

Configurer un cluster ESA (Email Security Appliance)

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Problème](#)

[Clusters sur ESA](#)

[Créer le cluster](#)

[Créer un cluster sur SSH](#)

[Créer un cluster sur CCS](#)

[Rejoindre un cluster actuel via SSH ou CCS](#)

[Joindre via SSH](#)

[Joindre via CCS](#)

[Éléments migrés dans une configuration de cluster](#)

[Éléments non migrés dans une configuration de cluster](#)

[Comment les groupes sont-ils configurés dans un cluster ESA ?](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer un cluster sur un dispositif de sécurité de la messagerie électronique Cisco (ESA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment joindre des appliances dans un cluster (gestion centralisée).
- Tous les ESA doivent avoir les mêmes versions AsyncOS (jusqu'à la révision).

 Remarque : dans la version 8.5+, la clé de gestion centralisée n'est plus nécessaire et n'est plus visible lorsqu'elle est ajoutée, car elle est une fonctionnalité intégrée dans AsyncOS.

- Si vous créez un cluster pour utiliser le port 22 (plus facile à configurer), assurez-vous qu'il n'y a pas de problèmes de pare-feu ou de routage entre les appliances sur le trafic du port

22.

- Si vous créez un cluster pour utiliser le port 2222 (Cluster Communication Service), assurez-vous que les règles de pare-feu sont définies pour permettre au trafic sur ce port d'être disponible sans inspection ni interruption.
- Les options de configuration de cluster doivent être effectuées via l'interface de ligne de commande sur l'ESA et ne peuvent pas être créées ou jointes dans l'interface utilisateur graphique.
- Si vous choisissez d'utiliser un nom d'hôte pour la communication, assurez-vous que les serveurs DNS définis sur les appliances sont capables de résoudre tous les autres appliances de votre réseau et que les adresses IP vers lesquelles les noms d'hôtes sont résolus sont affectées à une interface configurée pour écouter sur le port de communication sélectionné.
- Assurez-vous que le port et le service requis sont activés sur les interfaces de votre appliance (SSH ou CCS).

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Problème

Le problème est d'éviter d'avoir à modifier en permanence chaque appliance chaque fois qu'une configuration entre un grand groupe d'ESA doit être centralisée et synchronisée.

Clusters sur ESA

La fonction de gestion centralisée ESA vous permet de gérer et de configurer plusieurs appliances simultanément, afin d'améliorer la fiabilité, la flexibilité et l'évolutivité de votre réseau. Cela vous permet de gérer globalement tout en vous conformant aux stratégies locales.

Un cluster se compose d'un ensemble de machines avec des informations de configuration communes. Dans chaque grappe, les appareils peuvent être subdivisés en groupes de machines, où une seule machine peut être membre d'un seul groupe à la fois.

Les clusters sont mis en oeuvre dans une architecture peer to peer sans relation primaire/secondaire. Vous pouvez vous connecter à n'importe quel ordinateur pour contrôler et administrer l'ensemble du cluster ou du groupe. Cela permet à l'administrateur de configurer différents éléments du système à l'échelle d'un cluster, d'un groupe ou par machine, en fonction de leurs propres groupes logiques

Créer le cluster

Une fois que toutes les conditions requises sont remplies, pour créer le cluster, vous devez commencer dans la ligne de commande (CLI) du premier appareil.

 Conseil : sauvegardez votre configuration actuelle sur votre appliance avant de configurer votre cluster. Dans l'interface utilisateur graphique, System Administration > Configuration File. Décochez la case Mot de passe masqué et enregistrez la configuration localement sur votre PC.

Créer un cluster sur SSH

```
C370.1ab> clusterconfig
```

```
Do you want to join or create a cluster?
```

1. No, configure as standalone.
2. Create a new cluster.
3. Join an existing cluster over SSH.
4. Join an existing cluster over CCS.

```
[1]> 2
```

```
Enter the name of the new cluster.
```

```
[> NameOfCluster
```

```
Should all machines in the cluster communicate with each other by hostname or by IP address?
```

1. Communicate by IP address.
2. Communicate by hostname.

```
[2]> 1
```

```
What IP address should other machines use to communicate with Machine C370.1ab?
```

1. 10.1.1.11 port 22 (SSH on interface Management)
2. Enter an IP address manually

```
[> 1
```

```
Other machines will communicate with Machine C370.1ab using IP address 10.1.1.11 port 22. You can change this by using the COMMUNICATION subcommand of the clusterconfig command.
```

```
New cluster committed: DATE
```

```
Creating a cluster takes effect immediately, there is no need to commit.
```

```
Cluster NameOfCluster
```

```
Choose the operation you want to perform:
```

- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- CONNSTATUS - Show the status of connections between machines in the cluster.
- COMMUNICATION - Configure how machines communicate within the cluster.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.

Créer un cluster sur CCS

```
C370.lab> clusterconfig
```

```
Do you want to join or create a cluster?
```

1. No, configure as standalone.
2. Create a new cluster.
3. Join an existing cluster over SSH.
4. Join an existing cluster over CCS.

```
[1]> 2
```

```
Enter the name of the new cluster.
```

```
[> Test
```

```
Should all machines in the cluster communicate with each other by hostname or by IP address?
```

1. Communicate by IP address.
2. Communicate by hostname.

```
[2]> 1
```

```
What IP address should other machines use to communicate with Machine C370.lab?
```

1. 10.1.1.1 port 22 (SSH on interface Management)
2. Enter an IP address manually

```
[> 2
```

```
Enter the IP address for Machine C370.lab.
```

```
[> 10.1.1.1
```

```
Enter the port (on 10.66.71.120) for Machine C370.lab.
```

```
[22]> 2222
```

Une fois cette étape terminée, vous disposez d'un cluster et toutes vos configurations sont déplacées du niveau Machine vers le niveau Cluster. Il s'agit de la configuration héritée par toutes les autres machines lorsqu'elles sont jointes.

Rejoindre un cluster actuel via SSH ou CCS

Cette section explique comment ajouter de nouvelles appliances à votre cluster actuel que vous avez précédemment ou que vous venez de créer. La connexion à une grappe actuelle par l'une ou l'autre méthode est similaire dans l'approche, le seul point de différence clé est que CCS nécessite une étape supplémentaire pour la finaliser afin de permettre à la grappe d'accepter la nouvelle appliance.

Joindre via SSH



Remarque : la section indiquée en gras dans ces prochaines étapes doit être effectuée exactement, avec SSH, vous ne devez pas dire oui à l'activation CCS.

```
C370.lab> clusterconfig
```

Do you want to join or create a cluster?

1. No, configure as standalone.
2. Create a new cluster.
3. Join an existing cluster over SSH.
4. Join an existing cluster over CCS.

```
[1]> 3
```

While joining a cluster, you will need to validate the SSH host key of the remote machine to which you are joining. To get the public host key fingerprint of the remote host, connect to the cluster and run: `logconfig -> fingerprint`.

WARNING: All non-network settings will be lost. System will inherit the values set at the group or cluster level. Verify the non-network settings. Ensure that the cluster settings are compatible with your network settings (e.g. IP settings)

Exception: Centralized Policy, Virus, and Outbreak Quarantine settings are not inherited from the cluster. These settings on this machine will remain intact.

```
Do you want to enable the Cluster Communication Service on C370.lab? [N]>
```

Enter the IP address of a machine in the cluster.

```
[ ]> 10.66.71.120
```

Enter the remote port to connect to. This must be the normal admin ssh port, not the CCS port.

```
[22]>
```

Enter the name of an administrator present on the remote machine

```
[admin]>
```

Enter password:

Please verify the SSH host key for 10.66.71.120:

Public host key fingerprint: d2:6e:36:9b:1d:87:c6:1f:46:ea:59:40:61:cc:3e:ef

Is this a valid key for this host? [Y]>

Une fois la vérification effectuée, l'appliance se joint au cluster avec succès.

Joindre via CCS

Cette approche est similaire. La seule différence est qu'avant de décider d'autoriser la nouvelle appliance dans le cluster actuel, vous devez vous connecter à l'appliance active dans le cluster.

Sur l'appliance active dans le cluster :

```
(Cluster test)> clusterconfig
```

```
Cluster test
```

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.
 - CONNSTATUS - Show the status of connections between machines in the cluster.
 - COMMUNICATION - Configure how machines communicate within the cluster.
 - DISCONNECT - Temporarily detach machines from the cluster.
 - RECONNECT - Restore connections with machines that were previously detached.
 - PREPJOIN - Prepare the addition of a new machine over CCS.
- ```
[> prepjoin
```

Prepare Cluster Join Over CCS

No host entries waiting to be added to the cluster.

Choose the operation you want to perform:

- NEW - Add a new host that will join the cluster.
- ```
[> new
```

Enter the hostname of the system you want to add.

```
[> ESA.lab
```

Enter the serial number of the host ESA.lab.

```
[> XXXXXXXXXXXXXXX-XXXXXA
```

Enter the user key of the host ESA2.lab. This can be obtained by typing "clusterconfig prepjoin print" in the CLI on ESA.lab.

Press enter on a blank line to finish.

Une fois que vous avez entré l'empreinte SSH (qui est obtenue lorsque vous vous connectez à l'appliance qui tente de joindre votre cluster et avec la commande `clusterconfig prepjoin print`) dans l'exemple de code précédent et que vous entrez une ligne vide, il termine la jointure de préparation.

 **Remarque** : si vous exécutez l' `PREPJOIN` option, vous devez valider vos modifications sur l'ESA principal avant d'exécuter `clusterconfig` sur l'ESA secondaire et de joindre cette appliance à votre cluster nouvellement configuré. Ceci est noté dans le résultat tout au long de l'opération : pour joindre cet appareil à un cluster avec des clés pré-partagées, connectez-vous à l'ordinateur du cluster, exécutez la `clusterconfig > prepjoin > new` commande , entrez les détails suivants, et `commit` vos modifications.

Vous pouvez ensuite lancer le processus de jointure sur l'appliance qui tente de se connecter, pour référence, appelez-la **ESA2.lab** pour qu'elle corresponde à celle de l'étape précédente.

 **Remarque** : la clé SSH-DSS figure dans l'exemple suivant.

```
ESA2.lab> clusterconfig Do you want to join or create a cluster? 1. No, configure as standalone. 2. Create a new cluster. 3. Join an existing cluster over SS
To get the public host key fingerprint of the remote host, connect to the cluster and run: logconfig -> hostkeyconfig -> fingerprint. WARNING: All non-net
the non-network settings. Ensure that the cluster settings are compatible with your network settings (e.g. dnsconfig settings) Exception: Centralized Policy,
These settings on this machine will remain intact. In order to join a cluster over CCS, you must first log in to the cluster and tell it that this system is being
On a machine in the cluster, run "clusterconfig -> prepjoin -> new" with the following information and commit. Host: ESA2.lab Serial Number: XXXXXX
not the normal admin ssh port. [2222]>
```

Une fois que cela est confirmé, vous voyez la clé SSH-DSS. S'il correspond, vous pouvez accepter les termes et le cluster est joint avec succès.

Éléments migrés dans une configuration de cluster

La configuration du cluster migre :

- Paramètres de stratégie configurés
- Filtres de contenu
- Ressources textuelles
- Dictionnaires de contenu
- Paramètres LDAP
- Antispam Et Antivirus
- Paramètres globaux
- Paramètres du récepteur
- Paramètres de routage SMTP
- Paramètres DNS

Éléments **non** migrés dans une configuration de cluster

La configuration du cluster ne migre pas :

- Nom d'hôte local du périphérique.
- Interfaces IP configurées.
- Tables de routage configurées.
- Configuration de la quarantaine du spam local.
- Configurations de quarantaine des stratégies locales, des virus et des attaques
- Paramètres sous la `websecurityadvancedconfig` commande dans la ligne de commande (pour les versions 8.5 et ultérieures).



Remarque : si des filtres de contenu référencent des quarantaines qui n'existent pas, ils sont invalidés jusqu'à ce que les quarantaines de stratégie référencées aient été configurées sur l'ordinateur.

Comment les groupes sont-ils configurés dans un cluster ESA ?

Dans certains scénarios, il peut être exigé que peu d'AES du cluster travaillent d'une manière particulière que les autres. Pour ce faire, vous n'avez pas besoin de créer un nouveau cluster et vous pouvez poursuivre la création de groupes.



Remarque : les configurations effectuées au niveau du groupe sont prioritaires sur la configuration au niveau du cluster.

Pour la création de groupes, créez-la à partir de l'interface de ligne de commande ESA. Pour commencer la configuration, utilisez la commande clusterconfig --> ADDGROUP :

```
(Machine esalab.cisco.com)> clusterconfig
```

Cette commande est limitée au mode « cluster ». Voulez-vous passer en mode « cluster » ? [O]>

Cluster Cisco

Sélectionnez l'opération que vous souhaitez effectuer :

- ADDGROUP - Ajoute un groupe de clusters.
- SETGROUP - Définit le groupe dont les ordinateurs sont membres.
- RENAMEGROUP - Renommez un groupe de clusters.
- DELETEGROUP - Supprime un groupe de clusters.
- REMOVEMACHINE - Supprime un ordinateur du cluster.
- SETNAME - Définit le nom du cluster.
- LIST - Répertorie les machines du cluster.
- CONNSTATUS - Affiche l'état des connexions entre les machines du cluster.
- COMMUNICATION : configurez la manière dont les machines communiquent au sein du cluster.
- DISCONNECT (DÉCONNEXION) : déconnecte temporairement les ordinateurs du cluster.
- RECONNECT - Restaure les connexions avec les machines précédemment déconnectées.
- PREPJOIN - Préparer l'ajout d'une nouvelle machine sur CCS.

[> ADDGROUP

Entrez le nom du nouveau groupe de clusters à créer.

[> Nouveau_Groupe

Groupe de clusters créé par New_Group.

Pour ajouter des ESA du cluster actuel au nouveau groupe créé, utilisez la commande SETGROUP :

(Machine esalab.cisco.com)> clusterconfig

Cette commande est limitée au mode « cluster ». Voulez-vous passer en mode « cluster » ? [O]>

Cluster Cisco

Sélectionnez l'opération que vous souhaitez effectuer :

- ADDGROUP - Ajoute un groupe de clusters.
- SETGROUP - Définit le groupe dont les ordinateurs sont membres.
- RENAMEGROUP - Renommez un groupe de clusters.
- DELETEGROUP - Supprime un groupe de clusters.
- REMOVEMACHINE - Supprime un ordinateur du cluster.
- SETNAME - Définit le nom du cluster.

- LIST - Répertorie les machines du cluster.
- CONNSTATUS - Affiche l'état des connexions entre les machines du cluster.
- COMMUNICATION : configurez la manière dont les machines communiquent au sein du cluster.
- DISCONNECT (DÉCONNEXION) : déconnecte temporairement les ordinateurs du cluster.
- RECONNECT - Restaure les connexions avec les machines précédemment déconnectées.
- PREPJOIN - Préparer l'ajout d'une nouvelle machine sur CCS.

[> GROUPE DE CONFIGURATION

Sélectionnez la machine à déplacer vers un autre groupe. Séparez plusieurs machines par des virgules.

1. esalab.cisco.com (groupe ESA_Group)

[1]> 1

Sélectionnez le groupe dont esalab.cisco.com doit être membre.

1. Groupe_ESA

2. Nouveau_groupe

[1]> 2

esalab.cisco.com défini sur le groupe New_Group.

Pour renommer un groupe actuel dans le cluster ESA, utilisez la commande RENAMEGROUP:

(Machine esalab.cisco.com)> clusterconfig

Cette commande est limitée au mode « cluster ». Voulez-vous passer en mode « cluster » ? [O]>

Cluster Cisco

Sélectionnez l'opération que vous souhaitez effectuer :

- ADDGROUP - Ajoute un groupe de clusters.
- SETGROUP - Définit le groupe dont les ordinateurs sont membres.
- RENAMEGROUP - Renommez un groupe de clusters.
- DELETEDGROUP - Supprime un groupe de clusters.
- REMOVEMACHINE - Supprime un ordinateur du cluster.
- SETNAME - Définit le nom du cluster.
- LIST - Répertorie les machines du cluster.

- CONNSTATUS - Affiche l'état des connexions entre les machines du cluster.
- COMMUNICATION : configurez la manière dont les machines communiquent au sein du cluster.
- DISCONNECT (DÉCONNEXION) : déconnecte temporairement les ordinateurs du cluster.
- RECONNECT - Restaure les connexions avec les machines précédemment déconnectées.
- PREPJOIN - Préparer l'ajout d'une nouvelle machine sur CCS.

[]> RENOMMER LE GROUPE

Choisissez le groupe que vous souhaitez renommer.

1. Groupe_ESA
2. Nouveau_groupe

[1]> 2

Saisissez le nouveau nom du groupe.

[Nouveau_Groupe]> Groupe_Cluster

Groupe New_Group renommé Cluster_Group.

Pour supprimer un groupe actuel du cluster ESA, utilisez la commande DELETEDGROUP

(Machine esalab.cisco.com)> clusterconfig

Cette commande est limitée au mode « cluster ». Voulez-vous passer en mode « cluster » ? [O]>

Cluster Cisco

Sélectionnez l'opération que vous souhaitez effectuer :

- ADDGROUP - Ajoute un groupe de clusters.
- SETGROUP - Définit le groupe dont les ordinateurs sont membres.
- RENAMEGROUP - Renommez un groupe de clusters.
- DELETEDGROUP - Supprime un groupe de clusters.
- REMOVEMACHINE - Supprime un ordinateur du cluster.
- SETNAME - Définit le nom du cluster.
- LIST - Répertoire les machines du cluster.
- CONNSTATUS - Affiche l'état des connexions entre les machines du cluster.
- COMMUNICATION : configurez la manière dont les machines communiquent au sein du cluster.

- DISCONNECT (DÉCONNEXION) : déconnecte temporairement les ordinateurs du cluster.

- RECONNECT - Restaure les connexions avec les machines précédemment déconnectées.

- PREPJOIN - Préparer l'ajout d'une nouvelle machine sur CCS.

[]> DELETEDGROUP

Choisissez le groupe que vous souhaitez supprimer.

1. Groupe_Cluster

2. Groupe_ESA

[1]> 1

Sélectionnez le groupe vers lequel les ordinateurs dans Cluster_Group doivent être déplacés.

1. Groupe_ESA

[1]> 1

Groupe Cluster_Group supprimé.



Remarque : lorsque vous ajoutez/supprimez des machines dans Cluster, les modifications s'appliquent instantanément aux appliances sans commit. Alors que pour les groupes AES, toute action y relative n'est appliquée aux AES qu'après une commitévaluation.

Informations connexes

- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.