Cato Networks - Configuring Event Log Forwarding with Two Windows Servers

How to Configure Windows Event Forwarding for User Awareness

Cato Networks' User Awareness feature usually imports the audit log events directly from the Domain Controller (DC). These log events are shown in the Event Discovery window in the Cato Management Application. Some organizations prefer to forward these events from the DC (the forwarder) to another windows server (the collector) and configure the User Awareness to import the logs from that server.

The following diagram is a sample of Windows Event Forwarding (WEF) with 2 servers: one server is the DC that acts as the forwarder and the second server is the collector. The collector pulls the security events from the forwarder. The Cato PoP imports these events from the collector and shows them in the Cato Management Application.

This article explains how to configure WEF on Windows server.

Configuring Event Log Forwarding with Two Windows Servers

Prerequisites:

Two windows server (2016 or later) instances:

- Forwarder with active directory
- Collector

To configure the event log forwarding:

- Configure the Collector
- Configure the Forwarder

Configuring the Event Log Collector

This section describes how to configure the windows server instance as the collector. The collector is the server that pulls the event logs from the forwarder server (DC).

Enabling the Windows Remote Management (WinRM)

Windows Remote Management (WS-Management) is a Microsoft service that allow forwarding the events to the collector. This service is automatically running by default, if not, set the service configuration with status: running and startup type: automatically.

Enabling the PowerShell Remoting

Open the Windows PowerShell console and run the command: **Enable-PSRemoting**to enable the PowerShell Remote service. You can verify that the PSRemoting is enabled by running the command: **Invoke-Command -ComputerName**<COLLECTORHOSTNAME> **-ScriptBlock {1}**. If you don’t receive an error, then the service is running.

Starting the Subscription Collector Service

To start the subscription:

1. Open the Event Viewer and click on **Subscription.**
2. A popup window appears, Click **Yes** to confirm the service to run automatically.
3. Right Click select **Create Subscription.**
4. Add a Subscription name.
5. In the Destination log, select **ForwardedEvents.**
6. Under Subscription type and source computers, select **Collector initiated.**
7. Click Select Computers and enter the Forwarder hostname and click OK to apply. If you have multiple DCs, add them to the list.
8. Click on **Select Events** and verify that Event level: Information is selected.
9. Select By logs and choose the Security Events Logs.
10. To reduce many events, we recommend that you add the Event IDs that Cato uses for the User Awareness: 4768,4769,4770,4624,5145,5140,4625,4647,4608

The following screenshot shows a sample of a Subscription Properties window:

blobid1.png

Configuring the Forwarded Events Log File

To configure the forwarded events file to use the security events:

1. Open the Event Viewer and navigate to Windows Logs > **ForwardedEvents**
2. Right click on **ForwardedEvents** and click on Properties
3. Change the Log path to the %..\Security.evtx file and click **OK**

blobid5.png

Configuring the Forwarder (DC)

This section describes how to configure the DC as the forwarder.

Allowing Read Permissions to the Security Event Log

Open the Windows PowerShell console and run the command: **wevtutilgl security**. This command provides information about the Security event log. Copy the **channelAccess** string.

Configuring the Group Policy Management for the Forwarder

- Go to **Server Manger > Tools > Group Policy Management > Domains > Domain Controllers** and click on **Default Domain Controllers Policy**. Right Click and click Edit, when the Default Domain Controllers Policy window opens, navigate to *Computer Configuration → Policies → Administrative Templates → Windows Components → Event Forwarding → Configure target Subscription Manager and* Set the value for the target subscription manager: *Server=http://<FQDN of the collector>:5985/wsman/SubscriptionManager/WEC,Refresh=60*

The following screenshot shows an example of a Subscription Manager for the “MyCollector” server.

blobid3.jpg

2. Navigate to **Computer Configuration → Policies → Administrative Templates → Windows Components → Event Log Service → Security → Configure log access** select **Enabled** and paste the **channelAccess** string from the section above in the Log Access pane.

The following screenshot shows an example of log access configuration with the channelAccess value:

blobid4.png

Adding the Network Service into the Event Log Readers Group

Go to **Server Manger > Tools > Active Directory Users and Computers > <Domain name> Builtin**, Right click on **Event Log Readers** group and click Properties. when the window opens, go to Members tab and add the Network Service account and click OK.

Open the command line and run the command **gpupdate /force**to update the GPO. Changes to this group require a restart for WinRM to apply the changes.

Checking the Event Log Forwarding

When you complete the collector and the forwarder configuration, go to the Collector server and open the Event Viewer and navigate to **Windows Logs > Forwarded Events**. Make sure that you can see the events in this section.

Source: https://support.catonetworks.com/hc/en-us/articles/360013279817-How-to-Configure-Windows-Event-Forwarding-for-User-Awareness

If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.

Revision #4
Created 16 January 2025 08:52:57 by Richmond Abella
Updated 19 February 2025 05:25:44 by Richmond Abella