boldonjames
by HelpSystems

Event Forwarding Guide
Classifier Reporting

May 2021




Copyright Terms and Conditions

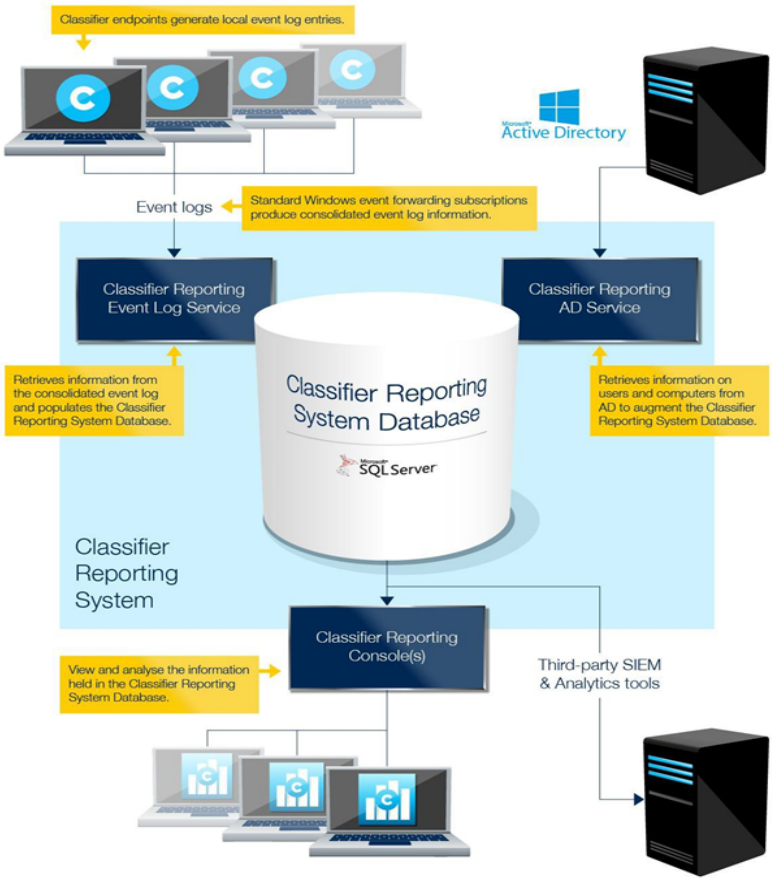
202105260223

Table of Contents

About Event Forwarding

This document explains how to configure event forwarding subscriptions to collect events from Classifier endpoints and store the events into a consolidated event log.

The Reporting Services Components diagram below shows the structural relationship between the components supplied and other system components.



Classifier Event Forwarding

Event forwarding allows you to collect events from client computers running Classifier to an Event Log on a central server called the Consolidated Event Log server. Event forwarding can be configured to be either collector initiated (pull) or source initiated (push).

> **NOTE:** These procedures use features of Microsoft Windows operating systems including Windows Remote Management (WinRM). These steps should be carried out by a Domain Administrator and apply to WinRM version 2.0. This section is just a brief introduction to event forwarding and contains a minimum set of steps. It does not explore situations such as forwarding events from computers outside of a domain. For more information on event forwarding, see Configure Computers to Forward and Collect Events.

Collector initiated Event Forwarding

To configure collector initiated event forwarding, steps have to be taken on each Classifier client computer and the Consolidated Event Log server.

Classifier Clients

On each of the Classifier client computers from which you wish to collect events, the Windows Remote Management (WinRM) service has to be started and the firewall has to be configured to allow events to be forwarded, this is done by completing the following step.

1. In a Windows Command console, type: winrm quickconfig and answer “y” (yes) when prompted.

Consolidate Event Log Servers

On the Consolidated Event Log server, define a subscription to collect the events from the Classifier client computers.

1. Start Event Viewer, select the Subscriptions node, and choose “Create Subscription…” from the context menu. The Subscription Properties dialog will be displayed.

   > **NOTE:** If this is the first Subscription to be created you will be prompted that the Windows Event Collector Service must be running. Press Yes and the Services program will be displayed allowing you to start the service.

2. Provide a name for the subscription, for example “Classifier Events Subscription".
3. Select the Boldon James/Classifier event channel from the Destination log: drop-down list. The Boldon James/Classifier event channel is created if you install the Event Log Service. Alternatively if you wish to collect events to a server without installing the service you can create the channel by running the Event Channel Wizard.
4. Select Collector Initiated.
5. Click Select Computers and identify the computers that you wish to collect events from.

6. Click Select Events.

   The Query Filter dialog is displayed.
7. Select all Event level check boxes.
8. Select By log and then select Boldon James/Classifier Event Channel in the Event Logs dropdown.
9. Press OK to return to the Subscription Properties dialog.
10. Set the User Account to the Domain Administrator e.g. MyDomain\Administrator by selecting Specific User and then pressing the User and Password... button.
11. Set Protocol to HTTP.
12. Press OK to return to the Subscription Properties dialog.
13. Press OK to complete the subscription.

    The events collected by this subscription must be collected in Event format, not RenderedText format which is not usable by the Classifier Reporting database.

To configure collecting in Event format run a Windows Command console and type wecutil ss "Classifier Events Subscription" /CF:Events

> **NOTE:** “Classifier Events Subscription” is the name of the subscription created in step 2 above.

Source initiated Event Forwarding using Group Policy Objects

Source initiated event forwarding uses Active Directory Groups and Group Policy Objects (GPO) to configure Classifier client computers to forward events to the Consolidated Event Log server.

1. Create an Active Directory group containing all the Classifier client computers that are to forward events.
2. Define a GPO and apply it to the group created above.
3. Define a Classifier events subscription on the system that is to receive the forwarded events and link it with the group.
4. Re-start all the Classifier client computers in the group so that the GPO settings can take effect.

Create a Classifier Client Group

The example assumes a Windows 2008 server environment. Specific commands, options and actions may vary with the environment, and site group policy and security standards must of course be considered.

The first step is to create an Active Directory group containing all the Classifier client computers that are to forward events.

1. Run Active Directory Users and Computers.
2. Right-click Computers, and choose New > Group.

3. Name the group something significant e.g. ClassifierClients, set the Group scope to Domain local and the Group type to Security.
4. Press OK to create the group.
5. Right-click the newly created group in the list of Computers in the right-hand pane of Active Directory Users and Computers, and select Properties.
6. Select the Members tab and click Add.
7. Click Object Types and select Computers.
8. Enter the name of all the Classifier client computers you want to add to the group and press OK twice.

> **NOTE:** Do not add the name of the Consolidated Event Log Server into the group.

Define a Group Policy Object for the Classifier Client Group

Create a Group Policy Object (GPO), apply it to the group created above (section Create a Classifier Client Group), and set policies on the GPO to collect and forward events.

Create a GPO and apply it to the group

1. Using Group Policy Management, expand the Group Policy Management->Forest->Domains->My Domain node.
2. Select the My Domain node, right-click Create a GPO in this domain, and select Link it here.
3. Enter a name for the GPO, (e.g. ClassifierClientsgpo) and click OK. This will create a new GPO that is shown in the Group Policy Management -> Forest ->Domains->My Domain->Group Policy Objects node.
4. Select ClassifierClientsgpo and details of the ClassifierClientsgpo will be displayed in the right-hand pane.
5. Set Enforced to Yes. Link Enabled should already be set to Yes.
6. Click Add and add the ClassifierClients group created above. This applies the GPO to the group.

Set policies on the GPO

Configure the GPO to enable event forwarding.

Enable the WinRM service

1. Using Group Policy Management, right-click the ClassifierClientsgpo object, and select Edit.
2. Select Computer Configuration >Policies >Windows Settings >Security Settings >System Services.
3. Right-click Windows Remote Management (WS-Management).
4. Select Properties. The Windows Remote Management (WS- Management) Properties dialog will be displayed.
5. Check Define this policy settings and set service startup mode to Automatic. Click OK.

6. Select the node Computer Configuration->Policies->Administrative Templates->Windows Components->Windows Remote Management (WinRM)->WinRM Service.
7. Select Allow automatic configuration of listeners, and select Edit the policy setting. The Allow automatic configuration of listeners dialog is displayed. (The policy setting for 2012 is Allow remote server management through WinRM.)
8. Select Enabled and set both the IPV4 and IPV6 filter value to *.
9. Click OK.

Enable Event Forwarding

1. Using Group Policy Management, select the policy object.
2. Select the node Computer Configuration->Policies-> Administrative Templates ->Windows Components->Event Forwarding.
3. Select Configure the server address, refresh interval, and issuer certificate authority of a target, and Edit the policy setting. The Server Configuration dialog is displayed.

   (The policy setting for 2012 is Configure target subscription manager.)
4. Select Enabled.
5. Click Show.

   The SubscriptionManagers dialog is displayed with a Server entry should be added in the first row.
6. Place the mouse into the row and enter the following:
   Server=http://MyServer:5985/wsman/SubscriptionManager/WEC

   > **NOTE:** Note: You must enter all the text including “Server=” where MyServer is either a full-qualified domain name or a hostname for the server which is to collect the forwarded events, and 5985 is the port that WinRM communicates over.

7. Press OK to close the SubscriptionManagers dialog.
8. Press OK to close the Server Configuration dialog.

Set WinRM permissions

The WinRM service runs under the Network Service account. So that the WinRM service can read event logs the Network Service account has to be added to the Event Log Readers Group. Doing this by GPO is a two-stage process. Firstly, the Event Log Readers group has to be added to the Restricted Groups in the GPO and then the Network Service account has to be added to the Event Readers group.

1. Using Group Policy Management, right-click select the policy object, and select Edit.
2. Select Computer Configuration->Policies-> Windows Settings->Security Settings.
3. Right-click Restricted Groups, and select Add Group.
3. Click Add and then click Browse. Add the Event Log Readers group by using the Select Groups dialog.
4. Click OK (three times) and the Event Log Readers group is now displayed in the right-hand side of the Group Policy Management Editor.
5. Right-click Event Log Readers, and select Properties.

   The Event Log Readers Properties dialog will be displayed.

6. Click Add (at the top of the dialog) and then click Browse.
7. Add the Network Service group by using the Select Users, Service Accounts, or Groups dialog.
8. Click OK (three times) and the Event Log Readers group, showing Network Service as a member will be displayed in the right-hand pane of the Group Policy Management Editor.

Define a Classifier Events Subscription

A subscription should be defined to collect events from Classifier client computers on the Consolidated Event Log server (this server should also host the Classifier Reporting Event Log service).

1. Start Event Viewer and right-click the Subscriptions node.
2. Click Create Subscription. The Subscription Properties dialog will be displayed.

   > **NOTE:** Note: If this is the first Subscription to be created you will be prompted that the Windows Event Collector Service must be running. Press Yes and Services will be displayed allowing you to start the service.

3. Provide a name for the subscription, for example “Classifier Events Subscription”.
4. Select the Boldon James/Classifier event channel from the Destination log: drop-down list. The Boldon James/Classifier event channel is created if you install the Event Log Service. Alternatively, if you wish to collect events to a server without installing the service you can create the channel by running the Event Channel Wizard.
5. Select Source computer initiated.
6. Click Select Computer Groups.

   The Computer Groups dialog is displayed
7. Click Add Domain Computers and select the computer group (e.g. ClassifierClients).
8. Click OK (twice) and return to the Subscription Properties dialog.
9. Click Select Events… and the Query Filter dialog is displayed
10. Select all the Event level check boxes.
11. Select By log and then select Boldon James/Classifier event channel in the Event Logs dropdown.
12. Click OK to return to the Subscription Properties dialog.
13. Click Advanced and the Advanced Subscription Settings dialog is displayed

    (Normal – 15 minutes, Minimize Bandwidth – 6 hours and Minimize Latency - 30 seconds)
14. Set Protocol to HTTP.
15. Press OK to return to the Subscription Properties dialog.
16. Press OK to complete the subscription.
17. Ensure that WinRM is operating and that the firewall allows events to be forwarded. From a Command prompt, run the following Windows command: winRM qc.

The events collected by this subscription must be collected in Event format, not RenderedText format which is not usable by the Classifier Reporting database.

To configure collecting in Event format run a Windows Command console and type: wecutil ss "Classifier Events Subscription" /CF:Events

NOTE: "Classifier Events Subscription" is the name of the subscription created above.

Restart Client Computers

You must restart all the Classifier client computers so that the changes to GPO can now take effect and configure the computers to start forwarding events.

When a client computer initiates event forwarding, an entry (Event ID = 111) appears in the Collector Event Viewer. Forwarded events will appear depending upon Latency set in Advanced Subscriptions Settings and Classifier events being generated on that computer.

You can check for Success and Errors (for example, incorrect configuration) for submitting computers via Event Viewer > Applications and Services Logs > Microsoft > Windows > Eventlog- ForwardingPlugin > Operational.

Forwarding Management Agent Events

If you deploy the Classifier Management Agent (MA) in your organisation, you may want to store the events it generates in the Classifier Reporting Database. MA events can be forwarded to the Consolidated Event Log server via the same subscriptions that forward Classifier events, or using separate subscriptions.

To collect MA events:

1. Open the Event Viewer.
2. Select the Boldon James Auditing/Classifier/Management Agent/Admin event which is created if you install the Event Log Service.

   Alternatively, if you wish to collect MA events to a server without installing the service, you can create the event channel on the collection server by running the Event Channel Wizard, see section Event Channel Wizard.

NOTE: The Boldon James Auditing/Classifier/Management Agent/Admin event channel is created by the MA on the Windows clients and is the location that the MA writes its events to. The MA events are forwarded to the Boldon James/Classifier event channel on the event collection server. However, the Boldon James Auditing/Classifier/Management Agent/Admin event channel has to be defined on the Event Collection Server so that a subscription can be defined to collect the events from the windows clients.

NOTE:
Version 1.0 of the Classifier Reporting Services created an incorrect name for the Boldon James Auditing/Classifier/Management Agent/Admin event channel. If you have created this event channel, remove it before you uninstall Version 1.0.

1. Run a command prompt with Administrator privileges and go to the C:\Program Files (x86)\Boldon James\Classifier Reporting Services directory.
2. Run the command: wevtutil um bjManAgentEvents.xml.

Filtering Classifier Events

If you configure event forwarding correctly, all events generated by Classifier applications will be collected. You can filter the events forwarded so that only events that you are interested in are transferred across the network and stored in the Classifier Events Database. For example, you may only want reports on email users and not document users or you may only want to produce reports showing Classifier check rules that produced warnings or preventions.

Event Subscription Filter dialog

The Classifier applications from which you wish to collect events can be configured by selecting items from the Event Source drop down on the Event Subscription Filter.

The Event Ids can also be selected. For example, if you only want to display the Email Sent by Classification and Documents Saved by Classification reports then you would only need to forward Events with Ids 1101 and 3000. This can be done by entering the Event Id. More information about Classifier event Ids is provided by the Classifier Administration Guide.

Defining an Event Subscription filter using XML

Event subscription filters are defined using XML. When a filter is defined on the Query Filter dialog, the XML definition of the filter can be viewed by selecting the XML tab.

You can define an Event Subscription filter by directly adding a XML definition.

1. In the Query Filter, click the Edit Query manually check box.

> **NOTE:** You will be warned that if you do enter a XML definition that it is not possible to use the Event Subscription dialog for this subscription.

Several pre-defined XML filters that can be copied into the XML definition field as shown above, are provided with this release. These include the following.

ApplicationEvents.xml:	Collect Classifier events from Excel, Outlook, PowerPoint, Project, Visio and Word.
ApplicationAndErrorEvents.xml	Collect only error and warning Classifier events from Excel, Outlook, PowerPoint, Project, Visio and Word.
DocumentEvents.xml	Collect Classifier events from Excel, PowerPoint and Word.
DocumentAndErrorEvents.xml	Collect only error and warning Classifier events from Excel, PowerPoint and Word.
EmailEvents.xml	Collect Classifier events from Outlook, OWA and Notes.

ApplicationEvents.xml:	Collect Classifier events from Excel, Outlook, PowerPoint, Project, Visio and Word.
EmailAndErrorEvents.xml	Collect only error and warning Classifier events from Outlook, OWA and Notes.
ManagementAgentEvents.xml	Collect only Management Agent Events.

Event Forwarding Troubleshooting

Issue	Note
Basic checks	It can take over 15 minutes for events to be forwarded in standard operation. You may want to set “Minimize Latency” from the Advanced dialog of the Subscription in evaluation stages to ensure events are forwarded more frequently (every 30 seconds).
Basic checks	Previously generated events on the forwarding machines are not forwarded when a subscription is set up in standard mode. You must generate new Classifier events on the forwarding machines (where events are forwarded to the Collecting machine) after the subscription has been set up.
Basic checks	Ensure that there is network connectivity between the collecting machine (where the Event Log subscription is setup; typically where the Classifier Reporting Event Log service runs) and the forwarding machine using standard tools such as ping and nslookup for DNS.
Basic checks	On the collecting machine, ensure that the subscription is Enabled by checking the status in the subscriptions section of the Event Log. Basic checks.
Basic checks	On the collecting machine, ensure that the Runtime Status of the subscription indicates that the forwarding computer is “Active”.
The collecting machine subscription “Runtime status” indicates “The client cannot connect to the destination…”	This suggests that the Windows Remote Management service is not running, or is not accessible, on the forwarding machine.

Issue	Note
The collecting machine subscription “Runtime status” indicates “Access is denied”	This indicates that the account used to run the subscription does not have permission to access the forwarding machine event logs. Check the account used to run the subscription (from the Advanced button on the subscription properties). You will need to give this account permission to the forwarding computer event log.
Basic checks	On the forwarding machine, check the Applications and Services Logs/Microsoft/Windows/Eventlog- ForwardingPlugin/Operational event log to see if the subscription has been successfully set up. If you have no event in this event log it is likely that winrm is not running on the forwarding machine, or that you have firewall issues. An event with id 100 indicates that the subscription has been set up. The event detail will confirm the name of the subscription that has been set up. An event of id 102 indicates an error. Typical problems include: • Incorrect channel name in subscription • Authentication issues

Issue	Note
Checking collecting machine configurations	Verify that the event query is valid: 1. View the subscription properties, and click Select Events. 2. On the XML tab, copy the contents of the query 3. Open a second instance of Event Viewer. 4. Right-click the Event Viewer, and then select Connect to Another Computer... Enter the hostname of the forwarding computer in the Another computer text box. 5. Right-click Custom Views, and select Create Custom View. 6. Select the XML tab. Click the 'Edit query manually' check box, and click Yes when prompted. 7. Click the query box and paste the previously copied query. Click OK. The new custom view appears and shows the matching events. If there are no events shown the query is incorrect. If events are shown, then the forwarding mechanism is failing. If there are no events shown in the above step, note that the Path element in the query should be "Classifier" for Classifier client events, and "Boldon James Auditing-Classifier-Management Agent/Admin". Be especially careful with the placement of the dashes, spaces and the slash. If there are events shown but they are not being forwarded, check that the Windows Remote Management service is running on the forwarding machine. On the forwarding machine, type in a console window: winrm enumerate winrm/config/Listener If this returns with no output, you may have not set up the service. On the forwarding machine, execute: winrm quickconfig
Checking forwarding machine configurations	From the collecting machine, check that you can connect to the WinRM service on the forwarding machine. In a console window type: winrm id -remote:<forwardingmachine>.<yourdomain>.<com> This should return with an IdentifyResponse indicating ProtocolVersion etc. If the return indicates "…client cannot connect to the destination…" then it is possible that there are firewall issues
Check collecting machine configuration	winrm id -remote:<forwardingmachine>.<yourdomain>.<com>> This should return with an IdentifyResponse indicating ProtocolVersion etc. If the return indicates "…client cannot connect to the destination…" then you may have firewall issues.

Issue	Note
winrm to forwarding machine cannot connect	On the forwarding computer, ensure that HTTP-In (typically port 80) or HTTPS (typically port 443) exceptions are available in your chosen firewall configuration. Running winrm quickconfig will set up the appropriate firewall exceptions for MS firewalls. On the collecting machine, ensure that HTTP-In for Windows Remote Management (typically port 5985) exception is available in your chosen firewall configuration.
Events are being forwarded but not processed	If you are getting events forwarded but they are not being processed by the Classifier Reporting Event Log service, ensure that the subscription is requesting events in Events format. On the collecting machine, in a console window, execute: wecutil gs “Your subscription name” [NB: run wecutil es to list your subscriptions] Check that the ContentFormat is listed as “Events” If this is not the case, execute wecutil ss "Your subscription name" /CF:Events This is only effective for new events forwarded to the collector.
I’m expecting to see more events in my reports	If you have events in the Classifier Reporting database but you expected more events, have you set up a filter on the subscription for particular events? Check the subscription Select Events dialog and review the filter.

Event Channel Wizard

The event channels, needed to collect Classifier and MA events, are created if the Classifier Event Log Service is installed. If you wish to collect events on a server where you have not installed the Service, the Event Channel Wizard can be used to create the two event channels instead. The Event Channel Wizard can be used to delete the event channels as well.

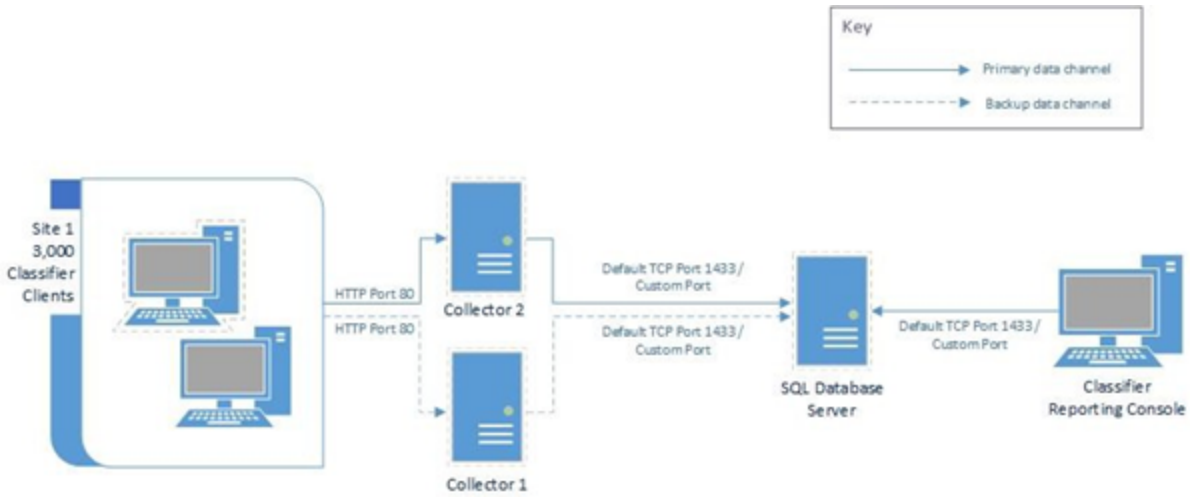
To use the Event Channel Wizard:

1. Run the ChannelWizard.exe located at C:\Program Files (x86)\Boldon James\Classifier Reporting Services.
2. Select which channel you wish to create or remove, and click Apply.

> **NOTE:**
> The Classifier event channel will be automatically created on your system if you install the Event Log Channel Wizard even if you do not also install the Event Log Services.
> The event channels are not automatically deleted if you uninstall the Event Log Services, but you can delete the channels using the Event Channel Wizard.

Event Collection Resilience

We recommend your configuration have only one event log service writing events into the ClassifierEventsDB at any one time. This section explains how to configure an event collection environment that meets this recommendation but also provides failover resilience.



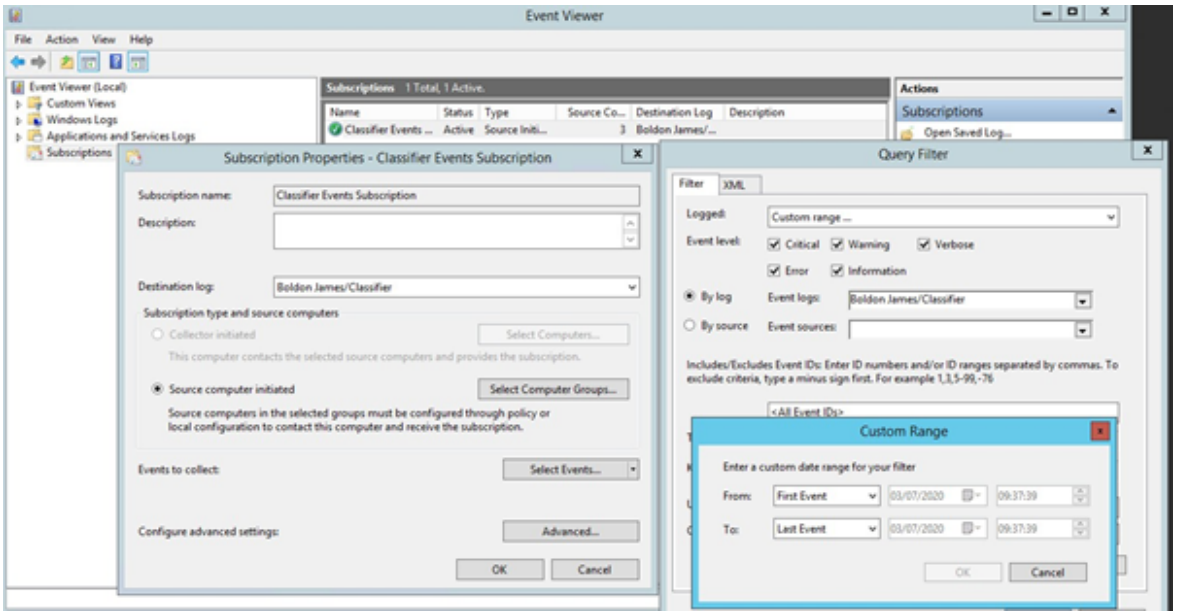
The diagram above shows an organization with 3000 Classifier clients, two event collection servers, and a single ClassifierEventsDB on a server running SQL Server.

Configure the event collecting environment

1. Install and configure the Classifier Reporting services on machines Collector 1 and Collector 2.
2. Define event collecting subscriptions on Collector 1 and Collector 2 and configure the event log services on the two servers to both write events to the ClassifierEventsDB database.
3. Disable the subscription on Collector 2 and shut down the server if you want.

If Collector 1 fails

1. Close down Collector 1.
2. Start Collector 2.
3. Configure the Classifier events subscription parameters on Collector 2 to start collecting events from the time that Collector 1 failed. See the diagram below.



4. Enable the subscription on Collector 2.

When Collector 1 is ready to go back on line

1. Disable the subscription on Collector 2.
2. Wait for event log service to finish processing events.
3. Close down server Collector 2.
4. Start Collector 1 and immediately disable the subscription.
5. Configure the subscription on Collector 1 to start collecting events from the time Collector 2 was shut down.
6. Enable the subscription on Collector 1.