

# Centralizing Windows Logs

You can use the tools in this article to centralize your Windows event logs from multiple servers and desktops. This will considerably reduce the time that it will take you to deploy the Network Box SIEM+ and begin sending data to it.

## Windows Event Subscription

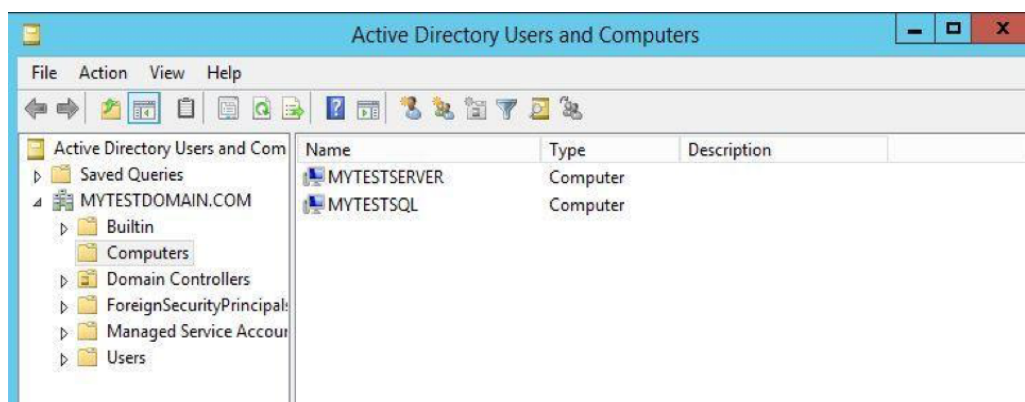
It is possible for a Windows server to forward its events to a **collector** server. In this scenario, the **collector** server becomes a central repository for Windows logs from other servers (called event **sources**) in the network. The stream of events from a source to a collector is called a **subscription**.

This procedure demonstrates how to set it up. These steps work on Windows Server 2008 R2, Windows Server 2012, and Windows Server 2019.

## Example System

We are using two Active Directory Domain-joined Windows Server 2012 systems. The domain name is [mytestdomain.com](http://mytestdomain.com) and both machines are registered with the domain.

**Source** server **MYTESTSQL** hosts a **SQL Server 2014** instance. **Collector** server **MYTESTSERVER** works as an **event log subscriber** to centralize all SQL Server-related logs from **MYTESTSQL**.



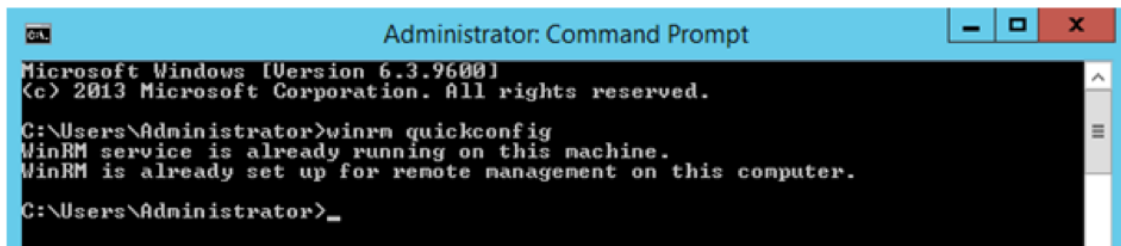
# Setup

## Enable the Windows Remote Management Service

**Windows Remote Management** (WinRM) is a protocol for exchanging information across systems in your infrastructure. You must enable it on each of your **source** computers to exchange log files.

1. Log into the **source** computer (MYTESTSQL) as a local or domain administrator.
2. Enable **Windows Remote Management Service** from a Command Prompt: `winrm quickconfig`

If it is already running, a message similar to this example is displayed



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>winrm quickconfig
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.

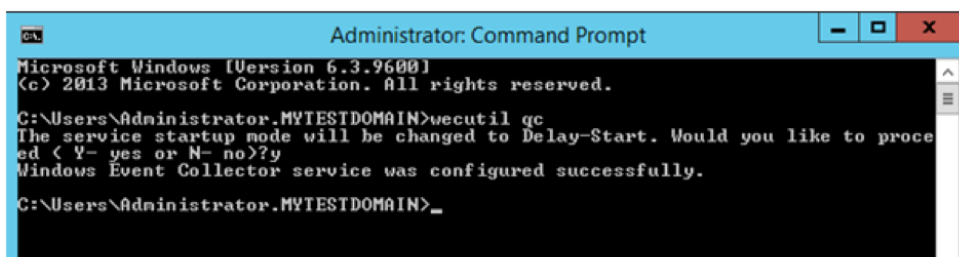
C:\Users\Administrator>_
```

## Configure the Windows Event Collector Service

You must enable the **Windows Event Collector Service** on your **collector** server to allow it to receive logs from your **sources**.

1. Log into the **collector** computer (MYTESTSERVER) as a local or domain administrator.
2. Configure the **Windows Event Collector Service** from a Command Prompt: `wecutil qc`

If prompted like the example, press `y`



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

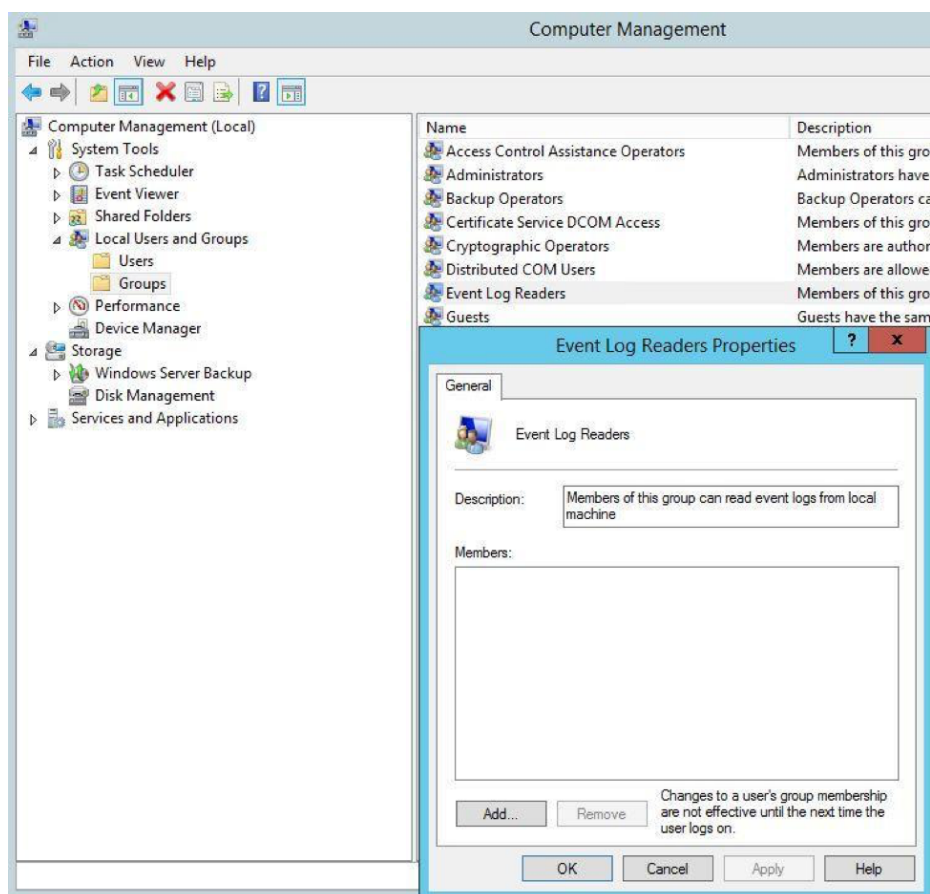
C:\Users\Administrator.MYTESTDOMAIN>wecutil qc
The service startup mode will be changed to Delay-Start. Would you like to proceed < Y- yes or N- no?y
Windows Event Collector service was configured successfully.

C:\Users\Administrator.MYTESTDOMAIN>_
```

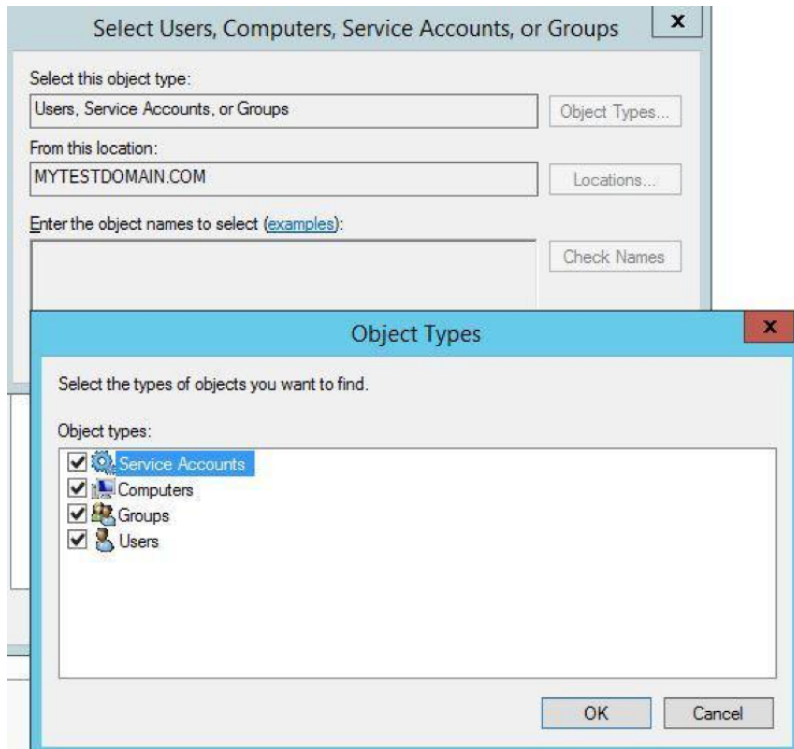
## Configure the Event Log Readers Group

By default, certain logs are restricted to administrators. This may cause problems when receiving logs from other systems. To avoid this, you can grant access to the **collector** computer by adding it to the **Event Log Readers** group.

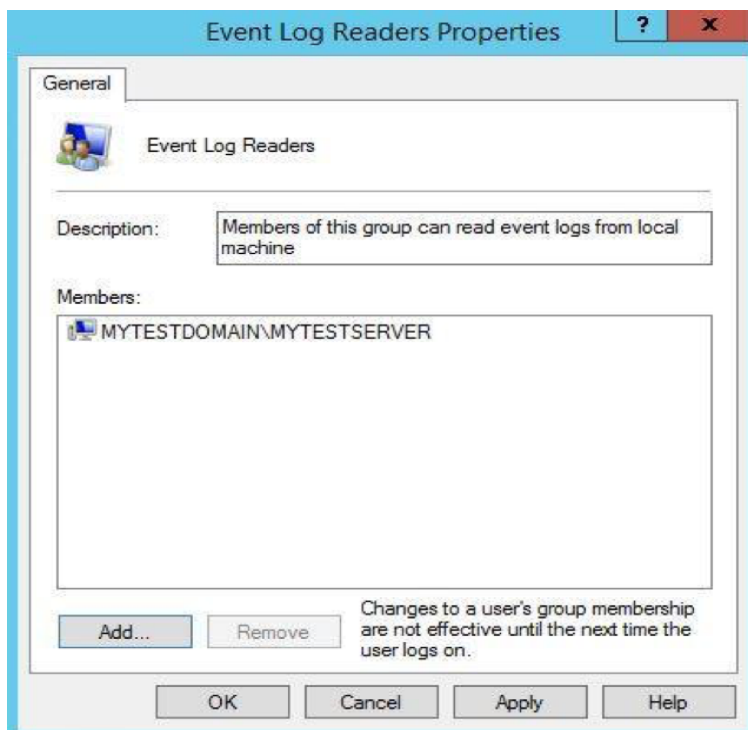
1. Go back to the **source** computer (MYTESTSQL).
2. Open **Server Manager**.
3. Open **Computer Management**.
4. Expand **Local Users and Groups** node from the Navigation pane and select **Groups**.
5. Double-click **Event Log Readers**.



6. Click **Add** to open the **Select Users, Computers, Service Accounts, or Groups** dialog.
7. Click **Object Types**.
8. Check **Computers** and click **OK**.

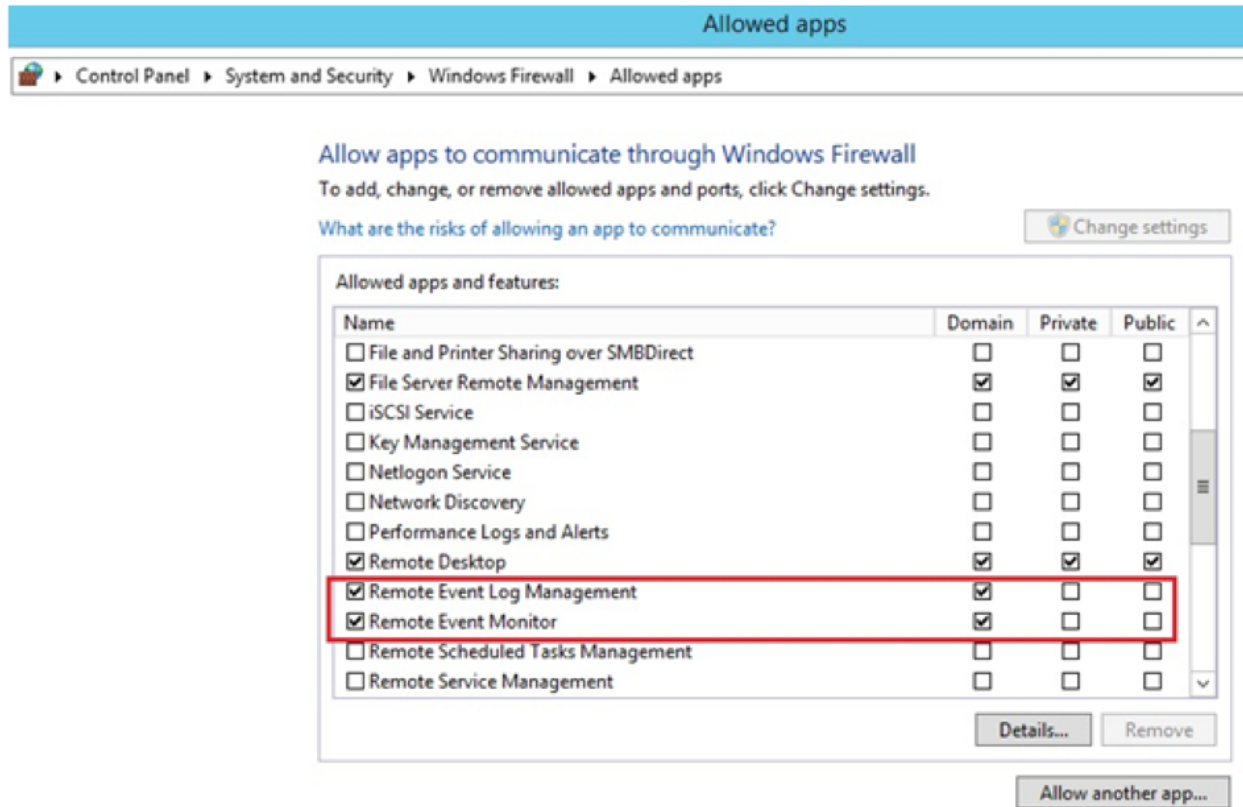


9. Enter **MYTESTSERVER** as the object name and click **Check Names**. If the computer account is found, it is confirmed with an underline.
10. Click **OK** twice to close the dialog boxes.



## Configure Windows Firewall

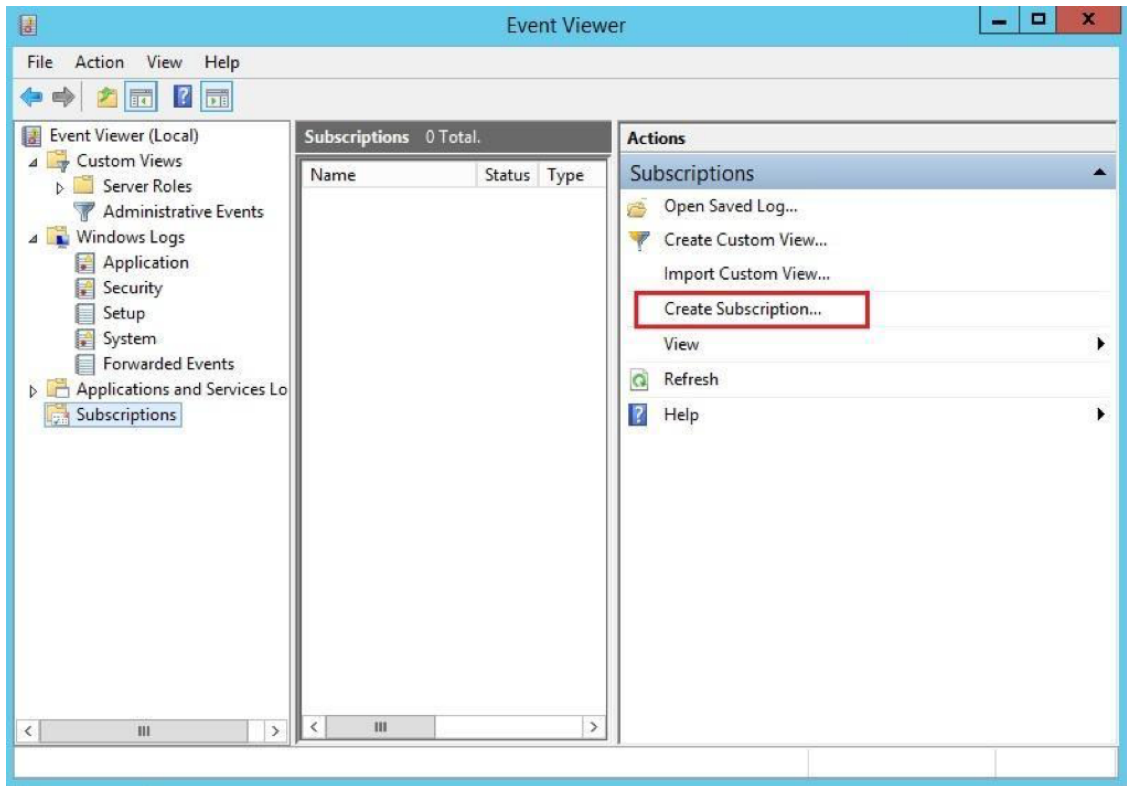
If the source computer is running Windows Firewall, ensure it allows **Remote Event Log Management** and **Remote Event Monitor** traffic.



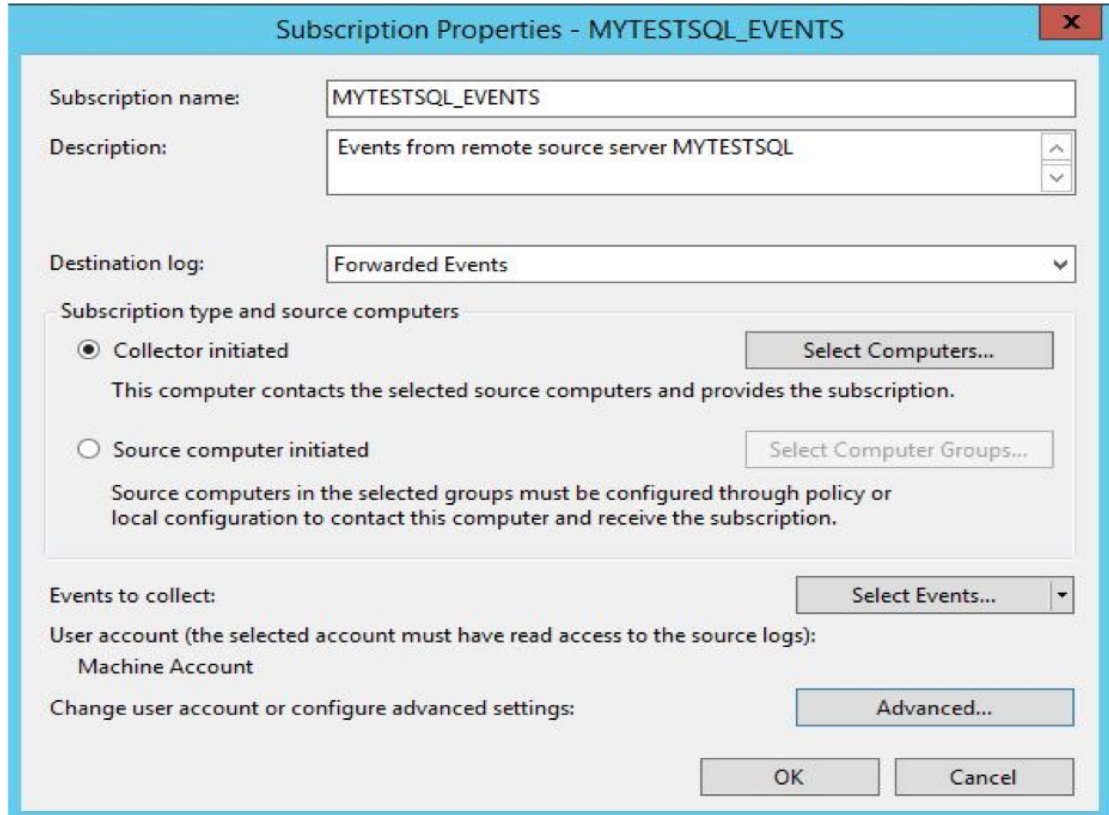
## Create a Subscription

Subscriptions define the relationship between a **collector** and a **source**. You can configure a **collector** to receive events from any number of **sources** (a source-initiated subscription), or specify a limited set of **sources** (a collector-initiated subscription). In this example, we create a **collector-initiated** subscription since we know which computer logs we want to receive.

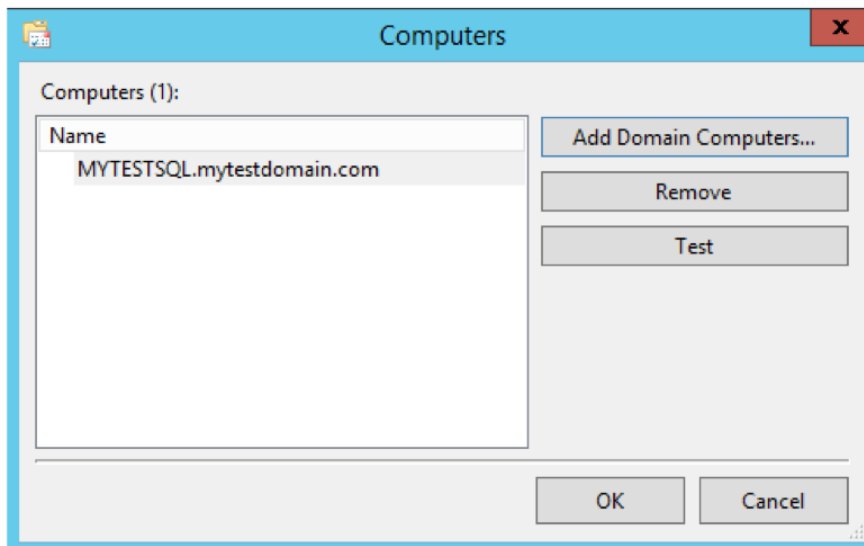
1. Start the Event Viewer application on the collector server **MYTESTSERVER**.
2. Select **Subscriptions** from the Navigation pane
3. Click **Create Subscription** in the Actions pane.



4. On the **Subscription Properties**, enter the following as shown in the example:  
Subscription name: **MYTESTSQL\_EVENTS**  
Description: **Events from remote source server MYTESTSQL**  
Destination log: **Forwarded Events**  
Select **Collector initiated** and click **Select Computers** to open the **Computers** dialog



5. Click **Add Domain Computers**.
6. Enter **MYTESTSQL** as the object name and click **Check Names**. If the computer is found, it is confirmed with an underline.
7. Click **OK**.



8. Click **OK** to return to the **Subscription Properties**.
9. Click **Select Events** to open the **Query Filter** and enter the following to set the remote server to forward all application events from the last 24 hours:  
Logged: **Last 24 hours**  
Check all **Event levels**  
Select **By log**  
Event logs: Select **Application** from the drop-down list

Query Filter

Filter XML

Logged: Last 24 hours

Event level:  Critical  Warning  Verbose  
 Error  Information

By log Event logs: Application

By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

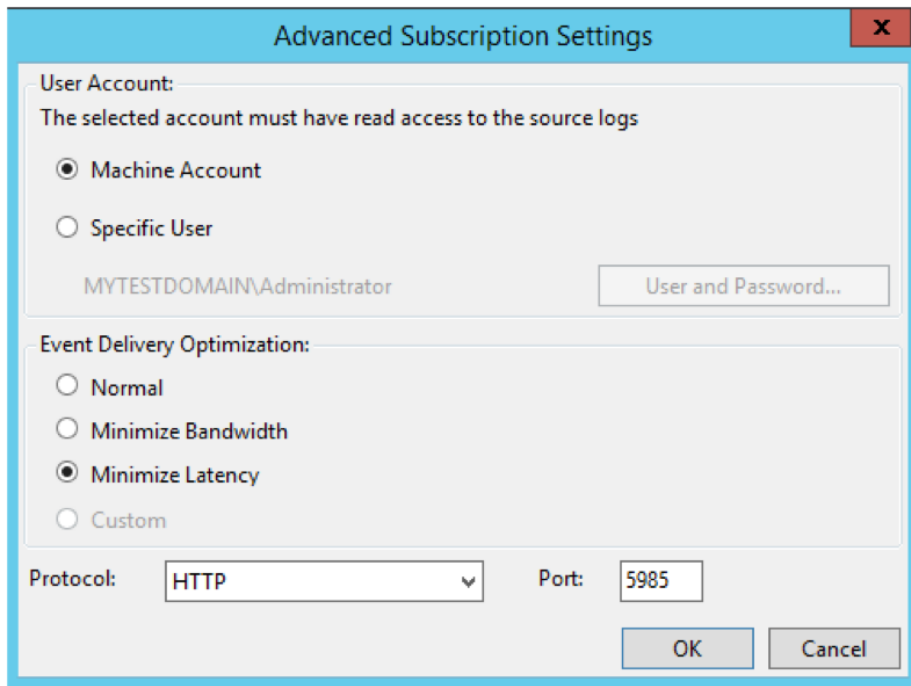
Computer(s): <All Computers>

Clear

OK Cancel

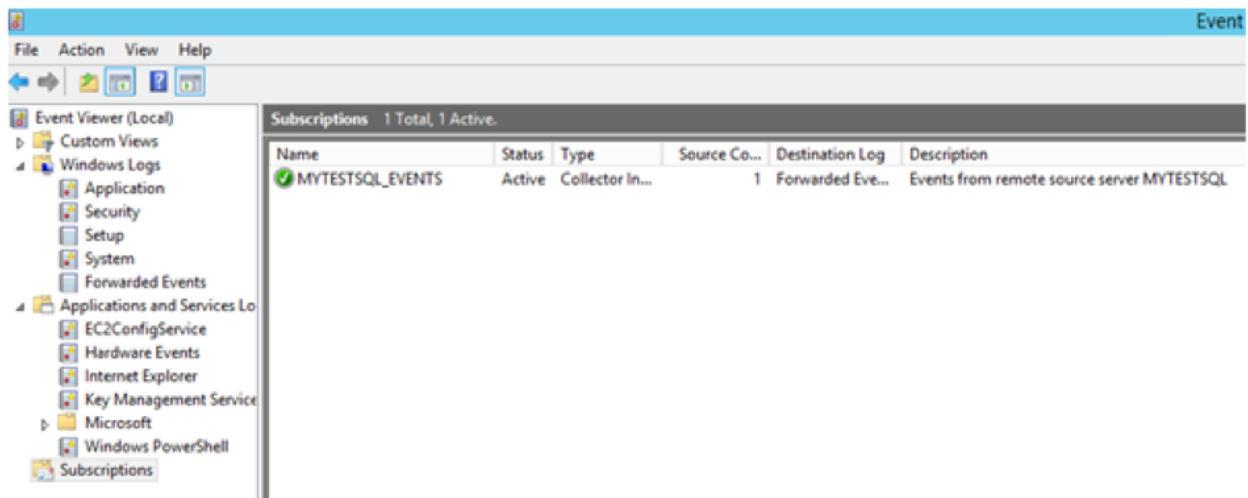
10. Click **OK** to return to the **Subscription Properties**.
11. Click **Advanced** to open the **Advanced Subscription Settings** and enter the following:  
Select **Machine Account**  
Select **Minimize Latency**  
Protocol: **HTTP**  
Port: **5985**





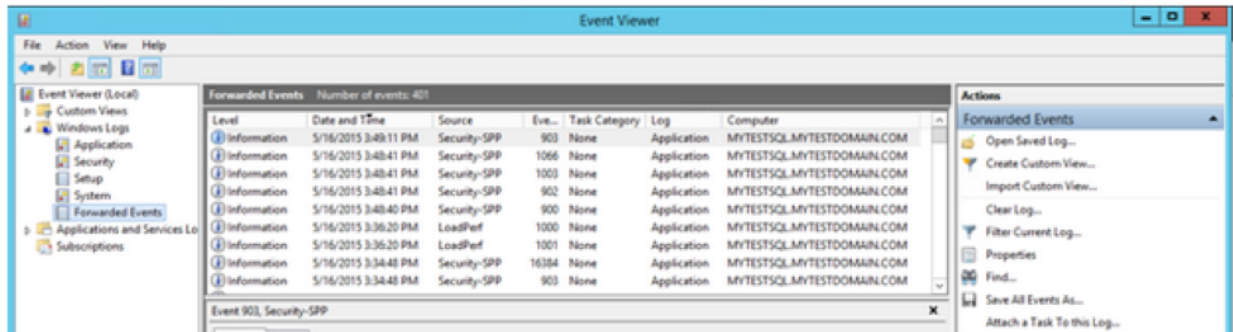
12. Click **OK** to return to the **Subscription Properties**.
13. Click OK to close.

The Subscription node in the collector computer event viewer now shows the new subscription.

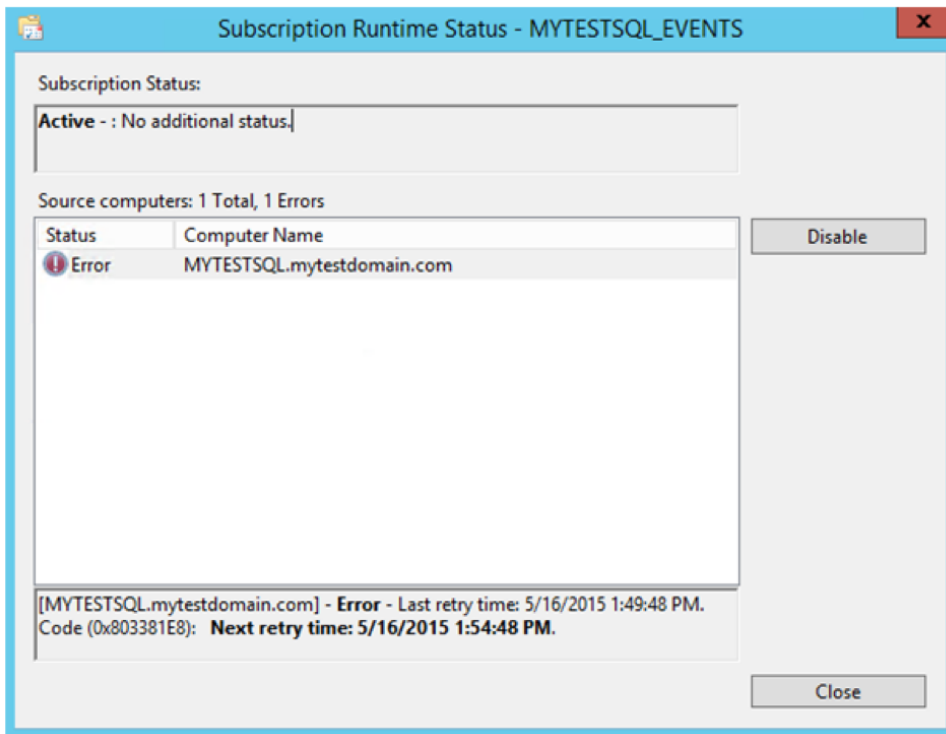


## Verify Events on Collector Computer

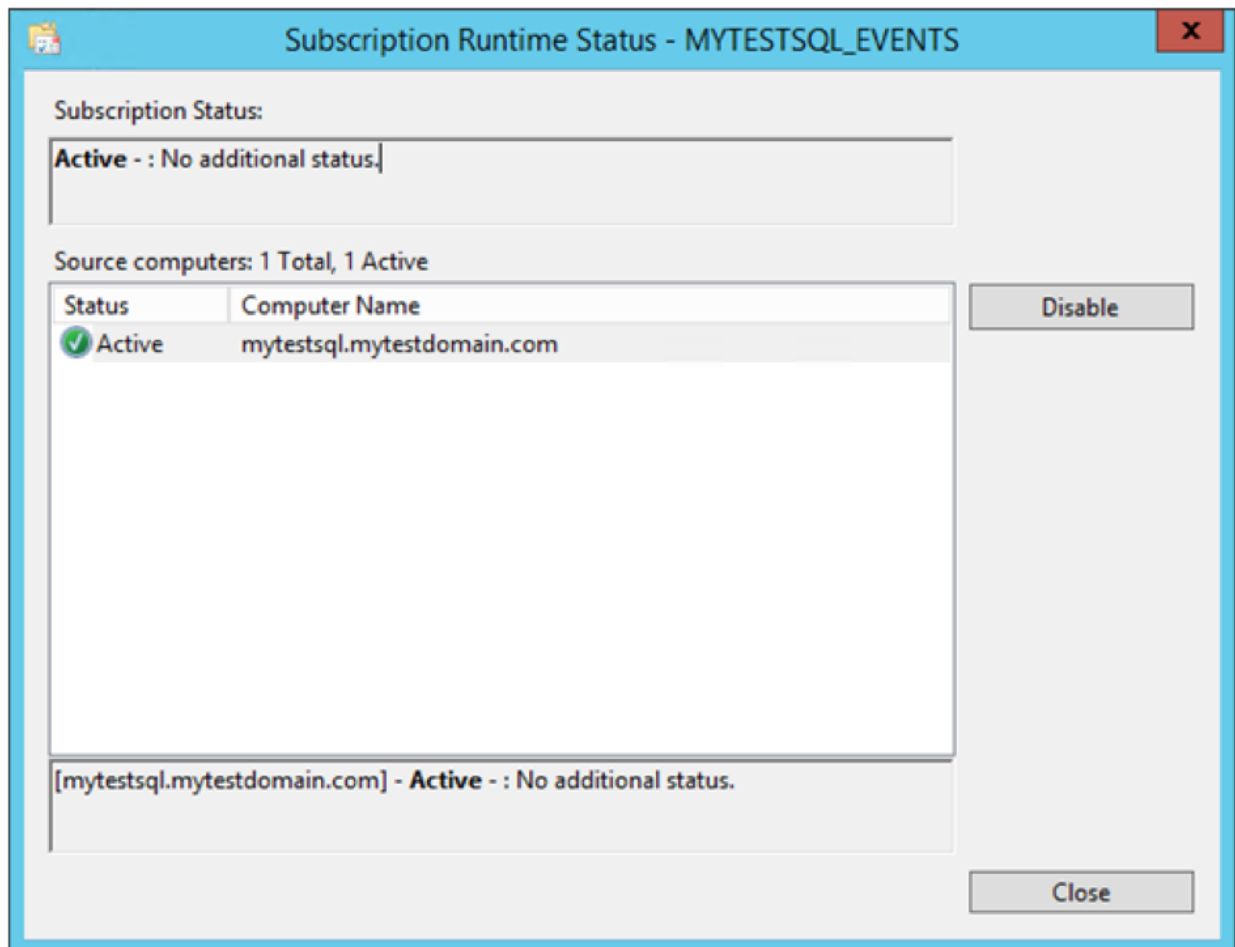
Select **Forwarded Events** from the Navigation pane on the collector computer.



The **Computer** column in the Details pane indicates the events are from the remote computer **MYTESTSQL.MYTESTDOMAIN.COM**. You can enable or disable the collector subscription by right-clicking on the subscription and choosing **Disable**. The status of the subscription is then shown as disabled in the main window. An active collector subscription does not mean it is succeeding. To see if the collector can connect to the source, right-click on the subscription and select **Runtime Status**. In this example, the collector can't connect to the source. By default, it retries every five minutes.



If all is OK, **Subscription Runtime Status** shows a green tick with an active status.



### Send your logs to Network Box SIEM+

At this point you are done; logs are arriving to your central server. Network Box has another document that will show you how to configure such server to send the logs to our SIEM+.