2	75

1. Go to the section **Impact of the unavailability of an interface on a firewall's quality indicator**.
2. Double-click in the **Weight** column of the interface that you wish to modify.
3. Enter the desired value.
4. Click on **Apply**.
   A message will suggest that you **Save** changes to the configuration.
5. As these changes to the configuration must be synchronized in the cluster, confirm that you wish to **Apply changes**.
   The icon will then appear in the upper panel of the web administration interface, indicating that the configuration requires synchronization.
6. Click on this icon to start synchronizing.
   A message will inform you that this synchronization may restart the passive firewall.
7. Confirm by clicking on **Synchronize the configuration**.
   Both members of the cluster are now synchronized.

System components involved in high availability

Several daemons and processes perform various tasks in the high availability mechanism.

Intrusion prevention management engine	Synchronizes: • TCP and UDP connection tables, • Host tables, • Tables of users authenticated on the firewall, • Status tables exclusively for FTP and SIP protocols, • Changes to the status of router objects, • IPState connection tables (GRE / ESP), • SCTP associations.
Serverd	• Manages HA setup, • Provides the initial connection between both firewalls to finalize the creation of the cluster, • Manages changes to the weights of interfaces.
Gatewayd	Internal messaging system. Both firewalls continuously exchange messages to replicate the tunnels defined in an IKEv2 only IPsec policy or a combination of IKEv1 / IKEv2. When an active IPsec policy contains only IKEv1 tunnels, they will not be replicated.
Stated	• Calculates the quality factor of the cluster member. The calculation of this quality factor is explained in the section Electing the active firewall. • Interprets information about the status of HA (passive member restarting, availability tests on HA links, synchronization in progress, etc.), • Decides when to swap statuses, • Calls up various synchronization commands (configuration files, Active Update databases, etc.), • Stated can be queried with *statectl*.
Corosync	• Transports information about HA status.
Sshd / Rsync	Staggers the synchronization of configuration files and Active Update databases through SSH.
Sshd / ldap	Synchronizes changes made to the internal LDAP directory in real time through SSH.
Eventd	• Manages periodic events. • Makes it possible to launch periodic and regular synchronizations of certificates, DHCP leases, Vulnerability Manager information, and the status of monitored routers through other daemons such as SSHD.
Alived - ICMP	Conducts liveness tests between members of the cluster.
Arpsync	Sends gratuitous ARP requests (periodically or during a swap).

Using CLI/Serverd commands in HA

The CLI / Serverd commands **CONFIG HA** and **HA** make it possible to configure and control HA through the CLI console of the web administration interface.

These commands are explained in detail in the CLI SERVERD Commands Reference Guide (CONFIG HA and HA menus).

Objects replicated in a cluster

The following are lists of the objects that are replicated from the active firewall to the passive firewall.

Objects synchronized in real time

- TCP and UDP connection tables,
- IPState connection tables (GRE / ESP),
- SCTP associations,
- Host tables,
- Tables of users authenticated on the firewall,
- Changes to the Internal LDAP directory,
- Status tables exclusively for FTP and SIP protocols,
- Statuses of monitored routers,
- Serial numbers of certificates,
- Security associations (IKE-SA and IPsec-SA) of IKEv2-based IPsec VPN connections,
- Anti-replay counters of IKEv2 IPsec VPN connections.

Objects synchronized periodically

- Active Update databases,
- Changes to the firewall configuration (upon request),
- DHCP leases (5 minutes),
- SN Vulnerability Manager event databases (60 minutes),
- New certificates and downloaded CRLs (60 minutes).

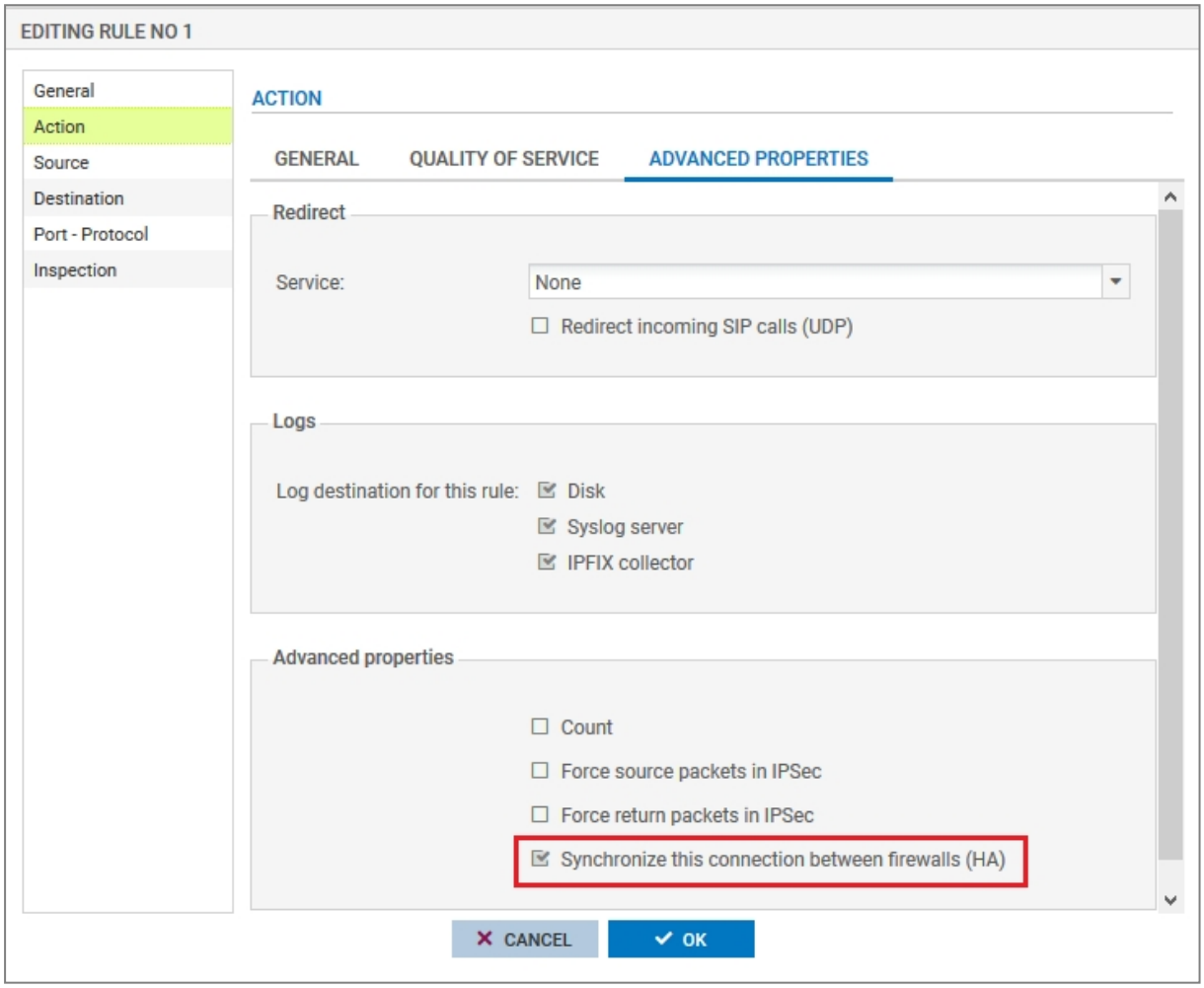
Objects that are not replicated

- Direct connections with the firewall, such as administration sessions via SSH, serverd, the web administration interface, etc.
- Connections handled by proxies.
- Logs.

Excluding TCP/UDP traffic from replication

In configurations that handle heavy traffic, it may be necessary to optimize the traffic to replicate.

Some categories of traffic can be excluded from synchronization in the filter policy, by unselecting the option **Synchronize this connection between firewalls (HA)**, which is selected by default (**Action** > **Advanced properties** in the filter rule dialog box):



The connections that match this rule will therefore not be replicated between members of the cluster.

Concept of synchronization

As of version 4 of SNS, traffic is synchronized within a cluster through the *Kernel To Kernel* (K2K) streaming protocol over UDP port 44242.

Synchronization in real time

Objects that need to be synchronized in real time (TCP and UDP connection tables, IPState connection tables [GRE / ESP], SCTP associations, host tables, etc.) are continuously sent from the active firewall to the passive firewall and statuses are synchronized on the fly.

This means that you no longer need to wait for the firewalls to swap for these tables to be integrated into the kernel of the passive firewall; connections will be there all the time in a larval state, i.e., they can be enabled when a swap occurs. So, since links between filter rules and connections are already set up in the kernel of the passive firewall, recovery time is shorter and performance is enhanced.

Part of the reason for the better performance is that the K2K protocol removes bulk updates.

Synchronization upon request

When an administrator changes the configuration of the active firewall, these changes are not immediately replicated on the passive firewall, which may need to restart in order to apply these changes in the cluster.

In such cases, the administrator may manually synchronize the firewalls at a chosen moment in one of two ways:

- Either by clicking on the icon that appears in the upper banner of the cluster's administration interface,
- Or by using the CLI command (**Configuration** > **System** > **CLI console**): HA SYNC.
  For more details on this command, refer to the **CLI SERVERD Commands Reference Guide**.

HA network traffic

The high availability mechanism requires the following traffic between both members of the cluster:

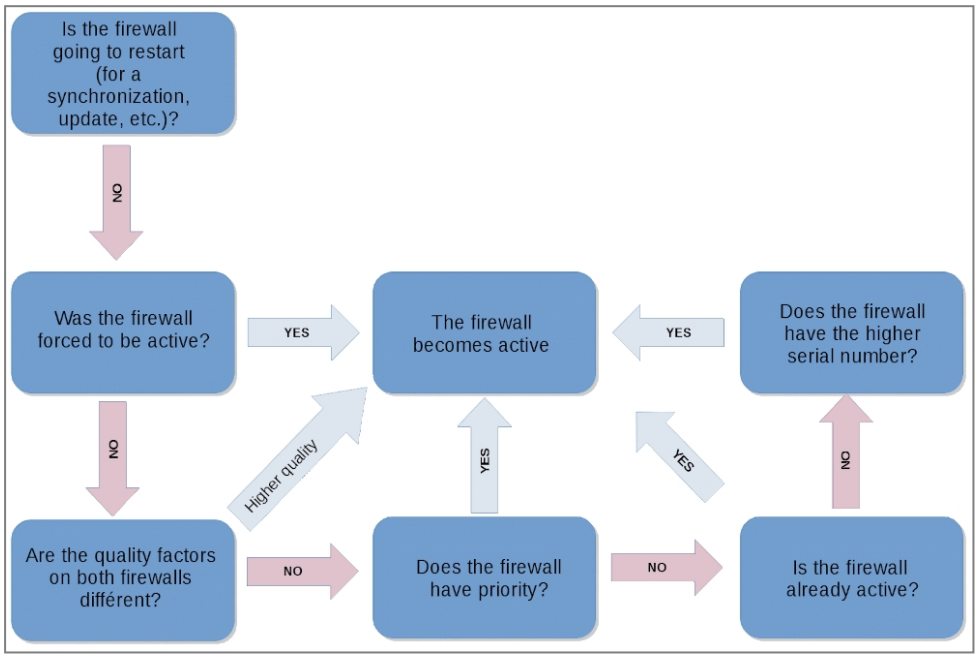
- **Kernel to Kernel traffic**: this protocol, which is used for real-time synchronization (see table of Objects synchronized in real time), is based on UDP port 44242 (only in IPv4). This port can be customized in the file ~/ConfigFiles/Protocols/hasync/common (all changes must be applied on both members of the cluster, followed by the command *enha*).
- **Traffic over TCP port 1300 (*serverd* daemon)**: the firewall that is added to the cluster uses this traffic to retrieve the HA configuration and the network configuration of the cluster.
- **Traffic over TCP ports 16058 and 16059 (*gatewayd* daemon)**: used in the synchronization of IPsec VPN statuses.
- **RSYNC traffic via SSH sessions (TCP port 22)**: this traffic allows the firewall joining the cluster to retrieve configuration files (synchronize, filtering, etc.) or synchronize changes to the LDAP directory.
- **Unicast and multicast traffic over UDP port 5405 (*corosync* daemon)**: used by both firewalls to exchange messages relating to HA and to monitor the network dedicated to HA over control links. The multicast address used by default is 226.94.1.1, but can be customized in the file ~/ConfigFiles/HA/highavailability.
  If HA links are set up through network switches, *IGMP snooping* features must be disabled on these devices to allow multicast traffic.
- **ICMP *echo request* traffic (*ping*)**: used to monitor a firewall's functional status from a network viewpoint.

Do note that these various types of traffic are allowed with an implicit filter rule (**Allow mutual access between the members of a firewall cluster (HA)**) that is enabled when high availability is set up.
When this rule is disabled, HA will immediately stop functioning.

Electing the active firewall

The process of electing the active member of the cluster takes place when HA starts up.

The following is a flowchart of the election process:



Do note that firewalls can be forced to be active **(Configuration > System > Maintenance > Configuration > High availability** menu). In this case, the firewall will be active even if its quality factor is lower. You are advised against using this option on clusters in production, as it is used only to debug configurations.

This process relies on the comparison of each firewall's quality factor, which will be explained further in this section.

Understanding how the quality factor is calculated

The quality factor is derived from a mathematical formula that takes into account various indicators:

- Status and weight of the firewall's active interfaces (HA interfaces are excluded from this calculation), including aggregated interfaces (LACP/redundancy).

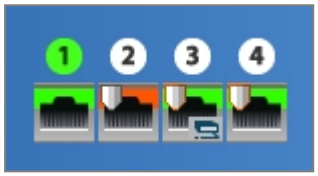
  Do note that by default in aggregates (LACP/redundancy), the firewall's quality factor starts to deteriorate after all members of the aggregate are lost. HA can be configured so that the loss of a single interface belonging to the aggregate suffices to deteriorate the quality factor. This parameter can be enabled using the CLI/Serverd commands `CONFIG HA CREATE` and `CONFIG HA UPDATE` by changing the value of the parameter below to **1** :

  - For an *LACP* aggregate: *LACPMembersHaveWeight=<0|1>*,
  - For a *Redundancy* aggregate (as of SNS version 4.3): *FailoverMembersHaveWeight=<0|1>*.
- Status(es) of the hard disk(s),

- Status of the TPM on models equipped with one.
  The configuration token *TPMQualityIncluded=1* found in the *[Global]* section of the configuration file *ConfigFiles/HA/highavailability* indicates that the status of the TPM has been applied.
- Status of additional modules (network, power supply, fans, etc.) on higher range models.

Example of how the quality index of interfaces is calculated

In this example, only interfaces 1 (*out*), 2 (*in*) and 4 (*dmz2*) are taken into account, since the *dmz1* interface is dedicated to HA. Do note that interface 2 (*in*) has connectivity issues:



The weights assigned to the interfaces are as follows:

IMPACT OF THE UNAVAILABILITY OF AN INTERFACE IN A FIREWALL'S QUALITY INDICATOR

Interface	Weight [0-9999]
out	100
in	100
dmz2	75

The quality index of the interfaces for this firewall is therefore: (1x100 + 0x100 + 1x75) / (100 + 100 + 75)=63%

The indicator calculated according to this method will be included in the overall calculation of the quality factor that takes into account other parameters.

HA control commands

The following commands can be executed through the console of either cluster member.

hainfo (-v)

Shows information about the HA status:

```
VMSNSX08K0012A9>hainfo

Nodes status:
                  VMSNSX08K0012A9 (local)       VMSNSX08K0013A9

model          :  EVAU                          EVAU
version        :  4.0.0.beta-2019-10-21-19:00-r 4.0.0.beta-2019-10-21-19:00-r
forced         :  No                            No
mode           :  Active                        Passive
  since        :  2019-10-22 11:33:45           2019-11-01 15:28:32
backup active  :  N/A                           N/A
backup ver.    :  N/A                           N/A
backup date    :  N/A                           N/A
quality        :  100                           100
priority       :  0                             0
file sync      :  None running                  None running
is conf sync   :  no                            yes
boot           :  2019-10-22 11:31:00           2019-10-22 11:38:46
main link      :  192.168.69.1: OK              192.168.69.2: OK
FwadminRevision:  00002                         00002
Notice: Some firewalls have local modifications in their configuration that haven't been synchronized yet: VMSNSX08K0012A9
```

```
VMSNSX08K0012A9>hainfo -v
Connecting to the HA cluster ...
Connected
Request node status ...
Requesting sync stats ...
Number of nodes connected to the command channel: 2
Got node status from VMSNSX08K0012A9
Got sync status from VMSNSX08K0012A9
Got node status from VMSNSX08K0013A9
Got sync status from VMSNSX08K0013A9

Nodes status:
                  VMSNSX08K0012A9 (local)       VMSNSX08K0013A9

model          :  EVAU                          EVAU
version        :  4.0.0.beta-2019-10-21-19:00-r 4.0.0.beta-2019-10-21-19:00-r
forced         :  No                            No
mode           :  Active                        Passive
  since        :  2019-10-22 11:33:45           2019-11-01 15:28:32
supervisor     :  true                          false
asqdump ver.   :  24                            24
conn sync ver. :  7                             7
balancing ver. :  13                            13
balanc. paused :  No                            No
backup active  :  N/A                           N/A
backup ver.    :  N/A                           N/A
backup date    :  N/A                           N/A
quality        :  100                           100
priority       :  0                             0
file sync      :  None running                  None running
is conf sync   :  no                            yes
last conf sync :  2019-10-22 11:38:09           2019-10-22 11:38:10
licence        :  Master                        Master
boot           :  2019-10-22 11:31:00           2019-10-22 11:38:46
state          :  Running                       Ready
syncid         :  130                           130
main link      :  192.168.69.1: OK              192.168.69.2: OK
  since        :  Tue Oct 22 11:39:15 2019      Fri Nov  1 15:28:36 2019
FwadminRevision:  00002                         00002
Notice: Some firewalls have local modifications in their configuration that haven't been synchronized yet: VMSNSX08K0012A9
```

hamode

Returns the status of the current firewall (**active** or **passive**).

hasync (-v)

Launches a staggered synchronization of cluster members:

```
VMSNSX08K0012A9>hasync
 Source          | Step                          |   P    | Info
-----------------+-------------------------------+--------+--------------------
 VMSNSX08K0013A9 | ( 1/13) Pre-command run       |  0/1   | {SET_SYNC_FLAG}
 VMSNSX08K0012A9 | ( 1/13) Pre-command run       |  0/1   | {SET_SYNC_FLAG}
 VMSNSX08K0012A9 | ( 2/13) Pre-command done      |  0/1   | {SET_SYNC_FLAG}
 VMSNSX08K0012A9 | ( 3/13) Pre-commands done     |  1/1   | (0) No error
 VMSNSX08K0013A9 | ( 2/13) Pre-command done      |  0/1   | {SET_SYNC_FLAG}
 VMSNSX08K0013A9 | ( 3/13) Pre-commands done     |  1/1   | (0) No error
 VMSNSX08K0013A9 | ( 4/13) Link evaluation       |  0/1   |
 VMSNSX08K0013A9 | ( 5/13) Link evaluation       |  1/1   |
 VMSNSX08K0013A9 | ( 6/13) Synchronization       |  1/23  | /etc/ssh
 VMSNSX08K0013A9 | ( 6/13) Synchronization       |  2/23  | /usr/Firewall/.ssh
 VMSNSX08K0013A9 | ( 6/13) Synchronization       |  3/23  | /data/System/secrets
 VMSNSX08K0013A9 | ( 6/13) Synchronization       |  4/23  | /usr/Firewall/Data/AntiVIRUS
 VMSNSX08K0013A9 | ( 6/13) Synchronization       |  5/23  | /usr/Firewall/Data/AntiVIRUS/Clamav
 VMSNSX08K0013A9 | ( 6/13) Synchronization       |  6/23  | /usr/Firewall/Data/AntiVIRUS/Kaspersky
 VMSNSX08K0013A9 | ( 6/13) Synchronization       |  7/23  | /usr/Firewall/Data/AntiSPAM
 VMSNSX08K0013A9 | ( 6/13) Synchronization       |  8/23  | /usr/Firewall/Data/AntiSPAM/RBL
 VMSNSX08K0013A9 | ( 6/13) Synchronization       |  9/23  | /usr/Firewall/Data/AntiSPAM/Vaderetro
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 10/23  | /usr/Firewall/Data/Pattern/Download
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 11/23  | /usr/Firewall/System/Language
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 12/23  | /usr/Firewall/Data/Templates
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 13/23  | /usr/Firewall/Data/URLGroups
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 14/23  | /usr/Firewall/Data/URLGroups/URLFiltering
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 15/23  | /usr/Firewall/Data/RootCertificates
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 16/23  | /usr/Firewall/Data/CustomPatterns/1/amd64/
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 17/23  | /usr/Firewall/Data/IPData/Download
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 18/23  | /usr/Firewall/ConfigFiles
 VMSNSX08K0013A9 | ( 7/13) Got change on         |  0/0   | /usr/Firewall/ConfigFiles/UserPrefs/admin
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 19/23  | /etc/tpasswd
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 20/23  | /usr/Firewall/var/Cad/cad-static-data
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 21/23  | /usr/Firewall/var/hastate
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 22/23  | /var/UserPrefs
 VMSNSX08K0013A9 | ( 6/13) Synchronization       | 23/23  | /usr/Firewall/Data/Pvm
 VMSNSX08K0013A9 | ( 8/13) Service(s) reactivation |  1/2  | cp -Rf /usr/Firewall/ConfigFiles/UserPrefs/ /var/UserPrefs; ens
 VMSNSX08K0013A9 | ( 9/13) Service(s) reactivated |  1/2   | cp -Rf /usr/Firewall/ConfigFiles/UserPrefs/ /var/UserPrefs; ens
 VMSNSX08K0013A9 | ( 8/13) Service(s) reactivation |  2/2  | enevent
 VMSNSX08K0013A9 | ( 9/13) Service(s) reactivated |  2/2   | enevent
 VMSNSX08K0013A9 | (10/13) File transfer done    |  1/1   |
 VMSNSX08K0013A9 | (11/13) Post-command run      |  0/2   | {SYNC_FW_NAME}
 VMSNSX08K0013A9 | (12/13) Post-command done     |  0/2   | {SYNC_FW_NAME}
 VMSNSX08K0013A9 | (11/13) Post-command run      |  1/2   | {SET_SYNC_FLAG}
 VMSNSX08K0013A9 | (12/13) Post-command done     |  1/2   | {SET_SYNC_FLAG}
 VMSNSX08K0013A9 | (13/13) Post-commands done    |  1/1   | (0) No error
 VMSNSX08K0012A9 | (11/13) Post-command run      |  0/2   | {SYNC_FW_NAME}
 VMSNSX08K0012A9 | (12/13) Post-command done     |  0/2   | {SYNC_FW_NAME}
 VMSNSX08K0012A9 | (11/13) Post-command run      |  1/2   | {SET_SYNC_FLAG}
 VMSNSX08K0012A9 | (12/13) Post-command done     |  1/2   | {SET_SYNC_FLAG}
 VMSNSX08K0012A9 | (13/13) Post-commands done    |  1/1   | (0) No error
OK
```

haactive / hapassive / hareset

Make it possible to force the status of the current firewall or to remove a forced status. The haactive and hapassive commands do not factor in the value of the quality factor on members of the cluster:

```
VMSNSX09L0712A9>hainfo

Nodes status:
                    VMSNSX[redacted] (local)        VMSNSX[redacted]

model           :   EVA2                            EVA1
version         :   4.0.2                           4.0.2
forced          :   Active                          No
mode            :   Active                          Passive
  since         :   2020-03-31 11:06:36             2020-03-31 11:06:33
backup active   :   N/A                             N/A
backup ver.     :   N/A                             N/A
backup date     :   N/A                             N/A
quality         :   100                             100
priority        :   0                               0
file sync       :   None running                    None running
is conf sync    :   yes                             yes
boot            :   2020-03-31 09:35:05             2020-03-31 09:35:10
main link       :   192.168.69.1: OK                192.168.69.2: OK
FwadminRevision:    N/A                             N/A
VMSNSX09L0712A9>
```

hadiff

Makes it possible to compare a configuration file between members of the cluster.

hasynctest

Evaluates unsynchronized configuration files:

```
VMSNSX08K0012A9>hasynctest
building file list ...
1886 files to consider
UserPrefs/
UserPrefs/admin
```

enha

Allows HA parameters to be reloaded:

```
VMSNSX08K0012A9>enha
Supervisor ?  OK || Local fw ? Running
```

Updating a cluster

The method below aims to minimize disruptions to the production environment during the software update of a firewall cluster.

Updating the passive firewall

1. Log in to the web administration interface of the cluster.
2. If there are changes to the configuration that have not yet been synchronized, click on the icon to start synchronizing the configuration before updating the cluster.
3. In **Configuration** > **System** > **Maintenance** > **System update** tab, select the update file (**Select the update** field),
4. In the **Select the firewall to update** field, select **The other firewall (remote)**.
5. Click on **Update firmware**.
6. Confirm the warning message *Another member of the cluster will restart* by clicking on **OK**.
7. Wait for the remote firewall to restart.

If your firewall is equipped with a TPM (Trusted Platform Module)

During a firmware update, PCRs (Platform Configuration Registers) known to the TPM may be modified, preventing access to secrets stored in the TPM. The access policy must be updated by refreshing the PCR values. For every cluster in SNS version 4.3.3 or higher, when the passive member of the cluster has restarted after being updated, the following procedure can be applied:

1. In the web administration interface of the active member of the cluster, go to **System > CLI Console.**
2. Enter the command `SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive` and click on **Run**.

More information about the command `SYSTEM TPM PCRSEAL`.

Updating the active firewall

When the passive member of the cluster has restarted after being updated:

1. Go back to **Configuration > System > Maintenance > System update** tab.
2. Select the update file (**Select the update** field).
3. In the **Select the firewall to update** field, select **This firewall**.
4. Click on **Update firmware**.
5. The other member of the cluster becomes active and connections that go through the cluster will not be disrupted.

If your firewall is equipped with a TPM (Trusted Platform Module)

1. In the web administration interface of the active member of the cluster, go to **System > CLI Console.**
2. Enter the command `SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive` and click on **Run**.

More information about the command `SYSTEM TPM PCRSEAL`.

Replacing the defective member of a cluster (Return Material Authorization - RMA)

When a member of the cluster is defective, the procedure described in this section explains what you need to do to replace it.

After Stormshield has accepted your RMA request, and when you have obtained the replacement firewall, apply the procedure below.

Deleting the serial number of the older firewall from the configuration of the cluster

This step consists of deleting the serial number of the defective firewall from the configuration of the cluster. If this step is not carried out, the replacement firewall will not be able to join the cluster and the error message *Too many firewalls in the HA cluster* will appear.

After you have disconnected the firewall that will be replaced:

1. Log in to the web administration interface of the cluster.
2. In **Configuration** > **System** > **CLI configuration**, type the command that will allow you to delete the serial number of the firewall to be replaced:

```
HA CLUSTER REMOVE SERIAL=remote
```

3. Apply this new configuration with the command:

```
HA CLUSTER ACTIVATE
```

Adding the replacement firewall to the cluster

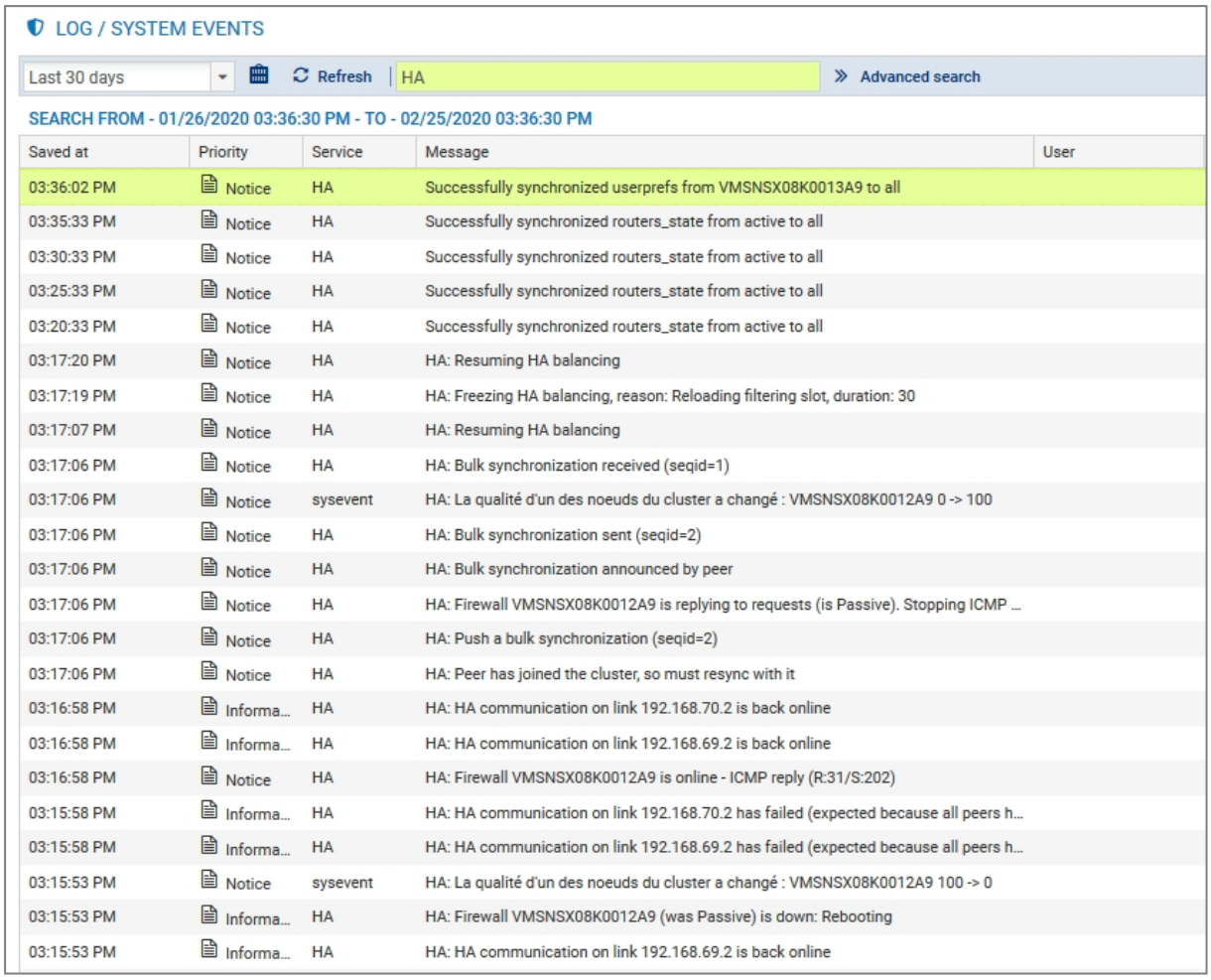
1. Connect the HA-dedicated links to the replacement firewall.
2. Do not connect the other links to this firewall.
3. Follow the process of allowing this firewall to join the cluster.

Troubleshooting

Most HA events are logged in the file /log/l_system and associated with the “HA” service. The following types of HA events are logged:

- Switching of the firewall's active/passive status,
- Failure to load a configuration on the passive firewall when the cluster is initialized,
- Shutdown of the Stated daemon on a cluster member,
- Startup of the Stated daemon on a cluster member,
- When HA is paused (e.g., when the filter policy is being reloaded),
- Failure to reload a configuration when HA restarts,
- Conflict of licenses between members of the cluster,
- Failure to initialize a synchronization,
- No response from the other member of the cluster during restart (switches the restarted firewall to active),
- The other member of the cluster was not detected,
- The other member of the cluster was detected (causes a full bulk update),
- When a bulk update is launched,
- Unsuccessful synchronization,
- Synchronization ended normally,
- When a cluster member shuts down or restarts,
- Network configuration reloaded,
- Date/time synchronization,
- Transmission error (packets lost),
- Configuration file synchronization error.

These events can be viewed in **Monitoring** > **Logs - Audit logs** > **System events** in the firewall’s web administration interface (shown below with a filter on the term *HA*):



LOG / SYSTEM EVENTS

Last 30 days | Refresh | HA | Advanced search

SEARCH FROM - 01/26/2020 03:36:30 PM - TO - 02/25/2020 03:36:30 PM

Saved at	Priority	Service	Message	User
03:36:02 PM	Notice	HA	Successfully synchronized userprefs from VMSNSX08K0013A9 to all	
03:35:33 PM	Notice	HA	Successfully synchronized routers_state from active to all	
03:30:33 PM	Notice	HA	Successfully synchronized routers_state from active to all	
03:25:33 PM	Notice	HA	Successfully synchronized routers_state from active to all	
03:20:33 PM	Notice	HA	Successfully synchronized routers_state from active to all	
03:17:20 PM	Notice	HA	HA: Resuming HA balancing	
03:17:19 PM	Notice	HA	HA: Freezing HA balancing, reason: Reloading filtering slot, duration: 30	
03:17:07 PM	Notice	HA	HA: Resuming HA balancing	
03:17:06 PM	Notice	HA	HA: Bulk synchronization received (seqid=1)	
03:17:06 PM	Notice	sysevent	HA: La qualité d'un des noeuds du cluster a changé : VMSNSX08K0012A9 0 -> 100	
03:17:06 PM	Notice	HA	HA: Bulk synchronization sent (seqid=2)	
03:17:06 PM	Notice	HA	HA: Bulk synchronization announced by peer	
03:17:06 PM	Notice	HA	HA: Firewall VMSNSX08K0012A9 is replying to requests (is Passive). Stopping ICMP ...	
03:17:06 PM	Notice	HA	HA: Push a bulk synchronization (seqid=2)	
03:17:06 PM	Notice	HA	HA: Peer has joined the cluster, so must resync with it	
03:16:58 PM	Informa...	HA	HA: HA communication on link 192.168.70.2 is back online	
03:16:58 PM	Informa...	HA	HA: HA communication on link 192.168.69.2 is back online	
03:16:58 PM	Notice	HA	HA: Firewall VMSNSX08K0012A9 is online - ICMP reply (R:31/S:202)	
03:15:58 PM	Informa...	HA	HA: HA communication on link 192.168.70.2 has failed (expected because all peers h...	
03:15:58 PM	Informa...	HA	HA: HA communication on link 192.168.69.2 has failed (expected because all peers h...	
03:15:53 PM	Notice	sysevent	HA: La qualité d'un des noeuds du cluster a changé : VMSNSX08K0012A9 100 -> 0	
03:15:53 PM	Informa...	HA	HA: Firewall VMSNSX08K0012A9 (was Passive) is down: Rebooting	
03:15:53 PM	Informa...	HA	HA: HA communication on link 192.168.69.2 is back online	

Further reading

Additional information and responses to questions you may have about high availability 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 2025. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.