La Redondance d'une Infrastructure 2 Tiers

via Active/Standby Failover sur ASAs 5506X

Ershad RAMEZANI

Table des matières

Une infrastructure redondée

Une infrastructure redondée est une configuration qui a été conçue de manière à inclure des copies de ses composants essentiels pour augmenter sa fiabilité. En cas de panne ou de défaillance d'un élément, les copies peuvent prendre le relais et assurer la continuité du service.

Il existe plusieurs niveaux de redondance qui peuvent être mis en place dans une infrastructure, allant de la simple duplication de matériel à l'utilisation de configurations complexes avec des systèmes de répartition de charge et de failover.

Nous allons construire une infrastructure en trois couches, comprenant des pares-feux, une couche centrale (cœur) et une couche d'accès. Pour mettre en place la redondance, nous allons utiliser plusieurs méthodes :

- **Le basculement au niveau des appareils** : pour rediriger le trafic vers un équipement de secours en cas de panne.
- Le **basculement au niveau des interfaces** : pour utiliser plusieurs liens de manière active/passive.
- **La mise en pile de commutateurs** : pour créer un groupe de commutateurs qui partagent une configuration et un pool de ressources.
- **L'agrégation de liens avec LACP** : pour combiner plusieurs liens physiques en un seul lien logique de plus grande capacité

Architecture réseau 2 et 3 Tiers

Le modèle en 3 tiers

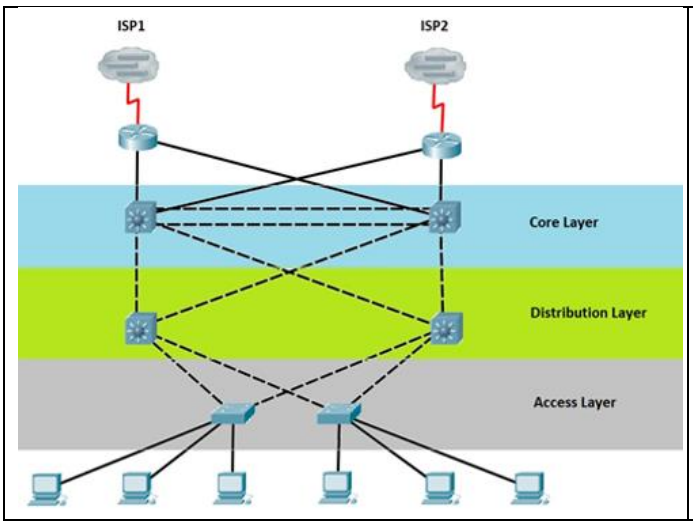
C'est une architecture de réseau qui comprend trois couches de commutateurs.

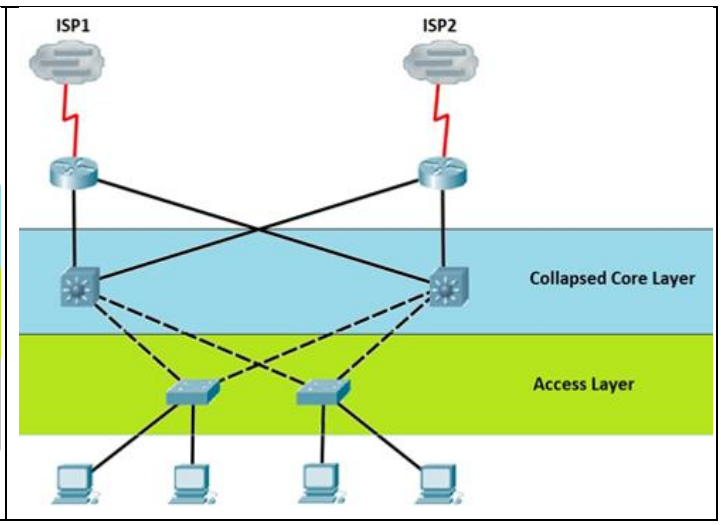
La couche centrale, ou "**core layer**", sert de colonne vertébrale au réseau et relie les commutateurs de la couche de distribution. Ces derniers, à leur tour, regroupent le trafic provenant des commutateurs de la couche d'accès, qui sont chargés de connecter les terminaux au réseau.

Le modèle en 2 tiers

Une alternative au modèle en 3 tiers est l'architecture en 2 tiers, également appelée "**Collapsed Core Architecture**".

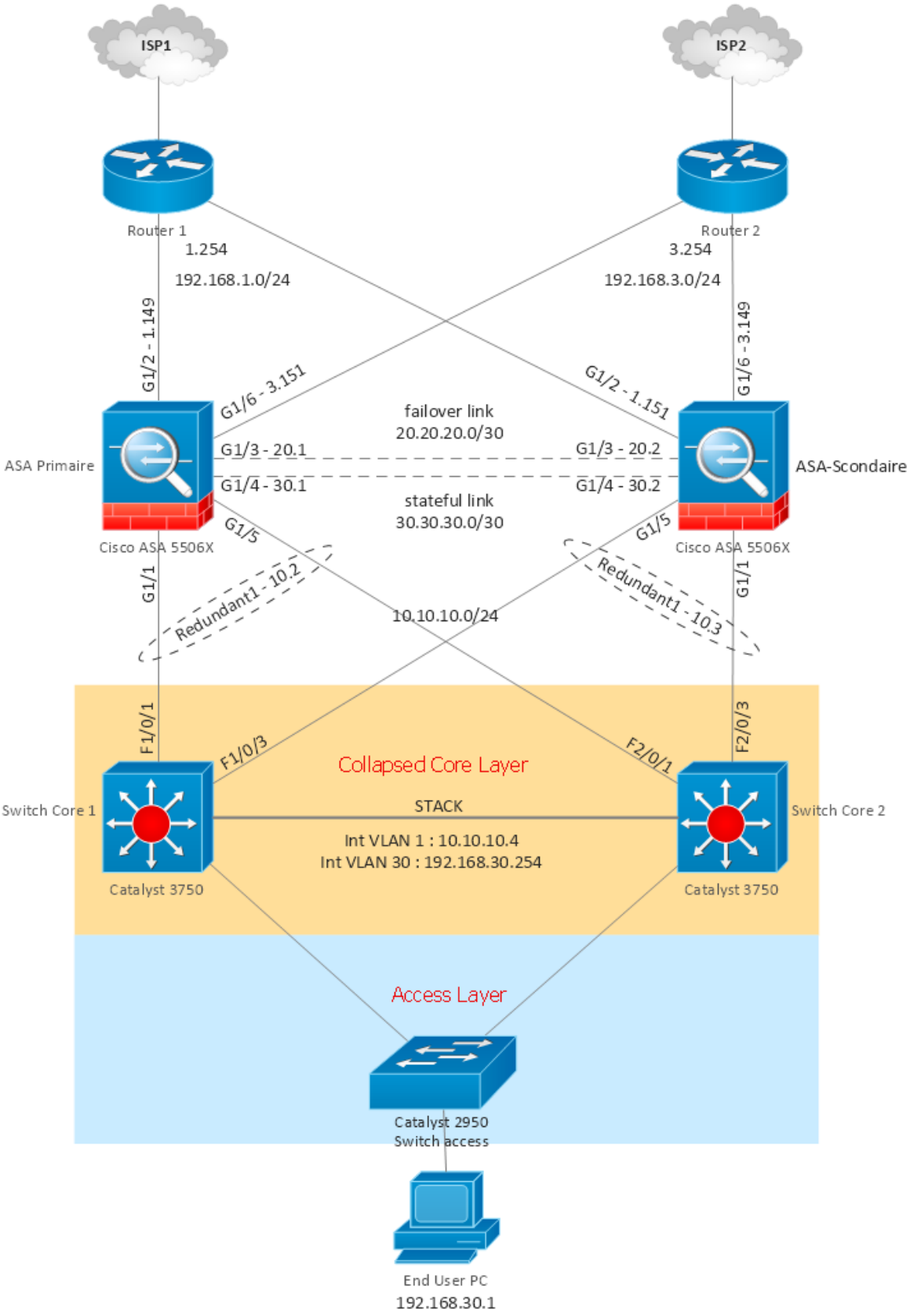
Dans ce cas, les couches centrale et de distribution sont combinées en une seule couche, ce qui permet à l'organisation d'économiser sur les coûts en réduisant le nombre de matériel nécessaire. Cette architecture est également considérée comme moins complexe à configurer et à gérer.





Le schéma du réseau 2 Tiers

Le schéma final de notre réseau sera organisé comme suit. Nous allons configurer chaque élément étape par étape dans cet article. Tout d'abord, nous allons configurer le basculement actif/passif sur les ASAs. Ensuite, nous configurons les commutateurs cœurs et finalement, nous configurons le côté WAN des ASAs qui va vers des routeurs FAI.



PREMIERE PARTIE : LE BASCULEMENT SUR LES ASA

Les types de basculement

Cisco ASA propose deux types de basculement : un qui se produit au niveau de l'appareil (device-level failover) et un autre qui se produit au niveau de l'interface (interface-level failover).

Basculement au niveau de l'appareil

Dans le basculement au niveau de l'appareil, si l'appareil active commence à rencontrer des problèmes tels qu'une panne matérielle, le standby peut changer de rôle et devenir l'actif.

Dans la configuration initiale du basculement au niveau de l'appareil, vous désignez un appareil comme primaire et l'autre comme secondaire. Si les deux appareils sont mis sous tension en même temps, l'appareil primaire devient active tandis que l'appareil secondaire assume le rôle standby.

Si l'appareil primaire/actif rencontre des problèmes et qu'un basculement se produit, l'appareil secondaire devient active. Lorsque l'appareil primaire récupère, elle reste dans le rôle standby jusqu'à ce qu'un basculement se produise sur l'appareil secondaire/active.

Différents types de basculement au niveau de l'appareil

Cisco ASA prend en charge deux types différents de basculement au niveau de l'appareil :

- Basculement actif/standby
- Basculement actif/actif

Basculement actif/standby

L'unité active est responsable du passage du trafic et l'appareil standby surveille l'état de l'appareil active. Les deux appareils envoient des messages d'accueil pour surveiller l'état l'une de l'autre.

Basculement actif/actif

Le basculement actif/actif est une fonctionnalité dans laquelle les deux appareils, tout en surveillant l'état de leurs homologues, transmettent activement le trafic. Les appareils en mode de basculement Actif/Actif ne peuvent être déployées qu'en multimode.

Active/Standby Failover

Lorsque deux dispositifs ASA identiques sont configurés en basculement, l'un des appareils, l'appareil actif, est responsable de :

- la création des tables d'état et de traduction,
- du transfert des paquets de données
- et de la surveillance de l'autre unité.

L'autre dispositif de sécurité, l'appareil standby, est chargé de surveiller l'état de l'unité active.

Lorsqu'une panne se produit sur l'appareil active, le standby prend le relais du rôle actif et commence à transférer le trafic. Cette appareil nouvellement active reprend également les adresses IP et MAC qui étaient utilisées par l'appareil précédente. Après la récupération de l'unité défaillante, elle assume le rôle de standby.

Lien de contrôle de basculement

Les appareils active et standby sont connectées via une liaison réseau dédiée pour s'envoyer mutuellement des messages liés au basculement. Cette connexion, connue sous le nom de *lien de contrôle de basculement* (*failover control link*), est établie via une interface LAN de basculement dédiée.

Le lien de contrôle de basculement fournit un support sur lequel les deux appareils peuvent communiquer et se mettre à jour sur les éléments suivants :

- L'état de l'unité (active ou standby)

- État du lien réseau
- Messages Hello ou keepalive (qui sont envoyés sur toutes les interfaces)
- Échange d'adresse MAC
- Réplication de la configuration de l'actif à standby

Configuration matérielle et logicielle requise pour la mise en œuvre de failover

Pour que le basculement fonctionne correctement, les spécifications suivantes doivent être identiques :

Numéro de produit ou de modèle de l'appareil : Par exemple, les deux appareils doivent être Cisco ASA 5506x. Vous ne pouvez pas utiliser un ASA 5506x et un ASA 5505 en basculement.

Quantité de RAM : Vous ne pouvez pas utiliser 512 Mo de RAM dans une appareil et 1024 Mo dans l'autre.

Nombre d'interfaces : Les deux appareils doivent avoir le même nombre d'interfaces physiques.

Module externe : Si vous disposez d'un module de sécurité, les deux appareils doivent l'avoir.

Clé d'activation avec les mêmes fonctionnalités : La clé d'activation doit avoir les mêmes fonctionnalités, telles que le mode de basculement, le niveau de chiffrement et le nombre de pairs VPN.

La version du logiciel ne doit pas nécessairement être la même sur les dispositifs de sécurité lorsque le basculement est configuré.

Conditions qui déclenchent le basculement

Pour que le basculement se produise, l'une des conditions suivantes doit être remplie :

- Un administrateur est manuellement passé d'active à standby.
- L'appareil active a perdu de l'alimentation ou est tombée en panne en raison de défauts matériels/logiciels.
- Une appareil standby a cessé de recevoir des paquets hello (ou keepalive) sur l'interface de contrôle de basculement.
- La liaison de l'interface de contrôle de basculement est interrompue.
- L'état de la liaison d'une interface de transmission de données est *down*.

Basculement au niveau de l'interface

Les appareils de sécurité peuvent fournir une couche supplémentaire de redondance en regroupant deux interfaces physiques dans une interface logique. De cette façon, si l'une des interfaces physiques tombe en panne, l'appareil de sécurité activera l'interface de secours de ce groupe, plutôt que d'activer un basculement de l'appareil.

Dans la redondance au niveau de l'interface, une seule interface physique est active à la fois tandis que l'autre interface est en veille. Lorsque l'interface active tombe en panne, l'interface de secours commence à transmettre le trafic pour éviter le basculement au niveau de l'appareil. Lorsque les deux interfaces physiques de l'interface logique redondante échouent, l'appareil de sécurité déclenche le basculement au niveau de l'appareil, en supposant qu'il est configuré et activé.

Préparation nécessaire pour configurer les ASAs

Pour commencer, il est important de réaliser les configurations de base sur les deux appareils de sécurité. Ces configuration comprennent :

Une fois que nous avons mis en place la fonction de basculement, la configuration de l'ASA primaire sera automatiquement dupliquée sur l'ASA secondaire. Il n'est donc pas nécessaire de configurer l'ASA secondaire, nous devons seulement configurer l'ASA primaire avec les paramètres nécessaires.

Le NAT :

```
object network obj_any
 subnet 0.0.0.0 0.0.0.0
object network nat-outside
 subnet 0.0.0.0 0.0.0.0
object network nat-BACKUP
 subnet 0.0.0.0 0.0.0.0
```

```
object network nat-outside
 nat (inside,outside) dynamic interface
object network nat-BACKUP
 nat (inside,BACKUP) dynamic interface
```

Les routes par défaut :

```
route inside 192.168.20.0 255.255.255.0 10.10.10.4 1
route inside 192.168.30.0 255.255.255.0 10.10.10.4 1
route inside 192.168.40.0 255.255.255.0 10.10.10.4 1
```

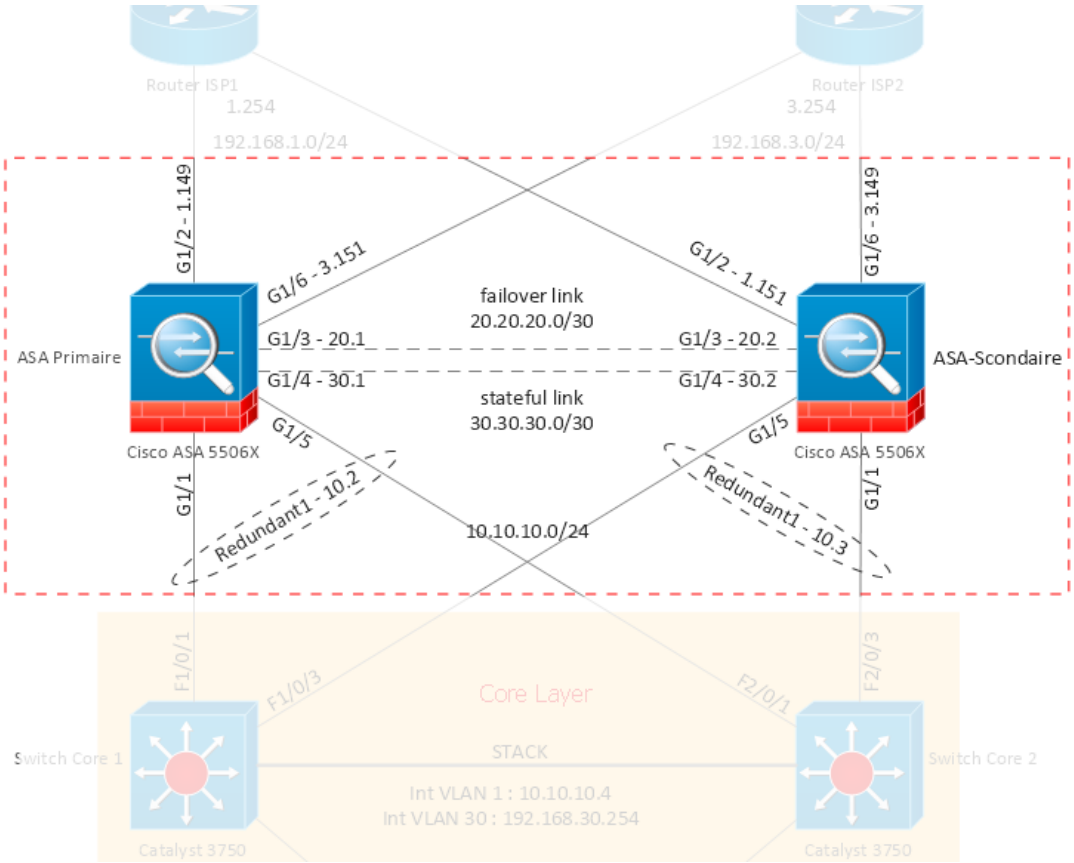
```
route outside 0.0.0.0 0.0.0.0 192.168.1.254 1 track 1
route BACKUP 0.0.0.0 0.0.0.0 192.168.3.254 100
```

Policy-map :

```
policy-map global_policy
 class inspection_default
inspect icmp
inspect http
```

La mise en œuvre de failover actif/standby

Il nous suffit de configurer le failover sur un ASA et celui-là va répliquer sa configuration sur la deuxième au moment d'activation de failover.



La configuration de la fonctionnalité de basculement actif/standby dans Cisco ASA est décomposée en sept étapes :

Étape 1 : Sélectionnez le lien de basculement.

Décidez quelle interface sera utilisée pour envoyer les messages de contrôle de basculement. Utilisez la commande **failover lan interface** suivie du nom de l'interface pour configurer le lien de basculement via l'interface de ligne de commande.

```
failover lan interface MONFAILOVER GigabitEthernet1/3
```

Étape 2 : Attribuez des adresses IP de basculement.

Pour que deux appareils de sécurité communiquent, l'interface de contrôle de basculement désignée doit être configurée avec deux adresses IP. La première adresse est utilisée par l'appareil active et la seconde adresse IP appartient à l'appareil standby. L'unité active utilise son adresse pour synchroniser la configuration en cours avec standby et pour envoyer et recevoir des messages d'accueil.

```
failover interface ip MONFAILOVER 20.20.20.1 255.255.255.252 standby 20.20.20.2
```

Après avoir sélectionné et attribué l'adresse IP active/standby sur l'interface de contrôle de failover, l'étape suivante consiste à configurer les interfaces de transmission de données pour le système et les adresses IP de standby. L'appareil active utilise les adresses IP du système, tandis que l'autre appareil utilise les adresses IP standby. Pour cela il faut d'abord choisir l'interface. Faites pareil pour l'interface G1/6 (les interfaces G1/1 et G1/5 seront configurés dans la prochaine étape).

```
interface GigabitEthernet1/2
 nameif outside
 security-level 0
 ip address 192.168.1.149 255.255.255.0 standby 192.168.1.151
!
```

Si vous ne savez pas si vous êtes sur le pare-feu actif ou en veille et que vous souhaitez envoyer des commandes à l'unité appropriée, vous pouvez utiliser la commande ***failover exec***.

```
ADRARFORM/pri/act(config)# failover exec ?

exec mode commands/options:
  active   Execute command on the active unit
  mate     Execute command on the peer unit
  standby  Execute command on the standby unit
ADRARFORM/pri/act(config)# failover exec active sh run
: Saved

:
: Serial Number: JAD211207KK
: Hardware:   ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
:
ASA Version 9.6(1)
!
hostname ADRARFORM
enable password 8Ry2YjIyt7RRXU24 encrypted
names
```

Étape 3 : Configurer le basculement au niveau des interfaces (G1/1 et G/1/5)

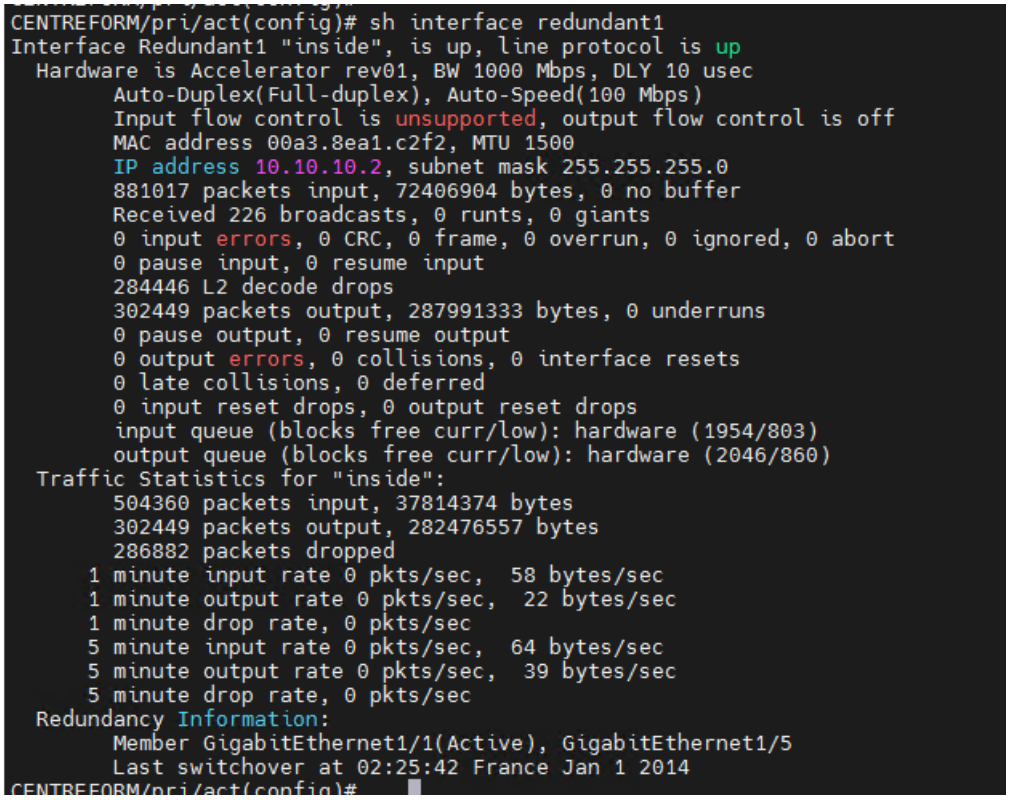
Voici comment configurer les interfaces redondantes sur un ASA :

- ASA(config)# interface Redundant1
- ASA(config-if)# member-interface GigabitEthernet1/1
- ASA(config-if)# member-interface GigabitEthernet1/5
- ASA(config-if)# nameif inside
- ASA(config-if)# security-level 100
- ASA(config-if)# ip address 10.10.10.2 255.255.255.0 standby 10.10.10.3

Une fois que l'interface redondante a été configurée, on peut utiliser la commande show running-config pour vérifier son état.

```
interface Redundant1
 member-interface GigabitEthernet1/1
 member-interface GigabitEthernet1/5
 nameif inside
 security-level 100
 ip address 10.10.10.2 255.255.255.0 standby 10.10.10.3
!
```

La commande show interface *redundant1* permet de voir des informations détaillées sur l'interface redondante que vous venez de configurer. Elle indique notamment la date du dernier changement de l'interface active.



Il est important de mentionner que l'interface redundant1 est considérée comme une seule interface par ASA, peu importe le nombre de membres physiques qu'elle peut avoir.

Étape 4 : Définir la clé de basculement (facultatif)

Pour sécuriser les messages de contrôle de basculement qui sont envoyés entre les appareils Cisco ASA, un administrateur peut éventuellement spécifier une clé secrète partagée. Il est fortement recommandé de spécifier le secret partagé pour chiffrer et authentifier les messages de basculement s'ils sont susceptibles d'être interceptés par des utilisateurs non autorisés. Si une clé de basculement n'est pas utilisée, l'appareil active envoie toutes les informations en texte clair, y compris les états UDP/TCP, les informations d'identification de l'utilisateur et les informations relatives au VPN.

```
failover key *****
```

Étape 5 : Désignez l'appareil primaire.

Les deux appareils de sécurité envoient des messages de contrôle de basculement via un câble réseau aux appareils identiques. Pour dire quel périphérique doit agir en tant que primaire ou secondaire, vous devez désigner l'état primaire et secondaire via la configuration logicielle.

```
failover lan unit primary
```

Étape 6 : Activez le basculement avec état (facultatif).

La fonction de basculement avec état des appareils Cisco réplique les tables d'état et de traduction de l'unité active vers l'unité standby. En cas de panne, l'unité standby devient active et commence à transmettre le trafic afin que les flux de données ne soient pas interrompus. La fonction de basculement avec état nécessite une connexion réseau entre les deux unités pour répliquer les informations d'état de connexion. Les appareils peuvent utiliser une interface de contrôle dédiée ou celui de failover pour répliquer les mises à jour. Vous pouvez utiliser l'interface LAN de failover si les mises à jour avec état ne surchargent pas la bande passante de l'interface. Configurez une interface différente pour le basculement avec état si vous craignez de surcharger l'interface de contrôle de basculement.

Dans notre laboratoire on va utiliser une interface de contrôle dédiée :

```
failover link STATEFULLINK GigabitEthernet1/4
```

```
failover interface ip STATEFULLINK 30.30.30.1 255.255.255.252 standby 30.30.30.2
```

Réplication HTTP

Remarque : Le basculement avec état ne réplique pas les connexions HTTP. Les connexions HTTP ont généralement une courte durée de vie et ne sont donc pas répliquées par défaut. De plus, ils ajoutent une charge considérable sur l'appareil de sécurité si la quantité de trafic HTTP est importante par rapport à d'autres trafics. Si vous souhaitez répliquer les connexions HTTP vers l'appareil de secours, vous pouvez utiliser la commande *failover replication http*.

```
ADRARFORM/pri/act(config)# failover replication ?

configure mode commands/options:
  http  Enable HTTP (port 80) connection replication
  rate  Configure bulk-sync connection replication rate
```

```
failover replication http
```

Étape 7 : Activez le basculement globalement.

La dernière étape de la configuration du basculement sur l'appareil primaire consiste à activer le basculement globalement.

```
ADRARFORM(config)# failover
```

Étape 8 : Configurez le basculement sur l'appareil secondaire.

Dans la fonction de basculement Cisco, il n'est pas nécessaire de configurer manuellement l'appareil secondaire. Au lieu de cela, il vous suffit de configurer quelques informations de base sur le basculement. Après cela, l'appareil principale/active commence à synchroniser sa configuration.

La configuration comprend les six paramètres de configuration suivants :

- Activation de l'interface de contrôle de basculement
- Désignation du basculement comme secondaire
- Interface de lien de basculement
- Mêmes adresses IP d'interface de basculement
- Même clé partagée de basculement
- Activation du basculement

```
failover lan unit secondary
failover lan interface MONFAILOVER GigabitEthernet1/3
failover key *****
```

```
failover interface ip MONFAILOVER 20.20.20.1 255.255.255.252 standby 20.20.20.2
```

```
ADRARFORM(config)# failover
ADRARFORM(config)# .
..

       Detected an Active mate
Beginning configuration replication from mate.

End configuration replication from mate.
```

Remarque : Lorsque le failover est activé sur l'ASA, il localise son partenaire primaire/actif et le reconnaît comme étant actif. Ensuite, la configuration est répliqué depuis l'ASA primaire jusqu'au l'ASA secondaire.

Show failover

Il est possible de visualiser l'état de la redondance de l'appareil en utilisant la commande *show failover* :

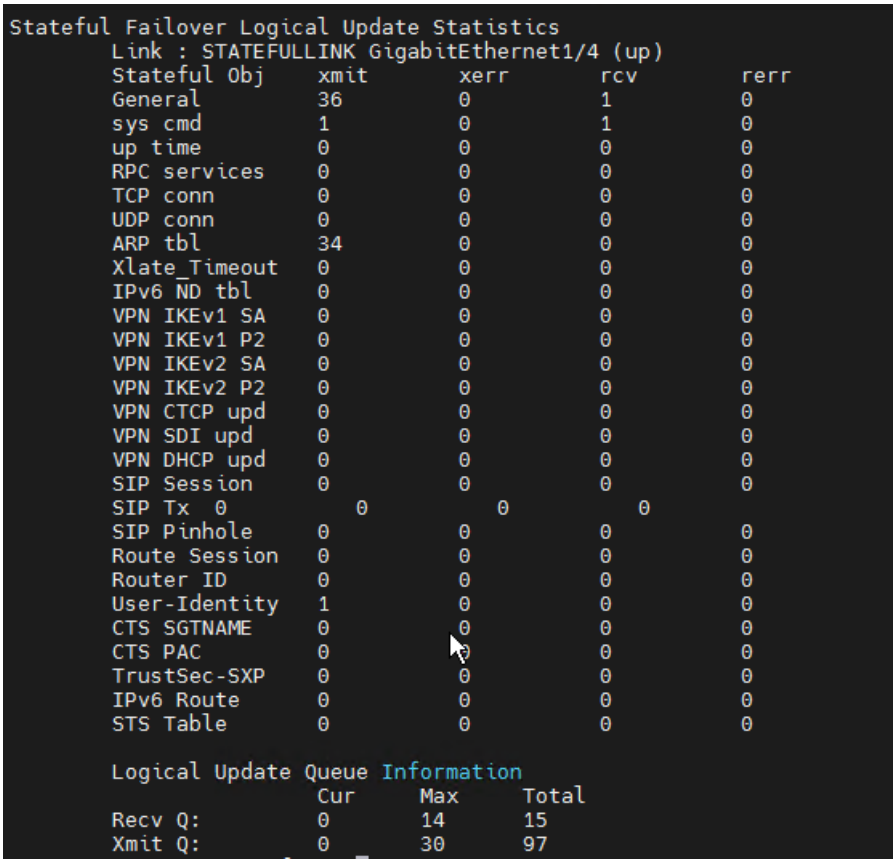
```
ADRARFORM(config)# sh failover
Failover On
Failover unit Secondary
Failover LAN Interface: MONFAILOVER GigabitEthernet1/3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 40 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.6(1), Mate 9.6(1)
Serial Number: Ours JAD21130JJ8, Mate JAD211[illegible]KK
Last Failover at: 20:33:31 UTC Jun 29 2022
        This host: Secondary - Standby Ready
                Active time: 86929 (sec)
                slot 1: ASA5506 hw/sw rev (2.0/9.6(1)) status (Up Sys)
                  Interface inside (10.10.10.3): Normal (Monitored)
                  Interface outside (192.168.1.151): Normal (Monitored)
                slot 2: SFR5506 hw/sw rev (N/A/6.2.2.4-34) status (Up/Up)
                  ASA FirePOWER, 6.2.2.4-34, Up, (Monitored)
        Other host: Primary - Active
                Active time: 2763 (sec)
                slot 1: ASA5506 hw/sw rev (2.0/9.6(1)) status (Up Sys)
                  Interface inside (10.10.10.2): Normal (Monitored)
                  Interface outside (192.168.1.149): Normal (Monitored)
                slot 2: SFR5506 hw/sw rev (N/A/6.2.2.4-34) status (Up/Up)
                  ASA FirePOWER, 6.2.2.4-34, Up, (Monitored)

Stateful Failover Logical Update Statistics
        Link : STATEFULLINK GigabitEthernet1/4 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         345        0          14685      0
        sys cmd         345        0          345        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          20         0
        UDP conn        0          0          49         0
        ARP tbl         0          0          14268      0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        VPN IKEv1 SA    0          0          0          0
        VPN IKEv1 P2    0          0          0          0
        VPN IKEv2 SA    0          0          0          0
        VPN IKEv2 P2    0          0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
```

Avec ou sans le lien stateful

Sans le lien stateful, nous sommes dans une situation stateless. Voici le résultat de la commande sh failover dans la situation stateless :

```
ADRARFORM/pri/act(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: MONFAILOVER GigabitEthernet1/3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 40 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.6(1), Mate 9.6(1)
Serial Number: Ours JAD211207KK, Mate JAD21130JJ8
Last Failover at: 20:33:34 UTC Jun 29 2022
        This host: Primary - Active
                Active time: 17 (sec)
                slot 1: ASA5506 hw/sw rev (2.0/9.6(1)) status (Up Sys)
                  Interface inside (10.10.10.2): Normal (Waiting)
                  Interface outside (192.168.1.149): Normal (Waiting)
                slot 2: SFR5506 hw/sw rev (N/A/6.2.2.4-34) status (Up/Up)
                  ASA FirePOWER, 6.2.2.4-34, Up, (Monitored)
        Other host: Secondary - Standby Ready
                Active time: 86929 (sec)
                slot 1: ASA5506 hw/sw rev (2.0/9.6(1)) status (Up Sys)
                  Interface inside (10.10.10.3): Normal (Waiting)
                  Interface outside (192.168.1.151): Normal (Waiting)
                slot 2: SFR5506 hw/sw rev (N/A/6.2.2.4-34) status (Up/Up)
                  ASA FirePOWER, 6.2.2.4-34, Up, (Monitored)

Stateful Failover Logical Update Statistics
        Link : Unconfigured.
```

Une fois le lien stateful configuré, on peut consulter les statistiques liées à ce dernier.

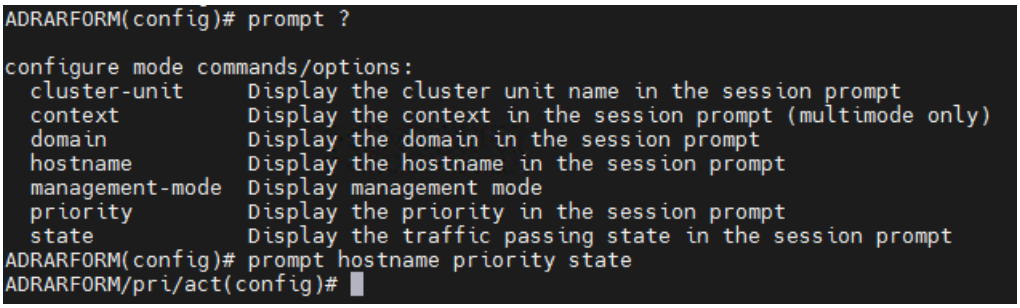


Les ASA sont maintenant identiques

Une fois le failover activé, les deux unités seront exactement les mêmes. Si nous modifions la configuration d'une unité, cette modification sera également appliquée à l'autre. Cela signifie que les deux unités n'ont plus leur propre identité indépendante. Lorsque l'unité de secours prend le relais, elle utilise l'adresse IP et MAC de l'unité active plutôt que les siennes.

Modifier le nom de l'invite de commande (prompt)

Pour savoir sur quelle unité on est connecté, on peut utiliser une commande pour changer le nom du prompt (ce qui apparaît avant chaque ligne de commande).



Dans l'image en haut, on peut voir que le nom du prompt a été modifié (ADRARFORM/pri/act) suite à une commande donnée. On peut également voir que cette unité est le primaire. Dans l'image suivante, le nom de l'unité secondaire a également été modifié de la même manière. Cela se produit car les deux unités sont considérées comme identiques et leur configuration est répliquée l'une sur l'autre.

```
ADRARFORM(config)#
ADRARFORM(config)#
ADRARFORM(config)#
ADRARFORM/sec/stby(config)#
ADRARFORM/sec/stby(config)#
ADRARFORM/sec/stby(config)#
ADRARFORM/sec/stby(config)#
ADRARFORM/sec/stby(config)#
```

Effectuer les commandes sur quelle unité?

Il est important de toujours effectuer les commandes sur l'unité active car c'est à partir de celle-ci que la réplication vers l'unité standby se fait. Si les commandes ne sont pas données sur l'unité active, les deux unités ne seront plus synchronisées.

```
ADRARFORM/sec/stby(config)# hostname ADRAR
**** WARNING ****
        Configuration Replication is NOT performed from Standby unit to Active unit.
        Configurations are no longer synchronized.
ADRAR/sec/stby(config)#
ADRAR/sec/stby(config)#
```

Voici donc pourquoi on peut utiliser la commande failover exec :

```
ADRAR/sec/stby(config)# failover exec active hostname ADRAR
ADRAR/sec/stby(config)#
ADRAR/sec/stby(config)#
```

Passer manuellement de l'état actif au standby et vice versa.

On peut changer qui est l'unité active et qui est l'unité standby en utilisant la commande *failover active* ou *no failover active*. Si l'unité active doit devenir la standby, on utilise la commande "failover active" sur l'unité standby. Si l'unité standby doit devenir active, on utilise la commande "no failover active" sur l'unité active.

```
CENTREFORM/pri/stby(config)#
CENTREFORM/pri/stby(config)#
CENTREFORM/pri/stby(config)# failover active

        Switching to Active
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)#
```

Configuration de la stratégie d'interface

L'appareil surveille l'état de toutes les interfaces. Si **l'une** des interfaces ne répond pas, un basculement se produit et l'Appliance standby reprend les connexions. Toutefois, si vous préférez que le système bascule lorsque **deux interfaces ou plus** ne répondent pas, vous pouvez modifier ce comportement par défaut en modifiant la stratégie de basculement de l'interface.

```
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)# failover interface-policy 2
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)#
```

Le résultat :

```
failover polltime unit msec 500 holdtime 3
failover polltime interface 6 holdtime 30
failover interface-policy 2
failover key *****
failover replication http
```

Note importante : Puisque nous n'avons qu'une seule interface (redundant1) sur le couple ASA et que nous devons attendre que le basculement se produise lorsque cette interface ne fonctionne plus, nous devons absolument configurer le failover interface-policy sur une seule interface.

Modification de la fréquence d'envoi des paquets keepalive

Les ASA envoient périodiquement des messages "keepalive" (ou "hello") pour vérifier l'état de leur paire de basculement. Si l'appareil standby ne reçoit pas de réponse à son message "keepalive", il effectue un basculement

seulement s'il est en meilleure condition que l'appareil actif actuel. Les appareils supportent deux types de messages de basculement :

- **Unité :** Envoyé toutes les secondes pour surveiller l'état de **l'interface de contrôle** de basculement.
- **Interface :** Envoyé toutes les 15 secondes pour surveiller la santé des **interfaces physiques**.

Vous pouvez toutefois modifier ce comportement par défaut pour envoyer des paquets keepalive en fonction de délais d'attente personnalisés. Par exemple, vous pouvez envoyer des paquets keepalive toutes les 500 millisecondes pendant 3 secondes (hold-time timer) pour surveiller l'état de l'interface de basculement. Les appareils envoient des paquets au partenaire toutes les 500 millisecondes. Si le temps de maintien de l'interface de l'unité est atteint (qui est de 3 secondes) et qu'aucune réponse n'a été entendue, le processus de basculement sera lancé. Les résultats du test d'interface déterminent si l'appareil secondaire doit initier un basculement.

```
CENTREFORM/pri/act(config)# failover polltime unit msec 500 holdtime 3
CENTREFORM/pri/act(config)# failover polltime inte
CENTREFORM/pri/act(config)# failover polltime interface 6 holdtime 30
CENTREFORM/pri/act(config)#
```

```
failover polltime unit msec 500 holdtime 3
failover polltime interface 6 holdtime 30
```

Surveillance des interfaces de basculement

Lorsqu'une appareil est configurée pour le basculement, qu'elle soit active/standby ou active/active, elle surveille l'état de toutes les principales interfaces physiques qui ont un **nameif** et une adresse IP configurés. Si vous ne souhaitez pas que le processus de basculement surveille une interface particulière, telle qu'une interface de test, vous pouvez désactiver la surveillance de cette interface.

Vous pouvez utiliser la commande **no monitor-interface** pour désactiver la surveillance de l'interface et **monitor-interface** pour activer la surveillance sur cette interface. Par exemple s'il y a une interface management que vous ne vouliez pas le surveiller.

```
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)# no monitor-interface inside
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)# monitor-interface inside
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)#
```

Surveillance et dépannage des basculements

Cisco ASA dispose d'un riche ensemble de commandes **show** et **debug** qui sont utiles pour surveiller l'état de l'appareil de secours. Ces commandes sont particulièrement importantes pour isoler un problème si quelque chose se comporte de manière inattendue.

Surveillance

Show failover

Une fois l'appareil primaire configurée pour le basculement, vérifiez que l'appareil reconnaît le basculement comme activé. Vous pouvez vérifier les adresses IP de failover ou standby à l'aide de la commande *show failover*. Si le basculement avec état est configuré, *show failover* affiche également les statistiques de basculement avec état, ainsi que le nombre de mises à jour qu'il a reçues et transmises.

Show ip

l'adresse IP de système est toujours la même chose chez les deux unités. Même si on change le rôle active d'un à l'autre. Mais quant à *Current Address IP* (adresse IP actuel de l'unité lui-même), c'est l'unité activé qui récupère l'adresse IP de système et l'autre récupère l'adresse IP de standby. On peut vérifier cela en changeant l'unité active à l'aide de la commande "failover active" sur l'unité standby.

```
CENTREFORM/sec/stby(config)#
CENTREFORM/sec/stby(config)#
CENTREFORM/sec/stby(config)# failover active

        Switching to Active
CENTREFORM/sec/act(config)#
CENTREFORM/sec/act(config)#
CENTREFORM/sec/act(config)#
CENTREFORM/sec/act(config)#
CENTREFORM/sec/act(config)# sh ip
System IP Addresses:
Interface                  Name                 IP address      Subnet mask      Method
GigabitEthernet1/1         inside               10.10.10.2      255.255.255.0    CONFIG
GigabitEthernet1/2         outside              192.168.1.149   255.255.255.0    CONFIG
GigabitEthernet1/3         MONFAILOVER          20.20.20.1      255.255.255.252  unset
GigabitEthernet1/4         STATEFULLINK         30.30.30.1      255.255.255.252  unset
Current IP Addresses:
Interface                  Name                 IP address      Subnet mask      Method
GigabitEthernet1/1         inside               10.10.10.2      255.255.255.0    CONFIG
GigabitEthernet1/2         outside              192.168.1.149   255.255.255.0    CONFIG
GigabitEthernet1/3         MONFAILOVER          20.20.20.2      255.255.255.252  unset
GigabitEthernet1/4         STATEFULLINK         30.30.30.2      255.255.255.252  unset
CENTREFORM/sec/act(config)#
CENTREFORM/sec/act(config)#
```

```
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)#
        Switching to Standby

CENTREFORM/pri/stby(config)#
CENTREFORM/pri/stby(config)# sh ip
System IP Addresses:
Interface                  Name                 IP address      Subnet mask      Method
GigabitEthernet1/1         inside               10.10.10.2      255.255.255.0    CONFIG
GigabitEthernet1/2         outside              192.168.1.149   255.255.255.0    CONFIG
GigabitEthernet1/3         MONFAILOVER          20.20.20.1      255.255.255.252  unset
GigabitEthernet1/4         STATEFULLINK         30.30.30.1      255.255.255.252  unset
Current IP Addresses:
Interface                  Name                 IP address      Subnet mask      Method
GigabitEthernet1/1         inside               10.10.10.3      255.255.255.0    CONFIG
GigabitEthernet1/2         outside              192.168.1.151   255.255.255.0    CONFIG
GigabitEthernet1/3         MONFAILOVER          20.20.20.1      255.255.255.252  unset
GigabitEthernet1/4         STATEFULLINK         30.30.30.1      255.255.255.252  unset
CENTREFORM/pri/stby(config)#
CENTREFORM/pri/stby(config)#
```

show failover state

Si le basculement se produit et que vous ne savez pas pourquoi il s'est produit, émettez la commande **show failover state**.

On voit qu'il y avait deux failover à cause de la défaillance de l'interface dans deux dates différentes.

```
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         Ifc Failure              14:43:57 UTC Jan 12 2014
Other host -   Secondary
               Standby Ready  Ifc Failure              19:16:05 UTC Jan 8 2014

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

Dépannage

Si le basculement est correctement configuré, mais que les appareils de sécurité ne parviennent pas à synchroniser la configuration, il faut vérifier l'état de ces appareils de sécurité.

```
CENTREFORM/pri/act(config)# show failover | include host
        This host: Primary - Active
        Other host: Secondary - Standby Ready
```

L'appareil de sécurité prend en charge un certain nombre de commandes de **debug** pour dépannage. Utilisez les commandes **debug fover** pour activer les messages de débogage de basculement.

```
CENTREFORM/pri/act(config)# debug fover ?

exec mode commands/options:
  cable     Failover LAN status
  cmd-exec  Failover EXEC command execution
  fail      Failover internal exception
  fmsg      Failover message
  ifc       Network interface status trace
  open      Failover device open
  rx        Failover Message receive
  rxdmp     Failover recv message dump (serial console only)
  rxip      IP network failover packet recv
  snort     Failover NGFW mode snort processing
  switch    Failover Switching status
  sync      Failover config/command replication
  tx        Failover Message xmit
  txdmp     Failover xmit message dump (serial console only)
  txip      IP network failover packet xmit
  verify    Failover message verify
CENTREFORM/pri/act(config)# debug fover cable
fover event trace on
CENTREFORM/pri/act(config)# fover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
fover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
fover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
fover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
fover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
fover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
ufover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
nfover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
defover_fail_check: send_msg_ifc(): 10.10.10.2->10.10.10.3 ifc 2 cmd FHELLO
fover_fail_check: send_msg_ifc(): 192.168.1.149->192.168.1.151 ifc 3 cmd FHELLO
fover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
bufover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
ggfover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
ing fover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
```

```
CENTREFORM/pri/act(config)# fover_fail_check: send_msg_ifc(): 192.168.1.149->192.168.1.151 ifc 2 cmd FHELLO
fover_fail_check: send_msg_ifc(): 192.168.3.149->192.168.3.151 ifc 3 cmd FHELLO
fover_fail_check: send_msg_ifc(): 10.10.10.2->10.10.10.3 ifc 4 cmd FHELLO
```

```
defover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
bfover_fail_check: send_msg_ifc(): 192.168.1.149->192.168.1.151 ifc 2 cmd FHELLO
fover_fail_check: send_msg_ifc(): 192.168.3.149->192.168.3.151 ifc 3 cmd FHELLO
fover_fail_check: send_msg_ifc(): 10.10.10.2->10.10.10.3 ifc 4 cmd FHELLO
```

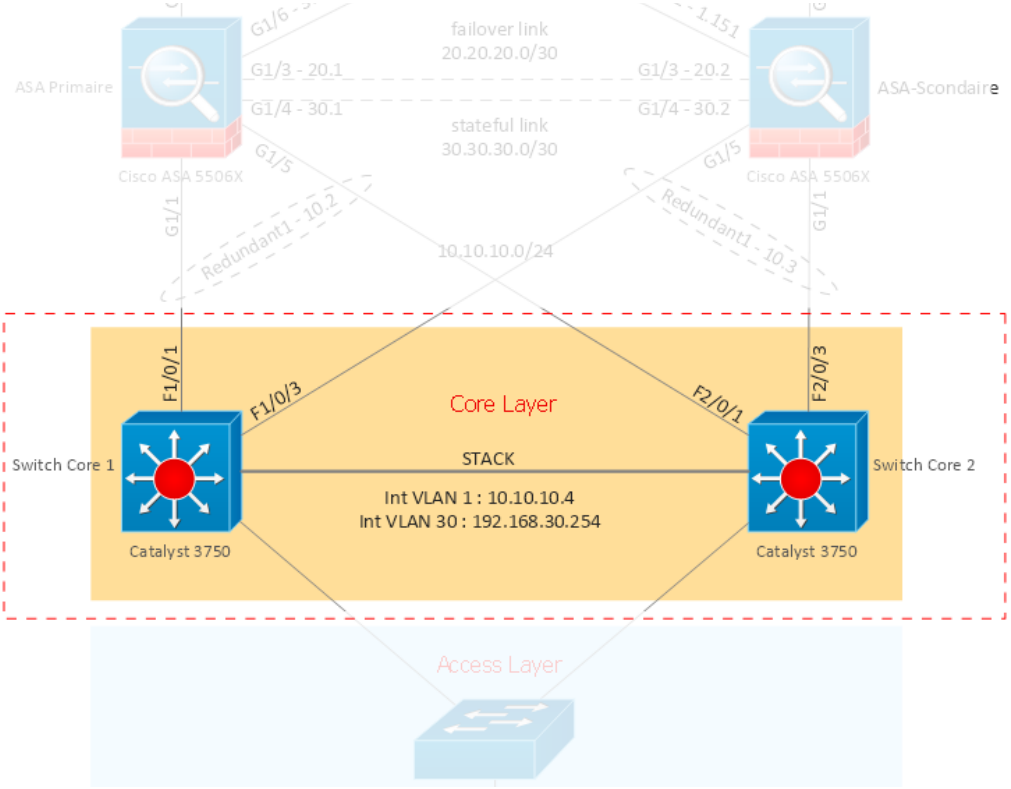
Utilisez la commande **undebug all** pour arrêter le débogage.

```
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
bufover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
fover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
g fover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
alfover_health_monitoring_thread: fover_lan_check() Failover LAN Check
fover_health_monitoring_thread: fover_lan_check() Failover Interface OK
l
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)#
```

DEUXIEME PARTIE : LA CONFIGURATION DES SWITCHES CŒURS

Dans la dernière partie nous avons configurés l'interface redundant1. Les interfaces G1/1 et G1/5 sont regroupés en tant qu'interface logique redundant1. G1/1 sur le pare-feu actif est physiquement connecté au SW-core-1, tandis que G1/5 est connecté au SW-core-2.

De même, G1/5 sur le pare-feu standby est physiquement connecté au SW-core-1, tandis que G1/1 est connecté au SW-core-2. Si l'une des interfaces physiques ne parvient pas à transmettre le trafic, l'interface de secours au sein de l'interface redondante commence à transmettre le trafic.



Le besoin pour une interface Multi-Chassis EtherChannel

Les interfaces G1/1 et G1/5 sur le ASA-primaire sont connectées au F1/0/1 de sw-core-1 et f2/0/1 de sw-core-2. Pour que ce lien de redondante fonctionne, les f1/0/1 et f2/0/3 doivent être les membre d'un interface Multi-Chassis EtherChannel.

EtherChannel vs Multi-Chassis EtherChannel

EtherChannel est une technologie d'agrégation de liens qui permet de regrouper plusieurs liens Ethernet physiques pour créer une lien Ethernet logique dans le but de fournir une tolérance aux pannes et des liens à haut débit entre les switches, les routeurs et les serveurs.

Quand les interfaces qui sont membres d'un lien EtherChannel appartiennent au switches qui sont physiquement séparés, ce lien sera un Multi-Chassis EtherChannel.

Multi-Chassis EtherChannel est un nom données par Cisco aux différents méthodes de mettre en place d'un lien EtherChannel entre les switches :

- Virtual Switching System (VSS) (Cisco Catalyst 4500 and 6500)
- Stackwise Virtual (Cisco Catalyst 3750, 3850, and 9000)
- Virtual Port Channel (Cisco Nexus switches)

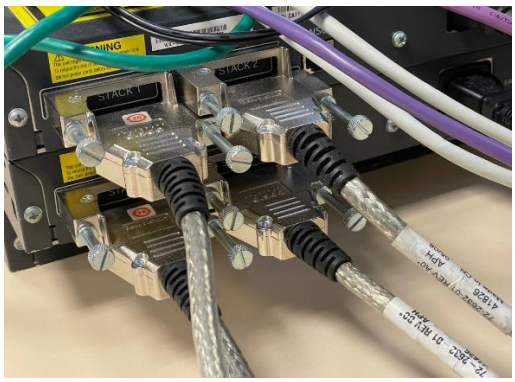
Un seul switch ne prendra pas en charge tous ces trois méthodes. Selon les plateformes de commutateurs, certaines peuvent supporter certaines options. Si un commutateur peut utiliser l'une d'entre elles, cela sera seulement celle-là. Par exemple, un commutateur peut gérer Stackwise, mais pas VSS ou vPC en même temps.

Dans ce cas, nos switches principaux sont les Catalyst 3750. Nous allons donc configurer l'EtherChannel multi-châssis en empilant ces deux switches.

Mise en pile des switches Catalyst 3750

Dans les commutateurs Catalyst 3750, Une pile de commutateurs est un ensemble de commutateurs connectés via leurs ports Cisco StackWise. L'un des commutateurs Catalyst 3750 contrôle le fonctionnement de la pile et est appelé le maître de la pile. Le voyant nommé Master sur le panneau avant du commutateur 3750 devient vert lorsque le commutateur devient maître dans la pile.

Le maître et les autres commutateurs Catalyst 3750 sont des membres de la pile. Les membres de la pile utilisent la technologie Cisco StackWise pour se comporter et travailler ensemble comme un système unifié. Les protocoles des couches 2 et 3 présentent l'ensemble de la pile de commutateurs comme une seule entité sur le réseau.



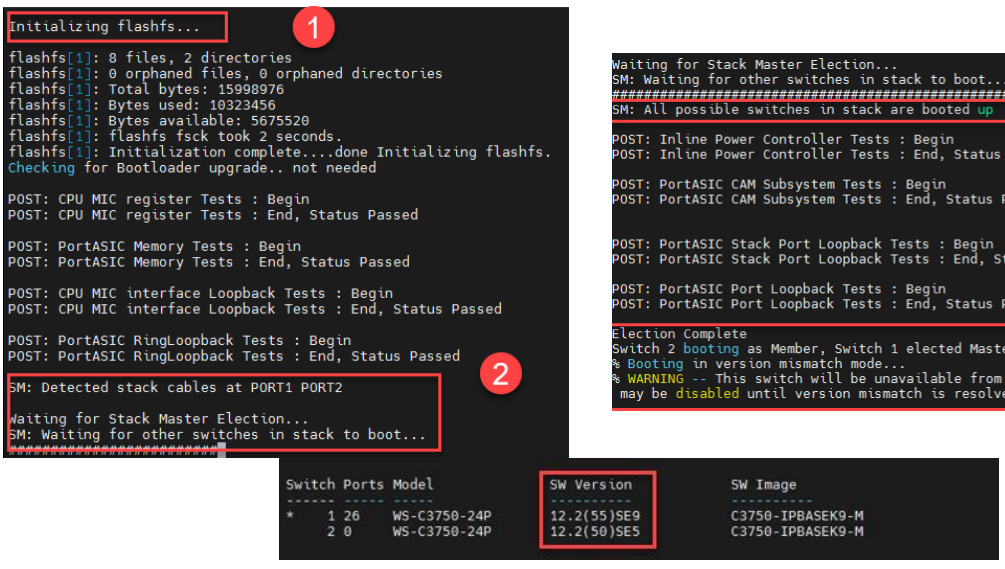
La compatibilité pour la mise en pile

- Les commutateurs avec des numéros de version majeurs différents sont incompatibles et ne peuvent pas exister dans la même pile de commutateurs.
- Les commutateurs avec le même numéro de version majeure mais avec un numéro de version mineure différent de celui du maître de la pile sont considérés comme partiellement compatibles.

Dans le dernier cas, lorsqu'il est connecté à une pile de commutateurs, le logiciel détecte l'incompatibilité de la version mineure et tente de mettre à niveau le commutateur en mode incompatibilité avec l'image de la pile de commutateurs ou avec une image de fichier tar de la mémoire flash de la pile de commutateurs.

Créer une pile de commutateurs

Il est facile de créer une pile de commutateurs à partir de deux commutateurs autonomes. Lorsque ces deux commutateurs sont fusionnés pour former la pile, ils effectuent une élection pour déterminer lequel d'entre eux sera le maître de la pile. Le commutateur esclave redémarrera et se joindra à la pile. Si les versions ne correspondent pas, une mise à niveau sera effectuée à ce stade.



```
Switch>sh switch
Switch/Stack Mac Address : 0011.bbda.9000
                                            H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Master 0011.bbda.9000     1      0       Ready
 2       Member 001c.0e7f.4c80     1      2       Version Mismatch
```

Dans cette étape, auto copy sera lancé automatiquement

```
*Mar  1 00:03:53.220: %IMAGEMGR-6-AUTO_COPY_SW_INITIATED: Auto-copy-software process initiated for switch number(s
 2
```

```
Switch>
Switch>
Extracting images from archive into flash on switch 2...
Switch>
Switch>
Switch>
```

```
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: Searching for stack member to act
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: as software donor...
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: Found donor (system #1) for
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: member(s) 2
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: System software to be uploaded:
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: System Type:          0x00000000
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: archiving c3750-ipbasek9-mz.122-55.SE9 (directory)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: archiving c3750-ipbasek9-mz.122-55.SE9/info (681 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: archiving c3750-ipbasek9-mz.122-55.SE9/c3750-ipbasek9-mz.122-55.SE
(12106358 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: archiving c3750-ipbasek9-mz.122-55.SE9 (directory)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: archiving c3750-ipbasek9-mz.122-55.SE9/info (683 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: archiving info (107 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: examining image...
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: extracting info (107 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: extracting c3750-ipbasek9-mz.122-55.SE9/info (681 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: extracting c3750-ipbasek9-mz.122-55.SE9/info (683 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: extracting info (107 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: Stacking Version Number: 1.45
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: System Type:          0x00000000
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:   Ios Image File Size:   0x00B8DA00
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:   Total Image File Size: 0x00B8C200
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:   Minimum Dram required: 0x08000000
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:   Image Suffix:          ipbasek9-122-55.SE9
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:   Image Directory:       c3750-ipbasek9-mz.122-55.SE9
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:   Image Name:            c3750-ipbasek9-mz.122-55.SE9.bin
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:   Image Feature:         IP|LAYER_3|SSH|3DES|MIN_DRAM_MEG=128
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: Old image for switch 2: flash2:/c3750-ipbasek9-mz.122-50.SE5
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:   Old image will be deleted before download.
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: Deleting `flash2:/c3750-ipbasek9-mz.122-50.SE5' to create required
e
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: c3750-ipbasek9-mz.122-55.SE9 (directory)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: extracting c3750-ipbasek9-mz.122-55.SE9/info (681 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: extracting c3750-ipbasek9-mz.122-55.SE9/c3750-ipbasek9-mz.122-55.S
n (12106358 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: c3750-ipbasek9-mz.122-55.SE9 (directory)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: extracting c3750-ipbasek9-mz.122-55.SE9/info (683 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: extracting info (107 bytes)
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: Installing (renaming): `flash2:/update/c3750-ipbasek9-mz.122-55.SE
'
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:                                    `flash2:/c3750-ipbasek9-mz.
5.SE9'
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: New software image installed in flash2:/c3750-ipbasek9-mz.122-55.S

1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW:
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: All software images installed.
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: Requested system reload in progress...
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: Software successfully copied to
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: system(s)2
1 00:10:05.179: %IMAGEMGR-6-AUTO_COPY_SW: Done copying software
1 00:10:05.187: %IMAGEMGR-6-AUTO_COPY_SW: Reloading system(s) 2
1 00:10:08.492: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 1 has changed to state DOWN
1 00:10:08.492: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 1 has changed to state DOWN
1 00:10:09.373: %STACKMGR-4-SWITCH_REMOVED: Switch 2 has been REMOVED from the stack
```

```
Election Complete
Switch 2 booting as Member, Switch 1 elected Master
HCOMP: Compatibility check PASSED
Waiting for feature sync....
Waiting for Port download...Complete
Stack Master is ready
```

```
Switch>sh switch
Switch/Stack Mac Address : 0011.bbda.9000
                                            H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Master 0011.bbda.9000     1      0       Ready
 2       Member 001c.0e7f.4c80     1      0       Ready

Switch>
```

```
Switch>show switch detail
Switch/Stack Mac Address : 0011.bbda.9000
                                            H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Master 0011.bbda.9000     1      0       Ready
 2       Member 001c.0e7f.4c80     1      0       Ready


         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
--------------------------------------------------------
  1        Ok          Ok               2        2
  2        Ok          Ok               1        1

Switch>
```

```
Switch#show platform stack manager all
Switch/Stack Mac Address : 0011.bbda.9000
                                            H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Master 0011.bbda.9000     1      0       Ready
 2       Member 001c.0e7f.4c80     1      0       Ready


         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
--------------------------------------------------------
  1        Ok          Ok               2        2
  2        Ok          Ok               1        1
```

Création de Multi-Chassis EtherChannel

Pour mettre en place des EtherChannel, on va regrouper deux interfaces de deux switches qui font partie du même stack. Par exemple, ici on va combiner l'interface fa 1/0/1 avec fa 2/0/1. Ces deux interfaces se trouvent sur des switches distincts mais qui appartiennent au même stack. Ensuite, elles sont connectées et redondantes avec l'ASA primaire.

L'avantage de cette configuration est que si un switch tombe en panne (coupure de courant, etc.), l'autre continuera à transférer les paquets sur le même ASA.

Pour configurer EtherChannel, il faut suivre ces deux étapes :

- Associer les deux interfaces au sein d'un channel-group.
- Sélectionner le protocole à utiliser sur cette interface dans le channel-group récemment créé.

LACP : le protocole de contrôle d'agrégation de lien

Le protocole LACP (Link Aggregation Control Protocol) est une norme définie par l'IEEE qui permet aux appareils de communiquer entre eux en utilisant des unités de données appelées LACPDU (Link Aggregation Control Protocol Data Units) afin de créer une connexion de regroupement de liens.

```
! choisir une interface
Sw-core(config)# interface fa 1/0/1
! Définir un numéro pour le channel-group et choisir le protocol LACP en mode active
Sw-core (config-if)# channel-group 5 mode active
! Choisir l'autre interface et le mettre dans le mettre channel-group et avec le même mode LACP (active)
Sw-core (config-if)# interface 2/0/1
Sw-core (config-if)# channel-group 5 mode active
Sw-core (config-if)# exit
```

```
sw-core(config-if)#channel-group 11 mode ?
  active      Enable LACP unconditionally
  auto        Enable PAgP only if a PAgP device is detected
  desirable   Enable PAgP unconditionally
  on          Enable Etherchannel only
  passive     Enable LACP only if a LACP device is detected
```

Pour vérifier l'état de l'EtherChannel, il faut utiliser les commandes show run et show interface EtherChannel. Ces commandes permettent de voir les paramètres et le fonctionnement de l'EtherChannel.

```
interface FastEthernet1/0/3
 channel-group 10 mode active
!
```

```
interface FastEthernet2/0/3
 channel-group 10 mode active
!
```

```
----
FastEthernet1/0/3:
Port state    = Up Sngl-port-Bndl Mstr Not-in-Bndl
Channel group = 10          Mode = Active          Gcchange = -
Port-channel  = null        GC   =   -             Pseudo port-channel = Po10
Port index    = 0           Load = 0x00            Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                          LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Fa1/0/3   SA      indep     32768         0xA       0xA     0x106       0x7D

Age of the port in the current state: 5d:07h:23m:16s
```

```
FastEthernet2/0/3:
Port state    = Up Sngl-port-Bndl Mstr Not-in-Bndl
Channel group = 10          Mode = Active          Gcchange = -
Port-channel  = null        GC   =   -             Pseudo port-channel = Po10
Port index    = 0           Load = 0x00            Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                          LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Fa2/0/3   SA      indep     32768         0xA       0xA     0x206       0x7D

Age of the port in the current state: 5d:07h:23m:19s
```

```
----
Port-channel10:Port-channel10   (Primary aggregator)

Age of the Port-channel   = 5d:07h:31m:50s
Logical slot/port   = 10/10          Number of ports = 0
HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
Protocol            =   LACP
Port security       = Disabled
```

Le reste des configurations pour les switches cœurs

Pour accomplir ce qui est demandé dans le projet, nous devons également configurer les trois VLAN 20, 30 et 40 sur la pile des commutateurs. En outre, nous devons configurer l'interface VLAN 1. Cette dernière nous permet de communiquer avec les interfaces Inside (Redundant1) des pares-feux via le VLAN 1 (VLAN par défaut).

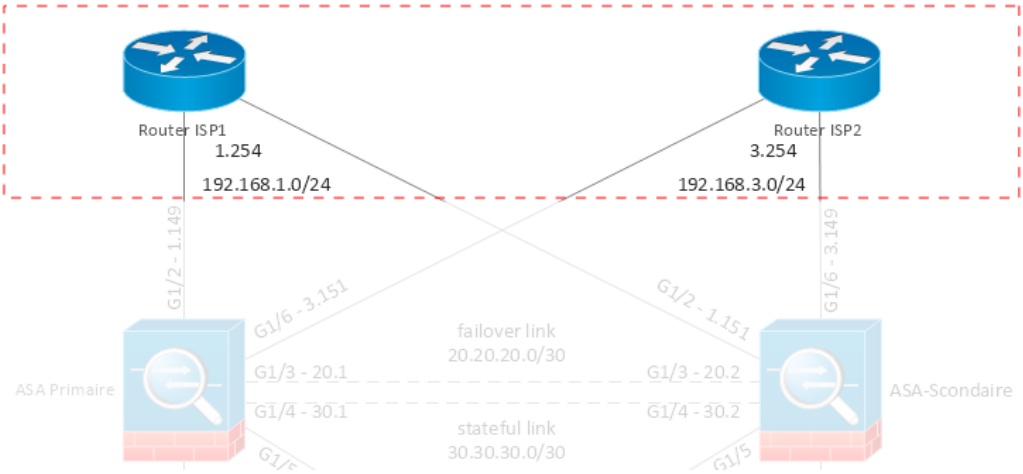
```
interface Vlan1
 ip address 10.10.10.4 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.254 255.255.255.0
 ip helper-address 192.168.40.200
!
interface Vlan30
 ip address 192.168.30.254 255.255.255.0
 ip helper-address 192.168.40.200
!
interface Vlan40
 ip address 192.168.40.254 255.255.255.0
!
```

La configuration de route par défaut est également une nécessité. Toutes les destinations qui ne sont pas connues seront envoyées vers l'adresse IP de l'interface "redundant1".

```
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.10.2
ip http server
ip http secure-server
```

TROISIEME PARTIE : LE LIEN REDONDANT VERS DEUX ROUTEURS FAI

Lorsque vous utilisez une ASA 5506x comme pare-feu, vous ne pouvez avoir qu'une seule connexion active au fournisseur d'accès à Internet (FAI). Cependant, si votre réseau a besoin de toujours être disponible, vous devrez peut-être avoir une interface de secours vers un autre FAI.



Il faut noter que les interfaces G1/2 et G1/6 ne feront pas partie d'une interface redondante sur les deux ASAs. Cela est dû au fait qu'elles sont chacune connectées à un routeur différent, ce qui les place dans des réseaux distincts. Nous avons déjà configuré ces deux interfaces dans la première partie du projet. Voici la situation actuelle de ces deux interfaces:

```
interface GigabitEthernet1/2
 nameif outside
 security-level 0
 ip address 192.168.1.149 255.255.255.0 standby 192.168.1.151
!
```

```
interface GigabitEthernet1/6
 nameif BACKUP
 security-level 0
 ip address 192.168.3.149 255.255.255.0 standby 192.168.3.151
!
```

Le lien de secours à l'aide de Static Route Tracking

Une manière de garantir la connectivité est de créer une interface de secours sur l'ASA. Le pare-feu n'utilise pas cette interface pour transférer le trafic de sortie dans des circonstances normales, mais si la liaison FAI principale échoue, la connexion devient active.

Pour s'assurer que l'on reste connecté, on peut mettre en place une interface de secours sur l'ASA (un équipement de sécurité réseau). En temps normal, le pare-feu n'utilise pas cette interface pour acheminer le trafic sortant, mais en cas de défaillance de la liaison FAI principale, cette connexion devient active et prend le relais.

Pour configurer un lien de secours, il est nécessaire d'avoir les éléments suivants :

Service Level Agreement (SLA) monitor : Le module de contrôle du contrat de niveau de service (SLA) vérifie la disponibilité du réseau externe sur le chemin du FAI principal et envoie ces informations de disponibilité au sous-système de routage.

Primary floating static : la route par défaut primaire reste active tant que le contrôleur SLA indique que le chemin est accessible. Si la connexion principale du FAI perd la connectivité externe, l'ASA supprime cette route de la table de routage.

Route par défaut secondaire : La route par défaut secondaire est une option de secours qui est utilisée lorsque la route principale n'est plus disponible. Elle a une distance administrative plus élevée, ce qui signifie qu'elle n'est activée que lorsque la route principale est absente de la table de routage grâce au moniteur SLA.

Il faut noter que la surveillance SLA continue de s'exécuter, de sorte que les routes flottantes associées peuvent revenir au système lorsque la connectivité réseau à la destination surveillée revient.

Configuration de Static Route Tracking

Les étapes de la configuration sont les suivants :

1. Configurer le SLA monitor :

```
asa(config)# sla monitor 1
asa(config-sla-monitor)# type echo protocol ipIcmpEcho 72.163.47.11 interface
outside1
asa(config-sla-monitor-echo)# frequency 120
asa(config-sla-monitor-echo)# num-packets 3
asa(config-sla-monitor-echo)# timeout 4000
asa(config-sla-monitor-echo)# exit
```

show run :

```
sla monitor 1
 type echo protocol ipIcmpEcho 8.8.8.8 interface outside
 num-packets 3
 timeout 4000
 frequency 20
sla monitor schedule 1 life forever start-time now
```

2. Commencez la surveillance de l'instance SLA configurée. Vous pouvez lancer cette surveillance à une heure précise de la journée et l'arrêter après une durée déterminée à l'avance. Dans ce cas, nous avons configuré la surveillance pour démarrer immédiatement et pour fonctionner en continu.

```
asa(config)# sla monitor schedule 1 life forever start-time now
```

3. On peut vérifier que le lien fonctionne correctement en utilisant la commande ***show sla monitor operational-state***.

```
CENTREFORM/pri/act(config)# show sla monitor  operational-state
Entry number: 1
Modification time: 15:51:18.428 France Fri Sep 2 2022
Number of Octets Used by this Entry: 2056
Number of operations attempted: 23254
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 01:02:18.429 France Thu Sep 8 2022
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

4. Dans cette étape, il faut créer une instance de suivi de route statique[1] et ensuite l'associer à l'instance de moniteur SLA[2]; utilisez les mêmes valeurs d'ID pour plus de simplicité :

```
asa(config)# track 1 rtr 1 reachability
```

show run :

```
track 1 rtr 1 reachability
```

5. Configurez la route par défaut principale et liez-la à l'instance de suivi de route. Tant que le la surveillance SLA associé indique que la connexion fonctionne, la route reste dans la table de routage.

```
asa(config)# route outside1 0.0.0.0 0.0.0.0 198.51.100.1 track 1
```

show run :

[1] Static route tracking instance
[2] SLA monitor instance

```
route outside 0.0.0.0 0.0.0.0 192.168.1.254 1 track 1
```

6. Il est essentiel d'appliquer cette étape. Après avoir déterminé l'adresse IP qui sera surveillée par le moniteur de SLA (l'adresse IP 8.8.8.8 définie à l'étape 1) et la route par défaut principale (la route à travers le routeur FAI principal défini à l'étape 5), nous devons créer une route statique vers 8.8.8.8 à travers le routeur FAI principal afin que le moniteur de SLA continue de fonctionner et que la route principal puisse être réintégré dans la table de routage lorsque la route principal est à nouveau accessible.

```
route outside 0.0.0.0 0.0.0.0 192.168.1.254 1 track 1
route BACKUP 0.0.0.0 0.0.0.0 192.168.3.254 100
route outside 8.8.8.8 255.255.255.255 192.168.1.254 1
route inside 192.168.20.0 255.255.255.0 10.10.10.4 1
route inside 192.168.30.0 255.255.255.0 10.10.10.4 1
route inside 192.168.40.0 255.255.255.0 10.10.10.4 1
```

7. Pour mettre en place une route de secours, il faut la configurer avec une métrique plus élevée, ce qui signifie qu'elle sera moins prioritaire que la route principale. La valeur par défaut de la métrique pour les routes statiques est 1, donc il faut la définir sur une valeur supérieure pour donner la priorité à la route principale.

```
asa(config)# route outside2 0.0.0.0 0.0.0.0 203.0.113.1 100
```

show run :

```
route BACKUP 0.0.0.0 0.0.0.0 192.168.3.254 100
```

Pour éviter que les connexions existantes ne continuent à être utilisées lorsque l'une des routes associées est basculée vers une autre interface, il est important de configurer ces connexions pour qu'elles expirent 30 secondes après le basculement. Cela permettra de garantir une transition en douceur et de minimiser les perturbations pour les utilisateurs.

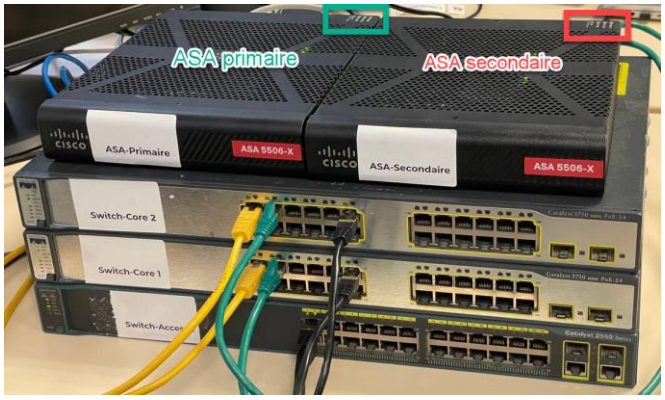
```
asa(config)# timeout floating-conn 0:0:30
```

show run :

```
timeout floating-conn 0:00:30
```

QUATRIEME PARTIE : VALIDATION

Dans cette partie nous allons procéder aux quelques tests de validation pour valider le bon fonctionnement de notre infrastructure.



Les voyants sur le boitier ASA

Le boîtier ASA a trois voyants Power, Status et Active et chacun peut avoir des couleur verte, rouge et jaune. Le voyant Active est celui qui nous intéresse le plus.. Il est utile de connaître la signification des voyants des ports réseau, qui se trouvent dans le tableau ci-dessous.

	Voyant	Description
1	Active	**État de la paire de basculement :** - **Vert fixe – La paire de basculement fonctionne normalement. La LED est verte toujours à moins que l'ASA dans une paire HA.** - **Orange – Lorsque l'ASA est dans une paire HA, le voyant est orange pour l'unité de secours.** - **Éteint – Le basculement n'est pas opérationnel.**
2	état des ports réseau	**Sur le panneau arrière, une paire de LED (état du lien et état de la connexion) pour chaque des huit ports réseau Gigabit Ethernet** **État du lien (L) :** - **Éteint – Aucune liaison ou port non utilisé.** - **Vert continu – Lien établi.** - **Vert clignotant – Activité de liaison.**

Situation actuelle du failover

Nous allons d'abord utiliser différentes commandes pour vérifier comment la failover fonctionne actuellement.

Niveau des appareil : La commande "show failover state" nous indique que l'ASA primaire est actuellement en mode actif (comme on peut le voir sur la capture d'écran ci-dessus).

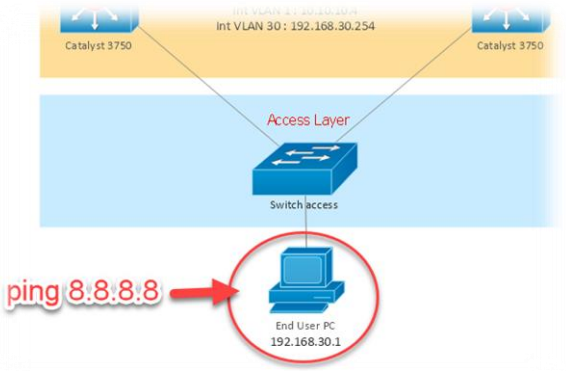
```
CENTREFORM/pri/act(config)# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure            02:02:43 France Jan 1 2014

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

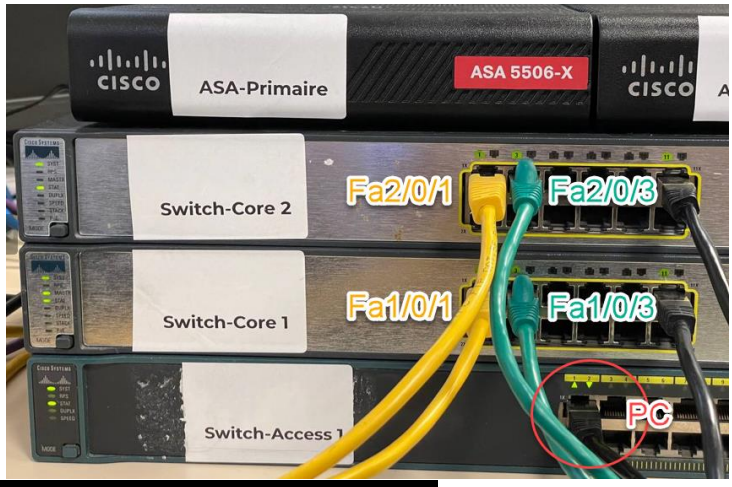
Niveau des interfaces : En utilisant la commande "show interface redundant 1", nous pouvons voir que l'interface G1/1 est active sur le ASA principal/actif. De plus, l'image ci-dessus montre que les deux interfaces sont connectées (voyant **L** vert sur les câbles jaunes).

```
  Redundancy Information:
        Member GigabitEthernet1/1(Active), GigabitEthernet1/5
        Last switchover at 09:53:47 France Sep 8 2022
```

Test du failover aux niveaux des interfaces et des appareils

Dans cette étape, nous allons effectuer un ping en continu sur un ordinateur qui se trouve dans le VLAN 30. Cet ordinateur est connecté à un switch Access et doit être capable d'accéder à Internet via un switch cœur 1 ou 2 et une passerelle ASA Primaire ou Secondaire grâce à une configuration de redondance au niveau du cœur et des pares-feux.






```
Carte Ethernet vEthernet (NIC1- Externe) :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . . : 192.168.30.1
   Masque de sous-réseau. . . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . . : 192.168.30.254

C:\Users\ershad>

C:\Users\ershad>ping 8.8.8.8 -t

Envoi d'une requête 'Ping'  8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=69 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=63 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=65 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=63 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=64 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=28 ms TTL=116
```

Couper le lien Fa1/0/1

Selon la situation actuelle dans la dernière étape, la connexion passe par l'interface G1/1 qui est connectée à l'interface Fa1/0/1 sur le switch cœur 1. Nous allons donc couper le lien Fa1/0/1. Nous voyons immédiatement que l'interface Fa2/0/1, qui est en LACP avec l'interface 1/0/1 et qui sont toutes les deux branchées sur l'interface redundant1 (sur le ASA primaire), devient active.

```
sw-core#
Sep  8 10:15:09.866: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/1, changed state to down
Sep  8 10:15:10.865: %LINK-3-UPDOWN: Interface FastEthernet1/0/1, changed state to down
sw-core#
sw-core#
sw-core#
Sep  8 10:15:22.055: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0/1, changed state to up
sw-core#
```

La commande show interface redundant 1 montre que l'interface active a été transférée de G1/1 à G1/5.

```
  Redundancy Information:
        Member GigabitEthernet1/5(Active), GigabitEthernet1/1
        Last switchover at 10:14:40 France Sep 8 2022
```

Avec cette fonction de secours au niveau des interfaces, le ping n'a perdu qu'un paquet, mais il continue à fonctionner normalement :

```
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=15 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=27 ms TTL=116
Délai d'attente de la demande dépassé.
Réponse de 8.8.8.8 : octets=32 temps=34 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=22 ms TTL=116
```

L'ASA est constamment en fonctionnement actif. Le test montre que la failover des interfaces a empêché tout basculement inutile sur les appareils :

```
CENTREFORM/pri/act(config)# sh failover state

               State          Last Failure Reason      Date/Time
This host   -  Primary
               Active         None
Other host  -  Secondary
               Standby Ready  Comm Failure             02:02:43 France Jan 1 2014
```

Couper le lien Fa2/0/1

Puis, nous allons couper le deuxième lien du EtherChannel, qui se trouve sur l'interface Fa2/0/1. Cette interface est connectée sur G1/5 sur l'ASA principal. Ce lien deviendra inactif et provoquera un basculement des appareils, car il n'y a plus aucune connexion depuis l'interface redundant1 de l'ASA primaire.

```
Sep  8 10:22:46.701: %LINK-3-UPDOWN: Interface FastEthernet1/0/1, changed state to down
Sep  8 10:23:21.380: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0/1, changed state to down
Sep  8 10:23:22.387: %LINK-3-UPDOWN: Interface FastEthernet2/0/1, changed state to down
sw-core#
sw-core#
```

```
CENTREFORM/pri/stby(config)# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Failed         Ifc Failure              10:22:56 France Sep 8 2022
                              inside: No Link
Other host -   Secondary
               Active         Comm Failure             02:02:43 France Jan 1 2014
```

En surveillant constamment le ping sur notre ordinateur, nous constaterons que le ping fonctionne toujours avec juste une perte de paquet :

```
Réponse de 8.8.8.8 : octets=32 temps=43 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=47 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=37 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=15 ms TTL=116
Délai d'attente de la demande dépassé.
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=15 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=17 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
```

Rebrancher l'interface Fa2/0/1

En reconnectant l'interface Fa2/0/1, l'ASA primaire revient à un état normal selon le message affiché sur la ligne de commande. Cependant, il reste en mode veille. Cela montre que l'ASA en mode veille ne redeviendra pas actif à moins qu'il y ait un problème avec l'ASA actif actuel.

```
sw-core#
Sep  8 10:27:16.202: %LINK-3-UPDOWN: Interface FastEthernet2/0/1, changed state to up
sw-core#
sw-core#
```

```
CENTREFORM/pri/stby(config)#  Primary: Switching to Ok for reason Interface check.
Primary: Switching to Ok for reason Interface check.
Primary: Switching to Ok for reason Interface check.
```

```
Last Failover at: 10:22:56 France Sep 8 2022
        This host: Primary - Standby Ready
                Active time: 173 (sec)
                slot 1: ASA5506 hw/sw rev (2.0/9.6(1)) status (Up Sys)
                  Interface outside (192.168.1.151): Normal (Monitored)
                  Interface BACKUP (192.168.3.151): Normal (Monitored)
                  Interface inside (10.10.10.3): Normal (Waiting)
                slot 2: SFR5506 hw/sw rev (N/A/6.2.2.4-34) status (Up/Up)
                  ASA FirePOWER, 6.2.2.4-34, Up, (Monitored)
        Other host: Secondary - Active
                Active time: 329 (sec)
                slot 1: ASA5506 hw/sw rev (2.0/9.6(1)) status (Up Sys)
                  Interface outside (192.168.1.149): Normal (Monitored)
                  Interface BACKUP (192.168.3.149): Normal (Monitored)
                  Interface inside (10.10.10.2): Normal (Waiting)
                slot 2: SFR5506 hw/sw rev (N/A/6.2.2.4-34) status (Up/Up)
                  ASA FirePOWER, 6.2.2.4-34, Up, (Monitored)
```

Le nouvel état de l'interface redundant1 sur l'ASA primaire :

```
Redundancy Information:
      Member GigabitEthernet1/5(Active)  GigabitEthernet1/1
      Last switchover at 10:22:16 France Sep 8 2022
```

Maintenant que l'ASA secondaire est actif, nous allons vérifier l'état de l'interface redundant1 sur ce dispositif :

```
    5 minute drop rate, 0 pkts/sec
  Redundancy Information:
      Member GigabitEthernet1/1(Active)  GigabitEthernet1/5
      Last switchover at 11:21:07 France Sep 8 2022
```

Couper le lien Fa2/0/3

Dans la dernière image qui montre l'interface redundant1 sur l'ASA secondaire, nous voyons que G1/1 est active. Nous allons déconnecter l'autre côté de ce lien sur le switch cœur 2 et l'interface active passera à G1/5. Cependant, comme prévu, le basculement des appareils ne se produit pas.

```
sw-core#
sw-core#
Sep  8 11:28:40.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/3, changed state to up
Sep  8 11:28:40.538: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0/3, changed state to down
Sep  8 11:28:41.544: %LINK-3-UPDOWN: Interface FastEthernet2/0/3, changed state to down
sw-core#
```

```
  Redundancy Information:
      Member GigabitEthernet1/5(Active), GigabitEthernet1/1
      Last switchover at 11:28:10 France Sep 8 2022
```

```
CENTREFORM/pri/stby(config)# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Standby Ready  Ifc Failure              10:27:47 France Sep 8 2022
                              inside: Failed
Other host -   Secondary
               Active         Ifc Failure              11:21:13 France Sep 8 2022
                              inside: Failed
```

Il y a eu une petite perte de paquets lors de l'utilisation de la fonction ping, mais la connexion internet n'a pas été coupée.

```
Réponse de 8.8.8.8 : octets=32 temps=15 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Réponse de 8.8.8.8 : octets=32 temps=20 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
```

Couper le Fa1/0/3

Nous allons couper la deuxième interface dans cette redundant1 et le failover se produit :

```
sw-core#
sw-core#
sw-core#
Sep  8 11:33:02.472: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/3, changed state to down
Sep  8 11:33:03.470: %LINK-3-UPDOWN: Interface FastEthernet1/0/3, changed state to down
sw-core#
sw-core#
sw-core#
```

```
CENTREFORM/pri/stby(config)#
CENTREFORM/pri/stby(config)#
        Switching to Active

CENTREFORM/pri/act(config)#
CENTREFORM/pri/act(config)#
```

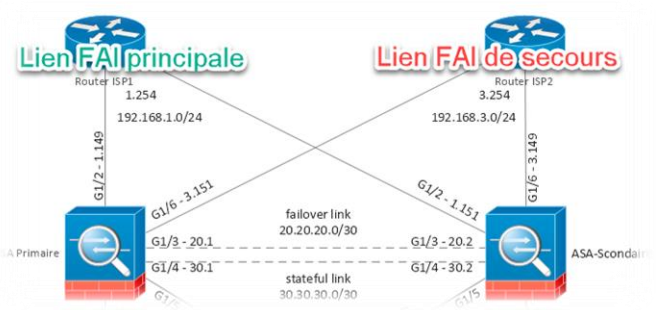
```
CENTREFORM/pri/act(config)# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         Ifc Failure              10:27:47 France Sep 8 2022
                              inside: Failed
Other host -   Secondary
               Failed         Ifc Failure              11:32:37 France Sep 8 2022
                              inside: No Link
```

Le ping continue toujours :

```
Réponse de 8.8.8.8 : octets=32 temps=15 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Délai d'attente de la demande dépassé.
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=17 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
```

Test du lien de secours vers la deuxième routeur FAI

Nous allons vérifier comment le Static Route Tracking fonctionne et comment la route par défaut sera modifiée lorsque la route principale ne fonctionne plus et qu'elle est remplacée par la route de secours.



Au début de notre essai, l'ASA principale est en mode actif et sa table de routage indique que sa passerelle actuelle (gateway of last resort) est 192.168.1.254 (la routeur FAI principale). En plus la commande *debug sla monitor trace* nous indique que cette route est en train d'être surveillé sans problème :

```
Gateway of last resort is 192.168.1.254 to network 0.0.0.0

S*        0.0.0.0 0.0.0.0 [1/0] via 192.168.1.254, outside
S         8.8.8.8 255.255.255.255 [1/0] via 192.168.1.254, outside
C         10.10.10.0 255.255.255.0 is directly connected, inside
L         10.10.10.2 255.255.255.255 is directly connected, inside
C         20.20.20.0 255.255.255.252 is directly connected, MONFAILOVER
L         20.20.20.1 255.255.255.255 is directly connected, MONFAILOVER
C         30.30.30.0 255.255.255.252 is directly connected, STATEFULLINK
L         30.30.30.1 255.255.255.255 is directly connected, STATEFULLINK
C         192.168.1.0 255.255.255.0 is directly connected, outside
L         192.168.1.149 255.255.255.255 is directly connected, outside
C         192.168.3.0 255.255.255.0 is directly connected, BACKUP
L         192.168.3.149 255.255.255.255 is directly connected, BACKUP
S         192.168.20.0 255.255.255.0 [1/0] via 10.10.10.4, inside
S         192.168.30.0 255.255.255.0 [1/0] via 10.10.10.4, inside
S         192.168.40.0 255.255.255.0 [1/0] via 10.10.10.4, inside
```

```
  <cr>
CENTREFORM/pri/act(config)# debug sla monitor trace
IP SLA Monitor TRACE debugging for all operations is on
CENTREFORM/pri/act(config)# IP SLA Monitor(1) Scheduler: Starting an operation
IP SLA Monitor(1) echo operation: Sending an echo operation
IP SLA Monitor(1) echo operation: RTT=2 OK
IP SLA Monitor(1) echo operation: RTT=5 OK
IP SLA Monitor(1) echo operation: RTT=7 OK
IP SLA Monitor(1) echo operation: RTT=10 OK
IP SLA Monitor(1) Scheduler: Updating result
IP SLA Monitor(1) Scheduler: Starting an operation
IP SLA Monitor(1) echo operation: Sending an echo operation
IP SLA Monitor(1) echo operation: RTT=2 OK
IP SLA Monitor(1) echo operation: RTT=5 OK
IP SLA Monitor(1) echo operation: RTT=7 OK
IP SLA Monitor(1) echo operation: RTT=10 OK
IP SLA Monitor(1) Scheduler: Updating result
sh route
```

Puis, nous allons couper l'accès principal en déconnectant le G1/2. Nous constatons que le sla monitor ne peut plus suivre la route par défaut. Ainsi, l'ASA supprime cette route de la table de routage et ajoute la route de secours.

```
CENTREFORM/pri/act(config)#  IP SLA Monitor(
IP SLA Monitor(1) echo operation: Sending ar
IP SLA Monitor(1) echo operation: Timeout
IP SLA Monitor(1) echo operation: Timeout
IP SLA Monitor(1) echo operation: Timeout
IP SLA Monitor(1) echo operation: Timeout
IP SLA Monitor(1) Scheduler: Updating result
IP SLA Monitor(1) Scheduler: Starting an ope
IP SLA Monitor(1) echo operation: Sending ar
IP SLA Monitor(1) echo operation: Timeout
IP SLA Monitor(1) echo operation: Timeout
IP SLA Monitor(1) echo operation: Timeout
IP SLA Monitor(1) echo operation: Timeout
IP SLA Monitor(1) Scheduler: Updating result
sh ruote
```

```
of last resort is 192.168.3.254 to network 0.0.0.0

0.0.0.0 0.0.0.0 [100/0] via 192.168.3.254, BACKUP
10.10.10.0 255.255.255.0 is directly connected, inside
10.10.10.2 255.255.255.255 is directly connected, inside
20.20.20.0 255.255.255.252 is directly connected, MONFAILOVER
20.20.20.1 255.255.255.255 is directly connected, MONFAILOVER
30.30.30.0 255.255.255.252 is directly connected, STATEFULLINK
30.30.30.1 255.255.255.255 is directly connected, STATEFULLINK
192.168.3.0 255.255.255.0 is
192.168.3.149 255.255.255.25
192.168.20.0 255.255.255.0 [1/0]
192.168.30.0 255.255.255.0 [1/0] via 10.10.10.4, inside
192.168.40.0 255.255.255.0 [1/0] via 10.10.10.4, inside
```

la route 8.8.8.8 n'est pas dans la table de routage non plus

Ensuite, nous allons reconnecter la route principale en reconnectant l'interface G1/2. Le moniteur de SLA fonctionne à nouveau et la route principale est de retour dans la table de routage.

```
IP SLA Monitor(1) echo operation: Sending an echo operation
IP SLA Monitor(1) echo operation: RTT=2 OK
IP SLA Monitor(1) echo operation: RTT=5 OK
IP SLA Monitor(1) echo operation: RTT=7 OK
IP SLA Monitor(1) echo operation: RTT=10 OK
IP SLA Monitor(1) Scheduler: Updating result

CENTREFORM/pri/act(config)# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 192.168.1.254 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.1.254, outside
S        8.8.8.8 255.255.255.255 [1/0] via 192.168.1.254, outside
C          10.10.10.0 255.255.255.0 is directly connected, inside
L          10.10.10.2 255.255.255.255 is directly connected, inside
C          20.20.20.0 255.255.255.252 is directly connected, MONFAILOVER
L          20.20.20.1 255.255.255.255 is directly connected, MONFAILOVER
C          30.30.30.0 255.255.255.252 is directly connected, STATEFULLINK
L          30.30.30.1 255.255.255.255 is directly connected, STATEFULLINK
C          192.168.1.0 255.255.255.0 is directly connected, outside
```

Test du failover coté WAN

Nous allons tester la bon fonctionnement du failover sur le coté WAN des ASAs (G1/2 et G1/6).

Pour cela nous allons au d'début vérifier l'état de failover. L'ASA primaire est actif :

```
CENTREFORM/pri/act(config)# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         Ifc Failure              15:27:32 France Sep 8 2022
                              outside: No Link
                              BACKUP: No Link
Other host -   Secondary
               Standby Ready  Ifc Failure              11:58:21 France Sep 8 2022
                              BACKUP: No Link
```

Ensuite, nous allons déconnecter le G1/2 qui est le lien vers le routeur principal du FAI (192.168.1.254). Cela entraînera une perte de connexion, mais le lien vers le routeur de secours sera toujours actif. Ainsi, la bascule ne se produira pas et le ping sur l'ordinateur de test fonctionnera toujours.

```
Last Failover at: 15:28:47 France Sep 8 2022
        This host: Primary - Active
                Active time: 1336 (sec)
                slot 1: ASA5506 hw/sw rev (2.0/9.6(1)) status (Up Sys)
                  Interface outside (192.168.1.149): No Link (Monitored)
                  Interface BACKUP (192.168.3.149): Normal (Monitored)
                  Interface inside (10.10.10.2): Normal (Monitored)
                slot 2: SFR5506 hw/sw rev (N/A/6.2.2.4-34) status (Up/Up)
                  ASA FirePOWER, 6.2.2.4-34, Up, (Monitored)
        Other host: Secondary - Standby Ready
                Active time: 75 (sec)
                slot 1: ASA5506 hw/sw rev (2.0/9.6(1)) status (Up Sys)
                  Interface outside (192.168.1.151): Normal (Monitored)
                  Interface BACKUP (192.168.3.151): Normal (Monitored)
                  Interface inside (10.10.10.3): Normal (Monitored)
                slot 2: SFR5506 hw/sw rev (N/A/6.2.2.4-34) status (Up/Up)
                  ASA FirePOWER, 6.2.2.4-34, Up, (Monitored)
```

```
Réponse de 8.8.8.8 : octets=32 temps=17 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=15 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=116
```

Ensuite nous allons couper le deuxième lien. Le basculement au niveau des appareil se produit car tous les deux liens sont plus disponible :

```
Serial Number: Ours JAD211207KK, Mate JAD21130JJ8
Last Failover at: 15:52:44 France Sep 8 2022
        This host: Primary - Failed
                Active time: 1437 (sec)
                slot 1: ASA5506 hw/sw rev (2.0/9.6(1)) status (Up Sys)
                  Interface outside (192.168.1.151): No Link (Waiting)
                  Interface BACKUP (192.168.3.151): No Link (Waiting)
                  Interface inside (10.10.10.3): Normal (Waiting)
                slot 2: SFR5506 hw/sw rev (N/A/6.2.2.4-34) status (Up/Up)
                  ASA FirePOWER, 6.2.2.4-34, Up, (Monitored)
        Other host: Secondary - Active
                Active time: 15 (sec)
                slot 1: ASA5506 hw/sw rev (2.0/9.6(1)) status (Up Sys)
                  Interface outside (192.168.1.149): Normal (Waiting)
                  Interface BACKUP (192.168.3.149): Normal (Waiting)
```

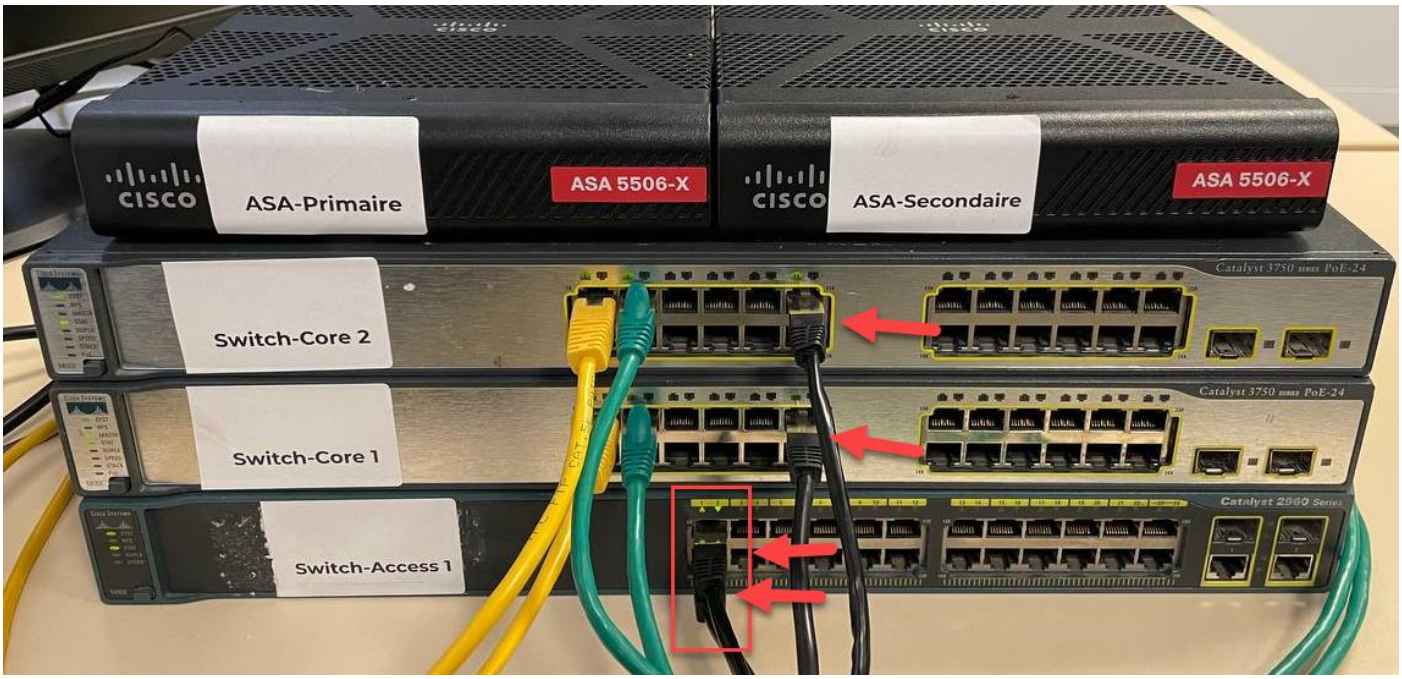
```
CENTREFORM/pri/stby(config)# sh failover state

               State          Last Failure Reason      Date/Time
This host   -  Primary
               Failed         Ifc Failure              15:52:44 France Sep 8 2022
                              outside: No Link
                              BACKUP: No Link

Other host  -  Secondary
               Active         Ifc Failure              11:58:21 France Sep 8 2022
                              BACKUP: No Link
```

Nous allons rebrancher tous les deux liens G1/2 et G1/6. Le primaire est à nouveau disponible mais il reste sur le mode standby :

```
        Mac set

CENTREFORM/pri/stby(config)# Primary: Switching to Ok for reason Interface check.
```

Redondance des switches niveau accès

Notre infrastructure comprend un switch d'accès redondant qui est connecté aux switches cœur 1 et 2.



Il existe également l'option d'utiliser deux liens LACP vers chaque switch cœur pour encore plus de fiabilité (au niveau des interfaces) et pour agréger les liens. Dans ce cas, si un switch cœur tombe en panne ou s'éteint, l'autre switch cœur assurera la connectivité au switch d'accès.

END