

# 配置郵件安全裝置(ESA)集群

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[問題](#)

[ESA上的群集](#)

[建立叢集](#)

[透過SSH建立叢集](#)

[透過CCS建立叢集](#)

[透過SSH或CCS加入當前集群](#)

[透過SSH加入](#)

[透過CCS加入](#)

[在叢集配置中移轉的內容](#)

[未在群集配置中遷移的內容](#)

[如何在ESA集群中配置組](#)

[相關資訊](#)

---

## 簡介

本文檔介紹如何在思科郵件安全裝置(ESA)上設定集群。


## 必要條件

### 需求

思科建議您瞭解以下主題：

- 如何將裝置加入集群 ( 集中管理 )。
- 所有ESA必須具有相同的AsyncOS版本 ( 向下到修訂版本 )。

---

 **注意：**在8.5+版本中，集中管理金鑰不再需要，增加時也不再可見，因為它是AsyncOS中的整合功能。

---

- 如果建立集群以使用埠22 ( 更易於配置 )，請確保埠22流量上的裝置之間不存在防火牆或路由問題。
- 如果您建立集群來使用埠2222 ( 集群通訊服務 )，請確保防火牆規則允許此埠上的流量在未被檢測或中斷的情況下可用。
- 群集配置選項必須透過ESA上的CLI完成，並且無法在GUI中建立或加入。

- 如果選擇使用主機名進行通訊，請確保裝置上設定的DNS伺服器能夠解析網路中的所有其他裝置，並且主機名解析的IP地址已分配給配置為偵聽所選通訊埠的介面。
- 確保在裝置介面上啟用所需的埠和服務 ( SSH或CCS )。

## 採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 問題

問題在於，每當需要集中化一組ESA之間的配置並保持同步時，就無需在每個裝置上持續進行修改。

## ESA上的群集

ESA集中管理功能允許您同時管理和配置多個裝置，以提高網路可靠性、靈活性和可擴充性。這允許您在遵守本地策略的同時進行全局管理。


集群由一組具有通用配置資訊的電腦組成。在每個集群內，裝置可以進一步劃分為多個電腦組，其中一台電腦一次只能屬於一個組。

集群在點對點體系結構中實現，沒有主要/次要關係。您可以登入任何機器以控制和管理整個叢集或群組。這可讓管理員在叢集範圍、群組範圍或每部機器上，根據其本身的邏輯群組來設定系統的不同元素

## 建立叢集

滿足所有要求後，要建立集群，您需要從第一個裝置的命令列(CLI)開始。

---

 提示：配置集群之前，請先在裝置上備份當前配置。在GUI中，依次選擇System Administration > Configuration File。取消選中遮蔽的密碼框並將配置本地儲存到您的PC。

---

## 透過SSH建立叢集

```
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.
```

```
[> 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.

## 透過CCS建立叢集

```
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.

```
[> 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 C370.1ab?

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

```
[ ]> 2
```

Enter the IP address for Machine C370.1ab.

```
[ ]> 10.1.1.1
```

Enter the port (on 10.66.71.120) for Machine C370.1ab.

```
[22]> 2222
```

完成此步驟後，您就擁有了一個集群，並且所有配置都將從電腦級別移動到集群級別。這是所有其他電腦在加入時全部繼承的配置。

## 透過SSH或CCS加入當前集群

本節介紹如何將之前或剛剛建立的任何新裝置增加到當前集群中。使用任何一種方法加入當前集群的方法都非常類似，唯一的不同之處是CCS需要執行額外的步驟才能最終完成，以允許集群接受較新的裝置。

### 透過SSH加入



**注意：**需要使用SSH準確地完成以下步驟中以粗體顯示的部分，您不能對CCS啟用說是。

```
<#root>
```

```
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]> 3
```

```
While joining a cluster, you will need to validate the SSH host key of the remote machine to which you .  
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 clus  
the non-network settings. Ensure that the cluster settings are compatible with your network settings (e  
settings)
```

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

```
Do you want to enable the Cluster Communication Service on C370.1ab? [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]>
```

檢查後，裝置將成功加入群集。

## 透過CCS加入

這和方法相似，唯一的區別是，在決定允許新裝置進入當前群集之前，您需要登入到群集中處於活動狀態的裝置。

在群集中的活動裝置上：

```
(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.
```

當您在前面的代碼示例中輸入SSH指紋(當您登入嘗試加入集群的裝置並使用`clusterconfig prepjoin print`命令時獲得)並輸入空行後，將完成準備加入。


---

 **注意：**如果運行 PREPJOIN 選項，則需要在輔助ESA上運行 `clusterconfig` 並將該裝置加入新配置的集群之前提交對主ESA的更改。此操作過程中的輸出中會記錄這一點：要使用預共用金鑰將此裝置加入集群，請登入集群電腦，運行 `clusterconfig > prepjoin > new` 命令，輸入下一個詳細資訊，然後輸 `commit` 您的更改。

---

然後，您可以在嘗試加入的裝置上開始加入過程，例如，將其稱為**ESA2.lab** 以與前一步的步驟匹配。

---

 **注意：**下一個示例中為SSH-DSS金鑰。

---

```
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 SSH.
To get the public host key fingerprint of the remote host, connect to the cluster and run: logconfig -> hostkeyconfig -> fingerprint. WARNING: All non-network
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]>
```

確認此情況後，您會看到SSH-DSS金鑰。如果匹配，您可以接受這些條款，並成功加入集群。

在叢集配置中移轉的內容

叢集配置移轉：

- 配置的策略設定
- 內容過濾器
- 文字資源
- 內容詞典
- LDAP設定
- 反垃圾郵件和防病毒
- 全域設定
- 監聽器設定
- SMTP路由設定
- DNS設定

## 叢集組態中未移轉的專案

### 叢集配置無法移轉：

- 裝置本地主機名。
- 已配置IP介面。
- 已配置路由表。
- 本地垃圾郵件隔離區配置。
- 本地策略、病毒和爆發隔離區配置
- 命令列中websecurityadvancedconfig 命令下的設定 ( 適用於版本8.5及更高版本 ) 。



注意：如果您具有引用不存在的隔離區的內容過濾器，則在電腦上配置所引用的策略隔離區之前，這些過濾器將失效。

---

### 如何在ESA集群中配置組

在某些場景中，可能要求集群中很少有ESA以特定方式工作，而不是以其它方式工作。若要達到此目的，您不需要建立新的叢集，而且您可以繼續建立「群組」。



---

注意：在「群組」層級建立的組態會優先於「叢集」層級組態。

---

要建立組，請從ESA CLI建立組。要開始配置，請使用命令 `clusterconfig --> ADDGROUP`：

(電腦esalab.cisco.com)> clusterconfig

此命令僅限於「集群」模式。 是否要切換至「叢集」模式？[Y]>

集群思科

選擇要執行的作業：

- ADDGROUP -增加群集組。

- SETGROUP -設定電腦所屬的組。
- RENAMEGROUP -重新命名群集組。
- DELETEDGROUP -刪除群集組。
- REMOVEMACHINE -從群集中刪除電腦。
- SETNAME -設定叢集名稱。
- LIST -列出群集中的電腦。
- CONNSTATUS -顯示群集中電腦之間的連線狀態。
- 通訊-設定機器在叢集中通訊的方式。
- 中斷連線-暫時將電腦從叢集中斷連線。
- 重新連線-恢復與先前已斷開的電腦的連線。
- PREPJOIN -準備在CCS上增加新電腦。

[> ADDGROUP

輸入要建立的新叢集組名稱。

[> New\_Group

已建立群集組New\_Group。

要將ESA從當前集群增加到建立的新組，請使用命令SETGROUP：

(電腦esalab.cisco.com)> clusterconfig

此命令僅限於「集群」模式。 是否要切換至「叢集」模式？[Y]>

集群思科

選擇要執行的作業：

- ADDGROUP -增加群集組。
- SETGROUP -設定電腦所屬的組。
- RENAMEGROUP -重新命名群集組。
- DELETEDGROUP -刪除群集組。
- REMOVEMACHINE -從群集中刪除電腦。
- SETNAME -設定叢集名稱。
- LIST -

列出群集中的電腦。

- CONNSTATUS -顯示集群中電腦之間的連線狀態。

- 通訊-設定機器在叢集中通訊的方式。

- 中斷連線-暫時將電腦從叢集中斷連線。

- 重新連線-恢復與先前已斷開的電腦的連線。

- PREPJOIN -準備在CCS上增加新電腦。

[>]設定組

選擇要移至其他群組的機器。 使用逗號分隔多台電腦。

1. esalab.cisco.com ( 組ESA\_Group )

[1]> 1

選擇esalab.cisco.com必須屬於的群組。

1. ESA\_Group

2. New\_Group

[1]> 2

esalab.cisco.com設定為New\_Group組。

要重新命名ESA集群中的當前組，請使用 RENAMEGROUP命令：

(電腦esalab.cisco.com)> clusterconfig

此命令僅限於「集群」模式。 是否要切換至「叢集」模式？[Y]>

集群思科

選擇要執行的作業：

- ADDGROUP -增加群集組。

- SETGROUP -設定電腦所屬的組。

- RENAMEGROUP -重新命名群集組。

- DELETEDGROUP -刪除群集組。

- REMOVEMACHINE -從群集中刪除電腦。

- SETNAME -設定叢集名稱。

- LIST -

列出群集中的電腦。

- CONNSTATUS -顯示集群中電腦之間的連線狀態。

- 通訊-設定機器在叢集中通訊的方式。

- 中斷連線-暫時將電腦從叢集中斷連線。

- 重新連線-恢復與先前已斷開的電腦的連線。

- PREPJOIN -準備在CCS上增加新電腦。

[>重新命名組

選擇要重新命名的組。

1. ESA\_Group

2. New\_Group

[1]> 2

輸入群組的新名稱。

[New\_Group]> Cluster\_Group

Group New\_Group已重新命名為Cluster\_Group。

要從ESA集群中刪除當前組，請使用命令 DELETEDGROUP

(電腦esalab.cisco.com)> clusterconfig

此命令僅限於「集群」模式。 是否要切換至「叢集」模式？[Y]>

集群思科

選擇要執行的作業：

- ADDGROUP -增加群集組。

- SETGROUP -設定電腦所屬的組。

- RENAMEGROUP -重新命名群集組。

- DELETEDGROUP -刪除群集組。

- REMOVEMACHINE -從群集中刪除電腦。

- SETNAME -設定叢集名稱。

- LIST -列出群集中的電腦。

- CONNSTATUS -

顯示集群中電腦之間的連線狀態。

- 通訊-設定機器在叢集中通訊的方式。
- 中斷連線-暫時將電腦從叢集中斷連線。
- 重新連線-恢復與先前已斷開的電腦的連線。
- PREPJOIN -準備在CCS上增加新電腦。

```
[1]> DELETEDGROUP
```

選擇要移除的群組。

1. Cluster\_Group
2. ESA\_Group

```
[1]> 1
```

選擇必須將Cluster\_Group中的電腦移動到的組。

1. ESA\_Group

```
[1]> 1
```

群組Cluster\_Group已移除。



注意：在群集中增加/刪除電腦時，所做的更改會立即應用到裝置，而不會顯示commit。但是，對於ESA組，任何與其相關的操作僅在commit之後才應用到ESA。

---

#### 相關資訊

- [思科技術支援與下載](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。