Centralizing Windows Events with Event Forwarding
Copyright Notice

The information contained in this document (“the Material”) is believed to be accurate at the time of printing, but no representation or warranty is given (express or implied) as to its accuracy, completeness or correctness. Avecto Ltd, its associated companies and the publisher accept no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance placed on this Material for any purpose.

Copyright in the whole and every part of this document belongs to Avecto Ltd (“the Owner”) and may not be used, sold, transferred, copied or reproduced in whole or in part in any manner or form or in or on any media to any person other than in accordance with the terms of the Owner’s Agreement or otherwise without the prior written consent of the Owner.

Trademarks

Microsoft Windows, Windows Vista, Windows Server, Windows PowerShell, ActiveX, Visual C++ and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
Contents

Introduction .................................................................................................................................. 4
Windows Event Forwarding Features .......................................................................................... 5
Architecture ................................................................................................................................. 6
Pre-Requisites .............................................................................................................................. 7
  Central Event Collector ............................................................................................................. 7
  Source Computers .................................................................................................................... 7
Downloads ................................................................................................................................... 8
Implementing Windows Event Forwarding ................................................................................... 9
  Installing Windows Remote Management (WinRM) ................................................................. 9
Windows Remote Management (WinRM) Configuration ............................................................. 9
  Configuring Services and Windows Firewall on the Event Collector ........................................ 9
  Configuring the WinRM Service via Group Policy ................................................................. 11
  Configuring the WinRM Enhanced Security via Group Policy ............................................. 13
Event Forwarding Configuration ................................................................................................. 14
  Configuring Services on Source Computers ........................................................................... 16
  Configuring Subscriptions on the Event Collector ................................................................. 16
Optimizing Event Forwarding ....................................................................................................... 21
  Pre-rendering .......................................................................................................................... 21
  Forwarder Resource Usage ....................................................................................................... 21
Testing Event Forwarding ............................................................................................................. 23
  Troubleshooting ..................................................................................................................... 24
    Check Policy has been applied to the Source Computer ....................................................... 24
    Check Windows Remote Management Service on the Source Computer .......................... 24
    Check Collector can reach the Source Computer via WinRM? ........................................... 24
    Check the Collector is using the Right Credentials (Collector Initiated Only) ..................... 24
    Check the Source Computer has registered with the Collector ......................................... 24
    Check the Forwarding/Operational event log on the Source Computer for error 105 ....... 24
Raising Actions & Tasks ............................................................................................................ 26
  Advanced options ............................................................................................................... 27
Introduction

This document provides guidance on how to centralize Privilege Guard events to a central server using Windows Event Forwarding. Event Forwarding is provided by Windows Remote Management (WinRM) which is Microsoft’s implementation of WS-Management Protocol, a SOAP based, firewall-friendly protocol, which provides a common way for systems to access and exchange management information across an IT infrastructure.

One of the most powerful features of WinRM is the ability to forward events which enables large scale health and state monitoring of Windows environments (also known as Windows Eventing 6.0). Not only is this feature built into the latest versions of Windows (originally shipped with Windows Vista and Windows Server 2008), but it's also available for down-level operating systems like Windows XP SP2+ and Windows Server 2003 SP1+. 
Windows Event Forwarding Features

1. **Standards Based:** Leveraging the DMTF WS-Eventing standard which allows it to interoperate with other WS-Man implementations (see OpenWSMAN at SourceForge).
2. **Agentless:** Event Forwarding and Event Collection are included in the operating system by default.
3. **Down-Level Support:** Event Forwarding is available for Windows XP SP2+ and Windows Server 2003 SP1+.
4. **Multi-Tier:** Forwarding architecture is very scalable where a Source Computer may forward to a large number of collectors and collectors may forward to collectors.
5. **Scalable:** Event Collection is very scalable where the collector can maintain subscriptions with a large number of Source Computers and events per second.
6. **Group Policy Aware:** The entire model is configurable by Group Policy.
7. **Schematized Events:** Windows Events are now schematized and rendered in XML which enables many scripting and export scenarios.
8. **Pre-Rendering:** Forwarded Windows Events can now be pre-rendered on the Source Computer negating the need for local applications to render Windows Events.
9. **Resiliency:** Designed to enable mobile scenarios where laptops may be disconnected from the Event Collector for extended periods of time without event loss (except when logs wrap) as well as leveraging TCP for guaranteed delivery.
10. **Security:** Certificate based encryption via Kerberos or HTTPS.
Architecture

The architectural approach used in this guide utilizes Group Policy to distribute event forwarding configuration to a group of domain computers. Each client will be configured to forward events to a central Event Collector.
Pre-Requisites

Central Event Collector

A central Event Collector must be used as a repository for all the events collected from the Source Computer.

Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2008 R2 can be Event Collectors (this feature is not supported for down-level operating systems). There are no built-in limitations when client operating systems are used as an Event Collector. However, it is recommended that Server 2008/R2 is used as the Event Collector as this will scale much better in high volume scenarios.

**NOTE:** When using Windows Vista or Windows Server 2008 as the Event Collector, it is strongly recommended that you upgrade to Windows Remote Management 2.0. This will allow Windows 7 clients to be monitored without any additional configuration.

Depending on the volume of events, the Event Collector can either be a dedicated or an existing machine. True enterprise class Windows Eventing is included with enterprise monitoring solutions like System Center Operations Manager (SCOM).

Source Computers

The minimum operating system level required on the Source Computer is Windows XP SP2. Events can be centralized onto any of the supported Windows Server operating system. Each Source Computer must have minimum of Windows Remote Management 1.1.

The following table shows the default installation for each OS:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Windows Remote Management Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>Not installed</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>1.1</td>
</tr>
<tr>
<td>Windows 7</td>
<td>2.0</td>
</tr>
<tr>
<td>Windows Server 2003/R2</td>
<td>Not installed</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>1.1</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>2.0</td>
</tr>
</tbody>
</table>
Downloads

Only Windows XP and Windows Server 2003 require a version of WinRM to be deployed. It is recommended that Windows Remote Management 2.0 is deployed to these computers.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Download</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>Windows Remote Management 1.1</td>
<td>1MB</td>
</tr>
<tr>
<td>Windows XP</td>
<td>Windows Remote Management 2.0</td>
<td>6MB</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>Windows Remote Management 2.0</td>
<td>34MB</td>
</tr>
<tr>
<td>Windows Vista (x64)</td>
<td>Windows Remote Management 2.0</td>
<td>34MB</td>
</tr>
<tr>
<td>Windows Server 2003/R2</td>
<td>Windows Remote Management 1.1</td>
<td>1MB</td>
</tr>
<tr>
<td>Windows Server 2003/R2</td>
<td>Windows Remote Management 2.0</td>
<td>6MB</td>
</tr>
<tr>
<td>Windows Server 2003/R2 (x64)</td>
<td>Windows Remote Management 2.0</td>
<td>10MB</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>Windows Remote Management 2.0</td>
<td>32MB</td>
</tr>
<tr>
<td>Windows Server 2008 (x64)</td>
<td>Windows Remote Management 2.0</td>
<td>34MB</td>
</tr>
</tbody>
</table>

**NOTE:** Windows Remote Management 2.0 packages also include Windows PowerShell 2.0.
Implementing Windows Event Forwarding

Installing Windows Remote Management (WinRM)

When the down-level machines are Source Computers ensure that the WinRM client is installed on these machines (refer to Downloads in the Pre-Requisites section). It is recommended that a software distribution server, such as System Center Configuration Manager (SCCM) or Systems Management Server (SMS) is used to deploy the WinRM packages.

**NOTE:** When upgrading an Event Collector from WinRM 1.1 to WinRM 2.0 ensure that there are no active Subscriptions running else the upgrade may fail.

Windows Remote Management (WinRM) Configuration

Configuring Services and Windows Firewall on the Event Collector

In order for Source Computers to communicate with the Event Collector machine the correct inbound firewall ports need to be open and accepting connections. In addition the WinRM and Event Collector services need to be running.

**Configuration Steps**

1. On the **Event Collector** machine open a command prompt.
2. Type `winrm quickconfig`

```
C:\Users\Administrator>winrm quickconfig
WinRM already is set up to receive requests on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:
Create a WinRM listener on HTTP://*/ to accept WS-Management requests to any IP on this machine.
Enable the WinRM firewall exception.
Make these changes [yn]? y
WinRM has been updated for remote management.
Created a WinRM listener on HTTP://*/ to accept WS-Management requests to any IP on this machine.
WinRM firewall exception enabled.
C:\Users\Administrator>
```

3. When prompted whether to continue with the configuration type `y`
This command will check the current configuration and make the necessary configuration changes. Upon completion the following will have been configured:

- **Windows Remote Management** service set to *Automatic (Delayed Start)* and *Started*.
- Windows Firewall port(s) **Windows Remote Management (HTTP-In) Port 5985** configured for inbound communication OR Windows Firewall port(s) **Windows Remote Management (HTTP-In) – Compatibility Mode - Port 80** configured for inbound communication.

**NOTE:** Quickconfig will only open the firewall ports for the version of WinRM running on the Event Collector. For example if you are running WinRM 2.0 the *Compatibility Mode* ports will not be opened. Therefore you will need to manually enable these ports, if required.

In addition Event Collector service needs to be configured and started.

**Configuration Steps**

1. On the **Event Collector** machine open a command prompt.
2. Type `wecutil qc`
3. When prompted whether to continue with the configuration type `y`
This command will check the current configuration and make the necessary configuration changes. Upon completion the following will have been configured:

- **Windows Event Collector** service set to **Automatic (Delayed Start)** and **Started**

### Configuring the WinRM Service via Group Policy

Group Policy may be used to enable and configure Windows Remote Management (WinRM). This section will focus on configuring the WinRM service to listen for incoming events. This can be configured via following Group Policy setting:

- **Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Management/WinRM Service/**

**NOTE:** When editing Group Policy settings ensure that the Event Collector(s) and Source Computer(s) are under the management scope of the Group Policy Object being editing.
Configuration Steps

1. Edit the Group Policy Object (GPO) being used.
2. Navigate to ./Allow automatic configuration of listeners (see above for full path).
3. Set this to Enabled.
4. Specify * as the filter.

NOTE: This Listener configuration should only be used in a trusted network environment. If the environment is not trusted (like the Internet), then configure only specific IP Addresses or ranges in the IPv4 and IPv6 filters.

If you are using Windows Server 2008 R2 as the Event Collector, or have upgraded to Windows Remote Management 2.0 (which is recommended), then you will need to enable Compatibility mode to receive events from down-level clients. The following Group Policy settings are used:

- ./Turn on Compatibility HTTP Listener
- ./Turn on Compatibility HTTPS Listener

Configuration Steps

1. Navigate to ./Turn on Compatibility HTTP Listener (see above for full path).
2. Set this to Enabled.
3. Navigate to ./Turn on Compatibility HTTPS Listener (see above for full path).
4. Set this to Enabled.
Configuring the WinRM Enhanced Security via Group Policy

For enhanced security, the following Group Policy settings may be configured for the WinRM Client and Service.

- **Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Management/**WinRM Client/**
- **Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Management/**WinRM Service/**

- **Basic Authentication**
  This policy setting allows you to manage whether the Windows Remote Management (WinRM) uses Basic authentication. If you enable this policy setting, the WinRM will use Basic authentication. If WinRM is configured to use HTTP transport, then the user name and password are sent over the network as clear text.

- **Allow CredSSP Authentication**
  This policy setting allows you to manage whether the Windows Remote Management (WinRM) uses CredSSP authentication. If you enable this policy setting, the WinRM will use CredSSP authentication.

- **Allow Unencrypted Traffic**
  This policy setting allows you to manage whether the Windows Remote Management (WinRM) sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM sends and receives unencrypted messages over the network.

- **Disallow unencrypted Traffic**
  If you disable or do not configure this policy setting, the WinRM sends or receives only encrypted messages over the network. This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication.

- **Disallow Kerberos Authentication**
  This policy setting allows you to manage whether the Windows Remote Management (WinRM) will not use Kerberos authentication directly. If you enable this policy setting, the Windows Remote Management (WinRM) will not use Kerberos authentication directly. Kerberos may still be used if the WinRM is using the Negotiate authentication and Kerberos is selected.

- **Disallow Negotiate Authentication**
  This policy setting allows you to manage whether the Windows Remote Management (WinRM) will not use Negotiate authentication. If you enable this policy setting, the WinRM will not use Negotiate authentication.

- **Trusted Hosts (Client Only)**
  If you enable this policy setting, the WinRM client uses a specified list to determine if the destination Event Collector is a trusted entity. The WinRM client uses this list when neither HTTPS nor Kerberos are used to authenticate the identity of the Event Collector.
Specify channel binding token hardening level (Service Only)
This policy setting allows you to set the hardening level of the Windows Remote Management (WinRM) service with regard to channel binding tokens. If Hardening Level is set to **Strict**, any request not containing a valid channel binding token will be rejected.

**NOTE:** It is important that these settings are compatible with your operating environment and that the WinRM Client and WinRM Service settings are compatible. Mis-configuration may stop the configuration from operating correctly.


Event Forwarding Configuration

Group Policy may be used to configure Source Computers (Clients) to forward events to a collector (or set of collectors). The policy is very simple. It merely tells the Source Computer to contact a specific FQDN (Fully Qualified Domain Name) or IP Address and request subscription specifics. All of the other subscription details are held on the Event Collector.

The following Group Policy Settings are used to configure event forwarding:

- Computer Configuration/Policies/Administrative Templates/Windows Components/Event Forwarding/
Configuration Steps

1. Edit the Group Policy Object (GPO) being used.
2. Configure the **Configure the server address...** option.
3. Set this to **Enabled**.
4. Click **Show**, the Subscription Managers dialog will be displayed.

5. Click **Add** and enter the address of the **Event Collector** in the following format:

   **WinRM 2.0 Settings**
   - Server=http://<Event Collectors FQDN>:5985/wsman/SubscriptionManager/WEC
   - Server=https://<Event Collectors FQDN>:5986/wsman/SubscriptionManager/WEC

   **WinRM 1.1**
   - Server=http://<Event Collectors FQDN>:80/wsman/SubscriptionManager/WEC
   - Server=https://<Event Collectors FQDN>:443/wsman/SubscriptionManager/WEC

   **NOTE:** The syntax used here will depend on the WinRM version running on the **Event Collector** and whether HTTP or HTTPS is used.

   If HTTPS is being used a valid SSL certificate will be needed refer to [http://msdn.microsoft.com/en-us/library/bb870973(VS.85).aspx](http://msdn.microsoft.com/en-us/library/bb870973(VS.85).aspx) for information configuring WinRM to utilize SSL certificates.

6. Click **OK**.
Configuring Services on Source Computers

In order for Source Computers to communicate with the Event Collector machine the Windows Remote Management service needs to be running on the Source Computers.

The following Group Policy Settings are used to configure event forwarding:

- Computer Configuration\Policies\Windows Settings\Security Settings\System Services

Configuration Steps

1. Navigate to the Windows Remote Management (WS-Management) service.
2. Double click the service.
3. Check Define this policy setting.
4. Select the Automatic radio button.
5. Click OK.

Configuring Subscriptions on the Event Collector

Windows Event Forwarding architecture stores the subscription definition on the Event Collector, in order to reduce the number of touch-points, in case a subscription needs to be created or modified. The following subscription will be configured to leverage Group Policy.

Subscriptions are created on the Event Collector through the new Event Viewer user interface by selecting the Create Subscription action, when the Subscriptions node is highlighted. The Subscription may also be created via the WECUTIL command-line utility.
Configuration Steps

1. On the Event Collector open the Event Viewer.
2. Navigate to the Subscriptions node.
3. From the menu bar, choose Action->Create Subscription...
4. The Subscriptions Properties dialog will appear:
From here, you can specify a name, description, and the destination log (where the events will be collected).

5. Select **Forwarded Events** for the destination log.
6. Choose **Source Computer Initiated** (as Group Policy configures the Source Computer to contact the Event Collector for subscriptions settings).

**NOTE:** The **Subscription Type** can also be configured as **Collector initiated**. In this case Source Computers will need to be manually added to the Subscription either through the Subscription configuration or the WECUTIL command-line utility (which can also be scripted using PowerShell).

It recommended that **Source computer initiated** is used, as this is the most reliable configuration.

7. Click **Select Computer Groups**.
8. Click **Add Domain Computers** and select the required Source Computers.

9. Click **OK** on the **Computer Groups** dialog.
10. Click **Select Events**.
11. Configure the following **Query Filter**:

   - Event Level = Critical, Warning, Error, Information
   - By Source = Avecto Privilege Guard Service
NOTE: In a production environment, it may be advantageous to gather all events from the Application and System logs that have a level of Critical, Error, or Warning. This event scope can be expanded to gather all events from these logs or even add additional logs (like the Security log).

If the Privilege Guard Agent is not installed on the Event Collector you will not be able to select Avecto Privilege Guard Service as the Event Source. It is recommended that the Privilege Guard Agent is installed and set to disabled. If it is not possible to install the agent the subscription can be configured to collect events from the Application event log and filtered on event IDs 100 to 116.

12. Click OK on the Query Filter dialog.
13. Click Advanced on the Subscription Properties dialog.
14. Select **Minimize Latency**.

![Advanced Subscription Settings]

**NOTE:**

**Normal**
This option ensures reliable delivery of events and does not attempt to conserve bandwidth. It is the appropriate choice unless you need tighter control over bandwidth usage or need forwarded events delivered as quickly as possible. It uses pull delivery mode, batches 5 items at a time and sets a batch timeout of 15 minutes.

**Minimize Bandwidth**
This option ensures that the use of network bandwidth for event delivery is strictly controlled. It is an appropriate choice if you want to limit the frequency of network connections made to deliver events. It uses push delivery mode and sets a batch timeout of 6 hours. In addition, it uses a heartbeat interval of 6 hours.

**Minimize Latency**
This option ensures that events are delivered with minimal delay. It is an appropriate choice if you are collecting alerts or critical events. It uses push delivery mode and sets a batch timeout of 30 seconds.

**Protocol**
HTTPS is preferred for the communication channel, as this is secure. However, you must configure the Event Collector to use a certificate.

15. Click **OK** on the **Advanced Subscription** dialog.
16. Click **OK** on the **Subscription Properties** dialog.
Optimizing Event Forwarding

Pre-rendering

If the Source Computer is generating a large volume of forwarded events (e.g. Security events from a Domain Controller) then it is recommended that event rendering is disabled on the Event Collector. The task of pre-rendering an event on the source computer can be CPU intensive for a large number of events.

Configuration Steps

1. On the Event Collector open a command prompt.
2. Type `wecutil ss <name of subscription> /cf:events`

This will change the ContentFormat to Events from RenderedText.

**NOTE:** To view Event Subscriptions use the WECUTIL command utility and type:

```
wecutil gs <name of subscription>
```

Forwarder Resource Usage

It is possible to control the volume of events sent to the Event Collector by the Source Computer, and this may be required in high volume environments.

The following Group Policy Settings are used to configure Forwarder Resource Usage:

- Computer Configuration/Policies/Administrative Templates/Windows Components/Event Forwarding/ForwardResourceUsage
This GPO controls resource usage for the forwarder (Source Computer) by controlling the Events/per second sent to the Event Collector. This setting applies across all subscriptions for the forwarder (Source Computer).
Testing Event Forwarding

If all of the Event Forwarding components are functioning (and there's minimal network latency), a test event created on the Source Computer should arrive in the Event Collector's **Forwarded Events** log within 60 seconds.

On the Source Computer create a Privilege Guard event. Alternatively if you have configured the subscription to capture all events from the application log you can use the following command line to create a test event.

1. On the **Source Computer** open a command prompt.
2. Type `eventcreate /id 999 /t error /l application /d "Test event."`

```
C:\>eventcreate /id 999 /t error /l application /d "Test event."
SUCCESS: An event of type 'error' was created in the 'application' log with 'EventCreate' as the source.
```

3. This event should appear on the **Event Collector** as follows:

```
NOTE: If the **Privilege Guard Agent** is not installed on the **Event Collector** the event may not be formatted correctly. It is recommended that the **Privilege Guard Agent** is installed on the **Event Collector** and set to disabled; this will ensure the events are displayed correctly.
```
**Troubleshooting**

If the events are not appearing on the Event Collector perform the following troubleshooting steps:

**Check Policy has been applied to the Source Computer**

This can be forced by running the following command on the Source Computer:

```plaintext
gpupdate /force
```

**Check Windows Remote Management Service on the Source Computer**

On the source computer navigate to the service.msc and check the WinRM service is running and set to start automatically.

**Check Collector can reach the Source Computer via WinRM?**

Run the following command on the Collector

```plaintext
winrm id /r:<Source Computer> /a:none
```

**Check the Collector is using the Right Credentials (Collector Initiated Only)**

Run the following command on the Collector

```plaintext
winrm id /r:<Source Computer> /u:<username> /p:<password>
```

**NOTE:** These are the credentials defined in the Subscription on the Event Collector. The credentials don’t need to be in the local administrators group on the Source Computer, as long as they are in the Event Log Readers group on the Source Computer (local administrators will also work).

**Check the Source Computer has registered with the Collector**

Run the following command on the Collector:

```plaintext
certutil gr <subscription name>
```

This will list all the registered Source Computers (if the Subscription is "Collector Initiated" then this will list all configured Source Computers), their state (from the Collector’s perspective), and their last heartbeat time.

**Check the Forwarding/Operational event log on the Source Computer for error 105**

Check the Windows Forwarding/Operational event log on the Source Computer for errors. Event ID 105 "The forwarder is having a problem communicating with the subscription manager address“ is often a result of the Windows Firewall on the Event collector blocking communication.
Ensure the following rules are accepting incoming connection:

- Windows Firewall port(s) **Windows Remote Management (HTTP-In) Port 5985** configured for inbound communication.

- Windows Firewall port(s) **Windows Remote Management (HTTP-In) – Compatibility Mode - Port 80** configured for inbound communication.

- Windows Firewall port(s) **Windows Remote Management (HTTPS-In)** configured for inbound communication.
Raising Actions & Tasks

In many situations administrator or security professionals many want to be informed when a particular event is collected. It is possible to trigger the following actions by assigning a task to be Event Collector’s forwarded events log.

- Start a program
- Email
- Display a message

For example an administrator may want to be informed, by e-mail, when a user has elevated an application using the On-demand facility (Event ID 101).

Configurations steps
1. Open the Event Viewer utility on the Event Collector.
2. Right click on the Forwarded Events log.
3. Click Assign a Task To this Log...
4. Give the Task a name and click Next.
5. Click Next.
6. Select the Action required.
7. Complete the action details click Next.
8. Click Finish (the task is now setup).
Advanced options

It is possible to set advanced configuration options and filters by reviewing the action for the Windows Task Scheduler -> Event Viewer Tasks: