RSA NetWitness Logs

Event Source Log Configuration Guide

Microsoft System Center Configuration Manager

Last Modified: Thursday, June 08, 2017

Event Source Product Information:

Vendor: Microsoft
Event Source: System Center Configuration Manager
Versions: 2007, 2012
Platforms: Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows 7, Windows 8

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: mssccm
Collection Method: Windows Eventing, Windows Legacy
Event Source Class.Subclass: Network.Configuration Management

Configure Microsoft System Center Configuration Manager using Windows Collection

There are two parts to configuring Windows collection:

I. Configure WinRM on the Windows Host

II. Configure RSA NetWitness Suite for Windows Collection.

Configure WinRM on a Windows Host

This section describes a shortcut method to configure the Windows host. It assumes that you have the following two RSA scripts available:

- `useradd`: sets up a user account with the necessary permissions.
- `RSA_SA_winevent_config.vbs`: sets up the WinRM listener

To set up and run the useradd script:

1. Open **useradd.vbs** for editing.
2. You need to enter your values for the following two parameters:
   - User account: in the **Name** field, enter the name for the RSA user account.
   - Domain: in the **compname** parameter, enter your domain name.

   Note: For the remainder of this document, we are using example values: **rsalog** for the user account, and **dsnetworking.com** for the domain name.
3. On the Windows host, open a Command Prompt, and run **useradd**:

   ```
   c:\Program Files\scripts>useradd.vbs
   ```

   Note: You need to run the script as an administrator.

   The script prompts you to open the file. Click **Yes** to run the script and set up your user.

To run the script to set up the WinRM listener:

1. On the Windows host, open a Command Prompt.
2. Navigate to the folder where the script is stored, and run it as follows:

   ```
   rsa_SA_winevent_config.vbs http
   ```

The script prompts you with a series of information and verification screens: accept them as they appear, in order to have the script succeed.

This completes your set up on the Windows host. Next, you configure RSA NetWitness Suite.

Configure RSA NetWitness Suite for Windows Collection

In RSA NetWitness Suite, you need to configure the Kerberos Realm, and then add the Windows Event Source type.

To configure the Kerberos Realm for Windows collection:

1. In the Security Analytics menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Windows/Kerberos Realm** from the drop-down menu.
4. In the Kerberos Realm Configuration panel toolbar, click + to add a new realm.

   The Add Kerberos Domain dialog is displayed.
5. Fill in the parameters, using the guidelines below.

Parameter	Details
Kerberos Realm Name	Enter the realm name, in all caps. For example, DSNETWORKING.COM. Note that the Mappings parameter is automatically filled with variations on the realm name.
KDC Host Name	Enter the name of the Domain Controller. ***Do not*** use a fully qualified name here: just the host name for the DC. **Note:** Make sure that the log collector is configured as a DNS client for the corporate DNS server. Otherwise, the LC will not know how to find the Kerberos Realm.
Admin Server	(Optional) The name of the Kerberos Administration Server in FQDN format.

6. Click **Save** to add the Kerberos domain.

Next, continue from the current screen to add a Windows Event Category and type.

To configure the Windows Event Type:

1. Select **Windows/Config** from the drop-down menu.
2. In the Event Categories panel toolbar, click + to add a source.

   The Add Source dialog is displayed.
3. Fill in the parameters, using the guidelines below.

Parameter	Details
Alias	Enter a descriptive name.
Authorization Method	Choose **Negotiate**.
Channel	For most event sources that use Windows collection, you want to collect from the **Security**, **System**, and **Application** channels.
User Name	Enter the account name for the Windows user account that you set up earlier for communicating with Security Analytics. Note that you need to enter the full account name, which includes the domain. For example, **rsalog@DSNETWORKING.COM**.
Password	Enter the correct password for the user account.
Max Events Per Cycle	(Optional). RSA recommends that you set this value to 0, which collects everything.
Polling Interval	(Optional). For most users, a value of **60** should work well.

4. Click **OK** to add the source.
   The newly added Windows event source is displayed in the Event Categories panel.
5. Select the new event source in the Event Categories panel.
   The **Hosts** panel is activated.
6. Click + in the Hosts panel toolbar.

7. Fill in the parameters, using the guidelines below.

Parameter	Details
Event Source Address	Enter the IP address for the Windows host.
Port	Accept the default value, **5985**.
Transport Mode	Enter **http**.
Enabled	Ensure the box is checked.

8. Click **Test Connection**.

Note: In Security Analytics versions prior to 10.4 patch 2, the Windows service had to be running in order for the test connection to work. In later versions, you should be able to successfully test the connection, even if the Windows service is not running.

For more information on any of the previous steps, see the following Help topics in the Security Analytics User Guide:

- Configure Windows Collection: https://community.rsa.com/docs/DOC-43410
- Microsoft WinRM Configuration Guide: https://community.rsa.com/docs/DOC-58163
- Test and Troubleshoot Microsoft WinRM Guide: https://community.rsa.com/docs/DOC-58164

Trademarks