

ESA クラスタ必要条件およびセットアップ

目次

[概要](#)

[問題](#)

[ESA のクラスタとは何か。](#)

[要件](#)

[クラスタの作成](#)

[SSH 上のクラスタの作成](#)

[CCS 上のクラスタの作成](#)

[SSH が CCS によって実在するクラスタに加わること](#)

[SSH によって加入](#)

[CCS によって加入](#)

[移行される何がクラスタ設定で](#)

[移行されない何がクラスタ設定で](#)

概要

この資料はクラスタの基本を、必要条件 Cisco E メール セキュリティ アプライアンス (ESA) のクラスタを設定する方法を記述したものです。

問題

多くの場合、マイナーまたはメジャー修正が行われるたびに ESA の大きいグループ間の設定を中心にし、それらを設定を変更しなければならないことのタスクを避けるために完全に同期しておく必要が 1 つの各アプライアンスあります。

ESA のクラスタとは何か。

ESA 中央集中型管理 機能はローカル ポリシーに従っている間柔軟性およびスケーラビリティを提供するために複数のアプライアンスを、ネットワーク内の高められた信頼性同時に管理し、設定することを、可能にしまグローバルに管理することを許可します。

クラスタは一組の一般的な 設定 情報のマシンで構成されています。各クラスタの中では、アプライアンスは単一 マシンが 1 グループだけの一度にメンバーである場合もあるマシングループに更に分けることができます。

クラスタは-マスター・スレーブ関係無しで...ピアツーピア な アーキテクチャで設定されます。全体のクラスタがグループを制御し、管理するためにマシンにログイン することができます。これは管理者が論理的なグループ化で cluster-wide、グループ全体の、または毎マシン基礎のシステムの異なる要素を、基づいた自分自身で設定することを可能にします

要件

始まりますクラスタ (中央集中型管理) にアプライアンスに加入する機能会う次を確認する必要があります:

- すべての ESA は AsyncOS 同じバージョンがなければ**なりません** (修正に)。
注: バージョン 8.5+ でそれが AsyncOS 内の組み込まれた機能であるので追加されたとき中央集中型管理 キーがもはや目に見えます必要とならないし、またもはや。
- 使用するためにクラスタを作成すればポート 22 トラフィック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ポート 22 は (設定すること容易な) 確認します。
- 使用するためにクラスタを作成すればこのポートのトラフィックがインスペクションが割り込みなしで利用可能であるようにファイアウォール ルールがなされるようにポート 2222 (クラスタ コミュニケーションサービス) はします。
- クラスタ設定 オプションは ESA の CLI によってする必要があり、GUI で作成されるか、または加入することができません。
- 通信のためにホスト名を使用するために選択する場合アプライアンスで設定される DNSサーバをできますネットワークの他のすべてのアプライアンスを解決こと確認して下さい。
- アプライアンスのインターフェイスで確認して下さい、必須ポートおよびサービスは有効になります (SSH が CCS)。

クラスタの作成

クラスタを作成するすべての必要条件が満たされればプロセスから始まるために最初のアプライアンスのコマンド・ラインで始める必要があります。

ヒント : クラスタを設定する前にアプライアンスの現在のコンフィギュレーションをバックアップして下さい。 GUI から、システム 管理 > コンフィギュレーション ファイル。 覆われたパスワードボックスのチェックを外し、PC に設定をローカルで保存して下さい。

SSH 上のクラスタの作成

```
C370.lab> clusterconfigDo 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]> 2Enter the name of the new cluster.[1]> NameOfClusterShould all machines in the cluster communicate with each other by hostname orby IP address?1. Communicate by IP address.2. Communicate by hostname.[2]> 1What IP address should other machines use to communicate with Machine C370.lab?1. 1.1.1.1 port 22 (SSH on interface Management)2. Enter an IP address manually[1]> 1Other machines will communicate with Machine C370.lab using IP address1.1.1.1 port 22. You can change this by using the COMMUNICATION subcommandof the clusterconfig command.New cluster committed: DATECreating a cluster takes effect immediately, there is no need to commit.Cluster NameOfClusterChoose 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.- DELETEDGROUP - 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 上のクラスタの作成

```
C370.lab> clusterconfigDo 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]> 2Enter the name of the new cluster.[> TestShould 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]> 1What IP address should other machines use to communicate with Machine C370.lab?1. 1.1.1.1 port 22 (SSH on interface Management)2. Enter an IP address manually[> 2Enter the IP address for Machine C370.lab.[> 1.1.1.1Enter the port (on 10.66.71.120) for Machine C370.lab.[22]> 2222
```

このステップが実行されれば、クラスタがあり、レベルをクラスタ化するためにコンフィギュレーションはすべてマシンからために移られます。これは他のマシンがすべて加入した上で受継ぐ設定です。

SSH が CCS によって実在するクラスタに加わること

このセクションはちょうどまたは前に作成されて作成した実在するクラスタに新しいアプライアンスを追加することをカバーします。どちらかの方式による実在するクラスタに加わることはアプローチで類似した、違いの唯一のキーポイントです CCS クラスタがより新しいアプライアンスを受け入れるようにそれを確定するように要求します特別なステップがです。

SSH によって加入

注: SSH を使用しているので丁度続かれるステップ下記の必要の太字で示されるセクション、CCS 有効になることに「Y」を言わないで下さい。

```
C370.lab> clusterconfigDo 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]> 3While 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. dnsconfigsettings)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.[> 10.66.71.120Enter 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:efIs this a valid key for this host? [Y]>
```

このチェックがされれば、アプライアンスは今クラスタに正常に加入します。

CCS によって加入

これは実在するクラスタに新しいアプライアンスを許可することにする前にアプローチで類似した、唯一の違いありますクラスタでアクティブのアプライアンスにログイン する必要がありますです。

クラスタのアクティブなアプライアンス:

```
(Cluster test)> clusterconfigCluster testChoose 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.- DELETEDGROUP - 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.[> prepjoinPrepare Cluster Join Over CCSNo 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.[> newEnter the hostname of the system you want to add.[> ESA.labEnter the serial number of the host ESA.lab.[> XXXXXXXXXXXXXXX-XXXXXAEnter 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.

(クラスタに加入するように試み、コマンド「clusterconfig prepjoin プリント」を使用するアプライアンスにログイン することによって得られる) 上で SSH フィンガープリント入力し、ブランク 行を入力すれば、準備加入を完了します。

、それからこの参照用の、私達に加入するように呼出します上記のステップのそれを一致するためにそれを "ESA2.lab" と試みるアプライアンスの加入プロセスを始めることができます。

注: 下記の例の SSH-DSS キー

```
ESA2.lab> clusterconfigDo 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]> 4While 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. dnsconfigsettings)Exception: Centralized Policy, Virus, and Outbreak Quarantine settings are not inherited from the cluster. 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 added. On a machine in the cluster, run "clusterconfig -> prepjoin -> new" with the following information and commit.Host: ESA2.labSerial Number: XXXXXXXXXXXXXXX-XXXXXAUser Key:ssh-dss AAAAB3NzaC1kc3.....BrccM=Choose the interface on which to enable the Cluster Communication Service:1. ClusterInterface (1.1.1.2/24: ESA2.lab)[1]> 1Enter the port on which to enable the Cluster Communication Service:[2222]Enter the IP address of a machine in the cluster.[> 1.1.1.1Enter the remote port to connect to. This must be the CCS port on the machine "1.1.1.1", not the normal admin ssh port.[2222]>
```

これが確認されれば、受け入れれば条件を一致し、クラスタが正常に加入されれば場合、SSH-DSS キーを示されます。

移行される何がクラスタ設定で

クラスタはすべての行われたポリシー設定、コンテンツ フィルター、テキスト リソース、コンテンツ 辞書、LDAP設定、反スパムおよびアンチウイルス グローバル な 設定を、リスナー設定、SMTP ルート設定、DNS 設定持って来ます。

移行されない何がクラスタ設定で

- アプライアンス ローカル ホスト名。
- 構成された 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пам検疫設定。
- ローカル ポリシー、ウイルスおよび発生検疫コンフィギュレーション
- コマンド・ラインの「websecurityadvancedconfig」コマンドの下の設定 (バージョン 8.5 お

よび それ以降のために)。

注: 現存しない検疫を参照しているコンテンツ フィルターがあれば、参照されたポリシー 検疫がマシンで設定されるまで無効になります。