

配置邮件安全设备(ESA)集群

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[问题](#)

[ESA上的集群](#)

[创建集群](#)

[通过SSH创建集群](#)

[通过CCS创建集群](#)

[通过SSH或CCS加入当前集群](#)

[通过SSH加入](#)

[通过CCS加入](#)

[在集群配置中迁移的内容](#)

[群集配置中未迁移的内容](#)

[如何在ESA集群中配置组](#)

[相关信息](#)

简介

本文档介绍如何在思科邮件安全设备(ESA)上设置集群。

先决条件

要求

Cisco 建议您了解以下主题：

- 如何将设备加入集群（集中管理）。
- 所有ESA必须具有相同的AsyncOS版本（一直到版本）。



注意：在8.5+版本中，集中管理密钥不再需要，添加时也不再可见，因为它是一个AsyncOS中的集成功能。

- 如果创建集群以使用端口22（更易于配置），请确保端口22流量上的设备之间不存在防火墙或路由问题。
- 如果创建集群以使用端口2222（集群通信服务），请确保制定防火墙规则以允许该端口上的流量可用，而不会被检测或中断。
- 群集配置选项必须通过ESA上的CLI完成，无法在GUI中创建或加入。

- 如果选择使用主机名进行通信，请确保设备上设置的DNS服务器能够解析网络中的所有其他设备，并且主机名解析的IP地址已分配给配置为侦听所选通信端口的接口。
- 确保在设备接口上启用所需的端口和服务（SSH或CCS）。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

问题在于，每当需要集中化一组ESA之间的配置并保持同步时，就无需在每个设备上持续进行修改。

ESA上的集群


通过ESA集中管理功能，您可以同时管理和配置多个设备，从而提高网络中的可靠性、灵活性和可扩展性。这样，您可以在遵守本地策略的同时进行全局管理。

集群由一组具有通用配置信息的计算机组成。在每个集群中，设备可以进一步划分为计算机组，其中一台计算机一次只能是一个组的成员。

集群在点对点架构中实施，没有主要/次要关系。您可以登录任何计算机以控制和管理整个集群或组。这样，管理员可以基于集群范围、组范围或每台计算机，基于自己的逻辑组配置系统的不同元素

创建集群

满足所有要求后，要创建集群，您需要在第一个设备的命令行(CLI)中开始。

 提示：在配置集群之前，请备份设备上的当前配置。在GUI中，依次选择System Administration > Configuration File。取消选中屏蔽的密码框并将配置本地保存到您的PC中。

通过SSH创建集群

```
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.
```

```
[1]> 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.

## 通过CCS创建集群

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
```


完成此步骤后，您就拥有了一个集群，并且所有配置都将从计算机移至集群级别。这是当其他计算机加入时所有计算机继承的配置。

## 通过SSH或CCS加入当前集群

本节介绍如何将之前或刚刚创建的任何新设备添加到当前集群中。使用任何一种方法加入当前集群的方法都类似，唯一的不同之处是CCS需要执行额外的步骤才能最终确认它，以便集群能够接受更新的设备。

### 通过SSH加入

---

 **注意：**需要使用SSH准确完成以下步骤中以粗体显示的部分，对于CCS的启用而言，您不能说“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 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. Please review the non-network settings. Ensure that the cluster settings are compatible with your network settings (e.g., DNS, NTP, etc. 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 C370.1ab? [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]>
```

检查后，设备成功加入集群。

## 通过CCS加入

这类似于方法，唯一的区别在于，在决定允许新设备进入当前集群之前，您需要登录到集群中处于活动状态的设备。

在集群中的活动设备上：

```
(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.
```

输入上一个代码示例中的SSH指纹(在登录尝试加入集群的设备时使用`clusterconfig prepjoin print`命令获得)并输入空行后，即完成准备加入。


---

 **注意：**如果运行 PREPJOIN 选项，则需要在辅助ESA上运行 `clusterconfig` 并将更改提交至主ESA之前，将该设备加入新配置的集群。此操作从整个操作的输出中标记此内容：要使用预共享密钥将此设备加入集群，请登录集群计算机，运行 `clusterconfig > prepjoin > new` 命令，输入下一个详细信息，然后输入 `commit` 您的更改。

---

然后，您可以在尝试加入的设备上开始加入进程，例如，将其称为**ESA2.lab**，以便与前一步骤的加入进程匹配。

---

 **注意：**下一个示例中为SSH-DSS密钥。

---

```
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]>
```

确认此情况后，您会看到SSH-DSS密钥。如果匹配，则可以接受这些术语，集群成功加入。

在集群配置中迁移的内容

集群配置迁移：

- 配置的策略设置
- 内容过滤器
- 文本资源
- 内容词典
- LDAP设置
- 反垃圾邮件和防病毒
- 全局设置
- 监听程序设置
- SMTP路由设置
- DNS设置

## 集群配置中未迁移的内容

### 群集配置不迁移：

- 设备本地主机名。
- 已配置IP接口。
- 配置的路由表。
- 本地垃圾邮件隔离区配置。
- 本地策略、病毒和爆发隔离区配置
- 命令行websecurityadvancedconfig 命令下的设置 ( 适用于版本8.5和更新版本 ) 。



**注意：**如果您具有引用不存在的隔离区的内容过滤器，则在计算机上配置引用的策略隔离区之前，这些内容过滤器将失效。

---

### 如何在ESA集群中配置组

在某些场景中，可能需要集群中的少数ESA以特定方式工作，而不是以其他方式工作。为此，您无需创建新的集群，并且您可以继续创建组。



---

注意：在组级别进行的配置优先于集群级别配置。

---

要创建组，请从ESA CLI创建组。要开始配置，请使用命令 `clusterconfig --> ADDGROUP`：

```
(计算机esalab.cisco.com)> clusterconfig
```

此命令仅限于“集群”模式。 是否要切换到“集群”模式？[Y]>

集群Cisco

选择要执行的操作：

- ADDGROUP -添加群集组。

- SETGROUP -设置计算机所属的组。
- RENAMEGROUP -重命名群集组。
- DELETEDGROUP -删除群集组。
- REMOVEMACHINE -从群集中删除计算机。
- SETNAME -设置群集名称。
- LIST -列出集群中的计算机。
- CONNSTATUS -显示集群中计算机之间的连接状态。
- 通信-配置计算机在集群内的通信方式。
- DISCONNECT -暂时将计算机从集群中分离。
- 重新连接-恢复与之前已断开的计算机的连接。
- PREPJOIN -准备通过CCS添加新计算机。

[> ADDGROUP

输入要创建的新群集组的名称。

[> New\_Group

已创建群集组New\_Group。

要将ESA从当前集群添加到创建的新组，请使用命令SETGROUP：

(计算机esalab.cisco.com)> clusterconfig

此命令仅限于“集群”模式。 是否要切换到“集群”模式？[Y]>

集群Cisco

选择要执行的操作：

- ADDGROUP -添加群集组。
- SETGROUP -设置计算机所属的组。
- RENAMEGROUP -重命名群集组。
- DELETEDGROUP -删除群集组。
- REMOVEMACHINE -从群集中删除计算机。
- SETNAME -设置群集名称。
- LIST -

列出集群中的计算机。

- CONNSTATUS -显示集群中计算机之间的连接状态。

- 通信-配置计算机在集群内的通信方式。

- DISCONNECT -暂时将计算机从集群中分离。

- 重新连接-恢复与之前已断开的计算机的连接。

- PREPJOIN -准备通过CCS添加新计算机。

[>]设置组

选择要移动到其他组的计算机。 使用逗号分隔多台计算机。

1. esalab.cisco.com ( 组ESA\_Group )

[1]> 1

选择esalab.cisco.com必须所属的组。

1. ESA\_Group

2. New\_Group

[1]> 2

esalab.cisco.com设置为New\_Group组。

要重命名ESA集群中的当前组，请使用命令 RENAMEGROUP：

(计算机esalab.cisco.com)> clusterconfig

此命令仅限于“集群”模式。 是否要切换到“集群”模式？[Y]>

集群Cisco

选择要执行的操作：

- ADDGROUP -添加群集组。

- SETGROUP -设置计算机所属的组。

- RENAMEGROUP -重命名群集组。

- DELETEDGROUP -删除群集组。

- REMOVEMACHINE -从群集中删除计算机。

- SETNAME -设置群集名称。

- LIST -

列出集群中的计算机。

- CONNSTATUS -显示集群中计算机之间的连接状态。

- 通信-配置计算机在集群内的通信方式。

- DISCONNECT -暂时将计算机从集群中分离。

- 重新连接-恢复与之前已断开的计算机的连接。

- PREPJOIN -准备通过CCS添加新计算机。

[>]重命名组

选择要重命名的组。

1. ESA\_Group

2. New\_Group

[1]> 2

输入组的新名称。

[New\_Group]> Cluster\_Group

Group New\_Group重命名为Cluster\_Group。

要从ESA集群中删除当前组，请使用命令 DELETGROUP

(计算机esalab.cisco.com)> clusterconfig

此命令仅限于“集群”模式。 是否要切换到“集群”模式？[Y]>

集群Cisco

选择要执行的操作：

- ADDGROUP -添加群集组。

- SETGROUP -设置计算机所属的组。

- RENAMEGROUP -重命名群集组。

- DELETGROUP -删除群集组。

- REMOVEMACHINE -从群集中删除计算机。

- SETNAME -设置群集名称。

- LIST -列出集群中的计算机。

- CONNSTATUS -

显示集群中计算机之间的连接状态。

- 通信-配置计算机在集群内的通信方式。

- DISCONNECT -暂时将计算机从集群中分离。

- 重新连接-恢复与之前已断开的计算机的连接。

- PREPJOIN -准备通过CCS添加新计算机。

```
[1]> DELETEDGROUP
```

选择要删除的组。

1. Cluster\_Group

2. ESA\_Group

```
[1]> 1
```

选择必须将Cluster\_Group中的计算机移动到的组。

1. ESA\_Group

```
[1]> 1
```

组Cluster\_Group已删除。



注意：在群集中添加/删除计算机时，所做的更改会立即应用到设备，而不会显示commit。但是，对于ESA组，与其相关的所有操作仅在commit之后才应用于ESA。

---

#### 相关信息

- [思科技术支持和下载](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。