Eメールセキュリティアプライアンス(ESA)クラスタの設定

内容

はじめに

このドキュメントでは、Cisco Eメールセキュリティアプライアンス(ESA)でクラスタをセットアップする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- アプライアンスをクラスタに参加させる方法（一元管理）
- すべての ESA で同じ AsyncOS バージョン（リビジョンまで）を持っていることが必須です。

注：バージョン8.5+では、一元管理キーはAsyncOS内の組み込み機能であるため、不要になり、追加しても表示されなくなります。

- ポート22（設定が簡単）を使用するクラスタを作成する場合、ポート22トラフィック上の

アプライアンス間にファイアウォールまたはルーティングの問題がないことを確認します。
- ポート2222（クラスター通信サービス）を使用するクラスターを作成する場合は、このポート上のトラフィックを検査または中断なしで使用できるようにファイアウォール規則が作成されていることを確認してください。
- クラスタ設定オプションは、ESA の CLI 経由で行う必要があり、GUI で作成したり、GUI に参加することはできません。
- 通信にホスト名を使用する場合は、アプライアンスに設定されたDNSサーバーがネットワーク内の他のすべてのアプライアンスを解決できること、およびホスト名の解決先のIPアドレスが、選択された通信ポートでリッスンするように構成されたインターフェイスに割り当てられていることを確認します。
- アプライアンスのインターフェイスで、必要なポートとサービス（SSHまたはCCS）が有効になっていることを確認します。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

問題は、大規模なESAグループ間の設定を一元化し、同期を維持する必要があるたびに、各アプライアンスで継続的に変更を行う必要がないことです。

ESAのクラスタ

ESAの一元管理機能を使用すると、複数のアプライアンスを同時に管理して設定し、ネットワーク内の信頼性、柔軟性、拡張性を向上させることができます。これにより、グローバルな管理が可能になると同時に、ローカル・ポリシーに準拠できます。

クラスタは、共通の設定情報を持つマシンのセットで構成されます。各クラスタ内で、アプライアンスはさらにマシン グループに分けることができます。ここで単独のマシンは一度に 1 つのグループのみでメンバーになれます。

クラスタは、プライマリ/セカンダリ関係のないピアツーピアアーキテクチャで実装されます。任意のマシンにログインして、クラスタ全体またはグループ全体を制御および管理できます。 これにより、管理者はシステムのさまざまな要素をクラスタ全体、グループ全体、またはマシンごとに、独自の論理グループに基づいて設定できます

クラスタの作成

すべての要件が満たされたら、クラスタを作成するために、最初のアプライアンスのコマンドラ

イン(CLI)から開始する必要があります。

ヒント：クラスタを設定する前に、アプライアンス上の現在の設定をバックアップしてください。GUI から、[System Management] > [Configuration File] に移動します。 マスクされたパスワードボックスのチェックを外し、設定をローカルのPCに保存します。

SSH経由でのクラスタの作成

```
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.lab?
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.lab 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.
```

CCS経由でのクラスタの作成

```
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
```

この手順が完了すると、クラスタが作成され、すべての設定がマシンからクラスタレベルに移行します。これは、他のすべてのマシンが参加時に継承する設定です。

SSHまたはCCSを使用した現行クラスタへの参加

このセクションでは、以前または直前に作成した現在のクラスタに新しいアプライアンスを追加する方法について説明します。どちらの方法でも現在のクラスタに参加する方法はアプローチが似ていますが、唯一重要な相違点は、クラスタが新しいアプライアンスを受け入れられるようにするには、CCSが追加の手順を実行してクラスタを終了する必要があることです。

SSHを介した参加

注：次の手順で太字で示されているセクションは正確に行う必要があります。SSHを使用する場合は、CCSをイネーブルにするために「yes」と発音しないでください。

```
<#root>

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
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.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]>
```

チェック後、アプライアンスはクラスタに正常に参加します。

CCSを通じて参加

これはアプローチが似ていますが、唯一の違いは、現在のクラスタに新しいアプライアンスを許可することを決定する前に、クラスタ内でアクティブなアプライアンスにログインする必要があることです。

クラスタ内のアクティブなアプライアンスで以下を実行します。

```
(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.
[]> XXXXXXXXXXXXX-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.
```

前のコード例で、SSHフィンガープリント(クラスタに参加しようとするアプライアンスにログインし、コマンドclusterconfig prepjoin printを使用して取得する)を入力して空白行を入力すると、準備参加が完了します。

注： PREPJOIN オプションを実行する場合、セカンダリESAで実行してアプライアンスを新しく設定したクラスタに参加させる前に、変更をプライマリESA clusterconfig にコミットする必要があります。 操作全体の出力からこれが示されます。事前共有キーを使用してアプライアンスをクラスタに参加させるには、クラスタマシンにログインし、 clusterconfig > prepjoin > new コマンドを実行し、次の詳細情報を入力して commit 変更します。

次に、参加を試みるアプライアンスで参加プロセスを開始します。たとえば、前の手順と一致させるために**ESA2.lab**という名前を付けます。

注:SSH-DSSキーは次の例です。

```
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]>
```

これが確認されると、SSH-DSSキーが表示されます。一致する場合は、条件を受け入れることができ、クラスタは正常に参加します。

クラスタ設定における移行対象

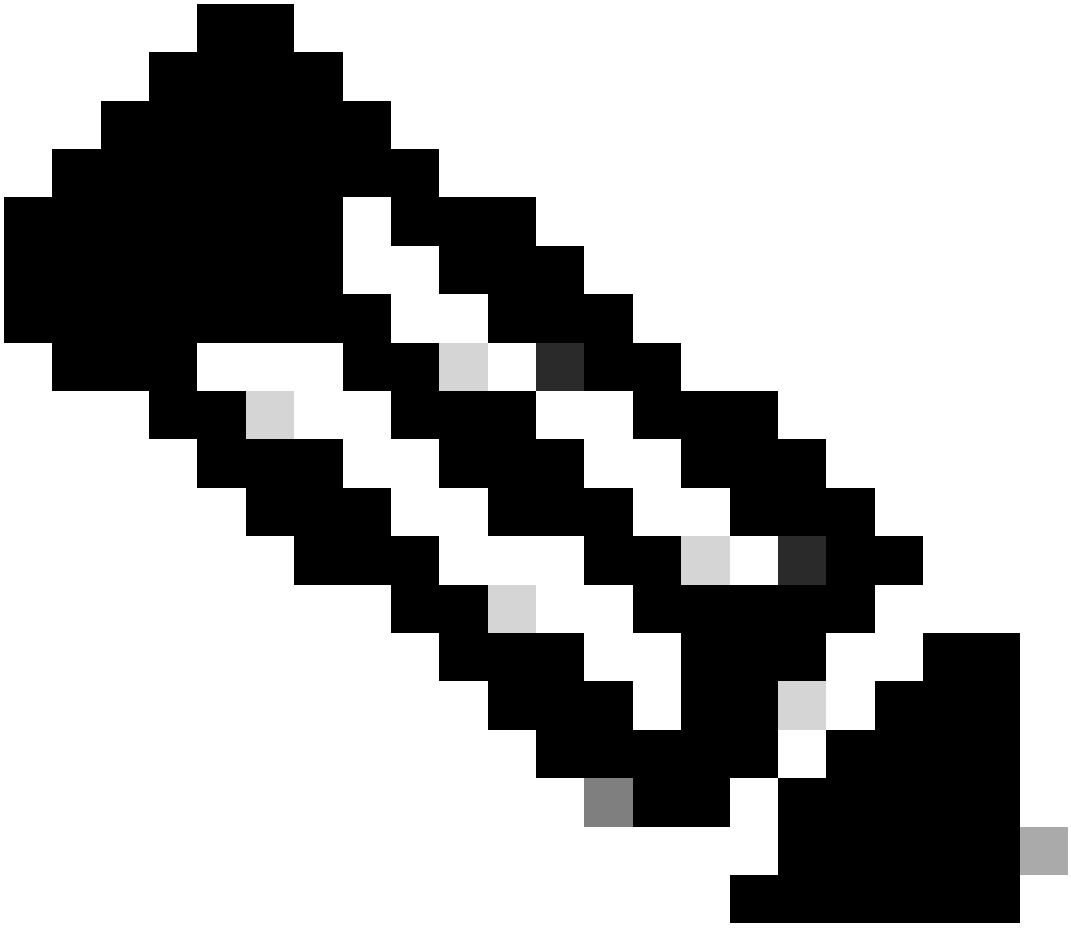
クラスタ設定の移行：

- ポリシー設定の構成
- コンテンツ フィルタ
- テキストリソース
- コンテンツ辞書
- LDAP設定
- アンチスパムおよびアンチウイルス
- グローバル設定
- リスナー設定
- SMTPルートの設定
- DNS設定

クラスタ設定における移行対象外

クラスタ構成は移行しません。

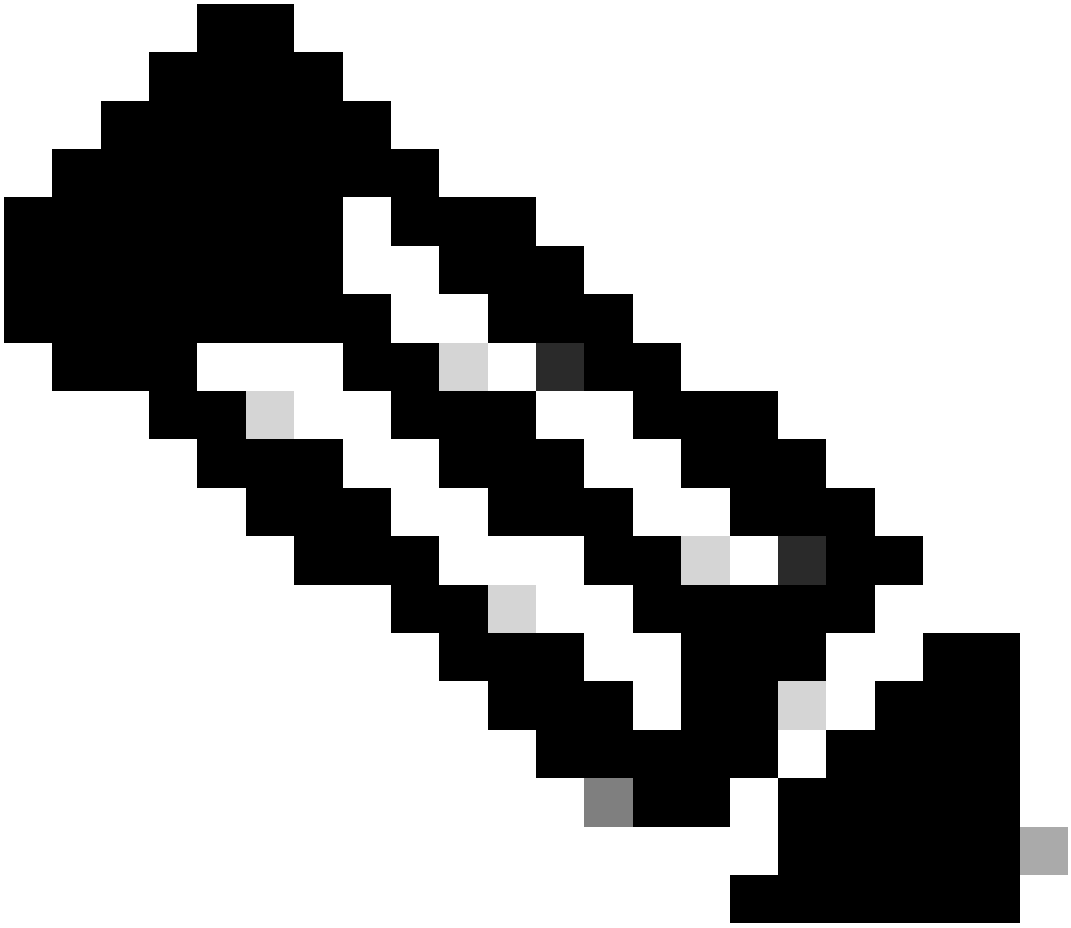
- アプライアンスのローカルなホスト名。
- 設定された IP インターフェイス。
- 設定されたルーティング テーブル。
- ローカル スパム隔離設定。
- ローカル ポリシー、ウイルスおよびアウトブレイク隔離設定
- コマンドラインのwebsecurityadvancedconfig コマンドでの設定（バージョン8.5以降）



注：存在しない隔離を参照するコンテンツフィルタがある場合、参照されるポリシー隔離がマシン上で設定されるまで、それらのフィルタは無効になります。

ESAクラスタでのグループの設定方法

特定のシナリオでは、クラスタ内の一部のESAが他のESAよりも特定の方法で動作することが必要になる場合があります。これを行うには、新しいクラスタを作成する必要はなく、グループの作成に進むことができます。



注：グループレベルで行われた設定は、クラスタレベルの設定よりも優先されます。

グループを作成するには、ESA CLIから作成します。設定を開始するには、 clusterconfig --> ADDGROUP コマンドを使用します。

(マシンesalab.cisco.com)> clusterconfig

このコマンドは「クラスタ」モードに制限されています。 「クラスタ」モードに切り替えますか？[Y]>

クラスタCisco

実行する操作を選択します。

- ADDGROUP – クラスタグループを追加します。

- SETGROUP – マシンが属するグループを設定します。

- RENAMEGROUP – クラスタグループ名を変更します。

- DELETEGROUP – クラスタグループを削除します。

- REMOVEMACHINE – クラスターからコンピューターを削除します。

- SETNAME – クラスタ名を設定します。

- LIST – クラスタ内のマシンを一覧表示します。

- CONNSTATUS – クラスタ内のマシン間の接続状態を表示します。

- COMMUNICATION – クラスタ内でマシンが通信する方法を設定します。

- DISCONNECT – クラスターからコンピューターを一時的に切断します。

- RECONNECT – 以前に切断されたマシンとの接続を復元します。

- PREPJOIN - CCS上に新しいマシンを追加する準備をします。

[]> ADDGROUP

作成する新しいクラスタグループの名前を入力します。

[]> New_Group

クラスタグループNew_Groupが作成されました。

現在のクラスタのESAを新しく作成したグループに追加するには、SETGROUPコマンドを使用します。

(マシンesalab.cisco.com)> clusterconfig

このコマンドは「クラスタ」モードに制限されています。 「クラスタ」モードに切り替えますか？[Y]>

クラスタCisco

実行する操作を選択します。

- ADDGROUP – クラスタグループを追加します。

- SETGROUP – マシンが属するグループを設定します。

- RENAMEGROUP – クラスタグループ名を変更します。

- DELETEGROUP – クラスタグループを削除します。

- REMOVEMACHINE – クラスターからコンピューターを削除します。

- SETNAME – クラスタ名を設定します。

- LIST –

クラスタ内のマシンを一覧表示します。

- CONNSTATUS – クラスタ内のマシン間の接続状態を表示します。

- COMMUNICATION – クラスタ内でマシンが通信する方法を設定します。

- DISCONNECT – クラスターからコンピューターを一時的に切断します。

- RECONNECT – 以前に切断されたマシンとの接続を復元します。

- PREPJOIN - CCS上に新しいマシンを追加する準備をします。

[]> SETGROUP

別のグループに移動するマシンを選択します。 複数のマシンはカンマで区切ります。

1. esalab.cisco.com（グループESA_Group）

[1]> 1

esalab.cisco.comがメンバーである必要があるグループを選択します。

1. ESA_グループ

2. New_Group（新規グループ）

[1] > 2

esalab.cisco.comをグループNew_Groupに設定します。

ESAクラスタの現在のグループの名前を変更するには、 RENAMEGROUPコマンドを使用します。

(マシンesalab.cisco.com)> clusterconfig

このコマンドは「クラスタ」モードに制限されています。 「クラスタ」モードに切り替えますか？[Y]>

クラスタCisco

実行する操作を選択します。

- ADDGROUP – クラスタグループを追加します。

- SETGROUP – マシンが属するグループを設定します。

- RENAMEGROUP – クラスタグループ名を変更します。

- DELETEGROUP – クラスタグループを削除します。

- REMOVEMACHINE – クラスターからコンピューターを削除します。

- SETNAME – クラスタ名を設定します。

- LIST –

クラスタ内のマシンを一覧表示します。

- CONNSTATUS – クラスタ内のマシン間の接続状態を表示します。

- COMMUNICATION – クラスタ内でマシンが通信する方法を設定します。

- DISCONNECT – クラスターからコンピューターを一時的に切断します。

- RECONNECT – 以前に切断されたマシンとの接続を復元します。

- PREPJOIN - CCS上に新しいマシンを追加する準備をします。

[]>名前グループの変更

名前を変更するグループを選択します。

1. ESA_グループ

2. New_Group（新規グループ）

[1] > 2

グループの新しい名前を入力します。

[New_Group]> Cluster_Group

グループNew_Groupの名前がCluster_Groupに変更されました。

ESAクラスタから現在のグループを削除するには、次のコマンドを使用します DELETEGROUP

(マシンesalab.cisco.com)> clusterconfig

このコマンドは「クラスタ」モードに制限されています。 「クラスタ」モードに切り替えますか？[Y]>

クラスタCisco

実行する操作を選択します。

- ADDGROUP – クラスタグループを追加します。

- SETGROUP – マシンが属するグループを設定します。

- RENAMEGROUP – クラスタグループ名を変更します。

- DELETEGROUP – クラスタグループを削除します。

- REMOVEMACHINE – クラスターからコンピューターを削除します。

- SETNAME – クラスタ名を設定します。

- LIST – クラスタ内のマシンを一覧表示します。

- CONNSTATUS –

クラスタ内のマシン間の接続状態を表示します。

- COMMUNICATION – クラスタ内でマシンが通信する方法を設定します。

- DISCONNECT – クラスターからコンピューターを一時的に切断します。

- RECONNECT – 以前に切断されたマシンとの接続を復元します。

- PREPJOIN - CCS上に新しいマシンを追加する準備をします。

[]> DELETEGROUP

削除するグループを選択します。

1. Cluster_Group

2. ESA_グループ

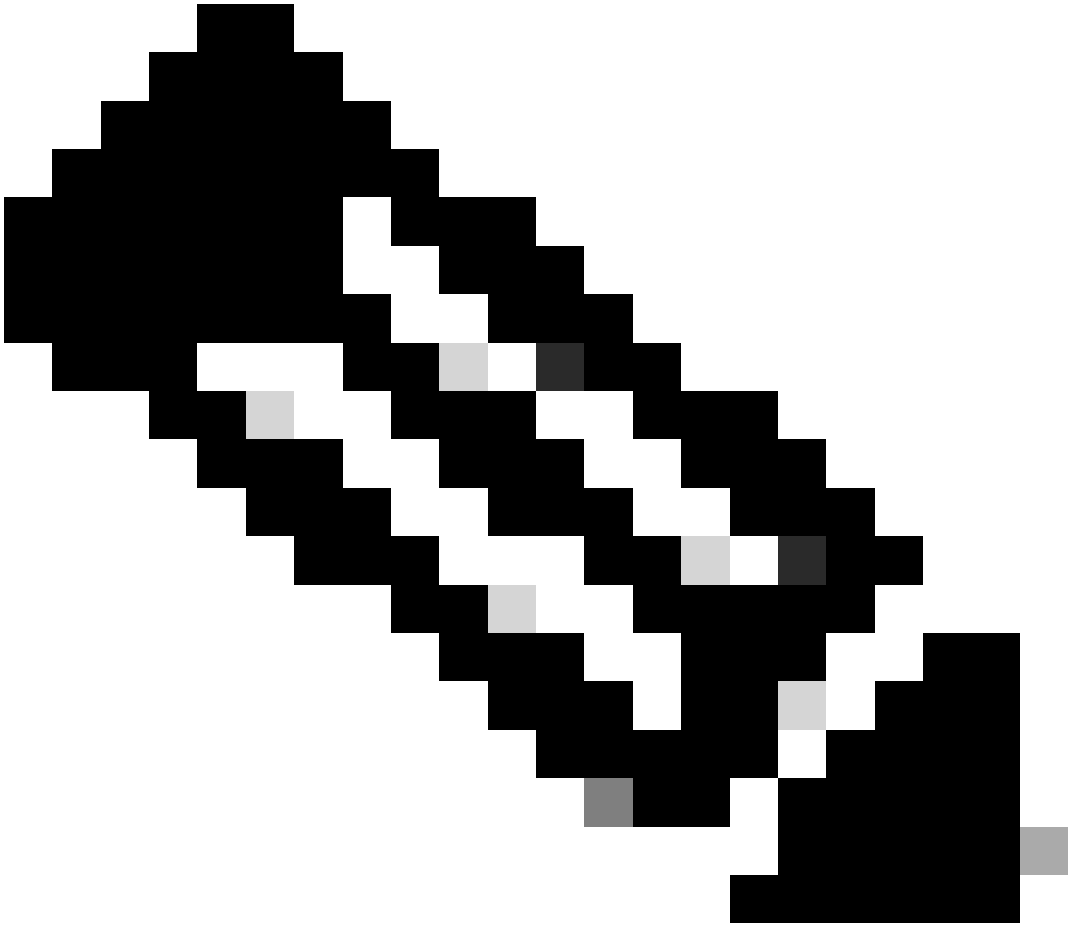
[1]> 1

Cluster_Group内のマシンの移動先のグループを選択します。

1. ESA_グループ

[1]> 1

グループCluster_Groupが削除されました。



注：クラスタ内のマシンを追加または削除すると、変更はcommitを実行せずに即座にアプライアンスに適用されます。一方、ESAグループでは、それに関連するアクションはcommitの実行後にのみESAに適用されます。

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。