Setting up a Source Initiated Subscription

Source-initiated subscriptions allow you to define a subscription on an event collector computer without defining the event source computers, and then multiple remote event source computers can be set up (using a group policy setting) to forward events to the event collector computer. This differs from a collector initiated subscription because in the collector initiated subscription model, the event collector must define all the event sources in the event subscription.

When setting up a source-initiated subscription, consider whether the event source computers are in the same domain as the event collector computer. The following sections describe the steps to follow when the event sources are in the same domain or not in the same domain as the event collector computer.

Note Any computer in a domain, local or remote, can be an event collector. However, when choosing an event collector, it is important to select a machine that is topologically close to where the majority of the events will be generated. Sending events to a machine at a distant network location on a WAN can reduce overall performance and efficiency in event collection.

Setting up a source-initiated subscription where the event sources are in the same domain as the event collector computer

Both the event source computers and the event collector computer must be configured to set up a source initiated subscription.

Note These instructions assume that you have administrator access to the Windows Server domain controller serving the domain in which the remote computer or computers will be configured to collect events.

Configuring the event source computer

1. Run the following command from an elevated privilege command prompt on the Windows Server domain controller to configure Windows Remote Management:

   winrm qc -q

2. Start group policy by running the following command:

   %SYSTEMROOT%\System32\gpedit.msc

3. Under the **Computer Configuration** node, expand the **Administrative Templates** node, then expand the **Windows Components** node, then select the **Event Forwarding** node.
4. Right-click the **SubscriptionManager** setting, and select **Properties**. Enable the **SubscriptionManager** setting, and click the **Show** button to add a server address to the setting. Add at least one setting that specifies the event collector computer. The **SubscriptionManager Properties** window contains an **Explain** tab that describes the syntax for the setting.
5. After the **SubscriptionManager** setting has been added, run the following command to ensure the policy is applied:

   gpupdate /force

Configuring the event collector computer

1. Run the following command from an elevated privilege command prompt on the Windows Server domain controller to configure Windows Remote Management:

   winrm qc -q

2. Run the following command to configure the Event Collector service:

   wecutil qc /q

3. Create a source initiated subscription. This can either be done programmatically, by using the Event Viewer, or by using **Wecutil.exe**. For more information about how to create the subscription programmatically, see the code example in Creating a Source Initiated Subscription. If you use Wecutil.exe, you must create an event subscription XML file and use the following command:

   wecutil cs *configurationFile.xml*

   The following XML is an example of the contents of a subscription configuration file that creates a source-initiated subscription to forward events from the Application event log of a remote computer to the ForwardedEvents log on the event collector computer.

XML

```
<Subscription xmlns="http://schemas.microsoft.com/2006/03/windows/events/subscription">
    <SubscriptionId>SampleSISubscription</SubscriptionId>
    <SubscriptionType>SourceInitiated</SubscriptionType>
    <Description>Source Initiated Subscription Sample</Description>
    <Enabled>true</Enabled>
    <Uri>http://schemas.microsoft.com/wbem/wsman/1/windows/EventLog</Uri>

    <!-- Use Normal (default), Custom, MinLatency, MinBandwidth -->
    <ConfigurationMode>Custom</ConfigurationMode>

    <Delivery Mode="Push">
        <Batching>
            <MaxItems>1</MaxItems>
            <MaxLatencyTime>1000</MaxLatencyTime>
        </Batching>
        <PushSettings>
            <Heartbeat Interval="60000"/>
        </PushSettings>
    </Delivery>

    <Expires>2018-01-01T00:00:00.000Z</Expires>

    <Query>
        <![CDATA[
            <QueryList>
                <Query Path="Application">
                    <Select>Event[System/EventID='999']</Select>
                </Query>
            </QueryList>
        ]]>
    </Query>

    <ReadExistingEvents>true</ReadExistingEvents>
    <TransportName>http</TransportName>
    <ContentFormat>RenderedText</ContentFormat>
    <Locale Language="en-US"/>
    <LogFile>ForwardedEvents</LogFile>
    <AllowedSourceNonDomainComputers></AllowedSourceNonDomainComputers>
```

```
    <AllowedSourceDomainComputers>O:NSG:NSD:(A;;GA;;;DC)(A;;GA;;;NS)
</AllowedSourceDomainComputers>
</Subscription>
```

Note When creating a source initiated subscription, if AllowedSourceDomainComputers, AllowedSourceNonDomainComputers/IssuerCAList, AllowedSubjectList, and DeniedSubjectList are all empty, then "O:NSG:NSD:(A;;GA;;;DC)(A;;GA;;;NS)" will be used as the default security descriptor for AllowedSourceDomainComputers. The default descriptor grants members of the Domain Computers domain group, as well as the local Network Service group (for the local forwarder), the ability to raise events for this subscription.

To validate that the subscription works correctly

1. On the event collector computer complete the following steps:
    a. Run the following command from an elevated privilege command prompt on the Windows Server domain controller to get the runtime status of the subscription:

       wecutil gr <*subscriptionID*>

    b. Verify that the event source has connected. You might need to wait until the refresh interval specified in the policy is over after you create the subscription for the event source to be connected.
    c. Run the following command to get the subscription information:

       wecutil gs <*subscriptionID*>

    d. Get the DeliveryMaxItems value from the subscription information.
2. On the event source computer, raise the events that match the query from the event subscription. The DeliveryMaxItems number of events must be raised for the events to be forwarded.
3. On the event collector computer, validate that the events have been forwarded to the ForwardedEvents log or to the log specified in the subscription.

Setting up a source initiated subscription where the event sources are not in the same domain as the event collector computer

Note These instructions assume that you have administrator access to a Windows Server domain controller. In this case, since the remote event collector computer or computer(s) are not in the domain served by the domain controller, it is essential to start an individual client by setting Windows Remote Management to "automatic" using Services (services.msc). Alternatively, you can run "winrm quickconfig" on each remote client.

The following prerequisites must be met before the subscription is created.

1. On the event collector computer, run the following commands from an elevated privilege command prompt to configure Windows Remote Management and the Event Collector service:

   winrm qc -q

   wecutil qc /q

2. The collector computer should have a server authentication certificate (certificate with a server authentication purpose) in a local computer certificate store.
3. On the event source computer, run the following command to configure Windows Remote Management:

   winrm qc -q

4. The source machine should have a client authentication certificate (certificate with a client authentication purpose) in a local computer certificate store .
5. Port 443 is opened on the event collector computer. To open this port, run the command:

   netsh firewall add portopening TCP 443 "Winrm HTTPS Remote Management"

To set up the subscription

1. Configure the event collector computer by completing the following steps.

   a. Set the certificate authentication with the following command.

      winrm set winrm/config/service/auth @{Certificate="true"}

   b. A WinRM HTTPS listener with the server authentication certificate thumb print should exist on the event collector computer. This can be verified with the following command:

      winrm e winrm/config/listener

      If you do not see the HTTPS listener, or if the HTTPS listener's thumb print is not same as the thumb print of the server authentication certificate on collector computer, then you can delete that listener and create a new one with the correct thumb print.

      To delete the https listener, use the following command:

      winrm delete winrm/config/Listener?Address=*+Transport=HTTPS

      To create a new listener, use the following command:

      winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<*FQDN of the collector*>**";CertificateThumbprint="**<*Thumb print of the server authentication certificate*>**"}**

2. Configure the event source computer by completing the following steps.

   a. Give NetworkService access to the private key file of the client authentication certificate. You can get the winhttpcertcfg.exe tool from this location: http://go.microsoft.com/fwlink/p/?linkid=100966

      i. Check that NetworkService has access to the private key file of the client authentication certificate by running the following command:

         winhttpcertcfg -l -c LOCAL_MACHINE\my -s <*subject name of the certificate*>

      ii. If NetworkService does not have access, then execute the following command to grant access:

         winhttpcertcfg -g -c LOCAL_MACHINE\my -s <subject of the certificate> -a NetworkService

   b. Set the event forwarding group policy setting by following these steps:

      i. Start group policy by running the following command:

         %SYSTEMROOT%\System32\gpedit.msc

      ii. Under the Computer Configuration node, expand the Administrative Templates node, then expand the Windows Components node, then select the Event Forwarding node.

iii. Right-click the SubscriptionManager setting, and select Properties. Enable the SubscriptionManager setting, and click the Show button to add a server address to the setting. Add at least one setting that specifies the event collector computer. The SubscriptionManager Properties window contains an Explain tab that describes the syntax for the setting. Use the following text for the setting:

Server=HTTPS://*<FQDN of the collector>***/wsman/SubscriptionManager/WEC,Refresh=***<Refresh interval in seconds>***,IssuerCA=***<Thumb print of the client authentication certificate>*

iv. After the SubscriptionManager setting has been added, run the following command to ensure the policy is applied:

gpupdate /force

c. Export the client authentication certificate to a .pfx file using the following command and copy the file to a share which can be accessed by the collector machine.

certutil -p *<Password>* **-exportPFX** *<Certificate ID ><pfx file name>*

Note The certificate ID is the certificate or CRL match token. This can be a serial number, an SHA-1 certificate, CRL, CTL or public key hash, a numeric cert index (0, 1, and so on), a numeric CRL index (.0, .1, and so on), a numeric CTL index (..0, ..1, and so on), a public key, signature or extension ObjectId, a certificate subject Common Name, an e-mail address, UPN or DNS name, a key container name or CSP name, or a CRL issuer Common Name. Many of these can result in multiple matches.

3. Configure the event collector computer by completing the following steps.

a. Import the .pfx file containing client authentication certificate to the Trusted Root Certificates node using following command:

certutil -p *<Password>* **-importPFX** *<pfx file name>*

b. Create a source initiated subscription.

You can use the Event Viewer application to create the subscription.

i. Open Event Viewer and create a new subscription.
ii. Enter the subscription name, description, and event query.
iii. Add the event source computer using the Add non-domain computers button.
iv. Click the Add certificates button. In the certificate list, select the client authentication certificate that was exported from the source computer and imported to the collector computer.
v. Click the Advanced button and select HTTPS.
vi. Complete the subscription by clicking on the OK button.

c. Check the subscription status (it should be Active) using the following command:

wecutil gr *<subscriptionID>*

If the source computer does not appear in the command output, you can wait until the refresh interval specified in the policy is over, and then check the status again to make sure it is active.