



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 **subscrip-tion**.

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 <u>mytestdomain.com</u> and both machines are registered with the domain.

Source server **MYTESTSQL** hosts a **SQL Server 2014** instance. **Collector** server **MYTEST-SERVER** 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 guickconfig

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



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 gcin

If prompted like the example, press y



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**.

Jsers, Service Accounts, or Groups	Object Types
rom this location:	
MYTESTDOMAIN.COM	Locations
Inter the object names to select (<u>examples</u>):	
	Check Names
Object	Types
Select the types of objects you want to find	
Select the types of objects you want to find. Object types: Object types: Computers Groups Users Users	

- 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.

	Event Log Readers Properties		
Seneral	nt Log Readers		
Description:	Members of this group can read event logs fr machine	rom loca	d
Members:			
WE WITLESTI	DOMAINMITTEOTOENVEN		
MT LEST			
S MILES II			
MILES I			
Add	Changes to a user's group m are not effective until the net user logs on.	iembersł xt time tł	nip

Configure Windows Firewall

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

	Allowed app	s			
🔗 🕨 Control Panel 🕨 System	m and Security Windows Firewall Allowed apps				
	Allow apps to communicate through Windows I To add, change, or remove allowed apps and ports, click Chan	Firewall ge settings.			
	What are the risks of allowing an app to communicate?		😗 Char	nge settir	ngs
	Allowed apps and features:				
	Name	Domain	Private	Public	~
	File and Printer Sharing over SMBDirect				П
	File Server Remote Management			•	
	□ iSCSI Service				
	Key Management Service				
	Netlogon Service				
	Network Discovery				=
	Performance Logs and Alerts				
	Remote Desktop			Y	
	Remote Event Log Management				
	Remote Event Monitor				
	Remote Scheduled Tasks Management				
	Remote Service Management				~
		De	tails	Remov	e
		1	Allow an	other ap	p

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.

8	Event View	er	_ _ ×
File Action View Help			
 Event Viewer (Local) Custom Views Server Roles Administrative Events Windows Logs Application Security Setup System Forwarded Events Mediations and Services Lo Subscriptions 	Subscriptions 0 Total.	Actions Subscriptions Import Saved Log Create Custom View Import Custom View Create Subscription View Refresh Help	•
	,		

 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

	Subscription Properties - MYTES	TSQL_EVENTS				
Subscription name:	MYTESTSQL_EVENTS					
Description:	Events from remote source server	MYTESTSQL				
Destination log:	Forwarded Events	~				
Subscription type and	source computers					
Collector initiated	ł	Select Computers				
This computer co	ntacts the selected source computers a	nd provides the subscription.				
Source computer local configuration	s in the selected groups must be config n to contact this computer and receive	ured through policy or the subscription.				
Events to collect:		Select Events 💌				
User account (the select Machine Account	ed account must have read access to th	e source logs):				
Change user account of	configure advanced settings:	Advanced				
		OK Cancel				

- 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 X
Filter XML	
Logged:	Last 24 hours
Event level:	Critical Varning Verbose
	Error Information
By log	Event logs: Application
O By source	Event sources:
Includes/Exclud exclude criteria,	les Event IDs: Enter ID numbers and/or ID ranges separated by commas. To type a minus sign first. For example 1,3,5-99,-76
Task category:	
Keywords:	
User:	<all users=""></all>
Computer(s):	<all computers=""></all>
	Clear
	OK Cancel

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

	Advanced Subscription Set	tings 🛛 🗙
User Accoun The selected	t: account must have read access to the source	logs
Machin	e Account	
O Specific	: User	
MYTEST	DOMAIN\Administrator	User and Password
Event Deliver	y Optimization:	
O Normal	I	
O Minimi	ze Bandwidth	
Minimi	ze Latency	
O Custom	1	
Protocol:	HTTP v Port:	5985
		OK Cancel

- 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

8				Event View	er				- 0 X
File Action View Help	Marchard a rate All						_		
Cutom Views Application Sourby Sourborptions	Date and Time S184/2015 3 48:11 PM S176/2015 3 48:41 PM S176/2015 3 48:41 PM S176/2015 3 48:41 PM S176/2015 3 48:40 PM S176/2015 3 3:44:40 PM S176/2015 3 3:34:48 PM S176/2015 3 3:34:48 PM	Source Security-SPP Security-SPP Security-SPP Security-SPP LoadPef LoadPef Security-SPP Security-SPP	Eve 903 1066 1003 902 900 1000 1001 16384 903	Task Category None None None None None None None None	Log Application Application Application Application Application Application	Computer MYTESTSCL.MYTESTDOMAIN.COM MYTESTSCL.MYTESTDOMAIN.COM MYTESTSCL.MYTESTDOMAIN.COM MYTESTSCL.MYTESTDOMAIN.COM MYTESTSCL.MYTESTDOMAIN.COM MYTESTSCL.MYTESTDOMAIN.COM MYTESTSCL.MYTESTDOMAIN.COM MYTESTSCL.MYTESTDOMAIN.COM	×	Forwarded Events	

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.

.	Subscription Runtime Status - MYTESTSQL_EVENTS	5	x
Subscription Active - : No	Status: additional status.		
, Source comp	outers: 1 Total, 1 Errors		
Status	Computer Name	Disable	
Error	MYTESTSQL.mytestdomain.com		
[MYTESTSQL Code (0x8033	mytestdomain.com] - Error - Last retry time: 5/16/2015 1:49:48 PM. 881E8): Next retry time: 5/16/2015 1:54:48 PM.		
1		Close	

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

6	Subscription Runtime Status - MYTESTSQL_EVENT	s ×
Subscription S	Status:	
Active - : No	additional status.	
[store 1 Tatal 1 Astive	
Status	Computer Name	Disable
Active	mytestsql.mytestdomain.com	
[mytestsql.my	/testdomain.com] - Active - : No additional status.	
		Close
		Close

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+.