



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

HAUTE DISPONIBILITÉ SUR SNS

Produits concernés : SNS 4.x, SNS 5.x

Dernière mise à jour du document : 29 septembre 2025

Référence : sns-fr-haute_disponibilite_note-technique



Table des matières

Historique des modifications	4
Avant de commencer	5
Recommandations et bonnes pratiques	6
Choisir un modèle de firewall supportant la HA	6
Acquérir des firewalls compatibles	6
Disposer de la même version de firmware	6
Respecter scrupuleusement les règles de sécurité et les précautions d'installation	7
Recommandations sur les liens dédiés à la HA	7
Architecture réseau - interconnexions	7
Configurer la HA	9
Préparer les firewalls	9
Créer le cluster	9
Intégrer le deuxième firewall dans le cluster	10
Vérifier l'état du cluster	11
État des voyants sur le firewall	13
Modifier certains paramètres de la HA	14
Modifier la clé pré-partagée entre les membres du cluster,	14
Sélectionner le firewall actif en cas d'égalité (firewall prioritaire)	14
Activer la synchronisation des sessions selon leur durée	15
Modifier la configuration du basculement d'un membre à l'autre du cluster	15
Modifier le poids d'une interface dans le calcul du facteur de qualité	16
Composants système impliqués dans la Haute Disponibilité	18
Utiliser les commandes CLI/Serverd relatives à la HA	19
Éléments répliqués au sein d'un cluster	20
Éléments synchronisés en temps réel	20
Éléments synchronisés périodiquement	20
Éléments non synchronisés	20
Exclure des flux TCP/UDP de la réplication	21
Principe de la synchronisation	22
Synchronisation en temps réel	22
Synchronisation à la demande	22
Flux réseau liés à la HA	23
Élection du firewall actif	24
Comprendre le calcul du facteur de qualité	24
Exemple de calcul de l'indicateur de qualité des interfaces	25
Commandes de contrôle de la HA	26
Mise à jour logicielle d'un cluster	29
Mettre à jour le firewall passif	29
Si votre firewall est équipé d'un TPM (Trusted Platform Module)	29



Mettre à jour le firewall actif	29
Si votre firewall est équipé d'un TPM (Trusted Platform Module)	30
Remplacement du membre défectueux d'un cluster (Return Material Authorization - RMA)	31
Supprimer de la configuration du cluster le numéro de série de l'ancien firewall	31
Ajouter le firewall remplaçant au cluster	31
Résoudre les incidents	32
Pour aller plus loin	34



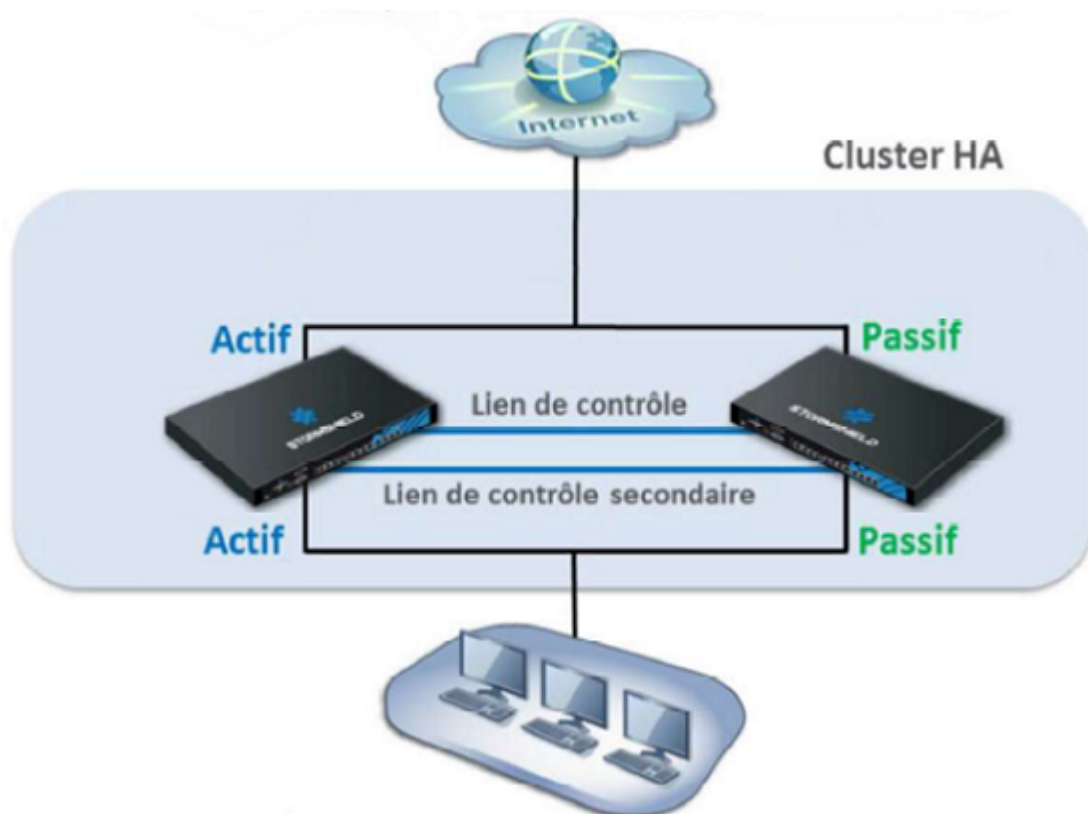
Historique des modifications

Date	Description
13 décembre 2024	Précision apportée sur l'utilisation du bypass
12 novembre 2024	Précisions apportées à la définition de la latence (section Recommandations et bonnes pratiques)
31 juillet 2020	Nouveau document



Avant de commencer

La fonctionnalité Haute Disponibilité (HA - *High Availability*) permet d'assurer la continuité de service en cas de panne (réseau ou firewall) en mettant en œuvre un cluster de firewalls. Cette architecture nécessite la duplication des liens qui permettent d'interconnecter les réseaux LAN et WAN, comme présenté ci-dessous :



Pour constituer le cluster en Haute Disponibilité, les deux firewalls sont reliés avec un ou deux liens de contrôle (le deuxième lien est facultatif mais fortement recommandé) sur des interfaces dédiées.

Les firewalls d'un même cluster possèdent une configuration identique. Ils fonctionnent en mode actif / passif, ce qui signifie qu'un seul firewall est actif (fonctionnel) à un instant donné, et que seul ce firewall gère l'ensemble du trafic transitant entre les réseaux connectés au cluster.



Recommandations et bonnes pratiques

La mise en place d'un cluster fonctionnel nécessite de respecter plusieurs paramètres, liés notamment à l'interconnexion des membres du cluster.

Choisir un modèle de firewall supportant la HA

- La HA est proposée pour l'ensemble de la gamme SNS à l'exception des firewalls modèles SN160(W) et SN210(W).
- La HA ne peut pas être configurée si le mécanisme de bypass est activé. Ces deux mécanismes sont incompatibles. Pour plus d'informations, reportez-vous à la section [Onglet Configuration générale](#) du *Manuel Utilisateur SNS*.
- Seuls deux firewalls d'un modèle identique peuvent composer un cluster.
- Dans le cas de firewalls acceptant des modules d'extension, les deux membres du cluster doivent comporter le même nombre d'interfaces réseau.
- La HA est supportée sur les plate-formes de virtualisation VMWare, HyperV et KVM. En revanche, elle n'est pas supportée sur les plate-formes publiques de virtualisation Microsoft Azure, Amazon Web Services et OpenStack.

Acquérir des firewalls compatibles

Pour établir un cluster de firewalls, il est nécessaire d'acquérir des firewalls selon l'un des deux modèles suivants :

- Un firewall standard (licence *master*) et un firewall de backup pour Haute disponibilité (licence *slave*),
- Deux firewalls standards (licence *master*).

Un cluster ne peut pas être configuré avec deux firewalls disposant chacun d'une option de licence HA *slave*.

Si vous avez opté pour une licence master et slave, vous pouvez identifier le FW de backup grâce à la mention HA sur l'étiquette de l'emballage (exemple : NA-SN6100 HA) ainsi que sur le bon de livraison du matériel.

Lors de la commande des firewalls participant au cluster, les options souscrites pour le firewall standard (Extended Web Control, Stormshield Network Vulnerability Manager, Antivirus avancé...) sont automatiquement reportées sur le firewall de backup, à l'exception de l'option "Échange express" qui est à souscrire pour chacun des firewalls, le cas échéant.

Disposer de la même version de firmware

- Pour que la HA soit fonctionnelle, la même version de firmware doit être installée sur les deux membres du cluster.
- Lorsque les deux firewalls disposent d'une version différente de firmware, le cluster fonctionne alors en mode dégradé afin de permettre la mise à jour du membre disposant de la version la plus ancienne de firmware.



Respecter scrupuleusement les règles de sécurité et les précautions d'installation

- Les firewalls sont accompagnés de documents précisant les règles de sécurité et les précautions d'installation : ces règles doivent impérativement être suivies afin de garantir une mise en œuvre optimale des firewalls Stormshield.
- Ces documents sont également accessibles au format PDF sur le site de [documentation technique Stormshield](#) (Guides d'installation, Règles de sécurité - Gamme SN, Règles de sécurité - SN6100 et Règles de sécurité - SNI40).
- Consultez également la section **Branchement optimal pour liens de Haute-Disponibilité (HA)** du [Guide de présentation et d'installation des produits](#) disponible sur le site de Documentation Technique Stormshield.

Recommandations sur les liens dédiés à la HA

- Les liens de contrôle HA peuvent être portés par des interfaces réseau hors agrégat (LACP) ou des interfaces VLAN hors agrégat (LACP).
- Un lien de contrôle HA doit être impérativement connecté à la même interface physique sur les deux membres du cluster (exemple : *dmz1*).
- Si les noeuds du cluster communiquent via une interface Ethernet, celle-ci doit être dédiée à cet usage. L'utiliser comme interface parent d'une interface virtuelle d'un VLAN n'est pas supporté.
- L'interface de communication entre les noeuds d'un cluster peut être isolée dans un VLAN. Dans ce cas, certaines fonctionnalités avancées liées à la communication des membres du cluster ne seront pas disponibles.
- Les liens de HA ne doivent pas faire l'objet de translation d'adresses ou de routage.
- Les liens HA peuvent transiter par des commutateurs compatibles avec le multicast. Veillez dans ce cas à ce que les fonctionnalités de type *IGMP snooping* soient désactivées sur les ports accueillant les liens HA.
Stormshield recommande néanmoins une liaison directe entre les deux membres du cluster.
- La perte de connectivité sur un lien de contrôle HA unique conduisant à une situation où chacun des membres du cluster tente de gérer les flux réseaux, ceci entraîne une forte instabilité du réseau.
Il est donc fortement recommandé de définir un lien de contrôle HA secondaire.
- La latence entre deux membres d'un cluster doit être inférieure à 200 ms. Il s'agit ici du temps aller/retour d'un paquet (soit 100 ms aller et 100 ms retour).

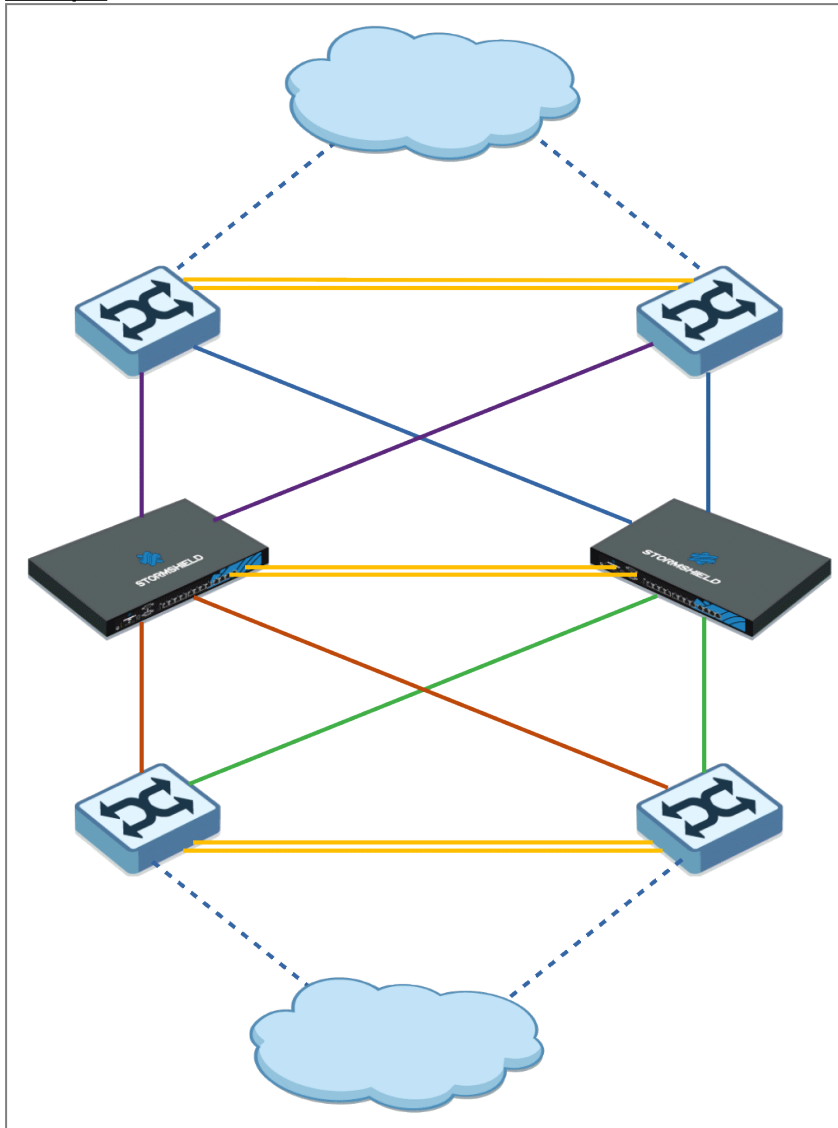
Architecture réseau - interconnexions

Afin d'éviter de créer un Single Point Of Failure (SPOF), il est fortement recommandé :

- De dupliquer les équipements réseau d'interconnexion (commutateurs),
- De raccorder les firewalls à chaque commutateur,
- De dupliquer les liens entre les commutateurs eux-mêmes.



Exemple :





Configurer la HA

La mise en œuvre d'un cluster HA de firewalls nécessite deux étapes :

- Créer le cluster sur le firewall déjà en activité,
- Intégrer l'autre firewall dans le cluster.
Notez que cette opération provoque un redémarrage du firewall intégrant le cluster. Ce redémarrage n'impacte pas la production (pas de coupure de flux).

Cette configuration peut être réalisée soit via la méthode basée sur une clé USB (voir la Note Technique [Configuration initiale par clé USB](#)), soit via l'interface Web d'administration des firewalls en suivant la procédure décrite ci-dessous.

Préparer les firewalls

- Les firewalls doivent être interconnectés via leurs interfaces HA avant de démarrer la création du cluster.
- Sur le firewall destiné à rejoindre le cluster, les interfaces réseau autres que celles dédiées à la HA ne doivent pas être connectées avant que le cluster soit entièrement défini, afin de ne pas provoquer de perturbations sur le réseau de production.

Créer le cluster

1. Connectez-vous à l'interface Web d'administration du firewall sur lequel vous souhaitez créer le cluster.
2. Cliquez sur **Système > Haute Disponibilité**.
La première étape de l'assistant de création du cluster s'affiche.
3. Sélectionnez **Créer un groupe de firewalls (cluster)**.
4. Cliquez sur **Suivant**.
5. Dans la partie **Configuration du lien principal**, sélectionnez l'**Interface** dédiée à la haute disponibilité (*dmz1* dans l'exemple).
6. Donnez un **nom** explicite à cette interface (*HA-main* dans l'exemple).
7. Définissez l'**Adresse IP et le masque réseau** pour cette interface (192.168.69.1/30 dans l'exemple).
Notez que les liens point à point acceptent des masques réseau de type /31. Dans ce cas, pour un réseau de type 192.168.69.0/31, les firewalls portent 192.168.69.0 et 192.168.69.1 comme adresse respective sur le lien HA.
8. Si vous souhaitez définir un lien de secours pour la HA, dans la partie **Lien secondaire (facultatif)**, cochez la case **Utiliser un second lien de communication**.
9. Donnez un **nom** explicite à cette interface (*HA-backup* dans l'exemple).
10. Définissez l'**Adresse IP et le masque réseau** pour cette interface (192.168.70.1/30 dans l'exemple).
11. Cliquez sur **Suivant**.



12. Indiquez et confirmez la **Clé pré-partagée** permettant de sécuriser la communication entre les membres du cluster.
Pour garantir une sécurité accrue, utilisez des mots de passe d'une longueur supérieure à 12 caractères et mixant différents types de caractères (majuscules, minuscules, chiffres et caractères spéciaux). Pour plus d'information sur la sécurité des mots de passe, consultez les [recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information \(ANSSI\)](#).
13. Vous pouvez choisir de **Chiffrer la communication entre les firewalls**, ce qui est recommandé si l'interconnexion des membres du cluster est réalisée au travers d'équipements réseau de type commutateurs.
Notez que cette option peut avoir un impact sur les performances en cas de configuration supportant un nombre élevé de connexions par seconde ou de tunnels IPsec.
14. L'option **Activer l'agrégation de liens lorsque le firewall est passif** est cochée par défaut. Elle permet dans une configuration utilisant des agrégats de liens (LACP) d'activer les agrégats même sur le membre passif du cluster. Désactivez cette option en décochant la case.
15. Cliquez sur **Suivant**.
16. Validez l'écran de résumé de la configuration en cliquant sur **Terminer**.

Intégrer le deuxième firewall dans le cluster

1. Connectez-vous à l'interface Web d'administration du firewall devant rejoindre le cluster créé précédemment.
2. Cliquez sur **Système > Haute Disponibilité**.
La première étape de l'assistant de création du cluster s'affiche.
3. Sélectionnez **Rejoindre un groupe de firewalls (cluster) existant**.
4. Cliquez sur **Suivant**.
5. Dans la partie **Configuration du lien principal**, sélectionnez l'**Interface** dédiée à la haute disponibilité.
Elle doit être identique à celle sélectionnée sur le premier firewall (*dmz1* dans l'exemple).
6. Définissez l'**Adresse IP et le masque réseau** pour cette interface. Cette adresse doit appartenir au réseau choisi pour le lien principal du premier firewall (*192.168.69.2/30* dans l'exemple).
7. Si vous avez défini un lien de secours pour la HA, dans la partie **Lien secondaire (facultatif)**, cochez la case **Utiliser un second lien de communication**.
8. Sélectionnez l'**Interface** dédiée à la haute disponibilité.
Elle doit être identique à celle sélectionnée sur le premier firewall (*dmz2* dans l'exemple).
9. Définissez l'**Adresse IP et le masque réseau** pour cette interface. Cette adresse doit appartenir au réseau choisi pour le lien secondaire du premier firewall (*192.168.70.2/30* dans l'exemple).
10. Cliquez sur **Suivant**.
11. Saisissez l'adresse IP du firewall à contacter (adresse affectée au lien HA du firewall sur lequel le cluster a été créé).
12. Indiquez la clé pré-partagée définie lors de la création du cluster.
13. Cliquez sur **Suivant**.
14. Validez l'écran de résumé de la configuration en cliquant sur **Terminer**.
Un message de confirmation s'affiche.



15. Confirmez l'opération en cliquant sur le bouton **Rejoindre le groupe de firewalls et redémarrer**.
Après avoir appliqué la nouvelle configuration réseau, le firewall ayant rejoint le cluster redémarre.
16. Une fois cette étape terminée, vous pouvez connecter les interfaces autres que celles dédiée à la HA.

Vérifier l'état du cluster

Dans l'interface Web d'administration du firewall sur lequel vous avez créé le cluster :

1. Cliquez sur l'onglet **Monitoring**.
2. Dans le widget **Indicateurs de santé**, l'icône **Lien HA** doit être verte :

The screenshot shows the Stormshield web administration interface. The 'DASHBOARD' tab is selected. The 'PROTECTION' section displays a list of events, including HA peer loss and IP address spoofing. The 'HEALTH INDICATORS' section shows various system health metrics, with the 'HA LINK' indicator highlighted in green, indicating a successful connection.

Date	Message	Action	Priority	Source	Destination
	HA: Peer lost : Firewall VMSNSX08K0013A9 doesn't reply to requests anymore (was Active). Starting ICMP monitoring (1)				
	HA: Peer lost : Firewall VMSNSX08K0013A9 doesn't reply to requests anymore (was Passive). Starting ICMP monitoring (2)				
	HA: Peer lost : Unexpected loss of firewall VMSNSX08K0013A9 (was Passive) - no ICMP reply (R:3639/S:3645) (1)				
	HA: Peer lost VMSNSX08K0013A9 (destination: 0.0.0.0) (5)				
	IP address spoofing (type=1) (destination: broadcast) (2)				
	Interactive connection detected (35)				
	Interface up: em0 (6)				
	Interface up: em2 (6)				
	Interface up: em3 (6)				

HEALTH INDICATORS

- HA LINK (Green)
- POWER (Green)
- FAN (Green)
- CPU (Green)
- MEMORY (Green)
- DISK (Green)
- RAID (Green)
- TEMPERATURE (Green)
- CERTIFICATES (Green)

3. Cliquez sur cette icône pour accéder au module **Supervision > Matériel / Haute Disponibilité**.



4. Cliquez sur l'onglet **Détails du cluster**.

L'état général des deux membres du cluster et des liens de haute disponibilité s'affiche :

MONITOR / HARDWARE / HIGH AVAILABILITY		
HARDWARE <u>CLUSTER DETAILS</u>		
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		



5. En cliquant sur **Indicateurs avancés**, vous pouvez afficher d'autres informations comme la date de dernière synchronisation, la date de dernier changement d'état du ou des liens HA :

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

État des voyants sur le firewall

Sur le firewall passif, le voyant *Online* (Run pour les SN6100 et SNI40) émet un clignotement (de l'ordre de 2 secondes éteint pour 1 seconde allumé). Ce voyant est fixe sur le firewall actif.



Modifier certains paramètres de la HA

Il est possible de modifier certains paramètres ou d'activer certaines options de la HA depuis le module **Configuration > Système > Haute Disponibilité > Configuration avancée**.

Modifier la clé pré-partagée entre les membres du cluster,

1. Positionnez-vous dans le cadre **Modifier la clé pré-partagée entre les firewalls du groupe de haute disponibilité**.
2. Entrez la **Nouvelle clé pré-partagée**.
3. Confirmez-la.
Une jauge indique le niveau de sécurité de la clé pré-partagée choisie.
4. Cliquez sur **Appliquer**.
Un message vous propose de **Sauvegarder** cette modification de configuration.
5. Ces modifications de configuration devant être synchronisées au sein du cluster, confirmez que vous souhaitez **Appliquer les modifications**.



L'icône s'affiche alors dans la partie supérieure de l'interface Web d'administration, indiquant qu'une synchronisation de configuration est attendue.

6. Cliquez sur cette icône pour provoquer la synchronisation.
Un message vous informe que cette synchronisation peut provoquer un redémarrage du firewall passif.
7. Validez en cliquant sur **Synchroniser la configuration**.
Les deux membres du cluster sont maintenant synchronisés.

Sélectionner le firewall actif en cas d'égalité (firewall prioritaire)

Le facteur de qualité est un paramètre calculé à partir de l'état de santé du firewall (plus de détails dans la section [Comprendre le calcul du facteur de qualité](#)).

En cas d'égalité de ce facteur de qualité sur les membres du cluster, vous pouvez forcer un membre du cluster à devenir le firewall actif (sélection **Automatique** par défaut).

Notez bien que cette action n'est valable qu'en cas d'égalité du facteur de qualité pour les membres du cluster : si le facteur de qualité se dégrade sur le membre du cluster sélectionné, celui-ci deviendra néanmoins passif.

1. Positionnez vous dans le cadre **Indicateur de qualité**.
2. Sélectionnez l'un des membres du cluster pour le champ **Firewall actif en cas d'égalité** :
 - *Ce firewall (numéro_de_serie_de_ce_firewall)*,
 - *L'autre firewall (distant) (numéro_de_serie_du_firewall_distant)*.
3. Cliquez sur **Appliquer**.
Un message vous propose de **Sauvegarder** cette modification de configuration.
4. Ces modifications de configuration devant être synchronisées au sein du cluster, confirmez que vous souhaitez **Appliquer les modifications**.
5. Si vous avez sélectionné *L'autre firewall (distant) (numéro_de_serie_du_firewall_distant)*, un message vous indique que la modification de priorité peut entraîner un basculement entre l'actif et le passif. Validez en cliquant sur **Appliquer**.
Dans le cas où le facteur d'égalité était identique sur les membres du cluster, le basculement est réalisé et vous êtes déconnecté de l'interface Web d'administration.



Lorsqu'un firewall a été choisi comme firewall actif par défaut, sa priorité devient alors égale à 50 (pas de priorité définie pour l'autre membre du cluster) :

MONITOR / HARDWARE / HIGH AVAILABILITY		
HARDWARE		
CLUSTER DETAILS		
Indicator	Local firewall	Remote firewall
Indicators		
Status	Active	Passive
Firmware version	4.0.2	4.0.2
Forced status	No	No
Quality index	100	100
Priority	50	
Configuration synchronization	✓ Synchronized	✓ Synchronized
HA link state	✓ OK	✓ OK
Backup HA link state	N/A	N/A
Advanced indicators		

Activer la synchronisation des sessions selon leur durée

Cette option permet de limiter le nombre de connexions synchronisées en favorisant les connexions ayant une durée supérieure à la valeur indiquée.

Les connexions très brèves et très fréquentes du type requêtes DNS ne seront ainsi pas synchronisées.

1. Positionnez-vous dans le cadre **Synchronisation des sessions**.
2. Cochez la case **Activer la synchronisation selon la durée des connexions**.
3. Indiquez la durée minimale (en secondes) que doivent respecter les connexions pour être synchronisées.
4. Cliquez sur **Appliquer**.
Un message vous propose de **Sauvegarder** cette modification de configuration.
5. Ces modifications de configuration devant être synchronisées au sein du cluster, confirmez que vous souhaitez **Appliquer les modifications**.



L'icône s'affiche alors dans la partie supérieure de l'interface Web d'administration, indiquant qu'une synchronisation de configuration est attendue.

6. Cliquez sur cette icône pour provoquer la synchronisation.
Un message vous informe que cette synchronisation peut provoquer un redémarrage du firewall passif.
7. Validez en cliquant sur **Synchroniser la configuration**.
Les deux membres du cluster sont maintenant synchronisés.

Modifier la configuration du basculement d'un membre à l'autre du cluster

Trois options peuvent être activées / désactivées :

- **Redémarrer toutes les interfaces pendant le basculement (à l'exception des interfaces HA) :**
lorsque cette option est active, les interfaces du bridge sont réinitialisées au moment du basculement pour forcer les commutateurs connectés au firewall à renouveler leur table ARP.



- **Activer l'agrégation de liens lorsque le firewall est passif** : lorsque cette option est active, dans une configuration utilisant des agrégats de liens (LACP), les agrégats sont activés même sur le membre passif du cluster.
 - **Transmettre périodiquement des requêtes ARP gratuites** : cette option permet d'envoyer à intervalle régulier des annonces ARP afin que les différents éléments du réseau (commutateurs, routeurs...) puissent mettre à jour leur propre table ARP.
1. Positionnez-vous dans le cadre **Configuration du basculement**.
 2. Activez ou désactivez un ou plusieurs de ces options.
 3. Cliquez sur **Appliquer**.
Un message vous propose de **Sauvegarder** cette modification de configuration.
 4. Ces modifications de configuration devant être synchronisées au sein du cluster, confirmez que vous souhaitez **Appliquer les modifications**.



L'icône s'affiche alors dans la partie supérieure de l'interface Web d'administration, indiquant qu'une synchronisation de configuration est attendue.

5. Cliquez sur cette icône pour provoquer la synchronisation.
Un message vous informe que cette synchronisation peut provoquer un redémarrage du firewall passif.
6. Validez en cliquant sur **Synchroniser la configuration**.
Les deux membres du cluster sont maintenant synchronisés.

Modifier le poids d'une interface dans le calcul du facteur de qualité

Le rôle et les composantes du facteur de qualité sont expliqués dans la partie [Comprendre le calcul du facteur de qualité](#).

Pour donner plus d'importance à une interface dans ce calcul, il suffit ainsi d'augmenter son poids (le poids d'une interface étant fixé à 100 par défaut) :

IMPACT OF THE UNAVAILABILITY OF AN INTERFACE IN A FIREWALL'S QUALITY INDICATOR	
Interface ▼	Weight [0-9999]
out	100
in	100
dmz2	75

1. Positionnez-vous dans le cadre **Impact de l'indisponibilité d'une interface dans l'indicateur de qualité d'un firewall**.
2. Double-cliquez dans la colonne **Poids** de l'interface dont vous voulez modifier ce paramètre.
3. Entrez la valeur souhaitée.
4. Cliquez sur **Appliquer**.
Un message vous propose de **Sauvegarder** cette modification de configuration.
5. Ces modifications de configuration devant être synchronisées au sein du cluster, confirmez que vous souhaitez **Appliquer les modifications**.



L'icône s'affiche alors dans la partie supérieure de l'interface Web d'administration, indiquant qu'une synchronisation de configuration est attendue.

6. Cliquez sur cette icône pour provoquer la synchronisation.
Un message vous informe que cette synchronisation peut provoquer un redémarrage du firewall passif.



7. Validez en cliquant sur **Synchroniser la configuration**.
Les deux membres du cluster sont maintenant synchronisés.



Composants système impliqués dans la Haute Disponibilité

Plusieurs démons ou processus assurent les différentes tâches au sein du mécanisme de Haute Disponibilité.

Moteur de gestion de prévention d'intrusion	En charge de la synchronisation des : • Tables de connexions TCP et UDP, • Tables d'hôtes, • Tables des utilisateurs authentifiés sur le firewall, • Tables d'état exclusivement pour les protocoles FTP et SIP, • Changements d'état des objets routeurs, • Tables de connexions IPState (GRE / ESP), • Associations SCTP.
Serverd	• Gère la mise en place de la HA, • Assure la connexion initiale entre les deux firewalls afin de finaliser la création du cluster, • Gère les changements de poids des interfaces.
Gatewayd	Système de messagerie interne. Les deux firewalls échangent en continu des messages pour la réplique des tunnels définis dans une politique IPsec exclusivement IKEv2 ou mixte IKEv1 / IKEv2. Lorsque la politique IPsec active ne contient que des tunnels IKEv1, ceux-ci ne sont pas répliqués.
Stated	• Calcule le facteur de qualité du membre du cluster. Le mode de calcul de ce facteur de qualité est précisé dans la section Élection du firewall actif. • Interprète les informations de l'état de la HA (membre passif en cours de redémarrage, tests de disponibilité des liens HA, synchronisation en cours...), • Décide des changements d'état (basculements), • Appelle les différentes commandes de synchronisation (fichiers de configuration, bases Active Update, ...), • Stated peut être interrogé à l'aide de l'outil <i>statedctl</i>.
Corosync	• Transport des informations d'état de la HA.
Sshd / Rsync	Synchronisation différentielle des fichiers de configuration et des bases Active Update au travers du protocole SSH.
Sshd / ldap	Synchronisation en temps réel des modifications apportées à l'annuaire LDAP interne au travers du protocole SSH.
Eventd	• Gestionnaire d'événements périodiques. • Permet de lancer à intervalle régulier les synchronisations périodiques de certificats, des baux DHCP, des informations issues de Vulnerability Manager, de l'état des routeurs supervisés au travers des autres démons comme SSHD.
Alived - ICMP	Tests de vie entre les membres du cluster.
Arpsync	Envoi des requêtes ARP gratuites (périodiquement ou à l'occasion d'un basculement).



Utiliser les commandes CLI/Serverd relatives à la HA

Les commandes CLI / Serverd **CONFIG HA** et **HA** permettent de configurer et de commander la HA au travers de la console CLI présente dans l'interface Web d'administration.

Le détail de ces commandes est disponible dans le [Guide de référence des commandes CLI / Serverd](#) (menus **CONFIG HA** et **HA**).



Éléments répliqués au sein d'un cluster

Les listes ci-dessous précisent les éléments répliqués entre le firewall actif et le firewall passif.

Éléments synchronisés en temps réel

- Tables des connexions TCP et UDP,
- Tables de connexions IPState (GRE / ESP),
- Associations SCTP,
- Tables d'hôtes,
- Tables des utilisateurs authentifiés sur le firewall,
- Modifications de l'annuaire LDAP interne,
- Tables d'état exclusivement pour les protocoles FTP et SIP,
- État des routeurs supervisés,
- Numéros de série des certificats,
- Associations de sécurité (IKE-SA et IPsec-SA) des connexions VPN IPsec basées sur le protocole IKEv2,
- Compteurs anti-rejeu des connexions VPN IPsec IKEv2.

Éléments synchronisés périodiquement

- Bases Active Update,
- Modifications de configuration du firewall (à la demande),
- Baux DHCP (5 minutes),
- Base d'événement de SN Vulnerability Manager (60 minutes),
- Nouveaux certificats et CRL téléchargées (60 minutes).

Éléments non synchronisés

- Connexions directes avec le firewall de type sessions d'administration (SSH, Serverd, interface Web d'administration ...)
- Connexions prises en charge par les proxies.
- Logs.



Exclure des flux TCP/UDP de la réplication

Dans des configurations soumises à de fortes charges réseau, il peut être nécessaire d'optimiser les flux répliqués.

Ainsi, au sein de la politique de filtrage, il est possible d'exclure des flux de la synchronisation en décochant l'option **Synchroniser cette connexion entre les firewalls (HA)** cochée par défaut (menu **Action > Configuration avancée** de la boîte d'édition de la règle de filtrage) :

The screenshot shows the 'EDITING RULE NO 1' window. On the left is a sidebar with tabs: General, Action (highlighted), Source, Destination, Port - Protocol, and Inspection. The main area is titled 'ACTION' and has three sub-tabs: GENERAL, QUALITY OF SERVICE, and ADVANCED PROPERTIES (which is selected). Under the 'ADVANCED PROPERTIES' tab, there are three sections: 'Redirect' with a 'Service' dropdown set to 'None' and an unchecked checkbox 'Redirect incoming SIP calls (UDP)'; 'Logs' with three checked checkboxes: 'Disk', 'Syslog server', and 'IPFIX collector'; and 'Advanced properties' with four checkboxes: 'Count', 'Force source packets in IPSec', 'Force return packets in IPSec', and 'Synchronize this connection between firewalls (HA)'. The last checkbox is checked and is enclosed in a red rectangular box. At the bottom of the window are 'CANCEL' and 'OK' buttons.

Les connexions traitées par cette règle ne seront ainsi pas répliquées entre les membres du cluster.



Principe de la synchronisation

Depuis la version 4 de SNS, la synchronisation en temps réel au sein du cluster est réalisée grâce au protocole *Kernel To Kernel* (K2K) basé sur le port 44242/UDP.

Synchronisation en temps réel

Les **éléments à synchroniser en temps réel** (tables des connexions TCP et UDP, tables de connexions IPState [GRE / ESP], associations SCTP, tables d'hôtes, ...) sont envoyés en permanence du firewall actif vers firewall passif et les états sont synchronisés à la volée.

Il n'est donc plus nécessaire d'attendre le basculement pour que ces tables soient intégrées dans le noyau du firewall passif : en effet, les connexions y sont présentes en permanence, dans un état dit "larvaire", c'est à dire prêtes à être activées en cas de basculement. Ainsi, par exemple, les liens entre règles de filtrage et connexions sont déjà établis dans le noyau du firewall passif, ce qui entraîne une reprise d'activité beaucoup plus rapide et des performances accrues.

Cet accroissement des performances est également lié à la suppression du mécanisme de synchronisations de masse (*bulk updates*) grâce au protocole K2K.

Synchronisation à la demande

Lorsqu'un administrateur modifie la configuration du firewall actif, cette modification n'est pas immédiatement répliquée car elle peut nécessiter un redémarrage du firewall passif pour être prise en compte au sein du cluster.

Dans ce cas, l'administrateur peut déclencher cette synchronisation au moment voulu de deux manières différentes :

- Soit en cliquant sur l'icône  affichée dans le bandeau supérieur de l'interface d'administration du cluster,
- Soit à l'aide de la commande CLI (module **Configuration** > **Système** > **Console CLI**) : HA SYNC

Pour plus de détails sur cette commande, veuillez vous référer au [Guide de référence des commandes CLI / Serverd](#).



Flux réseau liés à la HA

Le mécanisme de Haute Disponibilité nécessite les flux suivants entre les deux membres du cluster :

- **Trafic Kernel to Kernel** : utilisé pour la synchronisation en temps réel (cf. tableau des **Éléments synchronisés en temps réel**), ce protocole est basé sur le port UDP/44242 (uniquement en IPv4). Ce port peut être personnalisé dans le fichier `~/ConfigFiles/Protocols/hasync/common` (cette modification doit être réalisée sur les deux membres du cluster et suivie de la commande *enha* pour être prise en compte).
- **Trafic sur le port TCP/1300 (démon *serverd*)** : utilisé par le firewall qui rejoint le cluster pour récupérer la configuration HA et la configuration réseau du cluster.
- **Trafic sur les ports TCP/16058 et TCP/16059 (démon *gatewayd*)** : utilisé pour la synchronisation des états VPN IPsec.
- **Trafic RSYNC au travers d'une session SSH (TCP/22)** : permet au firewall qui rejoint le cluster de récupérer les fichiers de configuration (système, filtrage, ...) ou de synchroniser les modifications d'annuaire LDAP.
- **Trafic unicast et multicast sur les ports UDP/5404 et UDP/5405 (démon *corosync*)** : utilisé par les deux firewalls pour l'échange de messages en relation avec la HA et pour la supervision du réseau dédié à la HA sur le lien principal de contrôle. Lorsqu'un lien de secours est paramétré, celui-ci utilise les ports UDP/5406 et UDP/5407 pour ces mêmes opérations.
Si le mode sécurisé (option **Chiffrer la communication entre les firewalls**) a été choisi lors de la création du cluster, les ports UDP/5405 et UDP/5405 (UDP/5406 et UDP/5407 pour l'éventuel lien de secours) sont respectivement remplacés par les ports UDP/5414 et UDP/5415 (UDP/5416 et UDP/5417 pour l'éventuel lien de secours).
L'adresse multicast utilisée par défaut est 226.94.1.1. Celle-ci peut être personnalisée dans le fichier `~/ConfigFiles/HA/highavailability`.
Si les liens HA sont réalisés au travers de commutateurs réseau, il est nécessaire de désactiver les fonctions "*IGMP snooping*" sur ces équipements afin d'autoriser le trafic multicast.
- **Trafic ICMP echo request (Ping)** : utilisé pour contrôler le fonctionnement d'un firewall du point de vue réseau.

Notez que ces différents types de flux sont autorisés par le biais d'une règle de filtrage implicite (**Autoriser l'accès mutuel entre les membres d'un groupe de firewalls (cluster HA)**) activée lors de la mise en place de la Haute Disponibilité.

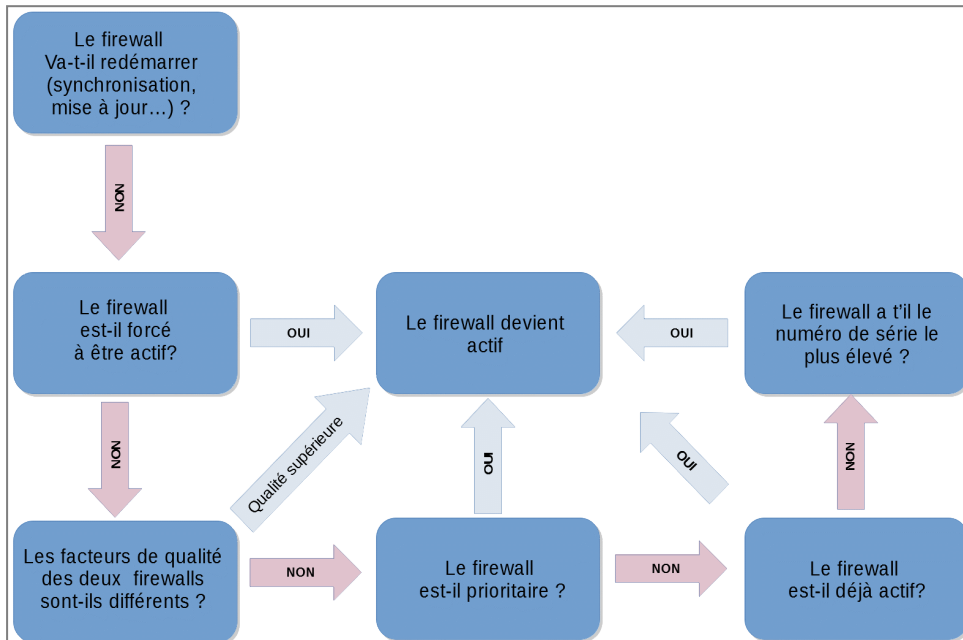
La désactivation de cette règle entraîne l'interruption immédiate du fonctionnement de la HA.



Élection du firewall actif

L'élection du membre actif du cluster est organisée lors du démarrage de la HA.

Cette élection respecte le processus suivant :



Il est important de noter qu'il est possible de forcer un firewall à être actif (menu **Configuration > Système > Maintenance > Configuration > Haute disponibilité**). Dans ce cas, ce firewall sera actif même si son facteur de qualité est inférieur. Il est déconseillé d'utiliser cette option pour un cluster en production. Cette option est à réserver pour le débogage d'une configuration.

Ce processus fait notamment référence à la comparaison du facteur de qualité de chacun des firewalls. Cette notion de facteur de qualité est expliquée dans la suite de cette section.

Comprendre le calcul du facteur de qualité

Le facteur de qualité est issu d'une formule mathématique calculée en tenant compte de différents indicateurs :

- État et poids des interfaces actives du firewall (les interfaces HA sont exclues de ce calcul), y compris pour les interfaces regroupées au sein d'un agrégat (LACP / Redondance).

Notez que dans le cas d'un agrégat (LACP / Redondance), par défaut, le facteur de qualité du firewall se dégrade après la perte de tous les membres de l'agrégat. Il est possible de paramétrer la HA pour que la perte d'une seule interface membre de l'agrégat dégrade le facteur de qualité. Ce paramètre peut être activé à l'aide des commandes CLI / Serverd **CONFIG HA CREATE** et **CONFIG HA UPDATE** en modifiant la valeur du paramètre ci-dessous à **1** :

- Pour un agrégat de type *LACP* : `LACPMembersHaveWeight=<0|1>`,
 - Pour un agrégat de type *Redondance* (à partir de la version SNS 4.3) : `FailoverMembersHaveWeight=<0|1>`.
- État du(des) disque(s) dur(s),



- État du TPM sur les modèles qui en disposent.
Le jeton de configuration *TPMQualityIncluded=1* présent dans la section *[Global]* du fichier de configuration *ConfigFiles/HA/highavailability* indique que l'état du module TPM est pris en compte.
- État des modules additionnels (réseau, alimentation, ventilateur ...) sur les modèles haut de gamme.

Exemple de calcul de l'indicateur de qualité des interfaces

Dans cet exemple, seules les interfaces 1 (*out*), 2 (*in*) et 4 (*dmz2*) entrent en compte, l'interface *dmz1* étant dédiée à la HA. Notez que l'interface 2 (*in*) présente un défaut de connectivité :



Les poids affectés aux interfaces sont les suivants :

IMPACT OF THE UNAVAILABILITY OF AN INTERFACE IN A FIREWALL'S QUALITY INDICATOR	
Interface ▾	Weight [0-9999]
out	100
in	100
dmz2	75

L'indicateur de qualité des interfaces pour ce firewall vaut donc : $(1 \times 100 + 0 \times 100 + 1 \times 75) / (100 + 100 + 75) = 63\%$

L'indicateur ainsi calculé sera intégré dans le calcul global du facteur de qualité tenant compte des [autres paramètres](#).



Commandes de contrôle de la HA

Les commandes suivantes peuvent être passées au travers de la console d'un des membres du cluster.

hainfo [-v]

Permet d'afficher les informations d'état de la HA :

```
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

Retourne l'état du firewall courant (actif ou passif).

hasync [-v]

Déclenche une synchronisation différentielle des membres du cluster :



```

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

Permettent de forcer l'état du firewall courant ou de supprimer ce forçage. Les commandes haactive et hapassive ne prennent pas en compte la valeur du facteur de qualité des membres du cluster :

```

VMSNSX09L0712A9>hainfo

Nodes status:
VMSNSX(09L0712A9)_(local) VMSNSX(08K0012A9)
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



Permet de comparer un fichier de configuration entre les membres du cluster.

hasyncctest

Évalue les fichiers de configuration non synchronisés :

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

enha

Permet de recharger les paramètres de la HA :

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



Mise à jour logicielle d'un cluster

La méthode ci-dessous est destinée à limiter les perturbations de production lors de la mise à jour logicielle d'un cluster de firewalls.

Mettre à jour le firewall passif

1. Connectez-vous à l'interface Web d'administration du cluster.
2. Si des modifications de configuration n'ont pas été synchronisés, cliquez sur l'icône  afin de provoquer une synchronisation de configuration avant la mise à jour du cluster.
3. Dans le menu **Configuration** > **Système** > **Maintenance** > onglet **Mise à jour du système**, sélectionnez le fichier de mise à jour (champ **Sélectionnez la mise à jour**),
4. Dans le champ **Firewall à mettre à jour**, sélectionnez **L'autre firewall (distant)**.
5. Cliquez sur **Mettre à jour le firewall**.
6. Validez le message d'avertissement *Un autre membre du groupe de firewalls (cluster) va redémarrer* en cliquant sur **OK**.
7. Attendez le redémarrage du firewall distant.

Si votre firewall est équipé d'un TPM (*Trusted Platform Module*)

Lors d'une mise à jour de firmware, les registres PCR (*Platform Configuration Registers*) connus du TPM peuvent être modifiés, rendant alors l'accès aux secrets stockés dans le TPM non fonctionnel. Il est alors nécessaire de mettre à jour la politique d'accès au TPM en actualisant les valeurs de PCR. Ainsi, pour tout cluster en version SNS 4.3.3 ou supérieure, lorsque le membre passif du cluster a redémarré suite à sa mise à jour, vous pouvez appliquer la procédure suivante :

1. Dans l'interface Web d'administration du membre actif du cluster, placez-vous dans le module **Système** > **Console / CLI**.
2. Tapez la commande `SYSTEM TPM PCRSEAL tpmpassword=<password> serial=passive` et cliquez sur **Exécuter**.



[Plus d'information sur la commande SYSTEM TPM PCRSEAL.](#)

Mettre à jour le firewall actif

Lorsque le membre passif du cluster a redémarré suite à sa mise à jour :

1. Retournez dans le menu **Configuration** > **Système** > **Maintenance** > onglet **Mise à jour du système**.
2. Sélectionnez le fichier de mise à jour (champ **Sélectionnez la mise à jour**).
3. Dans le champ **Firewall à mettre à jour**, choisissez **Ce firewall**.
4. Cliquez sur **Mettre à jour le firewall**.
5. L'autre membre du cluster devient actif et les connexions traversant le cluster ne sont pas interrompues.



Si votre firewall est équipé d'un TPM (*Trusted Platform Module*)

1. Dans l'interface Web d'administration du membre actif du cluster, placez-vous dans le module **Système** > **Console / CLI**.
2. Tapez la commande `SYSTEM TPM PCRSEAL tmpassword=<password> serial=passive` et cliquez sur **Exécuter**.



Plus d'information sur la commande `SYSTEM TPM PCRSEAL`.



Remplacement du membre défectueux d'un cluster (Return Material Authorization - RMA)

Lorsqu'un membre du cluster est défectueux, il est nécessaire de suivre la procédure décrite dans cette section pour procéder à son remplacement.

Après acceptation de la demande de RMA par Stormshield, et lorsque le firewall de remplacement est en votre possession, appliquez la procédure qui suit.

Supprimer de la configuration du cluster le numéro de série de l'ancien firewall

Cette étape consiste à supprimer de la configuration du cluster le numéro de série du firewall défectueux. Dans le cas contraire, le firewall de remplacement ne pourra pas rejoindre le cluster et le message d'erreur *Too many firewalls in the HA cluster* sera affiché.

Après avoir déconnecté le firewall destiné à être remplacé :

1. Connectez-vous à l'interface Web d'administration du cluster.
2. Dans le menu **Configuration > Système > Console CLI**, tapez la commande permettant de supprimer le numéro de série du firewall à remplacer :

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

3. Activez ce changement de configuration avec la commande :

```
HA CLUSTER ACTIVATE
```

Ajouter le firewall remplaçant au cluster

1. Connectez les liens dédiés à la HA sur le firewall de remplacement.
2. Ne connectez pas les autres liens sur ce firewall.
3. Appliquez la [procédure permettant à ce firewall de rejoindre le cluster](#).



Résoudre les incidents

Les événements liés à la HA sont enregistrés principalement dans le fichier `/log/l_system`. Ils sont associés au Service "HA". Les types d'événements HA enregistrés sont les suivants :

- Changement d'état (actif / passif) du firewall,
- Échec du chargement de configuration sur le passif lors de l'initialisation du cluster,
- Arrêt du démon Stated sur un des membres du cluster,
- Démarrage du démon Stated sur un des membres du cluster,
- Mise en pause de la HA (exemple : lors du rechargement de la politique de filtrage),
- Échec du rechargement de configuration au redémarrage de la HA,
- Conflit de licences entre les membres du cluster,
- Échec de l'initialisation d'une synchronisation,
- Pas de réponse de l'autre membre du cluster lors d'un redémarrage (provoque le passage en actif du firewall ayant redémarré),
- L'autre membre du cluster n'est pas détecté,
- L'autre membre du cluster est détecté (entraîne une synchronisation complète [*bulk update*]),
- Démarrage d'une synchronisation complète [*bulk update*],
- La synchronisation n'a pas abouti,
- La synchronisation s'est terminée normalement,
- Un membre du cluster s'arrête ou redémarre,
- Rechargement de la configuration réseau,
- Synchronisation de la date / heure,
- Erreur de transmission (perte de paquets),
- Erreur de synchronisation de fichiers de configuration.

Ils peuvent être consultés par le biais du menu **Monitoring > Logs - Journaux d'audit > Événements système** de l'interface Web d'administration du firewall (ci-dessous avec un filtre sur le terme *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	



Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sur la haute disponibilité sont disponibles dans la [base de connaissances Stormshield](#) (authentification nécessaire).



STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2025. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.