如何在 Data ONTAP 上配置 SNMP 监控

https://kb-cn-stage.netapp.com/on-prem/ontap/Ontap_OS/OS-KBs/How_to_configure_SNMP_monitori…
Updated: Wed, 22 Apr 2026 04:07:08 GMT

适用场景

- 集群模式Data ONTAP 8
- ONTAP 9

问题解答

注意：有关在较新版本的ONTAP中管理SNMP的信息，请参见以下内容： 用于管理SNMP的命令

- 简要介绍集群模式Data ONTAP中的简单网络管理协议(Simple Network Management Protocol、SNMP)和SNMP陷阱。
- 如何使用SNMP从C模式集群系统获取信息？
- 如何在所需客户端上配置SNMP陷阱并接收事件？

注：请参阅以下TR-Guide - 《**Data ONTAP**中的**SNMP**支持》

本报告旨在帮助客户和NetApp现场团队了解集群模式SNMP.2.x、8.3.x和ONTAP 9中的Data ONTAP 8支持级别。 它还

比较了7-模式和集群模式的OID可用性。它仅提供单个表或组级别的信息。NetApp.mib文件提供了有关表或组中支持的各种字段或变量的追加信息。MIB浏览器工具(如iReasoning)可用于轻松解释`netapp.mib` 文件的内容。

SNMP：

SNMP 是一个广泛使用的网络监视和控制协议。数据从SNMP代理(即报告每个网络设备(集线器、路由器或网桥)中的活动的硬件和/或软件进程)传递到用于监控网络的工作站控制台。代理返回管理信息库(Management Information Base、MIB)中包含的信息、管理信息库是一个数据结构、用于定义可从设备获取的内容以及可控制的内容(关闭或打开)。SNMP源自UNIX社区、已广泛应用于所有主要平台。
MiB描述设备子系统管理数据的结构；它们使用包含对象标识符(OID)的分层命名空间。每个OID用于标识一个可通过SNMP读取或设置的变量。

注意： NetApp不支持SNMP-set操作。此外、SNMP-support仅在集群范围内提供、不会进行虚拟化。但是、此操作将在8.1之后的版本中完成、并且与7G vfiler不同、因为SNMP支持从未进行过vfilerized。

启用/禁用SNMP：

可以使用CLI/ZAPI在集群上启用和禁用SNMP协议：

- 使用命令行界面在集群上启用SNMP -从ngsh运行`options -option-name snmp.enable -option-value` on
- 使用命令行界面在集群上禁用SNMP -从ngsh运行`options -option-name snmp.enable -option-value` off
- 使用ZAPI在集群上启用SNMP -使用ontapi或zexle.exe运行`API snmp-enable`
- 使用ZAPI在集群上禁用SNMP -使用ontapi或zexle.exe运行`API snmp-disable`

  示例：`$> ontapi snmp-[en|dis]able`
  注：SNMP协议只能在集群范围内启用或禁用。在Data ONTAP 8.1 C模式中，无法通过SNMP访问集群中的单个节点。

类似于7G的SNMP UI：

Data ONTAP C模式可利用一组用户界面(命令行界面和ZAPI)在集群上配置SNMP详细信息。下面简要介绍了有助于在集群模式系统上配置SNMP的每个命令行界面：

- `snmp contact:` 查看或修改联系人详细信息
- `snmp location:` 查看或修改位置详细信息
- `snmp init:` 启用或禁用从集群发送的陷阱[1->已启用、0->已禁用]
- `snmp authtrap:` 启用或禁用身份验证失败陷阱[1->ENABLE,0->DISABLE]
- `snmp community add|delete:` 要查看、添加或删除集群中的社区、将会有一个默认的"public"社区ro。
- **注意：** 仅支持只读社区。此外、要删除第一个SNMP社区条目、用户需要删除用于通知的陷阱主机。
- `snmp traphost add|delete:` 要查看、添加或删除集群中的陷阱主机、在这些主机运行时、集群中发生的所有陷阱(或事件)都会发送到这些主机`snmptrapd`

- `options snmp.enable`: 在集群上启用或禁用SNMP协议[on=>enABLED，off=>disABLED

下面简要介绍了有助于在集群模式Data ONTAP系统上配置SNMP的每个ZAPI：

- `snmp-enable`: 在集群上启用SNMP协议
- `snmp-disable`: 在集群上禁用SNMP协议
- `snmp-trap-enable`: 启用发送到陷阱主机的陷阱
- `snmp-trap-disable`: 禁用发送到陷阱主机的陷阱
- `snmp-community-add`: 添加SNMP社区。Data ONTAP 8.1 C模式仅支持ro社区
- `snmp-community-delete`: 删除现有社区
- `snmp-traphost-add`: 添加陷阱主机
- `snmp-traphost-delete`: 删除现有陷阱主机
- `snmp-status`: 提供集群上SNMP配置的详细信息(例如位置、联系人、陷阱、陷阱主机、社区详细信息)
- `snmp-get`: 当OID作为API的输入提供时读取对象值(类似于smpget UNIX实用程序)
- `snmp-get-next`: 读取作为OID提供的对象旁边的对象值(类似于snmpgetnnXT UNIX实用程序)
- `Add/modify/view contact`: 可以使用SNMP命令行界面添加或修改集群的联系人和位置详细信息。没有用于修改联系人或位置详细信息的相应API。但是、可以使用SNMP[walK|get|GETNEXt](或) SNMP-status读取集群详细信息(无法使用SNMP或ZAPI进行修改)

示例：

使用CLI添加/修改：

使用ZAPI调用读取：

```
$> ontapi -x snmp-status
```

使用SNMP调用读取：

```
$> snmpwalk -c public -v [1|2c]
```

如何在C模式系统上配置SNMPv3：

- 使用security login create命令行界面在集群上创建SNMPv3用户。
- 输入EngineID (使用本地EngineID、该值为默认值)。
- 输入身份验证协议并输入指定SNMPv3用户的密码。
- 通过指定-v 3并提供用户凭据、为SNMPv3用户运行`snmp[walk|get|getnext]`。

PDF中的附录部分举例说明了如何创建SNMPv3用户并对该用户运行`SNMP utilities`。

SNMP陷阱：

从代理到管理器的异步通知：包括当前sysUptime值、标识陷阱类型的OID以及可选的变量连接。陷阱的目标寻址以应用程序特定的方式确定、通常通过MIB中的陷阱配置变量来确定。陷阱消息的格式在SNMPv2中已更改、PDU重命名为SNMPv2-陷阱。

7-模式和C模式Data ONTAP中的SNMP及其陷阱：

标准SNMP陷阱：

根据RFC 12、共有5个标准SNMP陷阱：

- linkdown—关闭处于启动状态的活动物理端口时生成此陷阱(ifAdminStatus应从up更改为down)/陷阱消息中不包含ifIndex编号信息。)
- LinkUp -当启动关闭的物理端口时将生成此陷阱(ifAdminStatus应从down更改为up)/ifIndex编号信息不包括在陷阱消息中。)
- 热启动—正常重新启动时会生成热启动陷阱
- condstart - condstart陷阱表示发送协议实体正在重新初始化自身、从而可能更改代理的配置或协议实体实施
- 验证失败—当用户尝试使用不正确的Privileges登录到系统时、将生成验证失败陷阱

NetApp内置SNMP陷阱：

为了方便NetApp用户、SNMP具有大量内置陷阱。文件/mroot/etc/mib/netapp.mib 包含内置陷阱列表。每个陷阱都有一个唯一标识符或陷阱代码。例如、卷联机是内置陷阱、其陷阱代码为276。以下信息来自netapp.mib 文件。

OID后跟通知类型标记，表示它是陷阱，与问题描述和陷阱代码相关联，此处为276。

```
volumeOnline                    NOTIFICATION-TYPE
  OBJECTS                       {productTrapData, productSerialNum}
  STATUS                          current
  DESCRIPTION          Volume is online now. The string sent with trap specifies name
of volume which is online now.

          ::= { netapp 0 276 }
```

用户定义的SNMP陷阱：

这些陷阱可以根据用户要求进行配置。即使NetApp具有一些内置陷阱、用户仍可能出于其他原因需要生成事件。7-模式的基础架构支持用户定义的陷阱，但Data ONTAP 8™1的C模式基础架构不支持用户定义的陷阱。以下是计划的Data ONTAP 8 (在UI.1之后)、可帮助配置用户定义的陷阱：

- SNMP-陷阱 列表
- SNMP-陷阱 集
- SNMP-陷阱 删除
- SNMP-陷阱-重置
- SNMP-陷阱 加载

采用EMS的捆绑：

陷阱与EMS事件相关联。也可以使用事件CLI生成SNMP事件。

添加到SNMP陷阱主机列表中的所有陷阱主机都将复制到陷阱主机条目下名为事件目标表的另一个表中。

```
test-01::*> system snmp traphost show
        TRAPHOST1
        TRAPHOST2
test-01::*> event destination show -name traphost

                  Name: traphost

      Mail Destination: -
      SNMP Destination: TRAPHOST1
                        TRAPHOST2
    Syslog Destination: -
       Syslog Facility: -
   SNMP Trap Community: public
Hide Parameter Values?: false
```

可以使用event *命令行界面执行以下操作：

可以使用event Destination create命令行界面添加新的SNMP主机。将主机添加到默认陷阱主机列表后、它将复制到SNMP陷阱主机列表中、并且集群中触发的所有事件都将发送到此主机。

```
csiqa-3170-6a1365754940::*> snmp traphost
        -

csiqa-3170-6a1365754940::*> event destination show -name traphost

                  Name: traphost
      Mail Destination: -
      SNMP Destination: -
    Syslog Destination: -
       Syslog Facility: -
   SNMP Trap Community: qwerty
Hide Parameter Values?: false

csiqa-3170-6a1365754940::*> snmp community

csiqa-3170-6a1365754940
        ro  qwerty

csiqa-3170-6a1365754940::*> event destination modify -name traphost -hide-parameters
false -snmp 10.229.88.174 -snmp-community qwerty
```

```
csiqa-3170-6a1365754940::*> event destination show -name
traphost

                  Name: traphost
      Mail Destination: -
      SNMP Destination: csiqa-labopt-rh5-003.gdl.englab.netapp.com
    Syslog Destination: -
       Syslog Facility: -
   SNMP Trap Community: qwerty
Hide Parameter Values?: false

csiqa-3170-6a1365754940::*> snmp traphost
        csiqa-labopt-rh5-003.gdl.englab.netapp.com (csiqa-labopt-
rh5-003.gdl.englab.netapp.com) <10.229.88.174>

csiqa-3170-6a1365754940::*>
```

但是、如果用户要将主机配置为仅接收特定事件、则可以使用event route CLI将任何事件路由到该目标。要列出事件、请执行以下操作：

```
csiqa-3070-591287556400::*> event route show
                                                              Freq    Time
Message                          Severity       Destinations  Threshd Threshd
-------------------------------- -------------- ------------- ------- -------
EthrOutput.FamilyType.Err        ERROR          -             0       0
LUN.clone_snapshot_destroyed     NOTICE         -             0       0
LUN.destroy                      INFORMATIONAL  -             0       0
LUN.space_reservation_not_honored
                                 NOTICE         -             0       0
LUN.volume_processing_failed_no_space
                                 ERROR          -             0       0
Nblade.DidNotInitialize          ERROR          -             0       0
Nblade.JunctionRootLookup        WARNING        -             0       0
Nblade.Nfs4IllegalDirentName     ERROR          -             0       0
Nblade.NfsRaidError              ERROR          -             0       0
```

将相应事件映射到所需的目标。

并非所有事件都已启用SNMP陷阱。要了解与SNMP陷阱关联的所有陷阱，请使用以下命令行界面：

```
csiqa-3070-591287556400::*> event route show -snmp-support true
                                                              Freq    Time
Message                          Severity       Destinations  Threshd Threshd
```

```
-------------------------------- -------------- -------------- ------- -------
app.log.alert                    ALERT          -              0       0
app.log.crit                     CRITICAL       -              0       0
app.log.debug                    DEBUG          -              0       0
app.log.emerg                    EMERGENCY      -              0       0
app.log.err                      ERROR          -              0       0
app.log.info                     INFORMATIONAL  -              0       0
app.log.notice                   NOTICE         -              0       0
app.log.warn                     WARNING        -              0       0
asup.general.create              ERROR          -              0       0
asup.general.drop                ERROR          -              0       0
asup.general.drop.enqueue        INFORMATIONAL  -              0       0
```

SNMP陷阱—如何配置陷阱并生成事件

使用SNMP陷阱主机命令行界面添加陷阱主机：

```
$> snmp traphost add
```

-or-

```
$> snmp traphost add
```

注：请确保在集群上配置了DNS、以便解析陷阱主机名称。

1. 确保文件管理器上已启用SNMP协议：

   ```
   ::> options -option-name snmp.enable on
   ```

2. 在集群上启用SNMP陷阱。可以通过以下任一方式完成此操作：

   运行以下命令
   ： zapi -or-
   运行Cluster::> snmp init 1
   ：

   ```
   $> ontapi snmp-trap-enable
   ```

3. 触发和监控事件。

traps.dat 信息-参考：BURT # 460证明

traps.dat file尤其适用于用户定义的陷阱。Data ONTAP C模式尚不支持UDT (从Data ONTAP 8.1.1开始)

traps.dat 文件的末尾有额外的1、以帮助区分表内的OID和以0结尾的OID (表外)。不应将表中的ID限制在陷阱中、因此额外的混淆实际上有助于减少无效的用户定义陷阱

C模式OID信息-参考：BURT # 460证明 [1]

netapp.mib 文件中显示的OID是密钥、而不是实际的绝对OID值。要解决此问题、最好的方法是删除最后一位数字来执行snmpwalk：

示例：

- [rakeshc@cyclnb01 ~/p4]$ snmpwalk -v 1 -c public 10.10.10.10 .1.3.6.1.4.1.789.1.5.11.1.2
- SNMPv2-SMI::enterprises.789.1.5.11.1.2.1026 = STRING: "aggr0"
- SNMPv2-SMI::enterprises.789.1.5.11.1.2.1030 = STRING: "aggr0_br3040n2_rtp"
- SNMPv2-SMI::enterprises.789.1.5.11.1.2.1034 = STRING: "n1_aggr1"
- SNMPv2-SMI::enterprises.789.1.5.11.1.2.1038 = STRING: "n2_aggr1"
- SNMPv2-SMI::enterprises.789.1.5.11.1.2.1050 = STRING: "coral_aggr"

它会提供上述5个不同的操作系统ID (1026、1030、1034、1038、1050)、然后执行以下操作：

- [rakeshc@cyclnb01 ~/p4]$ snmpwalk -v 1 -c public 10.61.76.140 .1.3.6.1.4.1.789.1.5.11.1.2.1026
- SNMPv2-SMI::enterprises.789.1.5.11.1.2.1026 = STRING: "aggr0"

有关如何生成不同类型的陷阱/事件的详细操作步骤显示在下面的"附录"部分中：

启用SNMP并运行SNMP实用程序：

运行snmpwalk/snmpget/snpgetnext etc..以及执行此操作的配置步骤

```
 DOT_cluster::*> options snmp.enable

DOT_cluster
    snmp.enable                     on

DOT_cluster::*> network interface show -vserver DOT_cluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
DOT_cluster
            cluster_mgmt up/up    10.238.44.38/18    node1         e0c     true

DOT_cluster::*>
```

```
bash-3.2$ snmpwalk -c public -v 1 10.238.44.38 .1.3.6.1.4.1.789.1.5.11.1.2
SNMPv2-SMI::enterprises.789.1.5.11.1.2.1026 = STRING: "aggr0"
SNMPv2-SMI::enterprises.789.1.5.11.1.2.1030 = STRING: "aggr0_partnernode"
SNMPv2-SMI::enterprises.789.1.5.11.1.2.1034 = STRING: "aggr_node1"
bash-3.2$
```

禁用SNMP并运行SNMP实用程序：

正在禁用snmpwalk/snmpget/snpgetnext etc..以及执行此操作的配置步骤

```
 DOT_cluster::*> option snmp.enable off
  (options)
1 entry was modified.

DOT_cluster::*> net int show -vserver DOT_cluster
  (network interface show)
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
DOT_cluster
            cluster_mgmt up/up    10.238.44.38/18    node1         e0c     true

DOT_cluster::*>

bash-3.2$ snmpwalk -c public -v 1 10.238.44.38 .1.3.6.1.4.1.789.1.5.11.1.2
Timeout: No Response from 10.238.44.38
bash-3.2$ snmpget -c public -v 1 10.238.44.38 .1.3.6.1.4.1.789.1.5.11.1.2.1026
Timeout: No Response from 10.238.44.38.
bash-3.2$ snmpgetnext -c public -v 1 10.238.44.38 .1.3.6.1.4.1.789.1.5.11.1.2.1026
Timeout: No Response from 10.238.44.38.
bash-3.2$
```

添加SNMPv3用户并运行SNMP实用程序：

与SNMPv1|v2c相比、SNMPv3协议是一种安全协议；要为SNMPv3用户配置和运行SNMP工具、需要执行以下步骤

```
DOT_cluster::*> security login create -username snmpv3user -application snmp
-authmethod usm

Enter the authoritative entity's EngineID [local EngineID]:
```

```
Which authentication protocol do you want to choose (none, md5, sha) [none]: sha

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des) [none]: des

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

DOT_cluster::*>

bash-3.2$ snmpwalk -v 3 -u snmpv3user -a SHA -A testing123! -l authPriv -x DES -X
testing123! 10.238.44.38 .1.3.6.1.4.1.789.1.5.11.1.2
SNMPv2-SMI::enterprises.789.1.5.11.1.2.1026 = STRING: "aggr0"
SNMPv2-SMI::enterprises.789.1.5.11.1.2.1030 = STRING: "aggr0_partnernode"
SNMPv2-SMI::enterprises.789.1.5.11.1.2.1034 = STRING: "aggr_node1"
bash-3.2$
```

生成NetApp内置SNMP陷阱：

NetApp内置陷阱在netapp.mib 文件中定义；以下步骤说明如何在陷阱主机或SNMP目标上生成这些陷阱

```
DOT_cluster::*> snmp traphost
        -

DOT_cluster::*> snmp traphost add 10.229.88.174

DOT_cluster::*> snmp traphost
        10.229.88.174 (10.229.88.174) <10.229.88.174>

DOT_cluster::*> snmp init
        1

DOT_cluster::*> options
snmp.enable

DOT_cluster
    snmp.enable                     on
```

```
DOT_cluster::*>

DOT_cluster::*> volume offline -volume testvol -vserver vs0
Volume "vs0:testvol" is now
offline.

Volume modify successful on volume: testvol


DOT_cluster::*> volume online -volume testvol -vserver vs0
Volume "vs0:testvol" is now
online.

Volume modify successful on volume: testvol


DOT_cluster::*>


2013-05-03 05:30:00 prakashl-vsim1.sim.eng.btc.netapp.in [10.238.44.36] (via UDP:
[10.238.44.36]:161) TRAP, SNMP v1, community public
    SNMPv2-SMI::enterprises.789 Enterprise Specific Trap (275) Uptime: 1:10:12.70
    SNMPv2-SMI::enterprises.789.1.1.12.0 = STRING: "Volume testvol@vserver:17309c4f-
b3d6-11e2-a9a8-123478563412 is offline. "    SNMPv2-SMI::enterprises.789.1.1.9.0 =
STRING: "1-80-000011"

2013-05-03 05:31:55 prakashl-vsim1.sim.eng.btc.netapp.in [10.238.44.36] (via UDP:
[10.238.44.36]:161) TRAP, SNMP v1, community public
    SNMPv2-SMI::enterprises.789 Enterprise Specific Trap (276) Uptime: 1:12:12.07
    SNMPv2-SMI::enterprises.789.1.1.12.0 = STRING: "Volume testvol@vserver:17309c4f-
b3d6-11e2-a9a8-123478563412 is online. "    SNMPv2-SMI::enterprises.789.1.1.9.0 =
STRING: "1-80-000011"
```

使用event generate CLI生成陷阱：

也可以使用event generate CLI生成陷阱。

```
DOT_cluster::*> event destination show
                                                                        Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.      Params
---------------- ----------------- ------------------ ----------------- ------
```

```
allevents       -                 -                 -                 false
asup            -                 -                 -                 false
criticals       -                 -                 -                 false
pager           -                 -                 -                 false
traphost        -                 10.229.88.174
     -                  false
5 entries were displayed.

DOT_cluster::*> snmp traphost
        10.229.88.174 (10.229.88.174) <10.229.88.174>

DOT_cluster::*> event generate -messagename wafl.dir.size.warning -values TEST_EVENT

DOT_cluster::*>

2013-05-03 05:33:01 prakashl-vsim1.sim.eng.btc.netapp.in [10.238.44.36] (via UDP:
[10.238.44.36]:161) TRAP, SNMP v1, community public
   SNMPv2-SMI::enterprises.789 Enterprise Specific Trap (485) Uptime: 1:13:17.57
   SNMPv2-SMI::enterprises.789.1.1.12.0 = STRING: "Directory TEST_EVENT is
approaching the maxdirsize limit. "   SNMPv2-SMI::enterprises.789.1.1.9.0 = STRING:
"1-80-000011"
```

追加信息

在此处添加文本。