Требования кластера ESA и настройка

Содержание

Введение

Этот документ описывает основы кластера, требований и как установить кластер на Cisco Email Security Appliance (ESA).

Проблема

Часто, существует потребность централизовать конфигурацию между многочисленной группой ESA и поддержать их всех синхронизировавшими для предотвращения задачи необходимости изменить конфигурацию одно каждое устройство каждый раз, когда незначительная или основная модификация сделана.

Что такое кластер на ESA?

Функция централизованного управления ESA позволяет вам управлять и настраивать множественные устройства в то же время, предоставлять повышение надежности, гибкость и масштабируемость в вашей сети, позволяя вам управлять глобально при соответствии локальной политике.

Кластер состоит из ряда машин с информацией об обычной конфигурации. В каждом кластере устройства могут быть далее разделены на группы машины, где одиночная машина может быть участником только одной группы за один раз.

Кластеры внедрены в одноранговой архитектуре - без ведущего устройства/подчиненного отношения. Можно войти в любую машину, чтобы управлять и администрировать весь кластер или группу. Это позволяет администратору настраивать другие элементы системы на общекластерной, или основе на машину всей группы, с на основе их собственных

логических группировок

Требования

Чтобы быть в состоянии начаться, способность присоединиться к устройствам в Кластер (Централизованное управление), которое необходимо будет гарантировать, ниже приводится встреченная:

- Все ESA **MUST** имеют те же версии AsyncOS (вниз к пересмотру).

  Примечание: В версии 8.5 + ключ Централизованного управления больше не требуется и также больше не будет видим, когда добавлено, поскольку это - объединенная функция в AsyncOS.

- Если вы создаете кластер для использования порта 22 (легче настроить), гарантируют, что нет никакого межсетевого экрана или проблем маршрутизации между Устройствами на трафике порта 22.
- Если вы создаете кластер для использования порта 2222 (Кластерный Сервис подключения) гарантируют, что правила межсетевого экрана сделаны позволить трафику на этом порту быть доступным без контроля или прерывания.
- Опции конфигурации кластера нужно сделать через CLI на ESA и нельзя создать или присоединять GUI.
- Если вы принимаете решение использовать имя хоста для связи, гарантировать, что набор серверов DNS на устройствах в состоянии решить все другие устройства в вашей сети.
- Убедитесь на Интерфейсах своего устройства, требуемый порт и сервис включены (SSH или CCS).

Создание кластера

Для начала с процесса однажды, все требования удовлетворены для создания кластера, который необходимо будет начать в командной строке первого устройства.

> **Совет:** Резервное копирование ваша текущая конфигурация на вашем устройстве до настройки вашего кластера. От GUI, **Администрирование системы> Файл конфигурации**. Анчек поле пароля в маске и сохраните конфигурацию локально к вашему ПК.

Создание кластера по SSH

```
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.[]> 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[]> 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.- 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.
```

Создание кластера по CCS

```
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
```

Как только этот шаг выполнен, у вас будет кластер, и все ваши конфигурации будут перемещены от Машины до Кластерного уровня. Это будет конфигурацией **, которую все** другие машины наследуют после присоединения.

Присоединение к существующему кластеру через SSH или CCS

Этот раздел покроет добавление любого нового устройства в ваш существующий кластер, который вы только что создали или предшествующий созданный. Присоединение к существующему кластеру любым методом будет подобно в подходе, единственная ключевая точка различия является CCS, требует, чтобы дополнительный шаг завершил его, чтобы позволить кластеру принимать более новое устройство.

Присоединение через SSH

> **Примечание:** Раздел, обозначенный **полужирным** в шагах ниже, должен придерживаться точно, поскольку мы используем SSH, вы не должны говорить "Y" включению CCS.

```
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]>
```

Как только эта проверка сделана, устройство теперь присоединится к кластеру успешно.

Присоединение через CCS

Это будет подобно в подходе, единственная разница - прежде чем вы решите позволить новое устройство в существующий кластер, необходимо войти в устройство, которое активно в кластере.

На активном устройстве в кластере:

```
(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.- 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.[]> 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.[]> XXXXXXXXXXXXXX-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.
```

Как только вы вводите отпечаток пальца SSH (который получен путем вхождения в устройство, пытающееся присоединиться кластеру и использующий команду "clusterconfig prepjoin печать") в вышеупомянутом, и введите пустую строку, это завершит приготовительное соединение.

Затем можно начать процесс присоединения на устройстве, пытающемся присоединяться для этой ссылки, мы назовем его "ESA2.lab" для соответствия с тем из вышеупомянутого шага.

> **Примечание:** Ключ DSS SSH в примере ниже

```
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: XXXXXXXXXXXX-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]>
```

Как только это подтверждено, вам покажут ключ DSS SSH, если он совпадет, вы принимаете сроки, и к кластеру присоединятся успешно.

Что перемещено в Конфигурации кластера

Кластер принесет все настроенные параметры настройки политики, фильтры контента, текстовые ресурсы, словари содержания, Параметры LDAP, и антивирусные глобальные

параметры для защиты от спама, параметры настройки слушателя, настройки маршрута SMTP, параметры настройки DNS.

Что не перемещено в Конфигурации кластера

- Локальное имя хоста устройства.
- Настроенные IP - интерфейсы.
- Настроенные таблицы маршрутизации.
- Локальная карантинная конфигурация спама.
- Локальная политика, вирус и карантинные конфигурации вспышки
- Параметры настройки при "websecurityadvancedconfig" команде в Командной строке (для версий 8.5 и более новый).

Примечание: Если у вас будут фильтры контента, которые ссылаются на карантин, который не является существующим, то они будут лишены законной силы, пока Карантин (карантин) Политики, на который ссылаются, не был настроен на машине.