MetroCluster IP構成のメンテナンス手順

ONTAP MetroCluster

NetApp
September 06, 2024

目次

MetroCluster IP構成のメンテナンス手順

MetroCluster IPインターフェイスのプロパティの変更

ONTAP 9.10.1 以降では、 MetroCluster IP インターフェイスの IP アドレス、マスク、およびゲートウェイのプロパティを変更できます。パラメータは任意に組み合わせて更新できます。

これらのプロパティを更新する必要がある場合があります。たとえば、 IP アドレスが重複して検出された場合や、ルータの設定変更によってレイヤ 3 ネットワークでゲートウェイを変更する必要がある場合などです。

このタスクについて

- 一度に変更できるインターフェイスは 1 つだけです。他のインターフェイスが更新されて接続が再確立されるまで、そのインターフェイス上のトラフィックは中断されます。
- MetroCluster IP インターフェイス・プロパティを変更するには 'CLI MetroCluster configurion-settings interface modify' コマンドを使用します

> これらのコマンドは、特定のポートの特定のノードの設定を変更します。ネットワーク接続全体をリストアするには、他のポートでも同様のコマンドを実行する必要があります。同様に、ネットワークスイッチも構成を更新する必要があります。たとえば、ゲートウェイが更新されている場合は、 HA ペアの両方のノードが同じであるため変更することを推奨します。さらに、それらのノードに接続されたスイッチでも、ゲートウェイを更新する必要があります。

- 、、およびの各コマンドを使用して `metrocluster configuration-settings interface show` `metrocluster connection check` `metrocluster connection show` 、すべてのインターフェイスですべての接続が機能していることを確認します。

IP アドレス、ネットマスク、およびゲートウェイを変更します

MetroCluster IPインターフェイスのIPアドレス、ネットマスク、およびゲートウェイを変更するには、次の手順を実行します。

手順

1. 単一のノードとインターフェイスの IP アドレス ' ネットマスク ' およびゲートウェイを更新します MetroCluster の設定 - インターフェイスの変更

   次のコマンドは、 IP アドレス、ネットマスク、およびゲートウェイを更新する方法を示しています。

```
cluster_A::* metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_1 -home-port e0a-10 -address
192.168.12.101 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port “e0a-10”. Partner nodes
may need modifications for port “e0a-10” in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Setting up iSCSI target configuration. (pass2:iscsi13:0:-1:0):
xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO not supported
[Job 28] Establishing iSCSI initiator connections.
(pass6:iscsi14:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass8:iscsi15:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass9:iscsi16:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
[Job 28] Job succeeded: Interface Modify is successful.
cluster_A::*> metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_2 -home-port e0a-10 -address
192.168.12.201 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port “e0a-10”. Partner nodes
may need modifications for port “e0a-10” in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Job succeeded: Interface Modify is successful
```

2. [step2] すべてのインターフェイスですべての接続が機能していることを確認します。 MetroCluster configurion-settings interface show

   次のコマンドは、すべてのインターフェイスのすべての接続が機能していることを確認する方法を示しています。

```
cluster_A::*> metrocluster configuration-settings interface show
(metrocluster configuration-settings interface show)
DR              Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1     cluster_A node_A_2
                 Home Port: e0a-10
                      192.168.12.201  255.255.254.0   192.168.12.1
completed
                 Home Port: e0b-20
                      192.168.20.200  255.255.255.0   192.168.20.1
completed
                node_A_1
                 Home Port: e0a-10
                      192.168.12.101  255.255.254.0   192.168.12.1
completed
                 Home Port: e0b-20
                      192.168.20.101  255.255.255.0   192.168.20.1
completed
      cluster_B node_B_1
                 Home Port: e0a-10
                      192.168.11.151  255.255.255.0   192.168.11.1
completed
                 Home Port: e0b-20
                      192.168.21.150  255.255.255.0   192.168.21.1
completed
                node_B_2
                 Home Port: e0a-10
                      192.168.11.250  255.255.255.0   192.168.11.1
completed
                 Home Port: e0b-20
                      192.168.21.250  255.255.255.0   192.168.21.1
completed
8 entries were displayed.
```

3. すべての接続が機能していることを確認します。

「 MetroCluster configurion-settings connection show 」を参照してください

次のコマンドは、すべての接続が機能していることを確認する方法を示しています。

```
cluster_A::*> metrocluster configuration-settings connection show
  (metrocluster configuration-settings connection show)
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_A node_A_2
                  Home Port: e0a-10
                       192.168.10.200  192.168.10.101  HA Partner
completed
                  Home Port: e0a-10
                       192.168.10.200  192.168.11.250  DR Partner
completed
                  Home Port: e0a-10
                       192.168.10.200  192.168.11.151  DR Auxiliary
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.20.100  HA Partner
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.21.250  DR Partner
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.21.150  DR Auxiliary
completed
                 node_A_1
                  Home Port: e0a-10
                       192.168.10.101  192.168.10.200  HA Partner
completed
                  Home Port: e0a-10
                       192.168.10.101  192.168.11.151  DR Partner
completed
                  Home Port: e0a-10
                       192.168.10.101  192.168.11.250  DR Auxiliary
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.20.200  HA Partner
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.21.150  DR Partner
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.21.250  DR Auxiliary
completed
```

IP スイッチのメンテナンスと交換

IPスイッチを交換するか、既存のMetroCluster IPスイッチの使用方法を変更します

障害が発生したスイッチの交換、スイッチのアップグレードまたはダウングレード、既存のMetroCluster IPスイッチの使用の変更が必要になる場合があります。

このタスクについて

この手順 は、ネットアップ検証済みのスイッチを使用している場合に適用されます。MetroCluster 準拠のスイッチを使用している場合は、スイッチのベンダーを参照してください。

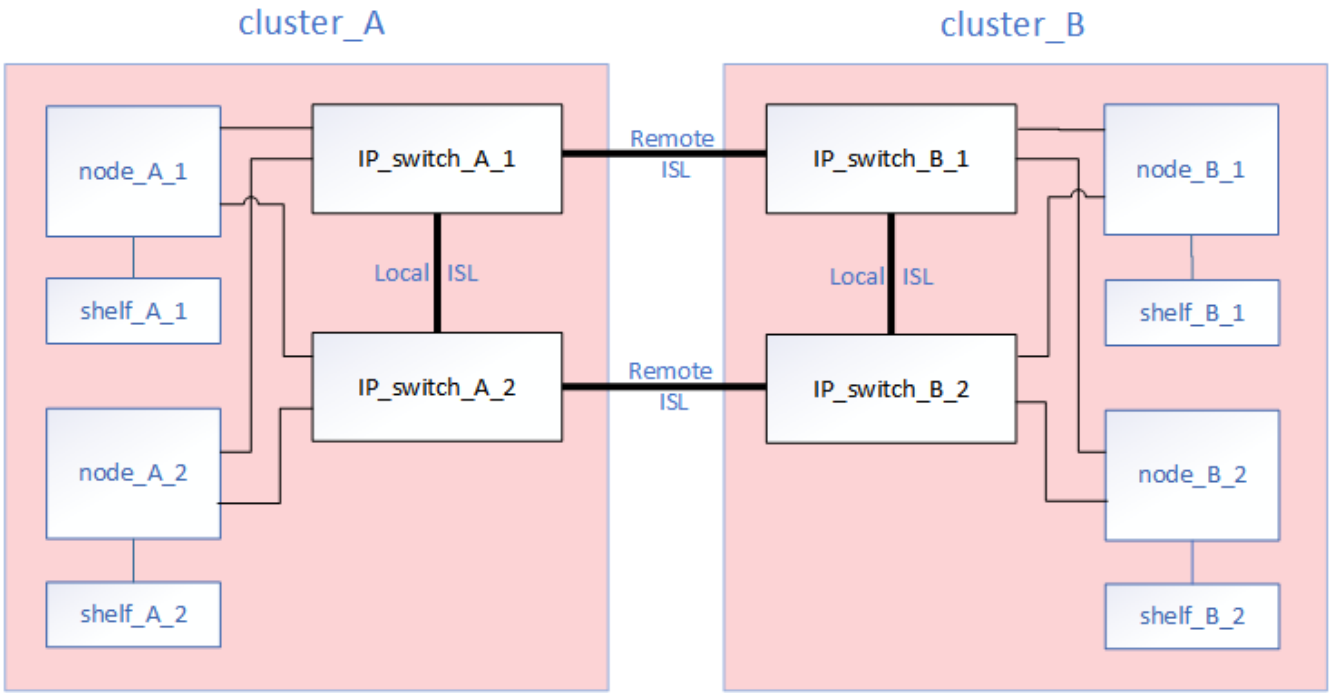
"コンソールログを有効にする" このタスクを実行する前に。

この手順 では、次の変換がサポートされています。

- スイッチのベンダー、タイプ、またはその両方を変更しています。スイッチに障害が発生した場合は、新しいスイッチを古いスイッチと同じにしたり、スイッチのタイプを変更（スイッチをアップグレードまたはダウングレード）したりできます。

  たとえば、AFF A400コントローラとBES-53248スイッチを使用する単一の4ノード構成からAFF A400コントローラを使用する8ノード構成にMetroCluster IP構成を拡張するには、新しい構成ではBES-53248スイッチはサポートされないため、スイッチをサポートされるタイプに変更する必要があります。

  障害が発生したスイッチを同じタイプのスイッチに交換する場合は、障害が発生したスイッチのみを交換します。スイッチをアップグレードまたはダウングレードする場合は、同じネットワークにある2つのスイッチを調整する必要があります。2つのスイッチがスイッチ間リンク（ISL）で接続されており、同じサイトに配置されていない場合、2つのスイッチは同じネットワークにあります。たとえば、次の図に示すように、ネットワーク1にはIP_switch_A_1とIP_switch_B_1が含まれ、ネットワーク2にはIP_switch_A_2とIP_switch_B_2が含まれています。



スイッチを交換する場合や別のスイッチにアップグレードする場合は、スイッチのファームウェアとRCFファイルをインストールすることでスイッチを事前に設定できます。

- 共有ストレージのMetroCluster スイッチを使用して、MetroCluster IP構成をMetroCluster IP構成に変換します。

  たとえば、AFF A700コントローラを使用する通常のMetroCluster IP構成で、NS224シェルフを同じスイッチに接続するようにMetroCluster を再設定する場合などです。

  - 共有ストレージMetroCluster IPスイッチを使用してMetroCluster IP構成のシェルフを追加または削除する場合は、の手順を実行します "共有ストレージMetroCluster スイッチを使用したMetroCluster IPへのシェルフの追加"
  - MetroCluster IP構成では、NS224シェルフまたは専用のストレージスイッチにすでに直接接続されている場合があります。

ポート使用ワークシート

次の例は、既存のスイッチを使用して2台のNS224シェルフを接続するMetroCluster IP構成を共有ストレージ構成に変換するワークシートです。

ワークシートの定義：

- Existing configuration：既存のMetroCluster 構成のケーブル接続。
- NS224シェルフを使用する新しい構成：ストレージとMetroCluster 間でスイッチを共有するターゲット構成。

このワークシートで強調表示されているフィールドは、次のとおりです。

- 緑：ケーブルを変更する必要はありません。
- 黄色：同じ構成または異なる構成のポートを移動する必要があります。
- 青：新しい接続のポート。

PORT USAGE OVERVIEW Example of expanding an existing 4Node MetroCluster with 2x NS224 shelves and changing the ISL's from 10G to 40/100G							
Switch port	Existing configuration				New configuration with NS224 shelves		
	Port use	IP_switch_x_1	IP_switch_x_2		Port use	IP_switch_x_1	IP_switch_x_2
1	MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'		MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'
2		Cluster Port 'A'	Cluster Port 'B'			Cluster Port 'A'	Cluster Port 'B'
3							
4							
5					Storage shelf 1 (9)	NSM-A, e0a	NSM-A, e0b
6						NSM-B, e0a	NSM-B, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster			ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'		MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'
10		Port 'A'	Port 'B'			Port 'A'	Port 'B'
11							
12							
13					ISL, MetroCluster, native speed 40G / 100G breakout mode 10G	Remote ISL, 2x 40/100G	Remote ISL, 2x 40/100G
14							
15							
16							
17					MetroCluster 1, Storage Interface	Storage Port 'A'	Storage Port 'B'
18						Storage Port 'A'	Storage Port 'B'
19							
20							
21	ISL, MetroCluster breakout mode 10G	Remote ISL, 10G	Remote ISL, 10G		Storage shelf 2 (8)	NSM-A, e0a	NSM-A, e0b
22						NSM-B, e0a	NSM-B, e0b
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							

手順

1. 構成の健全性を確認します。

   a. MetroCluster が構成されていて、各クラスタで通常モードであることを確認します。「 * MetroCluster show * 」

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. 各ノードでミラーリングが有効になっていることを確認します。「 * MetroCluster node show * 」

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

   c. MetroCluster コンポーネントが正常であることを確認します :'* MetroCluster check run*

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

d. ヘルス・アラートがないことを確認してください： * system health alert show *

2. 設置前に新しいスイッチを設定します。

   既存のスイッチを再利用する場合は、に進みます 手順 4。

   > スイッチをアップグレードまたはダウングレードする場合は、ネットワーク内のすべてのスイッチを設定する必要があります。

   の「 IP スイッチの設定」セクションの手順に従います "MetroCluster IP のインストールと設定"

   スイッチ _A_1 、 _A_2 、 _B_1 、または _B_2 に、適切な RCF ファイルを適用します。新しいスイッチが古いスイッチと同じ場合は、同じ RCF ファイルを適用する必要があります。

   スイッチをアップグレードまたはダウングレードする場合は、サポートされている最新の RCF ファイルを新しいスイッチに適用してください。

3. port show コマンドを実行してネットワークポートに関する情報を表示します。

   「 * network port show * 」と表示されます

   a. すべてのクラスタLIFを変更して自動リバートを無効にします。

   ```
   network interface modify -vserver <vserver_name> -lif <lif_name>
   -auto-revert false
   ```

4. 古いスイッチから接続を切断します。

古い構成と新しい構成で同じポートを使用していない接続だけを切断します。新しいスイッチを使用する場合は、すべての接続を切断する必要があります。

次の順序で接続を削除します。

a. ローカルクラスタインターフェイスを切断します
b. ローカルクラスタのISLを切断します
c. MetroCluster IPインターフェイスを切断します
d. MetroCluster ISLを切断します

を参照してください [port_usage_worksheet]スイッチは変更されません。MetroCluster ISLは再配置されます。切断する必要があります。ワークシートに緑色でマークされている接続を切断する必要はありません。

5. 新しいスイッチを使用する場合は、古いスイッチの電源をオフにしてケーブルを外し、古いスイッチを物理的に取り外します。

既存のスイッチを再利用する場合は、に進みます 手順 6。

管理インターフェイス（使用している場合）を除き、新しいスイッチをケーブル接続しないでください。

6. 既存のスイッチを設定します。

スイッチがすでに設定されている場合は、この手順を省略できます。

既存のスイッチを設定するには、次の手順に従ってファームウェアとRCFファイルをインストールおよびアップグレードします。

- "MetroCluster IP スイッチでのファームウェアのアップグレード"
- "MetroCluster IP スイッチの RCF ファイルをアップグレードします"

7. スイッチをケーブル接続します。

の「IPスイッチのケーブル接続」セクションの手順に従うことができます "MetroCluster IP のインストールと設定"。

次の順序でスイッチをケーブル接続します（必要な場合）。

a. リモートサイトにISLをケーブル接続します。
b. MetroCluster IPインターフェイスをケーブル接続します。
c. ローカルクラスタインターフェイスをケーブル接続します。

- スイッチタイプが異なる場合は、古いスイッチとは異なるポートが使用されることがあります。スイッチをアップグレードまたはダウングレードする場合は、ローカル ISL を * ケーブル接続しないでください。ローカルISLをケーブル接続するのは、2つ目のネットワークのスイッチをアップグレードまたはダウングレードするときに、一方のサイトの両方のスイッチのタイプとケーブル接続が同じ場合だけにしてください。
- Switch-A1とSwitch-B1をアップグレードする場合は、スイッチSwitch-A2とSwitch-B2について手順1~6を実行する必要があります。

8. ローカルクラスタのケーブル接続を完了します。
   a. ローカルクラスタインターフェイスがスイッチに接続されている場合は、次の手順を実行します。
      i. ローカルクラスタのISLをケーブル接続します。
   b. ローカルクラスタインターフェイスがスイッチに*接続されていない*場合：
      i. を使用します "ネットアップのスイッチクラスタ環境に移行する" 手順 ：スイッチレスクラスタをスイッチクラスタに変換します。に示すポートを使用します "MetroCluster IP のインストールと設定" または、RCFケーブル接続ファイルを使用してローカルクラスタインターフェイスを接続します。
9. スイッチに電源を投入します。

   新しいスイッチが同じ場合は、新しいスイッチの電源をオンにします。スイッチをアップグレードまたはダウングレードする場合は、両方のスイッチに電源を投入します。2 つ目のネットワークが更新されるまで、この構成は各サイトにある 2 つの異なるスイッチで動作します。

10. を繰り返して、MetroCluster 構成が正常であることを確認します 手順 1.。

    1 つ目のネットワークでスイッチをアップグレードまたはダウングレードする場合は、ローカルクラスタリングに関するアラートが表示されることがあります。

    ネットワークをアップグレードまたはダウングレードする場合は、 2 つ目のネットワークに対してすべての手順を繰り返します。

11. すべてのクラスタLIFを変更して自動リバートを再度有効にします。

```
network interface modify -vserver <vserver_name> -lif <lif_name> -auto
-revert true
```

12. 必要に応じて、NS224シェルフを移動します。

    NS224シェルフをMetroCluster IPスイッチに接続しないMetroCluster IP構成を再構成する場合は、該当する手順 を使用してNS224シェルフを追加または移動します。

    - "共有ストレージMetroCluster スイッチを使用したMetroCluster IPへのシェルフの追加"
    - "直接接続型ストレージを使用するスイッチレスクラスタから移行する"
    - "ストレージスイッチを再利用して、スイッチ接続ストレージを使用するスイッチレス構成から移行する"

オンラインまたはオフラインの**MetroCluster IP**インターフェイスポート

メンテナンスタスクを実行する際に、MetroCluster IPインターフェイスポートをオフラインまたはオンラインにしなければならない場合があります。

このタスクについて

"コンソールログを有効にする" このタスクを実行する前に。

手順

MetroCluster IPインターフェイスポートをオンラインまたはオフラインにするには、次の手順を実行します。

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

出力例

```
Cluster A_1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when
         directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

2. MetroCluster IPインターフェイスポートをオフラインにします。

```
system ha interconnect link off -node <node_name> -link <link_num, 0 or
1>
```

出力例

```
Cluster_A1::*> system ha interconnect link off -node node-a1 -link 0
```

a. MetroCluster IPインターフェイスがオフラインであることを確認します。

```
Cluster_A1::*> system ha interconnect port show
```

出力例

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                 Link           Layer     Layer      Physical   Physical
Active
Node             Monitor  Port  State     State       Link Up  Link Down
Link
---------------  -------  ----  --------  ---------  --------  ---------
------
node-a1        off
                              0  disabled  down              4          3
false
                              1  linkup    active            4          2
true
node-a2        off
                              0  linkup    active            4          2
true
                              1  linkup    active            4          2
true
2 entries were displayed.
```

3. MetroCluster IPインターフェイスポートをオンラインにします。

```
system ha interconnect link on -node <node_name> -link <link_num, 0 or
1>
```

出力例

```
Cluster_A1::*> system ha interconnect link on -node node-a1 -link 0
```

a. MetroCluster IPインターフェイスポートがオンラインであることを確認します。

```
Cluster_A1::*> system ha interconnect port show
```

出力例

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                 Link           Layer     Layer      Physical   Physical
Active
Node             Monitor  Port  State     State       Link Up  Link Down
Link
--------------  -------  ----  --------  ---------  --------  ---------
------
node-a1        off
                              0  linkup    active            5          3
true
                              1  linkup    active            4          2
true
node-a2        off
                              0  linkup    active            4          2
true
                              1  linkup    active            4          2
true
2 entries were displayed.
```

MetroCluster IP スイッチでのファームウェアのアップグレード

MetroCluster IP スイッチのファームウェアのアップグレードが必要になる場合があります。

このタスクについて

各スイッチでこのタスクを順に実行する必要があります。

"コンソールログを有効にする" このタスクを実行する前に。

手順

1. 構成の健全性を確認します。

   a. 各クラスタで MetroCluster が設定されており、通常モードであることを確認します。

      「 MetroCluster show 」

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

b. 各ノードでミラーリングが有効であることを確認します。

MetroCluster node show

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

c. MetroCluster コンポーネントが正常であることを確認します。

「 MetroCluster check run 」のようになります

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

a. ヘルスアラートがないことを確認します。

「 system health alert show 」というメッセージが表示されます

2. 最初のスイッチにソフトウェアをインストールします。

> スイッチには、 switch_A_1 、 switch_B_1 、 switch_B_2 、 switch_B_2 、 switch_B_2 、スイッチ _B_2 を順番にインストールします。

スイッチタイプがBroadcom、Cisco、NVIDIAのいずれであるかに応じて、該当するトピックのスイッチソフトウェアをインストールする手順に従います。

- "BroadcomスイッチのEFOSソフトウェアをダウンロードしてインストールする"
- "CiscoスイッチのNX-OSソフトウェアのダウンロードとインストール"
- "NVIDIA SN2100スイッチCumulusソフトウェアのダウンロードとインストール"

3. 各スイッチについて、同じ手順を繰り返します。
4. 繰り返します 手順 1. 構成の健全性を確認します。

MetroCluster IP スイッチの RCF ファイルをアップグレードします

MetroCluster IP スイッチ上の RCF ファイルのアップグレードが必要になる場合があります。たとえば、スイッチで実行しているRCFファイルのバージョンが、ONTAPのバージョン、スイッチのファームウェアのバージョン、またはその両方でサポートされていない場合などです。

RCFファイルがサポートされていることの確認

ONTAPまたはスイッチファームウェアのバージョンを変更する場合は、そのバージョンでサポートされるRCFファイルがあることを確認する必要があります。RCF ジェネレータを使用すると、正しい RCF ファイルが生成されます。

手順

1. RCF ファイルのバージョンを確認するには、スイッチから次のコマンドを使用します。

スイッチ	問題コマンド
Broadcomスイッチ	`(IP_switch_A_1) # show clibanner`
Cisco スイッチ	ip_switch _A_1# には、 banner motd が表示されます

いずれかのスイッチについて、 RCF ファイルのバージョンを示す行を出力から探します。たとえば、次の出力は Cisco スイッチを使用したもので、 RCF ファイルのバージョンが「 v1.80 」であることを示しています。

```
Filename : NX3232_v1.80_Switch-A2.txt
```

2. 特定の ONTAP バージョン、スイッチ、およびプラットフォームでサポートされているファイルを確認するには、 RcfFileGenerator を使用します。現在使用している設定またはにアップグレードする設定用の RCF ファイルを生成できる場合は、そのファイルがサポートされます。
3. スイッチファームウェアがサポートされていることを確認するには、次のマニュアルを参照してください。
   - "Hardware Universe"
   - "NetApp Interoperability Matrix を参照してください"

RCF ファイルをアップグレードします

新しいスイッチファームウェアをインストールする場合は、 RCF ファイルをアップグレードする前にスイッチファームウェアをインストールする必要があります。

このタスクについて

- この手順では、 RCF ファイルをアップグレードするスイッチ上のトラフィックが中断されます。新しい RCF ファイルが適用されると、トラフィックは再開されます。
- Switch_A_1、Switch_B_1、Switch_A_2、Switch_B_2の手順を一度に1つずつ実行します。
- "コンソールログを有効にする" このタスクを実行する前に。

手順

1. 構成の健全性を確認

   a. MetroCluster コンポーネントが正常であることを確認します。

      「 MetroCluster check run 」のようになります

```
cluster_A::*> metrocluster check run
```

この処理はバックグラウンドで実行されます。

b. MetroCluster check run オペレーションが完了したら ' MetroCluster check show を実行して結果を表示します

約 5 分後に、次の結果が表示されます。

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. 実行中の MetroCluster チェック処理のステータスを確認します。

MetroCluster オペレーション履歴 show -job-id 38`

b. ヘルスアラートがないことを確認します。

「 system health alert show 」というメッセージが表示されます

2. 新しい RCF ファイルを適用するための IP スイッチを準備します。

スイッチベンダーの手順に従います。

- "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"
- "Cisco IPスイッチを工場出荷時のデフォルトにリセットする"
- "NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセット"

3. スイッチベンダーに応じて、IP RCFファイルをダウンロードしてインストールします。

- "Broadcom IPのRCFファイルをダウンロードしてインストールする"
- "Cisco IP RCFファイルのダウンロードとインストール"
- "NVIDIA IP RCFファイルのダウンロードとインストール"

L2共有またはL3ネットワーク構成を使用している場合は、お客様の中間スイッチまたはお客様のスイッチでISLポートの調整が必要になることがあります。スイッチポートモードが「access」モードから「trunk」モードに変わることがあります。スイッチ_A_1とB_1の間のネットワーク接続が完全に機能していて、ネットワークが正常である場合にのみ、2つ目のスイッチペア（A_2、B_2）のアップグレードに進みます。

CleanUpFilesを使用して、Cisco IPスイッチのRCFファイルをアップグレードします

Cisco IPスイッチのRCFファイルのアップグレードが必要になる場合があります。たとえば、 ONTAP のアップグレードまたはスイッチファームウェアのアップグレードには、どちらも新しい RCF ファイルが必要です。

このタスクについて

- RcfFileGeneratorバージョン1.4a以降では、「write erase」を実行することなく、Cisco IPスイッチのスイッチ設定を変更（アップグレード、ダウングレード、または交換）するための新しいオプションが追加されています。
- "コンソールログを有効にする" このタスクを実行する前に。
- Cisco 9336C-FX2スイッチには2種類のスイッチストレージタイプがあり、RCFではそれぞれ異なる名前が付けられています。次の表を参照して、構成に適したCisco 9336C-FX2ストレージタイプを確認してください。

接続するストレージ	**Cisco 9336C-FX2**ストレージタイプを選択...	**RCF**ファイルのバナー/**MOTD**の例
• 直接接続SASシェルフ • 直接接続型NVMeシェルフ • NVMeシェルフを専用ストレージスイッチに接続	9336C-FX2–ダイレクト・ストレージのみ	`* Switch : NX9336C (direct storage, L2 Networks, direct ISL)`
• 直接接続SASシェルフ • MetroCluster IPスイッチに接続されたNVMeシェルフ イーサネット接続NVMeシェルフが少なくとも1つ必要です	9336C-FX2–SASおよびイーサネットストレージ	`* Switch : NX9336C (SAS and Ethernet storage, L2 Networks, direct ISL)`

作業を開始する前に

この方法は、構成が次の要件を満たしている場合に使用できます。

- 標準のRCF設定が適用されます。
- 。 "RcfFileGenerator の順にクリックします" 適用するRCFファイルは、同じバージョンおよび設定（プラットフォーム、VLAN）で作成できる必要があります。

- 適用されるRCFファイルは、特別な設定のためにネットアップから提供されたものではありません。
- RCFファイルは適用前に変更されませんでした。
- 現在のRCFファイルを適用する前に、スイッチを工場出荷時のデフォルトにリセットする手順を実行しました。
- RCFの適用後にスイッチ（ポート）の設定を変更していません。

これらの要件を満たしていない場合は、RCFファイルの生成時に作成されたCleanUpFilesは使用できません。しかし、この関数を利用して一般的なCleanUpFilesを作成することもできます。このメソッドを使用したクリーンアップは、「show running-config」の出力から得られます。これはベストプラクティスです。

> スイッチは、Switch_A_1、Switch_B_1、Switch_A_1、Switch_A_1、Switch_B_2、Switch_B_2の順序で更新します。または、Switch_A_1とSwitch_B_1を同時に更新し、Switch_A_1とSwitch_B_2を更新します。

手順

1. 現在のRCFファイルのバージョン、および使用するポートとVLANを確認します。「ip_switch_A_1# show banner motd」

> この情報は4つのスイッチすべてから取得し、次の情報の表を完成させる必要があります。

```
* NetApp Reference Configuration File (RCF)
*
* Switch : NX9336C (SAS storage, L2 Networks, direct ISL)
* Filename : NX9336_v1.81_Switch-A1.txt
* Date : Generator version: v1.3c_2022-02-24_001, file creation time:
2021-05-11, 18:20:50
*
* Platforms : MetroCluster 1 : FAS8300, AFF-A400, FAS8700
*              MetroCluster 2 : AFF-A320, FAS9000, AFF-A700, AFF-A800
* Port Usage:
* Ports 1- 2: Intra-Cluster Node Ports, Cluster: MetroCluster 1, VLAN
111
* Ports 3- 4: Intra-Cluster Node Ports, Cluster: MetroCluster 2, VLAN
151
* Ports 5- 6: Ports not used
* Ports 7- 8: Intra-Cluster ISL Ports, local cluster, VLAN 111, 151
* Ports 9-10: MetroCluster 1, Node Ports, VLAN 119
* Ports 11-12: MetroCluster 2, Node Ports, VLAN 159
* Ports 13-14: Ports not used
* Ports 15-20: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel 10
* Ports 21-24: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel
11, breakout mode 10gx4
* Ports 25-30: Ports not used
* Ports 31-36: Ports not used
*

#
IP_switch_A_1#
```

この出力から、次の2つの表に示す情報を収集する必要があります。

一般的な情報	MetroCluster	データ
RCF ファイルのバージョン		1.81
スイッチのタイプ		NX9336
ネットワークのタイプロジー		L2ネットワーク、直接ISL
ストレージタイプ		SASストレージ
プラットフォーム	1.	AFF A400
	2.	FAS9000

VLANの情報	ネットワーク	**MetroCluster**の設定	スイッチポート	サイト **A**	サイト **B**
VLANローカルクラスタ	ネットワーク1	1.	1、2	111	222
		2.	3、4	151.	251
	ネットワーク2.	1.	1、2	111	222
		2.	3、4	151.	251
VLAN MetroCluster の略	ネットワーク1	1.	9、10	119 番	119 番
		2.	11、12	159	159
	ネットワーク2.	1.	9、10	219	219
		2.	11、12	259	259

2. [[Create]- RCFファイルおよび-CleanUpFiles-or -create-generic-CleanUpFiles]]現在の設定用にRCFファイルとCleanUpFilesを作成するか、汎用のUpCleanFilesを作成します。

   ご使用の構成が前提条件に記載されている要件を満たしている場合は、*オプション1 *を選択します。お使いの構成が前提条件に記載されている要件を*満たしていない*場合は、*オプション2 *を選択します。

オプション**1**：**RCF**ファイルと**CleanUpFiles**を作成します

この手順 は、構成が要件を満たしている場合に使用します。

手順

a. RcfFileGenerator 1.4a以降を使用して、手順1で取得した情報を使用してRCFファイルを作成します。RcfFileGeneratorの新しいバージョンでは、CleanUpFilesのセットが追加されています。このセットを使用して、いくつかの設定を元に戻し、スイッチで新しいRCF設定を適用する準備をすることができます。

b. banner motdを、現在適用されているRCFファイルと比較します。プラットフォームタイプ、スイッチタイプ、ポート、およびVLANの使用方法は同じである必要があります。

RCFファイルと同じバージョンのCleanUpFilesを使用し、まったく同じ設定を行う必要があります。CleanUpFileを使用しても機能せず、スイッチの完全なリセットが必要になる場合があります。

用に作成したONTAP のバージョンは関係ありません。RCFファイルのバージョンのみが重要です。

RCFファイルには、同じバージョンのものも含まれており、プラットフォームの数が少ない場合もあればそれよりも多い場合もあります。プラットフォームがリストに表示されていることを確認します。

オプション**2**：一般的な**CleanUpFiles**を作成します

この手順 は、構成が*一部の要件を満たしていない場合に使用してください。

手順

a. 各スイッチから「show running-config」の出力を取得します。

b. RcfFileGeneratorツールを開き、ウィンドウの下部にある「Create generic CleanUpFiles」をクリックします

c. 手順1で取得した出力を「1」スイッチから上のウィンドウにコピーします。デフォルトの出力は削除することもそのまま使用することもできます。

d. 'CUFファイルの作成'をクリックします。

e. 下のウィンドウの出力をテキストファイルにコピーします（このファイルはCleanUpFileです）。

f. 構成内のすべてのスイッチについて、手順c、d、eを繰り返します。

この手順 の最後に、スイッチごとに1つずつ、合計4つのテキストファイルが必要です。これらのファイルは、オプション1を使用して作成できるCleanUpFilesと同じ方法で使用できます。

3. [[new-RCF -files-ing-new-configuration]]新しい設定用の「新しい」RCFファイルを作成します。前の手順で作成したファイルと同じ方法でこれらのファイルを作成します。ただし、ONTAP とRCFのそれぞれのファイルバージョンを選択してください。

この手順の完了後、それぞれ12個のファイルで構成される2セットのRCFファイルを用意する必要があり

ます。

4. ブートフラッシュにファイルをダウンロードします。

   a. で作成したCleanUpFilesをダウンロードします RCFファイルとCleanUpFilesを作成するか、現在の設定用の汎用CleanUpFilesを作成します

      このCleanUpFileは、適用されている現在のRCFファイル用であり、アップグレード先の新しいRCF用には*ありません。

      Switch-A1のCleanUpFileの例:'Cleanup_NX9336_v1.81_Switch-A1.txt

   b. で作成した新しいRCFファイルをダウンロードします 新しい構成用に「新しい」RCFファイルを作成します。

      Switch-A1のRCFファイルの例: NX9336_v1.90_Switch-A1.txt

   c. で作成したCleanUpFilesをダウンロードします 新しい構成用に「新しい」RCFファイルを作成します。 この手順はオプションです。あとでこのファイルを使用して、スイッチの設定を更新できます。現在適用されている設定に一致します。

      Switch-A1のCleanUpFileの例:'Cleanup_NX9336_v1.90_Switch-A1.txt

      正しい（一致する）RCFバージョンには、CleanUpFileを使用する必要があります。異なるRCFバージョンまたは別の設定に対してCleanUpFileを使用すると、設定のクリーンアップが正しく機能しない可能性があります。

      次に、3つのファイルをブートフラッシュにコピーする例を示します。

```
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.81_MetroCluster-
IP_L2Direct_A400FAS8700_xxx_xxx_xxx_xxx/Cleanup_NX9336_v1.81_Switch-
A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//NX9336_v
1.90_Switch-A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//Cleanup_
NX9336_v1.90_Switch-A1.txt bootflash:
```

+

   Virtual Routing and Forwarding（VRF；仮想ルーティング転送）を指定するように求められます。

5. CleanUpFileまたはGeneric CleanUpFileを適用します。

一部の設定はリバートされ、スイッチポートは「オフライン」になります。

a. スタートアップコンフィギュレーションに保留中の変更がないことを確認します。「show running-config diff」

```
IP_switch_A_1# show running-config diff
IP_switch_A_1#
```

6. システム出力が表示された場合は、実行コンフィギュレーションをスタートアップコンフィギュレーションに保存します

> システム出力は、スタートアップコンフィギュレーションと実行コンフィギュレーションが異なること、および保留中の変更であることを示します。保留中の変更を保存しないと、スイッチのリロードを使用してロールバックできません。

a. CleanUpFileを適用します。

```
IP_switch_A_1# copy bootflash:Cleanup_NX9336_v1.81_Switch-A1.txt
running-config

IP_switch_A_1#
```

> スイッチのプロンプトに戻るまでに時間がかかることがあります。出力は想定されません。

7. 実行コンフィギュレーションを表示して、コンフィギュレーションがクリアされたことを確認します。「show running-config」

現在の設定は次のように表示されます。

- クラスマップとIPアクセスリストは設定されていません
- ポリシーマップは設定されません
- サービスポリシーが設定されていません
- ポートプロファイルが設定されていません
- すべてのイーサネットインターフェイス（mgmt0を除くすべての構成を表示しないでください。VLAN 1だけを設定してください）。

  上記のいずれかが設定されている場合は、新しいRCFファイルの設定を適用できない可能性があります。ただし、実行コンフィギュレーションをスタートアップコンフィギュレーションに保存せずにスイッチ*をリロードすることで、以前のコンフィギュレーションに戻すことができます。スイッチは、以前の設定で起動します。

8. RCFファイルを適用してポートがオンラインであることを確認します。

a. RCFファイルを適用します。

```
IP_switch_A_1# copy bootflash:NX9336_v1.90-X2_Switch-A1.txt running-
config
```

設定の適用中にいくつかの警告メッセージが表示されます。通常、エラーメッセージは予期されません。ただし、SSHを使用してログインすると、次のエラーが表示されることがあります。 `Error: Can't disable/re-enable ssh:Current user is logged in through ssh`

b. 設定を適用したら、「show interface brief」、「show cdp neighbors」、「show lldp neighbors」のいずれかのコマンドを使用して、クラスタポートとMetroCluster ポートがオンラインになっていることを確認します

ローカルクラスタのVLANを変更したあとにサイトの最初のスイッチをアップグレードした場合、古い設定と新しい設定のVLANが一致しないため、クラスタヘルスモニタで状態が「正常」と報告されないことがあります。2番目のスイッチが更新されると、状態はhealthyに戻るはずです。

設定が正しく適用されていない場合、または設定を保持しない場合は、実行コンフィギュレーションをスタートアップコンフィギュレーションに保存せずにスイッチ*をリロードすることで、以前のコンフィギュレーションに戻すことができます。スイッチは、以前の設定で起動します。

9. 設定を保存し、スイッチをリロードします。

```
IP_switch_A_1# copy running-config startup-config

IP_switch_A_1# reload
```

Cisco IP スイッチの名前変更

構成内で一貫性のある名前を使用するために、 Cisco IP スイッチの名前変更が必要になる場合があります。

このタスクについて

- このタスクの例では、スイッチ名が「 m 」から「 ip_switch_a_1 」に変更されています。
- "コンソールログを有効にする" このタスクを実行する前に。

手順

1. グローバルコンフィギュレーションモードを開始します。

「 * configure terminal * 」

次の例は、構成モードのプロンプトを示しています。どちらのプロンプトにもスイッチ名「 m yswitch 」が表示されています。

```
myswitch# configure terminal
myswitch(config)#
```

2. スイッチの名前を変更します。

   '*switchname new-switch-name *

   ファブリック内の両方のスイッチの名前を変更する場合は、各スイッチで同じコマンドを使用します。

   CLI プロンプトの内容が新しい名前に変わります。

```
myswitch(config)# switchname IP_switch_A_1
IP_switch_A_1(config)#
```

3. 構成モードを終了します。

   「 * exit *

   最上位のスイッチプロンプトが表示されます。

```
IP_switch_A_1(config)# exit
IP_switch_A_1#
```

4. 現在の実行コンフィギュレーションをスタートアップコンフィギュレーションファイルにコピーします。

   '*copy running-config startup-config *

5. スイッチ名の変更が ONTAP クラスタのプロンプトに表示されることを確認します。

   新しいスイッチ名が表示され、古いスイッチ名（「 m 」スイッチ）は表示されないことに注意してください。

   a. advanced 権限モードに切り替え、プロンプトが表示されたら「 * y * 」を押します。 +`* set -privilege advanced * `
   b. 接続されているデバイスを表示します :+`* network device-discovery show *`
   c. admin 特権モードに戻ります :+**`set -privilege admin`**

      次の例では ' スイッチが新しい名前で表示されていますつまり 'ip_switch_a_1' です

```
cluster_A::storage show> set advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

cluster_A::storage show*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node_A_2/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/28  N9K-
C9372PX
            e1a    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/2       N3K-
C3232C
            e1b    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/10      N3K-
C3232C
.
.
.                                             Ethernet1/18      N9K-
C9372PX
node_A_1/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/26  N9K-
C9372PX
            e0a    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/1       N3K-
C3232C
            e0b    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/9       N3K-
C3232C
            e1a    IP_switch_A_1(FOC21211RBU)
.
.
.
16 entries were displayed.
```

Cisco IPスイッチのISLポートを無停止で追加、削除、変更

Cisco IPスイッチでISLポートの追加、削除、または変更が必要になる場合がありま

す。Cisco IPスイッチでは、専用ISLポートを共有ISLポートに変換したり、ISLポートの速度を変更したりできます。

このタスクについて

専用の ISL ポートを共有 ISL ポートに変換する場合は、新しいポートがに対応していることを確認してください "共有 ISL ポートの要件"。

ISL 接続を確保するためには、両方のスイッチですべての手順を実行する必要があります。

次の手順では、スイッチポート Eth1/24/1 に接続されている 10Gb ISL を、スイッチポート 17 と 18 に接続されている 2 つの 100Gb ISL に交換します。

> NS224シェルフを接続する共有構成でCisco 9336C-FX2スイッチを使用している場合は、ISLを変更するときに新しいRCFファイルが必要になることがあります。現在のISL速度が40Gbpsおよび100Gbpsの場合は、新しいRCFファイルは必要ありません。ISLの速度に対するその他の変更には、新しいRCFファイルが必要です。たとえば、ISLの速度を40Gbpsから100Gbpsに変更しても新しいRCFファイルは必要ありませんが、ISLの速度を10Gbpsから40Gbpsに変更するには新しいRCFファイルが必要です。

作業を開始する前に

の*スイッチ*セクションを参照してください。 "NetApp Hardware Universe の略" をクリックして、サポートされているトランシーバを確認します。

"コンソールログを有効にする" このタスクを実行する前に。

手順

1. 変更するファブリック内の両方のスイッチで、 ISL の ISL ポートを無効にします。

> 現在の ISL ポートを無効にするのは、ポートを別のポートに移動している場合や ISL の速度が変更されている場合だけです。既存の ISL と同じ速度の ISL ポートを追加する場合は、手順 3 に進みます。

次の例に示すように、設定コマンドを 1 行に 1 つ入力し、すべてのコマンドを入力したら Ctrl+Z キーを押す必要があります。

```
switch_A_1# conf t
switch_A_1(config)# int eth1/24/1
switch_A_1(config-if)# shut
switch_A_1(config-if)#
switch_A_1#

switch_B_1# conf t
switch_B_1(config)# int eth1/24/1
switch_B_1(config-if)# shut
switch_B_1(config-if)#
switch_B_1#
```

2. 既存のケーブルとトランシーバを取り外します。
3. 必要に応じて ISL ポートを変更します。

> NS224シェルフを接続する共有構成でCisco 9336C-FX2スイッチを使用していて、RCFファイルをアップグレードして新しいISLポートに新しい構成を適用する必要がある場合は、次の手順を実行します。 "MetroCluster IPスイッチでRCFファイルをアップグレードします。"

オプション	ステップ
ISL ポートの速度を変更する	速度に応じて、新しい ISL を指定のポートにケーブル接続します。使用しているスイッチの ISL ポートが MetroCluster IP インストールおよび設定に表示されていることを確認する必要があります。
ISL を追加する	ISL ポートとして追加するポートに QFSP を挿入します。MetroCluster IP のインストールと設定に表示されていることを確認し、それに応じてケーブルを接続します。

4. ファブリック内の両方のスイッチですべての ISL ポートを有効にします（有効になっていない場合）。最初に次のコマンドを入力します。

   'switch_A_1# conf t`

   設定コマンドを 1 行に 1 つ入力し、すべてのコマンドを入力したら Ctrl+Z キーを押す必要があります。

```
switch_A_1# conf t
switch_A_1(config)# int eth1/17
switch_A_1(config-if)# no shut
switch_A_1(config-if)# int eth1/18
switch_A_1(config-if)# no shut
switch_A_1(config-if)#
switch_A_1#
switch_A_1# copy running-config startup-config

switch_B_1# conf t
switch_B_1(config)# int eth1/17
switch_B_1(config-if)# no shut
switch_B_1(config-if)# int eth1/18
switch_B_1(config-if)# no shut
switch_B_1(config-if)#
switch_B_1#
switch_B_1# copy running-config startup-config
```

5. 両方のスイッチ間にISLとポートチャネルが確立されていることを確認します。

```
switch_A_1# show int brief
```

次の例に示すように、 ISL インターフェイスがコマンド出力に表示されます。

```
Switch_A_1# show interface brief
--------------------------------------------------------------------------------
--------
Ethernet        VLAN    Type Mode   Status  Reason                   Speed
Port
Interface
Ch #
--------------------------------------------------------------------------------
--------
Eth1/17         1       eth  access down    XCVR not inserted
auto(D) --
Eth1/18         1       eth  access down    XCVR not inserted
auto(D) --

--------------------------------------------------------------------------------
------------------
Port-channel VLAN    Type Mode   Status  Reason
Speed   Protocol
Interface
--------------------------------------------------------------------------------
------------------
Po10         1       eth  trunk  up      none
a-100G(D)  lacp
Po11         1       eth  trunk  up      none
a-100G(D)  lacp
```

6. ファブリック 2 についても手順を繰り返します。

MetroCluster IP 構成でのストレージの特定

ドライブまたはシェルフモジュールを交換する必要がある場合、まずその場所を特定する必要があります。

ローカルシェルフとリモートシェルフの ID

MetroCluster サイトのシェルフ情報を表示する場合、すべてのリモートドライブは 0m 、仮想 iSCSI ホストアダプタです。つまり、ドライブは MetroCluster IP インターフェイス経由でアクセスされます。それ以外のドライブはすべてローカルです。

シェルフがリモート（ 0m 上）かどうかを特定したら、シリアル番号、または構成でのシェルフ ID の割り当てによってはシェルフ ID で、ドライブまたはシェルフを詳細に特定できます。

ONTAP 9.4 を実行する MetroCluster IP 構成では、 MetroCluster サイト間でシェルフ ID を一意にする必要はありません。これには内蔵シェルフ（ 0 ）と外付けシェルフの両方が含まれます。シリアル番号は、どちらの MetroCluster サイトのどのノードから見ても変わりません。

シェルフ ID は、内蔵シェルフを除き、ディザスタリカバリ（ DR ）グループ内で一意である必要があります。

ドライブまたはシェルフモジュールを特定したら、該当する手順を使用してコンポーネントを交換できます。

"DS460C 、 DS224C 、 DS212C ディスクシェルフを保守します"

sysconfig -a の出力例

次に、「 sysconfig -a 」コマンドを使用して、 MetroCluster IP 構成のノード上のデバイスを表示する例を示します。このノードには次のシェルフとデバイスが接続されています。

- スロット 0 ：内蔵ドライブ（ローカルドライブ）
- スロット 3 ：外部シェルフ ID 75 および 76 （ローカルドライブ）
- スロット 0 ：仮想 iSCSI ホストアダプタ 0m （リモートドライブ）

```
node_A_1> run local sysconfig -a

NetApp Release R9.4:  Sun Mar 18 04:14:58 PDT 2018
System ID: 1111111111 (node_A_1); partner ID: 2222222222 (node_A_2)
System Serial Number: serial-number (node_A_1)
.
.
.
slot 0: NVMe Disks
                0    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500528)
                1    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500735)
                2    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501165)
.
.
.
slot 3: SAS Host Adapter 3a (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:80
Phy State:          [12] Enabled, 12.0 Gb/s
```

```
                    [13] Enabled, 12.0 Gb/s
                    [14] Enabled, 12.0 Gb/s
                    [15] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130640
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
                75.4 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502158)
.
.
.

Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3c (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:88
Phy State:          [0] Enabled, 12.0 Gb/s
                    [1] Enabled, 12.0 Gb/s
                    [2] Enabled, 12.0 Gb/s
                    [3] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130691
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
```

```
(S20KNYAG501793)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3d (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:8c
Phy State:          [4] Enabled, 12.0 Gb/s
                    [5] Enabled, 12.0 Gb/s
                    [6] Enabled, 12.0 Gb/s
                    [7] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:01
Mini-SAS HD Serial Number: 614130690
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 4: Quad 10 Gigabit Ethernet Controller X710 SFP+
.
.
.
slot 0: Virtual iSCSI Host Adapter 0m
                0.0  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500690)
                0.1  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500571)
                0.2  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500323)
                0.3  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
```

```
(S3NBNX0J500724)
                0.4  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500734)
                0.5  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500598)
                0.12 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501094)
                0.13 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500519)
.
.
.
Shelf 0: FS4483PSM3E  Firmware rev. PSM3E A: 0103  PSM3E B: 0103
Shelf 35: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 36: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

node_A_1::>
```

共有ストレージ **MetroCluster** スイッチを使用した **MetroCluster IP** へのシェルフの追加

共有ストレージ MetroCluster スイッチを使用して、 NS224 シェルフを MetroCluster に追加する必要がある場合があります。

ONTAP 9.10.1 以降では、共有のストレージ / MetroCluster スイッチを使用して、 MetroCluster から NS224 シェルフを追加できます。シェルフは一度に複数追加できます。

作業を開始する前に

- ノードで ONTAP 9.9.1 以降が実行されている必要があります。
- 現在接続されているすべての NS224 シェルフは、 MetroCluster と同じスイッチに接続する必要があります（共有ストレージ / MetroCluster スイッチ構成）。
- この手順を使用して、専用のイーサネットスイッチに接続された NS224 シェルフまたは NS224 シェルフを使用する構成を、共有ストレージ / MetroCluster スイッチを使用して構成に変換することはできません。
- "コンソールログを有効にする" このタスクを実行する前に。

カスタム **AutoSupport** メッセージをメンテナンス前に送信する

メンテナンスを実行する前に、 AutoSupport an 問題 message to notify NetApp technical support that maintenance is maintenancing （メンテナンスが進行中であることをネットアップテクニカルサポートに通知する）を実行システム停止が発生したとみなしてテクニカルサポートがケースをオープンしないように、メンテナンスが進行中であることを通知する必要があります。

このタスクについて

このタスクは MetroCluster サイトごとに実行する必要があります。

手順

1. サポートケースが自動で生成されないようにするには、アップグレードが進行中であることを示す AutoSupport メッセージを送信します。

   a. 次のコマンドを問題に設定します。

      「 system node AutoSupport invoke -node * -type all -message 」 MAINT=10h NS224 シェルフの追加または削除中」に進みます

      この例では、 10 時間のメンテナンス時間を指定しています。プランによっては、さらに時間をかけたい場合もあります。

      この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間が終了したことを通知する AutoSupport メッセージを起動できます。

   「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

   a. パートナークラスタに対してこのコマンドを繰り返します。

MetroCluster 構成の健全性の確認

移行を実行する前に、 MetroCluster 構成の健全性と接続を確認する必要があります。

手順

1. ONTAP で MetroCluster 構成の動作を確認します。

   a. システムがマルチパスかどうかを確認します。

      'node run -node _node-name_sysconfig -a

   b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

      「 system health alert show 」というメッセージが表示されます

   c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

      「 MetroCluster show 」

   d. MetroCluster チェックを実行します。

      「 MetroCluster check run 」のようになります

   e. MetroCluster チェックの結果を表示します。

      MetroCluster チェックショー

   f. Config Advisor を実行します。

      "ネットアップのダウンロード： Config Advisor"

   g. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

2. クラスタが正常であることを確認します。

   cluster show -vserver Cluster

```
cluster_A::> cluster show -vserver Cluster
Node            Health  Eligibility   Epsilon
--------------- ------  -----------   -------
node_A_1    true    true          false
node_A_2    true    true          false

cluster_A::>
```

3. すべてのクラスタポートが動作していることを確認します。

   「 network port show -ipspace cluster 」のように表示されます

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. すべてのクラスタ LIF が動作していることを確認します。

   「 network interface show -vserver Cluster 」のように表示されます

   各クラスタ LIF で、 Is Home には true 、 Status Admin/Oper には up/up と表示されるはずです

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. すべてのクラスタ LIF で自動リバートが有効になっていることを確認します。

   network interface show -vserver Cluster -fields auto-revert を実行します

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

新しい **RCF** ファイルをスイッチに適用しています

スイッチがすでに正しく設定されている場合は、以降のセクションを省略して、に直接進むことができます Cisco 9336C スイッチでの MACsec 暗号化の設定（該当する場合）またはに移動します 新しい NS224 シェルフを接続します。

- シェルフを追加するには、スイッチの構成を変更する必要があります。
- ケーブル接続の詳細については、を参照してください "プラットフォームポートの割り当て"。
- 構成に合わせて RCF ファイルを作成するには、 **RcfFileGenerator** ツールを使用する必要があります。。 "RcfFileGenerator の順にクリックします" また、各スイッチのポートごとのケーブル接続の概要についても説明します。正しいシェルフ数を選択していることを確認してください。RCF ファイルと一緒に追加ファイルが作成され、特定のオプションに一致する詳細なケーブルレイアウトが提供されます。新しいシェルフをケーブル接続する際には、このケーブル接続の概要を使用してケーブル接続を検証します。

MetroCluster IP スイッチでの **RCF** ファイルのアップグレード

新しいスイッチファームウェアをインストールする場合は、 RCF ファイルをアップグレードする前にスイッチファームウェアをインストールする必要があります。

この手順では、 RCF ファイルをアップグレードするスイッチ上のトラフィックが中断されます。新しい RCF ファイルが適用されると、トラフィックは再開されます。

手順

1. 構成の健全性を確認

    a. MetroCluster コンポーネントが正常であることを確認します。

「 * MetroCluster check run * 」のようになります

```
cluster_A::*> metrocluster check run
```

この処理はバックグラウンドで実行されます。

b. MetroCluster check run オペレーションが完了したら ' MetroCluster check show を実行して結果を表示します

約 5 分後に、次の結果が表示されます。

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. 実行中の MetroCluster チェック処理のステータスを確認するには、次のコマンドを使用します。 `+* MetroCluster operation history show -job-id 38*`

b. ヘルス・アラートがないことを確認します `+* system health alert show *`

2. 新しい RCF ファイルを適用するための IP スイッチを準備します。

Cisco IP スイッチを工場出荷時のデフォルトにリセットする

新しいバージョンのソフトウェアと RCF をインストールする前に、 Cisco スイッチの設定を消去し、基本的な設定を完了する必要があります。

この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。

1. スイッチを工場出荷時のデフォルトにリセットします。

a. 既存の設定を消去します。「 write erase 」

b. スイッチソフトウェアをリロードします

システムがリブートし、設定ウィザードが表示されます。起動中に、 Abort Auto Provisioning （自動プロビジョニングの中止）というプロンプトが表示され、通常のセットアップを続行する場合（ yes/no ） [n] 、「 yes 」と入力して続行します。

c. 設定ウィザードで、スイッチの基本設定を入力します。

- 管理パスワード
- スイッチ名
- アウトオブバンド管理設定
- デフォルトゲートウェイ
- SSH サービス（ RSA ）設定ウィザードが完了すると、スイッチがリブートします。

d. プロンプトが表示されたら、ユーザ名とパスワードを入力してスイッチにログインします。

次の例は、スイッチを設定する際のプロンプトとシステム応答を示しています。山括弧（「 <<<`) 」）は、情報を入力する場所を示します。

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

Enter the password for "admin": password
Confirm the password for "admin": password
---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to
skip the remaining dialogs.
```

次の一連のプロンプトで、スイッチ名、管理アドレス、ゲートウェイなどの基本情報を入力し、 SSH with RSA を選択します。

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
   Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
   Number of rsa key bits <1024-2048> [1024]:
 Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
 Configure default switchport interface state (shut/noshut) [noshut]:
shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

最後の一連のプロンプトで設定が完了します。

```
The following configuration will be applied:
 password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
 no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. 設定を保存します。

```
IP_switch-A-1# copy running-config startup-config
```

3. スイッチをリブートし、スイッチがリロードされるまで待ちます。

```
IP_switch-A-1# reload
```

4. MetroCluster IP 構成の他の 3 つのスイッチについて、上記の手順を繰り返します。

Cisco スイッチの NX-OS ソフトウェアのダウンロードとインストール

MetroCluster IP 構成の各スイッチにスイッチのオペレーティングシステムファイルと RCF ファイルをダウンロードする必要があります。

この作業には、 FTP 、 TFTP 、 SFTP 、 SCP などのファイル転送ソフトウェアが必要です。 ファイルをスイッチにコピーします。

この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。

サポートされているバージョンのスイッチソフトウェアを使用する必要があります。

"NetApp Hardware Universe の略"

1. サポートされている NX-OS ソフトウェアファイルをダウンロードします。

   "シスコソフトウェアのダウンロード"

2. スイッチソフトウェアをスイッチにコピーします。「 + copy sftp://root@server-IP-address/tftpboot/NX-OS -file-name bootflash:vrf management+

   この例では、 nxos.7.0.3.I4.6.bin ファイルを SFTP サーバ 10.10.99.99 からローカルブートフラッシュにコピーしています。

   ```
   IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
   bootflash: vrf management
   root@10.10.99.99's password: password
   sftp> progress
   Progress meter enabled
   sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
   /bootflash/nxos.7.0.3.I4.6.bin
   Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
   /tftpboot/nxos.7.0.3.I4.6.bin                  100%  666MB   7.2MB/s
   01:32
   sftp> exit
   Copy complete, now saving to disk (please wait)...
   ```

3. 各スイッチの bootflash: `d IR bootflash: ` に、スイッチの NX-OS ファイルが存在することを各スイッチで確認します

   次の例は、 FC_switch_A_1 にファイルが存在することを示しています。

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. スイッチソフトウェアをインストールします。“ install all nxos bootflash:nxos.version-number.bin “

   スイッチソフトウェアがインストールされると、スイッチは自動的にリロード（リブート）します。

   次の例は、 FC_switch_A_1 へのソフトウェアのインストールを示しています。

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

Performing module support checks.            [####################] 100%
-- SUCCESS

Notifying services about system upgrade.     [####################] 100%
-- SUCCESS
```

```
Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos                7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. スイッチがリロードされるまで待ってから、スイッチにログインします。

   スイッチがリブートされると、ログインプロンプトが表示されます。

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. スイッチソフトウェアがインストールされていることを確認します : 'how version

   次の例は、の出力を示しています。

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. MetroCluster IP 構成の残りの 3 つの IP スイッチについて、上記の手順を繰り返します。

Cisco 9336C スイッチでの MACsec 暗号化の設定

必要に応じて、サイト間で実行される WAN ISL ポートに MACsec 暗号化を設定できます。正しい RCF ファイルを適用したあとに MACsec を設定する必要があります。

MACsec 暗号化は、 WAN ISL ポートにのみ適用できます。

MACsec のライセンス要件

MACsec にはセキュリティライセンスが必要です。Cisco NX-OS ライセンス方式の詳細およびライセンスの取得方法と適用方法については、を参照してください "『 Cisco NX-OS Licensing Guide 』"

MetroCluster IP 構成での Cisco MACsec 暗号化 WAN ISL のイネーブル化

MetroCluster IP 構成では、 WAN ISL 上の Cisco 9336C スイッチに対して MACsec 暗号化をイネーブルにできます。

1. グローバルコンフィギュレーションモード「 configure terminal 」を入力します

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. デバイスで MACsec と MKA を有効にします。「 feature MACsec」

```
IP_switch_A_1(config)# feature macsec
```

3. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします

```
IP_switch_A_1(config)# copy running-config startup-config
```

Cisco MACsec Encryption をディセーブルにします

MetroCluster IP 構成では、 WAN ISL 上の Cisco 9336C スイッチに対して MACsec 暗号化を無効にする必要がある場合があります。

暗号化を無効にする場合は、キーも削除する必要があります。

1. グローバルコンフィギュレーションモード「 configure terminal 」を入力します

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. デバイスの MACsec 設定を無効にします：「 ACSEC SHUTDOWN 」

```
IP_switch_A_1(config)# macsec shutdown
```

no オプションを選択すると、 MACsec 機能が復元されます。

3. MACsec で設定済みのインターフェイスを選択します。

   インターフェイスのタイプと ID を指定できます。イーサネットポートの場合は、イーサネットスロット / ポートを使用します。

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. インターフェイスに設定されているキーチェーン、ポリシー、およびフォールバックキーチェーンを削除して、 MACsec 設定を削除します。「 no MACsec keychain -name policy -name fallback-keychain keychain -name 」

```
IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

5. MACsec が設定されているすべてのインターフェイスで、ステップ 3 と 4 を繰り返します。
6. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします

```
IP_switch_A_1(config)# copy running-config startup-config
```

MACsec キーチェーンおよびキーの設定

MACsec キーチェーンの設定の詳細については、ご使用のスイッチのシスコのマニュアルを参照してください。

新しい **NS224** シェルフを接続します

手順

1. キットに付属のパンフレットに従って、シェルフに付属のレールマウントキットを取り付けます。
2. パンフレットに従って、サポートブラケットとラックまたはキャビネットにシェルフを設置して固定します。
3. 電源コードをシェルフに接続し、電源コード固定クリップで固定してから、耐障害性を確保するために別々の電源に接続します。

   電源に接続するとシェルフの電源がオンになり、電源スイッチはありません。電源装置が正常に動作している場合は、 LED が緑色に点灯します。

4. シェルフ ID は、 HA ペア内および構成全体で一意の番号に設定します。
5. シェルフポートは次の順序で接続します。
   a. SMA-A 、 e0a をスイッチ（ Switch-A1 または Switch-B1 ）に接続します。

b. NSM-B 、 e0a をスイッチ（ Switch-A2 または Switch-B2 ）に接続します。

c. NSM-A'e0b をスイッチ（ Switch-A1 または Switch-B1 ）に接続します

d. NSM-B 、 e0b をスイッチ（ Switch-A2 または Switch-B2 ）に接続します。

6. **RcfFileGenerator** ツールで生成されたケーブルレイアウトを使用して、シェルフを適切なポートにケーブル接続します。

   新しいシェルフが正しくケーブル接続されると、 ONTAP はそのシェルフをネットワーク上で自動的に検出します。

MetroCluster IP構成でのエンドツーエンドの暗号化の設定

ONTAP 9.15.1以降では、MetroCluster IP構成のサイト間でNVLOGやストレージレプリケーションデータなどのバックエンドトラフィックを暗号化するようにエンドツーエンドの暗号化を設定できます。

このタスクについて

- このタスクを実行するには、クラスタ管理者である必要があります。
- エンドツーエンドの暗号化を設定する前に、次の手順を実行する必要があります。 "外部キー管理を設定"。
- MetroCluster IP構成でエンドツーエンドの暗号化を設定するために必要な、サポートされているシステムおよび最小ONTAPリリースを確認します。

最小ONTAPリリース	サポートされるシステム
ONTAP 9.15.1	• AFF A400 • FAS8300 • FAS8700 の場合

エンドツーエンドの暗号化を実現

エンドツーエンドの暗号化を有効にするには、次の手順を実行します。

手順

1. MetroCluster 構成の健全性を確認

   a. MetroCluster コンポーネントが正常であることを確認します。

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   この処理はバックグラウンドで実行されます。

b. のあとに入力します `metrocluster check run` 処理が完了しました。run：

```
metrocluster check show
```

約 5 分後に、次の結果が表示されます。

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. 実行中の MetroCluster チェック処理のステータスを確認します。

```
metrocluster operation history show -job-id <id>
```

b. ヘルスアラートがないことを確認します。

```
system health alert show
```

2. 両方のクラスタで外部キー管理が設定されていることを確認します。

```
security key-manager external show-status
```

3. DRグループごとにエンドツーエンドの暗号化を有効にします。

```
metrocluster modify -is-encryption-enabled true -dr-group-id
<dr_group_id>
```

◦ 例 *

```
cluster_A::*> metrocluster modify -is-encryption-enabled true -dr-group
-id 1
Warning: Enabling encryption for a DR Group will secure NVLog and
Storage
         replication data sent between MetroCluster nodes and have an
impact on
         performance. Do you want to continue? {y|n}: y
[Job 244] Job succeeded: Modify is successful.
```

+ 構成内のDRグループごとにこの手順を繰り返します。

4. エンドツーエンドの暗号化が有効になっていることを確認します。

```
metrocluster node show -fields is-encryption-enabled
```

◦ 例 *

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          true
1           cluster_A  node_A_2  configured          true
1           cluster_B  node_B_1  configured          true
1           cluster_B  node_B_2  configured          true
4 entries were displayed.
```

エンドツーエンドの暗号化を無効にする

エンドツーエンドの暗号化を無効にするには、次の手順を実行します。

手順

1. MetroCluster 構成の健全性を確認

   a. MetroCluster コンポーネントが正常であることを確認します。

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

この処理はバックグラウンドで実行されます。

b. のあとに入力します `metrocluster check run` 処理が完了しました。run：

```
metrocluster check show
```

約 5 分後に、次の結果が表示されます。

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. 実行中の MetroCluster チェック処理のステータスを確認します。

```
metrocluster operation history show -job-id <id>
```

b. ヘルスアラートがないことを確認します。

```
system health alert show
```

2. 両方のクラスタで外部キー管理が設定されていることを確認します。

```
security key-manager external show-status
```

3. 各DRグループでエンドツーエンドの暗号化を無効にします。

```
metrocluster modify -is-encryption-enabled false -dr-group-id
<dr_group_id>
```

◦例 *

```
cluster_A::*> metrocluster modify -is-encryption-enabled false -dr-group
-id 1
[Job 244] Job succeeded: Modify is successful.
```

+ 構成内のDRグループごとにこの手順を繰り返します。

4. エンドツーエンドの暗号化が無効になっていることを確認します。

```
metrocluster node show -fields is-encryption-enabled
```

◦ 例 *

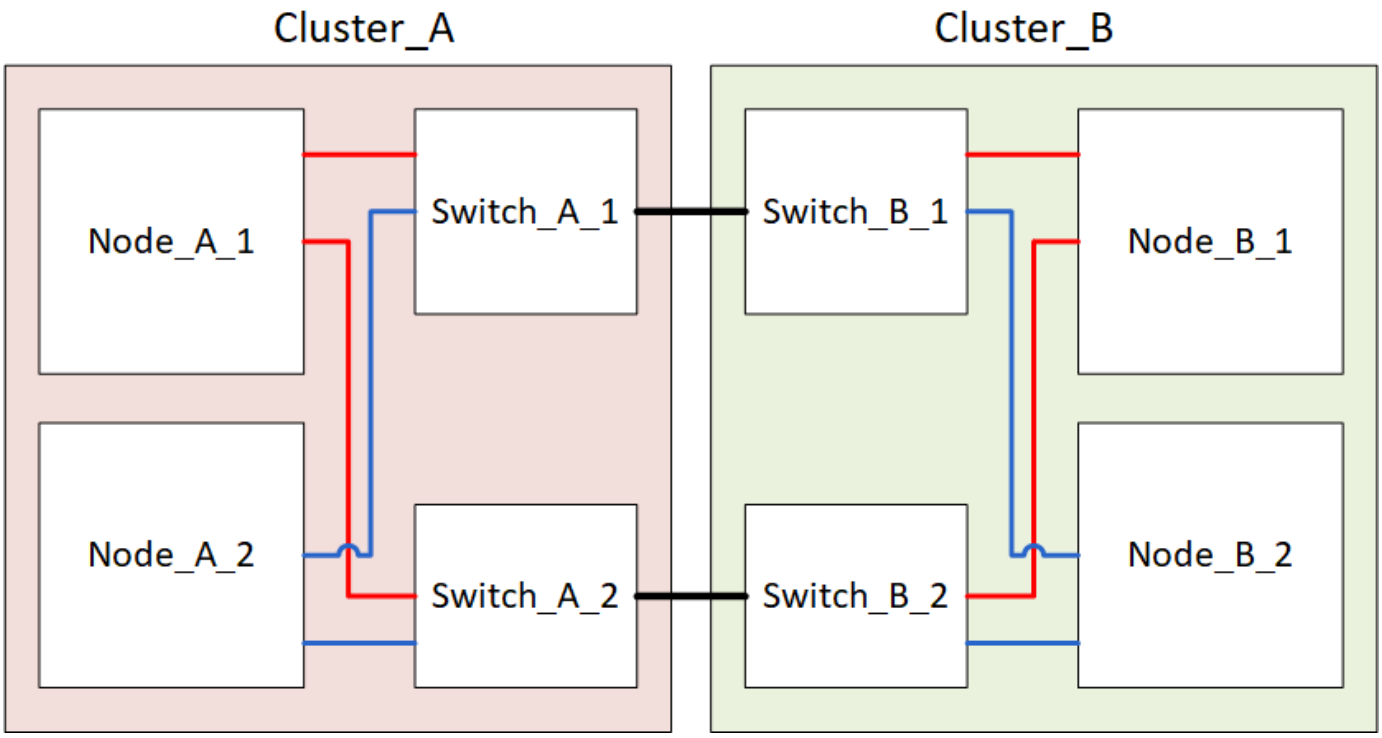
```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          false
1           cluster_A  node_A_2  configured          false
1           cluster_B  node_B_1  configured          false
1           cluster_B  node_B_2  configured          false
4 entries were displayed.
```

MetroCluster IP構成での単一サイトの電源オフと電源オン

MetroCluster IP構成でサイトのメンテナンスを実施したり、単一サイトを再配置したりする必要がある場合は、サイトの電源をオフにしてオンにする方法を把握しておく必要があります。

サイトを再配置して再設定する必要がある場合（4ノードクラスタから8ノードクラスタに拡張する必要がある場合など）は、これらのタスクを同時に実行することはできません。この手順では、サイトのメンテナンスを実行するため、またはサイトの構成を変更せずにサイトを再配置するために必要な手順のみを説明します。

次の図は、 MetroCluster 構成を示しています。メンテナンスのためにcluster_Bの電源がオフになっています。



MetroClusterサイトの電源をオフにする

サイトのメンテナンスや再配置を開始する前に、サイトとすべての機器の電源をオフにする必要があります。

このタスクについて

次の手順のすべてのコマンドは、電源をオンにしたままのサイトから実行されます。

手順

1. 開始する前に、ミラーされていないアグリゲートがサイトですべてオフラインになっていることを確認します。
2. ONTAP で MetroCluster 構成の動作を確認します。
   a. システムがマルチパスかどうかを確認します。

      'node run -node _node-name_sysconfig -a

   b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

      「 system health alert show 」というメッセージが表示されます

   c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

      「 MetroCluster show 」

   d. MetroCluster チェックを実行します + MetroCluster チェックを実行します
   e. MetroCluster チェックの結果を表示します。

      MetroCluster チェックショー

f. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

「 storage switch show 」と表示されます

g. Config Advisor を実行します。

"ネットアップのダウンロード： Config Advisor"

h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

3. 稼働したままにするサイトから、スイッチオーバーを実施します。

MetroCluster スイッチオーバー

```
cluster_A::*> metrocluster switchover
```

この処理が完了するまでに数分かかることがあります。

4. スイッチオーバーの完了を監視して確認します。

「 MetroCluster operation show 」を参照してください

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. ONTAP 9.6 以降を実行している MetroCluster IP 構成がある場合は、ディザスタサイトのプレックスがオンラインになり、修復処理が自動的に完了するまで待ちます。

ONTAP 9.5以前を実行しているMetroCluster IP構成では、ディザスタサイトのノードはONTAPで自動的にブートせず、プレックスはオフラインのままです。

6. ミラーされていないアグリゲートに属するボリュームとLUNをすべてオフラインにします。

a. ボリュームをオフラインにします。

```
cluster_A::* volume offline <volume name>
```

b. LUNをオフラインにします。

```
cluster_A::* lun offline lun_path <lun_path>
```

7. ミラーされていないアグリゲートをオフラインにします：「storage aggregate offline

```
cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
```

8. 構成と ONTAP のバージョンに応じて、ディザスタサイト（ cluster_B ）にあるオフラインの影響を受けるプレックスを特定して移動します。

   次のプレックスをオフラインにする必要があります。

   ◦ ディザスタサイトにあるディスクにあるミラーリングされていないプレックス

     ディザスタサイトのミラーされていないプレックスをオフラインにしないと、あとでディザスタサイトの電源をオフにしたときにシステムが停止する可能性があります。

   ◦ ディザスタサイトのディスクにあるミラーされたプレックスを使用してアグリゲートをミラーリングする。オフラインにすると、プレックスにアクセスできなくなります。

   a. 影響を受けるプレックスを特定します。

      サバイバーサイトのノードが所有するプレックスは、プール 1 のディスクで構成されます。ディザスタサイトのノードが所有するプレックスは、プール 0 のディスクで構成されます。

```
Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

影響を受けるプレックスは、クラスタ A のリモートにあるプレックスです次の表に、ディスクがクラスタ A に対してローカルかリモートかを示します。

ノード	プール内のディスク	ディスクをオフラインにする必要があるか	オフラインにするプレックスの例を指定します
Node_a_1 および Node_a_2	プール 0 内のディスク	いいえディスクはクラスタ A に対してローカルです	-

プール 1 内のディスク	はい。ディスクはクラスタ A に対してリモートです	node_A_1 の aggr0 / プレックス 4 を使用します node_A_1 の aggr1 / plex1 node_a_2_aggr0/plex4 Node_a_2_aggr1 / plex1 です	Node_B_1 および Node_B_2
プール 0 内のディスク	はい。ディスクはクラスタ A に対してリモートです	node_B_1 の aggr1 / plex0 node_B_1 の aggr0/plex0 node_B_2 の aggr0 / plex0 node_B_2 の aggr1 / plex0	プール 1 内のディスク

b. 影響を受けるプレックスをオフラインにします。

「ストレージアグリゲートのプレックスはオフライン」です

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+

この手順は、Cluster_Aに対してリモートのディスクを含むすべてのプレックスに対して実行します。

9. スイッチタイプに応じて、ISLスイッチポートを永続的にオフラインにします。
10. 各ノードで次のコマンドを実行して、ノードを停止します。

```
node halt -inhibit-takeover true -skip-lif-migration true -node <node-name>
```

11. ディザスタサイトの機器の電源をオフにします。

次の機器の電源を、記載されている順序でオフにする必要があります。

- ストレージコントローラ-ストレージコントローラは現在、 `LOADER` プロンプトが表示されたら、電源を完全にオフにする必要があります。
- MetroCluster IP スイッチ
- ストレージシェルフ

電源がオフになっている **MetroCluster** サイトの再配置

サイトの電源をオフにしたら、メンテナンス作業を開始できます。手順は、 MetroCluster コンポーネントを同じデータセンター内で再配置する場合も、別のデータセンターに再配置する場合も同じです。

- ハードウェアは、前のサイトと同じ方法でケーブル接続する必要があります。
- スイッチ間リンク（ ISL ）の速度、長さ、または数が変わった場合は、すべて再設定する必要があります。

手順

1. 新しい場所で正しく再接続できるように、すべてのコンポーネントのケーブル配線が慎重に記録されていることを確認します。
2. すべてのハードウェア、ストレージコントローラ、IPスイッチ、FibreBridge、およびストレージシェルフを物理的に再配置します。
3. ISL ポートを設定し、サイト間接続を確認します。
   a. IPスイッチの電源をオンにします。

      他の機器の電源はオンにしないでください。

4. スイッチのツールを使用して（使用可能な場合）、サイト間接続を確認します。

   リンクが正しく設定され、安定している場合にのみ続行してください。

5. リンクが安定していることがわかった場合は、リンクを再度無効にします。

MetroCluster 構成の電源をオンにして通常動作に戻します

メンテナンスを完了、またはサイトを移動したら、サイトの電源をオンにして MetroCluster 構成を再確立する必要があります。

このタスクについて

次の手順のすべてのコマンドは、電源をオンにしたサイトから実行します。

手順

1. スイッチの電源をオンにします。

   最初にスイッチの電源をオンにする必要があります。サイトを再配置した場合は、前の手順で電源がオンになっている可能性があります。

   a. 必要に応じて、または再配置中に実行されていない場合は、スイッチ間リンク（ ISL ）を再設定します。
   b. フェンシングが完了した場合、 ISL を有効にします。
   c. ISL を確認します。
2. ストレージコントローラの電源をオンにし、 `LOADER` プロンプト。コントローラが完全にブートしないようにする必要があります。

   自動起動が有効になっている場合は、 `Ctrl+C` コントローラの自動ブートを停止します。

3. シェルフの電源をオンにし、電源が完全にオンになるまで十分な時間を確保します。
4. ストレージが認識されていることを確認します。
   a. サバイバーサイトからストレージが認識されていることを確認します。オフラインのプレックスをオ

ンラインに戻して再同期処理を再開し、SyncMirrorを再確立します。

b. メンテナンスモードのノードからローカルストレージが認識されていることを確認します。

「ディスクショー V 」

5. MetroCluster 構成を再確立します。

の手順に従います "スイッチバックに向けたシステムの事前チェック" MetroCluster 構成に応じて修復処理とスイッチバック処理を実行します。

MetroCluster IP 構成全体の電源をオフにします

メンテナンスや再配置を開始する前に、 MetroCluster IP 構成全体とすべての機器の電源をオフにする必要があります。

ONTAP 9.8 以降では '**storage switch ***' コマンドは '***system switch**' に置き換えられています以下の手順は '*storage switch *' コマンドを示していますが 'ONTAP 9.8 以降を実行している場合は '*system switch *' コマンドを使用することをお勧めします

1. MetroCluster 構成の両方のサイトから MetroCluster 構成を確認します。
   a. MetroCluster の構成と運用モードが正常な状態であることを確認します。`+* MetroCluster show*`
   b. 次のコマンドを実行します :+**`MetroCluster interconnect show`**
   c. いずれかの MetroCluster ノードで次のコマンドを入力して、ディスクへの接続を確認します。 `+*run local sysconfig -v *`
   d. 次のコマンドを実行します :`+* storage port show *`
   e. 次のコマンドを実行します :`+* storage switch show *`
   f. 次のコマンドを実行します :`+* network interface show *`
   g. 次のコマンドを実行します :`+* network port show *`
   h. 次のコマンドを実行します :`+* network device-discovery show *`
   i. MetroCluster チェック :`+* MetroCluster check run*` を実行します
   j. MetroCluster チェックの結果を表示します :`+* MetroCluster check show*`
   k. 次のコマンドを実行します。 `+* MetroCluster configurion-settings interface show *`
2. 必要に応じて、 AUSO 障害ドメインをに変更して AUSO を無効にします

「 * auso-disabled * 」と表示されます

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```

MetroCluster IP 構成では、 ONTAP メディエーターが設定されていないかぎり、 AUSO 障害ドメインはすでに「 auso-disabled 」に設定されています。

3. コマンドを使用して、変更を確認します

   「 * MetroCluster operation show * 」と表示されます

```
cluster_A_site_A::*> metrocluster operation show
   Operation: modify
       State: successful
  Start Time: 4/25/2020 20:20:36
    End Time: 4/25/2020 20:20:36
      Errors: -
```

4. ノードを停止します。

   *halt *`

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore-quorum
-warnings true
```

5. サイトで次の機器の電源をオフにします。
   - ストレージコントローラ
   - MetroCluster IP スイッチ
   - ストレージシェルフ
6. 30分待ってから、すべてのストレージシェルフ、MetroCluster IPスイッチ、およびストレージコントローラの電源をオンにします。
7. コントローラの電源をオンにしたら、両方のサイトで MetroCluster 構成を確認します。

   設定を確認するには、手順 1 を繰り返します。

8. 電源再投入チェックを実行します。
   a. すべての同期元 SVM がオンラインであることを確認します。 +* vserver show *
   b. オンラインでない同期元の SVM をすべて起動します。 +* vserver start *

著作権に関する情報

商標に関する情報