



# ネットワーク情報の表示

## ONTAP 9

NetApp  
December 20, 2024

# 目次

ネットワーク情報の表示	1
ネットワーク情報の概要を表示する	1
ネットワークポート情報を表示します。	1
VLANに関する情報を表示する（クラスタ管理者のみ）	3
インターフェイスグループ情報の表示（クラスタ管理者のみ）	4
LIF情報を表示する	5
ルーティング情報を表示します。	8
DNSホストテーブルエントリを表示する（クラスタ管理者のみ）	9
DNSドメイン設定の表示	10
フェイルオーバーグループに関する情報を表示する	11
LIFのフェイルオーバーターゲットを表示します。	12
ロードバランシングゾーンのLIFを表示する	14
ONTAPのクラスタ接続を表示します。	15
ネットワークアクモンタイノシタンヨウコマンド	21
近接探索プロトコルによるネットワーク接続を表示します。	22

# ネットワーク情報の表示

## ネットワーク情報の概要を表示する

CLIを使用して、ポート、LIF、ルート、フェイルオーバールール、フェイルオーバーグループ、ファイアウォールルール、DNS、NIS、および接続に関する情報を表示できます。ONTAP 9.8以降では、ネットワークについてSystem Managerに表示されるデータもダウンロードできます。

この情報は、ネットワーク設定の再設定時やクラスタのトラブルシューティング時に役立ちます。

クラスタ管理者は、ネットワーク情報をすべて表示できます。SVM管理者は、割り当てられているSVMに関する情報のみを表示できます。

System Managerの\_リスト表示\_に情報を表示するときに\*[ダウンロード]\*をクリックすると、表示されているオブジェクトのリストがダウンロードされます。

- このリストは、カンマ区切り値（CSV）形式でダウンロードされます。
- 表示されている列のデータのみがダウンロードされます。
- CSV ファイル名は、オブジェクト名とタイムスタンプでフォーマットされます。

## ネットワークポート情報を表示します。

クラスタ内の特定のポート、またはすべてのノードのすべてのポートに関する情報を表示できます。

タスクの内容

次の情報が表示されます。

- ノード名
- ポート名
- IPspace名
- ブロードキャストドメイン名
- リンクステータス（upまたはdown）
- MTUの設定
- ポート速度の設定と動作ステータス（1ギガビットまたは10ギガビット/秒）
- 自動ネゴシエーション設定（trueまたはfalse）
- 二重モードと動作ステータス（halfまたはfull）
- ポートのインターフェイスグループ（該当する場合）
- ポートのVLANタグ情報（該当する場合）
- ポートのヘルスステータス（healthまたはdegraded）

- ポートがデグレードとマークされた理由

該当するデータがないフィールドの値はと表示されます（アクティブでないポートの二重モードの動作中や速度は表示されません）。 -

ステップ

コマンドを使用して、ネットワークポートの情報を表示します `network port show`。

各ポートの詳細情報を表示するには、パラメータを指定します。特定の情報を表示`-instance`するには、パラメータを使用してフィールド名を指定し`-fields`ます。

```

network port show
Node: node1

Ignore
Speed (Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0b      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0c      Default      Default      up    1500  auto/1000  degraded
false
e0d      Default      Default      up    1500  auto/1000  degraded
true
Node: node2

Ignore
Speed (Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0b      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0c      Default      Default      up    1500  auto/1000  healthy
false
e0d      Default      Default      up    1500  auto/1000  healthy
false
8 entries were displayed.

```

## VLANに関する情報を表示する（クラスタ管理者のみ）

クラスタ内の特定の VLAN またはすべての VLAN の情報を表示できます。

### タスクの内容

パラメータを指定すると、各VLANの詳細情報を表示できます `-instance`。特定の情報を表示するには、パラメータを使用してフィールド名を指定し ``-fields`` ます。

## ステップ

コマンドを使用して、VLANに関する情報を表示します `network port vlan show`。次のコマンドは、クラスタ内のすべてのVLANに関する情報を表示します。

```
network port vlan show
                Network Network
Node   VLAN Name Port   VLAN ID  MAC Address
-----
cluster-1-01
    a0a-10  a0a    10      02:a0:98:06:10:b2
    a0a-20  a0a    20      02:a0:98:06:10:b2
    a0a-30  a0a    30      02:a0:98:06:10:b2
    a0a-40  a0a    40      02:a0:98:06:10:b2
    a0a-50  a0a    50      02:a0:98:06:10:b2
cluster-1-02
    a0a-10  a0a    10      02:a0:98:06:10:ca
    a0a-20  a0a    20      02:a0:98:06:10:ca
    a0a-30  a0a    30      02:a0:98:06:10:ca
    a0a-40  a0a    40      02:a0:98:06:10:ca
    a0a-50  a0a    50      02:a0:98:06:10:ca
```

## インターフェイスグループ情報の表示（クラスタ管理者のみ）

インターフェイスグループに関する情報を表示して、その設定を確認できます。

### タスクの内容

次の情報が表示されます。

- インターフェイスグループが配置されているノード
- インターフェイスグループに含まれているネットワークポートのリスト
- インターフェイスグループの名前
- 分散機能（MAC、IP、ポート、またはシーケンシャル）
- インターフェイスグループの Media Access Control（MAC；メディアアクセス制御）アドレス
- ポートのアクティビティステータス。集約されたポートがアクティブであるかどうか（すべてのポートがアクティブであるかどうか）、アクティブであるポートがないかどうか（一部のポートがアクティブであるかどうか）、アクティブでないかどうかを示します

## ステップ

コマンドを使用して、インターフェイスグループに関する情報を表示します `network port ifgrp show`。

各ノードの詳細情報を表示するには、パラメータを指定し `-instance` ます。特定の情報を表示するには、パラメータを使用してフィールド名を指定し `-fields` ます。

次のコマンドは、クラスタ内のすべてのインターフェイスグループに関する情報を表示します。

```

network port ifgrp show
      Port      Distribution
Node   IfGrp      Function      MAC Address      Active
-----
cluster-1-01
      a0a      ip            02:a0:98:06:10:b2  full      e7a, e7b
cluster-1-02
      a0a      sequential    02:a0:98:06:10:ca  full      e7a, e7b
cluster-1-03
      a0a      port          02:a0:98:08:5b:66  full      e7a, e7b
cluster-1-04
      a0a      mac           02:a0:98:08:61:4e  full      e7a, e7b

```

次のコマンドは、1つのノードのインターフェイスグループの詳細情報を表示します。

```

network port ifgrp show -instance -node cluster-1-01

      Node: cluster-1-01
Interface Group Name: a0a
Distribution Function: ip
      Create Policy: multimode
      MAC Address: 02:a0:98:06:10:b2
Port Participation: full
      Network Ports: e7a, e7b
      Up Ports: e7a, e7b
      Down Ports: -

```

## LIF情報を表示する

LIFに関する詳細情報を表示して、その設定を確認できます。

この情報は、IPアドレスが重複していないか、ネットワークポートが正しいサブネットに属しているかなど、LIFの基本的な問題を診断するのにも便利です。Storage Virtual Machine (SVM) 管理者は、SVMに関連付けられているLIFの情報だけを表示できます。

タスクの内容

次の情報が表示されます。

- LIFに関連付けられているIPアドレス
- LIFの管理ステータス
- LIFの動作ステータス

データLIFの動作ステータスは、そのデータLIFが関連付けられているSVMのステータスによって決まります。SVMが停止すると、LIFの動作ステータスがdownに変わります。SVMが再び起動すると、動

作ステータスは up に変わります

- LIF が配置されているノードとポート

該当するデータがないフィールド（ステータスの詳しい情報がない場合など）については、と表示されます -。

ステップ

network interface show コマンドを使用して、LIF の情報を表示します。

各 LIF の詳しい情報を表示するには、-instance パラメータを指定します。特定の情報を表示するには、-fields パラメータを使用してフィールド名を指定します。

次のコマンドは、クラスタ内のすべての LIF に関する一般的な情報を表示します。



network interface show

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
example	lif1	up/up	192.0.2.129/22	node-01	e0d
false node	cluster_mgmt	up/up	192.0.2.3/20	node-02	e0c
false node-01	clus1	up/up	192.0.2.65/18	node-01	e0a
true	clus2	up/up	192.0.2.66/18	node-01	e0b
true	mgmt1	up/up	192.0.2.1/20	node-01	e0c
true node-02	clus1	up/up	192.0.2.67/18	node-02	e0a
true	clus2	up/up	192.0.2.68/18	node-02	e0b
true	mgmt2	up/up	192.0.2.2/20	node-02	e0d
true vs1	d1	up/up	192.0.2.130/21	node-01	e0d
false	d2	up/up	192.0.2.131/21	node-01	e0d
true	data3	up/up	192.0.2.132/20	node-02	e0c
true					

次のコマンドは、1つの LIF に関する詳細情報を表示します。

```
network interface show -lif data1 -instance

        Vserver Name: vs1
Logical Interface Name: data1
        Role: data
    Data Protocol: nfs,cifs
        Home Node: node-01
        Home Port: e0c
    Current Node: node-03
    Current Port: e0c
Operational Status: up
    Extended Status: -
        Is Home: false
    Network Address: 192.0.2.128
        Netmask: 255.255.192.0
    Bits in the Netmask: 18
    IPv4 Link Local: -
        Subnet Name: -
Administrative Status: up
    Failover Policy: local-only
    Firewall Policy: data
        Auto Revert: false
Fully Qualified DNS Zone Name: xxx.example.com
    DNS Query Listen Enable: false
    Failover Group Name: Default
        FCP WWPN: -
    Address family: ipv4
        Comment: -
    IPspace of LIF: Default
```

## ルーティング情報を表示します。

SVM内のルートに関する情報を表示できます。

### ステップ

表示するルーティング情報のタイプに応じて、該当するコマンドを入力します。

表示する情報	入力するコマンド
SVM の静的ルート	<code>network route show</code>
SVM の各ルートの LIF	<code>network route show-lifs</code>

パラメータを指定すると、各ルートの詳細情報を表示できます `-instance`。次のコマンドは、`cluster-1` のSVM内の静的ルートを表示します。

```
network route show
Vserver          Destination      Gateway          Metric
-----
Cluster
0.0.0.0/0        10.63.0.1       10
cluster-1
0.0.0.0/0        198.51.9.1      10
vs1
0.0.0.0/0        192.0.2.1       20
vs3
0.0.0.0/0        192.0.2.1       20
```

次のコマンドは、`cluster-1`のすべてのSVM内の静的ルートと論理インターフェイス（LIF）の関連付けを表示します。

```
network route show-lifs
Vserver: Cluster
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        10.63.0.1       -

Vserver: cluster-1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        198.51.9.1      cluster_mgmt,
cluster-1_mgmt1,

Vserver: vs1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1       data1_1, data1_2

Vserver: vs3
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1       data2_1, data2_2
```

## DNSホストテーブルエントリを表示する（クラスタ管理者のみ）

DNS hosts テーブルエントリは、ホスト名と IP アドレスのマッピングです。クラスタ内

のすべての SVM のホスト名およびエイリアス名と IP アドレスのマッピングを表示することができます。

#### ステップ

vserver services name-service dns hosts show コマンドを使用して、すべての SVM のホスト名エントリを表示します。

次の例は、ホストテーブルエントリを表示します。

```
vserver services name-service dns hosts show
Vserver      Address      Hostname      Aliases
-----
cluster-1
              10.72.219.36  lnx219-36     -
vs1
              10.72.219.37  lnx219-37     lnx219-37.example.com
```

コマンドを使用して、SVM で DNS を有効にし、ホスト名解決に DNS を使用するように設定でき `vserver services name-service dns` ます。ホスト名は外部 DNS サーバを使用して解決されます。

## DNS ドメイン設定の表示

クラスタ内の1つ以上の Storage Virtual Machine (SVM) の DNS ドメイン設定を表示して、正しく設定されているかどうかを確認できます。

#### ステップ

コマンドを使用して、DNS ドメイン設定を表示します `vserver services name-service dns show`。

次のコマンドは、クラスタ内のすべての SVM の DNS 設定を表示します。

```
vserver services name-service dns show
Vserver      State      Domains      Name
-----
cluster-1    enabled    xyz.company.com  192.56.0.129,
              192.56.0.130
vs1          enabled    xyz.company.com  192.56.0.129,
              192.56.0.130
vs2          enabled    xyz.company.com  192.56.0.129,
              192.56.0.130
vs3          enabled    xyz.company.com  192.56.0.129,
              192.56.0.130
```

次のコマンドを実行すると、SVM vs1 の DNS 設定の詳細が表示されます。

```
vserver services name-service dns show -vserver vs1
      Vserver: vs1
      Domains: xyz.company.com
      Name Servers: 192.56.0.129, 192.56.0.130
      Enable/Disable DNS: enabled
      Timeout (secs): 2
      Maximum Attempts: 1
```

## フェイルオーバーグループに関する情報を表示する

フェイルオーバーグループに関する情報を表示することができます。これには、各フェイルオーバーグループ内のノードとポートのリスト、フェイルオーバーの有効/無効、各 LIF に適用されているフェイルオーバーポリシーの種類が含まれます。

手順

1. コマンドを使用して、各フェイルオーバーグループのターゲットポートを表示します `network interface failover-groups show`。

次のコマンドは、2ノードクラスタのすべてのフェイルオーバーグループに関する情報を表示します。

```
network interface failover-groups show
      Vserver      Group      Failover
      -----      -
      Cluster
      vs1          Cluster
                  cluster1-01:e0a, cluster1-01:e0b,
                  cluster1-02:e0a, cluster1-02:e0b
      vs1          Default
                  cluster1-01:e0c, cluster1-01:e0d,
                  cluster1-01:e0e, cluster1-02:e0c,
                  cluster1-02:e0d, cluster1-02:e0e
```

2. コマンドを使用して、特定のフェイルオーバーグループのターゲットポートとブロードキャストドメインを表示します `network interface failover-groups show`。

次のコマンドは、SVM vs4 の data12 というフェイルオーバーグループに関する詳しい情報を表示します。

```
network interface failover-groups show -vserver vs4 -failover-group data12
```

```
Vserver Name: vs4
Failover Group Name: data12
Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                  cluster1-02:e0g
Broadcast Domain: Default
```

3. コマンドを使用して、すべてのLIFで使用されているフェイルオーバー設定を表示します `network interface show`。

次のコマンドは、各 LIF で使用されているフェイルオーバーポリシーとフェイルオーバーグループを表示します。

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver    lif                failover-policy    failover-group
-----
Cluster    cluster1-01_clus_1 local-only          Cluster
Cluster    cluster1-01_clus_2 local-only          Cluster
Cluster    cluster1-02_clus_1 local-only          Cluster
Cluster    cluster1-02_clus_2 local-only          Cluster
cluster1   cluster_mgmt       broadcast-domain-wide Default
cluster1   cluster1-01_mgmt1  local-only          Default
cluster1   cluster1-02_mgmt1  local-only          Default
vs1        data1               disabled            Default
vs3        data2               system-defined      group2
```

## LIFのフェイルオーバーターゲットを表示します。

LIF のフェイルオーバーポリシーとフェイルオーバーグループが正しく設定されているかどうかを確認しなければならない場合があります。フェイルオーバールールを間違っ  
て設定しないように、1つまたはすべての LIF のフェイルオーバーターゲットを表示できます。

### タスクの内容

LIF のフェイルオーバーターゲットを表示すると、次のことを確認できます。

- LIF に正しいフェイルオーバーグループとフェイルオーバーポリシーが設定されているかどうか
- 表示されたフェイルオーバーターゲットのポートが LIF に適しているかどうか
- データ LIF のフェイルオーバーターゲットが管理ポート（e0M）でないかどうか

## ステップ

コマンドのオプションを `network interface show`` 使用して、LIFのフェイルオーバーターゲットを表示します `failover。

次のコマンドは、2ノードクラスタのすべてのLIFのフェイルオーバーターゲットに関する情報を表示します。行はFailover Targets、特定のLIFにおけるノードとポートの組み合わせの（優先順位の高い）リストを示しています。

```
network interface show -failover
      Logical      Home      Failover      Failover
Vserver Interface  Node:Port      Policy      Group
-----
Cluster
      node1_clus1  node1:e0a      local-only    Cluster
      Failover Targets: node1:e0a,
                        node1:e0b
      node1_clus2  node1:e0b      local-only    Cluster
      Failover Targets: node1:e0b,
                        node1:e0a
      node2_clus1  node2:e0a      local-only    Cluster
      Failover Targets: node2:e0a,
                        node2:e0b
      node2_clus2  node2:e0b      local-only    Cluster
      Failover Targets: node2:e0b,
                        node2:e0a
cluster1
      cluster_mgmt node1:e0c      broadcast-domain-wide
                        Default
      Failover Targets: node1:e0c,
                        node1:e0d,
                        node2:e0c,
                        node2:e0d
      node1_mgmt1  node1:e0c      local-only    Default
      Failover Targets: node1:e0c,
                        node1:e0d
      node2_mgmt1  node2:e0c      local-only    Default
      Failover Targets: node2:e0c,
                        node2:e0d
vs1
      data1        node1:e0e      system-defined bcast1
      Failover Targets: node1:e0e,
                        node1:e0f,
                        node2:e0e,
                        node2:e0f
```

## ロードバランシングゾーンのLIFを表示する

ロードバランシングゾーンに属するすべてのLIFを表示することで、そのゾーンが正しく設定されているかどうかを確認できます。特定のLIFのロードバランシングゾーン、またはすべてのLIFのロードバランシングゾーンを表示することもできます。

### ステップ

次のいずれかのコマンドを使用して、必要なLIFとロードバランシングの詳細を表示します。

表示する内容	入力するコマンド
特定のロードバランシングゾーンに属する LIF	<code>network interface show -dns-zone zone_name</code> <code>'zone_name'</code> ロードバランシングゾーンの名前を指定します。
特定の LIF のロードバランシングゾーン	<code>network interface show -lif lif_name -fields dns-zone</code>
すべての LIF のロードバランシングゾーン	<code>network interface show -fields dns-zone</code>

### LIFのロードバランシングゾーンを表示する例

次のコマンドは、SVM vs0のstorage.company.comというロードバランシングゾーンに属するすべてのLIFの詳細を表示します。

```
net int show -vserver vs0 -dns-zone storage.company.com
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0	lif3	up/up	10.98.226.225/20	ndeux-11	e0c	true
	lif4	up/up	10.98.224.23/20	ndeux-21	e0c	true
	lif5	up/up	10.98.239.65/20	ndeux-11	e0c	true
	lif6	up/up	10.98.239.66/20	ndeux-11	e0c	true
	lif7	up/up	10.98.239.63/20	ndeux-21	e0c	true
	lif8	up/up	10.98.239.64/20	ndeux-21	e0c	true

次のコマンドは、data3というLIFのDNSゾーンの詳細を表示します。



```
network interface show -lif data3 -fields dns-zone
Vserver  lif      dns-zone
-----  -----  -----
vs0      data3    storage.company.com
```

次のコマンドは、クラスタ内のすべてのLIFとそれに対応するDNSゾーンのリストを表示します。

```
network interface show -fields dns-zone
Vserver  lif      dns-zone
-----  -----  -----
cluster  cluster_mgmt  none
ndeux-21 clus1     none
ndeux-21 clus2     none
ndeux-21 mgmt1    none
vs0      data1     storage.company.com
vs0      data2     storage.company.com
```

## ONTAPのクラスタ接続を表示します。

クラスタ内のすべてのアクティブな接続を表示したり、クライアント、論理インターフェイス、プロトコル、またはサービス別にノードのアクティブな接続数を表示したりできます。クラスタ内のリスンしている接続をすべて表示することもできます。

### クライアント別のアクティブな接続を表示する（クラスタ管理者のみ）

クライアント別にアクティブな接続を表示して、特定のクライアントが使用しているノードを確認したり、ノードあたりのクライアント数に不均衡がないかどうかを確認したりできます。

#### タスクの内容

クライアント別のアクティブな接続数の情報は、次のような場合に役立ちます。

- ビジー状態や過負荷のノードを見つける。
- 特定のクライアントからのボリュームへのアクセスが低速になっている理由を確認する。

クライアントがアクセスしているノードに関する詳細を表示し、ボリュームが配置されているノードと比較できます。ボリュームへのアクセスにクラスタ ネットワークのトラバースが必要な場合、オーバーサブスクライブされたリモート ノードにあるボリュームへのリモート アクセスにより、クライアントのパフォーマンスが低下することがあります。

- データ アクセスにすべてのノードが均等に使用されていることを確認する。
- 接続数が想定よりも多いクライアントを探す。
- 特定のクライアントがノードに接続しているかどうかを確認する。

#### ステップ

コマンドを使用して、ノードのアクティブな接続数をクライアント別に表示します `network connections active show-clients`。

リンク<http://docs.netapp.com/us-en/ontap-cli/network-connections-active-show-clients.html> [network connections active show-clients^]コマンドを参照してください。

```
network connections active show-clients
Node      Vserver Name      Client IP Address      Count
-----  -
node0     vs0                192.0.2.253            1
          vs0                192.0.2.252            2
          Cluster          192.10.2.124           5
node1     vs0                192.0.2.250            1
          vs0                192.0.2.252            3
          Cluster          192.10.2.123           4
node2     vs1                customer.example.com    1
          vs1                192.0.2.245            3
          Cluster          192.10.2.122           4
node3     vs1                customer.example.org    1
          vs1                customer.example.net    3
          Cluster          192.10.2.121           4
```

## プロトコル別のアクティブな接続を表示する（クラスタ管理者のみ）

ノードのアクティブな接続数をプロトコル（TCPまたはUDP）別に表示して、クラスタ内のプロトコルの使用状況を比較できます。

### タスクの内容

プロトコル別のアクティブな接続数の情報は、次のような場合に役立ちます。

- 接続が切断されているUDPクライアントを探す。

ノードの接続数が制限に近づいたときに最初に接続が切断されるのはUDPクライアントです。

- 他のプロトコルが使用されていないことを確認する。

### ステップ

コマンドを使用して、ノードのアクティブな接続数をプロトコル別に表示します `network connections active show-protocols`。

このコマンドの詳細については、マニュアルページを参照してください。

```

network connections active show-protocols
Node      Vserver Name  Protocol  Count
-----
node0
      vs0      UDP      19
      Cluster  TCP      11
node1
      vs0      UDP      17
      Cluster  TCP      8
node2
      vs1      UDP      14
      Cluster  TCP      10
node3
      vs1      UDP      18
      Cluster  TCP      4

```

サービス別のアクティブな接続を表示します（クラスタ管理者のみ）。

クラスタ内の各ノードのアクティブな接続数をサービスタイプ（NFS、SMB、マウントなど）別に表示できます。これは、クラスタ内のサービスの使用状況を比較するのに役立ちます。これは、ノードのプライマリワークロードを特定するのに役立ちます。

タスクの内容

サービス別のアクティブな接続数の情報は、次のような場合に役立ちます。

- すべてのノードが適切なサービス用に使用されていること、そのサービスのロード バランシングが機能していることを確認する。
- 他のサービスが使用されていないことを確認する。コマンドを使用して、ノードのアクティブな接続数をサービス別に表示します `network connections active show-services`。

このコマンドの詳細については、マニュアルページを参照してください。 ["ONTAPコマンド リファレンス"](#)

```

network connections active show-services
Node          Vserver Name      Service           Count
-----
node0
      vs0          mount              3
      vs0          nfs                14
      vs0          nlm_v4            4
      vs0          cifs_srv          3
      vs0          port_map          18
      vs0          rclopcp           27
      Cluster      ctlopcp           60
node1
      vs0          cifs_srv          3
      vs0          rclopcp           16
      Cluster      ctlopcp           60
node2
      vs1          rclopcp           13
      Cluster      ctlopcp           60
node3
      vs1          cifs_srv          1
      vs1          rclopcp           17
      Cluster      ctlopcp           60

```

## ノードおよびSVMのLIF別にアクティブな接続を表示する

ノードおよびStorage Virtual Machine (SVM) 別のLIFのアクティブな接続数を表示して、クラスタ内のLIF間で接続数の不均衡がないかどうかを確認できます。

### タスクの内容

LIF別のアクティブな接続数は、次のような場合に役立ちます。

- 各LIFの接続数を比較して過負荷のLIFを特定する。
- すべてのデータLIFに対してDNSロードバランシングが機能していることを確認する。
- さまざまなSVMへの接続数を比較して、最もよく使用されているSVMを特定する。

### ステップ

コマンドを使用して、SVMとノードのアクティブな接続数をLIF別に表示します `network connections active show-lifs`。

このコマンドの詳細については、マニュアルページを参照してください。 ["ONTAPコマンド リファレンス"](#)

```

network connections active show-lifs
Node      Vserver Name  Interface Name  Count
-----
node0
    vs0        datalif1        3
    Cluster    node0_clus_1    6
    Cluster    node0_clus_2    5
node1
    vs0        datalif2        3
    Cluster    node1_clus_1    3
    Cluster    node1_clus_2    5
node2
    vs1        datalif2        1
    Cluster    node2_clus_1    5
    Cluster    node2_clus_2    3
node3
    vs1        datalif1        1
    Cluster    node3_clus_1    2
    Cluster    node3_clus_2    2

```

クラスタ内のアクティブな接続を表示します。

クラスタ内のアクティブな接続に関する情報を表示して、個々の接続で使用されているLIF、ポート、リモートホスト、サービス、Storage Virtual Machine (SVM)、およびプロトコルを確認できます。

タスクの内容

クラスタ内のアクティブな接続の情報は、次のような場合に役立ちます。

- 個々のクライアントで正しいノードの正しいプロトコルやサービスを使用していることを確認する。
- クライアントで特定の組み合わせのノード、プロトコル、およびサービスを使用してデータにアクセスできない場合に、同様のクライアントを探して設定やパケットトレースを比較する。

ステップ

コマンドを使用して、クラスタ内のアクティブな接続数を表示します `network connections active show`。

このコマンドの詳細については、マニュアルページを参照してください"[ONTAPコマンド リファレンス](#)"。

次のコマンドは、ノードnode1のアクティブな接続の情報を表示します。

```

network connections active show -node node1
Vserver  Interface          Remote
Name     Name:Local Port      Host:Port           Protocol/Service
-----  -
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700   TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700   TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700   TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700   TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700   TCP/ctlopcp
vs1     data1:111           host1.aa.com:10741  UDP/port-map
vs3     data2:111           host1.aa.com:10741  UDP/port-map
vs1     data1:111           host1.aa.com:12017  UDP/port-map
vs3     data2:111           host1.aa.com:12017  UDP/port-map

```

次のコマンドは、SVM vs1のアクティブな接続の情報を表示します。

```

network connections active show -vserver vs1
Vserver  Interface          Remote
Name     Name:Local Port      Host:Port           Protocol/Service
-----  -
Node: node1
vs1     data1:111           host1.aa.com:10741  UDP/port-map
vs1     data1:111           host1.aa.com:12017  UDP/port-map

```

## クラスタ内のリスンしている接続を表示する

クラスタ内のリスンしている接続に関する情報を表示して、特定のプロトコルおよびサービスの接続を受け入れているLIFとポートを確認できます。

### タスクの内容

クラスタ内のリスンしている接続の表示は、次のような場合に役立ちます。

- 特定のLIFへのクライアント接続が必ず失敗する場合に、そのLIFを適切なプロトコルまたはサービスでリスンしていることを確認する。
- あるノードのボリュームのデータに別のノードのLIFを介してリモート アクセスできない場合に、それぞれのクラスタLIFでUDP / rcllopcpリスナーが開いていることを確認する。
- 同じクラスタの2つのノード間でのSnapMirror転送に失敗した場合に、それぞれのクラスタLIFでUDP / rcllopcpリスナーが開いていることを確認する。
- 異なるクラスタの2つのノード間でのSnapMirror転送に失敗した場合に、それぞれのクラスタ間LIFでTCP / ctlopcpリスナーが開いていることを確認する。

### ステップ

コマンドを使用して、ノードごとにリスンしている接続を表示します `network connections listening`

show。

```
network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: node0
Cluster           node0_clus_1:7700              TCP/ctlopcp
vs1               data1:4049                     UDP/unknown
vs1               data1:111                       TCP/port-map
vs1               data1:111                       UDP/port-map
vs1               data1:4046                      TCP/sm
vs1               data1:4046                      UDP/sm
vs1               data1:4045                      TCP/nlm-v4
vs1               data1:4045                      UDP/nlm-v4
vs1               data1:2049                      TCP/nfs
vs1               data1:2049                      UDP/nfs
vs1               data1:635                       TCP/mount
vs1               data1:635                       UDP/mount
Cluster           node0_clus_2:7700              TCP/ctlopcp
```

## ネットワークモニタリングコマンド

ネットワークの問題を診断するには、`tcpdump`などのコマンドを使用し、`ping`、`traceroute`、`ndp`、`ping6`、`traceroute6`などのコマンドを使用して、IPv6の問題を診断することもできます。

状況	入力するコマンド
ノードがネットワーク上の他のホストに到達できるかどうかをテストする	<code>network ping</code>
ノードがIPv6ネットワーク上の他のホストに到達できるかどうかをテストする	<code>network ping6</code>
IPv4パケットがネットワーク ノードまでたどったルートをトレースする	<code>network traceroute</code>
IPv6パケットがネットワーク ノードまでたどったルートをトレースする	<code>network traceroute6</code>
近隣探索プロトコル (NDP) を管理する	<code>network ndp</code>
指定したネットワーク インターフェイスまたはすべてのネットワーク インターフェイスで送受信されたパケットの統計情報を表示する	<code>run -node node_name ifstat</code> 注：このコマンドはノードシェルから使用できます。
クラスタ内の各ノードおよびポートから検出された隣接デバイスに関する情報 (リモートデバイスのタイプやデバイスプラットフォームなど) を表示する	<code>network device-discovery show</code>

ノードのCDP隣接デバイスを表示する（ONTAPはCDPv1通知のみをサポート）	<code>run -node node_name cdpd show-neighbors</code> 注：このコマンドはノードシェルから使用できます。
ネットワークで送受信されたパケットをトレースする	<code>network tcpdump start -node node-name -port port_name</code> 注：このコマンドはノードシェルから使用できます。
クラスタ間ノードまたはクラスタ内ノード間のレイテンシとスループットを測定	<code>`network test -path -source-node source_nodename local -destination-cluster destination_clustername -destination-node destination_nodename -session -type Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer`</code> 詳細については、を参照して" <a href="#">パフォーマンス管理</a> "ください。

これらのコマンドの詳細については、を参照して "[ONTAPコマンド リファレンス](#)"ください。

## 近接探索プロトコルによるネットワーク接続を表示します。

近接探索プロトコルによるネットワーク接続を表示します。

データセンターでは、近接探索プロトコルを使用して、物理システムまたは仮想システムのペアとそれらのネットワークインターフェイス間のネットワーク接続を表示できます。ONTAPでは、2つの近接探索プロトコルとして、Cisco Discovery Protocol（CDP）とLink Layer Discovery Protocol（LLDP）がサポートされます。

近接探索プロトコルを使用すると、ネットワーク内の直接接続されたプロトコル対応デバイスを自動的に検出し、その情報を表示できます。各デバイスは、ID、機能、および接続情報をアドバタイズします。この情報はイーサネットフレームでマルチキャストMACアドレスに送信され、隣接するすべてのプロトコル対応デバイスで受信されます。

2つのデバイスをネイバーにするには、各デバイスでプロトコルが有効になっており、正しく設定されている必要があります。検出プロトコルの機能は、直接接続されたネットワークに限定されます。ネイバーには、スイッチ、ルータ、ブリッジなどのプロトコル対応デバイスを含めることができます。ONTAPでは、2つの近接探索プロトコルがサポートされており、個別に使用することも一緒に使用することもできます

- シスコ検出プロトコル（CDP）\*

CDPは、Cisco Systemsが開発した独自のリンク層プロトコルです。クラスタポートのONTAPではデフォルトで有効になりますが、データポートに対しては明示的に有効にする必要があります。

- リンク層検出プロトコル（LLDP）\*

LLDPは、標準ドキュメントIEEE 802.1ABで指定されているベンダーに依存しないプロトコルです。すべてのポートに対して明示的にイネーブルにする必要があります。

### CDPを使用したネットワーク接続の検出

CDPを使用したネットワーク接続の検出は、導入に関する考慮事項の確認、データポートでのCDPの有効化、近隣デバイスの表示、CDPの設定値の調整（必要な場合）で構成されます。クラスタポートでは、CDPはデフォルトで有効になります。



近隣デバイスに関する情報を表示するには、スイッチとルーターでもCDPを有効にする必要があります。

ONTAP リリース	説明
9.10.1以前	CDPは、クラスタスイッチヘルスマニタでも使用され、クラスタネットワークスイッチと管理ネットワークスイッチを自動的に検出します。
9.11.1以降	CDPは、クラスタ、ストレージ、および管理ネットワークスイッチを自動的に検出するためにクラスタスイッチヘルスマニタでも使用されます。

## 関連情報

["システム管理"](#)

### CDPを使用する場合の考慮事項

デフォルトでは、CDP対応デバイスはCDPv2通知を送信します。CDP対応デバイスは、CDPv1通知を受信した場合にのみCDPv1通知を送信します。ONTAPはCDPv1のみをサポートします。そのため、ONTAPノードがCDPv1通知を送信すると、CDP対応の隣接デバイスがCDPv1通知を返します。

ノードでCDPを有効にする前に、次の点を考慮してください。

- CDPはすべてのポートでサポートされます。
- CDP通知はup状態のポートから送受信されます。
- CDP通知を送受信するには、送信デバイスと受信デバイスの両方でCDPを有効にする必要があります。
- CDP通知は一定の間隔で送信され、送信間隔を設定できます。
- LIFのIPアドレスが変更されると、ノードは更新された情報を次のCDP通知で送信します。
- ONTAP 9.10.1以前：
  - CDPはクラスタ ポートで常に有効になります。
  - 非クラスタ ポートでは、CDPはデフォルトで無効になります。
- ONTAP 9.11.1以降：
  - CDPはクラスタ ポートとストレージ ポートで常に有効になります。
  - 非クラスタ ポートと非ストレージ ポートでは、CDPはデフォルトで無効になります。



ノードでLIFが変更された場合、スイッチなどの受信デバイス側でCDP情報が更新されないことがあります。このような問題が発生した場合は、ノードのネットワーク インターフェイスをいったんdown状態にしてから、up状態に設定してください。

- CDP通知で送信されるのはIPv4アドレスのみです。
- VLANが設定されている物理ネットワーク ポートの場合、VLANに設定されているすべてのLIFが通知されます。
- インターフェイス グループの一部となっている物理ポートの場合、そのインターフェイス グループに設定されているすべてのIPアドレスが、各物理ポートで通知されます。
- VLANをホストするインターフェイス グループの場合、インターフェイス グループおよびVLANに設定されているすべてのLIFが各ネットワーク ポートで通知されます。

- CDPパケットの最大サイズは1500バイトであるため、LIFが多数設定されたポートでは、隣接するスイッチで報告されるIPアドレスの一部しかありません。

## CDPの有効化または無効化

CDP対応の近隣デバイスを検出して通知を送信するには、クラスタの各ノードでCDPが有効になっている必要があります。

ONTAP 9.10.1以前では、CDPはデフォルトでノードのすべてのクラスタポートで有効に、非クラスタポートで無効になります。

ONTAP 9.11.1以降では、CDPはデフォルトでノードのすべてのクラスタポートとストレージポートで有効に、非クラスタポートと非ストレージポートで無効になります。

### タスクの内容

オプションは `cdpd.enable`、ノードのポートでCDPを有効にするか無効にするかを制御します。

- ONTAP 9.10.1以前の場合、`on`を指定すると、非クラスタポートでCDPが有効になります。
- ONTAP 9.11.1以降では、`on`を指定すると、クラスタ以外のポートとストレージ以外のポートでCDPが有効になります。
- ONTAP 9.10.1以前の場合、`off`を指定すると非クラスタポートのCDPが無効になります。クラスタポートのCDPが無効にすることはできません。
- ONTAP 9.11.1以降では、`off`を指定すると、非クラスタポートとストレージポートでCDPが無効になります。クラスタポートではCDPが無効にすることはできません。

CDP対応デバイスに接続されているポートでCDPが無効にすると、ネットワークトラフィックが最適化されない場合があります。

### 手順

1. クラスタ内の1つまたはすべてのノードの、現在のCDP設定を表示します。

CDP 設定を表示する対象	入力するコマンド
ノード	<code>run - node &lt;node_name&gt; options cdpd.enable</code>
クラスタ内のすべてのノード	<code>options cdpd.enable</code>

2. クラスタ内の1つまたはすべてのノードで、すべてのポートのCDPを有効または無効に設定します。

CDPを有効または無効にする対象	入力するコマンド
ノード	<code>run -node node_name options cdpd.enable {on or off}</code>
クラスタ内のすべてのノード	<code>options cdpd.enable {on or off}</code>

## CDP近隣情報の表示

クラスタのノードのポートにCDP対応デバイスが接続されている場合は、そのポートの近隣デバイスの情報を表示することができます。ネイバー情報を表示するには、コマンドを使用し `network device-discovery show -protocol cdp` ます。

### タスクの内容

ONTAP 9.10.1以前では、CDPはクラスタポートで常に有効になっているため、これらのポートのCDP隣接情報が常に表示されます。非クラスタポートの隣接情報を表示するには、非クラスタポートでCDPを有効にする必要があります。

ONTAP 9.11.1以降では、クラスタポートとストレージポートのCDPは常に有効になっているため、それらのポートのCDP隣接情報が常に表示されます。非クラスタポートおよび非ストレージポートのネイバー情報を表示するには、これらのポートでCDPを有効にする必要があります。

### ステップ

クラスタ内のノードのポートに接続されているすべてのCDP対応デバイスの情報を表示します。

```
network device-discovery show -node node -protocol cdp
```

次のコマンドは、ノードsti2650-212のポートに接続されている近隣デバイスの情報を表示します。

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface      Platform
-----
sti2650-212/cdp
              e0M    RTP-LF810-510K37.gdl.eng.netapp.com (SAL1942R8JS)
                                   Ethernet1/14    N9K-
C93120TX
              e0a    CS:RTP-CS01-510K35          0/8            CN1610
              e0b    CS:RTP-CS01-510K36          0/8            CN1610
              e0c    RTP-LF350-510K34.gdl.eng.netapp.com (FDO21521S76)
                                   Ethernet1/21    N9K-
C93180YC-FX
              e0d    RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                   Ethernet1/22    N9K-
C93180YC-FX
              e0e    RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                   Ethernet1/23    N9K-
C93180YC-FX
              e0f    RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                   Ethernet1/24    N9K-
C93180YC-FX
```

このコマンドの出力には、指定したノードの各ポートに接続されているCiscoデバイスが一覧表示されます。

## CDPメッセージの保持時間の設定

保持時間は、CDP通知がCDP対応の近隣デバイスのキャッシュに格納される時間です。保持時間は各CDPv1パケットで通知され、ノードがCDPv1パケットを受信するたびに更新されます。

- このオプションの値は `cdpd.holdtime`、HAペアの両方のノードで同じに設定する必要があります。
- デフォルトの保持時間の値は180秒ですが、10~255秒の範囲の値を入力できます。
- 保持期限が切れる前にIPアドレスが削除された場合、CDP情報は保持期限が切れるまでキャッシュされません。

### 手順

1. クラスタ内の1つまたはすべてのノードのCDPの現在の保持時間を表示します。

保持時間を表示する対象	入力するコマンド
ノード	<code>run -node node_name options cdpd.holdtime</code>
クラスタ内のすべてのノード	<code>options cdpd.holdtime</code>

2. クラスタ内の1つまたはすべてのノードのすべてのポートでCDP保持時間を設定します。

保持時間を設定する対象	入力するコマンド
ノード	<code>run -node node_name options cdpd.holdtime holdtime</code>
クラスタ内のすべてのノード	<code>options cdpd.holdtime holdtime</code>

## CDP通知の送信間隔を設定する

CDP通知は、一定の間隔でCDP近隣機器に送信されます。ネットワークトラフィックの量やネットワークトポロジの変化に応じて、CDP通知の送信間隔を調節することができます。

- このオプションの値は `cdpd.interval`、HAペアの両方のノードで同じに設定する必要があります。
- デフォルトの間隔は60秒ですが、5~900秒の値を入力できます。

### 手順

1. クラスタ内の1つまたはすべてのノードについて、CDP通知の現在の送信間隔を表示します。

送信間隔を表示する対象	入力するコマンド
ノード	<code>run -node node_name options cdpd.interval</code>
クラスタ内のすべてのノード	<code>options cdpd.interval</code>

2. クラスタ内の1つまたはすべてのノードのすべてのポートについて、CDP通知の送信間隔を設定します。

送信間隔を設定する対象	入力するコマンド
ノード	<code>run -node node_name options cdpd.interval interval</code>
クラスタ内のすべてのノード	<code>options cdpd.interval interval</code>

### CDP統計情報の表示と消去

ネットワーク接続で発生する可能性のある問題を見つけるために、各ノードのクラスタポートと非クラスタポートのCDP統計情報を確認できます。CDP統計情報は、前回消去されたときからの累積値です。

#### タスクの内容

ONTAP 9.10.1以前では、CDPはポートに対して常にイネーブルになっているため、これらのポートのトラフィックについては常にCDP統計情報が表示されます。ポートの統計情報を表示するには、CDPをポートでイネーブルにする必要があります。

ONTAP 9.11.1以降では、クラスタポートとストレージポートのCDPは常に有効になっているため、これらのポートのトラフィックのCDP統計は常に表示されます。非クラスタポートまたは非ストレージポートの統計を表示するには、非クラスタポートまたは非ストレージポートでCDPを有効にする必要があります。

#### ステップ

ノードのすべてのポートに関する現在のCDP統計情報を表示、または消去します。

状況	入力するコマンド
CDP統計情報を表示	<code>run -node node_name cdpd show-stats</code>
CDP統計情報を消去	<code>run -node node_name cdpd zero-stats</code>

#### 統計情報の表示と消去の例

次のコマンドは、消去する前のCDP統計情報の例を示します。前回統計情報が消去されてから、送信および受信したパケットの総数が出力されています。

```
run -node nodel cdpd show-stats
```

#### RECEIVE

```
Packets:          9116 | Csum Errors:      0 | Unsupported Vers: 4561
Invalid length:    0   | Malformed:        0 | Mem alloc fails:   0
Missing TLVs:      0   | Cache overflow:   0 | Other errors:      0
```

#### TRANSMIT

```
Packets:          4557 | Xmit fails:       0 | No hostname:      0
Packet truncated:  0   | Mem alloc fails:  0 | Other errors:      0
```

#### OTHER

```
Init failures:    0
```

次のコマンドは、CDP統計情報を消去します。

```
run -node nodel cdpd zero-stats
```

```
run -node nodel cdpd show-stats
```

#### RECEIVE

```
Packets:          0   | Csum Errors:      0 | Unsupported Vers:  0
Invalid length:    0   | Malformed:        0 | Mem alloc fails:   0
Missing TLVs:      0   | Cache overflow:   0 | Other errors:      0
```

#### TRANSMIT

```
Packets:          0   | Xmit fails:       0 | No hostname:      0
Packet truncated:  0   | Mem alloc fails:  0 | Other errors:      0
```

#### OTHER

```
Init failures:    0
```

統計情報を消去すると、次にCDP通知が送信または受信された時点から情報が累積されていきます。

### CDPがサポートされないイーサネットスイッチへの接続

一部のベンダースイッチではCDPがサポートされていません。 ["ONTAPデバイス検出でスイッチではなくノードが表示される"](#) 詳細については、ナレッジベースの記事を参照してください。

この問題を解決するには、次の2つの方法があります。

- CDPを無効にし、LLDPを有効にします（サポートされている場合）。詳細については、[を参照してください](#) ["LLDPを使用したネットワーク接続の検出"](#)。
- CDPアドバタイズメントをドロップするように、スイッチにMACアドレスパケットフィルタを設定しま

す。

## LLDPを使用したネットワーク接続の検出

LLDPを使用したネットワーク接続の検出は、導入に関する考慮事項の確認、すべてのポートでのLLDPの有効化、隣接デバイスの表示、LLDPの設定値の調整（必要な場合）で構成されます。

ネイバーデバイスに関する情報を表示するには、スイッチおよびルータでもLLDPをイネーブルにする必要があります。

ONTAPは現在、次のType-Length-Value構造体（TLV）を報告します。

- シャーシID
- ポートID
- Time-To-Live（TTL）
- システム名

システム名TLVは、CNAデバイスでは送信されません。

X1143アダプタやUTA2オンボードポートなどの特定の統合ネットワークアダプタ（CNA）にはLLDPのオフロードサポートが含まれています。

- LLDPのオフロードは、Data Center Bridging（DCB）に使用されます。
- 表示される情報がクラスタとスイッチの間で異なる場合があります。

スイッチで表示されるシャーシIDとポートIDのデータは、CNAポートとCNA以外のポートで異なる場合があります。

例：

- CNA以外のポートの場合：
  - シャーシIDは、ノード上のいずれかのポートの固定MACアドレスです。
  - port IDは、ノード上のそれぞれのポートのポート名です。
- CNAポートの場合：
  - シャーシIDとポートIDは、ノード上の各ポートのMACアドレスです。

ただし、これらのタイプのポートについては、クラスタで表示されるデータに一貫性があります。



LLDP仕様では、SNMP MIBを介した収集された情報へのアクセスが定義されています。ただし、ONTAPは現在LLDP MIBをサポートしていません。

## LLDPの有効化または無効化

LLDP対応の近隣デバイスを検出して通知を送信するには、クラスタの各ノードでLLDPが有効になっている必要があります。ONTAP 9.7以降では、ノードのすべてのポートでLLDPがデフォルトで有効になります。

## タスクの内容

LLDP .10.1以前の場合ONTAP 9は、`lldp.enable`オプションでノードのポートでLLDPを有効にするか無効にするかを制御します。

- `on`すべてのポートでLLDPをイネーブルにします。
- `off`すべてのポートでLLDPをディセーブルにします。

LLDP.11.1以降の場合、ONTAP 9オプションは、`lldp.enable`ノードの非クラスタポートおよびストレージポートでLLDPを有効にするか無効にするかを制御します。

- `on`すべての非クラスタポートおよびストレージポートでLLDPをイネーブルにします。
- `off`すべての非クラスタポートおよびストレージポートでLLDPを無効にします。

## 手順

1. クラスタ内の1つまたはすべてのノードの現在のLLDP設定を表示します。
  - シングルノード： `run -node node_name options lldp.enable`
  - すべてのノード： オプション `lldp.enable`
2. クラスタ内の1つまたはすべてのノードのすべてのポートでLLDPを有効または無効にします。

LLDPを有効または無効にする対象	入力するコマンド
ノード	<code>`run -node node_name options lldp.enable {on</code>
<code>off}`</code>	クラスタ内のすべてのノード
<code>`options lldp.enable {on</code>	<code>off}`</code>

- シングルノード：

```
run -node node_name options lldp.enable {on|off}
```

- すべてのノード：

```
options lldp.enable {on|off}
```

## LLDP近隣情報の表示

クラスタのノードのポートにLLDP対応デバイスが接続されている場合は、そのポートの近隣デバイスの情報を表示することができます。近隣情報を表示するには、`network device-discovery show`コマンドを使用します。

## ステップ



1. クラスタ内のノードのポートに接続されているすべてのLLDP準拠デバイスの情報を表示します。

```
network device-discovery show -node node -protocol lldp
```

次のコマンドは、ノードcluster-1\_01のポートに接続されているネイバーの情報を表示します。出力には、指定したノードの各ポートに接続されているLLDP対応デバイスが表示されます。この`-protocol`オプションを省略すると、CDP対応デバイスも出力に表示されます。

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/          Local   Discovered
Protocol       Port   Device                               Interface      Platform
-----
cluster-1_01/lldp
                e2a    0013.c31e.5c60                       GigabitEthernet1/36
                e2b    0013.c31e.5c60                       GigabitEthernet1/35
                e2c    0013.c31e.5c60                       GigabitEthernet1/34
                e2d    0013.c31e.5c60                       GigabitEthernet1/33
```

## LLDP通知の送信間隔を調整する

LLDP通知は、一定の間隔でLLDPネイバーに送信されます。ネットワークトラフィックやネットワークポロジの変化に応じて、LLDP通知の送信間隔を増減できます。

### タスクの内容

IEEEが推奨するデフォルトの間隔は30秒ですが、5~300秒の値を入力できます。

### 手順

1. クラスタ内の1つまたはすべてのノードについて、LLDP通知の現在の間隔を表示します。
  - シングルノード：

```
run -node <node_name> options lldp.xmit.interval
```

- すべてのノード：

```
options lldp.xmit.interval
```

2. クラスタ内の1つまたはすべてのノードのすべてのポートについて、LLDP通知の送信間隔を調整します。

- シングルノード：

```
run -node <node_name> options lldp.xmit.interval <interval>
```

- すべてのノード：

```
options lldp.xmit.interval <interval>
```

## LLDP通知のTime-To-Live値を調整する

Time-To-Live (TTL) は、LLDP通知がLLDP準拠の隣接デバイスのキャッシュに格納される期間です。TTLは各LLDPパケットでアドバタイズされ、ノードがLLDPパケットを受信するたびに更新されます。TTLは発信LLDPフレームで変更できます。

### タスクの内容

- TTLは計算された値(`lldp.xmit.interval` (送信間隔の積) と保持乗数(`lldp.xmit.hold`) に1を足したものです。
- デフォルトの保持乗数の値は4ですが、1~100の範囲の値を入力できます。
- したがって、IEEEが推奨するデフォルトのTTLは121秒ですが、送信間隔と保持乗数の値を調整することで、発信フレームの値を6秒から30001秒に指定できます。
- TTLが期限切れになる前にIPアドレスが削除された場合、LLDP情報はTTLが期限切れになるまでキャッシュされます。

### 手順

1. クラスタ内の1つまたはすべてのノードの現在の保持の乗数を表示します。

- シングルノード：

```
run -node <node_name> options lldp.xmit.hold
```

- すべてのノード：

```
options lldp.xmit.hold
```

2. クラスタ内の1つまたはすべてのノードのすべてのポートで、保持の乗数を調整します。

- シングルノード：

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

- すべてのノード：

```
options lldp.xmit.hold <hold_value>
```

## LLDP統計の表示またはクリア

各ノードのクラスタポートと非クラスタポートのLLDP統計を表示して、ネットワーク接続の潜在的な問題を検出できます。LLDP統計情報は、最後に消去された時点からの累積値です。

### タスクの内容

LLDP.10.1以前の場合、ONTAP 9はクラスタポートで常に有効になっているため、これらのポートのトラフィックについては常にLLDP統計が表示されます。非クラスタポートの統計を表示するには、非クラスタポートでLLDPを有効にする必要があります。

LLDPはクラスタポートとストレージポートで常に有効になるため、LLDP統計はそれらのポートのトラフィックについて常に表示されますONTAP 9。非クラスタポートおよびストレージポートの統計情報を表示するには、非クラスタポートおよびストレージポートでLLDPを有効にする必要があります。

### ステップ

ノードのすべてのポートの現在のLLDP統計を表示または消去します。

状況	入力するコマンド
LLDP統計を表示します	<code>run -node node_name lldp stats</code>
LLDP統計情報をクリアします	<code>run -node node_name lldp stats -z</code>

### 統計情報の表示と消去の例

次のコマンドは、クリア前のLLDP統計情報を表示します。出力には、統計情報が最後に消去されてから送受信されたパケットの合計数が表示されます。

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
  Total frames:      190k | Accepted frames:   190k | Total drops:
0
TRANSMIT
  Total frames:      5195 | Total failures:    0
OTHER
  Stored entries:    64
```

次のコマンドは、LLDP統計情報をクリアします。

```
cluster-1::> The following command clears the LLDP statistics:  
run -node vsim1 lldp stats -z  
run -node node1 lldp stats
```

RECEIVE

```
Total frames:          0 | Accepted frames:      0 | Total drops:  
0
```

TRANSMIT

```
Total frames:          0 | Total failures:       0
```

OTHER

```
Stored entries:        64
```

統計情報を消去すると、次のLLDPアドバタイズメントが送信または受信されたあとに統計情報が蓄積され始めます。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。