Pulse Secure
Guide de mise à niveau matérielle : gamme SA/MAG vers PSA

Edité par Gesner et Sam pour faire correspondre les informations avec l'infrastructure de test.

Applicable à :
Pulse Connect Secure
Pulse Policy Secure

Date de publication : avril 2017

Pulse Secure LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134
États-Unis
+1 408-372-9600
www.pulsesecure.net

Guide de mise à niveau matérielle Pulse Secure : gamme SA/MAG vers PSA

Table des matières

PRÉSENTATION

Ce document présente les procédures à suivre pour la mise à niveau des anciennes plates-formes Secure Access et MAG vers les nouvelles plates-formes matérielles PSA, dont les configurations sources correspondent à des dispositifs autonomes ou à des clusters de deux nœuds ou plus.

Afin de procéder au transfert des configurations et des paramètres, il est recommandé d'exporter les configurations binaires et XML sélectives depuis l'ancien dispositif, puis de les importer vers le nouveau. En suivant les étapes présentées dans ce document, vous assurerez la migration réussie de vos configurations vers les dispositifs PSA nouvelle génération.

Notez que la migration IVS n'est pas directement prise en charge depuis les dispositifs Pulse Connect Secure SA vers le nouveau matériel, mais qu'elle doit faire l'objet d'une migration individuelle (manuelle) afin d'obtenir un IVS racine qui pourra ensuite être transféré vers les nouveaux dispositifs. Le présent document n'aborde pas cette procédure.

PRÉPARATION À LA MISE À NIVEAU

Les éléments nécessaires à la préparation de la migration sont présentés ci-dessous :

1. **Évaluation du site :** mettez en place un système de refroidissement et de ventilation adapté, et assurez-vous que le réseau entre les nœuds destinés à être mis en cluster bénéficie d'une connexion LAN à haut débit et à faible latence.

   (Voir https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB26035.)

   Matériel : veillez à ce qu'il ne manque aucun composant ni élément (châssis, câbles, connecteurs et kits de montage en rack).

   Licences : les licences requises doivent être générées et distribuées, qu'il soit nécessaire ou non d'effectuer une configuration en tant que membre d'un environnement Serveur de Licences Enterprise.

2. **Logiciels :** les dispositifs PSA sont fournis avec les versions d'usine 8.1R4.1 ou C5.2R2.1, ce qui détermine la version du logiciel qui sera ensuite utilisée pour les nouveaux dispositifs et les mises à niveau. Les dispositifs PSA nouvelle génération ne prennent pas en charge le retour vers des versions logicielles antérieures à la version par défaut.

3. **Sauvegarde de configuration :** il est recommandé de réaliser une sauvegarde des fichiers binaires « system.cfg » et « user.cfg » en même temps que l'exportation de **tous les paramètres réseau** et de **tous les rôles** juste avant de procéder à la migration. Le fichier « ivs.cfg » (en cas de mise à niveau depuis une plate-forme SAx500) n'est pas pris en charge par les dispositifs PSA et ne pourra donc pas être utilisé pour ces derniers. Sauvegardez-le toutefois pour toute conversion IVS manuelle ultérieure (procédure non abordée dans ce document).

4. **Configuration :** nous vous recommandons de consigner les paramètres locaux repris en grande partie dans le fichier « system.cfg », car certains d'entre eux devront être à nouveau saisis manuellement pour le ou les dispositifs PSA (configuration des clusters, par exemple). Pour les clusters de type A/A, vérifiez le filtre d'adresse IP sous **Réseau > Tunnel VPN > Filtre d'adresse IP (Network > VPN Tunneling > IP address filter)**, ainsi que les **paramètres du pool d'adresses IP (IP pool settings)** du profil du tunnel VPN. Certains paramètres tels que les protocoles SNMP et Syslog, et les paramètres de journal, peuvent par ailleurs être configurés en mode cluster ou pour des nœuds individuels.

REMARQUES :

1. Lors de la conversion d'un cluster, tous les dispositifs PSA concernés doivent présenter la même version et la même build, ainsi que les mêmes plates-formes matérielles, par exemple : PSA300 / PSA3000 / PSA5000 / PSA7000c / PSA7000f.

2. Lors de la conversion d'un cluster, assurez-vous d'utiliser le même nom de cluster et les mêmes définitions de port avant d'importer les fichiers XML. Dans le cas contraire, l'importation se soldera par un échec. Cela s'applique notamment à l'activation des ports externes, au nom du cluster et aux noms des nœuds.
3. Lors du passage de n'importe quelle plate-forme vers une plate-forme PSA7000f ou PSA7000c, l'importation au format XML des paramètres réseau risque d'échouer en raison de différences d'interface réseau. Assurez-vous donc de modifier le fichier XML en définissant les paramètres de port sur « **auto** » *(en minuscules, sans guillemets)*.
4. Lors du passage d'une plate-forme équipée d'un port de gestion vers une plate-forme qui en est dénuée, supprimez la section **<Management-Port>** du fichier XML avant de l'importer.
5. Si vous utilisez des serveurs d'authentification Active Directory (AD) ou ACE, il peut être nécessaire de créer à nouveau des objets ordinateurs AD pour les nouveaux dispositifs PSA ou pour les ACE, afin de générer / d'importer à nouveau le fichier **SDCONF.REC** vers les dispositifs si l'authentification échoue après l'importation.
6. Dans la cadre de cette migration, on considère que les nouveaux dispositifs PSA seront installés sur les réseaux utilisés pour les dispositifs SA/MAG qu'ils viennent remplacer.

PROCÉDURE DÉTAILLÉE

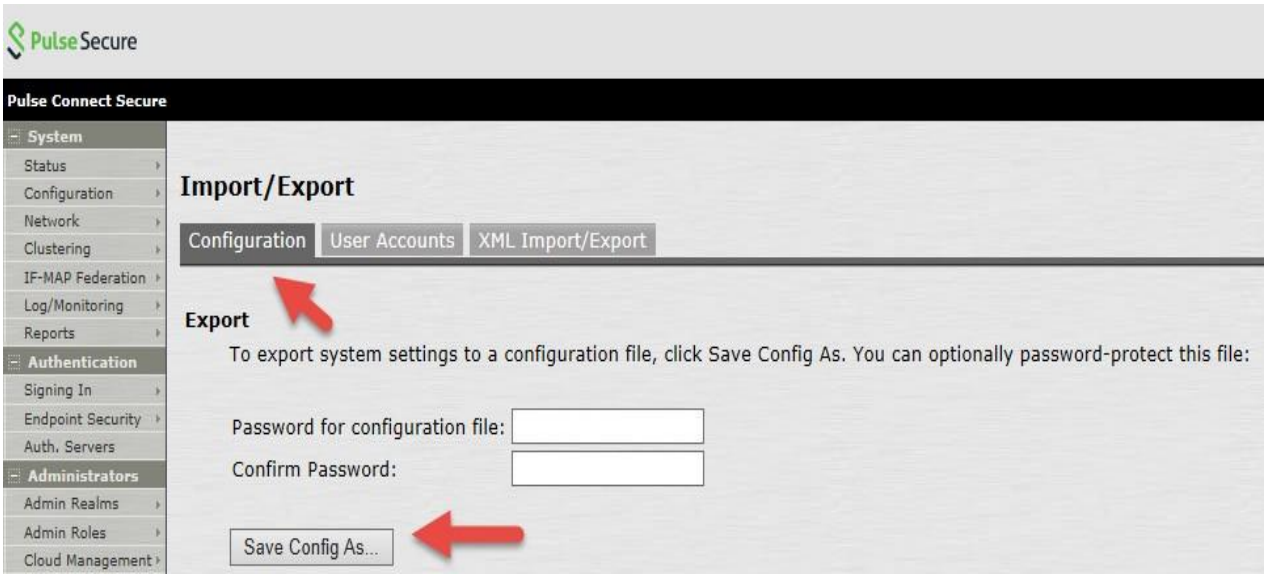
La procédure ci-dessous s'applique à la fois aux migrations pour dispositifs autonomes et en cluster. Les principales étapes complémentaires aux configurations de mise en cluster éventuellement nécessaires sont : la mise en correspondance des certificats et des ports, la configuration du client de gestion des licences en cas d'utilisation d'un serveur de licences Enterprise, la vérification des paramètres SNMP, la vérification et la configuration des profils VPN, le contrôle du transfert des configurations, et l'ajout et la correction manuels de différences, le cas échéant.

Étapes de la migration :

1. Sur la plate-forme SA/MAG existante, connectez-vous sur le dispositif autonome ou sur le premier nœud du cluster (nœud initial de formation du cluster), puis exportez ses configurations binaires (« **system.cfg** » et « **user.cfg** »), ainsi que les configurations XML des paramètres réseau.

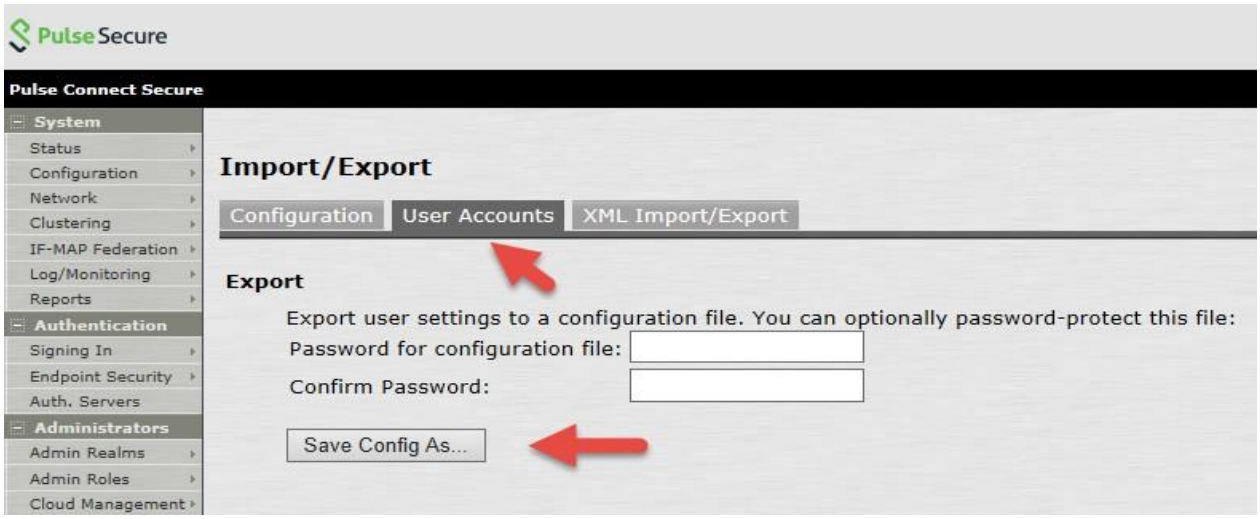
   Pour exporter les configurations binaires depuis un dispositif SA :

   a. Dans la console d'administration, sélectionnez **Maintenance** > **Importer/Exporter** > **Configuration (Maintenance > Import/Export > Configuration)**.
   b. Sous **Exporter (Export)**, définissez un mot de passe si vous souhaitez protéger le fichier de configuration.
   c. Cliquez sur **Enregistrer la configuration sous (Save Config As)** pour enregistrer le fichier. Le nom par défaut du fichier sera « **system.cfg** ».



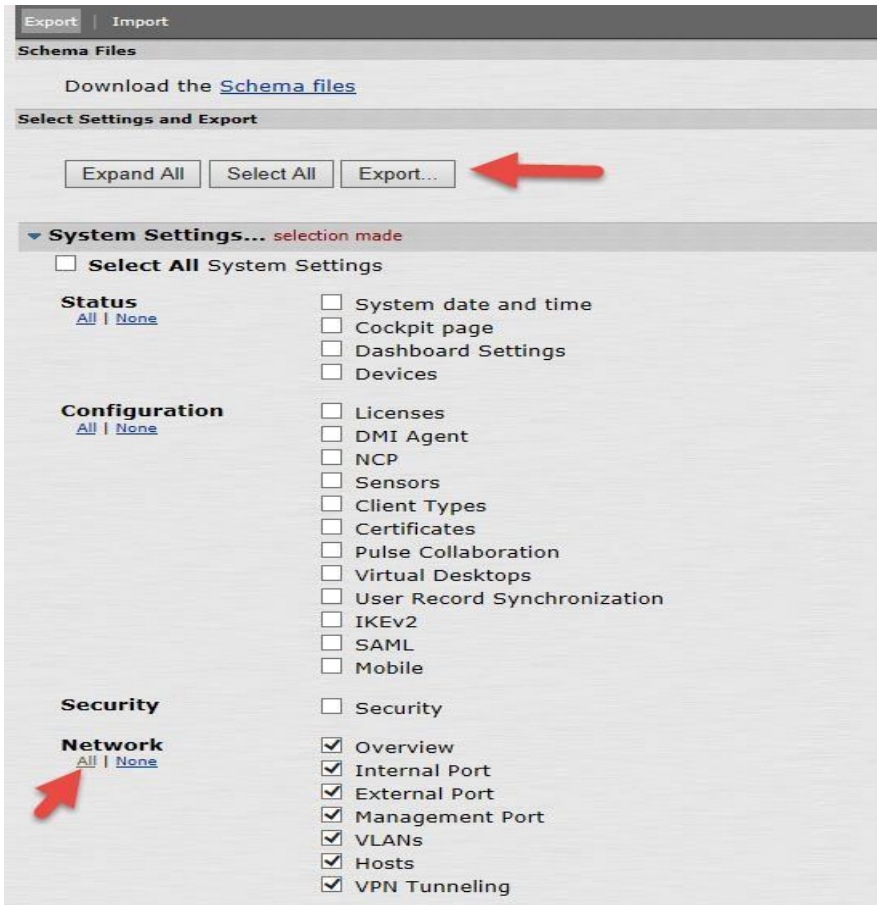
   d. Dans la console d'administration, sélectionnez **Maintenance** > **Importer/Exporter** > **Comptes utilisateur (Maintenance > Import/Export > User Accounts)**.
   e. Sous **Exporter (Export)**, définissez un mot de passe si vous souhaitez protéger le fichier de configuration.

f. Cliquez sur **Enregistrer la configuration sous (Save Config As)** pour enregistrer le fichier. Le nom par défaut du fichier sera « **user.cfg** ».

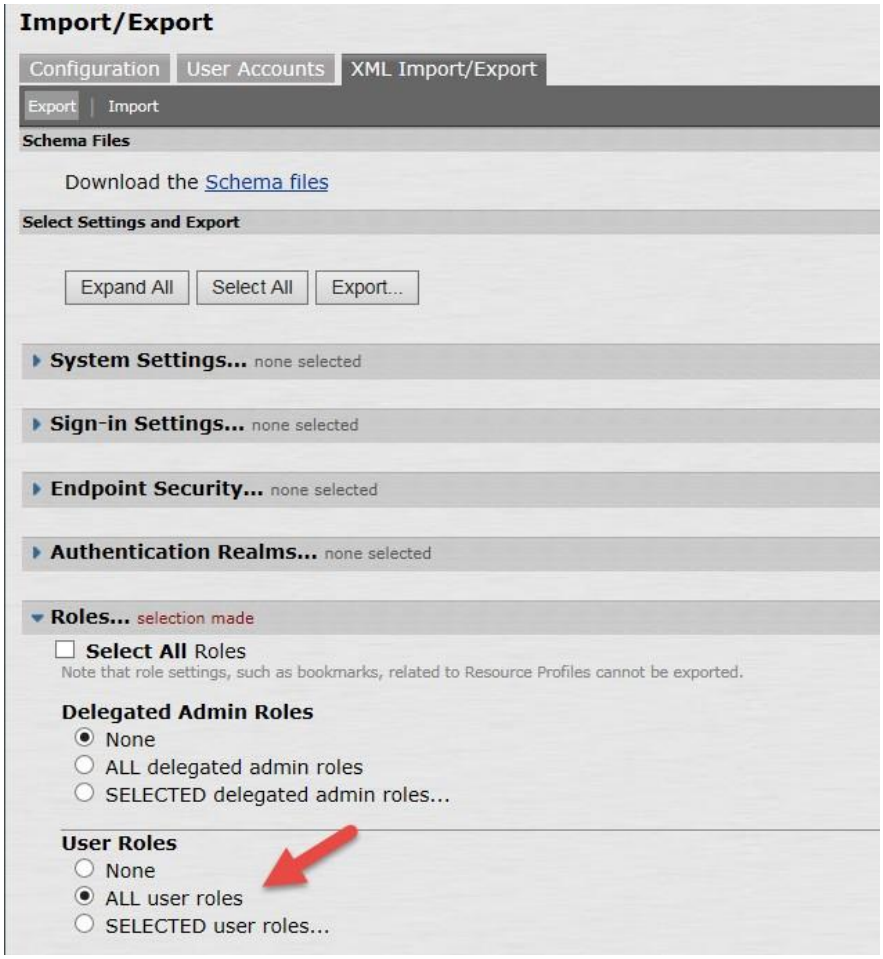


Pour exporter les configurations XML depuis un dispositif SA :

a. Dans la console d'administration, sélectionnez **Maintenance** > **Importer/Exporter** > **Exporter XML (Maintenance > Import/Export > Export XML)**.
b. Sous **Exporter (Export)**, développez **Paramètres système (System Settings)** et sélectionnez **Réseau** > **Tous (Network > All)**.
c. Cliquez sur **Exporter (Export)** et enregistrez le fichier XML.



d. Sous Exporter, développez **Rôles (Roles)** et sélectionnez **Tous les rôles utilisateur (All user roles)**.

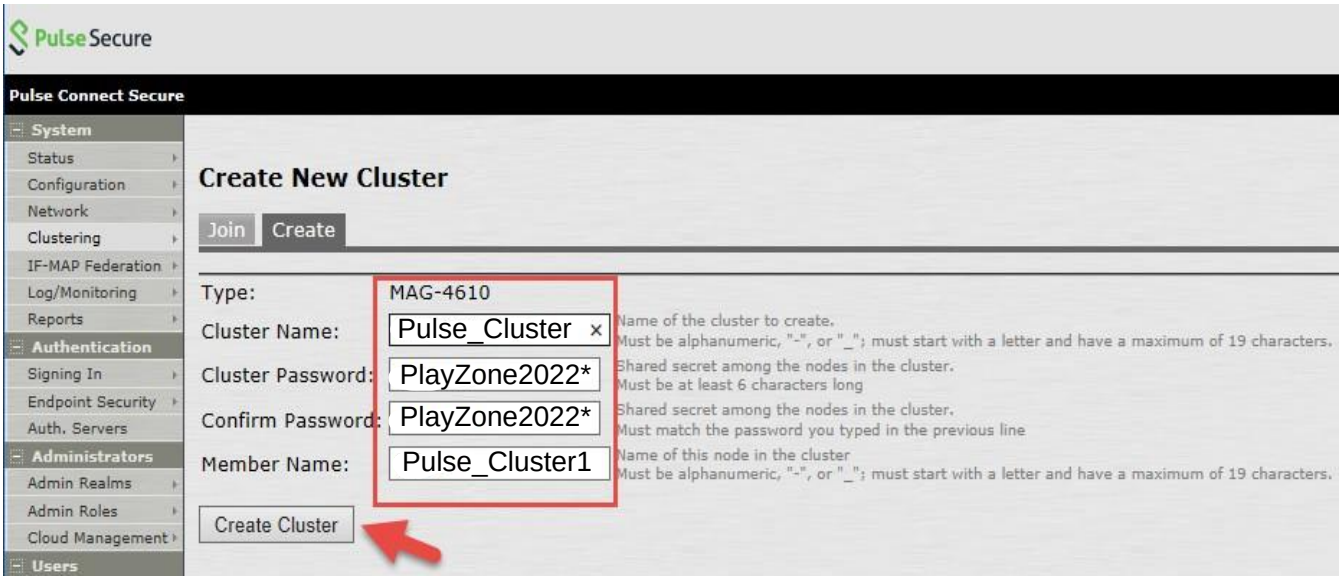


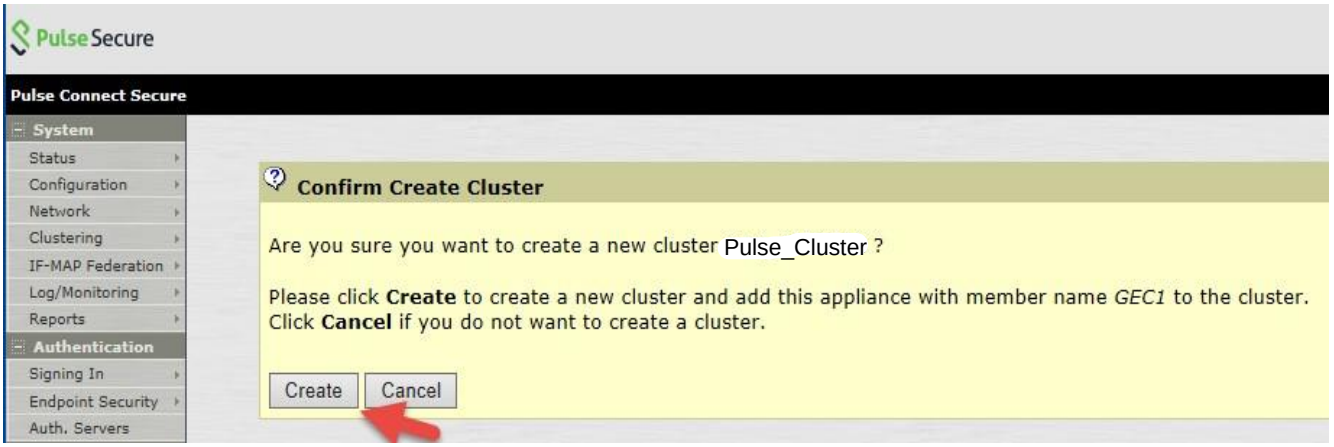
e. Cliquez sur **Exporter (Export)** et enregistrez le fichier XML.

2. Notez tous les paramètres locaux pour les deux nœuds (si cela n'a pas été fait au cours de la phase de préparation) : **informations IP, mise en cluster, ports virtuels, réseaux VLAN, hôtes, routes, paramètres DNS, protocoles SNMP (s'ils sont configurés), paramètres de journalisation / Syslog.**
3. Mettez hors tension les anciens dispositifs autonomes ou en cluster.
4. Configurez les nouveaux dispositifs PSA de sorte à leur attribuer les mêmes ports internes, externes et de gestion, les mêmes adresses IP que les anciens dispositifs et les paramètres DNS appropriés. Ne configurez aucun autre paramètre pour le moment.
5. Appliquez les licences adaptées aux nouveaux dispositifs PSA. Si le dispositif SA/MAG est lié à un serveur de licences Enterprise, vous devez recréer manuellement le client, puis le reconnecter au serveur de licences **une fois la migration effectuée**.

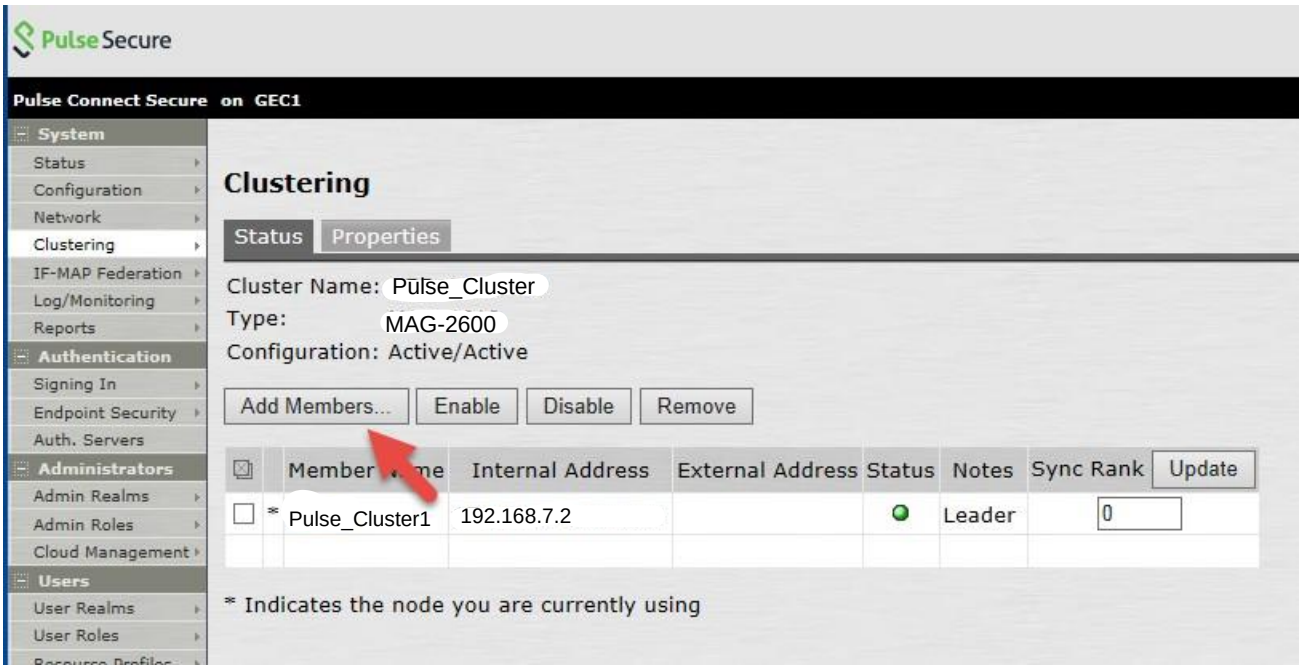
   Remarque : si vous mettez à niveau un dispositif SA/MAG autonome, reportez-vous à l'**étape 10**.

6. Sur le nouveau dispositif PSA (premier dispositif), créez manuellement un nouveau cluster avec un **nom**, des **paramètres** et des **noms de nœuds identiques** à ceux des anciens dispositifs SA/MAG du cluster.

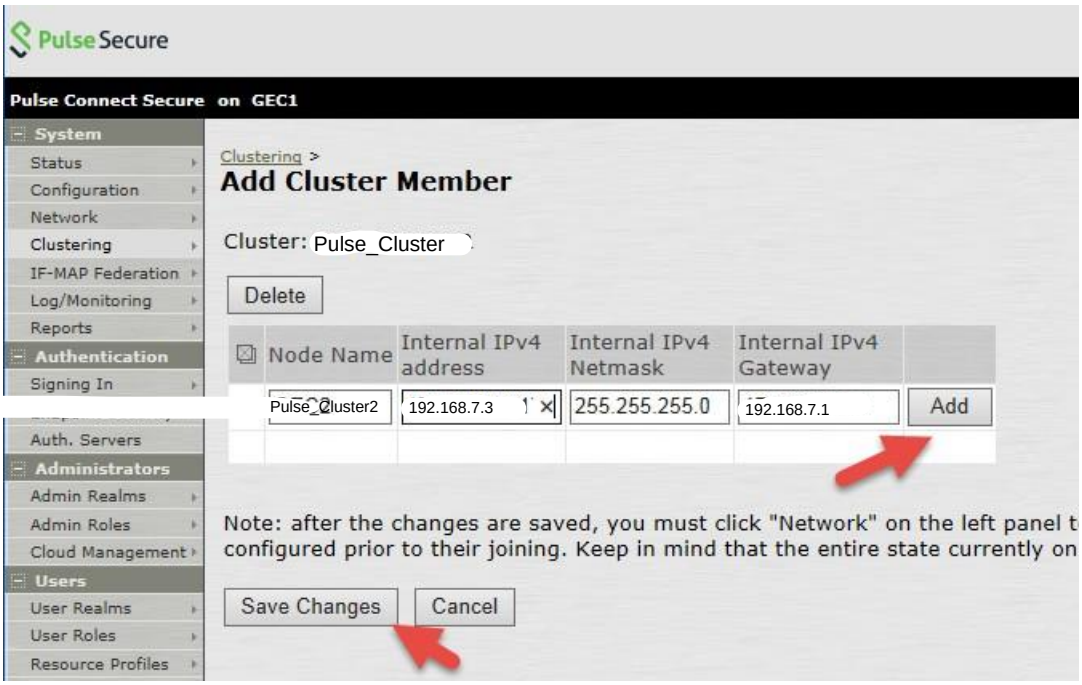




7. Ajoutez le deuxième dispositif au cluster dans la configuration principale et enregistrez les paramètres. Ajoutez un membre en cliquant sur **Ajouter des membres (Add Members)**.

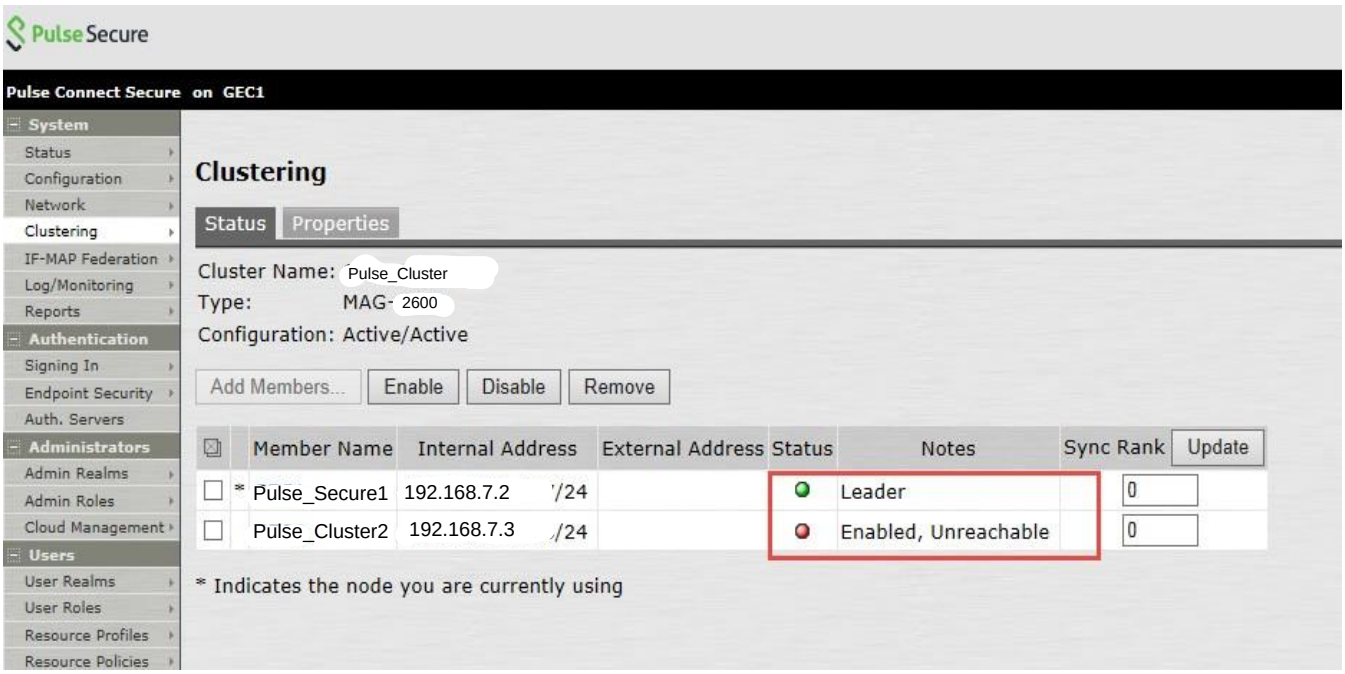


Saisissez le **nom de nœud** du membre et son **adresse IP**, et vérifiez le **masque de sous réseau** ainsi que la **passerelle**, puis cliquez sur **Ajouter (Add)**.



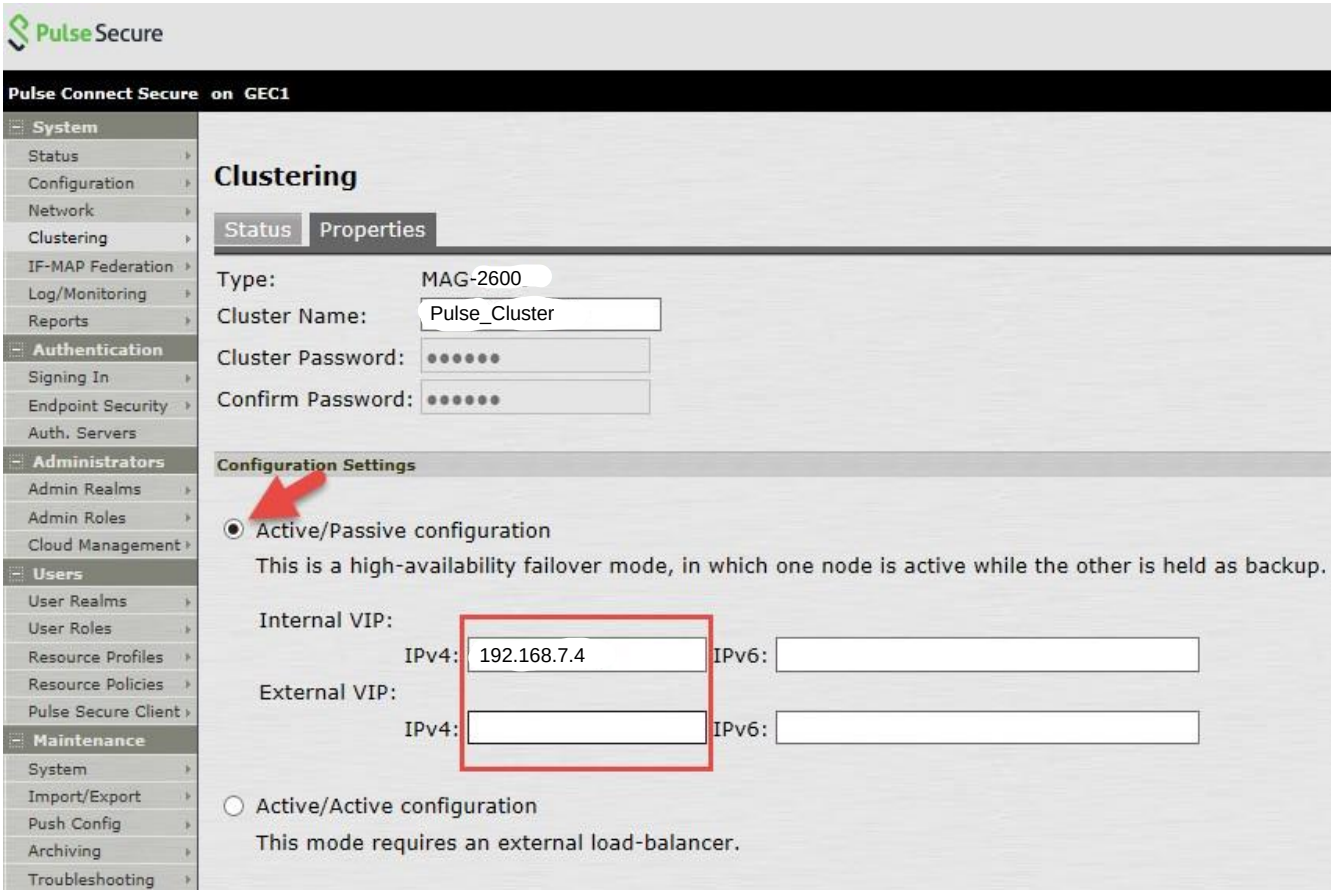
Enregistrez les modifications en cliquant sur **Enregistrer les modifications (Save Changes)**.

Vérifiez que l'**état** du cluster, d'abord en **transition**, passe à **Principal (Leader),** une fois le premier nœud activé.
Le deuxième nœud reste à l'état **Activé, inaccessible (Enabled, Unreachable)** jusqu'à ce qu'il rejoigne le cluster.

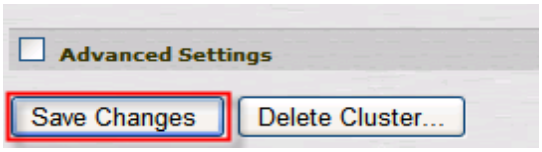


8. Si la configuration XML est exportée depuis un cluster **Actif/Passif**, il convient de configurer un port externe pour les membres du cluster (si les ports externes sont configurés en cluster) avant l'importation XML.

   Consultez la page **Mise en cluster** > **Propriétés du cluster (Clustering > Cluster Properties)** du système IVE. Changez le type de cluster de **Actif/Actif (Active/Active)** à **Actif/Passif (Active/Passive)** et ajoutez la ou les adresses VIP du cluster. (Les exemples présentés ici n'utilisent pas de ports externes.)

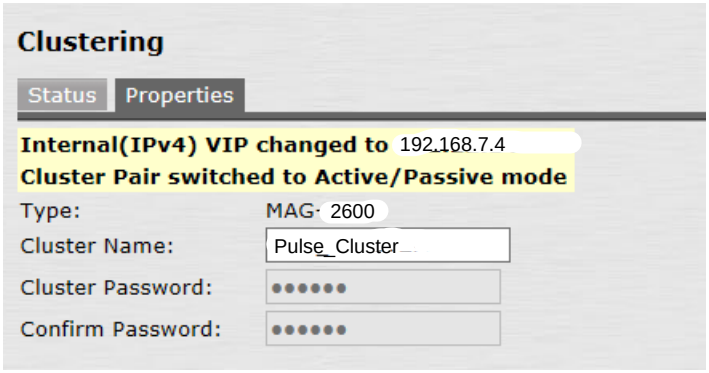


Enregistrez les paramètres de configuration du cluster.

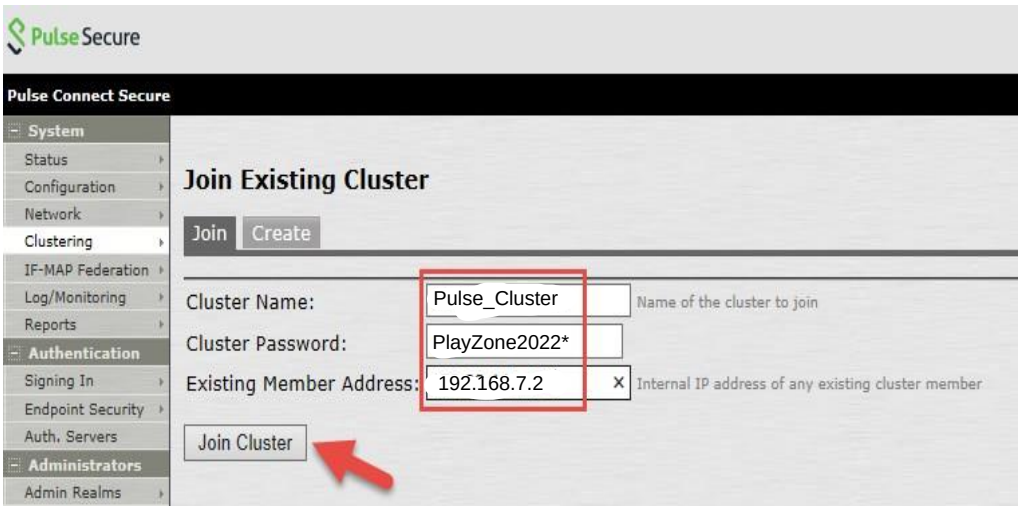


Un message apparaîtra pour confirmer le passage du mode **Actif/Actif** au mode **Actif/Passif**.

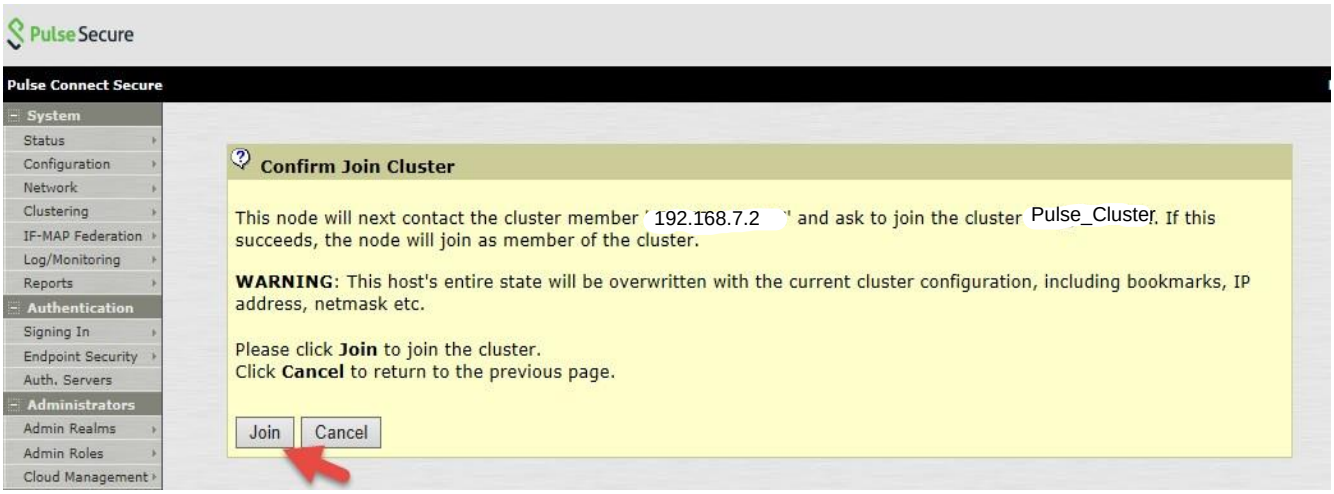
Note : nous n'utilisons pas les interfaces External par facitilité de configuration, la création du cluster n'avait pas fonctionné avec la première appliance qui avait l'interface external configurée.



9. Connectez-vous au deuxième dispositif MAG et ajoutez ce nœud au cluster en sélectionnant **Mise en cluster** > **Ajouter au cluster (Clustering>Join Cluster)**.

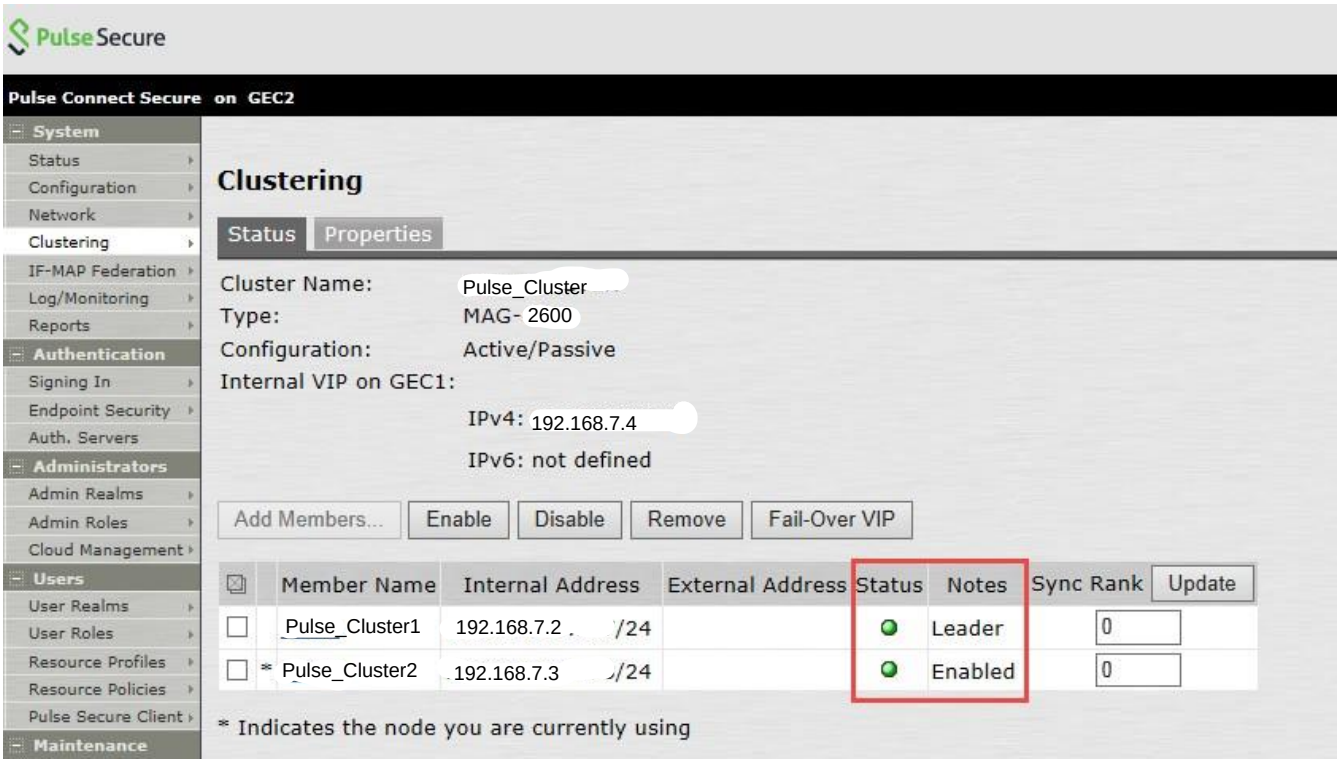


Sur la page de confirmation, cliquez sur **Ajouter (Join)**.



Après cet ajout, la session d'administration sera déconnectée du nœud secondaire ajouté.

10. Connectez-vous au premier nœud et vérifiez l'état du cluster. Ce dernier devrait être stable au bout de quelques minutes.

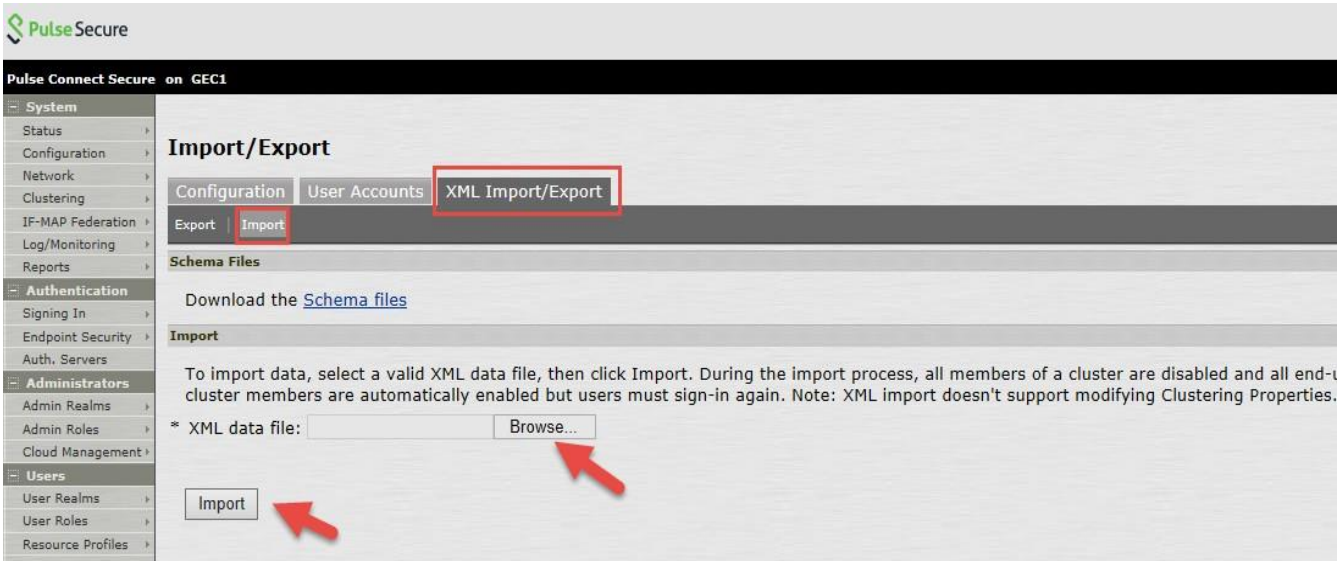


11. Dans le premier nœud du nouveau cluster, procédez à l'importation XML des paramètres réseau. Tous les paramètres réseau seront importés, y compris :

    Ports virtuels internes
    Ports virtuels externes
    Ports de gestion
    VLAN
    Routes statiques
    Paramètres de port

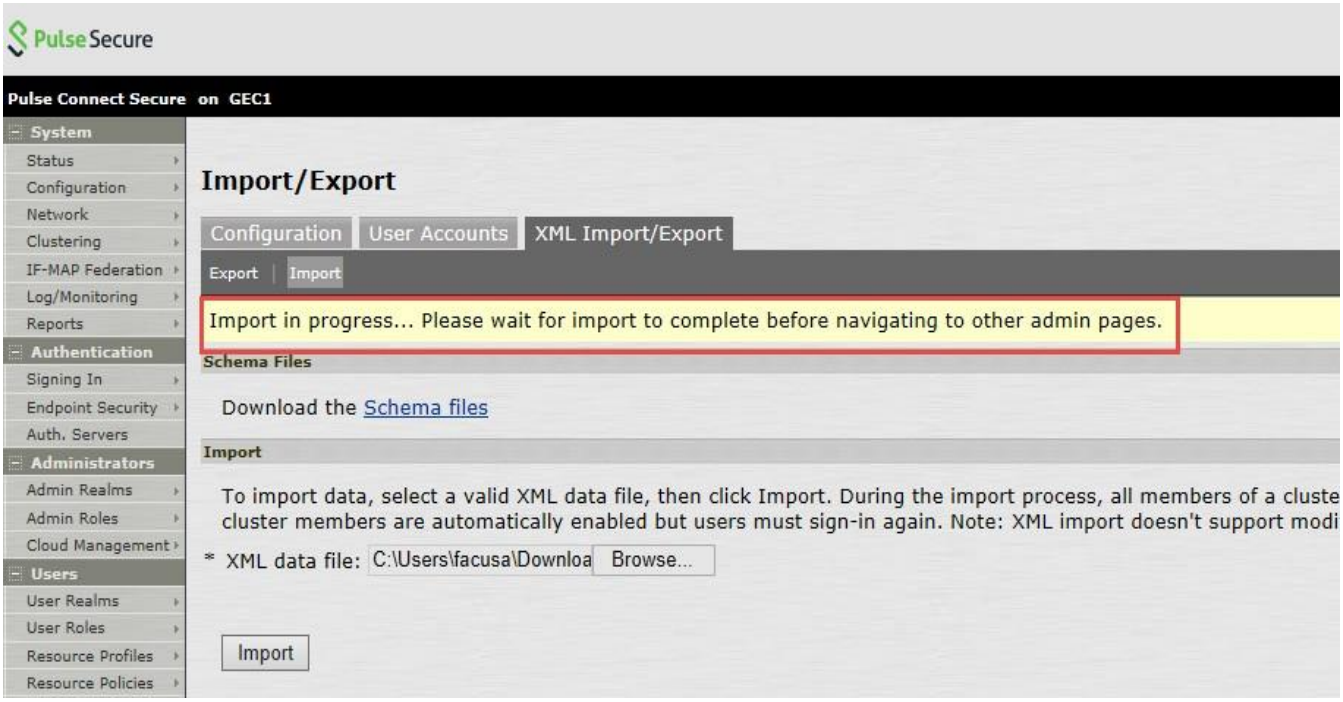
Note : nous n'avons pas importé les fichiers de config dans le deuxième noeud étant donné que les fichiers de config du premier noeud sont synchronisé grâce au Cluster.

    Sélectionnez **Maintenance** > **Importer/Exporter (Maintenance > Import/Export)**, choisissez **Importer XML (Import XML)**, indiquez l'emplacement du fichier réseau XML, puis cliquez sur **Importer (Import)**.



Si une erreur d'interfaçage est signalée, requérant par exemple une mise à niveau vers PSA7000f ou PSA7000c, modifiez le fichier XML comme suit avant de procéder à l'importation : (Paramétrez « link-speed » sur « **auto** » pour les paramètres de ports internes et externes.)

```
<internal-port>
    <node>SSLVPN-NODEX</node>
    <settings>
      <ip-address>10.10.10.n</ip-address>
      <netmask>255.255.255.224</netmask>
      <default-gateway>10.10.10.1</default-gateway>
      <link-speed>auto</link-speed>
      <arp-ping-timeout>5</arp-ping-timeout>
      <mtu>1500</mtu>
    </settings>
    <virtual-ports>
    </virtual-ports>
    <arp-cache>
    </arp-cache>
    <routes>
    </routes>
 </internal-port>
```

Remarque : si le dispositif source possède un port de gestion (par exemple, MAG-SM360) et que le dispositif PCS/PPS de destination n'en possède pas (par exemple, PSA300), l'importation XML échouera et l'erreur suivante apparaîtra :

Pour éviter ce problème, supprimez du fichier XML les paramètres du port de gestion (mis en évidence ci-dessous), puis relancez l'importation XML.

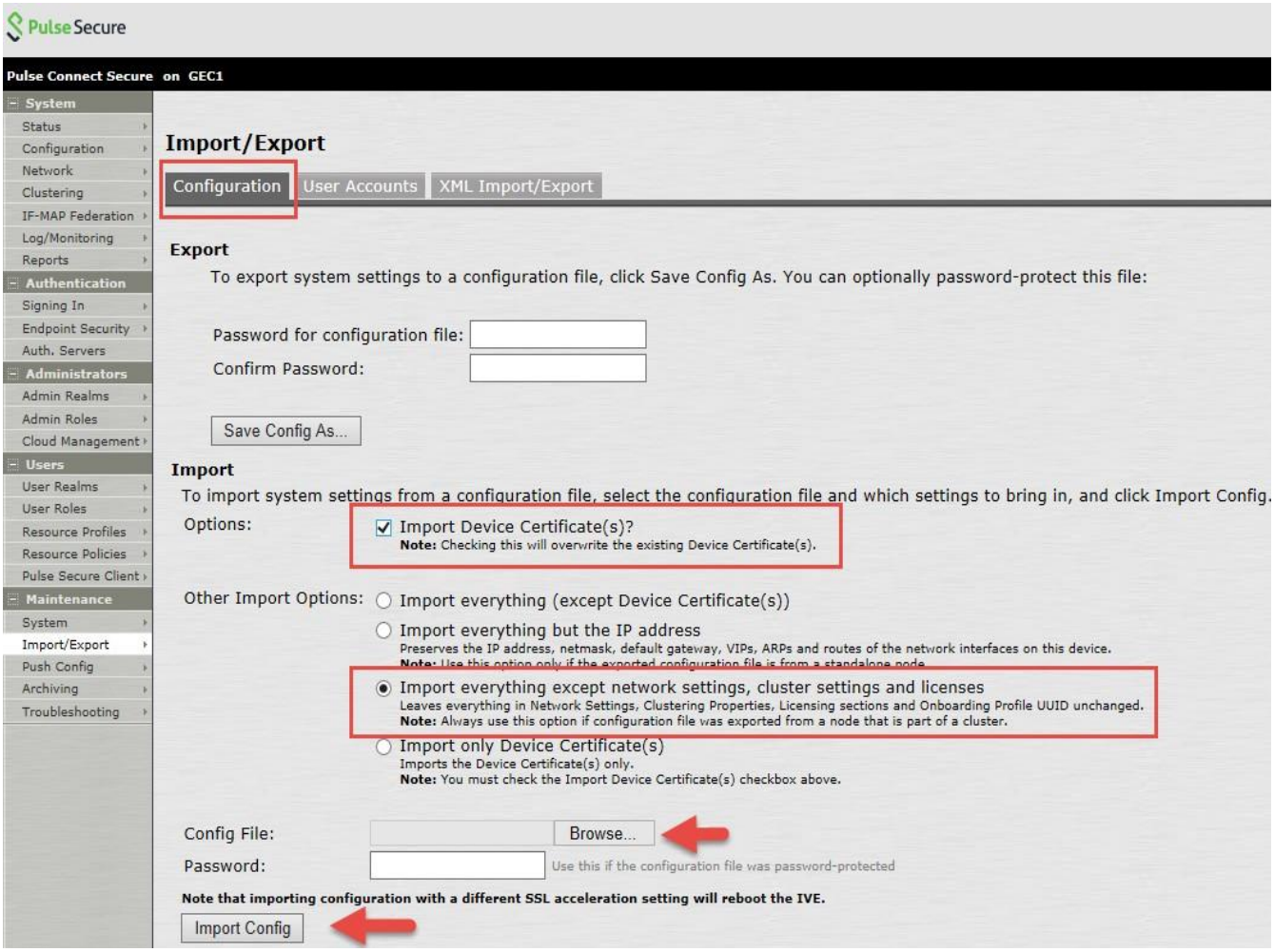
```
</internal-port>
        <management-port>
          <node>localhost2</node>
          <settings>
            <is-enabled>disabled</is-enabled>
            <ip-address></ip-address>
            <netmask></netmask>
            <default-gateway></default-gateway>
            <enable-ipv6>disabled</enable-ipv6>
            <ipv6-address></ipv6-address>
            <ipv6-prefix-length>64</ipv6-prefix-length>
            <ipv6-default-gateway></ipv6-default-gateway>
            <link-speed>auto</link-speed>
            <arp-ping-timeout>5</arp-ping-timeout>
            <mtu>1500</mtu>
          </settings>
          <arp-cache>
          </arp-cache>
          <ndp-cache>
          </ndp-cache>
          <routes>
          </routes>
          <ipv6-routes>
          </ipv6-routes>
        </management-port>
        <network-connect>
          <nc-base-ip>10.200.200.200</nc-base-ip>
          <network-ip-filter>
            <node>localhost2</node>
            <nc-ip-filters>
              <nc-ip-filter>
                <ip-filter>*</ip-filter>
              </nc-ip-filter>
            </nc-ip-filters>
          </network-ip-filter>
        </network-connect>
```


12. Dans le nœud principal du nouveau cluster, importez le fichier « **system.cfg** ». (La procédure est identique pour la mise à niveau de dispositifs autonomes.)

    Remarque : cette procédure d'exportation est identique pour la mise à niveau d'un dispositif autonome.

    Pour importer les configurations système sur le dispositif PSA :

    a. Dans la console d'administration, sélectionnez **Maintenance** > **Importer/Exporter** > **Configuration (Maintenance > Import/Export > Configuration)**.
    b. Indiquez si vous souhaitez importer le certificat Secure Access Service. Remarque : le certificat pourra uniquement être importé si vous activez la case à cocher **Importer le ou les certificats du dispositif ? (Import Device Certificate(s)?)**
    c. Sélectionnez **Importer tous les éléments à l'exception des paramètres réseau et des licences (Import everything except network settings and licenses)**. (Cette option importe tous les paramètres de configuration à l'exception des paramètres réseau, de cluster et de licence.)
    d. Indiquez l'emplacement du fichier de configuration nommé par défaut « **system.cfg** ».
    e. Saisissez le mot de passe préalablement choisi pour le fichier. Si vous n'avez pas défini de mot de passe avant d'exporter le fichier, laissez ce champ vide.
    f. Cliquez sur **Importer la configuration (Import Config)**.



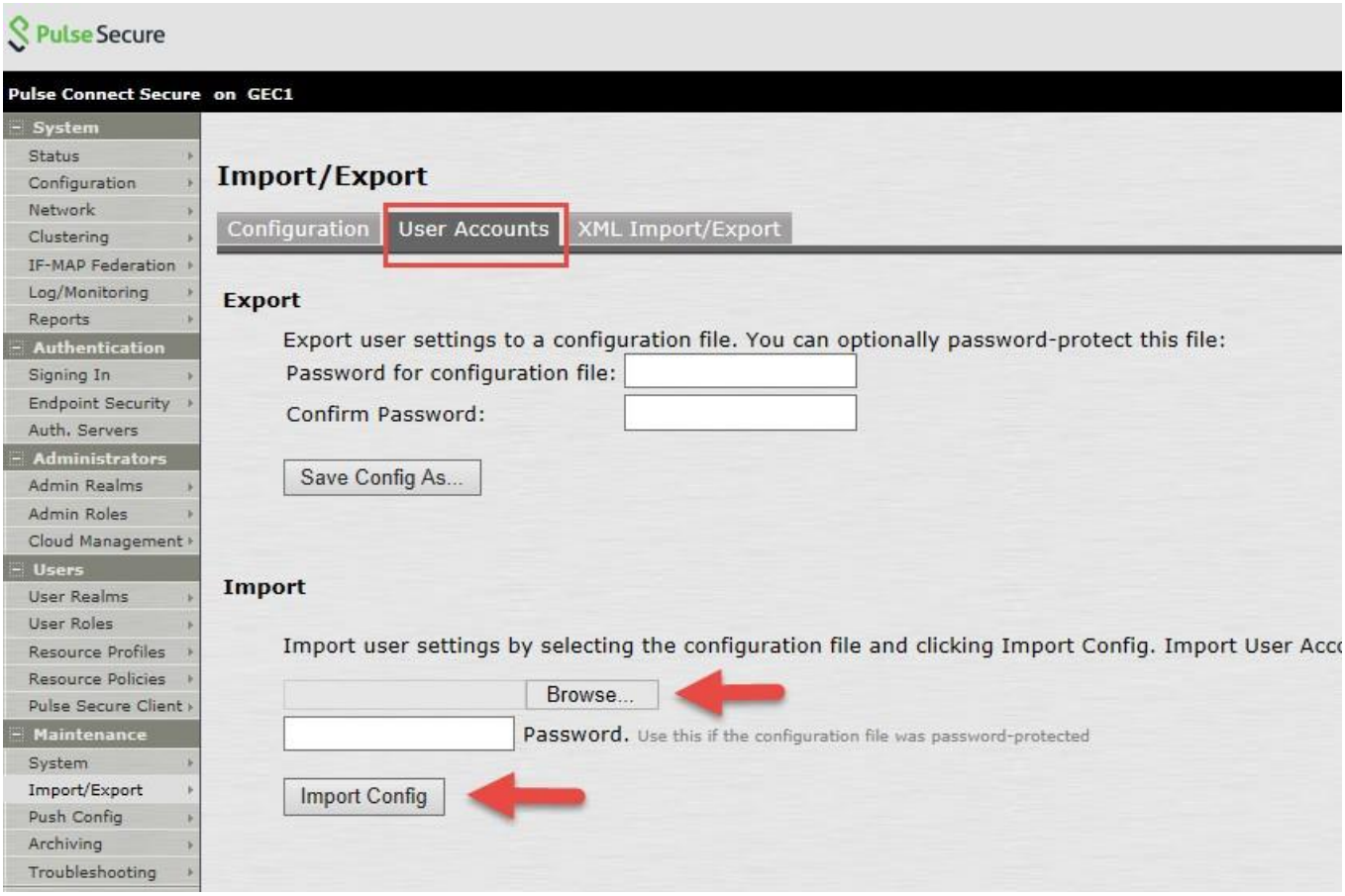
    Les paramètres système et les certificats sont importés.

13. Importez ensuite le fichier binaire « **user.cfg** » dans le même nœud principal.

Remarque : cette procédure d'exportation est identique pour la mise à niveau d'un dispositif autonome.

Pour importer les configurations système sur le dispositif PSA :

a. Dans la console d'administration, sélectionnez **Maintenance** > **Importer/Exporter** > **Comptes utilisateur (Maintenance > Import/Export > User Accounts.)**.
b. Indiquez l'emplacement du fichier de configuration nommé par défaut « **user.cfg** ».
c. Saisissez le mot de passe préalablement choisi pour le fichier. Si vous n'avez pas défini de mot de passe avant d'exporter le fichier, laissez ce champ vide.
d. Cliquez sur **Importer la configuration (Import Config)**.



14. Importez ensuite le fichier de configuration XML pour **Tous les rôles**. Cette étape restaure tous les paramètres de restriction des rôles pour les ports virtuels.
15. Après avoir importé les deux fichiers XML ainsi que les fichiers « system.cfg » et « user.cfg », vérifiez et/ou modifiez/ajoutez les paramètres locaux restants, ainsi que tout autre paramètre requis n'ayant pas été restauré, en suivant la procédure ci-dessous :

    a. **Réseau** > **Aperçu** (à définir en cluster ou en nœuds individuels)
    b. **Réseau** > **Routes** (pour les ports internes, externes et autres)
    c. **Réseau** > **Hôtes** (à définir en cluster ou en nœuds individuels)
    d. **Réseau** > **Port interne/externe** > **Ports virtuels** (si en cluster, à définir sur « Cluster entier »)
    e. **Réseau** > **VLAN** (si en cluster, à définir sur « Cluster entier »)
    f. **Réseau** > **Tunnel VPN** (à définir en cluster ou en nœuds individuels si différent)
    g. **Journal/Surveillance** > **SNMP** (à définir en cluster ou en nœuds individuels si différent)
    h. **Journal/Surveillance** > **Événements / Accès administrateur / Accès utilisateur** > **Paramètres** (à définir en cluster ou en nœuds individuels si différent)

i. **Configuration** > **Certificats** > **Certificats du dispositif** (y compris l'affectation de ses ports)
j. **Stratégies des ressources** > **Tunnel VPN** > **Profils de connexion** (si configurés)
k. **Serveurs d'authentification** > **Serveur d'authentification ACE** (si utilisé : vérifier l'état du fichier secret du nœud)
l. **Configuration** > **Attribution des licences** - Paramètres client-serveur de licences (si utilisé comme client de gestion des licences dans un environnement de serveur de licences Enterprise) + Licences adaptées installées

16. Vérifiez l'état du cluster (si les dispositifs sont configurés ainsi) et testez son bon fonctionnement en vous connectant aux adresses VIP (ou à l'adresse IP du dispositif autonome). Testez l'authentification en utilisant un serveur de type AD, ACE ou autre, puis contrôlez l'ensemble des fonctionnalités activées telles que NC ou Pulse.
17. Vous avez maintenant terminé la mise à niveau de la plate-forme matérielle.

RÉFÉRENCES

Guides des équipements PSA :

https://www.pulsesecure.net/download/techpubs/current/502/pulse-appliances/psa/psa7000HardwareGuide.pdf

https://www.pulsesecure.net/download/techpubs/current/501/pulse-appliances/psa/psa5000HardwareGuide.pdf

https://www.pulsesecure.net/download/techpubs/current/500/pulse-appliances/psa/psa3000HardwareGuide.pdf

https://www.pulsesecure.net/download/techpubs/current/499/pulse-appliances/psa/psa300HardwareGuide.pdf

Guide d'administration Pulse Connect Secure :

Admin guide (Guide d'administration, page 845) : Clustering (Mise en cluster)

Base de connaissances présentant le type de réseau pris en charge pour la mise en cluster :

https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB26035

Base de connaissances relative aux dispositifs PSA :

https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40034

https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40035

https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40391

