- Kvazar`s Blog - http://mcp.su -

Настройка Event Collector в Windows Server 2008

Posted By Kvazar On 18.02.2009 @ 15:39 In Windows Server 2008 | No Comments

В новой линейке Windows появилась замечательная функция сбора логов с разных серверов и рабочих станций. Это позволяет значительно сократить время на просмотр событий, если у вас несколько систем. То есть, на одном из серверов под управлением Windows Server 2008 вы настраиваете подписку на нужные Вам эвенты других компьютеров и просматриваете их в одной консоли. Можно собирать события с систем под управлением Windows Server 2008/Vista, а также, после установки дополнительного софта, и с Wisdows Server 2003.

Подготовка:

- На каждом компьютере, с которых вы хотите собирать логи, запустите команду ***winrm quickconfig***;
- Добавьте учетную запись компьютера, который будет собирать логи (целевой компьютер), в группу **«Event Log Readers»** (Читатели журналов событий) каждого из этих компов;
- В командной строке целевого компьютера выполните ***wecutil qc***.
  Если вы планируете изменять параметры Minimize Bandwidth или Minimize Latency, дополнительно введите команду ***winrm quickconfig****;*

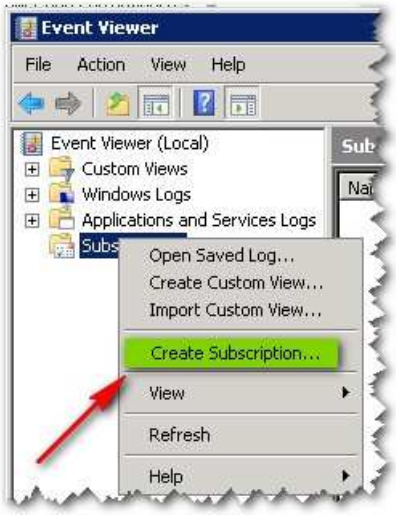
  Помимо ручной настроки, исходящий и целевой компьютеры можно настроить с помощью GPO. Для этого создайте группову политику, например ***GPO-EventForward***. Перейдите: ***Computer Configuration*** >> ***Policy*** >> ***Administrative Templates*** >> ***Windows Components*** >> ***Event Forwarding***. Выберите пункт ***Configure the server adress, refresh interval , and issuer certificate authority of a Target Subscription Manager***. Выберите ***Enable***, нажмите «***Show***» и введите в поле полный fqdn адрес целевого компьютера (сборщика событий).

  Далее, перейдите в ***Computer Configuration*** >> ***Policy*** >> ***Administrative Templates*** >> ***Windows Components*** >> ***Windows Remote management*** >> ***WinRM Service***. Выберите пункт **Allow automatic configuration of listeners**, поставьте галку «**Enable**«, а в полях **Ipv4 filter** и **Ipv6 filter** поставьте знак « * «. Прикрепите политику к необходимому подразделению.

Обращаю Ваще внимание, что все действия необходимо выполнять под учеткой администратора. Помимо этого, обязательно должна быть запущена служба **Microsoft Firewall** на всех компьютерах.

Настройка:

[1]«После того, как собирающий и исходные компьютеры подготовлены, необходимо «оформить» подписку, указывающую какие события предоставлять.



Для этого откройте консоль **Event Viewer** и выберите пункт «**Subscriptions**«. В меню правой кнопки мыши «**Create Subscription**«.

В появившемся окне Вы должны будете указать имя подписки, выбрать журнал, в который будут поступать присланные события, а также настроить фильтр отбора событий по тем или иным критериям.

Но главное, вы должны выбрать способ сбора и имена компьютеров, предоставляющих события – либо целевой компьютер в нужное ему время опрашивает исходные компы на наличие необходимых событий, либо исходные компьютеры предоставляют сборщику события по расписанию. В случае, если вы добавляете компьютер, не принадлежакщий домену, необходимо добавить сертификат, на основании которого пудет проверена подлинность этого компьютера.

Также, если для доступа к компьютеру используется канал WiFi либо медленное ADSL соединение, в разделе «Дополнительно» можно выбрать вариант уменьшенной пропускной способности сети.

После завершения настройки Вы сможете мониторить события всех ваших серверов с одного компьютера. В дальнейшем можно настроить при поступлении события выполнение различных действий, которые могут быть выражены в отправке сообщения по электронной почте, отображении локального сообщения или запуске программы или скрипта.

Удачи!

P.S. Вышел мой вебкаст на эту тему на Techdays – «Настройка централизованой системы сбора событий Windows Eventing Collector» [2]

Похожие статьи

- Настраиваем защиту против спама в Exchange 2007 [3]
- Расширение функциональности консоли управления пользователями и компьютерами домена (ADUC) [4]
- Создание сертификата для Exchange 2007 [5]

Article printed from Kvazar`s Blog: **http://mcp.su**

URL to article: **http://mcp.su/2009/02/event-collector-in-windows-server-2008/**

URLs in this post:

[1] Image: **http://mcp.su/wp-content/uploads/2009/02/2009-02-18_145122.jpg**
[2] «Настройка централизованой системы сбора событий Windows Eventing Collector»: **http://www.techdays.ru/videos/1292.html**
[3] Настраиваем защиту против спама в Exchange 2007: **http://mcp.su/2009/07/exchange-2007-antispam-configuring/**
[4] Расширение функциональности консоли управления пользователями и компьютерами домена (ADUC): **http://mcp.su/2010/02/aduc-extend/**

[5] Создание сертификата для Exchange 2007: **http://mcp.su/2009/09/exchange-2007-newcert/**