查看网络信息

ONTAP 9

NetApp
April 24, 2024

目录

查看网络信息

查看网络信息概述

使用命令行界面、您可以查看与端口、生命周期、路由、故障转移规则、故障转移组、 防火墙规则、DNS、NIS和连接。从ONTAP 9.8开始、您还可以下载System Manager中显示的网络数据。

在重新配置网络设置等情况下或对集群进行故障排除时，此信息非常有用。

如果您是集群管理员，则可以查看所有可用的网络信息。如果您是 SVM 管理员，则只能查看与分配的 SVM 相关的信息。

在System Manager中，当您在_List View_中显示信息时，您可以单击*Download*，显示的对象列表将被下载。

- 此列表将以逗号分隔值（ CSV ）格式下载。
- 仅下载可见列中的数据。
- CSV 文件名采用对象名称和时间戳的格式。

显示网络端口信息

您可以显示有关特定端口或集群中所有节点上所有端口的信息。

关于此任务

此时将显示以下信息：

- Node name
- 端口名称
- IPspace 名称
- 广播域名
- 链路状态（已启动或已关闭）
- MTU 设置
- 端口速度设置和运行状态（每秒 1 千兆位或 10 千兆位）
- 自动协商设置（ true 或 false ）
- 双工模式和运行状态（半双工或全满）
- 端口的接口组（如果适用）
- 端口的 VLAN 标记信息（如果适用）
- 端口的运行状况（运行状况或已降级）
- 端口标记为已降级的原因

如果字段的数据不可用(例如、非活动端口的操作双工和速度将不可用)、则字段值将列为 –。

步骤

使用显示网络端口信息 `network port show` 命令：

您可以通过指定来显示每个端口的详细信息 `-instance` 参数、或者通过使用指定字段名称来获取特定信息 `-fields` 参数。

```
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.
```

显示有关 VLAN 的信息（仅限集群管理员）

您可以显示有关特定 VLAN 或集群中所有 VLAN 的信息。

关于此任务

您可以通过指定来显示每个VLAN的详细信息 `-instance` 参数。您可以通过使用指定字段名称来显示特定信息 `-fields` 参数。

步骤

使用显示有关VLAN的信息 `network port vlan show` 命令：以下命令显示有关集群中所有 VLAN 的信息：

```
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
```

显示接口组信息（仅限集群管理员）

您可以显示有关接口组的信息以确定其配置。

关于此任务

此时将显示以下信息：

- 接口组所在的节点
- 接口组中包含的网络端口列表
- 接口组的名称
- 分发功能（ MAC ， IP ，端口或顺序）
- 接口组的介质访问控制（ MAC ）地址
- 端口活动状态；即所有聚合端口是否均处于活动状态（完全参与），某些端口是否处于活动状态（部分参与）或是否无处于活动状态

步骤

使用显示有关接口组的信息 `network port ifgrp show` 命令：

您可以通过指定来显示每个节点的详细信息 `-instance` 参数。您可以通过使用指定字段名称来显示特定信息 `-fields` 参数。

以下命令显示集群中所有接口组的相关信息：

```
network port ifgrp show
         Port     Distribution                    Active
Node     IfGrp    Function     MAC Address        Ports   Ports
-------- -------- ------------ -----------------  ------- --------
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
```

以下命令显示单个节点的详细接口组信息：

```
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: -
```

显示 LIF 信息

您可以查看有关 LIF 的详细信息以确定其配置。

您可能还需要查看此信息以诊断基本的 LIF 问题，例如检查重复的 IP 地址或验证网络端口是否属于正确的子网。Storage Virtual Machine （SVM）管理员只能查看与 SVM 关联的 LIF 的信息。

关于此任务

此时将显示以下信息：

- 与 LIF 关联的 IP 地址
- LIF 的管理状态
- LIF 的运行状态

  数据 LIF 的运行状态取决于与数据 LIF 关联的 SVM 的状态。停止 SVM 后， LIF 的运行状态将更改为 down 。当 SVM 重新启动时，运行状态将更改为 up

- 节点以及 LIF 所在的端口

如果字段的数据不可用(例如、如果没有扩展状态信息)、则字段值将列为 –。

步骤

使用 network interface show 命令显示 LIF 信息。

您可以通过指定 -instance 参数来查看每个 LIF 的详细信息，也可以通过使用 -fields 参数指定字段名称来获取特定信息。

以下命令显示有关集群中所有 LIF 的常规信息：

```
network interface show
           Logical    Status     Network          Current      Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node         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
```

以下命令显示有关单个 LIF 的详细信息：

```
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
```

显示路由信息

您可以显示有关 SVM 中路由的信息。

步骤

根据要查看的路由信息类型，输入相应的命令：

要查看有关以下内容的信息 ...	输入 ...
静态路由，每个 SVM	`network route show`
每个 SVM 的每个路由上的 LIF	`network route show-lifs`

您可以通过指定来显示每个路由的详细信息 `-instance` 参数。以下命令显示集群 1 中 SVM 内的静态路由：

```
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
```

以下命令显示 cluster-1 中所有 SVM 中静态路由和逻辑接口（ LIF ）的关联：

```
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
```

显示 DNS 主机表条目（仅限集群管理员）

DNS 主机表条目会将主机名映射到 IP 地址。您可以显示集群中所有 SVM 的主机名和别名及其映射到的 IP 地址。

步骤

使用 vserver services name-service dns hosts show 命令显示所有 SVM 的主机名条目。

以下示例显示了主机表条目：

```
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
```

您可以使用 `vserver services name-service dns` 命令以在SVM上启用DNS、并将其配置为使用DNS进行主机名解析。主机名可使用外部 DNS 服务器进行解析。

显示 DNS 域配置

您可以显示集群中一个或多个 Storage Virtual Machine （ SVM ）的 DNS 域配置，以验证其配置是否正确。

步骤

使用查看DNS域配置 `vserver services name-service dns show` 命令：

以下命令显示集群中所有 SVM 的 DNS 配置：

```
vserver services name-service dns show
                                                   Name
Vserver        State     Domains                   Servers
-------------- --------- ------------------------- -------------
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
```

以下命令显示 SVM vs1 的详细 DNS 配置信息：

```
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
```

显示有关故障转移组的信息

您可以查看有关故障转移组的信息，包括每个故障转移组中的节点和端口列表，是否已启用或禁用故障转移以及应用于每个 LIF 的故障转移策略类型。

步骤

1. 使用显示每个故障转移组的目标端口 `network interface failover-groups show` 命令：

   以下命令显示有关双节点集群上所有故障转移组的信息：

   ```
   network interface failover-groups show
                                 Failover
   Vserver        Group          Targets
   -------------- -------------- ---------------------------------
   Cluster
                  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. 使用显示特定故障转移组的目标端口和广播域 `network interface failover-groups show` 命令：

   以下命令显示 SVM vs4 的故障转移组 data12 的详细信息：

```
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. 使用显示所有LI使用的故障转移设置 `network interface show` 命令：

   以下命令显示每个 LIF 正在使用的故障转移策略和故障转移组：

```
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
```

显示 LIF 故障转移目标

您可能需要检查 LIF 的故障转移策略和故障转移组是否配置正确。为了防止故障转移规则配置不当，您可以显示一个 LIF 或所有 LIF 的故障转移目标。

关于此任务

通过显示 LIF 故障转移目标，您可以检查以下内容：

- LIF 是否配置了正确的故障转移组和故障转移策略
- 生成的故障转移目标端口列表是否适用于每个 LIF
- 数据 LIF 的故障转移目标是否不是管理端口（ e0M ）

步骤

使用显示LIF的故障转移目标 `failover` 的选项 `network interface show` 命令：

以下命令显示有关双节点集群中所有 LIF 的故障转移目标的信息。。 `Failover Targets` 行显示给定LIF的节

点-端口组合(按优先级排序)列表。

```
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
```

显示负载平衡区域中的 LIF

您可以通过显示属于负载平衡区域的所有 LIF 来验证是否已正确配置该区域。您还可以查看特定 LIF 的负载平衡区域或所有 LIF 的负载平衡区域。

步骤

使用以下命令之一显示所需的 LIF 和负载平衡详细信息

要显示 ...	输入 ...
特定负载平衡区域中的 LIF	`network interface show -dns-zone zone_name` `zone_name` 指定负载平衡区域的名称。
特定 LIF 的负载平衡区域	`network interface show -lif lif_name -fields dns-zone`
所有 LIF 的负载平衡区域	`network interface show -fields dns-zone`

显示 **LIF** 的负载平衡区域的示例

以下命令显示 SVM vs0 的负载平衡区域 storage.company.com 中所有 LIF 的详细信息：

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

         Logical    Status     Network            Current   Current Is
Vserver  Interface  Admin/Oper Address/Mask       Node      Port    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
```

以下命令显示 LIF data3 的 DNS 区域详细信息：

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

以下命令显示集群中所有 LIF 的列表及其对应的 DNS 区域：

```
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
```

显示集群连接

您可以按客户端，逻辑接口，协议或服务显示集群中的所有活动连接或节点上的活动连接计数。您还可以显示集群中的所有侦听连接。

按客户端显示活动连接（仅限集群管理员）

您可以按客户端查看活动连接，以验证特定客户端正在使用的节点，并查看每个节点的客户端数量之间可能存在的不平衡。

关于此任务

在以下情况下，按客户端显示的活动连接数非常有用：

- 查找繁忙或过载的节点。
- 确定特定客户端对卷的访问速度较慢的原因。

  您可以查看有关客户端正在访问的节点的详细信息，然后将其与卷所在的节点进行比较。如果访问卷需要遍历集群网络，则客户端可能会因远程访问超额预订的远程节点上的卷而导致性能下降。

- 验证所有节点是否均用于数据访问。
- 查找连接数意外高的客户端。
- 验证某些客户端是否已连接到节点。

步骤

使用按客户端显示节点上的活动连接计数 `network connections active show-clients` 命令：

有关此命令的详细信息，请参见手册页： "ONTAP 9 命令"

```
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
```

按协议显示活动连接（仅限集群管理员）

您可以按协议（ TCP 或 UDP ）显示节点上的活动连接计数，以比较集群中协议的使用情况。

关于此任务

在以下情况下，按协议显示的活动连接数非常有用：

- 查找断开连接的 UDP 客户端。

  如果某个节点接近其连接限制，则 UDP 客户端将最先被丢弃。

- 验证是否未使用任何其他协议。

步骤

使用按协议显示节点上的活动连接计数 `network connections active show-protocols` 命令：

有关此命令的详细信息，请参见手册页。

```
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
```

按服务显示活动连接（仅限集群管理员）

您可以按服务类型（例如 NFS ， SMB ，挂载等）显示集群中每个节点的活动连接计数。这对于比较集群中的服务使用情况非常有用，有助于确定节点的主工作负载。

关于此任务

在以下情况下，按服务显示的活动连接数非常有用：

- 验证所有节点是否都用于相应的服务，以及该服务的负载平衡是否正常工作。
- 验证是否未使用任何其他服务。使用按服务显示节点上的活动连接计数 `network connections active show-services` 命令：

有关此命令的详细信息，请参见手册页： "ONTAP 9 命令"

```
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
```

按 LIF 显示节点和 SVM 上的活动连接

您可以按节点和 Storage Virtual Machine （ SVM ）显示每个 LIF 的活动连接计数，以查看集群中 LIF 之间的连接不平衡。

关于此任务

在以下情况下，按 LIF 显示的活动连接数非常有用：

- 通过比较每个 LIF 上的连接数来查找过载的 LIF 。
- 验证 DNS 负载平衡是否适用于所有数据 LIF 。
- 比较与各种 SVM 的连接数以查找使用量最多的 SVM 。

步骤

使用按SVM和节点显示每个LIF的活动连接数 `network connections active show-lifs` 命令：

有关此命令的详细信息，请参见手册页： "ONTAP 9 命令"

```
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
```

显示集群中的活动连接

您可以显示有关集群中活动连接的信息，以查看各个连接使用的 LIF ，端口，远程主机，服务， Storage Virtual Machine （ SVM ）和协议。

关于此任务

在以下情况下，查看集群中的活动连接非常有用：

- 验证各个客户端是否在正确的节点上使用了正确的协议和服务。
- 如果客户端在使用节点，协议和服务的特定组合访问数据时遇到问题，您可以使用此命令查找类似的客户端以进行配置或数据包跟踪比较。

步骤

使用显示集群中的活动连接 `network connections active show` 命令：

有关此命令的详细信息，请参见手册页： "ONTAP 9 命令"

以下命令显示节点 node1 上的活动连接：

```
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
```

以下命令显示 SVM vs1 上的活动连接：

```
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
```

显示集群中的侦听连接

您可以显示集群中侦听连接的信息，以查看接受给定协议和服务连接的 LIF 和端口。

关于此任务

在以下情况下，查看集群中的侦听连接非常有用：

- 如果客户端与 LIF 的连接始终失败，请验证所需的协议或服务是否正在侦听 LIF 。
- 如果通过另一节点上的 LIF 对某个节点上的卷进行远程数据访问失败，请验证是否在每个集群 LIF 上打开了 UDP/rclopcp 侦听器。
- 如果同一集群中的两个节点之间的 SnapMirror 传输失败，验证是否在每个集群 LIF 上打开了 UDP/rclopcp 侦听器。
- 如果不同集群中两个节点之间的 SnapMirror 传输失败，请验证是否在每个集群间 LIF 上打开了 tcp/ctlopcp 侦听器。

步骤

使用显示每个节点的侦听连接 `network connections listening show` 命令：

```
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
```

用于诊断网络问题的命令

您可以使用等命令诊断网络上的问题 `ping`, `traceroute`, `ndp`, 和 `tcpdump`。您也可以使用等命令 `ping6` 和 `traceroute6` 诊断IPv6问题。

如果您要 ...	输入此命令 ...
测试节点是否可以访问网络上的其他主机	`network ping`
测试节点是否可以访问 IPv6 网络上的其他主机	`network ping6`
跟踪 IPv4 数据包到达网络节点的路由	`network traceroute`
跟踪IPv6数据包到达网络节点的路由	`network traceroute6`
管理邻居发现协议（NDP）	`network ndp`
显示有关在指定网络接口或所有网络接口上接收和发送的数据包的统计信息	`run -node` *`node_name`* `ifstat` **Note**:此命令可从noberhell中使用。
显示有关从集群中的每个节点和端口发现的相邻设备的信息，包括远程设备类型和设备平台	`network device-discovery show`
查看节点的 CDP 邻居（ONTAP 仅支持 CDPv1 公告）	`run -node` *`node_name`* `cdpd show-neighbors` **Note**:此命令可从noberhell中使用。
跟踪网络中发送和接收的数据包	`network tcpdump start -node` *`node-name`* `-port` *`port_name`* **Note**:此命令可从noberhell中使用。

测量集群间或集群内节点之间的延迟和吞吐量	`network test -path -source-node` *`source_nodename`* *`local`* `-destination -cluster` *`destination_clustername`* `-destination-node` *`destination_nodename`* `-session-type` *`Default`*, *`AsyncMirrorLocal`*, *`AsyncMirrorRemote`*, *`SyncMirrorRemote`*, or *`RemoteDataTransfer`* 有关详细信息，请参见 "性能管理"。

有关这些命令的详细信息，请参见相应的手册页： "ONTAP 9 命令"

显示使用邻居发现协议的网络连接

显示使用邻居发现协议的网络连接

在数据中心中，您可以使用邻居发现协议查看一对物理或虚拟系统及其网络接口之间的网络连接。ONTAP 支持两种邻居发现协议： Cisco 发现协议（ CDP ）和链路层发现协议（ LLDP ）。

通过邻居发现协议，您可以自动发现和查看有关网络中已启用协议的直连设备的信息。每个设备都会公布标识，功能和连接信息。此信息以以以太网帧的形式传输到多播 MAC 地址，并由所有已启用协议的相邻设备接收。

要使两个设备成为邻居，每个设备都必须启用并正确配置一个协议。发现协议功能仅限于直连网络。邻居可以包括启用了协议的设备，例如交换机，路由器，网桥等。ONTAP 支持两种邻居发现协议，可以单独使用，也可以同时使用。

- Cisco 发现协议（ CDP ） *

CDP 是 Cisco Systems 开发的一种专有链路层协议。默认情况下，它在 ONTAP 中对集群端口启用，但必须对数据端口明确启用。

- 链路层发现协议（ LLDP ） *

LLDP 是标准文档 IEEE 802.1AB 中指定的与供应商无关的协议。必须为所有端口显式启用此功能。

使用 **CDP** 检测网络连接

使用 CDP 检测网络连接包括查看部署注意事项，在数据端口上启用它，查看相邻设备以及根据需要调整 CDP 配置值。默认情况下， CDP 在集群端口上处于启用状态。

还必须在任何交换机和路由器上启用 CDP ，才能显示有关相邻设备的信息。

ONTAP 版本	Description
9.10.1及更早版本	集群交换机运行状况监控器还使用 CDP 自动发现集群和管理网络交换机。
9.11.1及更高版本	集群交换机运行状况监控器还使用CDP自动发现集群、存储和管理网络交换机。

相关信息

"系统管理"

使用 **CDP** 的注意事项

默认情况下， CDP 兼容设备会发送 CDPv2 公告。CDP 兼容设备仅在收到 CDPv1 公告时才会发送 CDPv1 公告。ONTAP 仅支持 CDPv1 。因此，当 ONTAP 节点发送 CDPv1 公告时， CDP 兼容的相邻设备会发回 CDPv1 公告。

在节点上启用 CDP 之前，应考虑以下信息：

- 所有端口均支持 CDP 。
- CDP 公告由处于 up 状态的端口发送和接收。
- 必须在传输和接收设备上启用 CDP ，才能发送和接收 CDP 公告。
- CDP 公告会定期发送，您可以配置时间间隔。
- 更改 LIF 的 IP 地址后，节点会在下一个 CDP 公告中发送更新后的信息。
- ONTAP 9.10.1及更早版本：
  - CDP 始终在集群端口上启用。
  - 默认情况下，所有非集群端口上都会禁用 CDP 。
- ONTAP 9.11.1及更高版本：
  - CDP始终在集群和存储端口上启用。
  - 默认情况下、所有非集群和非存储端口上都会禁用CDP。

> 有时，当节点上的 LIF 发生更改时， CDP 信息不会在接收设备端（例如交换机）进行更新。如果遇到此类问题，应将节点的网络接口配置为 down 状态，然后再配置为 up 状态。

- 只有 IPv4 地址才会在 CDP 公告中公布。
- 对于带有 VLAN 的物理网络端口，该端口上 VLAN 上配置的所有 LIF 都会公布。
- 对于属于接口组的物理端口，该接口组上配置的所有 IP 地址都会在每个物理端口上公布。
- 对于托管 VLAN 的接口组，接口组上配置的所有 LIF 和 VLAN 都会在每个网络端口上公布。
- 由于CDP数据包在端口上限制为不超过1500字节
  配置了大量LIP地址、只能在相邻交换机上报告其中一部分IP地址。

启用或禁用 **CDP**

要发现并向 CDP 兼容的相邻设备发送公告，必须在集群的每个节点上启用 CDP 。

默认情况下、在ONTAP 9.10.1及更早版本中、CDP会在节点的所有集群端口上启用、并在节点的所有非集群端口上禁用。

默认情况下、在ONTAP 9.11.1及更高版本中、CDP会在节点的所有集群和存储端口上启用、并在节点的所有非集群和非存储端口上禁用。

关于此任务

。 `cdpd.enable` 选项用于控制在节点的端口上启用还是禁用CDP：

- 对于ONTAP 9.10.1及更早版本、on会在非集群端口上启用CDP。
- 对于ONTAP 9.11.1及更高版本、on会在非集群和非存储端口上启用CDP。
- 对于ONTAP 9.10.1及更早版本、off会在非集群端口上禁用CDP；您不能在集群端口上禁用CDP。
- 对于ONTAP 9.11.1及更高版本、off会在非集群和非存储端口上禁用CDP；您不能在集群端口上禁用CDP。

如果在连接到 CDP 兼容设备的端口上禁用 CDP ，则网络流量可能无法优化。

步骤

1. 显示节点或集群中所有节点的当前 CDP 设置：

要查看 CDP 设置 …	输入 …
节点	`run - node <node_name> options cdpd.enable`
集群中的所有节点	`options cdpd.enable`

2. 在节点的所有端口或集群中所有节点的所有端口上启用或禁用 CDP ：

要启用或禁用 CDP ，请执行以下操作 …	输入 …
节点	`run -node node_name options cdpd.enable {on or off}`
集群中的所有节点	`options cdpd.enable {on or off}`

查看 **CDP** 邻居信息

您可以查看有关连接到集群节点的每个端口的相邻设备的信息，前提是该端口连接到 CDP 兼容设备。您可以使用 `network device-discovery show -protocol cdp` 命令以查看邻居信息。

关于此任务

在ONTAP 9.10.1及更早版本中、由于CDP始终为集群端口启用、因此始终会显示这些端口的CDP邻居信息。必须在非集群端口上启用 CDP ，才能显示这些端口的邻居信息。

在ONTAP 9.11.1及更高版本中、由于CDP始终为集群和存储端口启用、因此始终会显示这些端口的CDP邻居信息。必须在非集群和非存储端口上启用CDP、才能显示这些端口的邻居信息。

步骤

显示有关连接到集群中节点上端口的所有 CDP 兼容设备的信息：

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

以下命令显示了连接到节点sti2650/212上端口的邻居：

```
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
```

输出列出了连接到指定节点的每个端口的 Cisco 设备。

配置 **CDP** 消息的保持时间

保持时间是 CDP 公告存储在相邻 CDP 兼容设备的缓存中的时间段。保持时间在每个 CDPv1 数据包中公布，并且每当节点收到 CDPv1 数据包时都会更新。

- 的值 `cdpd.holdtime` 选项应在HA对的两个节点上设置为相同的值。
- 默认保持时间值为 180 秒，但您可以输入 10 秒到 255 秒之间的值。
- 如果在保持时间到期之前删除 IP 地址，则会缓存 CDP 信息，直到保持时间到期为止。

步骤

1. 显示节点或集群中所有节点的当前 CDP 保持时间：

要查看保持时间 …	输入 …
节点	`run -node node_name options cdpd.holdtime`
集群中的所有节点	`options cdpd.holdtime`

2. 在节点的所有端口或集群中所有节点的所有端口上配置 CDP 保持时间：

要设置保持时间 …	输入 …
节点	`run -node node_name options cdpd.holdtime holdtime`
集群中的所有节点	`options cdpd.holdtime holdtime`

设置发送 **CDP** 公告的间隔

CDP 公告会定期发送到 CDP 邻居。您可以根据网络流量和网络拓扑变化增加或减少发送 CDP 公告的间隔。

- 的值 `cdpd.interval` 选项应在HA对的两个节点上设置为相同的值。
- 默认间隔为 60 秒，但您可以输入一个介于 5 秒到 900 秒之间的值。

步骤

1. 显示节点或集群中所有节点的当前 CDP 公告时间间隔：

要查看间隔 …	输入 …
节点	`run -node node_name options cdpd.interval`
集群中的所有节点	`options cdpd.interval`

2. 配置为节点的所有端口或集群中所有节点的所有端口发送 CDP 公告的间隔：

要设置间隔 …	输入 …
节点	`run -node node_name options cdpd.interval interval`
集群中的所有节点	`options cdpd.interval interval`

查看或清除 **CDP** 统计信息

您可以查看每个节点上的集群和非集群端口的 CDP 统计信息，以检测潜在的网络连接问题。CDP 统计信息是自上次清除以来累积的。

关于此任务

在ONTAP 9.10.1及更早版本中、由于CDP始终为端口启用、因此始终会显示这些端口上的流量的CDP统计信息。必须在端口上启用CDP、才能显示这些端口的统计信息。

在ONTAP 9.11.1及更高版本中、由于CDP始终为集群和存储端口启用、因此始终为这些端口上的流量显示CDP统计信息。必须在非集群或非存储端口上启用CDP、才能显示这些端口的统计信息。

步骤

显示或清除节点上所有端口的当前 CDP 统计信息：

如果您要 ...	输入 ...
查看 CDP 统计信息	`run -node node_name cdpd show-stats`
清除 CDP 统计信息	`run -node node_name cdpd zero-stats`

显示和清除统计信息的示例

以下命令显示清除之前的 CDP 统计信息。输出将显示自上次清除统计信息以来已发送和接收的数据包总数。

```
run -node node1 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
```

以下命令将清除 CDP 统计信息：

```
run -node node1 cdpd zero-stats
```

```
run -node node1 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
```

清除统计信息后，在发送或接收下一个 CDP 公告后，这些统计信息将开始累积。

使用**LDP**检测网络连接

使用 LLDP 检测网络连接包括查看部署注意事项，在所有端口上启用 LLDP ，查看相邻设备以及根据需要调整 LLDP 配置值。

此外、还必须在任何交换机和路由器上启用CDP、才能显示有关相邻设备的信息。

ONTAP 当前报告以下类型 - 长度 - 值结构（ TLV ）：

- 机箱 ID
- 端口 ID
- 生存时间（ TTL ）
- 系统名称

  系统名称 TLV 不会在 CNA 设备上发送。

某些融合网络适配器（ CNA ）（例如 X1143 适配器和 UTA2 板载端口）包含 LLDP 卸载支持：

- LLDP 卸载用于数据中心桥接（ DCB ）。
- 显示的信息可能因集群和交换机而异。

  对于CNA端口和非CNA端口、交换机显示的机箱ID和端口ID数据可能有所不同。

例如：

- 对于非CNA端口：
  - 机箱ID是节点上某个端口的固定MAC地址
  - port ID是节点上相应端口的端口名称
- 对于CNA端口：
  - 机箱ID和端口ID是节点上相应端口的MAC地址。

但是、对于这些端口类型、集群显示的数据是一致的。

> LLDP 规范定义了通过 SNMP MIB 访问收集的信息。但是， ONTAP 当前不支持 LLDP MIB 。

启用或禁用**LDP**

要发现公告并将其发送到符合LDP的相邻设备、必须在集群的每个节点上启用LDP。从 ONTAP 9.7 开始，默认情况下会在节点的所有端口上启用 LLDP 。

关于此任务

对于ONTAP 9.10.1及更早版本、 `lldp.enable` 选项用于控制节点的端口上是启用还是禁用了LDP：

- `on` 在所有端口上启用LDP。
- `off` 在所有端口上禁用LDP。

对于ONTAP 9.11.1及更高版本、 `lldp.enable` 选项用于控制是否在节点的非集群和非存储端口上启用了LDP：

- `on` 在所有非集群和非存储端口上启用LDP。
- `off` 在所有非集群和非存储端口上禁用LDP。

步骤

1. 显示某个节点或集群中所有节点的当前LDP设置：
   - 单个节点 `run -node node_name options lldp.enable`
   - 所有节点：选项 `lldp.enable`
2. 在一个节点的所有端口或集群中所有节点的所有端口上启用或禁用LDP：

要启用或禁用的LDP…	输入 …
节点	`run -node node_name options lldp.enable {on
off}`	集群中的所有节点
`options lldp.enable {on	off}`

   - 单个节点

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

   - 所有节点：

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

查看**LDP**邻居信息

您可以查看有关连接到集群节点的每个端口的相邻设备的信息，前提是该端口连接到 LLDP 兼容的设备。您可以使用 network device-discovery show 命令查看邻居信息。

步骤

1. 显示有关连接到集群中某个节点上的端口的所有符合LDP的设备的信息：

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

以下命令显示了连接到节点 cluster-1_01 上端口的邻居。输出列出了连接到指定节点的每个端口且已启用 LLDP 的设备。如果 `-protocol` 如果省略选项、则输出还会列出已启用CDP的设备。

```
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
```

调整传输 **LLDP** 公告的间隔

将定期向lld邻居发送lld公告。您可以根据网络流量和网络拓扑的变化增加或减少发送LLDP公告的间隔。

关于此任务

IEEE 建议的默认间隔为 30 秒，但您可以输入一个介于 5 秒到 300 秒之间的值。

步骤

1. 显示某个节点或集群中所有节点的当前LDP公告时间间隔：
   - 单个节点

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

   - 所有节点：

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

2. 调整节点的所有端口或集群中所有节点的所有端口发送 LLDP 公告的间隔：
   - 单个节点

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

   - 所有节点：

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

调整 **LLDP** 公告的生存时间值

生存时间（ TTL ）是 LLDP 公告存储在相邻 LLDP 兼容设备的缓存中的时间段。TTL 会在每个 LLDP 数据包中

公布，并在节点收到 LLDP 数据包时进行更新。可以在传出 LLDP 帧中修改 TTL 。

关于此任务

- TTL是计算得出的值、即传输间隔的乘积 (`lldp.xmit.interval`)和保持乘数 (`lldp.xmit.hold`)加上一个。
- 默认保持倍数值为 4 ，但您可以输入 1 到 100 之间的值。
- 因此，根据 IEEE 的建议，默认 TTL 为 121 秒，但通过调整传输间隔和保持乘数值，您可以为传出帧指定一个介于 6 秒到 30001 秒之间的值。
- 如果在 TTL 过期之前删除 IP 地址，则 LLDP 信息将缓存，直到 TTL 过期为止。

步骤

1. 显示节点或集群中所有节点的当前保持乘数值：
   - 单个节点

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

   - 所有节点：

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

2. 调整节点的所有端口或集群中所有节点的所有端口上的保持倍数值：
   - 单个节点

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

   - 所有节点：

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

查看或清除**LLDP**统计信息

您可以查看每个节点上集群和非集群端口的LLDP统计信息、以检测潜在的网络连接问题。LLDP统计信息是自上次清除以来累积的。

关于此任务

对于ONTAP 9.10.1及更早版本、由于LLDP始终为集群端口启用、因此始终会显示这些端口上的流量的LLDP统计信息。必须在非集群端口上启用LLDP、才能显示这些端口的统计信息。

对于ONTAP 9.11.1及更高版本、由于LLDP始终为集群和存储端口启用、因此始终会显示这些端口上的流量的LLDP统计信息。必须在非集群和非存储端口上启用LLDP、才能显示这些端口的统计信息。

步骤

显示或清除节点上所有端口的当前LLDP统计信息：

如果您要 ...	输入 ...
查看LLDP统计信息	`run -node node_name lldp stats`
清除LLDP统计信息	`run -node node_name lldp stats -z`

显示并清除统计信息示例

以下命令显示清除前的LLDP统计信息。输出将显示自上次清除统计信息以来已发送和接收的数据包总数。

```
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
```

以下命令将清除LLDP统计信息。

```
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
```

清除统计信息后、在发送或接收下一个LLDP公告后、这些统计信息将开始累积。