Мониторинг виртуальных машин через SNMP

Для мониторинга параметров виртуальных машин Windows вам потребуется установить два элемента:

а. Сервер мониторинга

> Виртуальная машина, развернутая на VMhosts, предназначенная для внутреннего мониторинга каждого из клиентов. Он будет подключен к той же VLAN, что и клиент.
>
> Пример технических характеристик: Характеристики виртуальной машины: 1 ядро, 2 ГБ ОЗУ, 10 ГБ встроенной памяти.

б. Служба SNMP (агент), установленная на виртуальных машинах Windows, которые вы хотите отслеживать.

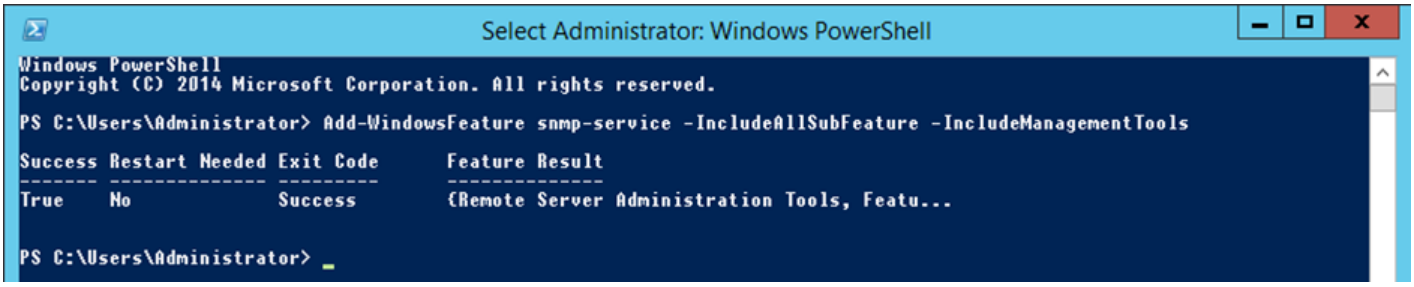
> Убедитесь, что брандмауэр (фаервол) Windows разрешает трафик SNMP.

Шаг 1:

Установка службы SNMP, дополнительных функций и инструментов управления. Это можно сделать с помощью функций добавления и удаления или с помощью PowerShell, используя следующую команду на назначенном сервере:

Для версии Wndows Powershell 2014 используйте:

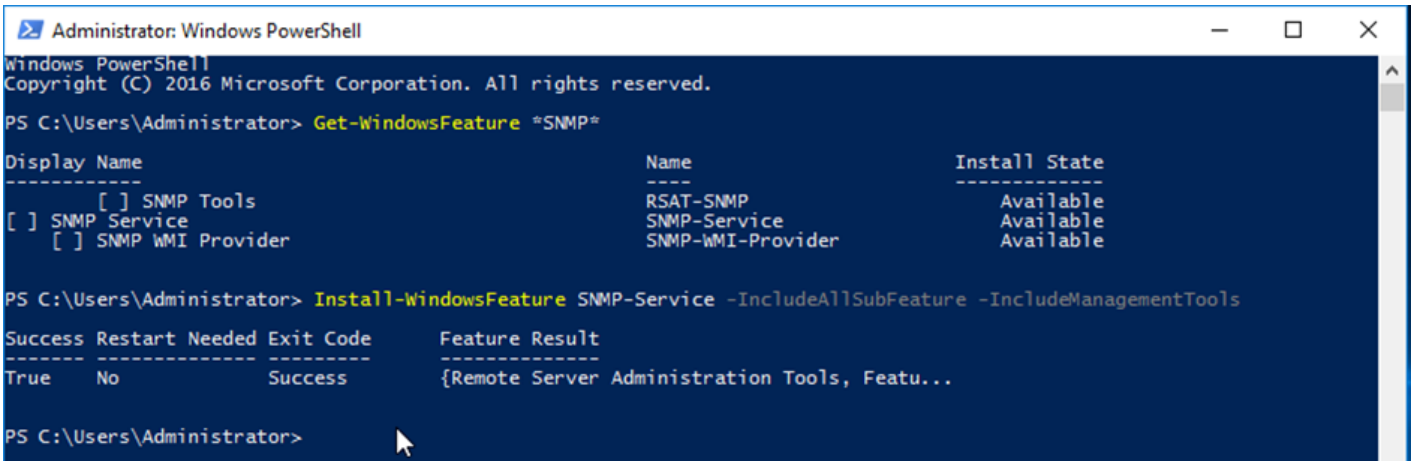
```
Add-WindowsFeature snmp-service –IncludeAllSubfeatures –IncludeManagementTools
```



Для выпуска Windows Powershell 2016 используйте

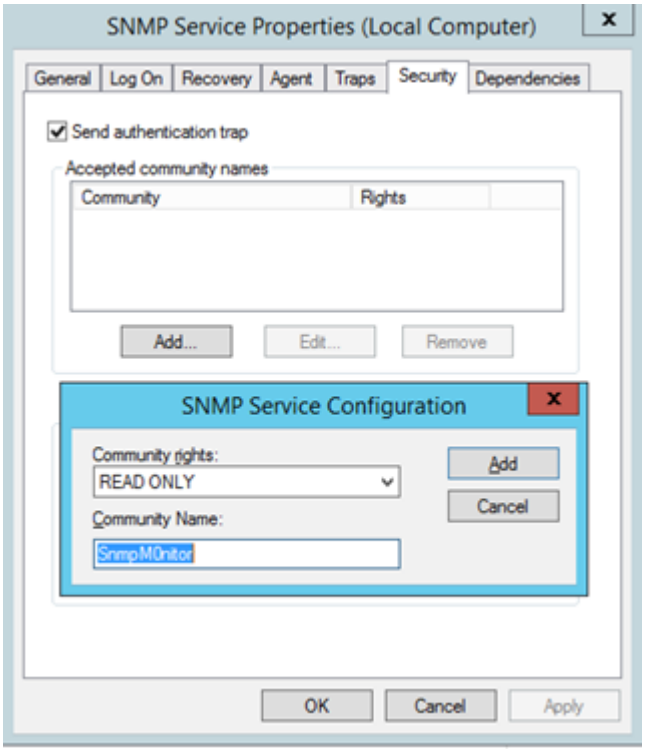
Чтобы проверить, установлен ли SNMP, выполните команду: `Get-WindowsFeature *SNMP*`

Чтобы установить SNMP, выполните команду `Install-WindowsFeature SNMP-Service -IncludeAllSubFeature -IncludeManagementTools`



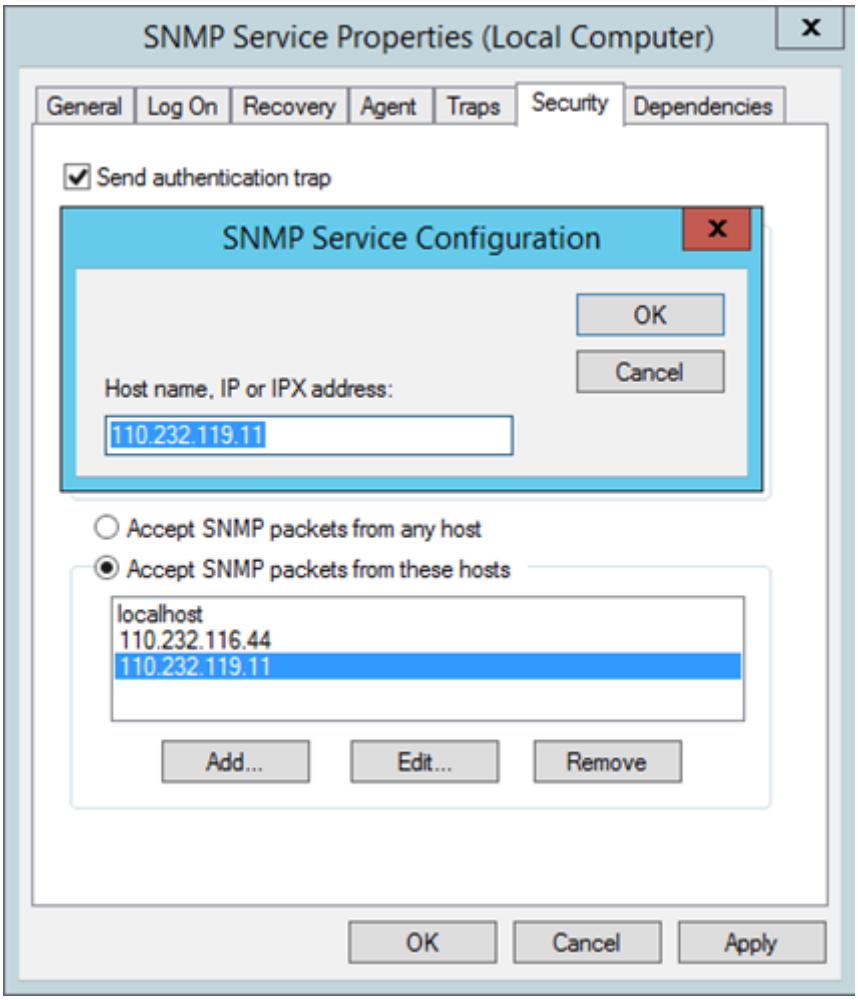
Шаг 2:

Откройте панель «Службы» через Панель управления/Администрирование или щелкнув правой кнопкой мыши кнопку «Пуск», выбрав «Выполнить» и введя Services.msc, а затем «OK».



Перейдите к «Службе SNMP» и дважды щелкните службу. Откроется диалоговое окно со свойствами службы SNMP.

Далее нам нужно будет перейти на вкладку «Безопасность», а затем нажать кнопку «Добавить» под заголовком «Принятые имена сообществ». Теперь вы можете ввести имя сообщества, которое вам подходит. Для этого примера мы использовали SnmpM0nitor.



Теперь нам нужно будет настроить, откуда сервер будет принимать пакеты SNMP, это настраивается в заголовке «Принимать пакеты SNMP от этих хостов», нажмите кнопку «ДОБАВИТЬ» и введите IP-адреса серверов мониторинга SNMP, которые вы используете. только что настроил.

После завершения выберите «Применить» и «OK», чтобы выйти. Перезапустите службу, щелкнув правой кнопкой мыши «Служба SNMP» и выбрав «Перезапустить».

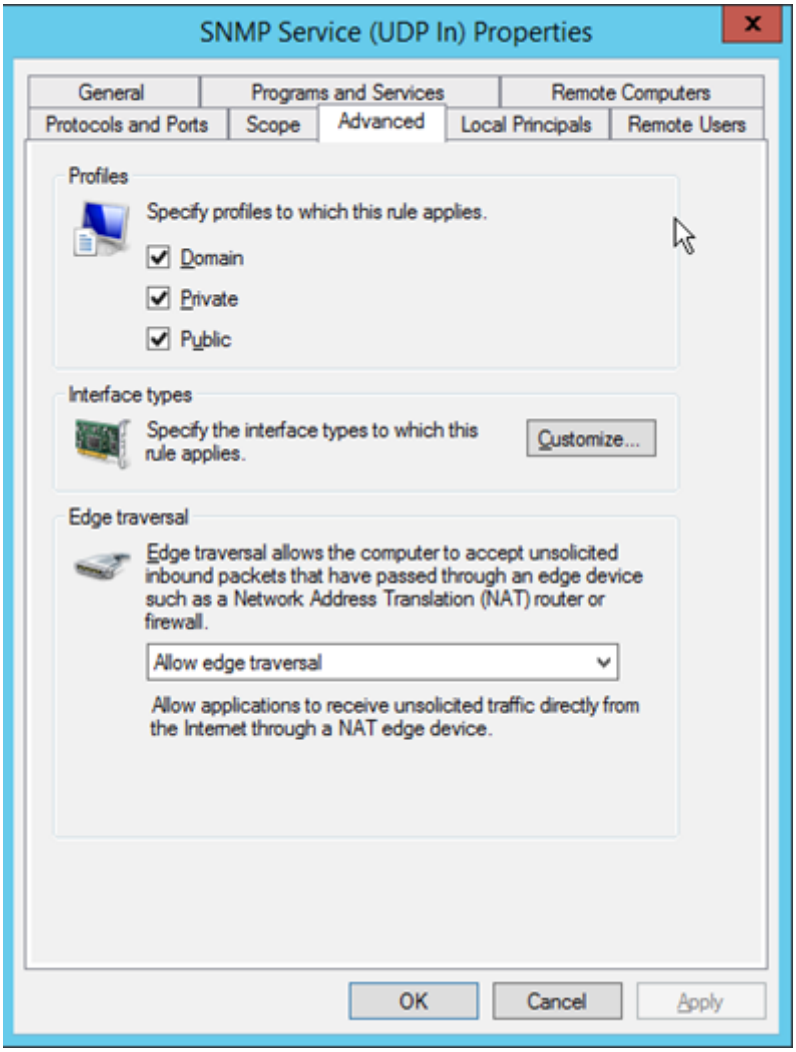
Шаг 3:

После установки и настройки SNMP вам необходимо будет скачать и установить следующее приложение «SNMP-Informant» — http://www.wtcs.org/informant/files/informant-std-17.zip.

Это предоставит SNMP правильные MIB для службы облачного мониторинга — дополнительная структура MIB содержит собранную информацию в совместимом формате.

Шаг 4:

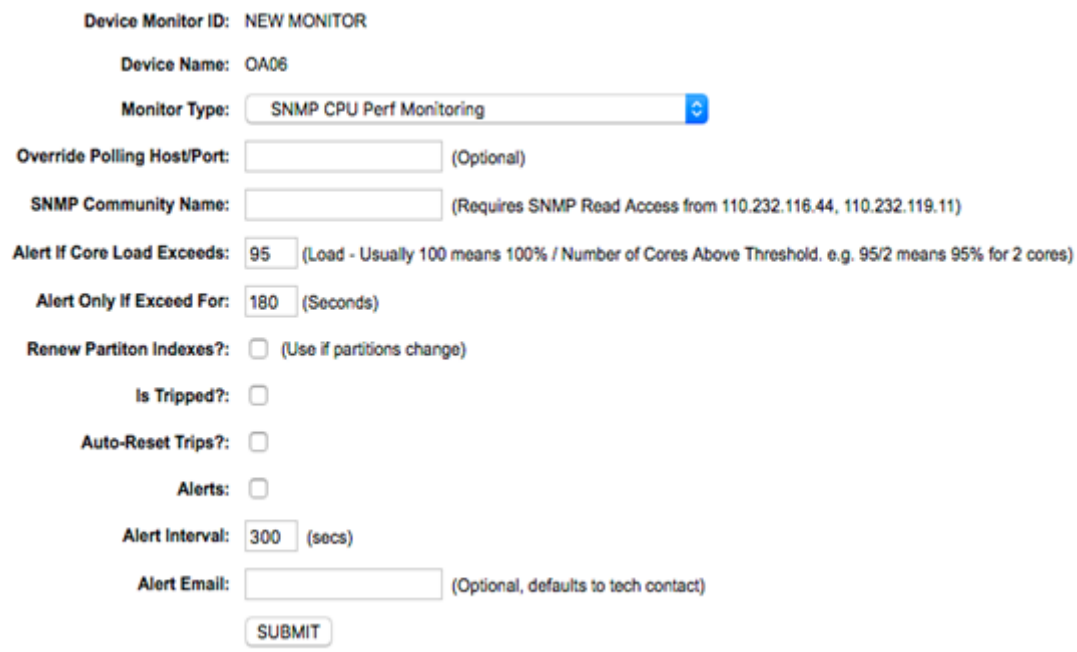
Правила брандмауэра необходимо обновить, чтобы разрешить входящие запросы SNMP. Откройте «Брандмауэр Windows с дополнительными настройками», который находится в «Панели управления», затем «Администрирование».



Найдите существующие правила обслуживания SNMP (UDP In) и дважды щелкните первое из них (какое из них не важно), выберите вкладку «Дополнительно» и убедитесь, что отмечены галочки «Домен», «Частный и общедоступный», затем измените «Edge Traversal». на «Разрешить обход края». Выберите OK и закройте оставшиеся окна..

Шаг 5:

На облачном портале перейдите к серверу, на котором установлен агент SNMP (вкладка «Службы» / «Серверы»). На странице «Сводка по серверу» выберите вкладку «Мониторинг».



Выберите «ДОБАВИТЬ НОВЫЙ МОНИТОР», а затем нужный вам «Тип монитора». Следующая страница будет содержать поля, необходимые вашей системе облачного мониторинга для успешного мониторинга нужного сервера.

Рекомендуем заполнить следующие поля:

Имя сообщества SNMP: будет строкой сообщества SNMP, ранее определенной на шаге 2.

Порог оповещения: если ваш ЦП мониторинга указывает загрузку ЦП, при которой будет выдаваться оповещение.

Только при превышении: продолжительность превышения порогового значения оповещения для срабатывания оповещения (важно, поскольку случаются кратковременные всплески ЦП).

Оповещение: это позволит создавать оповещения, если параметры оповещения будут соблюдены.

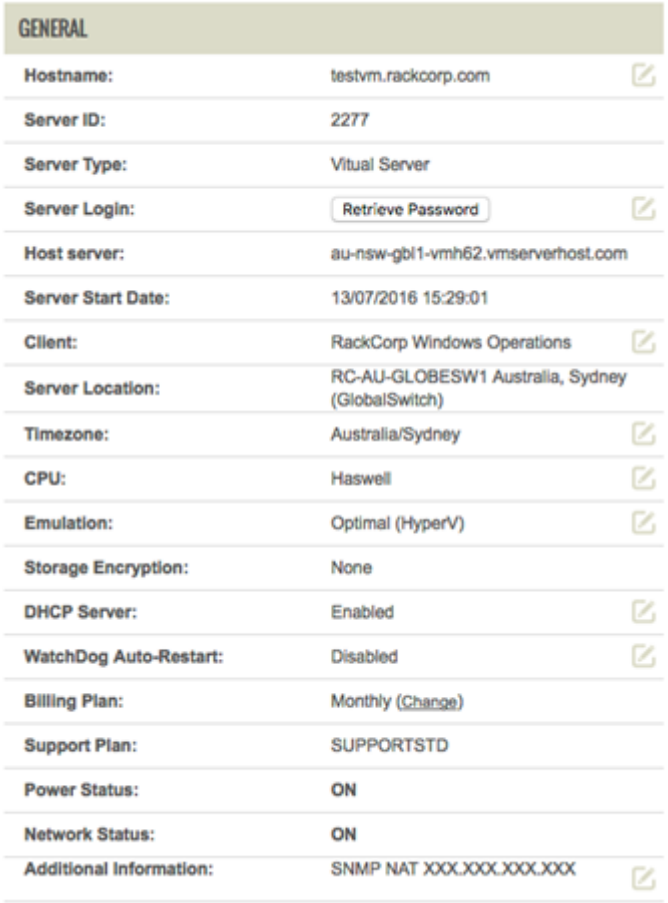
Электронная почта для оповещений: укажите адрес электронной почты для получения оповещений.

Если эти поля заполнены, нажмите «Отправить». Вы вернетесь на предыдущую страницу «Вкладка «Мониторинг», где увидите новый монитор. Метрики начнут поступать, и через 10 минут вы должны увидеть некоторую информацию. Затем вы можете добавить больше мониторов в зависимости от ваших требований.

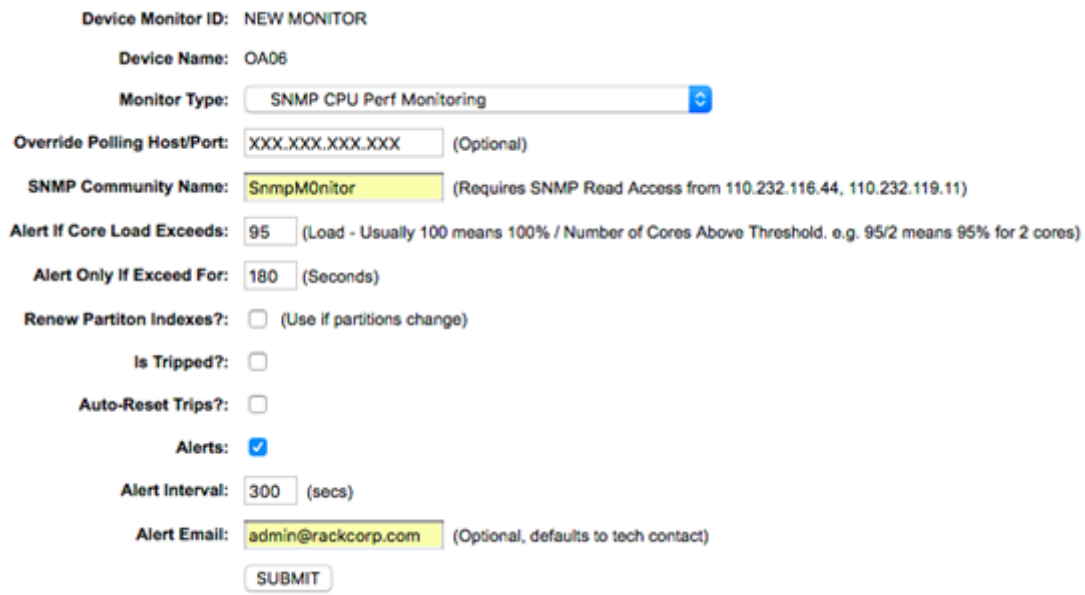
Шаг 6: Этот шаг необходим только в том случае, если ваш сервер имеет частный IP-адрес и находится за брандмауэром NAT.

Ожидается, что до этого шага на брандмауэре по периметру вашего брандмауэра будет установлен общедоступный IP-адрес NAT или PAT для назначенных серверов. Инструкции NAT и PAT не включены в этот документ из-за разнообразия доступных брандмауэров — мы рекомендуем вам обратиться к поставщику средств управления брандмауэром, чтобы настроить их для вас.

Как только вы узнаете о публичном IP-адресе вашего сервера и связанном с ним правиле брандмауэра, которое разрешает SNMP (порт 161 UDP), вам нужно будет отредактировать поле «Дополнительная информация» на странице сводки сервера.



Необходимо вставить следующую информацию: «SNMP NAT <ip-адрес>», где <ip-адрес> будет содержать общедоступный IP-адрес, предоставленный вашим поставщиком системы управления межсетевым экраном.



Вернитесь к монитору, который мы ранее настроили на вкладке «Монитор». Здесь нам нужно будет заполнить поле «Переопределить узел/порт опроса» общедоступным IP-адресом, ранее использовавшимся в поле «Дополнительная информация».

Если вы использовали AT, вам нужно будет указать порт после IP-адреса с точкой с запятой, используемой в качестве разделителя. например 110.232.116.11:14000

Нажмите «Отправить», и ваш монитор должен отобразить показатели в течение 10 минут.

.

Revision #2
Created 27 June 2024 08:22:54 by KonS
Updated 27 June 2024 08:31:08 by KonS