



Компания Netwell - российский дистрибьютор высокотехнологичного оборудования. Основные направления деятельности – сетевые технологии, системы хранения данных, сетевая и информационная безопасность.

Netwell является **официальным дистрибьютором компании NetApp**.



NETAPP TECHNICAL REPORT

Руководство администратора: Конфигурирование SNMP

Colin Chute, NetApp

Eyal Horowitz, NetApp

Март 2013 | TR-4149

Коротко о главном:

Кроме подробных технических наилучших практик и рекомендаций, разрабатываемых и публикуемых компанией NetApp, для системных администраторов также полезными являются краткие справочники действий при конфигурации, а также нормы и политики для успешной быстрой настройки выбранных систем. Эта серия документов нацелена на потребности системных администраторов, занимающихся практическим конфигурированием таких систем хранения.

Оглавление

| | |
|---|----|
| 1 Введение | 3 |
| 1.1 Обзор | 3 |
| 1.2 Версии SNMP | 3 |
| 1.3 SNMP Traps | 4 |
| 1.4 MIB | 4 |
| 2 Установка встроенных Traps в 7-Mode из командной строки | 5 |
| 2.1 Включение SNMP | 5 |
| 2.2 Задание Community Name для SNMPv1 | 5 |
| 2.3 Создание пользователя для работы с SNMPv3 | 5 |
| 2.4 Установка привилегии доступа к SNMP | 6 |
| 2.5 Задание Trap Hosts | 6 |
| 2.6 Проверка установок | 6 |
| 2.7 Определяемые пользователем (User-Defined) Traps | 7 |
| 3 Установка SNMP в Clustered Data ONTAP из командной строки | 7 |
| 3.1 Включение SNMP | 7 |
| 3.2 Задание Community Name для SNMPv1 | 8 |
| 3.3 Создание пользователя для работы с SNMPv3 | 8 |
| 3.4 Установка привилегии доступа к SNMP | 8 |
| 3.5 Задание Traphost | 8 |
| 4 Конфигурирование SNMP в OnCommand System Manager GUI (Data ONTAP 7-Mode and Clustered Data ONTAP) | 9 |
| 4.1 Вход в OnCommand System Manager | 9 |
| 4.2 Переход к экрану SNMP Configuration | 9 |
| 4.3 Конфигурирование SNMP через GUI | 9 |
| 5 Конфигурирование SNMP в OnCommand Operations Manager GUI (Data ONTAP 7-Mode и Clustered Data ONTAP) | 13 |
| 5.1 Вход в Operations Manager | 13 |
| 5.2 Переход к экрану SNMP Configuration | 13 |
| 5.3 Конфигурирование SNMP через GUI | 14 |
| 5.4 Конфигурирование уведомлений (Alarms) | 16 |

1 Введение

Этот документ предлагает обзор темы использования *Simple Network Management Protocol (SNMP)* и примеры его конфигурирования для NetApp® Data ONTAP® 7-Mode, clustered Data ONTAP, и системе управления *OnCommand® (GUI)*. Этот документ также предлагает пошаговые инструкции по настройке и установке SNMP для мониторинга систем.

1.1 Обзор

Протокол SNMP используется для обмена информацией по управлению и наблюдению за различными включенными в локальную сеть устройствами. Существует множество устройств, поддерживающих SNMP, куда входят маршрутизаторы, коммутаторы, серверы, рабочие станции и принтеры. Системы хранения, работающие под управлением Data ONTAP 7-Mode, Clustered Data ONTAP, и программной системы управления семейства *OnCommand* также могут использовать возможности и функциональность протокола SNMP.

Ключевые компоненты, входящие в архитектуру SNMP это:

- **SNMP manager.** Также называемый иногда *Network management system (NMS)*. NMS отвечает за взаимодействие с *SNMP agent*.
- **SNMP managed device.** Оборудование, требующее наблюдения.
- **SNMP agent.** Отвечает на запросы *SNMP manager*. *SNMP agent* обычно встроен в OS устройства, и вы можете включить или выключить его по необходимости. Агент работает как шлюз между *SNMP manager* и *Management information base (MIB)*.
- **Management information base (MIB).** Файл, который может использоваться для связи и взаимодействия между *manager* и *agent*. MIB содержит все значения, определенные для наблюдаемого устройства. Для понимания его работы давайте возьмем как пример букву Q в алфавите. Программа-менеджер запрашивает агента: "У вас есть Q в алфавитном списке?" Агент просматривает список с буквами алфавита (наш MIB) и отвечает: "Да, у нас есть Q и это 17 буква в алфавите." Без MIB, агент просто не понял бы, что у него спрашивает программа-менеджер.

После того, как вы включите SNMP в Data ONTAP, *SNMP manager* сможет отправлять запросы к агенту SNMP на системе хранения (определенные в MIB на системе хранения или в спецификации MIB-II). В ответ на запрос *SNMP agent* собирает информацию и отправляет ее на *SNMP manager* по протоколу SNMP.

SNMP agent также генерирует уведомления с помощью механизма *trap*, когда возникает заданная ситуация, и отправляет *traps* на *SNMP manager*. *SNMP manager* может, приняв эту информацию, предпринять заданные действия.

1.2 Версии SNMP

Для диагностики, мониторинга и сетевого управления Data ONTAP имеет *SNMP agent*, который поддерживает SNMP версий 1 и 3. Для доступа по версии протокола SNMPv1 используется строка так называемого *community*. В большинстве случаев, строка *community* по умолчанию – *public*. Эта строка позволяет другим системам получать доступ к SNMP на устройстве. Строка *community* похожа по своему смыслу на пароль, когда тому, кому нужен доступ к устройству, должен его предварительно знать. SNMPv3 использует уже имя и пароль, а также шифрование, чтобы повысить безопасность доступа. SNMPv3 поддерживает также спецификацию MIB-II.

1.3 SNMP Traps

Так называемые *SNMP traps* захватывают информацию системного мониторинга с Data ONTAP. Когда значение переменной MIB соответствует заданной величине, событие *trap* отсылается на хост сетевого управления, определенный в списке *traphost list*. Список, под названием *traphost list* определяет компьютеры, на которых установлено ПО *SNMP Manager*, принимающее *traps*.

Существует два типа *traps* в Data ONTAP:

- Встроенные *trap*
- Определяемые пользователем *trap*

Встроенные (built-in) *traps* заранее заданы в Data ONTAP. В случае, если происходит соответствующее событие, *trap* автоматически отсылается на адрес, заданный как *traphost*. Встроенные *traps* основываются на следующих:

- RFC 1213, который определяет такие *traps*, как *coldStart*, *linkDown*, *linkUp*, и *authenticationFailure*
- *Traps*, определенные в MIB устройства, такие как *diskFailedShutdown*, *cpuTooBusy*, и *volumeNearlyFull*

Определенные пользователем *traps* задаются командой `snmp trap` или в окне FilerView® *SNMP Traps*. Они посылаются с использованием *proxy trap ID* номером от 11 до 18, соответствующей приоритету *trap*-ов в MIB.

1.4 MIB

Файл MIB это текстовый файл, описывающий объекты SNMP и *traps*. MIB-ы это не конфигурационные файлы. Data ONTAP не читает эти файлы, и их содержимое не влияет на функциональность SNMP.

Data ONTAP 7-Mode и Clustered Data ONTAP предлагает два файла MIB:

- Custom MIB (`/etc/mib/netapp.mib`)
- iSCSI MIB (`/etc/mib/iscsi.mib`)

Data ONTAP также предоставляет файл с соответствием между идентификатором объектов (object identifier, OID) и коротким именем объекта: `/etc/mib/traps.dat`. Этот файл полезен при создании собственных, задаваемых пользователем *traps*.

Внимание: Свежие версии Data ONTAP MIBs и файлы `traps.dat` доступны в интернете на сайте Сайт NetApp Support (<http://support.netapp.com/>). Однако, версии файлов на сайте могут не соответствовать SNMP для установленной у вас версии Data ONTAP. Эти файлы помогут вам оценить возможности SNMP на наиболее новой версии Data ONTAP.

Data ONTAP MIB в *OnCommand* находится по адресу `<installationdirectory>/NTAPdfm/misc`.

Файл *OnCommand MIB* содержит *trapID* для событий *OnCommand*. Этот файл используется, когда *OnCommand* конфигурируется для отсылки *traps* в сторонние инструменты, такие как *IBM Tivoli* и *HP OpenView*.

OnCommand MIB (`dfm.mib`) находится по адресу `<installationdirectory>/NTAPdfm/misc`.

2 Установка встроенных Traps в 7-Mode из командной строки

2.1 Включение SNMP

```
options snmp.enable on
```

2.2 Задание Community Name для SNMPv1

```
snmp community add {rocommunity}
```

Значение по умолчанию для имени *community* в SNMP agent в Data ONTAP задано как `public`. Единственно возможный тип доступа к системе хранения, заданный по умолчанию, это `ro` (read-only).

2.3 Создание пользователя для работы с SNMPv3

1. Введите следующую команду для создания роли с возможностью `login-snmp`:

```
useradmin role add role_name -a login-snmp
```

`role_name` это имя роли с возможностью `login-snmp`.

Пример:

```
useradmin role add myrole1 -a login-snmp
```

2. Введите следующую команду для создания группы и добавления созданной роли в эту группу:

```
useradmin group add group_name -r role_name
```

`group_name` это имя группы, в которую вы хотите добавить созданную роль, по имени, `role_name`.

Пример:

```
useradmin group add mygroup1 -r myrole1
```

3. Введите следующую команду для создания пользователя и добавления его в созданную группу:

```
useradmin user add user_name -g group_name
```

`user_name` это имя пользователя, который принадлежит группе `group_name`.

Пример:

```
useradmin user add myuser1 -g mygroup1
```

4. Создайте пароль для нового пользователя. Убедитесь, что в пароле минимум восемь символов.

5. Запустите команду `snmpwalk` на системный MIB:

```
snmpwalk -v 3 -u user_name -l authNoPriv -A password storage_system system
```

`password` это пользовательский пароль, введенный на шаге 4. `storage_system` это система хранения, содержащая MIB-ы.

Пример:

```
snmpwalk -v 3 -u myuser1 -l authNoPriv -A johndoe123 host1 system
```

2.4 Установка привилегии доступа к SNMP

```
options snmp.access access_spec
```

`access_spec` содержит ключевые слова и их значения. Доступ может быть разрешен или ограничен для определенных имен хостов, IP и имен сетевых интерфейсов.

Пример: Для того чтобы разрешить доступ по протоколу SNMP для сетевых интерфейсов `e0`, `e1`, and `e2`, введите команду:

```
options snmp.access if=e0,e1,e2
```

2.5 Задание Trap Hosts

```
snmp traphost [{add|delete} { hostname|ipaddress}]
```

где опции добавляют (`add`) или удаляют (`delete`) хосты SNMP, которые могут принимать трапы Data ONTAP.

Если на вашей системе хранения включен IPv6, вы можете добавить или удалить адрес IPv6 для `traphost`. Вы можете задать адрес IPv6 (но не имя хоста), для определения `IPv6 traphost`.

Команда без опций показывает заданный текущий `traphost` в Data ONTAP.

2.6 Проверка установок

После выполнения необходимых шагов конфигурации, Data ONTAP будет сконфигурирована на автоматическую отсылку событий на компьютер с системой сетевого управления, определенную в `traphost`. В Таблице 1 вы можете посмотреть синтаксис команд SNMP и их описание. Если вы задаете значение в опции команды SNMP, то оно устанавливается или же изменяется уже установленное. Однако если значение не задано, то возвращается текущее значение для данной опции.

В таблице 1 показан синтаксис команд SNMP.

Таблица 1) Синтаксис команд SNMP.

| Команда | Описание |
|--|--|
| <code>snmp</code> | Показывает текущие заданные значения всех опций SNMP, таких как <code>init</code> , <code>community</code> , <code>contact</code> , и <code>traphost</code> . |
| <code>snmp authtrap [0 1]</code> | С заданным значением: Включает (при задании 1) или выключает (при задании 0) <code>traps</code> для события <code>authentication failure</code> в <code>SNMP agent</code> . Без заданного значения: Показывает текущее значение <code>authtrap</code> в Data ONTAP. |
| <code>snmp community</code> | Отображает текущий список <code>communities</code> . |
| <code>snmp community add rocommunity</code> | Добавляет <code>community</code> . Значение по умолчанию: Значение <code>community</code> по умолчанию для <code>SNMP agent</code> в Data ONTAP задано как <code>public</code> . Единственно возможный вариант доступа к SMTP на системе хранения - <code>ro</code> (read-only). |
| <code>snmp community delete {all rocommunity}</code> | Удаляет одно или все <code>communities</code> . |

| | |
|---|--|
| snmp contact [contact] | С заданным значением: Указывает значение <i>contact name</i> для системы хранения. Вы должны указывать значение заключенным в кавычки (“ ”) если строка содержит пробелы. Вы можете ввести в качестве контактной информации строку длиной 255 символов. Без заданного значения: Показывает текущее значение <i>contact name</i> в Data ONTAP. |
| snmp init [0 1] | С заданным значением: Включает (при задании 1) или выключает (при задании 0) встроенные <i>traps</i> и определенные командой <code>snmp traps</code> . Без заданного значения: Показывает текущее значение <code>snmp init</code> в Data ONTAP. Значение по умолчанию: По умолчанию, <i>SNMP traps</i> отключены в Data ONTAP; это эквивалентно <code>snmp init 0</code> . |
| snmp location [location] | С заданным значением: Указывает значение <i>location</i> для системы хранения. Вы должны указывать значение заключенным в кавычки (“ ”) если строка содержит пробелы. Вы можете ввести в качестве <i>location</i> строку длиной 255 символов. Без заданного значения: Показывает текущее значение в Data ONTAP. |
| snmp traphost [{add delete} {hostname ipaddress}] | С заданным значением: Добавляет или удаляет хосты SNMP, принимающие <i>traps</i> от Data ONTAP. Когда на системе включено использование IPv6, вы можете добавить <i>traphosts</i> с использованием IPv6. Вы можете задать адрес IPv6, но не имя хоста, для указания <i>traphosts</i> с использованием IPv6. Без заданного значения: Показывает текущее значение <i>traphosts</i> в Data ONTAP. |
| snmp traps [options] | Показывает список определенных пользователем <i>traps</i> в Data ONTAP |

2.7 Определяемые пользователем (User-Defined) Traps

User-defined traps это дополнительная возможность Data ONTAP. Если предустановленных встроенных *traps* недостаточно для создания нужных администратору уведомлений, вы можете создать свои собственные *traps* в Data ONTAP. Перед созданием нового *trap* вам следует внимательно просмотреть Data ONTAP MIB, так как нужный вам *trap* уже вполне может там существовать.

Внимание: Специальная конфигурация SNMP выходит за рамки этого документа, так как использовать определяемые пользователем *traps* не требуется в большинстве случаев типовой установки системы хранения. Если необходимо использовать пользовательские *trap*, то следует рассмотреть вариант с использованием продуктов OnCommand, он имеет многочисленные специальные возможности и прост в использовании. Конфигурирование *traps* в OnCommand будет рассмотрено ниже в этом документе.

Для подробного рассмотрения темы *user-based traps*, смотрите **Data ONTAP Network Management Guide**, доступный на сайте NetApp Support site (<http://support.netapp.com/>).

3 Установка SNMP в Clustered Data ONTAP из командной строки

3.1 Включение SNMP

Из консоли кластера выполните команду, идентичную команде для 7-Mode.

```
options snmp.enable on
```

3.2 Задание Community Name для SNMPv1

Задайте *community name* из консоли кластера.

```
system snmp community add -community-name thecommunity
```

3.3 Создание пользователя для работы с SNMPv3

Запустите приведенную команду и ответьте на предлагаемые вопросы.

Внимание: Команда длинная, и часть ее в данном документе перенесена на вторую строку. Вы должны ввести ее целиком в одну строку.

```
security login create -username mysnpuser -application snmp -authmethod usm -role  
readonly -vserver Cluster01
```

Enter the authoritative entity's EngineID [local EngineID]: нажмите Enter для принятия значения по умолчанию.

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

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

Enter the authentication protocol password again: Повторно введите пароль.

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

3.4 Установка привилегии доступа к SNMP

В Clustered Data ONTAP, привилегии доступа к SNMP конфигурируются через настройки файрволла. Для конфигурирования на пользовательском сайте используйте подсеть IP и привилегии доступа.

```
system services firewall policy modify -policy data -service snmp -action allow -ip-  
list 172.17.0.0/16
```

Внимание: Команда длинная, и часть ее в данном документе перенесена на вторую строку. Вы должны ввести ее целиком в одну строку.

3.5 Задание Traphost

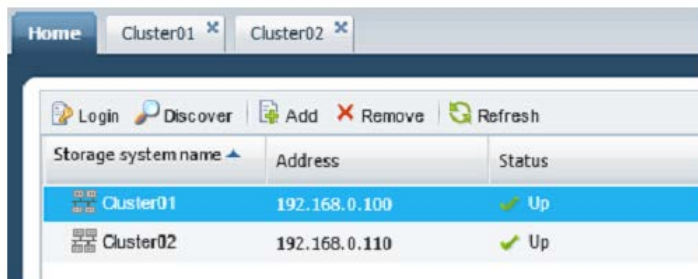
Определите IP-адрес вашего *traphost*.

```
system snmp traphost add 172.17.68.4
```

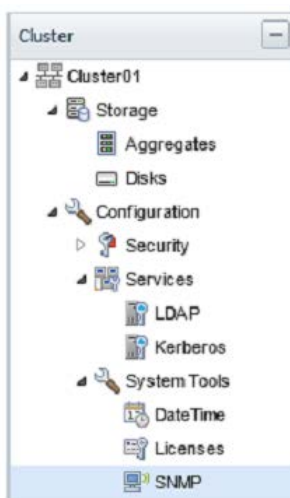
SNMP успешно сконфигурирован в Clustered Data ONTAP.

4 Конфигурирование SNMP в OnCommand System Manager GUI (Data ONTAP 7-Mode and Clustered Data ONTAP)

4.1 Вход в OnCommand System Manager



4.2 Переход к экрану SNMP Configuration

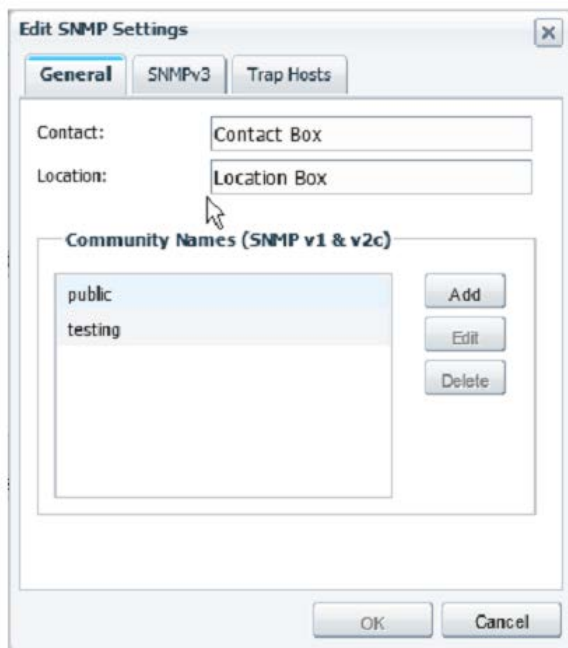


4.3 Конфигурирование SNMP через GUI

1. Щелкните **Edit**.



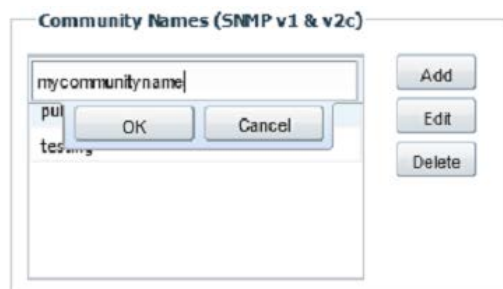
2. Появится окно **Edit SNMP Settings**. Введите **Contact and Location details**.



3. Если вы используете *SNMPv1*, перейдите к шагу 4. Если *SNMPv3*, перейдите к шагу 5.

4. Если вы используете *SNMPv1*, щелкните **Add** и введите *community name*.

Щелкните **OK** для записи изменений.



5. Если вы используете *SNMPv3*, щелкните закладку **SNMPv3**. И затем щелкните **Add**.



6. Появится окно **Add SNMPv3 User**.

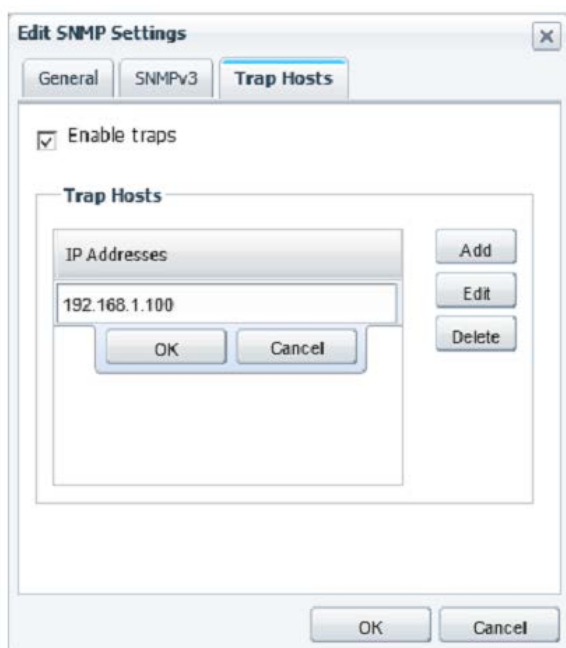
- Введите **User Name**.
- Значение по умолчанию появится в **Engine ID**.

- По умолчанию, *md5* появится в качестве протокола аутентификации по умолчанию. Вы можете выбрать нужный вам.
- Введите и подтвердите пароль.
- Укажите **Privacy Protocol** как *none*.
- Щелкните **OK**.



7. Для конфигурирования *trap host*, щелкните закладку **Trap Hosts**.

- Отметьте чекбокс **Enable Traps**.
- Щелкните **Add** и введите IP-адрес *trap host*.
- Щелкните **OK**.



8. Щелкните **OK** для перемещения на главный экран.

SNMP home screen показывает все изменения, которые будут выполнены.



9. Если вы пользуетесь *Data ONTAP 7-Mode*, перейдите на шаг 10. Если вы пользуетесь *Clustered Data ONTAP*, перейдите на шаг 9.

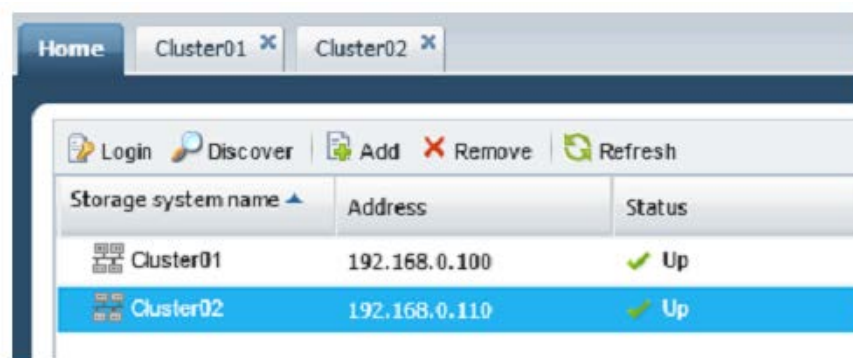
Щелкните кнопку **Advanced** и просмотрите выпадающее меню **SNMP service** для подтверждения изменений, применяемых к кластеру.



10. Если вы используете *Data ONTAP 7-Mode*, повторите все указанные шаги на другом узле НА-пары контроллеров.

Если вы используете *Clustered Data ONTAP*, повторите все указанные шаги на других кластерах, если такие у вас есть.

Внимание: Установка SNMP распространяется на все узлы кластера при конфигурировании *Clustered Data ONTAP*. Не требуется отдельно конфигурировать каждый узел кластера в отдельности. Например, если вы используете *Clustered Data ONTAP* и используете один кластер из двух узлов в нем, вы должны выполнить указанные процедуры только один раз.



Итак, вы успешно сконфигурировали SNMP на вашей системе хранения.

5 Конфигурирование SNMP в OnCommand Operations Manager GUI (Data ONTAP 7-Mode и Clustered Data ONTAP)

5.1 Вход в Operations Manager

5.2 Переход к экрану SNMP Configuration

- Щелкните **Setup > Network Credentials**.



- Появится экран **Network Credentials**:

Network Credentials

20 Dec 14:43

Add Network Credentials

Network Address
(e.g. 172.24.1.0, 172.24.1.0/24, ABCD:EF01:0::2345, ABCD:EF01:0::2345/60)

Network Mask or Prefix Length
(e.g. 255.255.240.0, 24)

Preferred SNMP Version:

SNMPv1 Settings

SNMP Community
(If unspecified then SNMPv1 will be disabled for the network)

SNMPv3 Settings

Auth Protocol:

Login
(If unspecified then SNMPv3 will be disabled for the network)

Password
(Mandatory when Login is specified)

Privacy Password

| Network Address | Prefix Length | Preferred SNMP Version | SNMP Community | Auth Protocol | Login | Privacy Enabled | Edit Delete |
|-----------------|---------------|------------------------|----------------|---------------|-------|-----------------|----------------------|
| default | | SNMPv1 | public | | | | edit |

5.3 Конфигурирование SNMP через GUI

1. Для использования *SNMPv1*, выполните следующие шаги:

- Введите данные об адресе сети и подсети.
- Убедитесь что в **Preferred SNMP Version** установлен *SNMPv1*.
- Введите имя **SNMP Community**.
- Щелкните **Add**.

| Add Network Credentials | |
|--|--|
| Network Address (e.g. 172.24.1.0, 172.24.1.0/24, ABCD:EF01:0::2345, ABCD:EF01:0::2345/60) | <input type="text" value="172.17.0.0"/> |
| Network Mask or Prefix Length (e.g. 255.255.240.0, 24) | <input type="text" value="255.255.0.0"/> |
| Preferred SNMP Version | <input type="text" value="SNMPv1"/> |
| SNMPv1 Settings | |
| SNMP Community (If unspecified then SNMPv1 will be disabled for the network) | <input type="text" value="thecomunity"/> |
| SNMPv3 Settings | |
| Auth Protocol | <input type="text" value="MD5"/> |
| Login (If unspecified then SNMPv3 will be disabled for the network) | <input type="text"/> |
| Password (Mandatory when Login is specified) | <input type="text"/> |
| Privacy Password | <input type="text"/> |
| <input type="button" value="Back"/> <input type="button" value="Add"/> | |

Новая конфигурация будет показана в нижней части экрана.

2. Для использования SNMPv3, выполните следующие шаги:

- Введите данные об адресе сети и подсети.
- Измените значение в **Preferred SNMP Version** на *SNMPv3*.
- Оставьте поле **SNMP Community name** пустым. По умолчанию, *MD5* появится как протокол аутентификации по умолчанию. Вы можете выбрать другой протокол аутентификации, если это необходимо.
- Введите имя пользователя в **Login**.
- Введите пароль для этого имени пользователя в поле **Password**.
- Оставьте поле **Privacy Password** пустым.
- Щелкните **OK**.

| Add Network Credentials | |
|--|--|
| Network Address (e.g. 172.24.1.0, 172.24.1.0/24, ABCD:EF01:0::2345, ABCD:EF01:0::2345/60) | <input type="text" value="172.17.0.0"/> |
| Network Mask or Prefix Length (e.g. 255.255.240.0, 24) | <input type="text" value="255.255.0.0"/> |
| Preferred SNMP Version | <input type="text" value="SNMPv3"/> |
| SNMPv1 Settings | |
| SNMP Community (If unspecified then SNMPv1 will be disabled for the network) | <input type="text"/> |
| SNMPv3 Settings | |
| Auth Protocol | <input type="text" value="MD5"/> |
| Login (If unspecified then SNMPv3 will be disabled for the network) | <input type="text" value="snmpv3login"/> |
| Password (Mandatory when Login is specified) | <input type="text" value="*****"/> |
| Privacy Password | <input type="text"/> |
| <input type="button" value="Back"/> <input type="button" value="Add"/> | |

Новая конфигурация будет показана в нижней части экрана.

3. Для нормальной работы всей системы укажите идентичные настройки SNMP как на системе хранения, так и в OnCommand.

На скриншоте вы видите указанное имя *community* как **public**. Убедитесь, что вы используете отдельное имя *community* или указали настройки v3 на всех используемых системах хранения и экземплярах OnCommand, использование уникального имени *community* вместо *public*, послужит дополнительным уровнем обеспечения безопасности доступа.

```
C:\>dfm host diag fas02

Network Connectivity
IP Address          192.168.0.151
Network            192.168.0.0/24 <last searched 20 Dec 15:38>
DNS Aliases        fas02.demo.netapp.com
DNS Addresses      192.168.0.151
SNMP Version in Use  SNMPv1
SNMPv1             Passed <47 ms>
SNMP Community     public
SNMP sysName       fas02.demo.netapp.com
SNMP sysObjectID   .1.3.6.1.4.1.789.2.3 <Clustered Filer>
SNMP productid    0135099476
SNMPv3             Failed: No SNMPv3 username specified.

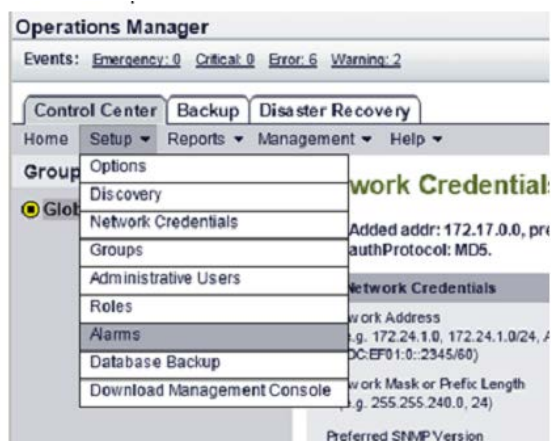
SNMPv3 Auth Protocol
SNMPv3 Privacy Enabled No
SNMPv3 Username
ICMP Echo          Passed <0 ms>
HTTP               Passed <0 ms>
```

4. Протокол SNMP сконфигурирован на вашей системе.

5.4 Конфигурирование уведомлений (Alarms)

Как дополнительные настройки, вы можете сконфигурировать рассылку уведомлений (alarms) в Operations Manager для отправки *SNMP traps* в случае возникновения какого-либо события. Выполните следующие шаги.

1. Щелкните **Setup > Alarms**.



2. Появится окно **Alarms**:

Alarms

20 Dec 15:06

Add an Alarm

Group:

Global

Select Event By

Severity Event Name

Critical or Worse

All

Email Recipient

DEMO\Administrator

[Advanced Version](#)

[Show all columns](#)

| Event | Severity | Group | Recipients | Disable | Edit | Test | Delete |
|-------|----------|-------|------------|---------|------|------|--------|
|-------|----------|-------|------------|---------|------|------|--------|

3. Укажите уровень важности для генерируемых уведомлений.

В **SNMP Trap Hosts**, введите IP-адрес вашего *trap host* и щелкните **Add**.

Select Event By

Severity Event Name

Critical or Worse

All

Event Class
(regular expression to select a class of events e.g. env\temp)

Recipients

Email Recipients - Admins
(specify full login names of administrators)

Email Recipients - Non-Admins
(specify email addresses)

Page Recipients - Admins
(specify full login names of administrators)

Page Recipients - Non-Admins
(specify pager addresses)

SNMP Trap Hosts

172.17.101.202

Other Options

Time From

00:00

Time To

23:59

Repeat Notify

No

Repeat Interval

30

Disable

No

[Simple Version](#)

Новое уведомление создано, и Operations Manager сконфигурирован на отсылку *SNMP traps* на компьютер *trap host*.