クラスタを使用した中央集中型管理

この章は、次の項で構成されています。

クラスタを使用した中央集中型管理の概要

シスコの中央集中型管理機能を使用して複数のアプライアンスを同時に管理、設定することにより、管理に要する時間を短縮し、ネットワーク全体で設定の一貫性を確保することができます。複数のアプライアンスを管理するためにハードウェアを追加購入する必要はありません。中央集中型管理機能によって、ネットワーク内の信頼性、柔軟性、およびスケーラビリティが向上し、ローカル ポリシーを順守しながらグローバルな管理を行うことができます。

クラスタ とは、設定情報を共有する一連のマシンのことです。クラスタの内部では、マシン（Cisco アプライアンス）がグループに分割されます。どのクラスタにも 1 つ以上のグループがあります。個々のマシンは、必ずいずれかのグループのメンバになります。管理者ユーザは、システムのさまざまな要素をクラスタ単位、グループ単位、またはマシン単位で設定できます。これにより、Cisco アプライアンスを、ネットワーク、地域、部署、または論理的な関係に基づいて分割できます。

クラスタはピアツーピア アーキテクチャで実装されるため、クラスタ内にマスター/スレーブの関係は存在しません。どのマシンにログインしても、クラスタの制御と管理を行うことができます。（ただし、一部のコンフィギュレーション コマンドは制限されます。制限コマンド（16 ページ） を参照してください）。

ユーザデータベースはクラスタ内のすべてのマシン間で共有されます。つまり、ユーザのセットと管理者（および対応するパスフレーズ）はクラスタ全体で1つしか存在しません。クラスタに参加するすべてのマシンは1つの管理者パスフレーズを共有します。これをクラスタの管理パスフレーズと呼びます。

（注） 1つのクラスタに20を超えるアプライアンスがあると、クラスタの通信におけるエラーの原因となる可能性があります。

クラスタの要件

- クラスタ内の各マシンには、DNS で解決可能なホスト名が必要です。代わりに IP アドレスを使用することもできますが、両者を混在させることはできません。

  DNS とホスト名の解決 （21 ページ）を参照してください。クラスタの通信は、通常、マシンの DNS ホスト名を使って開始されます。

- 1 つのクラスタは、全体として同じバージョンの AsyncOS を実行しているマシンで構成されている必要があります。

  クラスタのメンバをアップグレードする方法については、クラスタ内のマシンのアップグレード （14 ページ）を参照してください。

- 各マシンは、SSH（通常はポート 22）と Cluster Communication Service（CCS）のいずれかを使ってクラスタに参加できます。

  クラスタ通信 （20 ページ）を参照してください。

- クラスタに参加したマシンは、SSH または CCS 経由で通信できます。使用するポートは設定可能です。SSH は通常ポート 22 上でイネーブルになっており、CCS はデフォルトでポート 2222 上でイネーブルになっていますが、どちらのサービスも別のポートに設定できます。

  アプライアンスに対して開く必要がある通常のファイアウォールポートに加えて、クラスタ化されたマシンが CCS 経由で通信する場合は、各マシンが CCS ポート経由で相互に接続できる必要があります。クラスタ通信 （20 ページ）を参照してください。

- マシンのクラスタの作成、クラスタへの参加、およびクラスタの設定を行うには、CLI（コマンド ライン インタフェース）の **clusterconfig** コマンドを使用する必要があります。

  クラスタを作成した後は、クラスタ以外の設定を GUI または CLI から管理できます。

  クラスタの作成とクラスタへの参加 （4 ページ）およびGUI でのクラスタの管理 （18 ページ）を参照してください。

- アプライアンスで二要素認証を有効にしている場合は、事前共有キーを使用してクラスタマシンに参加させることができます。CLI の `clusterconfig > prepjoin` コマンドを使用して、この設定を構成します。

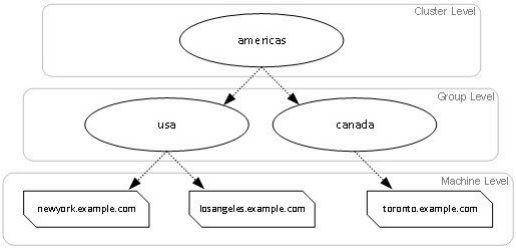
または

クラスタを作成したりそれに参加したりする前に、E メール セキュリティ アプライアンスで二要素認証を無効にします。詳細については、二要素認証の無効化を参照してください。

クラスタの構成

クラスタでは、設定情報が3つのグループ（レベル）に分かれています。最上位レベルはクラスタの設定、中位レベルはグループの設定、最下位レベルはマシンごとの設定をそれぞれ表します。

図 *1*: クラスタのレベル階層



各レベルには、設定が可能なメンバが1つ以上存在します。これらをモードと呼びます。モードは特定のレベルに含まれる名前の付いたメンバを表します。たとえば、「usa」グループは図に示した2つのグループ モードの1つです。レベルは一般的な用語ですが、モードは具体的なものを示します。モードは常に名前で参照されます。上の図に示されているクラスタは、6つのモードを持っています。

設定は特定のレベルで設定されますが、それらは常に特定のモードに対して設定されます。すべてのモードに対する設定を1つのレベルで設定する必要はありません。クラスタ モードは特別なケースです。クラスタは1つしか存在しないため、クラスタ モードの設定はすべてクラスタ レベルで設定されると言えます。

通常、ほとんどの設定はクラスタ レベルで設定する必要があります。ただし、下位レベルで個別に設定された設定は上位レベルで設定された設定よりも優先されます。したがって、クラスタ モードの設定をグループ モードやマシン モードの設定で上書きできます。

たとえば、最初にクラスタ モードでグッド ネイバー テーブルを設定し、クラスタ内のすべてのマシンでその設定を使用するとします。次に、このテーブルをマシン モードでマシン newyork 用に設定します。この場合、クラスタ内の他のすべてのマシンは引き続きクラスタ レベルで定義されたグッド ネイバー テーブルを使用しますが、マシン newyork はクラスタの設定をマシン モードの個別の設定で上書きします。

特定のグループやマシン用にクラスタの設定を上書きする機能によって、非常に柔軟な設定が可能になります。ただし、多くの設定をマシン モードで個別に設定すると、クラスタの当初の目的である管理のしやすさが大きく損なわれます。

初期設定

ほとんどの機能については、新しいモードで設定を始めたときのデフォルトの初期設定は空です。設定が空であることとモードの設定が存在しないことは明確に区別されます。例として、1 つのグループと 1 台のマシンからなる非常に簡単なクラスタを考えます。LDAP クエリーがクラスタ レベルで設定されているとします。グループ レベルとマシン レベルでは何も設定されていません。

クラスタ	(ldap queries: a, b, c)
グループ	
マシン（Machine）	

ここで、グループに対して新しいLDAPクエリーの設定を作成したとします。その結果は次のようになります。

クラスタ	(ldap queries: a, b, c)
グループ	(ldap queries: None)
マシン（Machine）	

すると、クラスタ レベルの設定がグループ レベルの設定で上書きされますが、新しいグループ設定は初期状態では空です。グループ モードには、独自に設定された LDAP クエリーが実際には存在しません。このグループ内のマシンは、この「空の」LDAPクエリーをグループから継承します。

次に、このグループに次のような LDAP クエリーを追加します。

クラスタ	(ldap queries: a, b, c)
グループ	(ldap queries: d)
マシン（Machine）	

これで、クラスタ レベルで設定されたクエリーとは別に、グループにもクエリーが設定されました。マシンはグループのクエリーを継承します。

クラスタの作成とクラスタへの参加

クラスタの作成とクラスタへの参加は、グラフィカル ユーザ インターフェイス（GUI）からはできません。クラスタの作成、クラスタへの参加、およびクラスタの設定を行うには、コマンドライン インターフェイス（CLI）を使用する必要があります。クラスタの作成後は、GUI と CLI のどちらからも設定を変更できます。

注意 アプライアンスで二要素認証を有効にしている場合は、事前共有キーを使用してクラスタ マシンに参加させることができます。CLI の `clusterconfig > prepjoin` コマンドを使用して、この設定を構成します。

または

クラスタを作成したりそれに参加したりする前に、E メール セキュリティ アプライアンスで二要素認証を無効にします。詳細については、二要素認証の無効化を参照してください。

clusterconfig コマンド

マシン上でクラスタの作成やクラスタへの参加を行うには、`clusterconfig` コマンドを使用します。

- 新しいクラスタを作成すると、そのクラスタのすべての初期設定はそのクラスタを作成したマシンから継承されます。マシンがすでに「スタンドアロン」モードで設定されている場合は、クラスタを作成したときにそのスタンドアロンの設定が使用されます。
- マシンがクラスタに参加すると、そのマシンのすべてのクラスタ化可能な設定がクラスタ レベルから継承されます。つまり、そのマシン固有の設定（IP アドレスなど）を除くすべての設定が消失し、そのマシンが参加したクラスタ、グループ、またはその両方の設定に置き換わります。マシンがすでに「スタンドアロン」モードで設定されている場合は、クラスタを作成するときにそのスタンドアロンの設定が使用され、マシン レベルの設定は保持されません。

現在のマシンがまだクラスタに含まれていない場合は、`clusterconfig` コマンドを実行すると、既存のクラスタに参加するか、新しいクラスタを作成するかのオプションが表示されます。

この時点で、新しいクラスタにマシンを追加できます。これらのマシンは、SSH または CCS を使用して通信できます。

```
newyork.example.com> 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.

[]> americas

New cluster committed: Wed Jun 22 10:02:04 2005 PDT

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

Cluster americas
```

```
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.

- LISTDETAIL - List the machines in the cluster with detail.

- 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.

[]>
```

既存のクラスタへの参加

既存のクラスタに参加するには、クラスタに追加するホスト上で clusterconfig コマンドを実行します。SSH と CCS のどちらを使用してクラスタに参加するかを選択できます。

既存のクラスタにホストを参加させるには、次の要件を満たす必要があります。

- クラスタ内のマシンの SSH ホスト キーを検証できること
- クラスタ内のマシンの IP アドレスを知っており、そのマシンに（SSH や CCS 経由で）接続できること
- クラスタに属するマシン上の管理ユーザの管理者パスフレーズを知っていること

SSH を使った既存クラスタへの参加

次の表に、SSH オプションを使ってマシン「losangeles.example.com」をクラスタに追加する例を示します。

```
losangeles.example.com> 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 ->
hostkeyconfig -> fingerprint.


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

Do you want to enable the Cluster Communication Service on
losangeles.example.com? [N]> n

Enter the IP address of a machine in the cluster.

[]> IP address is entered

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

[22]> 22

Enter the admin passphrase for the cluster.
The administrator passphrase for the clustered machine is entered

Please verify the SSH host key for IP address:

Public host key fingerprint: xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx

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

Joining cluster group Main_Group.

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

Cluster americas

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.

- LISTDETAIL - List the machines in the cluster with detail.

- 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.

[]>
```

```
(Cluster americas)>
```

CCS を使った既存クラスタへの参加

SSH を使用できない場合は、代わりに CCS を使用します。CCS の唯一の利点は、そのポートではクラスタ通信しか行われない（ユーザ ログインや SCP などは行われない）ことです。CCS を使って既存のクラスタにマシンを追加するには、clusterconfig の `prepjoin` サブコマンドを使ってクラスタに追加するマシンの準備を行います。次の例では、マシン「newyork」上で `prepjoin` コマンドを実行して、クラスタに追加するマシン「losangeles」の準備を行っています。

`prepjoin` コマンドを実行してから、クラスタに追加するホストの CLI で「`clusterconfig prepjoin print`」と入力し、現在クラスタに含まれているホストのコマンドラインにキーをコピーすることにより、クラスタに追加するホストのユーザ キーを取得します。

マシンがクラスタに追加された後は、`clusterconfig` コマンドを使ってクラスタのさまざまな設定が可能です。

```
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.

- LISTDETAIL - List the machines in the cluster with detail.

- 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.

[]> losangeles.example.com
```

```
Enter the serial number of the host mail3.example.com.

[]> unique serial number is added

Enter the user key of the host losangeles.example.com. This can be obtained by typing
"clusterconfig prepjoin print" in the CLI on mail3.example.com. Press enter on a blank
line to finish.


unique user key from output of prepjoin print is pasted

Host losangeles.example.com added.

Prepare Cluster Join Over CCS

1. losangeles.example.com (serial-number)

Choose the operation you want to perform:

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

- DELETE - Remove a host from the pending join list.

[]>


(Cluster Americas)> clusterconfig

Cluster americas

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.

- LISTDETAIL - List the machines in the cluster with detail.

- 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.

[]>
```

事前共有キーによる SSH を使った既存クラスタへの参加

次の表は、事前共有キーを使用して SSH 経由でマシン（testmachine.example.com）を（test_cluster）クラスタに参加させる方法を示しています。

```
testmachine.example.com> 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 ->
hostkeyconfig -> fingerprint.

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

Do you want to enable the Cluster Communication Service on
testmachine.example.com? [N]>

Enter the IP address of a machine in the cluster.

[]> IP address entered

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

[22]>

Would you like to join this appliance to a cluster using pre-shared keys?
Use this option if you have enabled two-factor authentication on the appliance.) [Y]>
yes

To join this appliance to a cluster using pre-shared keys, log in to the cluster machine,

run the clusterconfig > prepjoin > command, enter the
following details, and commit your changes.
Host: pod1226-esa07.ibesa
Serial Number: 42291A18D741EDB4C601-BC14E5579F34
User Key:

ssh-dss
AAAAB3NzaC1kc3MAAACBAJ6Xm+ja4aau9n4DOcJs/gGwEDEUWgERYchhgWApKt6IW+s58I7knGM81rQgQbNdNCO58D
EqaVGmP0Vyb0TTpgvh6f0mr80OuTgWh9bqg4uiOJvbKvlTvDt0o7//mTklm159zr2KT/qFH+9L5i+8iIMX62R5y+a
6E8JV0BrJCNAAAAFQCmK+WOu9HSribsC0f/5dVoADdxEwAAAIA5p7NR74rlSrs0JWWYItNAtE1SamAN+gqCOdUWGPPHT
qdrtBIlPQ9tfFoThZElqY4Tx8lku9laasoRLruQ2Z36R3bQGzIn4jzQqujvvbxTvLK9eLoSr8yFbEE3ZvuUo0+vhDn
LIDX2N65AQSQsTaOrKX+yQZ8yAVt48CsctpsDrgAAAIAVROGlWoSl8g3FFm2eRTa+/oZ+cMjv+pSZiZoiUCoaIlouc
u1ZDpN413QBnf6p/3D8wVD8m5uo8O4N/HXasAMektZvGoP4Sf+shItPuISRv3lrMTEYsD0sqVcMc7vIXUeD2jpOk7MB
ooVkTZB/rdTbNMfXrhDkNJ2IAPQQiUKVnw==

Before you proceed to the next step, make sure you add the 'Host', Serial Number' and
'User Key'
details to the cluster machine.
```

```
Would you like to continue? [Y]> yes

Joining cluster group Main_Group.

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

Cluster test_cluster

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.

- LISTDETAIL - List the machines in the cluster with detail.

- 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.

[]>

(Cluster test_cluster)>
```

グループの追加

すべてのクラスタには1つ以上のグループが含まれている必要があります。新しいクラスタを作成すると、「**Main_Group**」という名前のデフォルトのグループが自動的に作成されます。しかし、クラスタ内に追加のグループを作成することもできます。次の例は、既存のクラスタ内に追加のグループを作成し、そのグループにマシンを割り当てる方法を示しています。

手順

ステップ1 **clusterconfig** コマンドを実行します。

ステップ2 **addgroup** サブコマンドを選択し、新しいグループの名前を入力します。

ステップ3 **setgroup** サブコマンドを使用して、新しいグループに割り当てるマシンを選択します。

クラスタの管理

CLI でのクラスタの管理

クラスタに含まれるマシンでは、CLI を異なるモードに切り替えることができます。モードはあるレベルに含まれる特定の（名前の付いた）メンバを表していることを思い出してください。

CLI のモードに応じて、設定が変更される正確な場所が決まります。デフォルトは、ユーザがログインしたマシン（「ログイン ホスト」）を示す「マシン」モードです。

別のモードに切り替えるには、clustermode コマンドを使用します。

表 *1:* クラスタの管理

コマンドの例	説明
`clustermode`	クラスタ モードへの切り替えを確認するプロンプトが表示されます。
`clustermode group northamerica`	グループ「northamerica」用のグループ モードに切り替わります。
`clustermode machine losangeles.example.com`	マシン「losangeles」用のマシン モードに切り替わります。

CLI プロンプトの表示が現在のモードに変わります。

```
(Cluster Americas)>
```

または

```
(Machine losangeles.example.com)>
```

マシン モードでは、プロンプトにマシンの完全修飾ドメイン名が表示されます。

設定のコピーと移動

すべての非制限コマンド（制限コマンド （16 ページ）を参照）に、新しい操作として **CLUSTERSHOW** と **CLUSTERSET** が追加されました。**CLUSTERSHOW** は、コマンド設定のモードを表示するときに使用します（新たに追加された操作 （16 ページ）を参照）。**CLUSTERSET** 操作は、（現在のコマンドで設定できる）現在の設定をモード間またはレベル間で（たとえば、あるマシンからあるグループへ）移動またはコピーするときに使用します。

コピー すると、現在のモードの設定が保持されます。移動 すると、現在のモードの設定がリセット（クリア）されます。つまり、移動した後は、現在のモードに設定が設定されなくなります。

たとえば、（**destconfig** コマンドで）グループ **northamerica** にグッド ネイバー テーブルを設定し、クラスタ全体にこの設定を適用する場合は、**destconfig** コマンド内で **clusterset** 操作を使って現在の設定をクラスタ モードにコピー（または移動）できます。（新しい設定の実験 （13 ページ） を参照）。

注意 設定を移動またはコピーするときは、依存関係に矛盾が生じないように注意してください。たとえば、免責事項のスタンプが設定されたリスナーを別のマシンに移動またはコピーしても、その新しいマシンに同じ免責事項が設定されていない場合、新しいマシンでは免責事項のスタンプがイネーブルになりません。

新しい設定の実験

クラスタの最も効果的な使用方法の1つは、新しい設定を実験することです。まず、分離された環境で、マシンモードでの変更を行います。次に、設定に問題がなければ、設定変更を上位のクラスタ モードに移動し、すべてのマシンに適用します。

次の例は、あるマシンでリスナーの設定を変更し、準備ができたらその設定をクラスタの残りのマシンにパブリッシュする手順を示しています。通常、リスナーはクラスタ レベルで設定されるため、この例では最初に設定をあるマシンのマシン モードに格下げしてから、設定の変更を行い、テストしています。このような実験的な変更は、クラスタ内の他のマシンで同じ変更を行う前に、1 つのマシン上でテストする必要があります。

手順

ステップ 1 **clustermode cluster** コマンドを使ってクラスタ モードに変更します。

clustermode コマンドは、モードをクラスタ、グループ、およびマシン レベルに変更するときに使用する CLI コマンドです。

ステップ 2 **listenerconfig** を実行して、クラスタに設定されたリスナーの設定を表示します。

ステップ 3 実験するマシンを選び、clusterset コマンドを使って設定をクラスタから「下位の」マシン モードにコピーします。

ステップ 4 次のように clustermode コマンドを使って実験マシンのマシン モードに移行します。

```
clustermode machine newyork.example.com
```

ステップ 5 実験マシンのマシン モードで listenerconfig コマンドを実行し、実験マシンに固有の変更を行います。

ステップ 6 変更を確定します。

ステップ 7 実験マシン上で設定変更の実験を続行し、必ず変更を確定します。

ステップ 8 新しい設定を他のすべてのマシンに適用する準備ができたら、clustersetコマンドを使って設定を上位のクラスタ モードに移動します。

ステップ 9 変更を確定します。

クラスタからの脱退（削除）

マシンをクラスタから永続的に削除するには、clusterconfig の REMOVEMACHINE 操作を使用します。マシンをクラスタから永続的に削除すると、その設定は「平板化」され、そのマシンはクラスタに含まれていたときと同じように動作します。たとえば、クラスタ モードのグローバル配信停止テーブルしかない場合にマシンをクラスタから削除すると、そのグローバル配信停止テーブルのデータがマシンのローカル設定にコピーされます。

クラスタ内のマシンのアップグレード

クラスタには、異なるバージョンの AsyncOS を実行しているマシンを接続できません。

AsyncOS のアップグレードをインストールする前に、clusterconfig コマンドを使ってクラスタ内の各マシンを切断する必要があります。すべてのマシンをアップグレードしたら、clusterconfig コマンドを使ってクラスタを再接続します。マシンを同じバージョンにアップグレードする間は、2 つのクラスタを別個に稼働させることができます。また、GUI の [アップグレード（Upgrades）] ページでクラスタ化されたマシンをアップグレードすることもできます。

バックグラウンドでアップグレードをダウンロードできるため、アップグレードをインストールする準備が整うまで、クラスタ内のマシンを切断する必要はありません。

（注） クラスタから個々のマシンを切断する前にアップグレード コマンドを使用すると、AsyncOS によってクラスタ内のすべてのマシンが切断されます。マシンをアップグレードする前に、各マシンをクラスタから切断することを推奨します。各マシンを切断してアップグレードしている間、他のマシンは引き続きクラスタとして動作します。

手順

ステップ 1 クラスタ内のマシン上で、clusterconfig の disconnect 操作を使用します。たとえば、マシン losangeles.example.com を切断するには、clusterconfig disconnect losangeles.example.com と入力します。commit は必要ありません。

ステップ 2 必要に応じて、suspendlistenerコマンドを使ってアップグレード処理中の新しい接続やメッセージの受信を停止します。

ステップ 3 upgrade コマンドを実行して、AsyncOS を新しいバージョンにアップグレードします。

（注） クラスタ内のマシンをすべて切断するように求める警告または確認メッセージは無視してください。マシンがすでに切断されているため、この時点で AsyncOS によってクラスタ内の他のマシンが切断されることはありません。

ステップ 4 マシンの AsyncOS のバージョンを選択します。アップグレードが完了すると、マシンが再起動します。

ステップ 5 アップグレードされたマシン上で resume コマンドを使って新しいメッセージの受信を開始します。

ステップ 6 クラスタ内のマシンごとにステップ 1 ～ 5 を繰り返します。

（注） クラスタからマシンを切断すると、そのマシンを使って他のマシンの設定を変更できなくなります。クラスタの設定を変更することはできますが、設定の同期が取れなくなるため、マシンが切断されている間は設定を変更しないでください。

ステップ 7 すべてのマシンをアップグレードした後で、アップグレードされたマシンごとに clusterconfig の reconnect 操作を実行してマシンを再接続します。たとえば、マシン losangeles.example.com を切断するには、clusterconfig reconnect losangeles.example.com と入力します。クラスタに接続できるのは、同じバージョンの AsyncOS を実行しているマシンだけです。

CLI コマンドのサポート

すべてのコマンドがクラスタに対応

AsyncOS のすべての CLI コマンドがクラスタ対応になりました。一部のコマンドは、クラスタモードで実行したときの動作がやや異なります。たとえば、次のコマンドをクラスタに含まれるマシン上で実行すると、コマンドの動作が変更されます。

commit および clearchanges コマンド

commit

commit コマンドは、現在のモードに関係なく、すべての変更をクラスタの 3 つのレベルのすべてで確定します。

commitdetail

commitdetail コマンドは、クラスタ内のすべてのマシンに反映された設定変更の詳細を表示します。

clearchanges

clearchanges（clear）コマンドは、現在のモードに関係なく、すべての変更をクラスタの 3 つのレベルのすべてでクリアします。

新たに追加された操作

CLUSTERSHOW

各コマンドに、コマンド設定時のモードを表示する CLUSTERSHOW 操作が追加されました。

下位レベルの既存の設定で上書きされる操作を実行するCLIコマンドを入力すると、通知メッセージが表示されます。たとえば、クラスタモードでコマンドを入力すると、次のような通知メッセージが表示されることがあります。

```
Note: Changes to these settings will not affect the following groups and machines
because they are overriding the cluster-wide settings:

East_Coast, West_Coast

facilities_A, facilities_B, receiving_A
```

グループ モードの設定を編集した場合も、同じようなメッセージが表示されます。

制限コマンド

ほとんどの CLI コマンドとそれに対応する GUI ページは、任意のモード（クラスタ、グループ、マシン）で実行できます。しかし、一部のコマンドとページは1つのモードだけに制限されています。

システム インターフェイスには（GUI と CLI のどちらにも）、コマンドが制限されること、およびどのように制限されるかが必ず明示されます。コマンドを設定するための適切なモードに簡単に切り替えることができます。

- GUI では、[モードを変更（Change Mode）] メニューまたは [この機能の設定は現在、次で定義されています：（Settings for this features are currently defined at:）] リンクを使ってモードを切り替えます。
- CLI では、clustermode コマンドを使ってモードを切り替えます。

表 *2:* クラスタ モードに制限されるコマンド

clusterconfig	sshconfig
clustercheck	userconfig
passwd	

上記のコマンドをグループ モードまたはマシン モードで実行しようとすると、警告メッセージが表示され、適切なモードに切り替えることができます。

（注） passwd コマンドは、ゲスト ユーザが使用できるようにするための特例です。ゲスト ユーザがクラスタ内のマシン上で passwd コマンドを実行すると、警告メッセージは表示されず、ユーザのモードを変更せずにクラスタ レベルのデータに対して操作が行われます。他のすべてのユーザに対しては、上記の（他の制限されるコンフィギュレーション コマンドと同じ）動作が行われます。

次のコマンドは、マシン モードに制限されます。

antispamstatus	etherconfig	resume	suspenddel
antispamupdate	featurekey	resumedel	suspendlistener
antivirusstatus	hostrate	resumelistener	techsupport
antivirusupdate	hoststatus	rollovernow	tophosts
bouncerecipients	interfaceconfig	routeconfig	topin
deleterecipients	ldapflush	sbstatus	trace
delivernow	ldaptest	setgateway	version
diagnostic	nslookup	sethostname	vofflush
dnsflush	quarantineconfig	settime	vofstatus
dnslistflush	rate	shutdown	workqueue
dnslisttest	reboot	status	
dnsstatus	resetcounters	suspend	

上記のコマンドをクラスタ モードまたはグループ モードで実行しようとすると、警告メッセージが表示され、適切なモードに切り替えることができます。

次のコマンドは、さらにログイン ホスト（ユーザがログインしているマシン）に制限されます。これらのコマンドを使用するには、ローカル ファイル システムにアクセスできる必要があります。

表 *3:* ログイン ホスト モードに制限されるコマンド

last	resetconfig	tail	アップグレード

ping	supportrequest	telnet	who

GUI でのクラスタの管理

GUI では、クラスタの作成、クラスタへの参加、およびクラスタ固有の設定の管理（**clusterconfig** コマンドと同等の操作）を行うことはできませんが、クラスタ内のマシンの参照、設定の作成や削除、およびクラスタ間、グループ間、マシン間での設定のコピーや移動（つまり、**clustermode** および **clusterset** と同等の操作）を行うことができます。

[受信メールの概要（Incoming Mail Overview）] ページは、表示しているメール フロー モニタリングのデータがローカル マシンに格納されるため、ログイン ホストに制限されるコマンドの例です。別のマシンの [受信メールの概要（Incoming Mail Overview）] レポートを表示するには、そのマシンの GUI にログインする必要があります。

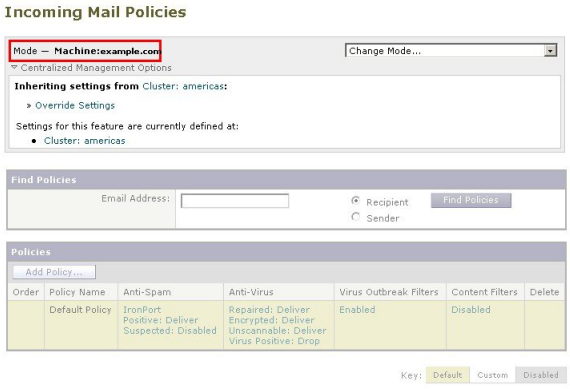
アプライアンス上でクラスタリングがイネーブルになっている場合は、ブラウザのアドレス フィールドの URL に注意してください。この URL には、必要に応じて **machine**、**group**、または **cluster** という単語が含まれています。たとえば、最初にログインしたときの [受信メールの概要（Incoming Mail Overview）] ページの URL は次のように表示されます。

https://ホスト名/**machine**/連番**/monitor/incoming_mail_overview**

（注） [モニタ（Monitor）] メニューの [受信メールの概要（Incoming Mail Overview）] ページと [受信メールの詳細（Incoming Mail Details）] ページは、ログイン マシンに制限されます。

[メールポリシー（Mail Policies）]、[セキュリティサービス（Security Services）]、[ネットワーク（Network）]、[システム管理（System Administration）] の各タブには、ローカル マシンに制限されないページが表示されます。[メールポリシー（Mail Policies）] タブをクリックすると、GUI 内の中央集中型管理情報が変更されます。

図 *2: GUI* の中央集中型管理機能：設定が規定されていない場合



上の図では、このマシンの現在の機能に関する設定がクラスタ モードから継承されています。継承された設定は薄いグレーで表示（プレビュー）されます。これらの設定を保持することも、クラスタ レベルの設定をこのマシン用に上書きして変更することも可能です。

（注） 継承された設定（プレビュー表示）には、常にクラスタから継承した設定が表示されます。グループ レベルとクラスタ レベルの間で依存するサービスをイネーブルまたはディセーブルにするときは注意してください。詳細については、設定のコピーと移動 （12 ページ）を参照してください。

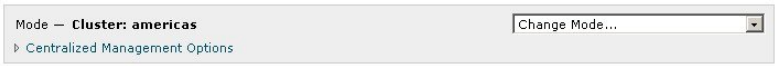
[設定を上書き（Override Settings）] リンクをクリックすると、この機能に対応する新しいページが表示されます。このページでは、マシン モードの新しい設定を作成できます。デフォルト設定をそのまま使用することもできますが、別のモードですでに設定している場合は、それらの設定をこのマシンにコピーすることもできます。

図 *3 : GUI* の中央集中型管理機能：新しい設定の作成

または、図「GUI の中央集中型管理機能：設定が規定されていない場合」に示すように、この設定がすでに定義されているモードに移動することもできます。これらのモードは、中央集中型管理ボックスの下部にある [この機能の設定は現在、次で定義されています：（Settings for this feature are currently defined at:）] に表示されます。ここには、設定が実際に規定されているモードだけが表示されます。別のモードで規定された（別のモードから継承された）設定のページを表示すると、ページ上にそれらの設定が表示されます。

表示されたいずれかのモード（たとえば、図「GUI の中央集中型管理機能：設定が規定されていない場合」に示す [クラスタ：南/北/中央アメリカ（Cluster: Americas）] リンク）をクリックすると、そのモードの設定を表示して管理できる新しいページが表示されます。

図 *4 : GUI* の中央集中型管理機能：定義された設定



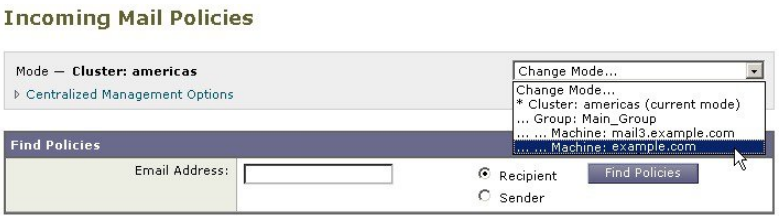
特定のモードで設定を規定すると、中央集中型管理ボックスがすべてのページに最小化された状態で表示されます。[集約管理オプション（Centralized Management Options）] リンクをクリックすると、ボックスが展開され、現在のモードで現在のページに関して設定できるオプションのリストが表示されます。[設定を管理（Manage Settings）] ボタンをクリックすると、現在の設定を別のモードにコピーまたは移動したり、設定を完全に削除したりできます。

たとえば、次の図では、[集約管理オプション（Centralized Management Options）] リンクがクリックされ、設定可能なオプションが表示されています。

図 *5: GUI* の中央集中型管理機能：設定の管理

ボックスの右側には [モードを変更（Change Mode）] メニューが表示されます。このメニューには現在のモードが表示され、このメニューを使っていつでも他のモード（クラスタ、グループ、またはマシン）に移動できます。

図 *6: [*モードを変更（*Change Mode***）*]* メニュー**



別のモードを表すページに移動すると、中央集中型管理ボックスの左側にある「モード—」というテキストが一時的に黄色で点滅し、モードが変更されたことを知らせます。

特定のタブに含まれる一部のページは、マシンモードに制限されています。ただし、（現在のログイン ホストに制限される）[受信メールの概要（Incoming Mail Overview）] ページとは異なり、これらのページはクラスタ内のどのマシンでも使用できます。

図 *7:* 中央集中型管理機能：マシンに制限される機能

[モードを変更（Change Mode）] メニューから管理するマシンを選択します。テキストが一時的に点滅し、モードが変更されたことを知らせます。

クラスタ通信

クラスタ内のマシンは、メッシュ ネットワークを使って相互に通信します。デフォルトでは、すべてのマシンが他のすべてのマシンに接続します。1 つのリンクが切断されても、他のマシンが更新を受信できなくなることはありません。

デフォルトでは、クラスタ内のすべての通信が SSH を使って保護されます。各マシンは、ルートテーブルのコピーをメモリ内に保持し、リンクの切断と確立に応じてメモリ内のテーブルを変更します。また、クラスタに含まれる他のすべてのマシンに対して定期的に（1 分間隔で）「ping」を実行します。これにより、リンクの最新状態を確認し、ルータや NAT がタイムアウトした場合でも接続を維持します。

（注） アプライアンスがクラスタ モードであり、他のアプライアンスのデータにリモートでアクセスする（設定関連ではなく、たとえば隔離内に存在するメッセージを表示したり、レポートの更新を高速化したりする）計画がある場合、クラスタの再接続が試行され、その結果、アラートやエラーが生成される場合があります。アプライアンスは自動的に再接続されるため、手動による介入は不要です。

DNS とホスト名の解決

マシンをクラスタに接続するには、DNS が必要です。クラスタの通信は、通常、（マシン上のインターフェイスのホスト名ではなく）マシンの DNS ホスト名を使って開始されます。ホスト名を解決できないマシンは、形式的にはクラスタに含まれていても、実際にはクラスタ内の他のマシンと通信できません。

ホスト名がアプライアンス上の SSH または CCS をイネーブルにした正しい IP インターフェイスを指すように、DNS を設定する必要があります。これは非常に重要です。DNS が SSH または CCS をイネーブルにしていない別の IP アドレスを参照すると、ホストが見つかりません。中央集中型管理では、インターフェイスごとのホスト名ではなく、sethostname コマンドで設定した「メイン ホスト名」が使用されます。

IP アドレスを使ってクラスタ内の他のマシンに接続する場合は、接続先のマシンが接続元の IP アドレスの逆ルックアップを実行できる必要があります。DNS 内にその IP アドレスがないために逆ルックアップがタイムアウトすると、そのマシンはクラスタに接続できません。

クラスタリング、完全修飾ドメイン名、およびアップグレード

AsyncOS をアップグレードすると、DNS の変更によって接続が失われることがあります。（クラスタ内のマシン上のインターフェイスのホスト名ではなく）クラスタ内のマシンの完全修飾ドメイン名を変更する必要がある場合は、AsyncOS をアップグレードする前に、sethostname を使ってホスト名の設定を変更し、そのマシンの DNS レコードを更新する必要があることに注意してください。

クラスタ通信のセキュリティ

Cluster Communication Security（CCS）は、標準の SSH サービスに似たセキュア シェル サービスです。シスコが CCS を実装したのは、クラスタ通信に標準の SSH を使用することに対する懸念に応えるためです。マシン間の SSH 通信では、同じポートで（管理者などの）通常のログインを開きます。多くの管理者は、クラスタ化されたマシン上で通常のログインを開くことを好みません。

ヒント：CCS はデフォルトですが、クラスタ化されたマシン間のポート 22 の通信がファイアウォールによってブロックされない場合は、CCS をイネーブルにしないでください。クラスタリングでは、すべてのマシン間でフル メッシュの SSH トンネル（ポート 22 上）が使用されます。いずれかのマシンですでに CCS をイネーブルにした場合は、クラスタからすべてのマシ

ンを削除し、最初からやり直してください。クラスタ内の最後のマシンを削除すると、クラスタが削除されます。

CCSは、管理者がCLIへのログインではなく、クラスタ通信を開始できるように強化されています。デフォルトでは、このサービスはディセーブルです。interfaceconfigコマンドで他のサービスをイネーブルにするためのプロンプトが表示されたときに、CCSをイネーブルにするかどうかの選択を求められます。次に例を示します。

```
Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?

[22]>

Do you want to enable Cluster Communication Service on this interface?

[N]> y

Which port do you want to use for Cluster Communication Service?

[2222]>
```

CCS のデフォルトのポート番号は 2222 です。必要な場合は、これを別の開いている未使用のポート番号に変更できます。マシンの参加が完了し、参加したマシンにクラスタのすべての設定データが適用されると、次の質問が表示されます。

```
Do you want to enable Cluster Communication Service on this interface? [N]> y


Which port do you want to use for Cluster Communication Service?

[2222]>
```

クラスタの整合性

「クラスタ対応」のマシンは、クラスタ内の他のマシンへのネットワーク接続を継続的に確認します。この確認は、クラスタ内の他のマシンに対する定期的な「ping」によって行われます。

特定のマシンとの通信の試行がすべて失敗すると、通信を試行したマシンはリモートホストが切断されたことを示すメッセージをログに記録します。システムはリモートホストがダウンしたことを示すアラートを管理者に送信します。

マシンがダウンしても、確認用の ping は引き続き送信されます。マシンがクラスタのネットワークに再び参加すると、それまでオフラインだったマシンが更新をダウンロードできるように、同期コマンドが実行されます。この同期コマンドは、一方のマシンに含まれる変更がもう一方のマシンに含まれるかどうかも判定します。含まれない場合は、それまでダウンしていたマシンが更新をサイレントでダウンロードします。

切断/再接続

マシンは、クラスタから切断できます。時折、たとえばマシンをアップグレードするために、マシンを意図的に切断することがあります。切断は、たとえば停電やソフトウェアまたはハー

ドウェアのエラーのために突発的に起きることもあります。1 台のアプライアンスがセッションで許可されている SSH 接続の最大数を超えて開こうとする場合も、切断が起きることがあります。クラスタから切断されたマシンに直接アクセスしてマシンを設定することはできますが、切断されたマシンを再接続するまでは、クラスタ内の他のマシンに変更が反映されません。

マシンをクラスタに再接続すると、そのマシンはただちにすべてのマシンに再接続しようとします。

理論的には、クラスタから2台のマシンを切断した場合、同じような変更が各マシンのローカルデータベースに同時に確定される可能性があります。これらのマシンをクラスタに再接続すると、これらの変更の同期が試行されます。競合がある場合は、最新の変更が記録されます（他の変更はすべて破棄されます）。

アプライアンスは、変更されるすべての変数を確定時にチェックします。確定データには、バージョン情報、連番ID、その他の比較可能な情報が含まれます。変更しようとしているデータが以前の変更と競合することがわかった場合は、変更を破棄するオプションが表示されます。たとえば、次のようなメッセージが表示されます。

```
(Machine mail3.example.com)> clustercheck

This command is restricted to "cluster" mode. Would you like to switch to "cluster"

mode? [Y]> y

Checking Listeners (including HAT, RAT, bounce profiles)...

Inconsistency found!

Listeners (including HAT, RAT, bounce profiles) at Cluster enterprise:

mail3.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on

mail3.example.com

test.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on

mail3.example.com

How do you want to resolve this inconsistency?

1. Force entire cluster to use test.example.com version.


2. Force entire cluster to use mail3.example.com version.

3. Ignore.

[1]>
```

変更を破棄しなかった場合、変更は（確定されませんが）保持されます。変更を現在の設定に照らして確認し、その後の処理方法を決めることができます。

また、いつでも `clustercheck` コマンドを使ってクラスタが正常に動作していることを確認できます。

```
losangeles> clustercheck
```

```
Do you want to check the config consistency across all machines in the cluster? [Y]> y

Checking losangeles...

Checking newyork...

No inconsistencies found.
```

互いに依存する設定

クラウドEメールセキュリティアプライアンスでは次の設定を行わないことをお勧めします。

中央集中型管理環境では、互いに依存する設定が異なるモードで設定されることがあります。設定モデルの高い柔軟性によって複数のモードで設定できるため、個々のマシンでどの設定が使用されるかは継承の法則に基づいて決まります。しかし、一部の設定は他の設定に依存しており、依存する設定の適用範囲は同じモードの設定に制限されません。したがって、あるレベルで特定のマシン用に設定された設定を参照する設定を別のレベルで設定することも可能です。

互いに依存する設定の最も一般的な例は、ページ上の別のクラスタ セクションからデータを取得する選択フィールドに関するものです。たとえば、次の機能をそれぞれ異なるモードで設定できます。

- LDAP クエリーの使用
- ディクショナリまたはテキスト リソースの使用
- バウンス プロファイルまたは SMTP 認証プロファイルの使用。

中央集中型管理には、制限コマンドと非制限コマンドがあります。（制限コマンド （16 ページ） を参照）。非制限コマンドは、通常、クラスタ全体で共有できるコンフィギュレーション コマンドです。

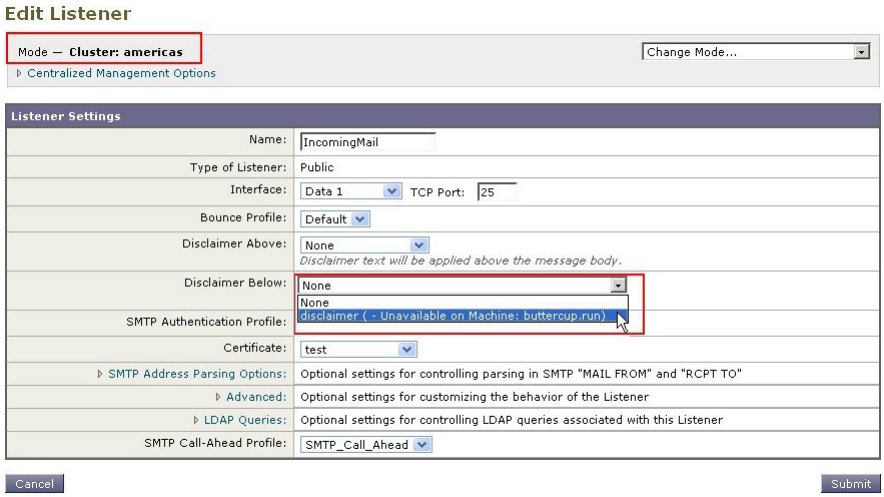
listenerconfig コマンドは、クラスタ内のすべてのマシンに設定できるコマンドの例です。非制限コマンドは、クラスタ内のすべてのマシンに反映できるため、マシンごとにデータを変更する必要がないコマンドです。

一方、制限コマンドは特定のモードだけに適用されるコマンドです。たとえば、ユーザを特定のマシン用に設定することはできません。ユーザはクラスタ全体に1セットしか設定できません（そうしないと、同じログイン名でリモート マシンにログインすることができなくなります）。同じように、メールフローモニタのデータ、システム概要のカウンタ、およびログファイルは、マシン単位でしか保持されないため、これらのコマンドやページはマシンだけに制限する必要があります。

定期レポートはクラスタ全体で同じに設定できますが、レポートの表示はマシン別に行われます。したがって、GUI の [定期レポート（Scheduled Reports）] ページは 1 つでも、設定はクラスタ モードで行い、レポートの表示はマシン モードで行う必要があります。

[システム時刻（System Time）] のページには、**settz**、**ntpconfig**、**settime** の各コマンドが含まれ、制限コマンドと非制限コマンドが混在しています。この場合、settime は（時間の設定がマシンに固有のものであるため）マシンモードだけに制限する必要がありますが、**settz** と **ntpconfig** はクラスタ モードまたはグループ モードで設定できます。

図 *8* : 互いに依存する設定の例



この図では、リスナー「IncomingMail」がマシン レベルでのみ設定された「disclaimer」という名前のフッターを参照しています。使用可能なフッター リソースのドロップダウン リストには、クラスタでは使用できるのにマシン「buttercup.run」では使用できないフッターが表示されています。このジレンマを解消するには、次の 2 つの方法があります。

- フッター「disclaimer」をマシン レベルからクラスタ レベルに格上げする
- リスナーをマシン レベルに格下げして、相互依存を解消する

中央集中型管理されたシステムの特長を最大限に活かすためには、1 つめの方法を推奨します。クラスタ化されたマシンの設定を調整するときは、設定間の相互依存に注意してください。

クラスタ化されたアプライアンスの設定のロード

AsyncOS では、クラスタ化されたアプライアンスにクラスタ設定をロードできます。次のようなシナリオでクラスタ設定をロードできます。

- オンプレミス環境からホスト環境に移行する際に、オンプレミスのクラスタの設定をホスト環境に移行する場合。
- クラスタ内のアプライアンスがダウンしたまたは廃棄する必要があり、そのアプライアンスから、クラスタに追加する予定の新しいアプライアンスに設定をロードする場合。
- アプライアンスをクラスタに追加するときに、クラスタ内の既存のアプライアンスの 1 つから新しく追加したアプライアンスに設定をロードする場合。
- バックアップ設定をクラスタにロードする場合。

必要に応じて、クラスタの設定またはアプライアンスの設定を有効なクラスタ設定ファイルからロードできます。

（注） スタンドアロンアプライアンスの設定をクラスタ化されたアプライアンスにロードすることはできません。

はじめる前に

- 有効で完全な XML コンフィギュレーション ファイルがあることを確認します。コンフィギュレーション ファイルのロードを参照してください。
- 設定のロード先とするアプライアンスの現在の設定のバックアップを作成します。現在の設定ファイルの保存およびエクスポートを参照してください。
- セットアップに含める予定のすべてのアプライアンスを使用してクラスタのセットアップを作成します。クラスタの作成とクラスタへの参加 （4 ページ）を参照してください。

（注） すべてのアプライアンスを 1 つのグループにまとめることができます。セットアップのクラスタ通信用インターフェイスの名前と SSH および CCS 設定が、XML コンフィギュレーション ファイルでの設定と同じであることを確認します。

手順

ステップ 1 [システム管理（System Administration）] > [設定ファイル（Configuration File）] をクリックします。

ステップ 2 [モード（Mode）] ドロップダウン メニューからクラスタを選択します。

ステップ 3 クラスタの設定とアプライアンスの設定のどちらをロードするかに応じて、次のいずれかを実行します。

- **クラスタの設定のロード**

  1. [設定をロード（Load Configuration）] セクションで、ドロップダウン リストから [クラスタ（Cluster）] を選択します。
  2. [ロード（Load）] をクリックしてクラスタの設定をロードします。コンフィギュレーション ファイルのロードを参照してください。
  3. ロードした設定からクラスタのアプライアンスにグループを割り当て、選択したグループに含まれるアプライアンスの設定を対応するアプライアンスにコピーします。[グループ設定（Group Configuration）] および [アプライアンス設定（Appliance Configuration）] ドロップダウン リストを使用します。

     アプライアンスの設定をコピーしない場合は、[アプライアンス設定（Appliance Configuration）] ドロップダウン リストから [コピー禁止（Don't Copy）] を選択します。

     1. 設定の内容を確認します。[レビュー（Review）] をクリックします。
     2. [確認（Confirm）] をクリックします。
     3. [続行（Continue）] をクリックします。

- **アプライアンスの設定のロード**

  1. [設定をロード（Load Configuration）] セクションで、ドロップダウン リストから [クラスタのアプライアンス（Appliance in cluster）] を選択します。

2. [ロード（Load）]をクリックして設定をロードします。コンフィギュレーションファイルのロードを参照してください。スタンドアロンアプライアンスの設定をクラスタ化されたアプライアンスにロードすることはできないことに注意してください。
3. ロードした設定からアプライアンスの設定を選択し、その設定をロードする、クラスタ内の対象アプライアンスを選択します。ドロップダウン リストを使用します。
4. [OK] をクリックします。
5. [続行（Continue）] をクリックします。
6. アプライアンスの設定を複数のアプライアンスにコピーするには、ステップ **a** ～ **e** を繰り返します。

ステップ 4 クラスタ化されたアプライアンスのネットワーク設定を確認してから、変更を確定します。

ベスト プラクティスとよく寄せられる質問（FAQ）

ベストプラクティス

クラスタを作成すると、現在ログインしているマシンが自動的に最初のマシンとしてクラスタに追加され、Main_Group にも追加されます。マシン レベルの設定は、できる限りクラスタ レベルに移動されます。グループ レベルの設定は存在せず、マシン レベルに残された設定は、クラスタ レベルでは意味を成さないのでクラスタ化できません。例として、IP アドレスやライセンス キーなどがあります。

設定はできる限りクラスタ レベルに残します。クラスタ内の 1 つのマシンにだけ異なる設定が必要な場合は、そのクラスタ設定をそのマシンのマシン レベルにコピーします。この場合は、設定を移動しないでください。工場出荷時のデフォルト値がない設定（HAT テーブル、SMTPROUTES テーブル、LDAP サーバ プロファイルなど）を移動すると、クラスタ設定を継承するシステムに空のテーブルが作成され、電子メールが処理されなくなるおそれがあります。

マシンにクラスタ設定を再度継承させるには、CM の設定を管理し、マシンの設定を削除します。マシンがクラスタ設定を上書きするかどうかは、次のメッセージが表示されたときにわかります。

Settings are defined:

To inherit settings from a higher level: Delete Settings for this feature at this mode.

You can also Manage Settings.

Settings for this feature are also defined at:

`Cluster: xxx`

または、次のメッセージが表示されます。

Delete settings from:

`Cluster: xxx`

Machine: yyyy.domain.com

コピーと移動の違い

コピーする必要がある場合：クラスタに設定を作成し、グループまたはマシンには設定を作成しないか、別の設定を作成する場合。

移動する必要がある場合：クラスタには設定を作成せず、グループまたはマシンに設定を作成する場合。

適切な CM の設計方法

LIST 操作で CM マシンのリストを出力すると、次のように表示されます。

cluster = CompanyName

Group Main_Group:

Machine lab1.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab2.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Group Paris:

Machine lab3.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab4.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Group Rome:

Machine lab5.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab6.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

現在変更しているレベルを忘れないように注意してください。たとえば、（RENAMEGROUP を使って）Main_Group の名前を変更した場合は、次のように表示されます。

cluster = CompanyName

Group London:

Machine lab1.cable.nu (Serial #: 000F1FF7B3F0-CF2SX51)

...

しかし、最初にグループ レベルで London のシステムを変更すると、クラスタ レベルを基本的な設定を行うための通常の設定レベルとして使用しなくなるため、このような設定は管理者にとって混乱の元です。

ヒント：グループにクラスタと同じ名前を付けること（クラスタ「London」とグループ「London」など）は推奨しません。グループ名としてサイト名を使用する場合、クラスタに場所を表す名前を付けることは推奨しません。

正しい方法は、前述のように、できるだけ多くの設定をクラスタ レベルに残すことです。ほとんどの場合、プライマリ サイトや主要なマシン群を Main_Group に残し、グループを追加のサイト用に使用してください。これは、両方のサイトを「同等」に扱う場合にも当てはまります。CM にはプライマリ/セカンダリ サーバやマスター/スレーブ サーバがなく、クラスタ化されたすべてのマシンがピアになることを思い出してください。

ヒント：追加のグループを使用する場合は、マシンをクラスタに追加する前にグループを簡単に準備できます。

クラスタのセットアップでスパム隔離またはポリシー隔離へアクセスするためのベスト プラクティス

ログインしているアプライアンスからクラスタ内の他のアプライアンスのスパム隔離またはポリシー隔離にアクセスすると、ログインしているアプライアンスの CPU 使用率を過度に増加させる原因となる場合があります。この状況を回避するには、それぞれのアプライアンスにログインして、スパム隔離またはポリシー隔離にアクセスします。

手順：サンプル クラスタの設定

このサンプル クラスタを設定するには、clusterconfig を実行する前に、すべてのマシン上ですべての GUI からログアウトします。プライマリ サイトのいずれかのマシン上で clusterconfig を実行します。次に、他のローカル マシンとリモート マシンのうち、（IP アドレスなどのマシン専用の設定を除いて）できるだけ多くの設定を共有する必要があるマシンだけをこのクラスタに追加します。clusterconfig コマンドを使ってリモート マシンをクラスタに追加することはできません。リモート マシン上の CLI を使って clusterconfig（既存のクラスタへの参加）を実行する必要があります。

前述の例では、lab1 にログインし、clusterconfig を実行して CompanyName という名前のクラスタを作成しています。同じ要件のマシンは 1 つしかないので、lab2 にログインし、saveconfig で既存の設定を保存します（この設定は lab1 の設定のほとんどを継承して大幅に変更されます）。次に、lab2 上で clusterconfig を使って既存のクラスタに参加します。他にも同じようなポリシーと設定を必要とするマシンがこのサイトにある場合は、上記の手順を繰り返します。

CONNSTATUS を実行して、DNS でホスト名が正しく解決されることを確認します。マシンがクラスタに追加されると、新しいマシンのほとんどの設定は lab1 から継承され、古い設定は消失します。追加されたマシンが運用マシンである場合は、これまでの設定の代わりに新しい設定を使ってメールが引き続き処理されるかどうかを予測する必要があります。マシンをクラスタから削除しても、そのマシンが古い専用の設定に戻ることはありません。

次に、例外となるマシンの数を数えます。例外が 1 台しかない場合は、マシン レベルの設定をいくつか追加すればよく、そのマシン用に追加のグループを作成する必要はありません。そのマシンをクラスタに追加し、設定をマシン レベルにコピーする作業を始めます。このマシンが既存の運用マシンである場合は、設定をバックアップし、前述のように電子メール処理の変更を検討する必要があります。

前述の例のように、例外が 2 台以上ある場合は、それらのマシンがクラスタで共有されない設定を共有するかどうかを判断します。共有する場合は、これらのマシン用のグループを 1 つ以上作成します。共有しない場合は、各マシンでマシン レベルの設定を作成すればよく、追加のグループを作成する必要はありません。

前述の例では、クラスタにすでに含まれているいずれかのマシン上で CLI の clusterconfig を実行し、ADDGROUP を選択する必要があります。この作業を 2 回行います（Paris に対して 1 回、Rome に対して 1 回）。

これで、GUIとCLIを使ってクラスタ用の設定とすべてのグループ（まだマシンがないグループも含む）用の設定を作成できます。各マシンのマシン固有の設定を作成できるようになるのは、マシンをクラスタに追加した後 です。

上書き（例外）用の設定を作成する最適な方法は、上位レベル（クラスタなど）から下位レベル（グループなど）に設定をコピーすることです。

たとえば、クラスタを作成した後の dnsconfig の初期設定は次のようになりました。

Configured at mode:

Cluster: Yes

Group Main_Group: No

Group Paris: No

Group Rome: No

Machine lab2.cable.nu: No

この DNS の設定を「グループにコピー」すると、次のようになります。

Configured at mode:

Cluster: Yes

Group Main_Group: No

Group Paris: Yes

Group Rome: No

Machine lab2.cable.nu: No

ここで、Paris グループ レベルの DNS の設定を編集すると、Paris グループの他のマシンはその設定を継承します。Paris グループ以外のマシンは、マシン固有の設定がない限り、クラスタの設定を継承します。DNS の設定に加えて、SMTPROUTES の設定もグループ レベルで作成するのが一般的です。

ヒント CLI のさまざまなメニューで CLUSTERSET 機能を使用するときは、設定をすべてのグループにコピーする特別なオプションを使用できます。このオプションはGUIでは使用できません。

完成されたリスナーは、グループまたはクラスタから自動的に継承されるため、通常はクラスタ内の最初のシステム上でのみリスナーを作成します。これによって管理作業が大幅に軽減されます。ただし、そのためにはグループまたはクラスタ全体でインターフェイスに同じ名前を付ける必要があります。

設定をグループ レベルで正しく規定した後は、マシンをクラスタに追加し、このグループに含めることができます。これには次の 2 つの手順が必要です。

まず、残りの 4 つのシステムをクラスタに追加するため、各システム上で clusterconfig を実行します。大きく複雑なクラスタほど、追加処理にかかる時間も長くなり、数分かかることもあります。LIST および CONNSTATUS サブコマンドを使って追加処理の進行状況をモニタできます。追加処理が完了したら、SETGROUP を使ってマシンを Main_Group から Paris および

Rome に移動します。クラスタに追加されたすべてのマシンが最初に Paris や Rome の設定ではなく Main_Group の設定を継承することは避けられません。これは、新しいシステムがすでに稼働中である場合、メール フローのトラフィックに影響する可能性があります。

ヒント　試験用マシンを運用マシンと同じクラスタに含めないでください。試験用システムには新しいクラスタ名を使用してください。これによって、予期しない変更（たとえば、誰かが試験用システムを変更し、誤って運用メールを消失するなど）に対する防御層が追加されます。

GUI でクラスタのデフォルト以外の CM 設定を使用する場合のオプションの要約

設定の上書き（デフォルトの設定から開始）。たとえば、SMTPROUTES 設定のデフォルトの設定は空のテーブルであり、テーブルを最初から作成できます。

設定の上書き（ただし、クラスタ「xxx」またはグループ「yyy」から現在継承している設定のコピーから開始）。たとえば、SMTPROUTES テーブルの新しいコピーをグループ レベルで使用できます。このテーブルは、初期状態ではクラスタのテーブルとまったく同じです。（SETGROUP で）同じグループに追加されたすべての Cisco アプライアンスにこのテーブルが適用されます。このグループに含まれないマシンでは、引き続きクラスタ レベルの設定が使用されます。この独立したテーブルで SMTPROUTES を変更しても、他のグループ、クラスタの設定を継承するマシン、および個々のマシン レベルで設定が規定されているマシンには影響しません。これが最も一般的な選択です。

中央集中型管理オプションのサブメニューである [設定を管理（Manage Settings）]。このメニューでは、上記のように設定をコピーできますが、設定を移動または削除することもできます。SMTPROUTES をグループまたはマシン レベルに移動すると、ルート テーブルはクラスタ レベルでは空になり、より具体的なレベルに存在することになります。

[設定を管理（Manage Settings）]。同じ SMTPROUTES の例で削除オプションを使用した場合も、クラスタの SMTPROUTES テーブルが空になります。SMTPROUTES をグループ レベルまたはマシン レベルですでに設定している場合は、これで問題ありません。クラスタ レベルの設定を削除し、グループまたはマシンの設定だけに依存することは推奨しません。クラスタ全体の設定は、新しく追加したマシンに対するデフォルトとして有用であり、これを保持することによって、管理する必要があるグループまたはサイトの設定の数が 1 つ減ります。

セットアップと設定に関する質問

Q. これまでスタンドアロンとして設定されていたマシンがあり、既存のクラスタに参加しました。これまでの設定はどうなりますか。

A. マシンがクラスタに参加すると、そのマシンのすべてのクラスタ化可能な設定がクラスタ レベルから継承されます。クラスタに参加した時点で、ローカルで設定されたネットワーク以外の設定は消失し、クラスタや関連するグループの設定で上書きされます。（これにはユーザ/パスフレーズのテーブルも含まれ、パスフレーズとユーザはクラスタ内で共有されます）。

Q. クラスタ化されたマシンがあり、それをクラスタから（永続的に）削除しました。これまでの設定はどうなりますか。

A.マシンをクラスタから永続的に削除すると、その設定階層は「平板化」され、そのマシンは引き続きクラスタに含まれていたときと同じように動作します。マシンに継承されたすべての設定が、スタンドアロンとして設定されたマシンに適用されます。

たとえば、クラスタ モードのグローバル配信停止テーブルしかない場合にマシンをクラスタから削除すると、そのグローバル配信停止テーブルのデータがマシンのローカル設定にコピーされます。

一般的な質問

Q. 中央集中型で管理されるマシンの間でログ ファイルは集約されますか。

A. いいえ。ログ ファイルは引き続き個々のマシンごとに保持されます。セキュリティ管理アプライアンスを使って複数のマシンのメール ログを集約し、トラッキングやレポート作成に利用できます。

Q. ユーザ アクセスはどうなりますか。

A. Cisco アプライアンスはクラスタ全体で 1 つのデータベースを共有します。特に、admin アカウント（およびパスフレーズ）は、クラスタ全体で 1 つしかありません。

Q. データセンターをクラスタ化するにはどうすればよいですか。

A.データセンターは、それ自体をクラスタにせずに、クラスタ内の「グループ」にするのが理想的です。しかし、データセンター間で共有する設定が多くない場合は、各データセンターを別個のクラスタにした方がうまくいく場合があります。

Q. オフラインのシステムを再接続するとどうなりますか。

A. クラスタにシステムを再接続すると、システム間の同期が試行されます。

ネットワークに関する質問

Q. 中央集中型管理機能は「ピアツーピア」アーキテクチャと「マスター/スレーブ」アーキテクチャのどちらですか。

A：すべてのマシンにすべてのマシン用のあらゆるデータ（使用されないマシン固有の設定を含む）があるため、中央集中型管理機能は「ピアツーピア」アーキテクチャと見なすことができます。

Q.ピアにならないようにアプライアンスをセットアップするにはどうすればよいですか。「スレーブ」システムを設定する必要があります。

A. このアーキテクチャでは、本物の「スレーブ」マシンは設定できません。しかし、マシン レベルで HTTP（GUI）アクセスと SSH（CLI）アクセスをディセーブルにすることは可能です。このように GUI アクセスや CLI アクセスができないマシンは、clusterconfig コマンドでのみ 設定可能です（つまり、ログイン ホストではなくなります）。これはスレーブを設定するのに似ていますが、ログイン アクセスを再度イネーブルにすると、この設定は無効になります。

Q. 複数のセグメント化されたクラスタを作成できますか。

A.クラスタを「島」のように分離することは可能です。実際、たとえばパフォーマンス上の理由などで、このようなクラスタを作成するのが有益な場合もあります。

Q. クラスタ化されたアプライアンスのうち、1 台の IP アドレスとホスト名を再設定したいのですが、再設定した場合、再起動コマンドを実行できるようになる前にGUI/CLIセッションが終了しませんか。

A. 次の手順に従ってください。

1. 新しい IP アドレスを追加します。
2. リスナーを新しいアドレスに移動します。
3. クラスタを脱退します。
4. ホスト名を変更します。
5. どのマシンから表示した clusterconfig の接続リストにも、古いマシン名が表示されないことを確認します。
6. すべての GUI セッションがログアウトしたことを確認します。
7. （interfaceconfig または [ネットワーク（Network）] > [リスナー（Listeners）] を使って）どのインターフェイスでも CCS がイネーブルになっていないことを確認します。
8. マシンを再びクラスタに追加します。

Q. 送信先コントロール機能をクラスタ レベルで適用できますか。それともこの機能はローカル マシン レベル専用ですか。

A. クラスタ レベルでも設定できますが、制限はマシン単位で適用されます。したがって、接続を 50 個に制限すると、クラスタ内のそれぞれのマシンにその制限が設定されます。

計画と設定

Q：クラスタをセットアップするときに、効率を最大限に高め、問題を最小限に抑えるにはどうすればよいですか。

1. 初期の計画
   - できるだけ多くの項目をクラスタ レベルで設定します。
   - 例外のみをマシン単位で管理します。
   - データセンターが複数ある場合は、たとえば、グループを使ってクラスタ共通でもマシン固有でもない特性を共有します。
   - 各アプライアンスのインターフェイスとリスナーに同じ名前を使用します。
2. 制限コマンドに注意してください。
3. 設定間の相互依存に注意してください。

   たとえば、listenerconfig コマンドは、（クラスタ レベルでも）マシン レベルにしか存在しないインターフェイスに依存します。クラスタ内のどのマシンにもマシン レベルのインターフェイスが存在しない場合、そのリスナーはイネーブルになります。

   インターフェイスの削除も listenerconfig に影響します。
4. 設定に注意してください。

すでに設定されているマシンがクラスタに参加すると、そのマシン単独の設定は消失します。前に設定した設定の一部を再び適用する場合は、クラスタに参加する前にすべての設定をメモしてください。

「切断された」マシンは、まだクラスタに含まれています。マシンを再接続すると、オフライン中に行った変更がクラスタの他のマシンと同期化されます。

マシンをクラスタから永続的に削除すると、そのマシンはクラスタのメンバとして持っていたすべての設定を保持します。しかし、考えを変えて再びそのマシンをクラスタに追加すると、そのマシンのスタンドアロンの設定はすべて消失します。

saveconfig コマンドを使って設定の記録を取ってください。