RSA NetWitness Platform

Event Source Log Configuration Guide

Avecto Privilege Guard

Last Modified: Thursday, October 31, 2019

Event Source Product Information:

Vendor: Avecto
Event Source: Privilege Guard
Version: 3.5
Platforms: Windows Server 2008 R2, Windows Server 2012

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: avectopg
Collection Method: Windows Event Logs
Event Source Class.Subclass: Security.Access Control

Configure NetWitness Platform for Windows Collection

You need to set up Windows Event Logs collection for the Avecto Privilege Guard event source.

To configure WinRM, see the following document on RSA Link: Microsoft WinRM Configuration and Troubleshooting. For more details about Windows Collection in the RSA NetWitness Platform, see the Configure Windows Collection topic on RSA Link.

Note: When you configure the Windows Event Type as described in the Microsoft WinRM Configuration Guide, you need to specify the channel from which you wish to collect. Make sure to enter **Application** for the channel value.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.