**Setting up Windows Event Log Collection**

**Setting up Collector on Windows Server (Must be 2008R2+ and Up)**

Step1: [start some services]

On the command line run these commands:

winrm qc

wecutil qc

Step 2: [Creating your Subscriptions]

Open up “Server Manager” -> “Diagnostics” -> “Event Viewer” -> “Subscriptions”

On the right hand side click on “Create Subscription…”

Enter a name for your subscription

Enter a Description

Destination Log: “Forwarded Events”

Click on “Select Source Computer initiated”

Click on “Select Computer Groups…”

Click on “Add Domain Computers”

In the “Enter the object name select” type in “domain computers” and select “check names”

Then Click okay

Next click on “Select Events”

Select “critical, warning, verbose, Error, Information”

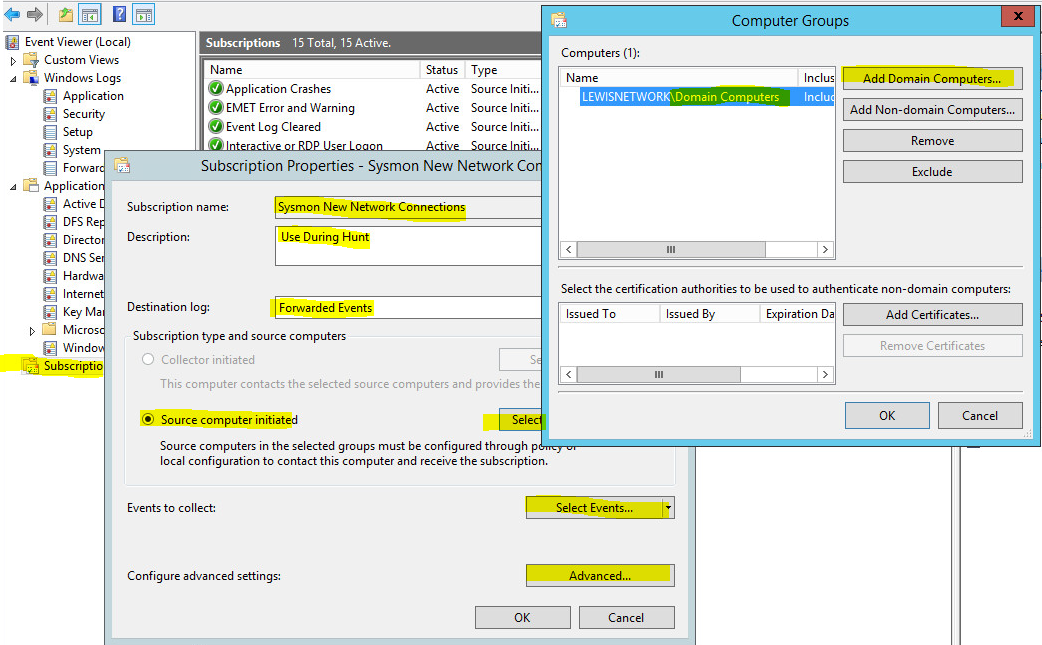
Select Radial button that says “By Log”

Select Drop down and Select whatever subscription you want. In my case I will select “application, system, and security” under the Windows Log section

Enter the event ID’s you want to receive comma separated (if are not specified the subscription will collect all events from al computers in the domain):

“4624,4625,4648,4723,4724,1102,7040,4697,7034,400,4670,4717,602,4649”

Select “OK”

****

Step3: [Setting up Filters to view the logs from your subscription (on the Collector)]

Open up “Server Manager” -> “Diagnostics” -> “Event Viewer” -> “Custom Views”

On the right side of the screen select “Create Custom View”

Select Radial button that says “By Log”

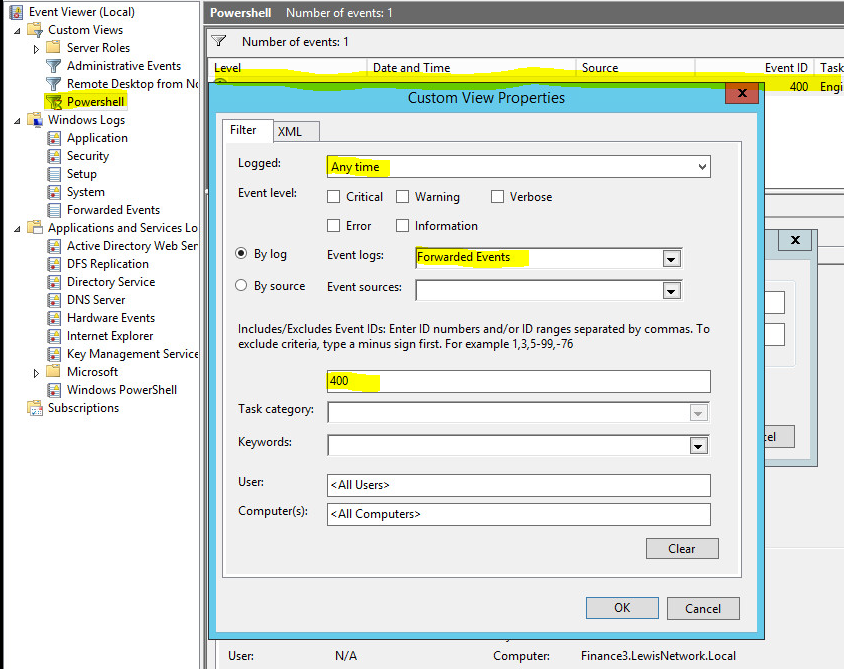
Select Drop down and Select “Forwarded Events” in the Windows Logs Drop down area

Select okay

Give it a name and description

Select Okay

Bata bing ☺



**Creating the Event Forwarding GPO:**

Step1: (Open Group Policy Management)

Click on the “start button” -> “Administrative Tools” -> “Group Policy Management”

Step2: (create a new GPO)

Navigate to “Domain” -> “name of your domain IE: juarbe.local”

Right click on “Group Policy Objects” -> “New”

Name your Group Policy IE “Event Forwarding”

Your new GPO will now appear on the list under “Group Policy Objects”

Right Click and select “edit”

Step3: (Configure your new GPO) [Windows Remote Management]

Navigate to “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> ”System Settings” -> “System Services” ->

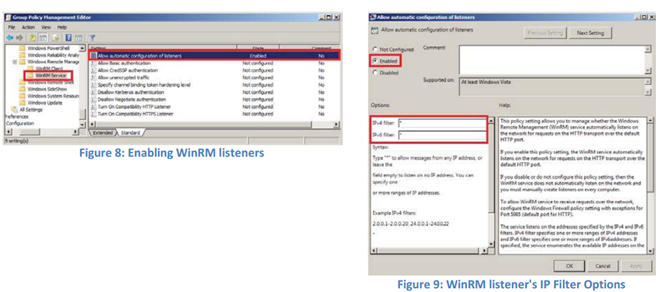
Right click on “Windows Remote Management (WS-Management)” and select “Properties”

Select the “Define this Policy Setting”

Select “Automatic”

Select “Apply”

Select “OK”



Step4: [Event Forwarding]

Navigate to “Computer Configuration” -> “Policies” -> “Administrative Templates” -> “Windows Components” -> “Event Forwarding” ->

Right click on “Configure the server address, refresh time interval, …” and select “edit”

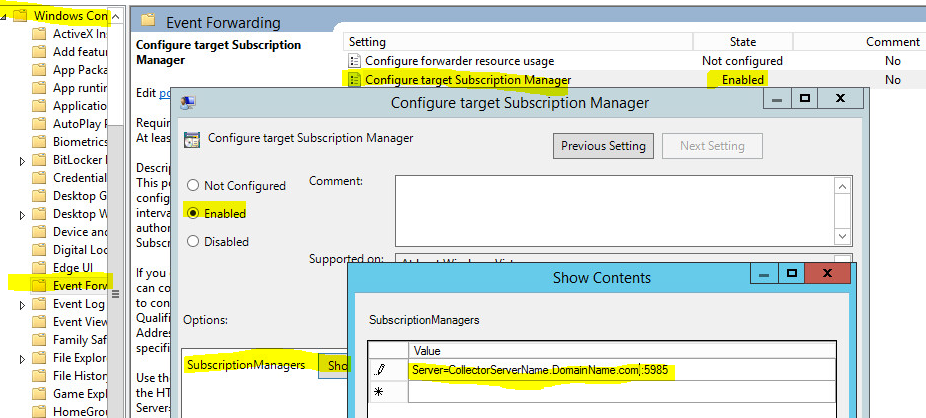
Select the “enabled”

Select “show”

In the Value Field Type in “Server=ComputerNameOfTheCollectorServer.DomainName:5985”

Select “OK”

Select “OK” again



Step5: [NETWORK Service and EVENT LOG READERS]

NOTE: Windows 7 and above sources are not permitted to read event Logs for event forwarding. The sources need to add the NETWORK SERVICE account to the EVENT LOG READERS group under the Restricted Groups in the EventSource GPO/ The members of the Event Log Readers group are permitted to read event logs. Win RM runs with Network Service permissions on Windows 7 and above.

Navigate to “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Restricted Groups” ->

Right click on the white area and select “add group”

Click “browse”

Type “Event Log Readers”

Select “Check Names”

Select “OK”

Select “ADD” in the “Members of this Group” Section

Select “Browse”

Type “Network Service”

Select “Check Names”

Select “OK”

Select “OK”

Select “APPLY”

Select “OK”

Step5: [FIREWALL RULE in the GPO]

Navigate to “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Windows Firewall with advanced Security” -> “Windows Firewall with advanced Security -LDAP” -> “INBOUND RULES”

Right click on the white area or “INBOUND RULES” and select “New Rule”

Select Port

Select “TCP”

Select “Specific Local Ports”

Type “5985”

Select “Allow the Connection”

Select “Domain” Deselect the other 2 (PRIVATE and PUBLIC)

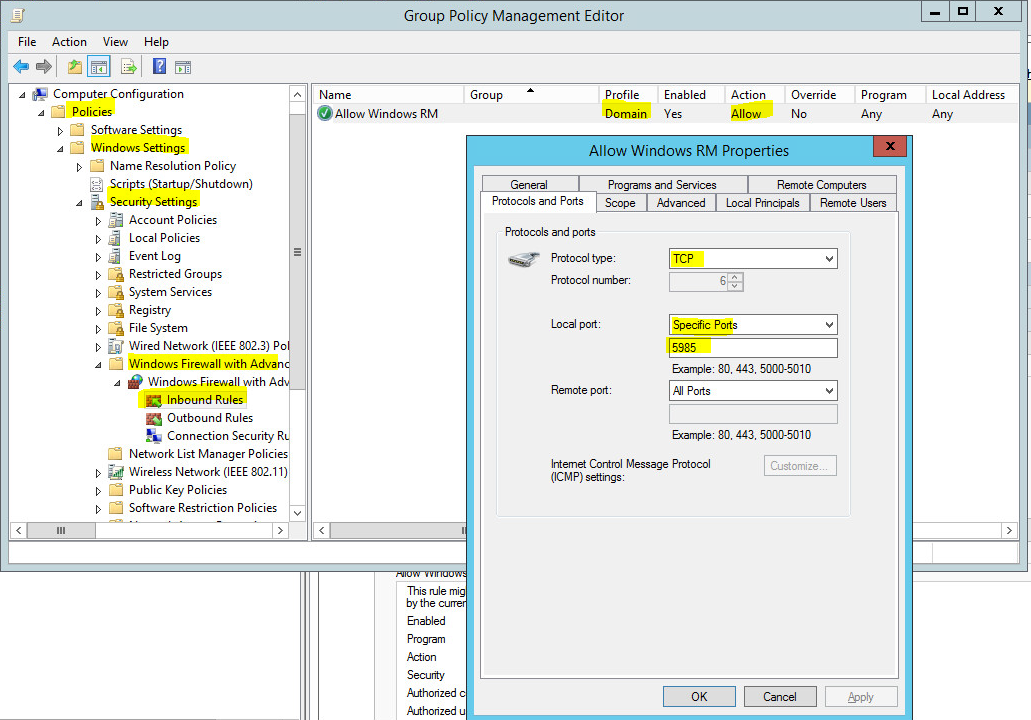
Select “Next”

Type whatever you want to name your rule IE: “Allow Windows RM”

Select “Finish”

Right click and select “Properties” on the rule you just created and verify it looks like this one below

Close Group Policy Management Editor window



Step5: [Apply GPO to appropriate Organizational Units]

Go to the Group Policy Management Window

Right Click on your Domain

Select Link an Existing GPO

Select the GPO you just created and select “OK”

Right Underneath Your Domain name Tree icon you should see the newly added GPO

Right Click on the new GPO you just added and Select “Enforced”

Restart Your Machine twice and the hosts on your domain twice

Batabing ☺

Sadasdsadsadsada

