RSA NETWITNESS® PLATFORM

Microsoft WinRM Configuration

Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

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 EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

March 2019

Contents

Introduction **4**

When to Use the winrmconfig Script 4

Troubleshoot Collection Issues in Report Mode **5**

winrmconfig as a Configuration Tool **6**

Enable HTTP or HTTPS Listeners 6

Enable Access to the Security Event Log 6

Permissions to Access the Windows WMI Subsystem Remotely 6

Permissions to Access the WinRM WMI Plugin 7

Add User as a Member of Event Log Readers Group 7

Network Service Account to Access the Security Event Log 7

Running the winrmconfig Script on a Single System **8**

winrmconfig Modes **9**

Report Mode 9

Enable Mode 10

Other Script Options **12**

WinRM Compatible Certificates used with HTTPS Listeners 12

WinRM Over HTTPS with Mutual Authentication 13

Group Policy Method for Mass-enabling WinRM **16**

WinRM over HTTPS SSL Certificate Deployment 16

Create Certificate Templates 17

Link Certificate Templates to Group Policies 22

Create GPO to Push the winrmconfig Script 25

Firewall Information **29**

Systems running Windows built-in Firewall 29

Other Firewall Considerations 29

Introduction

This document provides information for configuring the Windows WinRM (Windows Remote Management) service to allow RSA NetWitness to collect event logs from Microsoft Windows machines. In this document, the word "Collector" refers to either the RSA NetWitness Log Collector or the Virtual Log Collector. The word “Channel” refers to a Windows event log, for example, Security, System, Forwarded Event, or DNS.

This topic also documents the requirements and permissions to collect events and SIDs (Security Identifiers displayed in the events which can be translated to human user and group names by RSA NetWitness) from a system using a non-administrative account. RSA recommends using a non-administrator account for the collection user. You can perform the steps to create these permissions manually on each target system, or you can use a Group Policy Object (GPO). You can also use an RSA-supplied PowerShell script to accomplish these tasks either manually on each Windows system or as a logon script via a GPO to apply the same configuration across a broad number of systems. This is described in this document in Group Policy Method for Mass-enabling WinRM.

Note: RSA recommends that you test the script first by running it manually on a test machine in a lab to observe what it does, before pushing it out on a large scale across multiple systems via GPO.

You can use the PowerShell script (**winrmconfig**) to:

- Automate all of the steps to create a WinRM Listener that accepts requests from a collector
- Enable system access to the Security event log (in order to read Security Event logs via WinRM)
- Create user permissions, as well as other features

You can download the script from RSA Link here: https://community.rsa.com/docs/DOC-58018.

When to Use the winrmconfig Script

The winrmconfig script can be used in the following ways:

- Troubleshoot collection issues with **report** mode. For information, see Troubleshoot Collection Issues in Report Mode
- Configuration tool to enable HTTP or HTTPS listeners, enable security log access, create user permissions to access WMI remotely and access the WinRM WMI plugin (for SID enumeration). For information, see winrmconfig as a Configuration Tool
- Push the script via GPO to multiple systems. For information, see Group Policy Method for Mass-enabling WinRM

Troubleshoot Collection Issues in Report Mode

You can use the script in **report** mode to troubleshoot issues with WinRM collection. **report** mode is described in detail in later in this document in Report Mode. (More troubleshooting details can be found in Test and Troubleshoot Microsoft WinRM, which is located on RSA Link, in the Event Source Configuration Guides space).

winrmconfig as a Configuration Tool

When you use the script as a configuration tool, you have all the capabilities of report mode plus the ability to configure WinRM and to make updates to fix issues.

Enable HTTP or HTTPS Listeners

Because WinRM is a web-based protocol, you can create a listener for HTTP, HTTPS, or both protocols. (Although it makes little sense to use both, if HTTPS is required, all clients, such as RSA NetWitness, should use that protocol). HTTP is simple, with only one real option, port selection, which is by default 5985 for HTTP, and 5986 for HTTPS. WinRM listens on these ports for all interfaces. An HTTPS listener requires a certificate, much like a web server serving HTTPS pages does. This certificate must have sufficient Enhanced Key Usage (EKU) bits enabled (it must have at least the Server Authentication EKU; for more information, see https://support.microsoft.com/en-us/kb/2019527). This is needed to allow WinRM to create the listener. Also, the certificate's **Subject** field must be the FQDN of the system. In WinRM terms, a viable certificate is said to be bound to the listener port that is selected. In **enable** mode, the **winrmconfig.ps1** script can create either HTTP or HTTPS listeners (provided a viable certificate is found).

Enable Access to the Security Event Log

In **enable** mode, the script will automatically enable the local Windows Network Service account to access the Security Event log. This is an important step because Windows Security Events are probably the most critical data that RSA NetWitness collects. The Windows Remote Management service in the services panel uses the Network Service account by default. You can check this by right-clicking the WinRM service, selecting **Properties**, and clicking the **Logon** tab. The script modifies the Access Control List (ACL) for the security event log and adds the account to it.

Permissions to Access the Windows WMI Subsystem Remotely

In **enable** mode, the script configures permissions to access the Windows WMI subsystem remotely, which is the equivalent of using the **wmimgmt** Windows application to enable remote access to the WMI root/CIM namespace (see Test and Troubleshoot Microsoft WinRM on RSA Link for more details). The script uses the Windows Security API to create an Access Control Entry (ACE) for the collection user in WMI with remote access permissions, which allows remote collection of events.

Permissions to Access the WinRM WMI Plugin

In **enable** mode, the script configures permissions to access the WinRM WMI plugin, which is the equivalent of running the Windows **winrm configsddl WMI** command to enable read access to the WinRM WMI plugin. Without this permission, the user account cannot be used to enumerate SIDs, and there would be no translation of SID strings to user/group names within certain event log message types, which are useful in reports and investigations.

Add User as a Member of Event Log Readers Group

In order to read events from event logs, the Collection user must be part of the following groups:

- The Domain-level Event Log Readers group if collecting from a domain controller.
- The local Event Log Readers group if collecting from a non-domain controller member server or a standalone machine (not a part of a domain).

The script adds the user to the correct Event Log Readers group, regardless of the type of machine it is running on (if the user has not already been added).

Network Service Account to Access the Security Event Log

As stated above, collecting security event logs is a key source of event data for RSA NetWitness. By default, the WinRM service which runs as the **Network Service** account does not have access to the security event logs. The script uses the **wevtutil** Windows command to grant Network Service access (see Test and Troubleshoot Microsoft WinRM on RSA Link for more details).

Running the winrmconfig Script on a Single System

The **winrmconfig.ps1** PowerShell script can be run with either of the following syntaxes

```
Powershell -command "c:\temp\winrmconfig.ps1 -Action report -User
mycollectionuser@mydomain.com"
```

Notice the double quotes around the command and arguments and the full path to the script location.

```
Powershell -File winrmconfig.ps1 -Action report -User mycollectionuser@mydomain.com
```

Note: Notice that there are no double quotes around the command and arguments and no requirement for a full path to the script location.

winrmconfig Modes

winrmconfig operates in two modes, **report** mode (used mainly for troubleshooting) and **enable** mode. The difference between the two modes is that **report** mode makes no changes. It runs a list of checks and reports back from each check with text in green (good), yellow (warnings), and red (errors).

In **enable** mode, the script attempts to fix any issue that could prevent collection and queries for SIDs, whether there is a listener-related issue if the **-ListenerType** command is specified on the command line, or an issue with user permissions, if **-User** is specified.

To select a mode, use the **-Action** command, for example:

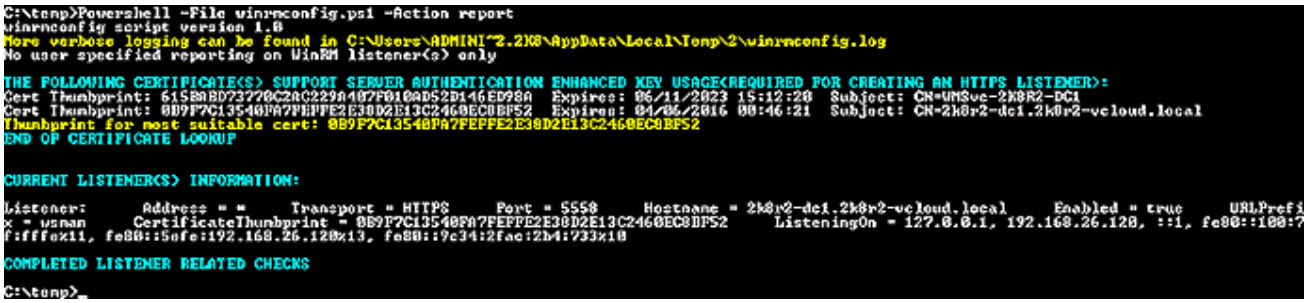
```
-Action report
```

or

```
-Action enable.
```

Report Mode

This mode returns the listener states via the **-Action report** command, as shown below:



The report above returns information on the available certificates that might be used when creating an HTTPS listener, with a recommendation on which to choose, and also information on any currently configured listener(s). Adding the collection user account as shown below using the **-User** parameter yields information on the collection user account.

```
C:\temp>Powershell -File winrmconfig.ps1 -Action report -User newcoluser@2k8r2-vcloud
winrmconfig script version 1.0
More verbose logging can be found in C:\Users\ADMINI~2.2K8\AppData\Local\Temp\2\winrmconfig.log

THE FOLLOWING CERTIFICATE(S) SUPPORT SERVER AUTHENTICATION ENHANCED KEY USAGE(REQUIRED FOR CREATING AN HTTPS LISTENER):
Cert Thumbprint: 615BABD73770C2AC229A407F010AD52D146ED98A  Expires: 06/11/2023 15:12:20  Subject: CN=WMSvc-2K8R2-DC1
Cert Thumbprint: 0B9F7C13540FA7FEFFE2E38D2E13C2460EC8BF52  Expires: 04/06/2016 00:46:21  Subject: CN=2k8r2-dc1.2k8r2-vclou
Thumbprint for most suitable cert: 0B9F7C13540FA7FEFFE2E38D2E13C2460EC8BF52
END OF CERTIFICATE LOOKUP


CURRENT LISTENER(S) INFORMATION:

Listener:      Address = *     Transport = HTTPS     Port = 5558     Hostname = 2k8r2-dc1.2k8r2-vcloud.local     Enabled =
x = usman     CertificateThumbprint = 0B9F7C13540FA7FEFFE2E38D2E13C2460EC8BF52     ListeningOn = 127.0.0.1, 192.168.26.120
f:fffex11, fe80::5efe:192.168.26.120%13, fe80::9c34:2fac:2b4:733%10

SECURITY LOG ACCESS FOR NETWORK SERVICE ACCOUNT CHECK BEGINS(WINRM SERVICE USES THIS ACCOUNT TO READ EVENT LOGS)
Network Service SID is already added to the Security Channel ACL (Security Analytics can collect Security Event logs using
8r2-vcloud account)

SECURITY LOG ACCESS FOR NETWORK SERVICE ACCOUNT CHECK ENDS
COLLECTION USER RIGHTS CONFIGURATION BEGINS...

Checking access to the WinRM WMI Plugin (necessary for SID resolution)
User: newcoluser@2k8r2-vcloud with SID: S-1-5-21-4205194981-1966238051-3092141446-72291 is not part of the WinRM WMI Plugi
would not be possible using this account)
Checking access to the CIM Root (necessary for Event log collection)
User newcoluser@2k8r2-vcloud with SID: S-1-5-21-4205194981-1966238051-3092141446-72291 is already enabled
for WMI access via WinRM (Security Analytics can collect Event logs using this account)

Checking user newcoluser@2k8r2-vcloud membership to the Event Log Readers group
User newcoluser@2k8r2-vcloud is already a member of Event Log Readers group

COLLECTION USER RIGHTS CHECK ENDS HERE...


C:\temp>_
```

This output displays the following information:

1. Certificate information (including the recommended certificate for the HTTPS listener).
2. Current listener information (necessary for the collector to access the service remotely).
3. Current access to the security log for the Network Service account.
4. Access to the WinRM WMI plugin (required for SID enumeration). Note the warning that the user is not in the plugin's ACL list.
5. Current access to the WMI root (for event log collection). Note that it states in green (for good) that the user is already in that ACL.
6. Finally, a check is made to verify if the user is a member of the domain or local Event Log Readers group, whichever applies to the current system.

If all responses are green, everything is good. Event collection and SID enumeration are configured and are ready to use.

Enable Mode

In the **-Action enable** mode, the script can correct issues automatically or create a new configuration (for example, a new listener). In this mode, the steps are the same as for the **report** mode (it has the same features as **report** mode, and it makes updates to fix any issues).

As in **report** mode, a user can be omitted (see number 4 above), so the script only checks and enables a listener based on the arguments that are passed in.

The example below shows the results of running the following command:

```
Powershell -File winrmconfig.ps1 -Action enable -ListenerType https -User newcoluser@2k8r2-
vcloud
```

```
winrmconfig script version 1.0
More verbose logging can be found in C:\Users\ADMINI~2.2K8\AppData\Local\Temp\2\winrmconfig.log

THE FOLLOWING CERTIFICATE(S) SUPPORT SERVER AUTHENTICATION ENHANCED KEY USAGE(REQUIRED FOR CREATING AN HTTPS LISTENER):
Cert Thumbprint: 615BADD73770C2AC229A407F010AD52D146ED90A  Expires: 06/11/2023 15:12:20  Subject: CN=VMSvc-2K8R2-DC1
Cert Thumbprint: 0B9F7C13540FA7FEFFE2E38D2E13C2460EC8BF52  Expires: 04/06/2016 00:46:21  Subject: CN=2k8r2-dc1.2k8r2-vcloud.local
Thumbprint for most suitable cert: 0B9F7C13540FA7FEFFE2E38D2E13C2460EC8BF52
END OF CERTIFICATE LOOKUP


Discovered HTTPS Listener on port 5999

HTTPS Listener requested
HTTPS Listener already configured on port 5999 which is different than selected: 5986 so deleting...
Attempting to delete the existing HTTPS Listener on port 5999
Creating HTTPS Listener with: thumbprint 0B9F7C13540FA7FEFFE2E38D2E13C2460EC8BF52 Port 5986 FQDN 2k8r2-dc1.2k8r2-vcloud.local
HTTPS listener created successfully on port 5986
Removing the Allow unencrypted setting while creating HTTPS Listener (for added Security)
Skipping firewall rule for port 5986 inbound access as the firewall service is not running

CURRENT LISTENER(S) INFORMATION:

Listener:      Address = *      Transport = HTTPS      Port = 5986      Hostname = 2k8r2-dc1.2k8r2-vcloud.local      Enabled = true      URLPrefi
x = wsman      CertificateThumbprint = 0B9F7C13540FA7FEFFE2E38D2E13C2460EC8BF52      ListeningOn = 127.0.0.1, 192.168.26.120, ::1, fe80::100:7
f:fffe%11, fe80::5efe:192.168.26.120%13, fe80::9c34:2fac:2b4:733%10


Configuring security event log access for the NETWORK SERVICE accout (WinRM Service uses this account to read event logs)
Network Service SID is already added to the Security Channel ACL (Security Analytics can collect Security Event logs using the newcoluser@2k
8r2-vcloud account)

SECURITY LOG ACCESS FOR NETWORK SERVICE ACCOUNT CHECK ENDS
COLLECTION USER RIGHTS CHECK BEGINS HERE...

Checking access to the WinRM WMI Plugin (necessary for SID resolution)
User: newcoluser@2k8r2-vcloud with SID: S-1-5-21-4205194981-1966230051-3092141446-72291 is not part of the WinRM WMI Plugin (SID resolution
would not be possible using this account) so adding to SDDL...
Created new WMI Plugin SDDL with newcoluser@2k8r2-vcloud's SID
Checking access to the CIM Root (necessary for Event log collection)
User newcoluser@2k8r2-vcloud with SID: S-1-5-21-4205194981-1966230051-3092141446-72291 is already enabled
for WMI access via WinRM (Security Analytics can collect Event logs using this account)

Checking user newcoluser@2k8r2-vcloud membership to the Event Log Readers group
User newcoluser@2k8r2-vcloud is already a member of Event Log Readers group

COLLECTION USER RIGHTS CHECK ENDS HERE...

Changes have been made that require a WinRM Service restart, restarting...
WinRM Service restarted.
```

Now that the script is in **enable** mode, an HTTP, or in this case an HTTPS listener, can be created. A **-Port** option was not passed to the script, so the default port number of 5986 is assumed for HTTPS. The script first confirms that the certificate is correct, and then deletes the old listener and creates the new one on the requested port.

The script continues by checking access to the Security Event log, and detects that the Network Service account is already added to the ACL for the Security Event log.

The script then checks access to the WMI WinRM plugin. Note that the example shows text in yellow, which is warning-level and states that RSA NetWitness would not be able to collect SIDs. In the following few lines, the script corrects this, and in green text (for good results) states that it created a new WMI Plugin SDDL. Note that this action requires a restart of the **winrm** service, which it does at the end.

Next, the script checks the WMI Remote privileges for the Collection user. This step is critical in collecting events remotely. Without it, the RSA NetWitness Collector could not collect event logs. In this case, the check results in a green message, stating that this step was already completed.

Finally, the script enables user permissions to read the events by adding the user to the Event Log Readers group. The script does this whether the system is a standalone machine, a domain member, or a domain controller.

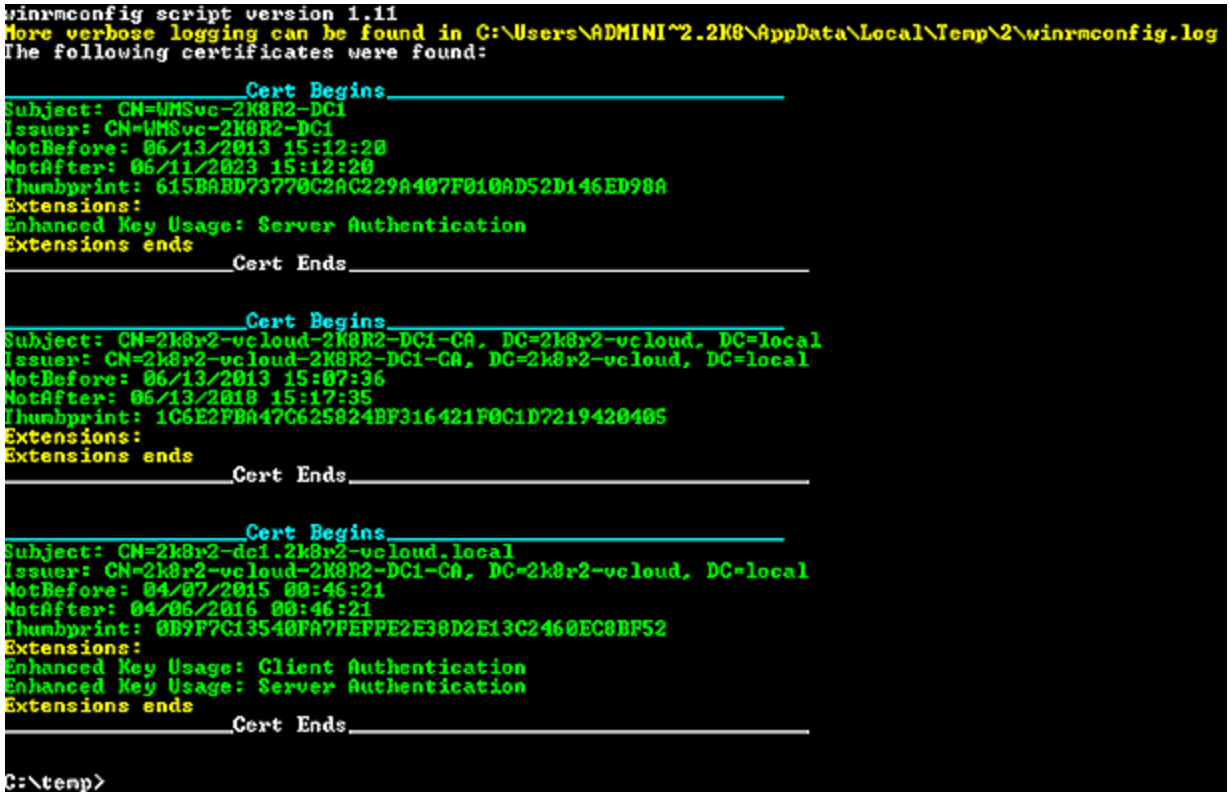
Other Script Options

The following sections describe certificate features that apply when you are using HTTPS.

WinRM Compatible Certificates used with HTTPS Listeners

The **ShowAllCerts** command dumps all machine certificates, along with their EKU bits. (A WinRM HTTPS listener requires a certificate that has at least “Server Authentication” EKU.)

```
Powershell -File winrmconfig.ps1 -Action ShowAllCerts
```



In this output, and the previous **enable** command, the last certificate in this list was selected by the script to use for creating the listener for the following reasons:

- The certificate is not expired
- The certificate has the Server Authentication EKU bit enabled
- The certificate's **Subject** field contains the FQDN of the system (which makes it a good choice in its favor since the subject CN must be the FQDN of the host for the listener creation to succeed)

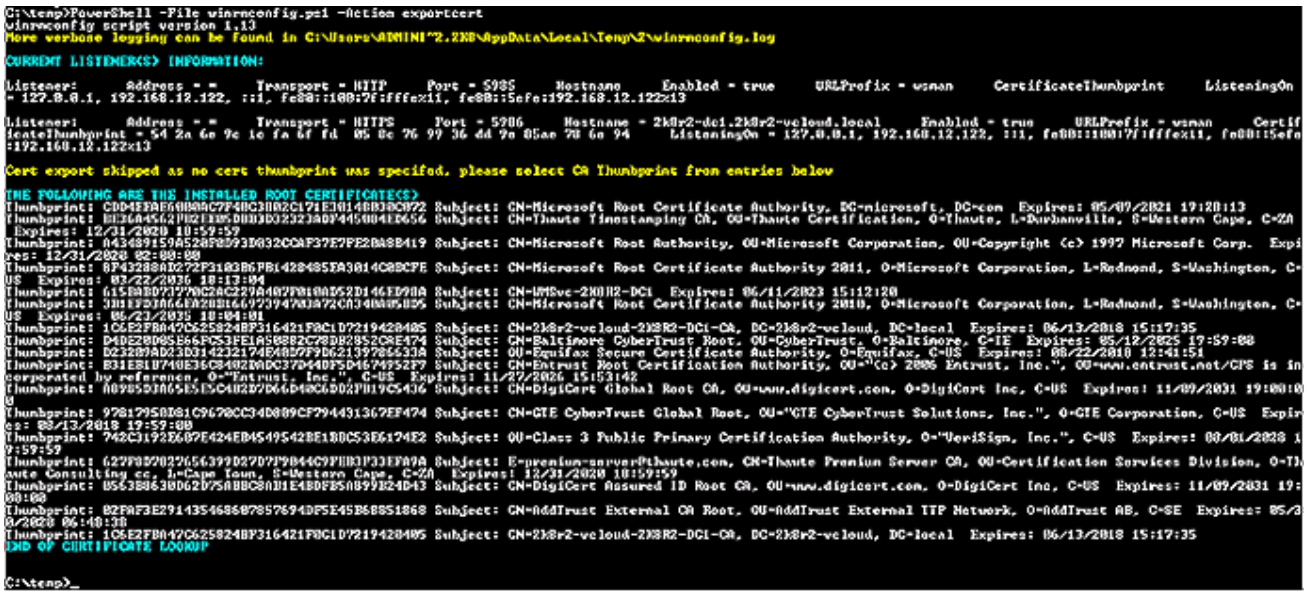
If another certificate has the FQDN in its **Subject** and is better suited, you can select it from the command line using the **-Thumbprint** option. The following example creates a new listener by selecting the certificate that has the specified thumbprint.

```
Powershell -File winrmconfig.ps1 -Action enable -ListenerType https -Port 5555 -User
newcoluser@2k8r2-vcloud -ThumbPrint 615BABD7377 229A407F010AD52D146ED98A
```

WinRM Over HTTPS with Mutual Authentication

You can enable HTTPS-based log collection, without importing certificates, via the RSA NetWitness console. In the event source, HTTPS is selected, but the certificate field is left empty. This mode of operation is the same as using HTTPS for a web server without setting up user certificates. However, you can perform the extra step to import each Windows system's CA certificate into the Collector and configure the certificate name in each event source. This provides mutual authentication, that is, it allows the Collector to verify that the target system is configured for log collection. The **winrmconfig** script makes this process easier by using the **exportcacert** action and **-ExportCertPath** and **-ThumbPrint** options. For example, the following command lists all CA certificates on the system, as shown in the image below the string:

```
PowerShell -File winrmconfig.ps1 -Action exportcert
```



This command lists all the CA (Root) certificates. Typically, a CA certificate with the domain/hostname in the subject is the correct certificate.

You can select the thumbprint of the certificate from the list and then run the following command to export the certificate, convert it to PEM format, and save it to the path specified.

```
PowerShell -File winrmconfig.ps1 -Action exportcert -ExportCertPath c:\temp\ -ThumbPrint
1C6E2FBA47C625824BF316421F0C1D7219420405
```

The PEM filename is a concatenation of the certificate subject and the thumbprint with .pem extension as shown below:

```
2k8r2-dc1.2k8r2-vcloud.local-CA-1C6E2FBA47C625824BF316421F0C1D7219420405.pem
```

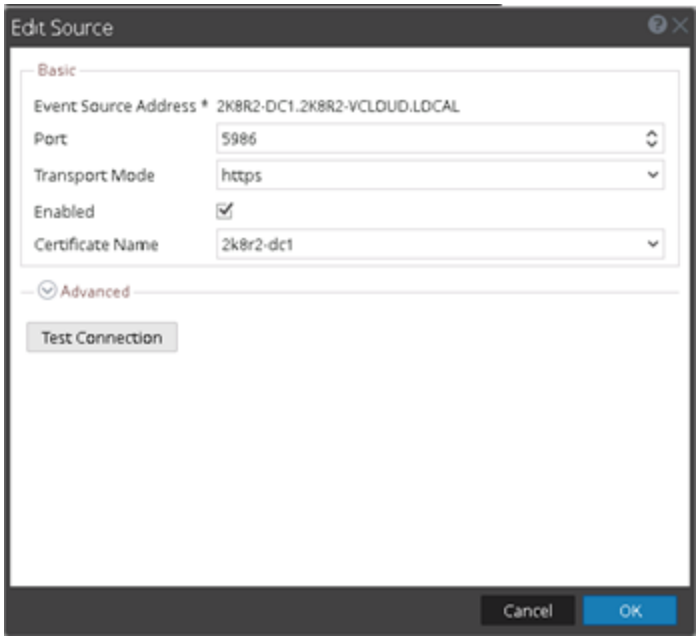
The **ExportCertPath** path can be a secure common share where the RSA NetWitness UI can be used to import all the exported CA certificates.

To import the certificate into RSA NetWitness:

1. Log on to the RSA NetWitness Platform.
2. At the top of the page, click **Dashboard > ADMIN > Services**.
3. Select a Log Collector service, and in the **Actions** column, click the down arrow and select **View** > **Config**.
4. Click the **Settings** tab and from the left pane, select **Certificates**. The Certificates pane is displayed.
5. Click the plus sign to add a certificate. The Add Cert dialog is displayed.

6. Create a name for the certificate that is based on the system that the certificate came from, for example, the hostname.
7. Click **Browse** to select the newly exported PEM file. The script does not export the private key. (There is no requirement for the key to connect to the system.)
8. Click **Save**. (The password is not required for certificates exported by the script.)
9. Select the imported certificate in the Event Source (remember to change the port to HTTPS, the default is

5986).


Edit Source
Basic
Event Source Address * 2K8R2-DC1.2K8R2-VCLOUD.LOCAL
Port
5986
Transport Mode
https
Enabled
Certificate Name
2k8r2-dc1
Advanced
Test Connection
Cancel
OK

Group Policy Method for Mass-enabling WinRM

Using Microsoft Group Policy Object (GPO) to enable WinRM can be very flexible. There are many ways to scope the number or types of systems the GPO is pushed to, for example, by using a WMI filter or by selecting specific domain names by using active directory domain trees. As described in Configuring Windows Collection, there are a number of decisions to be made before you decide to use GPO:

- Do I use an administrative or non-administrative account to collect events? (RSA strongly recommends using a non-administrative account.)
- Do I use HTTP or HTTPS transport ? (It's not uncommon to see both in use in the same domain, for example, HTTP for domain members and HTTPS for domain controllers.)
- Do all the systems, from which I collect events while using HTTPS transport, already have certificates?

With the answers to these questions in mind, taking the steps to deploy WinRM via GPO is actually quite simple, as the PowerShell script takes care of almost everything. The previous sections of this guide describe the **report** and **enable** modes of the script. In this section, only the **enable** mode is used, because we are setting up a GPO to configure systems from which RSA NetWitness collects events.

Systems that require encrypted collection, for example, HTTPS, must have machine certificates installed that support at least server authentication key usage. Usually, this is not an issue for domain controllers. However, domain members and standalone systems often do not have certificates. This document has a section that describes pushing this type of certificate to those systems. There is no mandate that you use a single GPO to push the **winrmconfig** script. For example, HTTPS could be used to collect from domain controllers, and HTTP could be used for domain members. Separate GPO's could be created, one for each class of system to push the same script, with different parameters, to each of the different types of system.

WinRM over HTTPS SSL Certificate Deployment

If you have decided to enable WinRM using HTTPS transport, the systems from which RSA NetWitness collects events must have a viable certificate installed. The first step is to ensure that the systems from which RSA NetWitness collects events have SSL certificates.

If those systems have certificates, skip this section. For example, most domain controllers already have a local machine certificate, so this step may not be necessary if you are collecting solely from domain controllers.

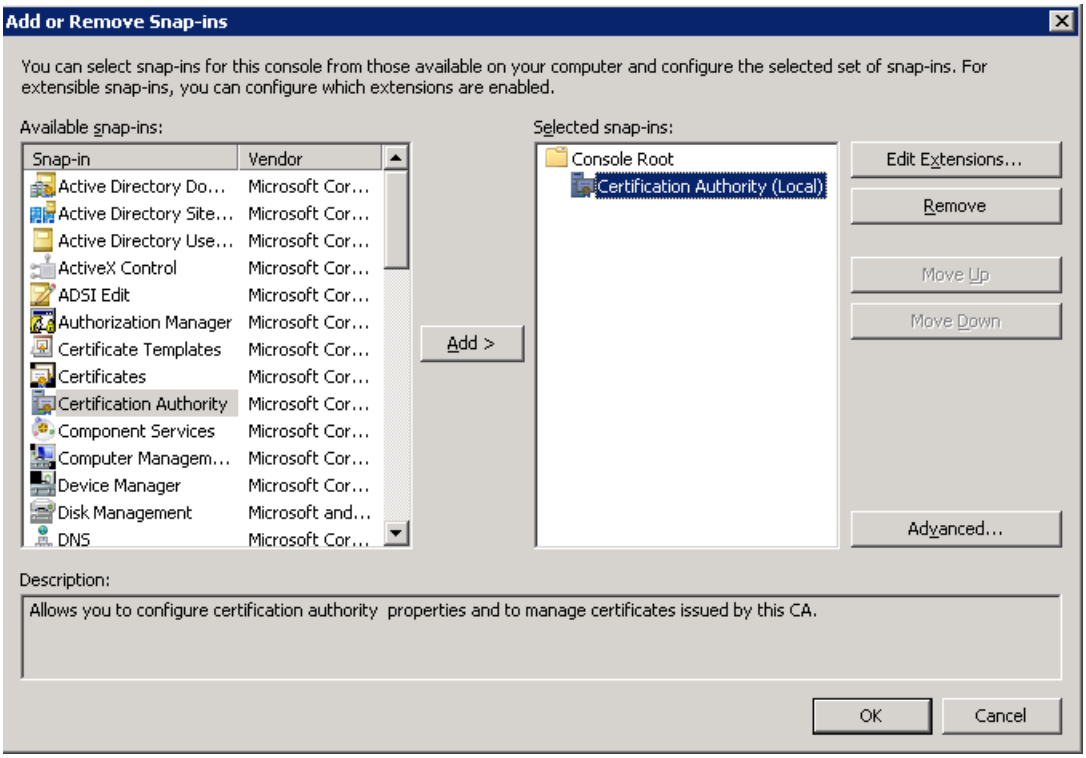
However, standalone machines might not have certificates. You can use a GPO to push certificates to machines that do not already have them by following the steps in this procedure.

Create Certificate Templates

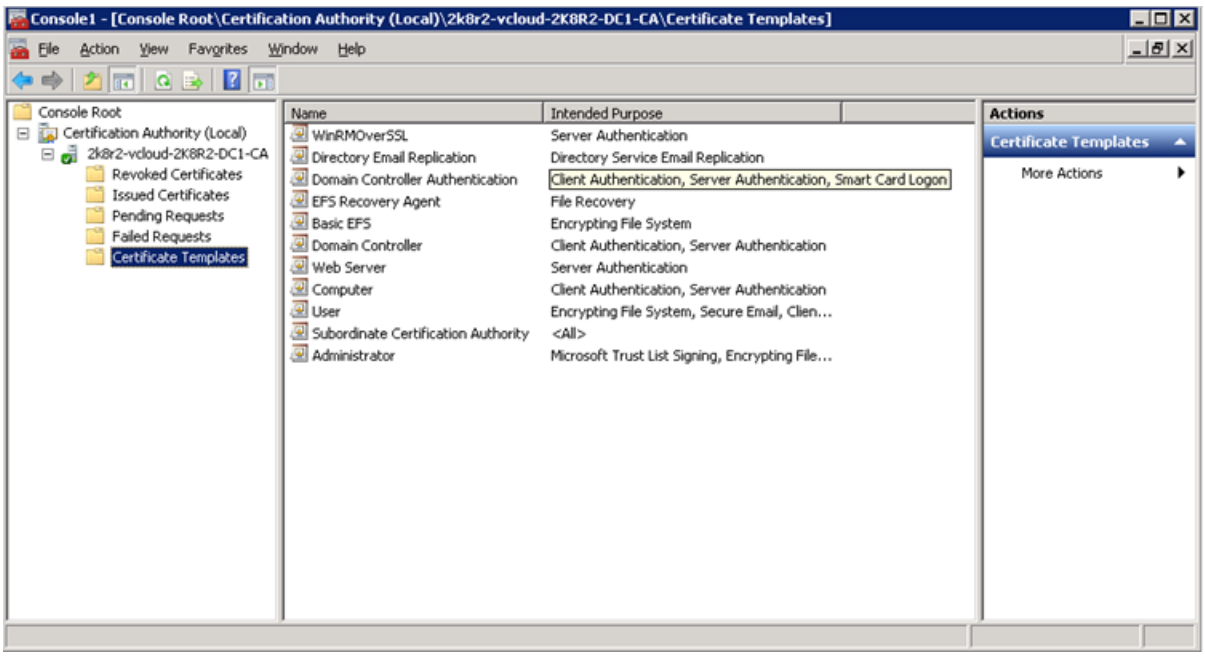
1. Run the local certificate authority application on the domain controller:

   a. At a command prompt, type `certsrv`.

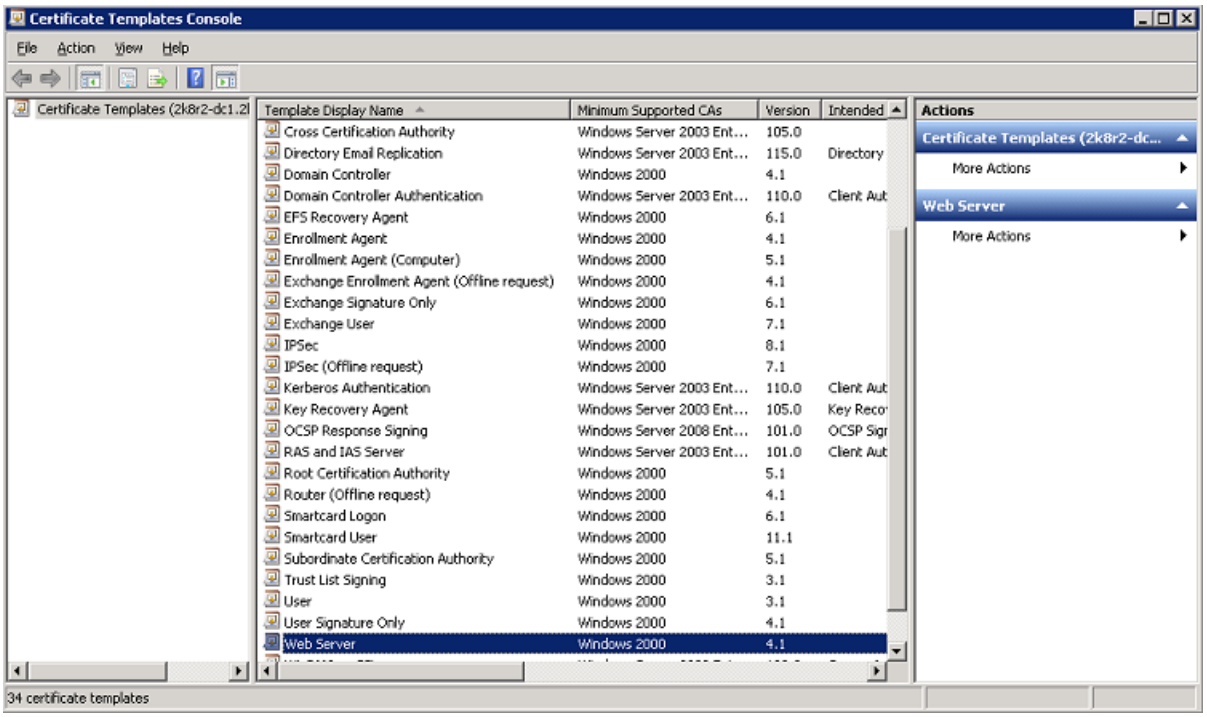
   b. Run `mmc`, click **File** > **Add/Remove Snapin**, and then add the Certificate Authority as shown in the following figure.



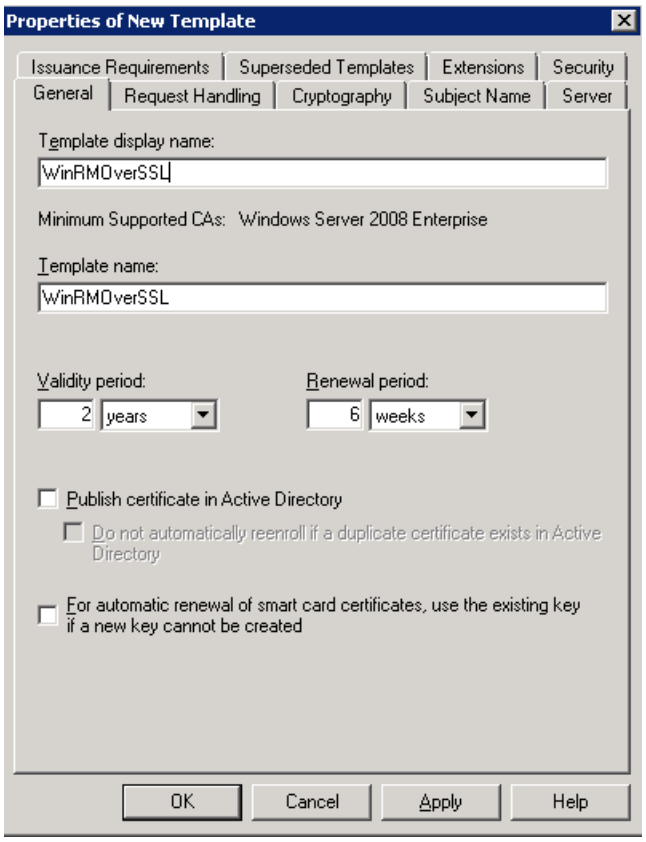
The Certificate Templates window opens.



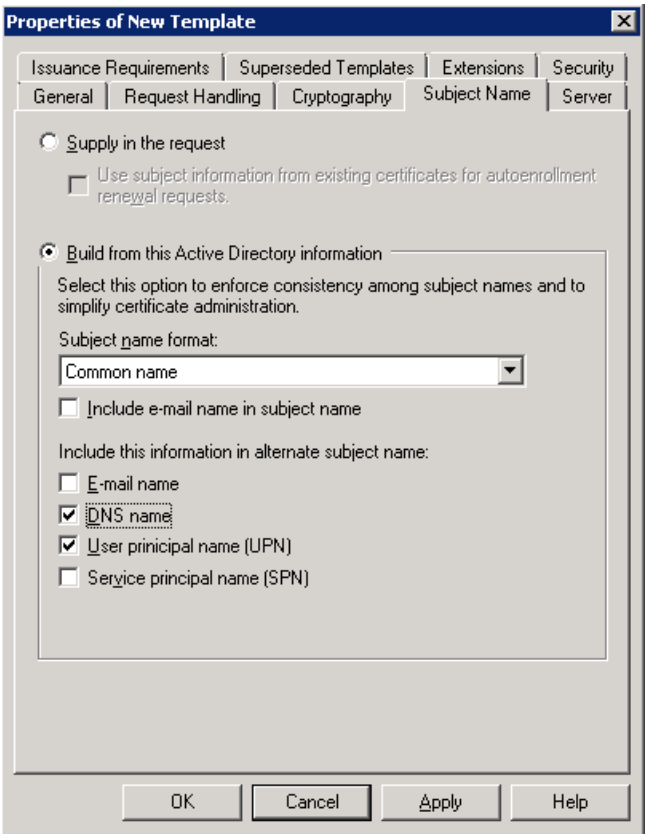
2. In the left pane, right-click **Certificate Templates** and select **Manage**. The Certificate Templates Console window is displayed.



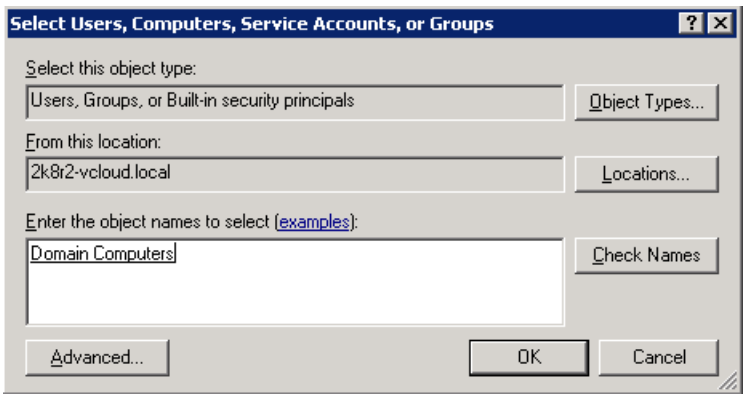
3. In the middle pane, right-click **Web Server** and select **Duplicate Template**. The Properties of New Template dialog opens.



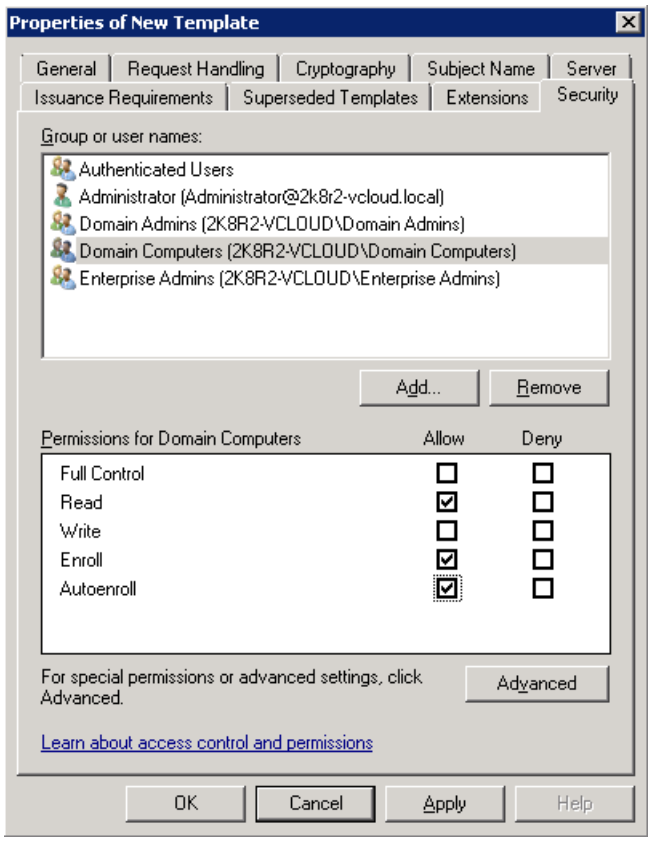
4. On the **General** tab, in both the **Template display name** and the **Template name** fields, type `WinRMOverSSL`.
5. Use the **Validity period** and **Renew period** fields to select a time period in which the certificate expires. Ensure that this time period complies with your company's policies.
6. Click the **Subject Name** tab and ensure that **Build from this Active Directory information** is selected.



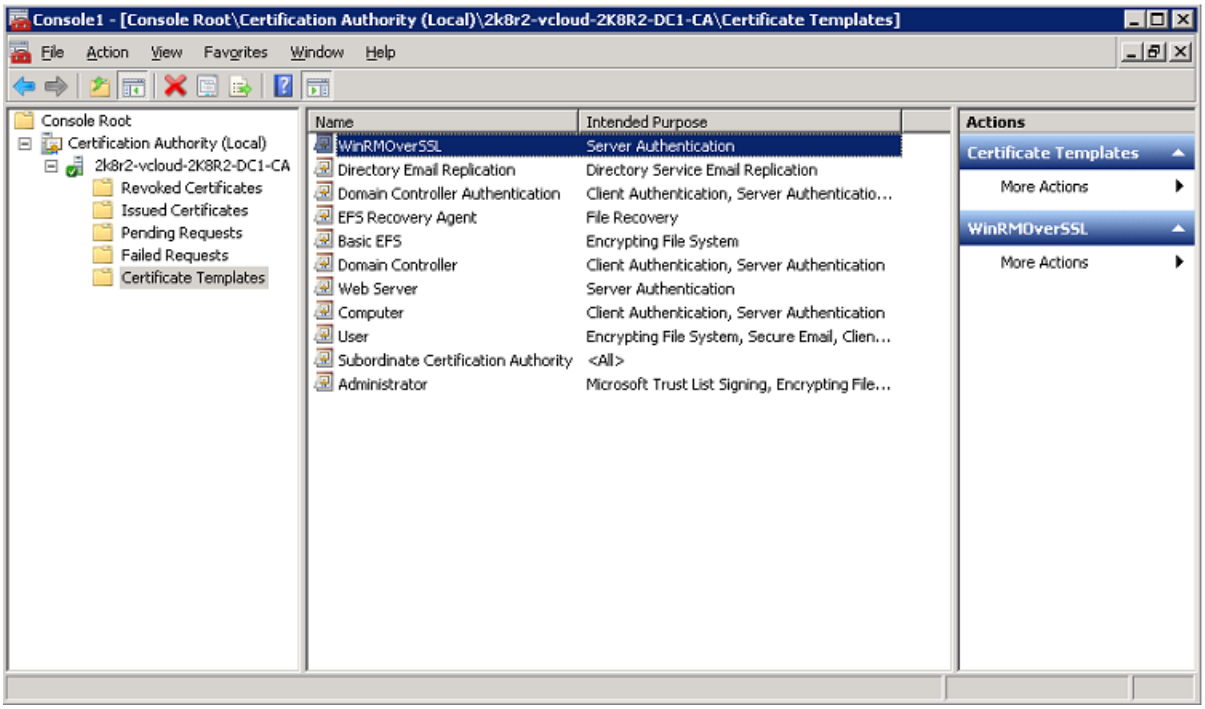
7. From the **Subject name format** drop-down menu, select **Common name**.
8. Under **Include this information in alternate subject name**, select **DNS Name**.
9. Click the **Security** tab, and then click **Add**. The Select Users, Computers, Service Accounts, or Groups dialog opens.



10. Click **Object Types**, select **Computers**, and click **OK**.
11. Click **Check Names**, enter `Domain Computers`, and click **OK**.
12. To configure permissions, click the **Security** tab.



13. Select **Allow** for **Read**, **Enroll**, and **AutoEnroll**. Click **Apply** and then click **OK** and close the Certificate Templates console.
14. To enable the new template, in the Certification Authority console, right-click **Certificate Templates**, click **New** > **Certificate Template to issue**, and select the template that you just created.

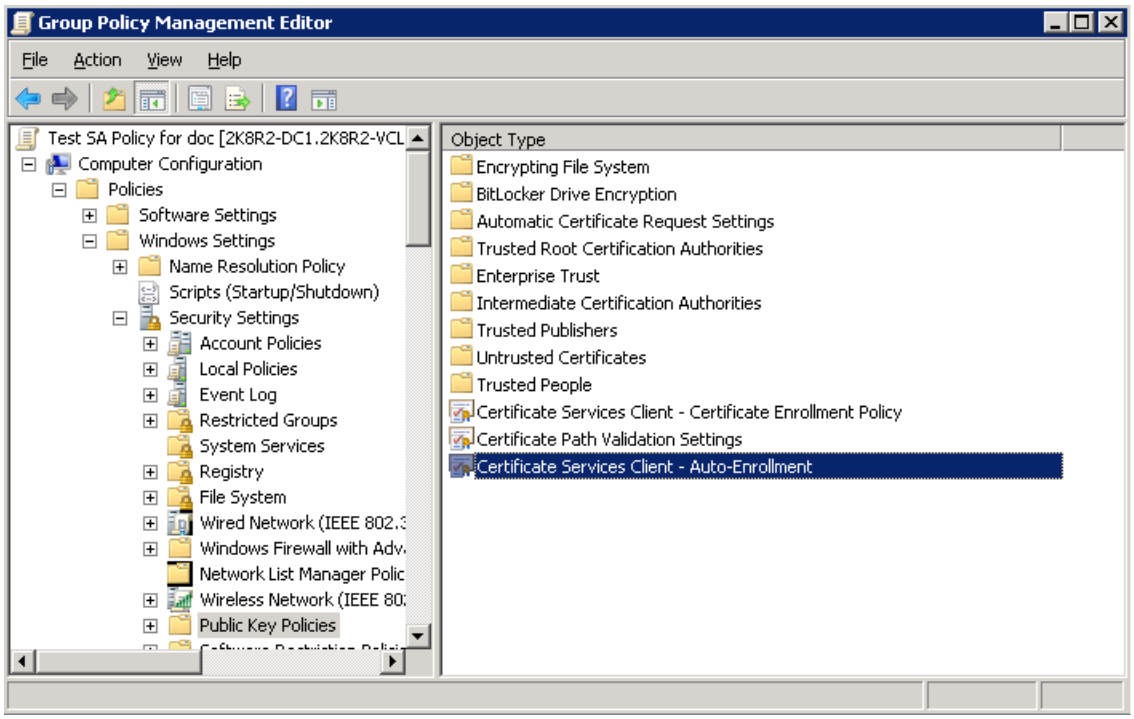


Link Certificate Templates to Group Policies

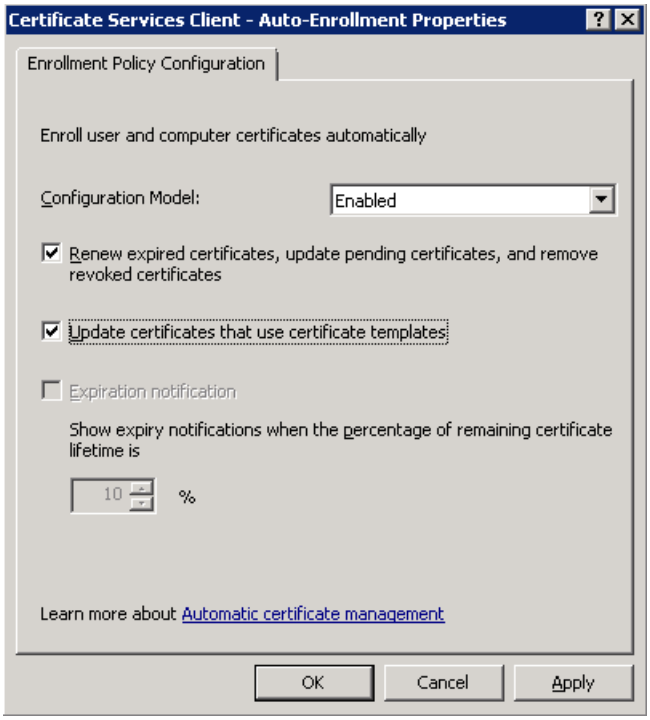
To create and publish certifications, you must link certificate templates to Group Policy Objects (GPOs).

To link a template to a Group Policy Object:

1. To open the Group Policy Management Console on the domain controller, click **Start** > **Administrative Tools** > **Group Policy Management**, and in the left pane, browse to the **Group Policy Objects** folder for your domain.
2. Right-click the Group Policy Objects folder and click **New**
3. Type `WinRMCertEnrollment`, and leave **Source starter GPO** as none.
4. Right-click on the `WinRMCertEnrollment` policy and click **Edit**. The Group Policy Management Editor dialog opens.



a. Select **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Polices**. In the right pane, double-click on **Certificate Services Client - Auto Enrollment**. The Certificate Services Client - Auto-Enrollment Properties dialog opens.



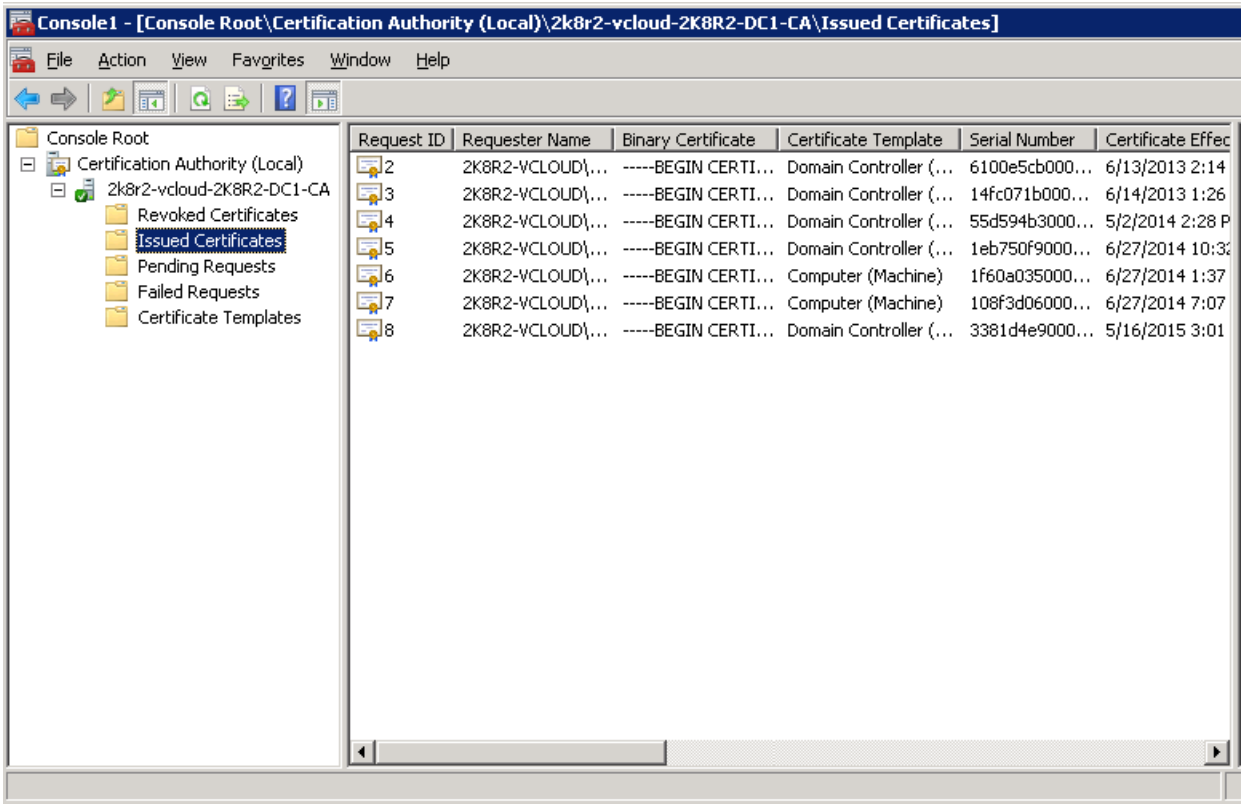
b. To set up automatic renewal of user and computer certificates, select **Renew expired certificates update pending certifications, and remove revoked certificates** and **Update certificates that use certificate templates**.

Note: It may take several hours before the policy is pushed and actioned. To deploy the certificate faster, run `gpupdate /force` from an elevated command line on any system that is covered by the GPO.

Use the Issued Certificates page in the Certificate Authority to see if the GPO is causing certificates to be pushed. It is important to find out when your GPO pushed certificates to all the machines within the scope of the GPO, because the HTTPS listeners that you create only work after the certificates have been pushed to those machines.

To find out if your GPO is causing certificates to be pushed:

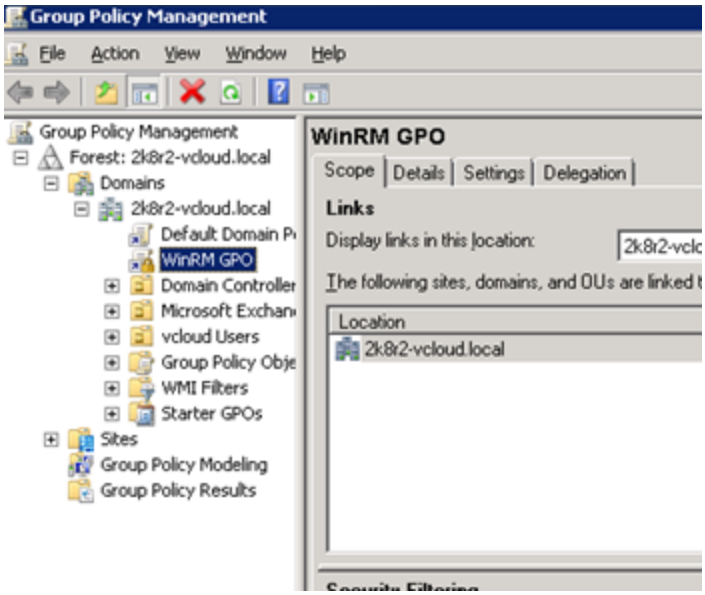
1. In the Certificate Templates Console, in the left pane, click **Issued Certificates**
2. In the right pane, information about requests for certificates is displayed.



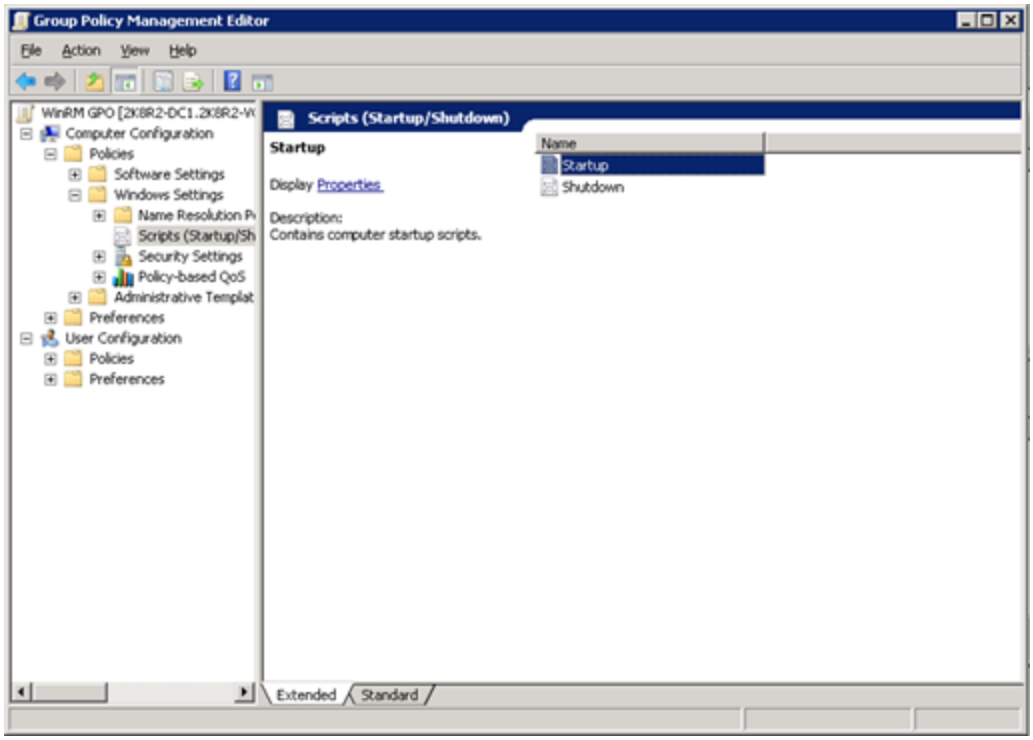
Create GPO to Push the winrmconfig Script

To vastly simplify WinRM configuration via GPO, you can push the **winrmconfig** PowerShell script to all systems from which RSA NetWitness collects events. The script runs as a system startup. It creates any listeners that are needed and enables the relevant permissions for a non-administrative account to be used to collect events and enumerate SIDs (which are the two operations that a RSA NetWitness Collector performs). If the collection user was an administrative account and the listener type was HTTP, a very simple GPO could be used. However, as previously stated, RSA does not recommend using an administrative account.

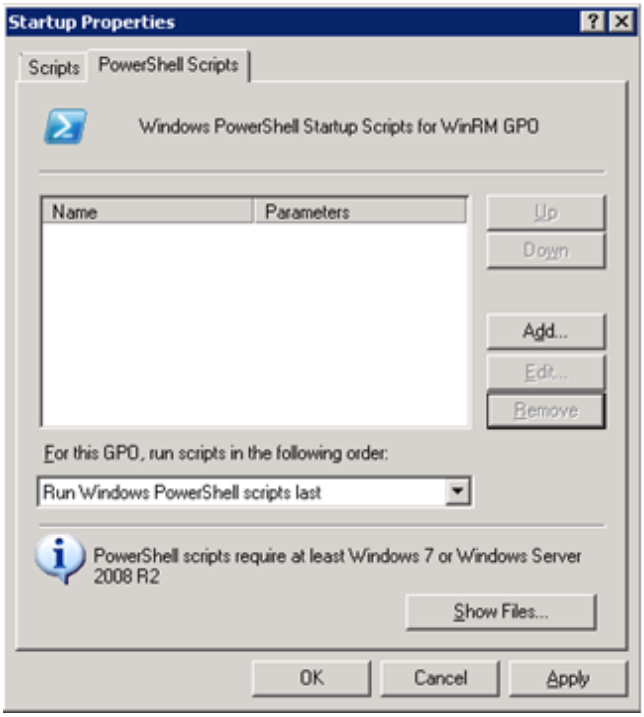
1. Open the Group Policy Management Console on the domain controller: Click **Start** > **Administrative Tools** > **Group Policy Management**, and in the left pane, browse to the **Group Policy Objects** folder for your domain.
2. Create a new Group Policy object, for example, `WinRM GPO`. Refer to your network administrator when deciding on the scope of the GPO. Defining the scope of the GPO directly chooses the machines the script will be run on. See step 8 in this procedure for information about WMI filters.



3. Right-click the newly-created Group Policy object and click **Edit**.



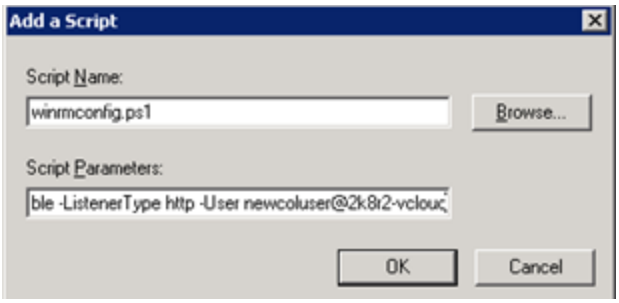
4. Expand **Computer Configuration** > **Windows Settings** > **Scripts** and double-click **Startup**.



5. Click the **PowerShell Scripts** tab, click **Add**, and then click **Browse**. The default directory in the Browse dialog should be the current **sysvol** path, for example:

```
\\2k8r2.local\SysVol\2k8r2.local\Policies\{68EB4039-9768-48B2-9E0B-
58153D188233}\Machine\Scripts\Startup
```

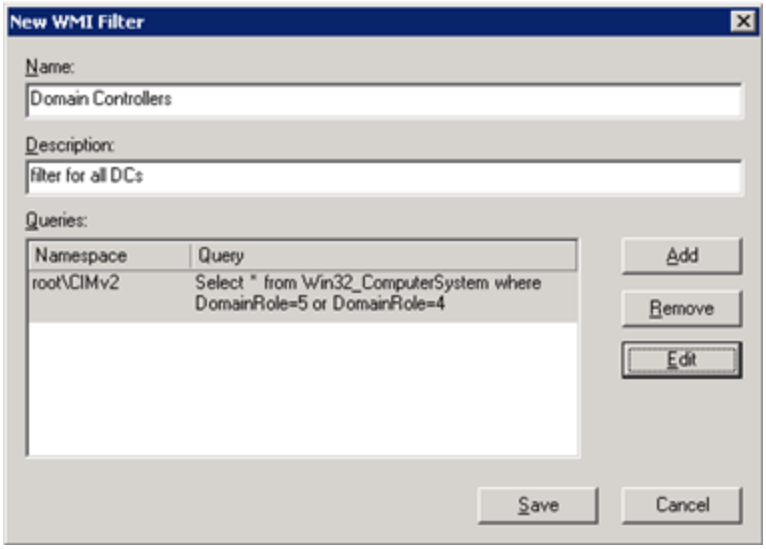
6. Copy and paste the path from the Browse dialog, and using that path, copy the **winrmconfig** script to that location using Windows Explorer. The script is displayed in the Browse dialog. Select the script. The Add a Script dialog is displayed.



The **Script Parameters** field is the key to configuring listener and collection user permissions, as this is where options such as the listener type and collection user account is specified. In this document, the sections winrmconfig Modes and Other Script Options describe options for the script. Here are some examples of script options:

- **Action enable -ListenerType http -User myuser@domain.com** causes the script to create an HTTP listener on each system that the GPO is applied to, and creates all the permissions for the **myuser@domain.com** account to enable event collection from those systems.
- **Action enable -ListenerType https -User myuser@domain.com** causes the script to create an HTTPS listener using any available non-expired certificate that has the Server Authentication key usage enabled, with a Subject DN string that matches the name of the system. If the certificate is not available, it should have been pushed to the listener using the previous steps to push certificates to systems via GPO.
- **Port xxxx** causes the script to create a listener on a customer port other than the default 5985 for HTTP or 5986 for HTTPS (-Port 5999 for example).

7. Paste the string that you selected in step 6 into the **Script Parameters** field and click **OK**, **Apply**, and **OK** to return to the Group Policy Editor dialog.
8. Link the GPO to a container in the Active directory that fits the scope of the systems to which to apply the GPO. In this case, the scope is the whole domain or all systems in the domain. You can select a WMI filter to better isolate the machines to which to push the GPO.



In this example, the GPO will be pushed to the domain primary and backup domain controllers only.

With the GPO linked and enabled, if a system in the scope of the GPO is rebooted, the script will execute on restart and configure WinRM in the manner determined by the script parameters of the startup script.

Firewall Information

The following information is relevant for systems that are using firewalls.

Systems running Windows built-in Firewall

If the winrmconfig script is run with the `--enable` option on a system that has the Windows local firewall service running, the script automatically adds the necessary local firewall port rules, based on the selected port or the default WinRM listener port for the listener type.

Other Firewall Considerations

Note that the Collector must be able to poll each configured WinRM system. So, if there is a firewall between the Collector(s) and system being collected from via WinRM, the configured listener port must be opened. This is true regardless of the authentication type selected in the Event Category section of the WinRM configuration.

If you selected "Negotiate" as the authentication method, the collector needs to obtain a TGT (Ticket Granting Ticket) in order to get Service Tickets for the configured systems being collected from. This applies to all collectors, both local and remote, that are performing collection via WinRM. That is, each Windows system being collected from would need a rule to open port 88 udp/tcp for all configured Domain controllers configured under the Kerberos realms configuration tab.

Note: RSA highly recommends that if you are using the Negotiate method of communication, you create a firewall rule to open port 88 for UDP and TCP, in the direction of the Log Collector to the Domain Controllers being configured. Requests go from the LC to the DC only, so the rule can be one-way.

Both TCP and UDP access (at least one way from collector to Domain controller) is required as the Kerberos implementation on the collector initially attempts to request the TGT or ST using UDP on port 88. However, the response to Kerberos may be too large for a single UDP response. The Domain Controller will then respond with a "response too large" message which will cause the collector will switch automatically to TCP on port 88 and re-request the tickets.