RSA Security Analytics

Event Source Log Configuration Guide

Microsoft Windows Eventing Collection

Event Source Product Information:

Vendor: Microsoft
Event Source: Windows
Versions: Windows 7 and 8; Windows Server 2008 R2; Windows Server 2008 and 2012

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Collection Method: Windows

Chapter 1: Microsoft Windows Eventing Collection Overview

Perform the following tasks to configure Windows systems so that the RSA Security Analytics Log Collector can collect events from them.

I. (optional) If you have Windows event sources that use non-English languages, you must download and install the English language packs for Windows. Language packs are available as free downloads from Microsoft downloads site, **http://www.microsoft.com/downloads**.

II. **Create a User Account for the RSA Security Analytics Log Collector**

III. Enable Windows Remote Management (WinRM):

- **Enable Windows Remote Management over HTTP**
- **Enable Windows Remote Management over HTTPS**

After you configure your event sources, you must configure the **RSA Security Analytics Log Collector**.

Refer to **Configure Windows Event Sources** and **Configure Kerberos Authentication** for Security Analytics Log Collector Windows configuration.

For Local Collectors, when you configure the Log Decoder, review the parsers selected in the Device Parsers Configuration section and select Start Capture. Please refer to **Decoder Device System View** for information about Security Analytics Log Decoder.

Chapter 2: Create a User Account for the RSA Security Analytics Log Collector

RSA recommends that the user account that the RSA Security Analytics Log Collector uses to authenticate to the event source has only enough privileges to allow event collection. Perform the following tasks to set up a "least privileged" account:

I. Create a non-Administrator user account for Security Analytics Log Collector

II. Add the user account to the Event Log Readers local user group

III. Assign privileges and enable remote access

Create a non-Administrator User Account for Security Analytics Log Collector

Note: The RSA Security Analytics Log Collector for version 10.2 only supports using local accounts with basic authentication. RSA Security Analytics 10.2 SP1 and above support using both local and domain accounts. Use domain accounts with negotiate authentication. Refer to **Windows Event Source Configuration Parameters** for details on how to enter the username and pick authentication mechanisms when configuring Security Analytics Log Collector.

If your event source is a part of a Windows domain, you must create this user account on the domain controller. If the event sources are not part of any domain, you must create this user account on each of the individual event sources.

To create a non-administrator user account for Security Analytics Log Collector:

1. On the event source, click **Start** > **Administrative Tools** > **Server Manager** to open the Server Manager console.
2. Use Server Manager to create a new user account with the following parameters.:

   Note: You must create one user account for each domain you want to collect. Ensure that there are no local accounts with the same user name.

Field	Description
User name	Enter a user name for the account, for example, logcollector
Full name	Enter a full name for the user account.
Description	Enter a description of the user account, for example, Account for remote collection of events in RSA Security Analytics Log Collector.

Field	Description
Password	Enter a strong password, and select **User cannot change password** and **Password never expires**.

Add the User Account to the Event Log Readers Local User Group

This group is a special-purpose user group created for accounts that are permitted only to read the events generated on a Windows machine. Perform these steps on all of the event sources from which you will be collecting events.

To add the user account to the Event Log Readers local user group:

1. Click **Start** > **Administrative Tools** > **Server Manager**.
2. Click **Configuration** > **Local Users and Groups** > **Groups**.
3. Double-click the **Event Log Readers** group.
4. Click **Add**, and add the user account that you created for the RSA Security Analytics Log Collector.
5. Click **OK** twice, and close the Server Manager console.

Provide the user name and password of this account when you are configuring the RSA Security Analytics Log Collector.

Assign Privileges and Enable Remote Access

Perform these steps on all of the event sources from which you will be collecting events.

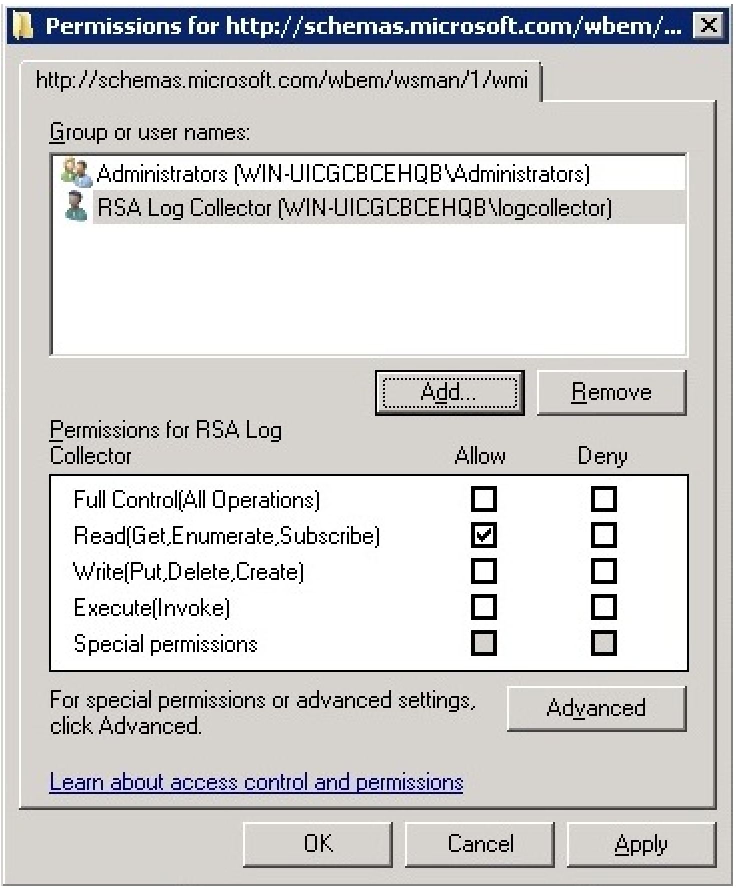
To assign privileges and enable remote access:

1. Assign privileges to the user account as follows:
   a. Open a command prompt, and type:

   ```
   winrm configsddl wmi
   ```

   Note: On Windows Server 2008 SP2, type `winrm configsddl`. Do not use the `wmi` parameter.

b. Grant **Read** permission to the user account.



Permissions for http://schemas.microsoft.com/wbem/...

http://schemas.microsoft.com/wbem/wsman/1/wmi

Group or user names:

- Administrators (WIN-UICGCBCEHQB\Administrators)
- RSA Log Collector (WIN-UICGCBCEHQB\logcollector)

Permissions for RSA Log Collector	Allow	Deny
Full Control(All Operations)	□	□
Read(Get,Enumerate,Subscribe)	☑	□
Write(Put,Delete,Create)	□	□
Execute(Invoke)	□	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

2. Enable remote access to the Windows Management Infrastructure (WMI) resource **Win32_AccountSID**, using the WMI Management console. Follow these steps:

   a. Open a command prompt, and type:

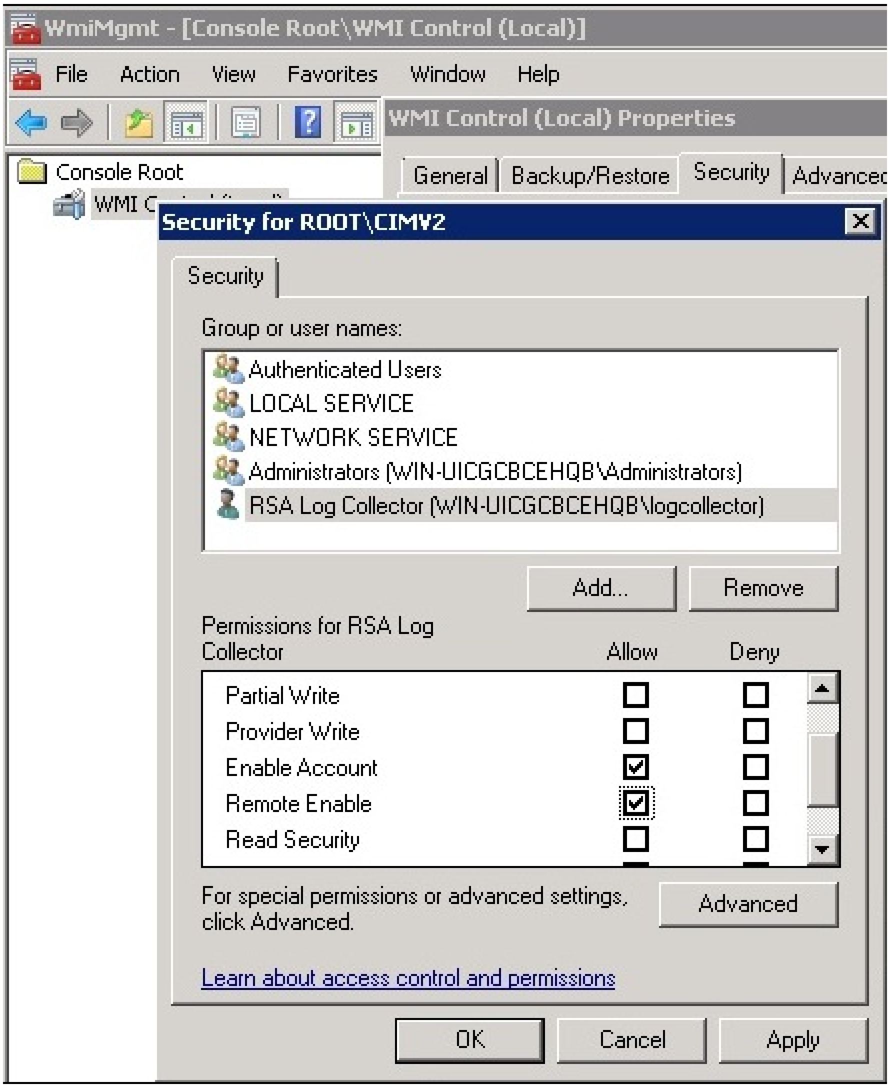
   ```
   wmimgmt
   ```

   b. Select the **Properties** icon, or right-click on **WMI Control**, and select **Properties**.

   c. In the **Security** tab, select **CIMV2**, and click **Security**.

   d. Add the user account to the list of groups and users.

   e. Grant the **Enable Account** and **Remote Enable** permissions to the user account.



Security for ROOT\CIMV2

Security

Group or user names:

- Authenticated Users
- LOCAL SERVICE
- NETWORK SERVICE
- Administrators (WIN-UICGCBCEHQB\Administrators)
- RSA Log Collector (WIN-UICGCBCEHQB\logcollector)

Permissions for RSA Log Collector	Allow	Deny
Partial Write	□	□
Provider Write	□	□
Enable Account	☑	□
Remote Enable	☑	□
Read Security	□	□

For special permissions or advanced settings, click Advanced.

Chapter 3: Enable Windows Remote Management over HTTP

If you want to use the RSA Security Analytics Log Collector to collect events from multiple Windows servers, you can use a Group Policy object or the manual method to deploy remote management to your servers over HTTP.

This section describes how to deploy WinRM over HTTP. It describes how to enable listeners on each event source from a central location. Use one of the following procedures to enable Windows Remote Management over HTTP:

- **Manually Enable WinRM over HTTP Using Windows Commands**
- **Use a Group Policy Object to Enable Windows Remote Management over HTTP**

Manually Enable WinRM over HTTP Using Windows Commands

You can manually configure multiple Windows event sources instead of Group Policy Object by following this procedure:

Note: To execute the manual procedure, you must use an account with Administrator privileges.

To enable Windows Remote Management Service over HTTP:

1. Ensure that you have followed the instructions to **Create a User Account for the RSA Security Analytics Log Collector**.
2. On the Windows server, open a command prompt, and type:

   ```
   winrm quickconfig
   ```

   When prompted to make changes, press Y.

   Note: If you are using a firewall other than Windows Firewall, you must open the firewall ports for HTTP manually.

3. To allow Basic authentication, change the default winrm setting for the "Auth/Basic" setting from false to true by entering the following:

   ```
   winrm set winrm/config/service/auth @{Basic="true"}
   ```

   For security reasons, RSA recommends that this be used only with https transport mode. Also, only local user accounts work with Basic.

4. To allow HTTP requests, change the default winrm setting for the **AllowUnencrypted** parameter, from **false** to **true**. Type:

   ```
   winrm set winrm/config/service @{AllowUnencrypted="true"}
   ```

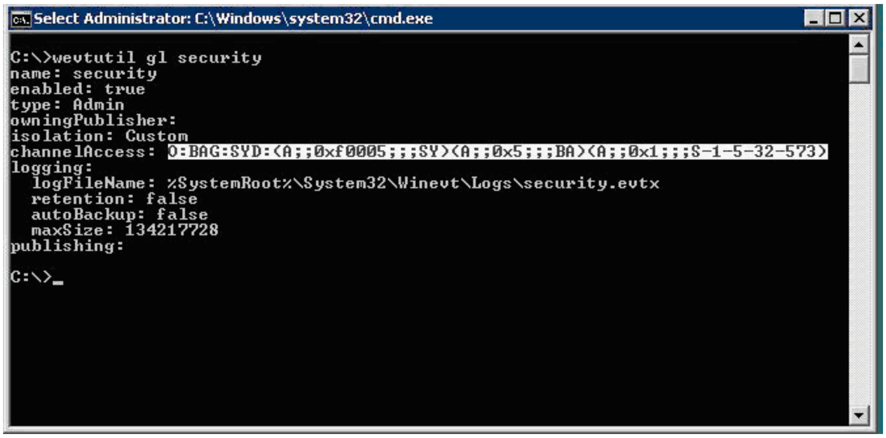
This command allows the WinRM Service to request unencrypted traffic. By default, the WinRM Service requires encrypted network traffic.

5. - To enable read access to the Security event log, while avoiding overwriting any existing Security channel settings, follow these steps:

   a. Open a command prompt, and type:

      wevtutil gl security

   b. Select and copy the existing SDDL string from the **channelAccess** parameter.
      The following figure shows an example.



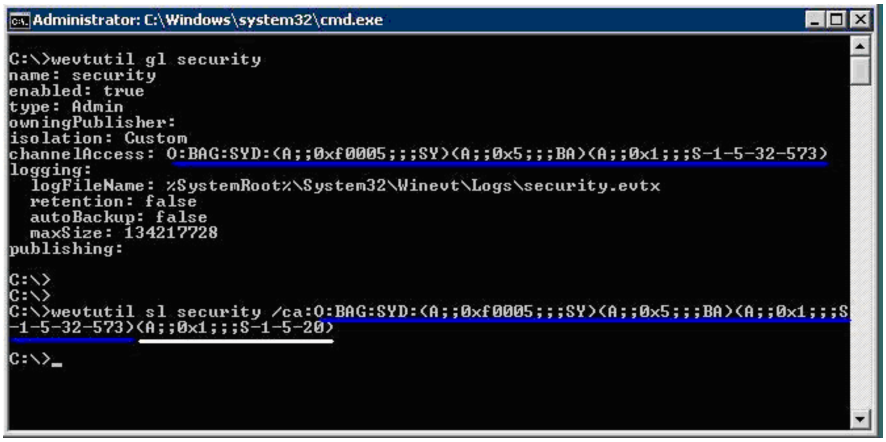
```
C:\>wevtutil gl security
name: security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\security.evtx
  retention: false
  autoBackup: false
  maxSize: 134217728
publishing:

C:\>_
```

   c. Execute the command below by pasting the copied string from the above step, and appending with the string, **(A;;0x1;;;S-1-5-20)**

      wevtutil sl security /ca:*existing-SDDL-string*(A;;0x1;;;S-1-5-20)

      where *existing-SDDL-string* is the string that you copied in step b.

      The following figure shows an example.



```
C:\>wevtutil gl security
name: security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\security.evtx
  retention: false
  autoBackup: false
  maxSize: 134217728
publishing:

C:\>
C:\>
C:\>wevtutil sl security /ca:O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S
-1-5-32-573)(A;;0x1;;;S-1-5-20)

C:\>_
```

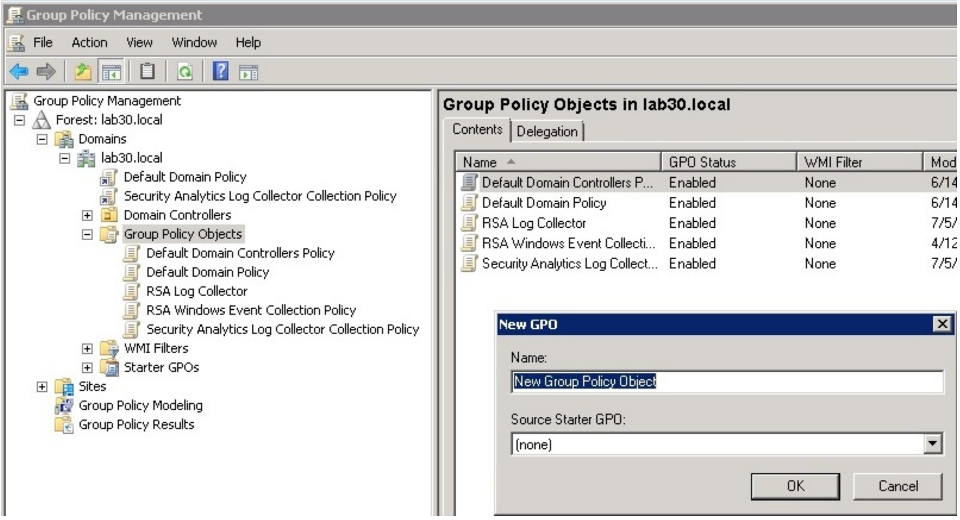
Use a Group Policy Object (GPO) to Enable Windows RM over HTTP

If you have a domain controller, you can use a Group Policy object to configure multiple Windows event sources instead of manually configuring event sources.

Note: The following instructions are general. For detailed steps, see the Microsoft documentation.

To configure unsecured communication using a Group Policy object:

1. Ensure that you have followed the instructions to Create a User Account for the RSA Security Analytics Log Collector.
2. To open the Group Policy Management Console on the domain controller, click **Start** > **Administrative Tools** > **Group Policy Management**, and, in the left-hand tree, browse to the **Group Policy Objects** folder for your domain.
3. Create a new Group Policy object, for example, Security Analytics Log Collector Collection Policy.



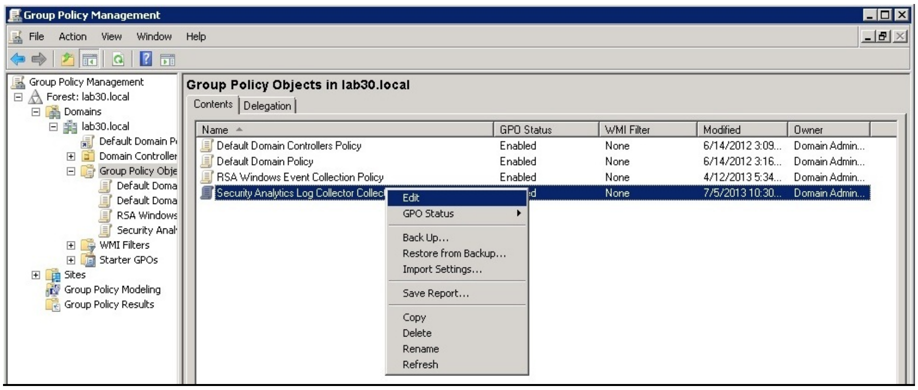
Group Policy Objects in lab30.local

Name	GPO Status	WMI Filter	Mod
Default Domain Controllers P...	Enabled	None	6/14
Default Domain Policy	Enabled	None	6/14
RSA Log Collector	Enabled	None	7/5/
RSA Windows Event Collecti...	Enabled	None	4/12
Security Analytics Log Collect...	Enabled	None	7/5/

Name: New Group Policy Object

Source Starter GPO: (none)

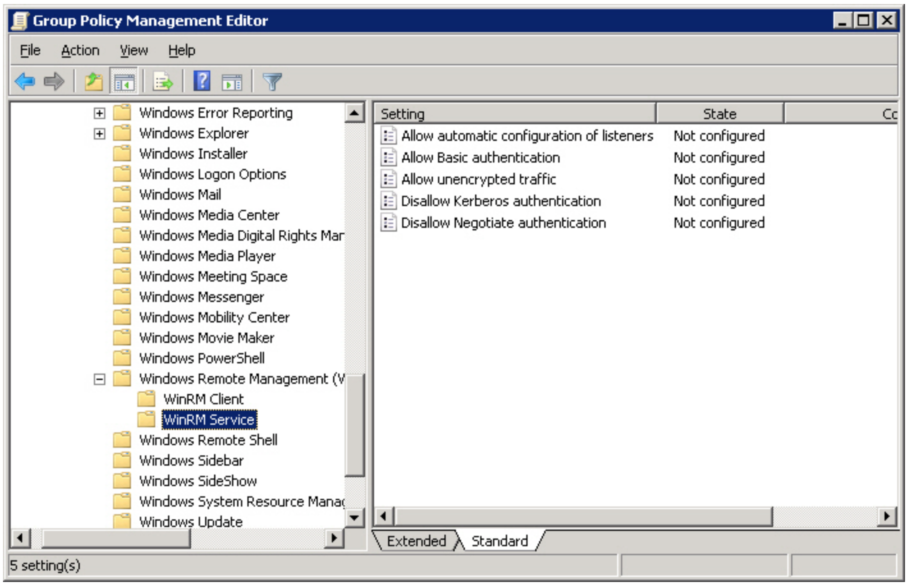
4. To edit the new Group Policy object, follow these steps:
   a. Right-click the newly created Group Policy object, and click **Edit**.



Group Policy Objects in lab30.local

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	6/14/2012 3:09...	Domain Admin...
Default Domain Policy	Enabled	None	6/14/2012 3:16...	Domain Admin...
RSA Windows Event Collection Policy	Enabled	None	4/12/2013 5:34...	Domain Admin...
Security Analytics Log Collector Collec	d	None	7/5/2013 10:30...	Domain Admin...

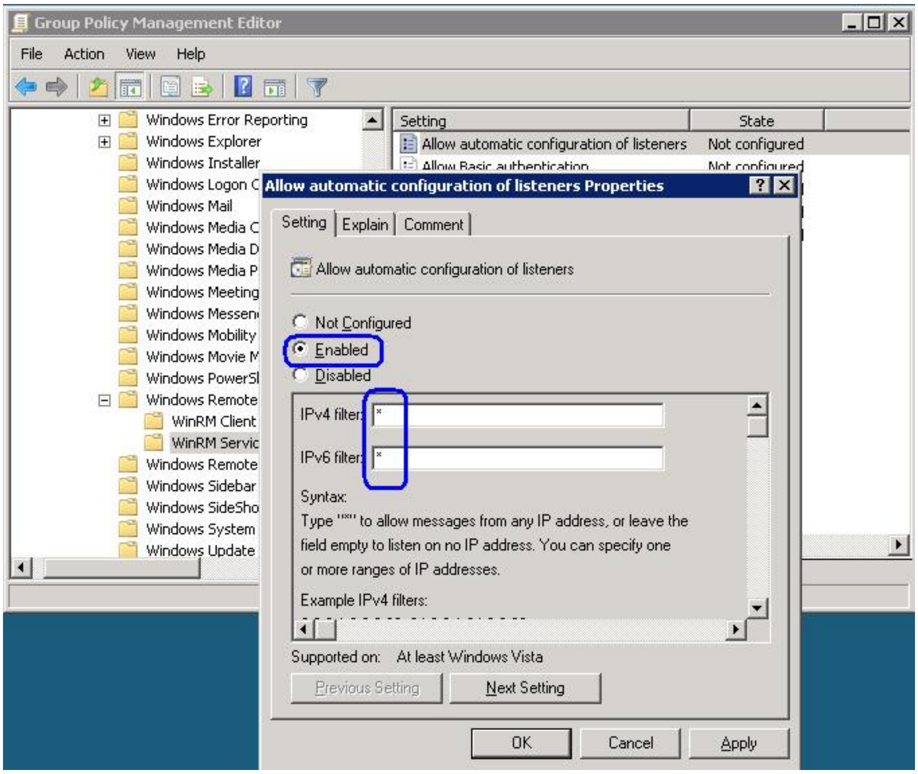
b. Expand **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components**, **Windows Remote Management (WinRM)**, and click **WinRM Service**.



Setting	State
Allow automatic configuration of listeners	Not configured
Allow Basic authentication	Not configured
Allow unencrypted traffic	Not configured
Disallow Kerberos authentication	Not configured
Disallow Negotiate authentication	Not configured

5 setting(s)

c. In the right-hand pane, double-click **Allow automatic configuration for listeners** to open the Properties dialog box. Select **Enabled**, and, in both the **IPv4** filters and **IPv6** filters fields, type *.



Allow automatic configuration of listeners

○ Not Configured
● Enabled
○ Disabled

IPv4 filter: *

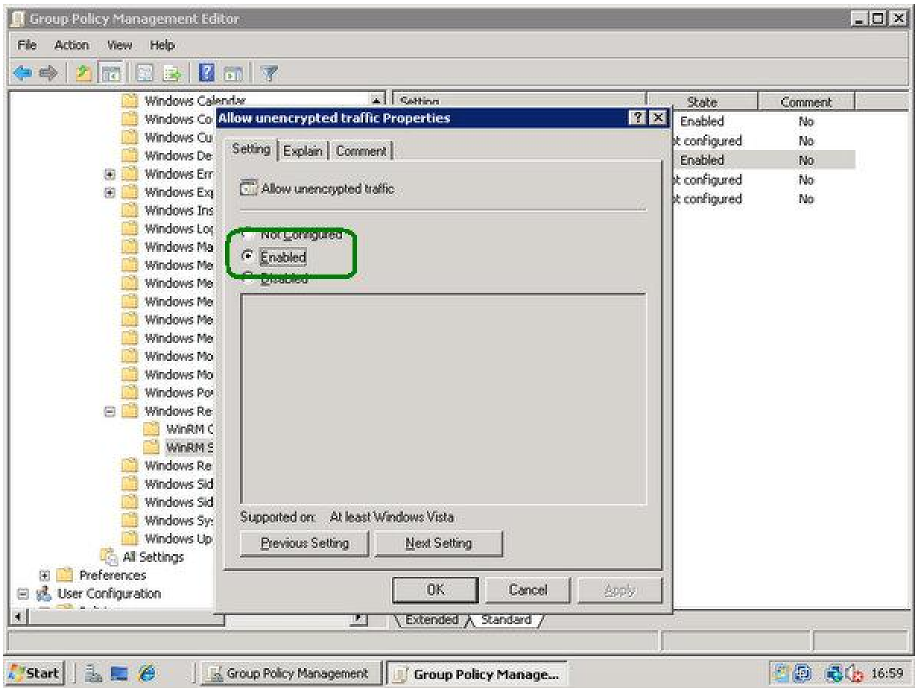
IPv6 filter: *

Syntax:
Type "*" to allow messages from any IP address, or leave the field empty to listen on no IP address. You can specify one or more ranges of IP addresses.

Example IPv4 filters:

Supported on: At least Windows Vista

d. Click **Next Setting** twice, and, in the Allow unencrypted traffic Properties dialog box, select **Enabled**.


Allow unencrypted traffic Properties

Allow unencrypted traffic

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Vista

e. Click **OK**.

5. To allow the WinRM service access to the Security log channel, follow these steps:

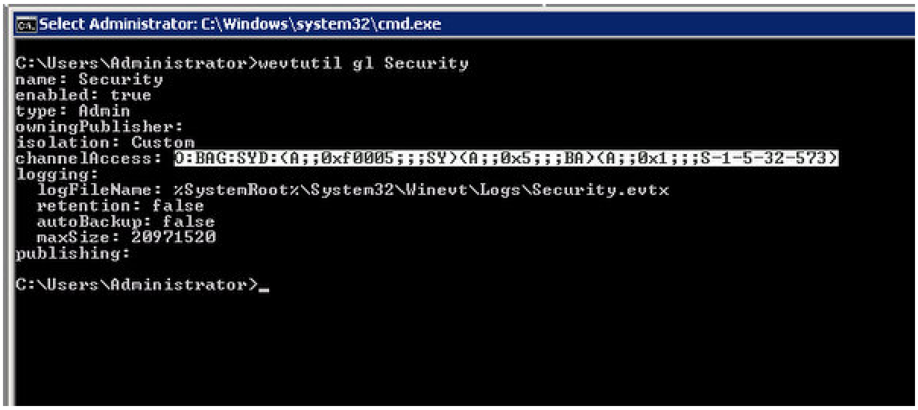
Note: The WinRM service requires explicit access to read events from the Security log channel. Access to Windows log channels are controlled using Security Descriptor Definition Language (SDDL) strings.

a. Without closing the Group Policy Management Editor window, click **Start** > **Run**, and type **cmd**.

b. To obtain the existing SDDL string from the domain controller, type:

```
wevtutil gl Security
```

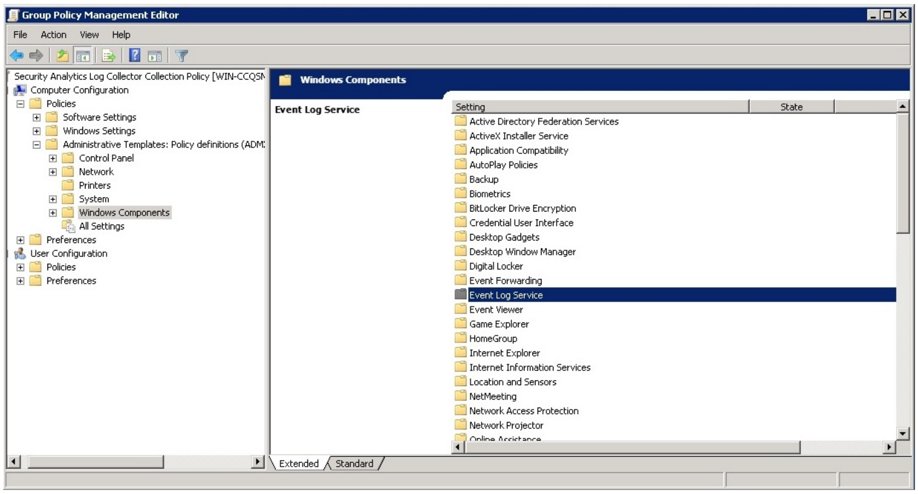
c. Copy the **channelAccess** string into the clipboard.



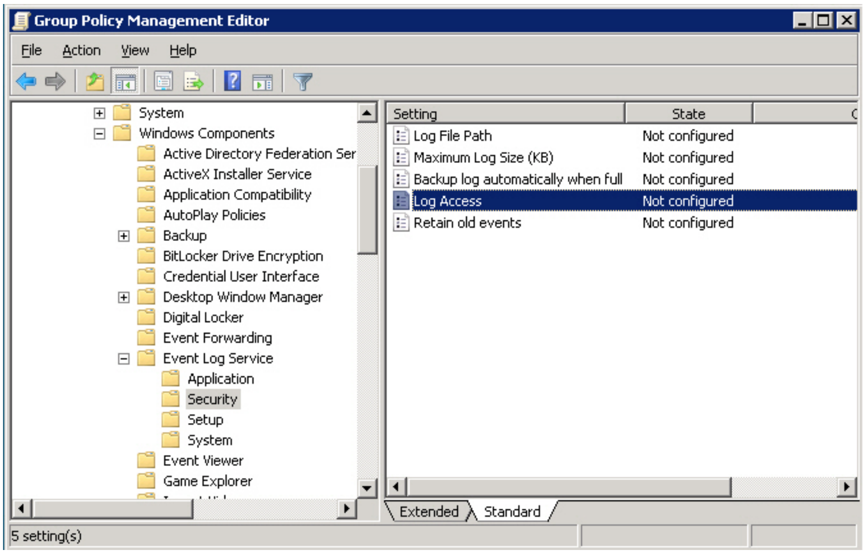
```
C:\Users\Administrator>wevtutil gl Security
name: Security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\Security.evtx
  retention: false
  autoBackup: false
  maxSize: 20971520
publishing:

C:\Users\Administrator>_
```

d. In the Group Policy Management Editor, expand **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Component**.

e. In the right-hand pane, double-click **Event Log Service**.



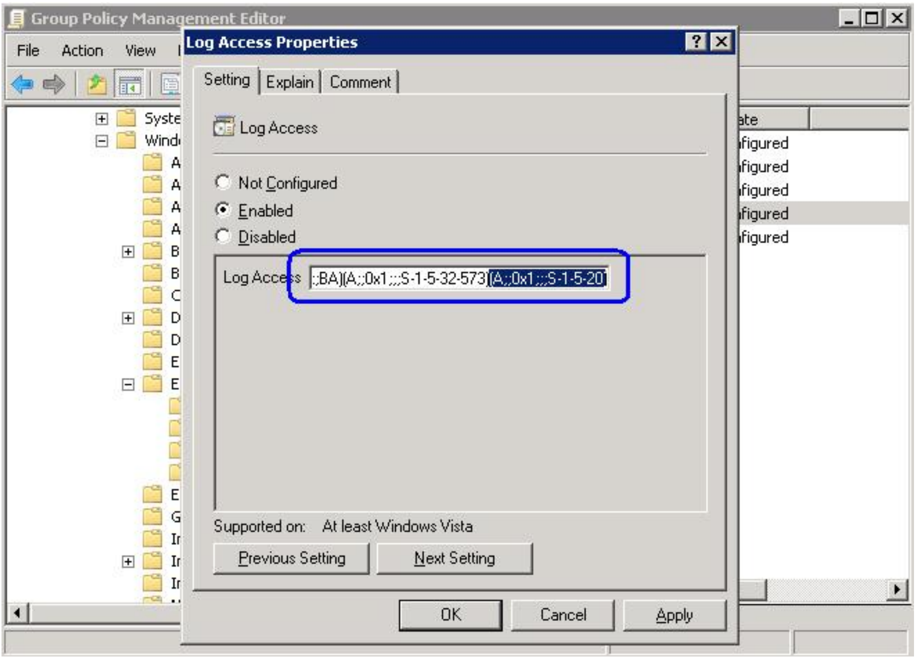
f. In the right-hand pane, expand **Security** in the left-hand pane, and double-click **Log Access**.



Setting	State
Log File Path	Not configured
Maximum Log Size (KB)	Not configured
Backup log automatically when full	Not configured
Log Access	Not configured
Retain old events	Not configured

g. Select **Enabled**, and, in the **Log Access** field, paste the security SDDL string that you copied in step 4 c, and append the following string: **(A;;0x1;;;S-1-5-20)**

Note: By appending the string to the existing SDDL string, you gain read access to the Security log channel, and avoid overwriting your existing settings.



○ Not Configured
● Enabled
○ Disabled

Log Access ;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)

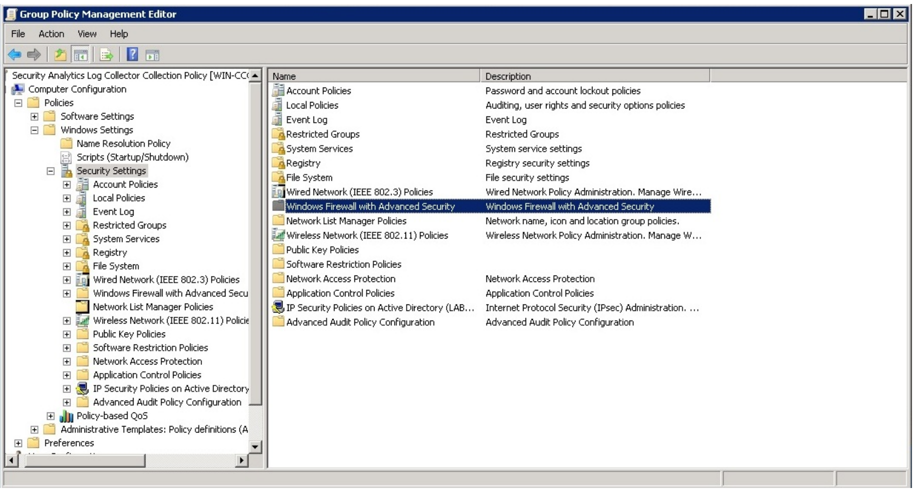
Supported on: At least Windows Vista

h. Click **OK**.

6. To create a new firewall rule, follow these steps:

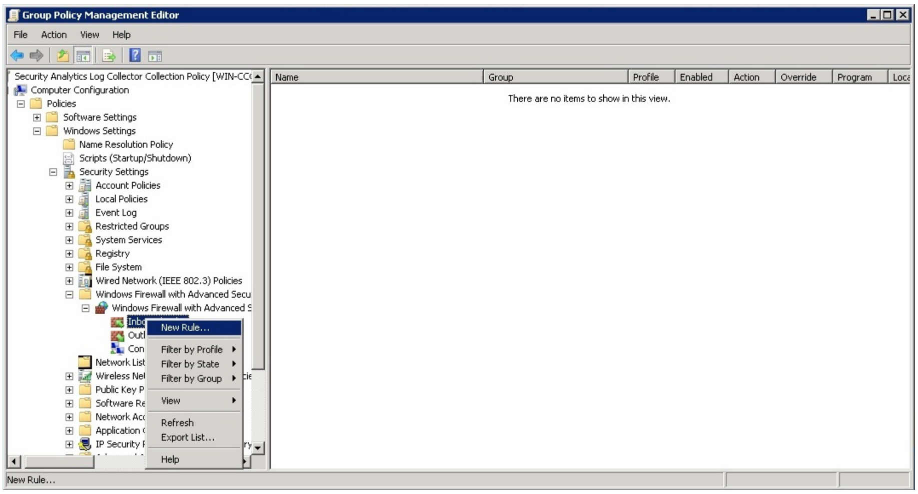
Note: This procedure is an example for Windows Firewall. If your organization uses another firewall, see the vendor documentation or your security officer for instructions.

a. Expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Windows Firewall with Advanced Security**.


Group Policy Management Editor
File
Action
View
Help
Security Analytics Log Collector Collection Policy [WIN-CC
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Policie
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (A
Preferences

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Event Log	Event Log
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File security settings
Wired Network (IEEE 802.3) Policies	Wired Network Policy Administration. Manage Wire…
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Wireless Network (IEEE 802.11) Policies	Wireless Network Policy Administration. Manage W…
Public Key Policies	
Software Restriction Policies	
Network Access Protection	Network Access Protection
Application Control Policies	Application Control Policies
IP Security Policies on Active Directory (LAB…	Internet Protocol Security (IPsec) Administration. …
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

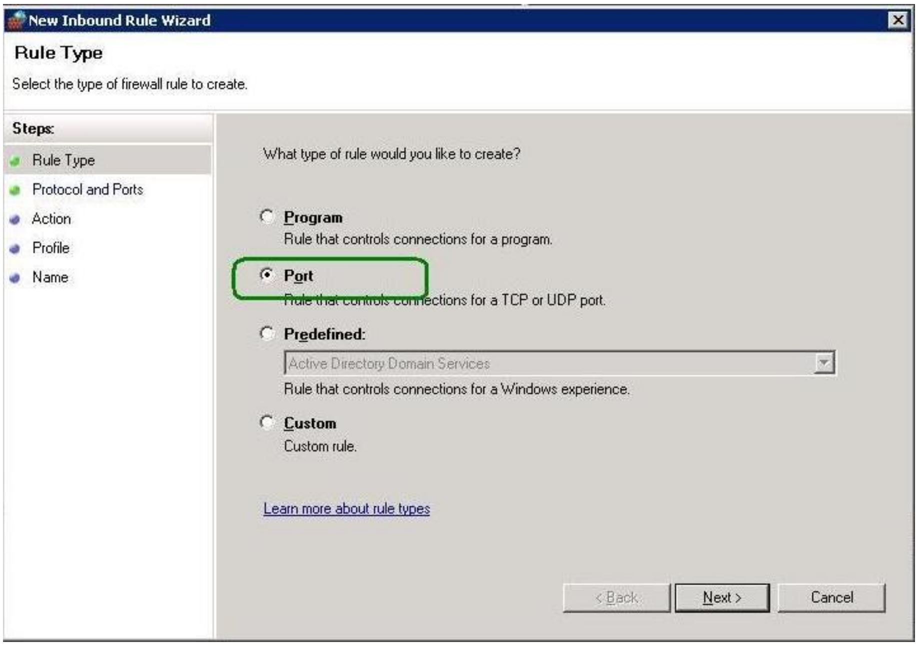
b. Expand **Windows Firewall with Advanced Security**, right-click **Inbound Rules**, and select **New Rule** to open the New Inbound Rule Wizard.



Name	Group	Profile	Enabled	Action	Override	Program	Loca

There are no items to show in this view.

c. Create a new firewall rule to allow WinRM traffic into event sources.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ Program
Rule that controls connections for a program.

● Port
Rule that controls connections for a TCP or UDP port.

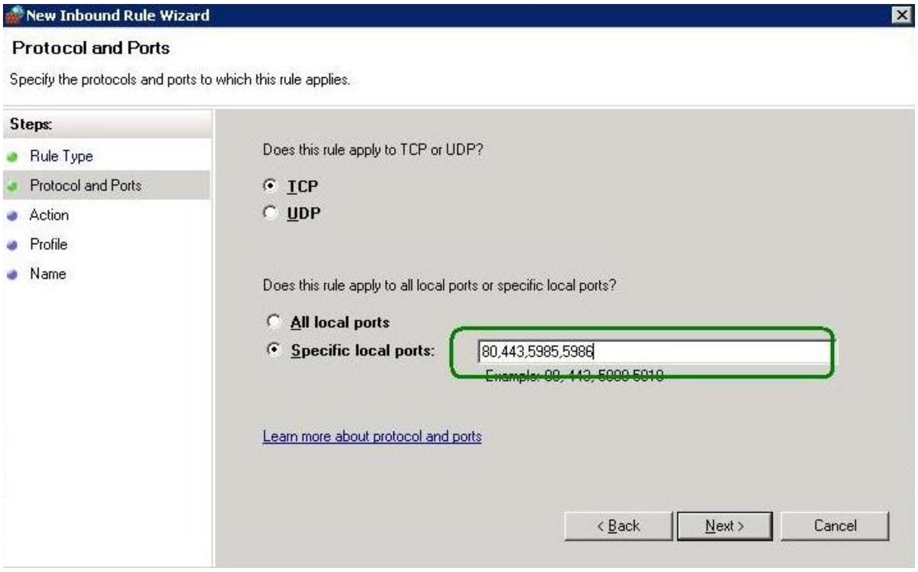
○ Predefined:
Active Directory Domain Services
Rule that controls connections for a Windows experience.

○ Custom
Custom rule.

d. Select **TCP**, and, in the **Specific local ports** field, enter the port numbers, separated by commas, for which you want to add the firewall rule.

By default, depending on the event source, the WinRM service uses the ports shown in the following table to enable collection using the RSA Security Analytics Log Collector.

Operating System	HTTP	HTTPS
Windows Server 2008	80	443
Windows 7, Windows Server 2008 R2 and Windows Server 2012	5985	5986



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

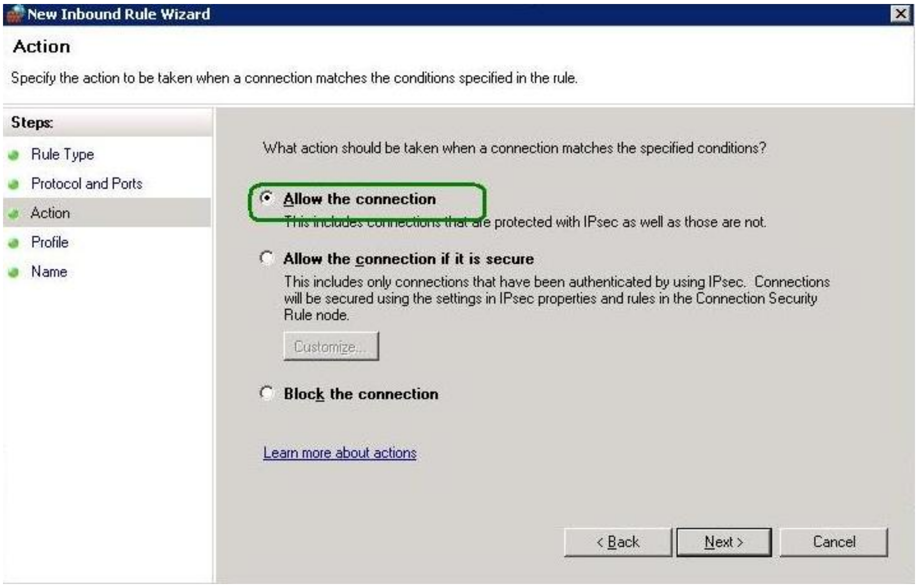
Does this rule apply to TCP or UDP?

● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 80,443,5985,5986
Example: 80, 443, 5000-5010

e. Select **Allow the connection**.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

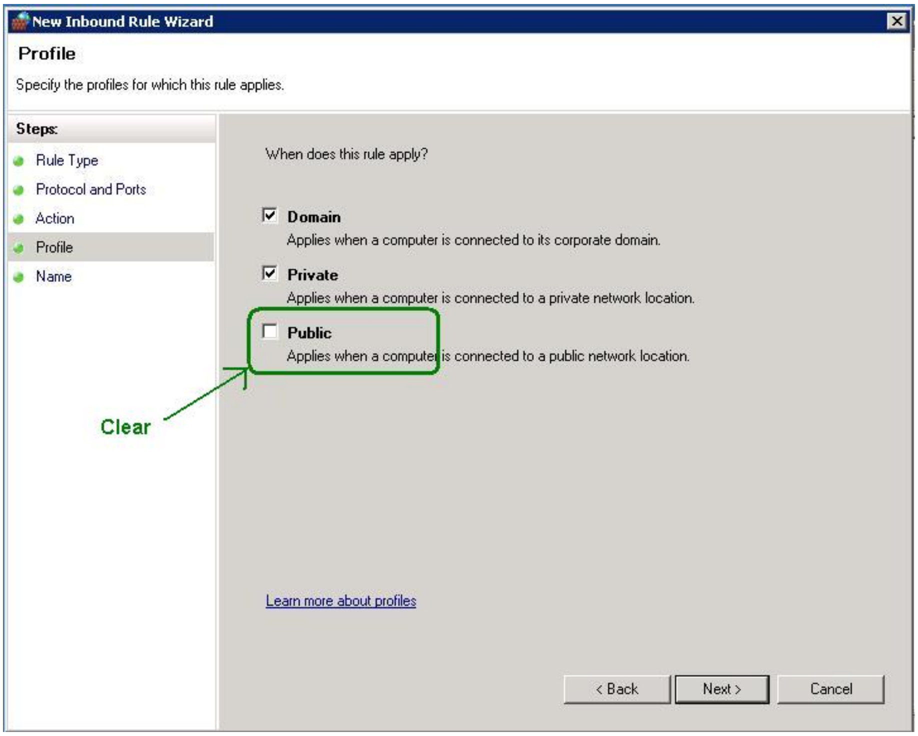
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

f. On the Profile page, clear **Public**. You do not need to open the ports for the public domain.



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

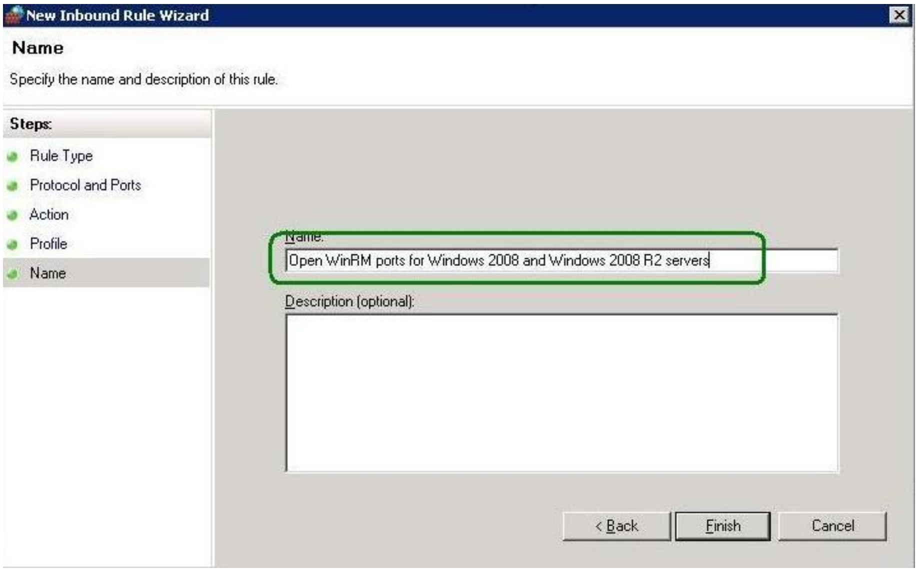
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

□ **Public**
Applies when a computer is connected to a public network location.

g. Specify an appropriate name for your firewall rule.



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

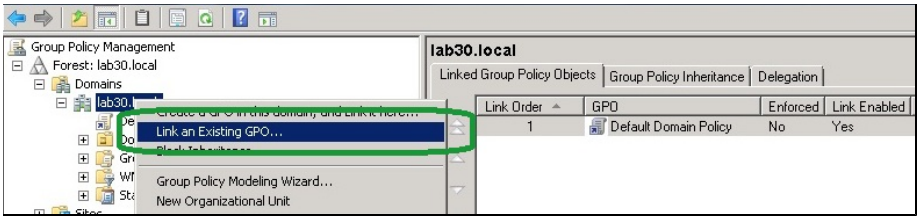
Name:
Open WinRM ports for Windows 2008 and Windows 2008 R2 servers

Description (optional):

h. Click **Finish**, and close the Group Policy Management Editor window.

7. To link the Group Policy object to the domain, follow these steps:

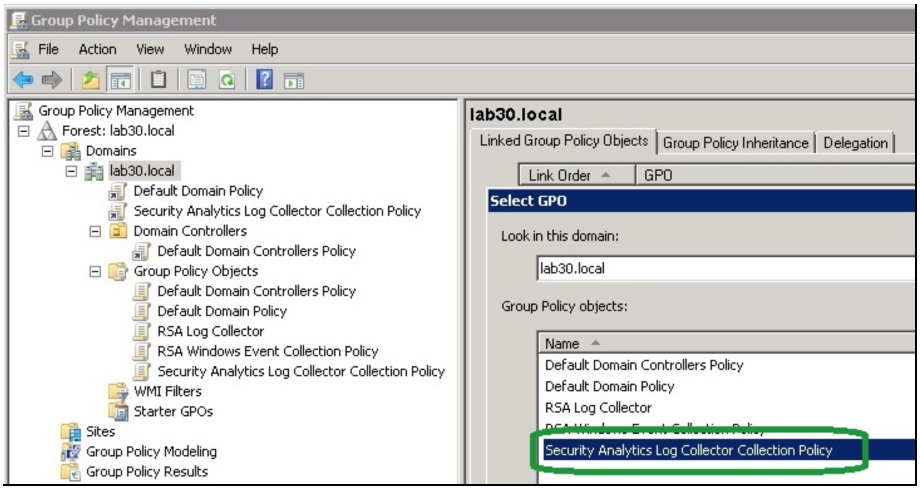
a. Right-click the domain, and click **Link an Existing GPO**.



lab30.local

Link Order	GPO	Enforced	Link Enabled
1	Default Domain Policy	No	Yes

b. Select the Group Policy object that you created.



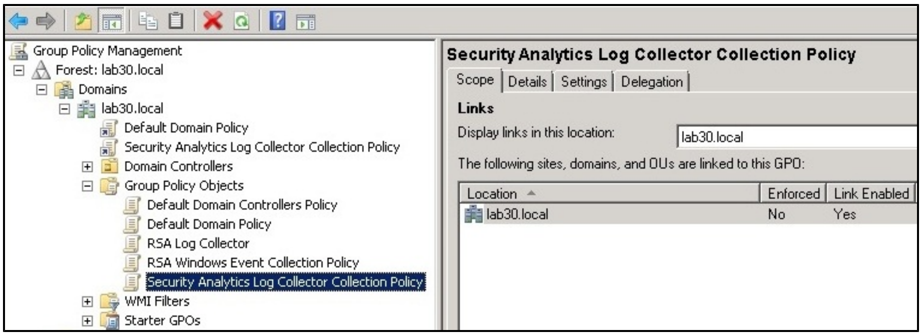
Select GPO

Look in this domain:
lab30.local

Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
RSA Log Collector
RSA Windows Event Collection Policy
Security Analytics Log Collector Collection Policy

A window similar to the following figure opens.


Group Policy Management
Forest: lab30.local
Domains
lab30.local
Default Domain Policy
Security Analytics Log Collector Collection Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
RSA Log Collector
RSA Windows Event Collection Policy
Security Analytics Log Collector Collection Policy
WMI Filters
Starter GPOs
Security Analytics Log Collector Collection Policy
Scope
Details
Settings
Delegation
Links

Display links in this location: lab30.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled
lab30.local	No	Yes

8. To enable and update the policy for all the hosts from which you want to collect events, do one of the following:
   - Run **gpupdate** on the individual event sources.
   - Wait for the Group Policy update to happen automatically on the hosts.

Chapter 4: Enable Windows Remote Management over HTTPS

If you want to use the RSA Security Analytics Log Collector to monitor multiple Windows servers, you can manually deploy remote management to your servers over HTTPS.

This section describes how to enable listeners on each event source from a central location. Before performing the tasks described in this section, make sure that you have already established an SSL connection.

Run the following procedures to enable Windows Remote Management over HTTPS:

I. **Provision an SSL Certificate and Extract the Thumbprint of the Certificate**

II. **Manually Enable Windows Remote Management over HTTPS**

Provision an SSL Certificate and Extract the Thumbprint of the Certificate

Before you can configure a WinRM listener to establish communication over HTTPS, you must provision an SSL certificate to the Windows system from which you will collect events.

To provision an SSL certificate:

Depending on whether you want to use a certification authority (CA) to issue the SSL certificate, do one of the following:

- If you want to use a CA to issue the SSL certificate, follow these steps:
  1. If you do not already have a CA, deploy a Microsoft Certification Authority within the domain in which the RSA Security Analytics Log Collector is installed, or purchase a third-party certification authority tool, such as Verisign or Thales.
  2. Use a central management tool, such as Microsoft Identity Lifecycle Manager (ILM), to issue an SSL certificate to the WinRM service running on each of the Windows servers from which the RSA Security Analytics Log Collector will collect events.
- If you do not want to use a CA to issue the SSL certificate, create a self-signed certificate for the WinRM service running on the Windows server from which the RSA Security Analytics Log Collector will collect events.

To extract the thumbprint of the certificate:

1. To install the Certificates Snap-in, follow these steps:
    a. On the event source, click **Start** > **Run**, type **mmc**, and click **OK**.
    b. Click **File** > **Add/Remove Snap-in**.
    c. Select **Certificates**, and click **Add**.
    d. Select **Computer Account**, and click **Next**.
    e. Select **Local Computer**, and click **Finish**.
    f. Click **OK** to return to the Console Root dialog box.
    g. Expand **Certificates (Local Computer)**.
2. Expand **Personal**, and click **Certificates**.
3. Double-click the SSL certificate that you provisioned.
4. Make sure that you have the thumbprint of the certificate available.
5. On the **Details** tab, in the list of fields, scroll down to **Thumbprint**, select the thumbprint, and copy the value.

Manually Enable Windows Remote Management over HTTPS

You can manually enable WinRM or create a script that runs these commands.

To enable Windows Remote Management Service over HTTPS:

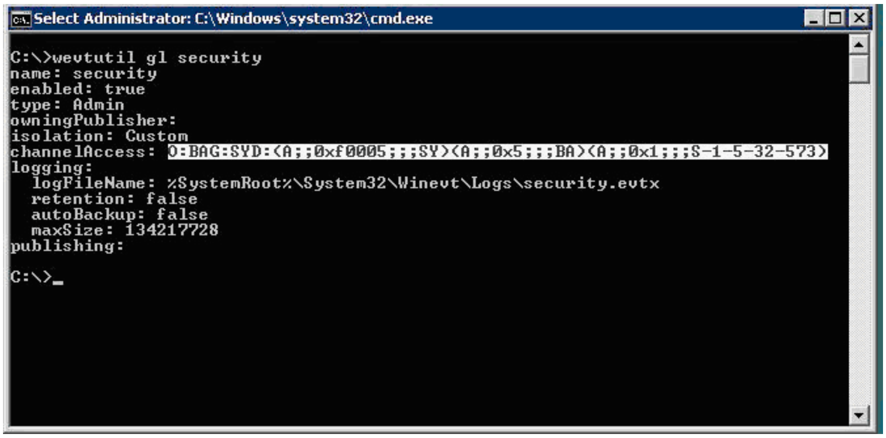
1. Ensure that you have followed the instructions to **Create a User Account for the RSA Security Analytics Log Collector**.
2. On the Windows server, open a command prompt, and type:

    ```
    winrm quickconfig
    ```

    When prompted to make changes, press Y.
3. - To enable read access to the Security event log, while avoiding overwriting any existing Security channel settings, follow these steps:
        a. Open a command prompt, and type:

        ```
        wevtutil gl security
        ```

        b. Select and copy the existing SDDL string from the **channelAccess** parameter.
        The following figure shows an example.



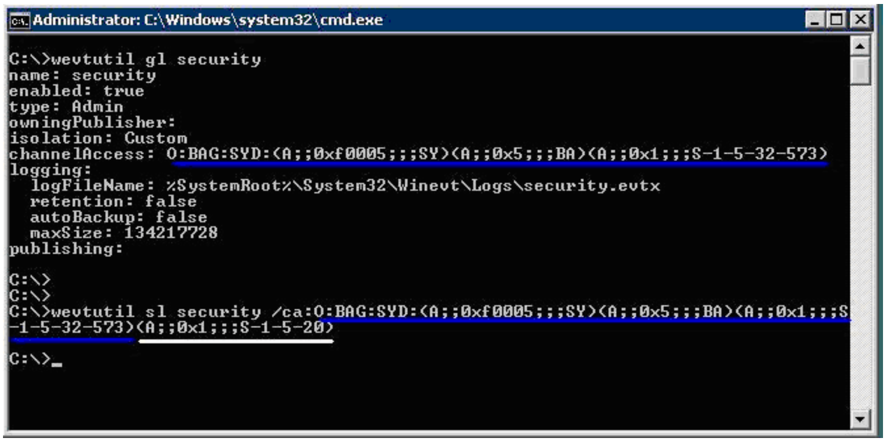
```
C:\>wevtutil gl security
name: security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\security.evtx
  retention: false
  autoBackup: false
  maxSize: 134217728
publishing:

C:\>_
```

c. Execute the command below by pasting the copied string from the above step, and appending with the string, **(A;;0x1;;;S-1-5-20)**

wevtutil sl security /ca:*existing-SDDL-string*(A;;0x1;;;S-1-5-20)

where *existing-SDDL-string* is the string that you copied in step b.

The following figure shows an example.



```
C:\>wevtutil gl security
name: security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\security.evtx
  retention: false
  autoBackup: false
  maxSize: 134217728
publishing:

C:\>
C:\>
C:\>wevtutil sl security /ca:O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S
-1-5-32-573)(A;;0x1;;;S-1-5-20)

C:\>_
```

4. On the Windows server, follow these steps to enable event collection over a secure connection:

   a. Obtain an SSL certificate for the event source.

   Note: Keep the certificate thumbprint available, as you need it for the next step.

   b. On the event source, to create an HTTPS listener, to enable event collection over the Secure channel, open a command prompt, and type:

   winrm create winrm/config/listener?Address=*+Transport=HTTPS @ {Hostname="hostname";CertificateThumbprint="thumbprint"}

For information on how to extract the thumbprint of the certificate, see **Extract the thumbprint of the certificate**.

Note: If you copy this command, be sure to paste it and run it as a single line. Also, if you copy the command, make sure that there is a space between HTTPS and @.

c. Open the firewall port for the HTTPS transport by adding a new firewall Incoming rule that allows the WinRM ports. Follow these steps:

Note: If you are using a firewall other than Windows Firewall, you must open the firewall ports for HTTPS manually.

i. Click **Start** > **Administrative Tools** to launch Server Manager.

ii. Expand **Server Manager** > **Configuration** > **Windows Firewall with Advanced Security** > **Inbound Rules**.

iii. Right-click on **Inbound Rules**, and select **New Rule**.

iv. In the New Inbound Rule Wizard, select **Port** for the **Rule Type**, and click **Next**.

v. On the Protocol and Ports page, ensure that **TCP** is selected, and in the **Specific local ports** field, enter the port number for WinRM over HTTPS. For example, the default ports are 443 on Windows Server 2008 hosts and 5986 on Windows Server 2008 R2 and 2012 hosts.

vi. On the Action page, click **Next**.

vii. On the Profile page, click **Next**.

viii. Specify a name for the rule, for example, **Open ports for WinRM over HTTPS**, and click **Finish**.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**. Published in the USA.