The Zenoss Enablement Series:

MONITORING WINDOWS SERVERS WITH MICROSOFT WINDOWS ZENPACK AND WINRM

Document Version P4

Zenoss, Inc.

www.zenoss.com

Table of Contents

About this Document

In this article, we prepare four Windows server versions (2012 R2, 2012, 2008R2, 2003 SP2 Standard Edition) for monitoring using the Windows Zenpack. We discuss preparing servers using both Group Policy (to standardize configuration across all servers) and individual server configuration. The documented procedures are standardized around a low security configuration using local system (as opposed to domain) credentials and no encryption of credentials or payload. This scenario provides a good base configuration for ease of setup and testing, but in production the use of a single domain service for authentication will improve ease of administration. The use of a domain service account requires the use of Kerberos to encrypt credentials, which will improve security. Security can be improved further still by configuring WinRM to encrypt its payload using SSL. Each section of this document includes these additional configurations for administrators who need to implement them. These higher security configurations are recommended in production environments.

Applies To

The procedure outlined in this document applies to the following versions:

- Windows Server 2012 & 2012 R2
- Windows Server 2008R2
- Windows Server 2003 SP2 Standard Edition

About Windows Authentication for WinRM Monitoring

Like any monitoring system, Zenoss must authenticate to the Windows systems it will monitor using either local system or Windows domain credentials. The Windows user account used for WinRM authentication must have specific permissions granted on each Windows system to be monitored. By default, Windows Administrator accounts already have the necessary permissions, but best practices dictate that Administrator accounts not be used for purposes such as WinRM monitoring. Instead, a dedicated User account (a “service account”) should be created specifically for the purpose of WinRM monitoring with only the necessary permissions granted to the account.

Instead of manually editing the necessary permissions, a Windows PowerShell®, hereafter referred to as *PowerShell*, script can be used to modify the necessary permissions in a single step. For administrator convenience, Zenoss has created a sample script that modifies the permissions necessary for an example service account (“zenny” in the case of a domain user, or “benny” in the case of a local user account). The *zenoss-lpu.ps1* script can be downloaded from https://github.com/zenoss/microsoft.tools/tree/develop/lpu. The file can be edited as necessary to suit specific production environments.

Note: The sample script includes two lines that must be located and deleted before the functions in the script will execute. These lines have been deliberately included to encourage administrators to thoroughly review the script before deploying it to ensure (i) that administrators fully understand the functions it performs and (ii) they have made any necessary edits before deploying it.

The relevant sections below describe methods to configure Windows system permissions using a PowerShell script such as *zenoss-lpu.ps1* that has been tailored to a specific environment.

Windows Server 2012 & 2012 R2

The following sections describe how to configure Windows Server 2012 and Windows Server 2012 R2.

Note: Windows 2012 R2 is specifically called out only when there is a difference in method between the two Windows server versions.

Configuring Windows Server 2012 Using Group Policy (Basic Authentication, no Encryption)

Note: This configuration uses a local user account on each monitored Windows system for authentication instead of a domain account. The local user account must be present on each system before Zenoss can monitor it.

1. Log on to a domain controller as a user with 'Domain Admin' privileges.
2. On Server 2012 (non R2):

   i. Press the **Windows** key on the keyboard to display the *Start* screen.
   ii. Click the **Group Policy Management** tile.
   Note: The *Group Policy Management Console (GPMC)* is normally installed by default on the domain controller. You can install GPMC on a member server as long as it is a member of the domain. If the tile is not present and you need to install it, use the instructions provided at: http://technet.microsoft.com/en-us/library/cc725932.aspx.

3. On Server 2012 R2:

   i. Press the **Windows** key on the keyboard to display the *Start* screen
   ii. Click **Server Manager**.
   iii. Click **Tools** in the upper right
   iv. Select **Group Policy Management**.
   Note: The *Group Policy Management Console (GPMC)* is normally installed by default on the domain controller. You can install GPMC on a member server as long as it is a member of the domain. If the tile is not present and you need to install it, use the instructions provided at: http://technet.microsoft.com/en-us/library/dn265969.aspx.

4. Navigate to your target domain in the tree at the left:

   i. Expand the section for the domain Forest you want to edit.
   ii. Expand **Domains**.
   iii. Expand your target domain.

5. Right-click **Group Policy Objects** and select *New*. In the form that displays:

   i. Enter a name for your new Group Policy Object, for example, *WinRM_Monitoring*.
   ii. Leave "(none)" in the **Source Starter GPO** field.
   iii. Click **OK** to save and exit the form.

6. Select your new **Group Domain Policy Object**, *WinRM_Monitoring*, for example.
7. Right click your new **Group Domain Policy Object** and select *Edit* to open the Group Policy Management Editor.
8. Expand the **Computer Configuration** section of the tree and navigate the tree to:

```
Policies\Administrative Templates:Policy...\Windows
Components\Windows Remote Management(WinRM)
```

9. Enable remote server management:

   i. Click on **WinRM Service** to access the *WinRM Service Group Policy* settings in the right pane.
   ii. Double-click the **Allow remote server management through WinRM** property.
   iii. Click the **Enabled** radio button.
   iv. Place an asterisk as a wildcard (' * ') in the *IPv4 filer* and *IPv6 fields* or specify a range of IP addresses for WinRM to listen on.
   v. Click **OK** at the bottom to submit the form.

10. Enable authentication:

    i. Double-click the **Allow Basic authentication** property in the right pane.
    ii. Select the **Enabled** radio button.
    iii. Click **OK** at the bottom to submit the form.

11. Specify unencrypted traffic:

    i. Double-click the **Allow unencrypted traffic** property.
    ii. Select the **Enabled** radio button.
    iii. Click **OK** at the bottom to submit the form.

12. Select *Windows Remote Shell* in the left pane to set its **Group Policy** settings. This is located in the group policy tree in the following location (which might be located right below *WinRM* service in the tree):

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Shell
```

13. Configure remote shell access:

    i. In the right pane, double-click **Allow Remote Shell Access**.
    ii. Select the **Enabled** radio button.
    iii. Click **OK** at the bottom to submit the form.

14. Configure shell processes:

    i. In the right pane, double-click **Specify maximum number of processes per Shell**.
    ii. Select the **Enabled** radio button.
    iii. Enter the value **2,000,000,000** (without commas or spaces) in the *MaxProcessPerShell* field.
    iv. Click **OK** at the bottom to submit the form.

15. Configure the number of remote shells:

    i. In the right pane, double-click **Specify maximum number of remote shells per user**.
    ii. Select the **Enabled** radio button.
    iii. Enter the value **2,000,000,000** (without commas or spaces) in the *MaxShellsPerUser* field.
    iv. Click **OK** at the bottom to submit the form.

16. Configure shell timeout value:

    i. In the Right pane, double-click **Specify Shell Timeout**.
    ii. Select the **Enabled** radio button.
    iii. Enter the value **7,200,000** (without commas or spaces) in the *ShellTimeOut* field.
    iv. Click **OK** at the bottom to submit the form.

Windows Server 2012: Configuring Firewall Group Policies

WinRM listens on port 5985 when data payload encryption is not used and on port 5986 when encryption is used. Additionally, ICMP (ping) requests must be enabled because Zenoss uses them as a source of availability monitoring.

The appropriate port must be opened on the firewalls of monitored servers. You can use Group Policy to open the required ports on all servers across the organization.

1. In the Group Policy Manager Editor, navigate to:

   ```
   Computer Configuration\Policies\Windows Settings\Security Settings\Windows
   Firewall with Advanced Security\Windows Firewall with Advanced Security -
   LDAP;...\Inbound Rules
   ```

2. Create a new *Inbound Rules* policy for **Windows Remote Management**:

   i. Right click **Inbound Rules** in the left pane.
   ii. Select **New Rule...**
   iii. Select the **Predefined** radio button.
   iv. Select **Windows Remote Management** from the drop down list.
   v. Click **Next**.
   vi. Ensure that all items in the list are checked.
   vii. Click **Next**.
   viii. Ensure that the **Allow the connection** radio button is selected.
   ix. Click **Finish**.

3. Create a new *Inbound Rules* policy for **Echo Request ICMP** (ping) requests:

   i. Right click **Inbound Rules** in the left pane.
   ii. Select **New Rule...**
   iii. Select the **Predefined** radio button.
   iv. Select **File and Printer Sharing** from the drop down list.
   v. Click **Next**.
   vi. Ensure the check boxes for the following items are selected:

      - **File and Printer Sharing (Echo Request-ICPMv4-IN)**
      - **File and Printer Sharing (Echo Request-ICPMv6-IN)**
        You can de-select any additional check boxes unless you require them specifically.

   vii. Click **Next**.
   viii. Ensure that the **Allow the connection** radio button is selected.
   ix. Click **Finish**.

4. Exit the *Group Policy Management Editor*:

   Select **File > Exit**

5. Link your new GPO to one or more Organizational Units (OU) containing servers to which you wish to have the policies applied. Alternatively, you can apply the policies to all Windows servers in the domain by linking the new GPO to the domain itself. To link the GPO to the domain, complete the following process.

   Note: Substitute a specific OU for the domain if you want to link only to a subset of servers.

   i. Right-click your domain in the left pane of the *Group Policy Management* window.
   ii. Choose **Link an Existing GPO...**

   iii. Select your new GPO, *WinRM_Monitoring* for example, from the list that displays.
   iv. Click **OK** to complete the process.

6. Exit the Group Policy Management window:

   Select **File > Exit**

7. Before adding servers to Zenoss for monitoring, wait a sufficient amount of time for Group Policy to automatically refresh on the server(s). Alternatively, you can manually refresh Group Policy from the command prompt of target servers using this command:

```
gpupdate /force
```

Windows Server 2012: Configuring Windows Credentials in Zenoss

When one or more servers are ready for addition to Zenoss, perform the following steps within the Zenoss web interface. If the same user account name was created on each server, the following procedure will specify it for all servers in the device class:

1. Navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class.
3. Click the **Details** icon.
4. Click **Configuration Properties** in the left pane.
5. In the right pane, set the configuration properties for *zWinRMUser* and *zWinRMPassword*, supplying the appropriate Windows credentials.

   Note: For ease of setup and testing, the local Administrator account can be used in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled *About Windows Authentication for WinRM Monitoring* for more on WinRM authentication.

   To configure Windows to allow monitoring using a non-Administrator service account, see the section below titled *Windows Server 2012: Configuring a WinRM Service Account on Individual Windows Systems* or the section titled *Windows Server* 2012: Group Policy Deployment of a PowerShell Script for Service Account Configuration.
6. Click **See All**.
7. Add windows servers using the web interface or `ZenBatchload`.

Note: If the user names and passwords used on servers are different, each server must be added and its individual *zWinRMUser* and *zWinRMPassword* configuration properties must be set. Perform the following steps to add the server information:

i. Add the server to the **Server/Microsoft/Windows** device class, but opt out of modeling the device when adding as follows:
   - If you are adding via the web interface, leave the **Model Device:** box unchecked.
   - If you are adding through the `zenbatchload` command, be sure the device has the `--nomodel` flag set.

ii. When the device displays in the device list, click on its name.

iii. Click on **Configuration Properties** in the left pane, and set the configuration properties for *zWinRMUser* and *zWinRMPassword*, supplying the appropriate Windows credentials.

iv. Model the device by clicking the Action Wheel (gear-shaped) icon in the lower left and select **Model Device...**

Windows Server 2012: Improving Security by Using a Domain Service Account & Encrypting Credentials with Kerberos

Note: When switching from the use of local system accounts for authentication to a single domain service account, the use of Kerberos to encrypt credentials is mandatory.

Note: The Zenoss master and / or any collectors tasked with monitoring Windows servers that use Kerberos must have Kerberos installed on the host operating system.

1. Log in to the host as *root*, or as a user with *superuser* privileges.
2. Determine whether the Kerberos authentication package is installed:

   ```
   # rpm -qa | grep -i krb5-workstation
   ```

3. If the command returns a result, Kerberos authentication is installed and no additional action is necessary.

   If the command does <u>not</u> return a result, install Kerberos:

   ```
   # yum -y install krb5-workstation
   ```

The Kerberos authentication process requires an available ticket granting server. In the Microsoft Active Directory (AD) environment the AD Server also acts as the Key Distribution Center (KDC). The `zWinKDC` configuration property in Zenoss must be set to the IP address of the AD Server. Each collector used to monitor Windows servers must be able to send Kerberos packets to this server. To specify the ticket granting server in Zenoss, perform the following steps:

1. In the Zenoss web UI, navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class in the left pane.
3. Click the **Details** icon.
4. Click **Configuration Properties** in the left pane.
5. Edit the configuration property in the right pane for *zWinKDC*. Double click *zWinKDC* and specify the IP address of your Active Directory Server.
6. Edit the value for *zWinRMUser* name to be the *complete domain name* of the user, for example, *user@test.loc*.

   Note: A *zWinRMUser* name value in the form of *user@domain* is the trigger for Zenoss to (i) use a domain account rather than a local system account and (ii) to use Kerberos encryption for credentials. When the value of *zWinRMUser* name takes the form of *user*[only] instead of *user@domain,* Zenoss will use a local user account on the system being monitored.

   Note: For ease of setup and testing, the local Administrator account might be preferable to use in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled *About Windows Authentication for WinRM Monitoring* for more on WinRM authentication.

   To configure Windows to allow monitoring using a non-Administrator service account, see the section below titled *Windows Server 2012: Configuring a WinRM Service Account on Individual Windows Systems* or the section titled *Windows Server* 2012: Group Policy Deployment of a PowerShell Script for Service Account Configuration.

Note: The Zenoss server and collectors must be able to resolve the target server's pointer records (PTR) to their Active Directory fully qualified domain name. Administrators can meet this requirement by using one of three methods:

i. Configuring the Zenoss server to access the Windows DNS server for its DNS resolutions.

ii. Manually entering PTR records for each server in to the `/etc/hosts` file.

For example, the server *r2d2.example.com* at the IP address **77.77.77.77** has the following PTR record:

77.77.77.77 r2d2.example.com

iii. Using the zWinRMServerName property as follows:

- Specify the monitored server's name with the zWinRMServerName property field.

  Note: The `zWinRMServerName` property should only be used in conjunction with domain authentication when the DNS PTR record for a monitored server's managed IP address does not resolve to the name by which the server is known in Active Directory. For example, if *myserver1* is known as **myserver1.ad.example.com** by Active Directory and is being managed by IP address *192.51.100.21*, but IP address 192.51.100.21 resolves to *www.example.com*, you must set the `zWinRMServerName` property to **myserver1.ad.example.com** for domain authentication to work.

- If many Windows servers in your environment do not have DNS PTR records that match Active Directory, it is recommended that you:
  - set the monitored device's name to be the fully-qualified Active Directory name in Zenoss
  - set *zWinRMServerName* to `${here/titleOrId}` at the */Server/Microsoft/Windows* device class.

This method avoids setting the `zWinRMServerName` property on every device.

We recommend that you leave the `zWinRMServerName` property blank if local authentication is used, or DNS PTR records match the Active Directory listings. The result is that Zenoss does not have to rely on DNS resolution while monitoring and it avoids the additional overhead of configuring the `zWinRMServerName` properties.

Windows Server 2012: Configuring WinRM and WinRS on Individual Servers (Basic Authentication, no Encryption)

Perform the following steps to configure WinRM and WinRS:

1. Log on to the target server as a user with *Domain Admin* or local *Admin* privileges.
2. Press the **Windows** key on the keyboard to display the *Start* screen.
3. Click the **Windows PowerShell** tile.

   i. Configure the system to accept WS-Management requests from other systems. Enter the following at the command prompt:

   ```
   winrm quickconfig
   ```

   ii. Specify *http* instead of *https* (SSL) connections. Enter the following command:

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

   iii. Configure the maximum number of concurrent operations per user. Use the following command:

   ```
   winrm s winrm/config/service
   '@{MaxConcurrentOperationsPerUser="4294967295"}'
   ```

   iv. Configure the *maximum number of shells per user*. Enter the following command:

   ```
   winrm s winrm/config/winrs '@{MaxShellsPerUser="2147483647"}'
   ```

   v. Configure the *idle timeout*. Enter the following command:

   ```
   winrm s winrm/config/winrs '@{IdleTimeout="7200000"}'
   ```

   vi. Specify *Basic Authentication*. Enter the following command:

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

   vii. Exit PowerShell:

   ```
   exit
   ```

4. Configure the firewall to allow connections on port 5985.

   i. Press the **Windows** key on the keyboard to display the *Start* screen.
   ii. Click the **Server Manager** tile.
   iii. Click **Local Server** on the left.
   iv. Edit the firewall profile currently in use. Click the value to the right of **Windows Firewall** to change it.
   For example, "Windows Firewall" might display in grey font and to the right of it, in blue colored font, "Domain: On." In this case, click the blue **Domain On** value to display the *Windows Firewall* page.
   v. In the left pane of the *Windows Firewall* page, click **Allow an app or feature through Windows Firewall**.

vi. Scroll down through the list that displays and confirm that **Windows Remote Management** is checked for the current firewall profile in use (and any other profiles required).
Note: Remote management includes allowing connections on port 5985.

vii. Click **OK**.

5. If your firewall settings are NOT set by group policy, perform the following, depending on your server, to enable response to ping requests that are necessary for Zenoss to perform availability monitoring:

Windows 2012 R2:

i. In *Server Manager*, click **Local Server** in the left pane.

ii. In the right pane, click the entry for *Windows Firewall* **Domain: On** (in blue letters) to display the *Windows Firewall* dialog.

iii. Click **Allow an app or feature through Windows Firewall** to display the *Allowed apps* dialog.

iv. Click **File and Printer Sharing**.

v. Click **Next.**

vi. Ensure the boxes are checked for:

- **File and Printer Sharing (Echo Request - ICMPv6-In)**
- **File and Printer Sharing (Echo Request - ICMPv4-In)**

This enables the response to ping requests, you can uncheck any additional boxes unless you require them specifically.

vii. Click **OK.**

Windows 2012

i. In *Server Manager*, click **Local Server** in the left pane.

ii. In the right pane, click the entry for *Windows Firewall* **Domain: On** (in blue letters) to display the *Windows Firewall* dialog.

iii. In the left pane of the *Windows Firewall* page, click **Allow an app or feature through Windows Firewall** to display the *Allowed apps* dialog.

iv. Scroll down through the list that displays and confirm that **Windows Remote Management** is checked for the current firewall profile in use (and any other profiles required).
Note: Choosing remote management opens port 5985.

v. Click **OK.**

6. Configure Zenoss to monitor the server. Perform the following steps within the Zenoss web interface:

i. Navigate to the **Infrastructure** page.
ii. Select the **Server/Microsoft/Windows** device class.
iii. Click the **Details** icon.
iv. Click **Configuration Properties** in the left pane.
v. In the right pane, confirm that the configuration properties for *zWinRMUser* and *zWinRMPassword* match the appropriate Windows credentials on the system being monitored.

Note: For ease of setup and testing, the local Administrator account may be preferable to use in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled *About Windows Authentication for WinRM Monitoring* for more on WinRM authentication.

To configure Windows to allow monitoring using a non-Administrator service account, see the section below titled *Windows Server 2012: Configuring a WinRM Service Account on Individual Windows Systems* or the section titled *Windows Server* 2012: Group Policy Deployment of a PowerShell Script for Service Account Configuration.

If the credentials listed are correct, click **See All** and add the server to Zenoss.

vi. If the credentials listed are not appropriate to the target server, the server must be added and the server's individual *zWinRMUser* and *zWinRMPassword* configuration properties must be set. Perform the following steps to add the server information:

a. Add the server to the **Server/Microsoft/Windows** device class, but opt out of modeling the device when adding it:
  - If you are adding via the web interface, leave the **Model Device:** box unchecked.
  - If you are adding via the zenbatchload command, be sure the device has the --nomodel flag set.

b. When the device displays in the device list, click on its name.

c. Click on **Configuration Properties**, and set the configuration properties for *zWinRMUser* and *zWinRMPassword*, supplying the appropriate Windows credentials.

d. Model the device by clicking the Action Wheel (gear-shaped) icon in the lower left and select **Model Device...**

Windows Server 2012: Configuring Individual Servers to Use a Domain Service Account & Encrypt Credentials with Kerberos

The Zenoss master and / or any collectors tasked with monitoring Windows servers with Kerberos must have Kerberos installed on the host operating system.

1. Log in to the host as *root*, or as a user with *superuser* privileges.
2. Determine whether the Kerberos authentication package is installed:

```
# rpm -qa | grep -i krb5-workstation
```

3. If the command returns a result, Kerberos authentication is installed and no additional action is necessary.
4. If the command does not return a result, install Kerberos:

```
# yum -y install krb5-workstation
```

The Kerberos authentication process requires an available ticket granting server. In the Microsoft Active Directory (AD) environment, the AD Server also acts as the Key Distribution Center (KDC). The *zWinKDC* configuration property in Zenoss must be set to the IP address of the AD Server. Each collector that monitors Windows servers must be able to send Kerberos packets to this server. To specify the ticket granting server in Zenoss, perform the following steps:

1. In the Zenoss web UI, navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class.
3. Click **Details**.
4. Edit the configuration property for *zWinKDC* to specify the IP address of your Active Directory Server.
5. Edit the value for *zWinRMUserName* to be the complete domain name of the user, for example, *administrator@test.loc*.

Note: A *zWinRMUserName* value in the form of *user@domain* is the trigger for Zenoss to use Kerberos encryption for credentials. When the value of *zWinRMUsername* takes the form of *user*[only] instead of *user@domain,* Zenoss will not use Kerberos.

Note: For ease of setup and testing, the local Administrator account can be used in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled *About Windows Authentication for WinRM Monitoring* for more on WinRM authentication.

To configure Windows to allow monitoring using a non-Administrator service account, see the section below titled *Windows Server 2012: Configuring a WinRM Service Account on Individual Windows Systems* or the section titled *Windows Server* 2012: Group Policy Deployment of a PowerShell Script for Service Account Configuration.

Note: The Zenoss server and collectors must be able to resolve the target server's pointer records (PTR) to their Active Directory fully qualified domain name. Administrators can meet this requirement by using one of three methods:

i. Configuring the Zenoss server to access the Windows DNS server for its DNS resolutions.

ii. Manually entering PTR records for each server in to the /etc/hosts file.

   For example, the server *r2d2.example.com* at the IP address **77.77.77.77** has the following PTR record:

```
77.77.77.77 r2d2.example.com
```

iii. Using the `zWinRMServerName` property as follows:

- Specify the monitored server's name with the `zWinRMServerName` property field.

  Note: The `zWinRMServerName` property should only be used in conjunction with domain authentication when the DNS PTR record for a monitored server's managed IP address does not resolve to the name by which the server is known in Active Directory.
  For example, if *myserver1* is known as **myserver1.ad.example.com** by Active Directory and is being managed by IP address *192.51.100.21*, but IP address 192.51.100.21 resolves to *www.example.com*, you must set the zWinRMServerName property to **myserver1.ad.example.com** for domain authentication to work.

- If many Windows servers in your environment do not have DNS PTR records that match Active Directory, it is recommended that you:
  - set the monitored device's name to be the fully-qualified Active Directory name in Zenoss
  - set **zWinRMServerName** to `${here/titleOrId}` at the */Server/Microsoft/Windows* device class.

This method avoids setting the `zWinRMServerName` property on every device.

We recommend that you leave the `zWinRMServerName` property blank if local authentication is used, or DNS PTR records match the Active Directory listings. The result is that Zenoss does not have to rely on DNS resolution while monitoring and it avoids the additional overhead of configuring the `zWinRMServerName` properties.

Windows Server 2012: Improving Individual Server Security - Specify SSL for WinRM & WinRS

To successfully encrypt the payload between Resource Manager and Windows clients, you must install a *Server Authentication* certificate on each monitored server. Log on to your Certificate Authority server as a user with Administrator privileges to create a Certificate Template for use in creating each server's certificate. This step only needs to be completed once because the new Certificate Template is then used repeatedly to create each server's certificate. In the following steps, the standard *Web Server Certificate Template* is duplicated to create a new Certificate Template.

1. Press the **Windows** key on the keyboard to display the *Start* screen.
2. Click the **Windows PowerShell** tile.
3. Launch the **Microsoft Management Console** (mmc). Enter the following command:

   ```
   mmc
   ```

   Within the mmc create the duplicate template:

   i. Click the **File** menu, and select **Add/Remove Snap-in...** to display the *Add or Remove Snap-ins* dialog.
   ii. From the list on the left, select **Certificate Templates**.
   Note: If the **Certificate Templates** option does not display in the list, you must add the CA role to your server.
   iii. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
   iv. Click **OK**.
   v. Click on **Certificate Templates ([server name])** in the window on the left to display the full list of Certificate Templates.
   vi. Scroll down the list and locate **Web Server**.
   vii. Right click the *Web Server* template and select **Duplicate Template** to display the *Properties of New Template* window.
   viii. Select the **Request Handling** tab, and check the box next to *Allow private key to be exported*.
   ix. Select the **General** tab and specify a value for *Template display name*.
   x. Select the **Security** tab and add the certificate authority computer account to the template with at minimum *Enroll* permissions.
   xi. Click **OK** to save the changes and exit the *Properties of New Template* window.

4. In the mmc, configure the *Certificate Template*:

   i. Click the **File** menu.
   ii. Select **Add/Remove Snap-in...**
   iii. From the list on the left, select **Certification Authority**.
   iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
   If a window titled *Certification Authority* displays:

      a. Select the radio button next to *Local computer* under *This snap-in will always manage*:
      b. Click **Finish**.
      c. Click **OK**.

   v. Expand the list under **Certification Authority (Local)** and the list under your server name.
   vi. Right click **Certificate Templates** in the list under your server name.
   vii. Select **New => Certificate Template to Issue**.

viii. In the *Enable Certificate Templates* window, select the new template you created in the previous steps.
ix. Click **OK**.
x. Exit the mmc:

Select **File > Exit**

Creating a Certificate for Each Server

In the following steps, use the new certificate template to create a certificate for each server you want to monitor using SSL encryption. These steps are repeated for each server.

1. If necessary, launch the Microsoft Management Console (mmc). Press the **Windows** key on the keyboard to display the *Start* screen.
2. Click the Windows PowerShell tile.
3. Launch the **Microsoft Management Console** (mmc) with the following command:

```
mmc
```

In the mmc:

i. Click the **File** menu.
ii. Select **Add/Remove Snap-in...**.
iii. From the list on the left, select **Certificates**.
iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
v. In the *Certificates* snap-in window, select *Compute account* under **This snap-in will always manage certificates for:**
vi. Click **Next** (or **Finish** if your using an existing mmc console).
vii. Click **Local computer** under **This snap-in will always manage:** if you are presented with the *Select Computer* dialogue (which occurs if opening a new mmc console).
viii. Click **Finish**.
ix. Click **OK**.

4. Request and enroll the new certificate. In the *Certificate* mmc:

i. Navigate to **Console Root > Certificates (Local Computer) > Personal > Certificates**.

ii. Select **Action** in the menus at the top of the mmc to display the drop down list.

iii. Select **All Tasks > Request New Certificate**.

iv. Click **Next** to display the next window with *Active Directory Enrollment Policy* highlighted.

v. Click **Next**.

vi. Place a check mark in the box next to your copied certificate template and click the link to launch the *Properties* edit window.

a. In the **Subject** tab, choose **Common name** from *the Type:* drop-down of the *Subject name* field. Enter the fully qualified domain name of the server to be monitored (for example, *mytestmachine.mynetwork.com*) in the **Value:** field.

b. Click **Add**.

c. If desired, enter additional identification information, including the organization, street address, etc., in the same manner.

d. Select the **General** tab and populate the *friendly name* field.

vii. Click **OK**.

viii. Click **Enroll**.

ix. Click **Finish**.

5. Expand the tree under **Certificates**.
6. Expand the tree under **Personal**.
7. Click on **Certificates** to highlight it and display a list of certificates on the right.
8. Right click the new certificate and select **All Tasks**.

   i. Select **Export**.
   ii. In the *Certificate Export Wizard* window, click **Next**.
   iii. Select the radio button next to **Yes, export the private key**.
   iv. Click **Next**.

9. On the next page:

   i. Verify that the radio button next to **Personal Identification Exchange - PKCS #12 (.pfx)** is selected.
   ii. Verify that the checkbox next to Include all certificates in the certification path if possible is checked.
   iii. Click **Next**.

10. On the *Security* page of the wizard:

    i. Check the box next to **Password**.
    ii. Create a password to secure the private key.
    iii. Click **Next**.

11. On the *File to Export* page:

    i. Select a *destination* for the key export.
    ii. Create a *file name*.
    iii. Click **Save**
    iv. Click **Next**.

12. On the *Completing the Certificate Export Wizard* page, click **Finish**.
13. Click **OK** to close *the Certificate Export Wizard*.
14. Move or copy the exported certificate to the target (monitored) server.

Installing the Certificate on the Target Computer

1. On the target computer, launch the Microsoft Management Console (mmc) with the following command:

```
mmc
```

2. In the mmc:

   i. Click the **File** menu.
   ii. Select **Add/Remove Snap-in...**
   iii. From the list on the left, select **Certificates**.

iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
v. In the *Certificates* snap-in window, select **Computer account** under **This snap-in will always manage certificates for:**.
vi. Click **Next**.
vii. On the *Select a computer page*, click the radio button next to **Local computer**.
viii. Click **Finish**.
ix. Click **OK** on the *Add or Remove Snap-ins* page.

Importing the Certificate

1. In the mmc console, expand the **Certificates (Local Computer)** branch of the tree.
2. Right click **Personal**.
3. Select **All Tasks => Import**.
4. On the first page of the *Certificate Import Wizard*, click **Next**.
5. On the *File to import* page:

    i. Click **Browse**.
    ii. Navigate to the location of the certificate copied to the target system above.
    iii. Select the file.
    Note: You might need to change the file type in the file browser window to *Personal Information Exchange* for the file to display.
    iv. Select the certificate file.
    v. Click **Open**.
    vi. Click **Next**.

6. On the *Private key protection* page:

    i. Enter the password for the key.
    ii. Verify that the checkboxes for **Include all Extended Properties** and **Mark this key as exportable** are selected.
    iii. Click **Next**.

7. On *the Certificate Store* page:

    i. Select the radio button next to **Place all certificates in the following store**.
    ii. Verify that *Personal* appears in the field for **Certificate Store**.
    iii. Click **Next**.

8. On the *Completing the Certificate Import Wizard* page, click **Finish**.
9. Click **OK** to exit the *Certificate Wizard*.

Verifying the Details and Copying the Thumbprint

1. In the mmc console:

    i. Expand the *Certificates (Local Computer)* branch of the tree.
    ii. Expand *Personal*.
    iii. Click on **Certificates**.
    iv. Double click on the certificate to view its details.

2. In the **General** tab of the *Certificate* window:

    i. Verify that the *hostname* is correct for the target server.
    ii. Select the **Details** tab
    iii. Scroll down to **Thumbprint** in the *Field* list.
    iv. Click on **Thumbprint**.
    v. Copy the thumbprint from the lower window for use in later steps.

3. If the server has not been previously configured for monitoring using WinRM, complete the steps listed above in the section Windows Server 2012: Configuring WinRM and WinRS on Individual Servers (Basic Authentication, no Encryption) on page 10 and omit the step that specifies SSL not be used. Substitute the steps in the following section, Configuring the Firewall (below) for firewall configuration. If the server has previously been configured for monitoring but without using SSL, proceed directly to the section, Configuring the Firewall (below).

Configuring the Firewall

1. Configure the firewall to allow connections on port 5986 on individual servers. If desired, use these instructions to instead modify a Group Policy object (for example as directed in Page 4 of this document) to make the change on large numbers of servers.

    i. Press the **Windows** key on the keyboard to display the *Start* screen.
    ii. Click the **Server Manager** tile.
    iii. Click **Local Server** on the left.
    iv. Edit the Firewall profile currently in use. Click the value to the right of **Windows Firewall** to change the value.
    For example, you might see *Windows Firewall* in grey font and to the right of it, in blue font, **Domain: On**.
    In this case, click the blue **Domain On** value.
    v. Click on **Advanced Settings** on the left.

2. In the *Windows Firewall with Advanced Security* window:

    i. Click on **Inbound Rules** on the left.
    ii. Click on **New Rule...** on the far right under **Actions**.

3. In the *New Inbound Rule Wizard* window:

    i. Select the radio button next to **Port**.
    ii. Click **Next**.
    iii. Verify that the radio buttons next to **TCP** and **Specific local ports** are selected.
    iv. Enter the value `5986` in the field for **Specific local ports**.
    v. Click **Next**.
    vi. On the next page, verify that the radio button next to **Allow the connection** is selected.
    vii. Click **Next**.
    viii. On the next page, select the firewall profiles for which the rule should apply.
    ix. Click **Next**.
    x. On the next page, give the rule a name.
    xi. Click **Finish**.

Creating the WinRM Listener Using SSL

1. Press the **Windows** key on the keyboard to display the *Start* screen.

2. Click the *Windows PowerShell* tile.

3. At the PowerShell command line, type the following command, substituting your values for the certificate *thumbprint* and *serverfqdn* (server fully qualified domain name of the monitoring server):

```
winrm create
winrm/config/Listener?Address=*+Transport=HTTPS  '@{Hostname="[serverfqdn]";C
ertificateThumbprint="[thumbprint]"}'
```

for example:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS '@{Hostname="
mytestmachine.mynetwork.com";CertificateThumbprint="07bfff656edab6d9b4dd27f02
0f768f54fee5eb8"}'
```

Note: The thumbprint value must be entered without the spaces displayed in the *Detail* tab of the *Certificate information* window. For example, the displayed value: `07 bf ff 65 6e da …`
must be entered as: `07bfff656eda…`

4. Specify *https (SSL)* instead of *http* connections. Enter the following command:

```
winrm s winrm/config/service '@{AllowUnencrypted="false"}'
```

Note: If this is already controlled through a policy, an error displays. In that case, modify the appropriate GPO. The instructions on Page 2 of this document can be used as a guide.

Adding the Server to Zenoss

In the Zenoss web UI:

1. Navigate to the **Infrastructure** page.
2. If the server has not yet been added to Zenoss, add it the **Server/Microsoft/Windows** device class and opt out of modeling.
3. Click on the name of the target (monitored) server (or on the **Server/Microsoft/Windows** device class if you would like these changes to apply to all Windows servers).
4. Click on Configuration Properties.
5. Edit the configuration property for *zWinScheme* to be *https*.
6. Edit the value for *zWinRMPort* to be *5986*.
7. Verify that the values for *zWinRMUser* and *zWinRMPassword* are correct. Correct means the appropriate Windows credentials. Edit as necessary.
8. To verify that all settings are correct, model the device. Click the **Action Wheel** (gear-shaped) icon in the lower left and select **Model Device...**

Windows Server 2012: Configuring a WinRM Service Account on Individual Windows Systems

See the section above titled *About Windows Authentication for WinRM Monitoring* if necessary for more background on Windows permissions requirements when monitoring with WinRM.

Note: You cannot create a local service account if the machine is configured as a domain controller (AD DS) because the *local users and groups* options no longer exist in that configuration. There are no local accounts on a domain controller, only domain accounts.

Complete the following steps on each non-domain controller server to configure your service account:

1. Add a new local user for use as a service account:
   i. Open *Server Manager*.
   ii. Click on **Tools** in the upper right and select **Computer Management** from the menu that displays.
   iii. In the left pane of the *Computer Management* window, expand **Local Users and Groups**.
   iv. Right click on **User** and select **New User** from the menu that displays.
   v. Complete the *New User* form. Uncheck **User must change password at next logon** and check (if desired) the **Password never expires** box.
   vi. Click **Create.**
   vii. Click **Close** to exit the *New User* form.
2. Copy your permissions configuration script, for example an edited version of the *zenoss-lpu.ps1* script, to the target server.
3. Run the PowerShell Script:
   i. Press the **Windows** key on the keyboard to display the *Start* screen.
   ii. Click the **Windows PowerShell** tile.
   iii. Run your service account configuration script by typing the full path to the script in the command line, then appending the script with the `–u` option and the name of your service account. For example, if you are using an edited version of the zenoss-lpu.ps1 script and your service account is named “benny,” enter the command at the PowerShell prompt:

```
C:\tmp\zenoss-lpu-ps1 –u benny
```

Note: depending on the security policies enforced on your server, you might encounter an error such as:

```
File C:\tmp\zenoss-lpu-ps1 cannot be loaded because running scripts is
disabled on this system…..
```

If you encounter this error, you can bypass the security restrictions for this script by including the `–executionpolicy bypass` option, for example:

```
Powershell -executionpolicy bypass -file C:\tmp\zenoss-lpu.ps1 -u benny
```

Windows Server 2012: Group Policy Deployment of a PowerShell Script for Service Account Configuration

Refer to the section above titled *About Windows Authentication for WinRM Monitoring* for background on service account requirements.

Prerequisites for Configuring a Service Account

The prerequisites for configuring a service account include:

- Creation of a domain user account for use as the service account.
- Completion of the appropriate preparatory sections.

Creating the Domain User (Service) Account

Perform the following to create a new domain user (service) account, if necessary:

1. Log on to an Active Directory server for the domain.
2. Open *Server Manager* and click **Tools** in the upper right**.**
3. Select **Active Directory Users and Computers** from the drop-down list.
4. In the left pane of the *Active Directory Users and Computers* window, find and expand your domain, for example, *doctest.loc.*
5. Right-click *Users* and select **New > User**
6. In the *New Object – User* window, provide a **First name** and a **User logon name**, *zenny* for example.
7. Verify the domain field has the correct domain identification. For example, *@doctest.loc*
8. Click **Next** to display the password dialog for the new user.
9. In the *Password* fields, enter and verify the new user password.
10. Uncheck the **User must change password at next logon**.
11. Check the option for **Password never expires**. We recommend this option to prevent issues later on because your new domain user (*zenny* in this example) never logs on as a human user.
12. Click **Next**.
13. Click **Finish**. Your new user, *zenny* for example, displays in the list of users for the domain.

Completing Preparatory Sections

The following procedure assumes that you have completed the following preparatory sections:

- Windows Server 2012: Configuring Firewall Group Policies

  Note: This method of deploying a PowerShell script across a large group of Windows systems is most likely to be employed in combination with the use of a single domain service account for WinRM authentication. The use of a domain service account mandates the use of Kerberos to encrypt credentials. See the relevant section in this document for instructions on configuring a domain service account and Kerberos if you have not already:

- Windows Server 2012: Improving Security

PowerShell Script Deployment

Perform the following procedure to create a new GPO and to deploy the PowerShell script.

1. Create your service account configuration script (or edit, as appropriate, the sample script referenced above in the section titled *About Windows Authentication for WinRM Monitoring*).

2. Copy the script (for example "`zenoss-lpu.ps1`") to a *Netlogon* folder such as

   ```
   \\yourdomain\SYSVOL\yourdomain\scripts
   ```

3. Open *Group Policy Management*, from the **Server Manager** console:

   Click **Tools** in the upper right, and then choose **Group Policy Management.**

4. Create a new policy.
   i. In the left pane, navigate to:

      Forest: *yourdomain* **> Domains >** *yourdomain* **> Group Policy Objects**

   ii. Right click **Group Policy Objects**
   iii. Select **New** to display the *NEW GPO* dialog.
   iv. Name your policy, for example: *zenoss_lpu*
   v. Click **OK** to save and exit the *New Policy* window.

5. Edit your new policy.
   i. In the left pane, navigate to your new *Group Policy Object*. For example:

      Forest: *yourdomain* **> Domains >** *yourdomain* **> Group Policy Objects > zenoss_lpu**

   ii. Right click the policy and select **Edit** to display the *Group Policy Management Editor*.
   iii. In the left pane of the Group Policy Management window, navigate to:

      Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown)

   iv. Click **Scripts (Startup/Shutdown)**.
   v. In the right pane (Scripts (Startup/Shutdown), double-click **Startup** to launch the *Startup Properties* dialog.
   vi. In the *Startup Properties* dialog box, select the **PowerShell Scripts** tab.
   vii. Click **Add** to display the *Add a Script* dialog box:
      a. Specify the script name and path. In the *Script Name* field, enter the path to the script, or click Browse to locate the script file.
         Note: Scripts should be located in the Netlogon shared folder on the domain controller. For example:
         \\yourdomain`\SYSVOL\yourdomain\scripts`

      b. Select the `zenoss-lpu.ps1` PowerShell script.
      c. Click **Open**.
      d. In the **Script Parameters** box, enter *-u yourusername@yourdomain* for a domain user or *-u yourusername* for basic authentication of a local computer account user.

         Note: Basic authentication relies on local computer accounts. To successfully authenticate to any particular computer, you must have a local account on that machine.

      e. Click **OK** to save the information and exit the *Add a Script* window.

         If you have multiple scripts and want them to run in a particular order, use the Up and Down buttons in the Startup Properties window to set their run order.

      f. Click **OK** to exit the *Startup Properties* window.

6. Exit the *Local Group Policy Editor*:

   File > Exit

7. Link your new GPO to one or more Organizational Units (OU) containing servers to which you want to have the policies applied. Alternatively, you can apply the policies to all Windows servers in the domain by linking the new GPO to the domain itself. To link the GPO to the domain, complete the following process.

   Note: Substitute a specific OU for the domain if you want to link only to a subset of servers.

   i. Right-click your domain in the left pane of the *Group Policy Management* window.
   ii. Choose **Link an Existing GPO...**
   iii. Select your new GPO from the list that displays.
   iv. Click **OK** to complete the process.

8. Exit the Group Policy Management window:

   File > Exit

9. Manually refresh Group Policy from the command prompt of target servers:

   ```
   gpupdate /force
   ```

10. Reboot your member servers to have the script run for the first time.

Windows Server 2008R2

Configuring Windows Server 2008 Using Group Policy (Basic Authentication, no Encryption)

1. Log on to a domain controller as a user with 'Domain Admin' privileges.
2. Launch the Group Policy Editor. Use one of the following methods:

    - Click the **Start** button and navigate to **All Programs > Administrative Tools > Group Policy Management**.
    - Click **Start**, enter the word *Group* in the search field and select **Group Policy Management**. **Note:** The *Group Policy Management Console (GPMC)* is normally installed by default on the domain controller. You can install GPMC on a member server as long as it is a member of the domain. If it is not present and you need to install it, use the instructions provided at: http://technet.microsoft.com/en-us/library/cc725932.aspx.

3. Right-click **Group Policy Objects** and select *New*. In the form that displays:

    i. Enter a name for your new Group Policy Object, for example, *WinRM_Monitoring*.
    ii. Leave "(none)" in the **Source Starter GPO** field.
    iii. Click **OK** to save and exit the form.

4. Select your new **Group Domain Policy Object**, *WinRM_Monitoring*, for example.
5. Right click your new **Group Domain Policy Object** and select *Edit* to open the Group Policy Management Editor.
6. In the Group Policy Management Editor window, expand the *Computer Configuration* section of the tree and navigate the tree to:

    ```
    Policies\Administrative Templates:Policy...\Windows Components\Windows
    Remote Management(WinRM)
    ```

7. Enable remote server management:

    i. Click on **WinRM Service** to access the *WinRM Service Group Policy* settings in the right pane.
    ii. Double-click the **Allow automatic configuration of listeners** property.
    iii. Click the **Enabled** radio button.
    iv. Place an asterisk (' * ') as a wildcard in the *IPv4 filer* and *IPv6 fields* or specify a range of IP addresses for WinRM to listen on.
    v. Click **OK** at the bottom to submit the form.

8. Enable authentication:

    i. Double-click the **Allow Basic authentication** property in the right pane.
    ii. Select the **Enabled** radio button.
    iii. Click **OK** at the bottom to submit the form.

9. Specify unencrypted traffic:

    i. Double-click the **Allow unencrypted traffic** property.
    ii. Select the **Enabled** radio button.
    iii. Click **OK** at the bottom to submit the form.

10. Select *Windows Remote Shell* in the left pane to set its **Group Policy** settings. This is located in the group policy tree at the following path, which should be located right below *WinRM* service in the tree: `Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell`

11. Configure remote shell access:

    i. In the right pane, double-click **Allow Remote Shell Access**.
    ii. Select the **Enabled** radio button.
    iii. Click **OK** at the bottom to submit the form.

12. Configure shell processes:

    i. In the right pane, double-click Specify maximum number of processes per Shell.
    ii. Select the **Enabled** radio button.
    iii. Enter the value `2,000,000,000` (without commas or spaces) in the *MaxProcessesPerShell* field.
    iv. Click **OK** at the bottom to submit the form.

13. Configure the number of remote shells:

    i. In the right pane, double-click Specify maximum number of remote shells per user.
    ii. Select the **Enabled** radio button.
    iii. Enter the value `2,000,000,000` (without commas or spaces) in the *MaxShellsPerUser* field.
    iv. Click **OK** at the bottom to submit the form.

14. Configure the shell timeout value:

    i. In the Right pane, double-click **Specify Shell Timeout**.
    ii. Select the **Enabled** radio button.
    iii. Enter the value `7,200,000` (without commas or spaces) in the **ShellTimeOut field**.
    iv. Click **OK** at the bottom to submit the form.

Windows 2008: Configuring Firewall Group Policies

Windows firewall must allow incoming ICMP (ping) requests. Additionally, WinRM listens on port 5985 when SSL is not used and on port 5986 when SSL is used. These ports must be opened on the firewalls of monitored servers. You can use Group Policy to open these ports on all servers across the organization.

In the **Group Policy Management Editor**, navigate to:
`Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security - LDAP;...\Inbound Rules`

1. Create a new *Inbound Rules* policy:

    i. Right click **Inbound Rules** in the left pane.
    ii. Select **New Rule...** to display the *New Inbound Rule Wizard*
    iii. Select the **Predefined** radio button in the right pane.
    iv. Select **Windows Remote Management** from the drop down list.
    v. Click **Next**.
    vi. Ensure that all items in the list are checked.
    vii. Click **Next**.
    viii. Ensure that the **Allow the connection** radio button is selected.
    ix. Click **Finish**.

2. Exit the Group Policy Management Editor:
   Select **File > Exit**

3. Link your new GPO to one or more Organizational Units (OU) containing servers to which you want to have the policies applied. Alternatively, you can apply the policies to all Windows servers in the domain by linking the new GPO to the domain itself. To link the GPO to the domain, complete the following process.

   Note: Substitute a specific OU for the domain if you want to link only to a subset of servers.

   i. Right-click your domain in the left pane of the *Group Policy Management* window.
   ii. Choose Link an Existing GPO...
   iii. Select your new GPO from the list that displays, *WinRM_Monitoring*, for example.
   iv. Click **OK** to complete the process.

4. Exit the *Group Policy Management* window:
   Select **File > Exit**

5. Before adding servers to Zenoss for monitoring, wait a sufficient amount of time for Group Policy to automatically update on the server(s). Alternatively, you can manually refresh Group Policy on target servers by typing the following at the command prompt:

```
gpupdate /force
```

Windows 2008: Configuring Windows Credentials in Zenoss

When one or more servers are ready for addition to Zenoss, perform the following steps within the Zenoss web interface:

1. Navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class.
3. Click the **Details** icon.
4. Click **Configuration Properties** in the left pane.
5. In the right pane, set the configuration properties for *zWinRMUser* and *zWinRMPassword*, supplying the appropriate Windows credentials.

   Note: For ease of setup and testing, the local Administrator account can be used in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled *About Windows Authentication for WinRM Monitoring* for more on WinRM authentication.

   To configure Windows to allow monitoring using a non-Administrator account, see the sections below titled *Windows 2008: Configuring a WinRM Service Account on Individual Servers*, or *Windows 2008: Using Group Policy to Configure a Service Account on all Servers*.

6. Click **See All**.
7. Add windows servers using the web interface or `ZenBatchload`.

Windows 2008: Improving Security by Using a Domain Service Account & Encrypting Credentials with Kerberos

Note: When switching from the use of local system accounts for authentication to a single domain service account, the use of Kerberos to encrypt credentials is mandatory.

Note: The Zenoss master and / or any collectors tasked with monitoring Windows servers that use Kerberos must have Kerberos also installed on the host operating system.

The Zenoss master and / or any collectors tasked with monitoring Windows servers that use Kerberos must have Kerberos also installed on the host operating system.

1. Log in to the host as *root*, or as a user with *superuser* privileges.
2. Determine whether the Kerberos authentication package is installed:

   ```
   # rpm -qa | grep -i krb5-workstation
   ```

3. If the command returns a result, Kerberos authentication is installed and no additional action is necessary.

   If the command does not return a result, install Kerberos:

   ```
   # yum -y install krb5-workstation
   ```

The Kerberos authentication process requires an available ticket granting server. In the Microsoft Active Directory (AD) environment the AD Server also acts as the Key Distribution Center (KDC). The zWinKDC configuration property in Zenoss must be set to the IP address of the AD Server. Each collector used to monitor Windows servers must be able to send Kerberos packets to this server. To specify the ticket granting server in Zenoss, perform the following steps:

1. In the Zenoss web UI, navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class in the left pane.
3. Click the **Details** icon.
4. Click **Configuration Properties** in the left pane.
5. Edit the configuration property in the right pane for *zWinKDC*. Double click *zWinKDC* and specify the IP address of your Active Directory Server.
6. Edit the value for *zWinRMUser* name to be the *complete domain name* of the user, for example, *administrator@test.loc*.

   Note: A *zWinRMUser* name value in the form of *user@domain* is the trigger for Zenoss to use Kerberos encryption for credentials. When the value of *zWinRMUser* name takes the form of *user*[only] instead of *user@domain,* Zenoss will not use Kerberos.

   Note: The Zenoss server and collectors must be able to resolve the target server's pointer records (PTR) to their Active Directory fully qualified domain name. Administrators can meet this requirement by using one of three methods:

   i. Configuring the Zenoss server to access the Windows DNS server for its DNS resolutions.
   ii. Manually entering PTR records for each server in to the /etc/hosts file.

      For example, the server *r2d2.example.com* at the IP address **77.77.77.77** has the following PTR record:

      ```
      77.77.77.77 r2d2.example.com
      ```

   iii. Using the *zWinRMServerName* property by specifying the monitored server's name with the `zWinRMServerName` property field.

Note: The *zWinRMServerName* property should only be used in conjunction with domain authentication when the DNS PTR record for a monitored server's managed IP address does not resolve to the name by which the server is known in Active Directory.
For example, if *myserver1* is known as **myserver1.ad.example.com** by Active Directory and is being managed by IP address *192.51.100.21*, but IP address 192.51.100.21 resolves to *www.example.com*, you must set the zWinRMServerName property to **myserver1.ad.example.com** for domain authentication to work.

- If many Windows servers in your environment do not have DNS PTR records that match Active Directory, it is recommended that you:
    - set the monitored device's name to be the fully-qualified Active Directory name in Zenoss.
    - set `zWinRMServerName` to `${here/titleOrId}` at the */Server/Microsoft/Windows* device class.

This method avoids setting the `zWinRMServerName` property on every device.

We recommend that you leave the `zWinRMServerName` property blank if local authentication is used, or DNS PTR records match the Active Directory listings. The result is that Zenoss does not have to rely on DNS resolution while monitoring and it avoids the additional overhead of configuring the `zWinRMServerName` properties.

Windows 2008: Configuring WinRM and WinRS on Individual Servers (Basic Authentication, no Encryption)

Perform the following steps to configure WinRM and WinRS:

1. Log on to the target server as a user with *Domain Admin* or local *Admin* privileges.
2. Launch Windows PowerShell:

   - Click the **Windows PowerShell** icon if it exists in the tool bar.
   - Click **Start**, enter the word *Power* in the search field and select **Windows PowerShell**.

3. Within Windows PowerShell:

   i. Configure the system to accept WS-Management requests from other systems. Enter the following at the command prompt:

   ```
   winrm quickconfig
   ```

   ii. Specify *http* instead of *https* (SSL) connections. Enter the following command:

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

   iii. Configure the maximum number of concurrent operations per user. Use the following command:

   ```
   winrm s winrm/config/service
   '@{MaxConcurrentOperationsPerUser="4294967295"}'
   ```

   iv. Configure the *maximum number of shells per user*. Enter the following command:

   ```
   winrm s winrm/config/winrs '@{MaxShellsPerUser="2147483647"}'
   ```

   v. Configure the *idle timeout*. Enter the following command:

   ```
   winrm s winrm/config/winrs '@{IdleTimeout="7200000"}'
   ```

   vi. Specify *Basic Authentication*. Enter the following command:

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

   vii. Exit PowerShell:

   ```
   exit
   ```

4. Configure the firewall to allow connections on port 5985.

   i. Click the **Start** button and navigate to **All Programs > Administrative Tools > Server Manager**.
   ii. In the left pane, navigate to **Server Manager > Configuration > Windows Firewall with Advanced Security>Inbound Rules**.
   iii. In the right pane, scroll down through the list that displays and confirm that *Windows Remote Management* is enabled for the current firewall profile in use (and any other profiles required).

Note: Remote management includes allowing connections on port 5985 when SSL is not being used.

If **Windows Remote Management** does not appear in the right pane:

a. Right click **Inbound Rules** in the left pane.
b. Select **New Rule...**
c. Select the **Predefined** radio button.
d. Select **Windows Remote Management** from the drop down list.
e. Click **Next**.
f. Ensure that all items in the list are checked.
g. Click **Next**.
h. Ensure that the **Allow the connection** radio button is selected.
i. Click **Finish**.

5. Configure Zenoss to monitor the server. Perform the following steps within the Zenoss web interface:

i. Navigate to the **Infrastructure** page.
ii. Select the **Server/Microsoft/Windows** device class.
iii. Click the **Details** icon.
iv. Click **Configuration Properties** in the left pane.
v. In the right pane, confirm that the values for the *zWinRMUser* and *zWinRMPassword* properties are populated with the correct Windows credentials for your Windows servers.

Note: For ease of setup and testing, the local Administrator account can be used in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled *About Windows Authentication for WinRM Monitoring* for more on WinRM authentication.

To configure Windows to allow monitoring using a non-Administrator account, see the section below titled *Windows 2008: Configuring a WinRM Service Account on Individual Servers*.

vi. If the credentials listed are correct, click **See All** and add the server to Zenoss.
vii. If the credentials listed are not appropriate to the target server, the server must be added and the server's individual *zWinRMUser* and *zWinRMPassword* configuration properties must be set. Perform the following steps to add the server information:

a. Add the server to the **Server/Microsoft/Windows** device class, but opt out of modeling the device when adding as follows:
   - If you are adding via the web interface, leave the **Model Device:** box unchecked.
   - If you are adding via the `zenbatchload` command, be sure the device has the *--nomodel* flag set.
b. When the device displays in the device list, click on its name.
c. Click on **Configuration Properties**, and set the configuration properties for *zWinRMUser* and *zWinRMPassword*, supplying the appropriate Windows credentials.

viii. Model the device by clicking the Action Wheel (gear-shaped) icon in the lower left and select **Model Device...**

Windows 2008: Configuring Individual Servers to Use a Domain Service Account & Encrypt Credentials with Kerberos

The Zenoss master and / or any collectors tasked with monitoring Windows servers with Kerberos must have Kerberos installed on the host operating system.

1. Log in to the host as *root*, or as a user with *superuser* privileges.
2. Determine whether the Kerberos authentication package is installed:

   ```
   # rpm -qa | grep -i krb5-workstation
   ```

3. If the command returns a result, Kerberos authentication is installed and no additional action is necessary.
4. If the command does <u>not</u> return a result, install Kerberos:

   ```
   # yum -y install krb5-workstation
   ```

The Kerberos authentication process requires an available ticket granting server. In the Microsoft Active Directory (AD) environment, the AD Server also acts as the Key Distribution Center (KDC). The zWinKDC configuration property in Zenoss must be set to the IP address of the AD Server. Each collector that monitors Windows servers must be able to send Kerberos packets to this server. To specify the ticket granting server in Zenoss, perform the following steps:

1. In the Zenoss web UI, navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class.
3. Click **Details**.
4. Edit the configuration property for *zWinKDC* to specify the IP address of your Active Directory Server.
5. Edit the value for *zWinRMUserName* to be the complete domain name of the user, for example, *administrator@test.loc*.

   Note: A *zWinRMUserName* value in the form of *user@domain* is the trigger for Zenoss to use Kerberos encryption for credentials. When the value of *zWinRMUsername* takes the form of *user*[only] instead of *user@domain,* Zenoss will not use Kerberos.

   Note: The Zenoss server and collectors must be able to resolve the target server's pointer records (PTR) to their Active Directory fully qualified domain name. Administrators can meet this requirement by using one of three methods:

   i. Configuring the Zenoss server to access the Windows DNS server for its DNS resolutions.
   ii. Manually entering PTR records for each server in to the /etc/hosts file.

      For example, the server *r2d2.example.com* at the IP address **77.77.77.77** has the following PTR record:

      77.77.77.77 r2d2.example.com

   iii. Using the *zWinRMServerName* property as follows:
      - Specify the monitored server's name with the *zWinRMServerName* property field.

Note: The zWinRMServerName property should only be used in conjunction with domain authentication when the DNS PTR record for a monitored server's managed IP address does not resolve to the name by which the server is known in Active Directory.
For example, if *myserver1* is known as **myserver1.ad.example.com** by Active Directory and is being managed by IP address *192.51.100.21*, but IP address 192.51.100.21 resolves to *www.example.com*, you must set the `zWinRMServerName` property to **myserver1.ad.example.com** for domain authentication to work.

- If many Windows servers in your environment do not have DNS PTR records that match Active Directory, it is recommended that you:
  - set the monitored device's name to be the fully-qualified Active Directory name in Zenoss
  - set `zWinRMServerName` to ${here/titleOrId} at the */Server/Microsoft/Windows* device class.

This method avoids setting the `zWinRMServerName` property on every device.

We recommend that you leave the `zWinRMServerName` property blank if local authentication is used, or DNS PTR records match the Active Directory listings. The result is that Zenoss does not have to rely on DNS resolution while monitoring and it avoids the additional overhead of configuring the `zWinRMServerName` properties.

Windows 2008: Improving Individual Server Security - Specify SSL for WinRM & WinRS

Creating a New Certificate Template

To successfully encrypt the payload between Resource Manager and Windows clients, you must install a *Server Authentication* certificate on each monitored server. Log on to your Certificate Authority server as a user with *Administrator* privileges to create a Certificate Template for use in creating each server's certificate. This step only needs to be completed once because the new Certificate Template is then used repeatedly to create each server's certificate. In the following steps, the standard *Web Server Certificate Template* is duplicated to create a new Certificate Template.

1. Log on to your Certificate Authority server as a user with Administrator privileges.
2. Launch Windows PowerShell:

   i. Click the **Windows PowerShell** icon if it exists in the tool bar.
   ii. Click **Start**, enter the word *Power* in the search field and select **Windows PowerShell**.

3. Launch the **Microsoft Management Console** (mmc). Enter the following command:

   ```
   mmc
   ```

   Within the mmc create the duplicate template:

   i. Click the **File** menu, and select **Add/Remove Snap-in...**
   ii. From the list on the left, select **Certificate Templates**.
   iii. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
   iv. Click **OK**.

4. Click on **Certificate Templates** in the left window to display the full list of Certificate Templates.

   i. Scroll down the list and locate **Web Server**.
   ii. Right click the *Web Server* template and select **Duplicate Template**. The *Duplicate Template* dialog displays with radio button choices.
   iii. Select **Windows Server 2008 Enterprise** and click **OK** to display the *Properties of New Template window.*
   iv. In the **General** tab specify a value for *Template display name*.
   v. Select the **Request Handling** tab, and check the box next to *Allow private key to be exported*.
   vi. Select the **Security** tab and add the certificate authority computer account to the template with at minimum *Enroll* permissions.
   vii. Click **OK**.

5. In the mmc configure the Certificate Template:

   i. Click the **File** menu.
   ii. Select Add/Remove Snap-in...
   iii. From the list on the left, select **Certification Authority**.
   iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
   If a window titled *Certification Authority* displays:

      a. Select the radio button next to *Local computer* under **This snap-in will always manage:**

b. Click **Finish**.
c. Click **OK**.

v. Expand the list under **Certification Authority (Local)** and the list under your server name.
vi. Right click **Certificate Templates** in the list under your server name.
vii. Select **New => Certificate Template to Issue**.
viii. In the *Enable Certificate Templates* window, select the new template you created in the previous steps.
ix. Click **OK**.

Creating a Certificate for Each Server

In the following steps, use the new certificate template to create a certificate for each server you want to monitor using SSL encryption. These steps are repeated for each server.

1. If necessary, launch the Microsoft Management Console (mmc) with the following command:

```
mmc
```

2. Open the Certificates MMC:

   i. Click the **File** menu.
   ii. Select Add/Remove Snap-in...
   iii. From the list on the left, select **Certificates**.
   iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
   v. In the **Certificates** snap-in window, select the option **This snap-in will always manage certificates for Computer account** to display the *Select Computer* window.
   vi. Select the radio button for **This snap-in will always manage Local Computer**.
   vii. Click **Finish**
   viii. Click **OK**.

3. Request and enroll the new certificate. In the Certificate mmc:

   i. Navigate to **Console Root > Certificates (Local Computer) > Personal > Certificates**.
   ii. Select **Action** in the menus at the top of the mmc to display the drop down list.
   iii. Select **All Tasks > Request New Certificate**.
   iv. Click **Next** to display the next window with *Active Directory Enrollment Policy* highlighted.
   v. Click **Next**.
   vi. Place a check mark in the box next to your copied certificate template and click the link to launch the *Properties* edit window.

      a. In the **Subject** tab, choose *Common name* from the *Type:* drop-down of the *Subject name* field. Enter the fully qualified domain name (for example, *mytestmachine.mynetwork.com*) in the *Value*: field.
      b. Click **Add**.
      c. If desired, enter additional identification information, including the *organization*, *street address*, etc., in the same manner.
      d. Select the **General** tab and populate the *friendly name* field.

   vii. Click **OK**.
   viii. Click **Enroll**.
   ix. Click **Finish**.

4. Export the certificate. In the *Certificates* mmc:

i. Expand the tree under **Certificates - Local Computer > Personal > Certificates**.
ii. Right click the new certificate and select **All Tasks**.
iii. Select **Export** to display the *Certificate Export Wizard*.
iv. In the *Certificate Export Wizard* window, click **Next**.
v. Select the radio button for *Yes, export the private key*. Click **Next**.
vi. On the next page:

a. Verify that the **Personal Information Exchange** radio button is selected.
b. Select the check box for Include all certificates in the certification path if possible.
c. Click **Next**.

5. Create and confirm a password.
6. Click **Next** to display the *File to Export* page.

On the *File to Export page*:

i. Browse to select a *destination* for the exported key.
ii. Create a *file name*.
iii. Click **Save**.
iv. Click **Next**.

7. On the *Completing the Certificate Export Wizard* page, verify the information. Click **<Back** if you need to edit the information.
8. Click **Finish**.
If the export is successful, the *Certificate Export Wizard* displays a success message.
9. Click **OK** to close the message and exit the wizard.
10. Move or copy the exported certificate to the target server.

Installing the Certificate on the Target Computer

1. On the target computer, launch **Windows PowerShell**:
   - Click the **Windows PowerShell** icon if it exists in the tool bar.
     or
   - Click **Start**, enter the word *Power* in the search field and select **Windows PowerShell**.
2. Launch the Microsoft Management Console (mmc):

```
mmc
```

3. Add the **Certificate** snap-in to the mmc:

i. Click the **File** menu.
ii. Select **Add/Remove Snap-in...**
iii. From the list on the left, select **Certificates**.
iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
v. In the Certificates snap-in window, select **Computer account** under *This snap-in will always manage certificates for:.*
vi. Click **Next**.
vii. On the *Select a computer* page, select **Local computer**.
viii. Click **Finish**.
ix. Click **OK** on the *Add or Remove Snap-ins* page.

Importing the Certificate

1. In the mmc console, expand the **Certificates (Local Computer)** branch of the tree.
2. Highlight and right click **Personal**.
3. Select **All Tasks => Import** to launch the *Certificate Import Wizard*.
4. On the first page of the *Certificate Import Wizard*, click **Next**.
5. On the *File to import* page:,

    i. Click **Browse**.
    ii. Navigate to the location of the certificate file you copied to the target system and select the file.
    Note: If your file name does not display, change the file type in the file browser window to *Personal Information Exchange*.
    iii. Click **Open**.
    iv. Click **Next** to display the *Private key protection* page.

6. On the Private key protection page:

    i. Enter the password for the key.
    ii. Verify that the checkboxes for **Mark this key as exportable** and **Include all Extended Properties** are selected.
    iii. Click **Next**. to display the *Certificate Store* page.

7. On the Certificate Store page:

    i. Select **Place all certificates in the following store**.
    ii. Verify that *Personal* appears in the field for Certificate Store.
    iii. Click **Next** to display the Completing the Certificate Import Wizard page.

8. On the *Completing the Certificate Import Wizard* page, verify the certificate information.
9. Click **Finish** to exit the wizard.
If the export is successful, The Certificate Export Wizard displays a success message.
10. Click **OK** to close the message and exit the wizard.

Verifying the Details and Copying the Thumbprint

1. If necessary, launch the mmc with the *Certificate snap-in*. In the mmc console:

    i. Expand the *Certificates (Local Computer)* branch of the tree.
    ii. Expand *Personal*.
    iii. Click on Certificates.
    iv. Double click on the certificate in the right pane to launch the *Certificate* window and view its details.

2. Copy the thumbprint. In the **General** tab of the *Certificate* window:

    i. Verify that the *hostname* is the correct fully qualified domain name for the target server.
    ii. Select the **Details** tab
    iii. Scroll down to **Thumbprint** in the *Field* list.
    iv. Click on **Thumbprint**.

v. Copy the 40 digit thumbprint from the lower window for use in later steps, for example:

3a 79 6b ce 83 82 85 55 32 31 30 11 16 e5 bd 14 f0 2d 61 89

Note: The forty digit thumbprint value that displays contains spaces. These spaces must be removed before using it in commands.

Note: If the server has not been configured for monitoring using WinRM, complete the steps listed in the section **Windows 2008: Configuring WinRM and WinRS On Individual Servers (Basic Authentication, no encryption)**, and omit the step that specifies SSL not be used. Substitute the steps in the following section, *Configuring the Firewall* (below) for firewall configuration.

If the server has been configured for monitoring but without using SSL, proceed directly to the section, *Configuring the Firewall* (below).

Configuring the Firewall

1. Configure the firewall to allow connections on port 5986:

    i. Click the Start button and navigate to **All Programs > Administrative Tools > Server Manager**.
    ii. In the left pane, navigate **to Server Manager > Configuration > Windows Firewall with Advanced Security>Inbound Rules**.

    i. Create a *New Inbound Rule*. Click on **New Rule...** on the right under **Actions** to display the *New Inbound Rule Wizard* window.

2. Create *New Inbound Rules* and specify ports in the *New Inbound Rule Wizard* window:

    i. Select the radio button next to **Port**.
    ii. Click **Next**.
    iii. Verify that the radio buttons next to **TCP** and **Specific local ports** are selected.
    iv. Enter the value *5986* in the field for **Specific local ports**.
    v. Click **Next**.
    vi. On the next page, verify that the radio button next to **Allow the connection** is selected.
    vii. Click **Next**.
    viii. On the next page, select the firewall profiles for which the rule should apply.
    ix. Click **Next**.
    x. On the next page, give the rule a name.
    xi. Click **Finish**.

Creating the WinRM Listener Using SSL

1. Launch the Windows Power Shell:

    i. Click the **Windows PowerShell** icon if it exists in the tool bar.
    or
    ii. Click **Start**, enter the word *Power* in the search field and select **Windows PowerShell**.

2. Create the listener referencing the newly created Certificate. At the PowerShell command line, type the following command, substituting your values for the certificate *thumbprint* and *serverfqdn* (server fully qualified domain name):

```
winrm create
winrm/config/Listener?Address=*+Transport=HTTPS  '@{Hostname="[serverfq
dn]";CertificateThumbprint="[thumbprint]"}'
```

For example:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS
'@{Hostname="mymachinename.mynetwork.com";CertificateThumbprint="3a796b
ce838285553231301116e5bd14f02d6189"}'
```

Note: The thumbprint value must be entered without the spaces that are displayed in the **Detail** tab of the *Certificate Information* window.

3. Specify *https (SSL)* instead of *http* connections. Enter the following command:

```
winrm s winrm/config/service '@{AllowUnencrypted="false"}'
```

Note: If this is already controlled through a policy, an error displays.

Adding the Server to Zenoss

In the Zenoss web UI:

1. Navigate to the **Infrastructure** page.
2. If the server has not yet been added to Zenoss, add it the **Server/Microsoft/Windows** device class and opt out of modeling.
3. Click on the name of the target server.
4. Click on the server's Configuration Properties.
5. Edit the configuration property for *zWinScheme* to be *https*.
6. Edit the value for *zWinRMPort* to be *5986*.
7. Verify that the values for *zWinRMUser* and *zWinRMPassword* are correct. This means the appropriate Windows credentials, for example, *Bill* and *billspassword*, respectively. Edit as necessary.
8. To verify that the settings have been successfully entered, model the device. Click the **Action Wheel** (gear-shaped) icon in the lower left and select **Model Device...**

Windows 2008: Configuring a WinRM Service Account on Individual Servers

See the section above titled *About Windows Authentication for WinRM Monitoring* if necessary for more background on Windows permissions requirements when monitoring with WinRM. Complete the following steps on each server to configure your service account:

1. Add a new local user for use as a service account:
    - i. Open **Server Manager**.
    - ii. Expand *Configuration* in the left pane.
    - iii. Expand *Local Users and Groups* in the left pane.
    - iv. Right click on **Users** and select **New User** from the menu that displays.
    - v. Complete the New User form. Uncheck **User must change password** at next logon and check (if desired) the **Password never expires** box.
    - vi. Click **Create**.
    - vii. Click **Close** to exit the *New User* form.
2. Copy your permissions configuration script, for example the *zenoss-lpu.ps1* script, to the target server.
3. Run the PowerShell Script:
    - i. Click the *Windows PowerShell* icon, if present, in the Taskbar. If the icon is not present, click **Start** in the taskbar and enter “Powershell” in the search field to locate PowerShell.
    - ii. Run your service account configuration script by typing the full path to the script in the command line and append the script with the *-u* option and the name of your service account. For example, if you are using an edited version of the *zenoss-lpu.ps1* script and your service account is named “benny,” enter the following command at the PowerShell prompt:

      ```
      C:\tmp\zenoss-lpu.ps1 –u benny
      ```

Note: depending on the security policies enforced on your server, you might encounter an error such as:

```
File C:\tmp\zenoss-lpu-ps1 cannot be loaded because running scripts is
disabled on this system…..
```

If you encounter this error, you can bypass the security restrictions for this script by including the

`-executionpolicy bypass` option, for example:

```
Powershell -executionpolicy bypass -file C:\tmp\zenoss-lpu.ps1 -u benny
```

Windows 2008: Using Group Policy to Configure a Service Account on all Servers

Important note: If the Group Policies for your Windows 2008R2 domain have been left at their default settings, Windows may block the execution of PowerShell scripts over the network without active user confirmation at the command line that the script should be permitted to run. This request for user intervention can cause Windows systems to hang on boot for an extended period when a startup script is run, pending user intervention (which cannot be given because administrators cannot log on to the system while it waits). Group Policy objects that work around this issue can be created that do the following:

1. Set the PowerShell execution policy to *allow all scripts*.
2. Add the hostname (or the hosts's domain) of the server hosting the script on a shared directory in the Trusted Sites Internet Zone.
3. Edit registry keys to disable Internet Explorer's Enhanced Security Configuration (this is necessary to add items to the Trusted Sites Internet Zone).

Administrators should weigh the security implications of these policies against the benefits of being able to deploy the PowerShell script from a central location using Group Policy instead of running the script manually on each server to be modified. To make these changes, complete the next section.

Enabling Script Execution (If Necessary)

1. Click **Start** in the taskbar and enter *Group Policy Management* in the search bar to locate *Group Policy Management*.

   i. In the left pane of the *Group Policy Manager* window, navigate to **Forest: *yourdomain* > Domains > *yourdomain* > Group Policy Objects**

   For example:

   ```
   Forest: doctest.loc > Domains > doctest.loc > Group Policy Objects
   ```

   ii. Right click *Group Policy Objects* and select **New** to display the *NEW GPO* dialog.
   iii. Name your policy, for example *script_execution.*
   iv. Click **OK** to save and exit the *New Policy* window.

2. Edit your new policy.
   i. In the left pane, navigate to your new Group Policy Object. For example:

   ```
   Forest: doctest.loc > Domains > doctest.loc > Group Policy Objects >
   script_execution
   ```

   ii. Right click the policy and select **Edit** to display the *Group Policy Management Editor.*

   a. In the left pane of the *Group Policy Management* window, navigate to:

   ```
   Computer Configuration/Policies/Administrative Templates/Windows
   Components/Internet Explorer/Internet Control Panel/Security Page/
   ```

   b. In the right panel, double click **Site to Zone Assignment List**
   c. Click the **Enabled** radio button
   d. Add the hostname of the system hosting your PowerShell script (or the domain where it is located if broader permissions are desired) by clicking the **Show** button.

Note: In the right *Help* menu you are provided with guidance on how to add domains or individual hosts.

e. Choose the value '2' for your site or domain to put it into the *Trusted Sites Zone*.

f. Click **OK** at the bottom of the form.

iii. In the left pane of the *Group Policy Management* window, navigate to:

```
Computer Configuration/Policies/Administrative Templates/Windows
Components/Windows PowerShell/
```

a. In the right pane, double-click **Turn on Script Execution**

b. In the *Turn on Screen Execution* dialog window, click the **Enabled** radio button.

c. Click **OK**

d. In the dropdown list under *Execution Policy,* choose **Allow all scripts**.

e. Click **OK** at the bottom.

iv. In the left pane of the *Group Policy Management* window, navigate to:

```
Computer Configuration/Preferences/Windows Settings/Registry/
```

a. Right-click on *Registry* and select **New > Registry Item**.

b. Either enter the following Key Path or use the [**…**] button to use the *Registry Item Bowser* to navigate to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed
Components\{A509B1A7-37EF-4b3f-8CFC-4F3A74704073}
```

c. In the lower pane, click **IsInstalled**

d. Click the **Select** button to display the *New Registry Properties* dialog box.

e. In the *New Registry Properties* dialog box, select the **General** tab and verify the following settings:

- *Action* is set to **Update**.
- The *Hive* is **HKEY_LOCAL_Machine**
- The *Key Path* is the one specified in step b.
- The *Value name* is **IsInstalled** and the *Default* box is **unchecked**.
- The *Value type is* **REG_DWORD**
- The checkbox for *Base* is set to **Hexadecimal**

f. Change the *Value data* entry from the Default of *00000001* (enabled) to the new value of **00000000** (disabled)

g. Click **OK** to close the dialog and save the changes.

9. Link your new GPO to one or more Organizational Units (OU) containing servers to which you want the policies applied. Alternatively, you can apply the policies to all Windows servers in the domain by linking the new GPO to the domain itself. To link the GPO to the domain, complete the following process.

   Note: Substitute a specific OU for the domain if you want to link only to a subset of servers.

   i. Right-click your domain in the left pane of the *Group Policy Management* window.
   ii. Choose **Link an Existing GPO...**
   iii. Select your new GPO from the list that displays.
   iv. Click **OK** to complete the process.

10. Exit the Group Policy Management window:

    Select **File > Exit**

11. Manually refresh Group Policy from the command prompt of target servers:

    ```
    gpupdate /force
    ```

    Note: you may need to reboot the server for the Internet Explorer settings to take effect.

Creating the Domain User (Service) Account

Perform the following to create a new domain user (service) account, if necessary:

1. In the left panel of Server Manager, Navigate to your target domain in the tree at the left:
   i. Expand *Roles*
   ii. Expand *Active Directory Domain Services*
   iii. Expand *Active Directory Users and Computers*
   iv. Expand your domain.
2. Right-click *Users* and select **New > User**.
3. In the *New Object – User* window, provide a First name and a User logon name, *zenny* for example.
4. Verify the domain field has the correct domain identification. For example, *@doctest.loc*
5. Click **Next** to display the password dialog for the new user.
6. In the *Password* fields, enter and verify the new user password.
7. Uncheck the selection for **User must change password at next logon.**
8. Check the option for **Password never expires**.
9. Click **Next**.
10. Click **Finish**. Your new user, *zenny* for example, displays in the list of users for the domain.

Completing Preparatory Sections

The following procedure assumes that you have completed the following preparatory sections:

- *Windows 2008: Configuring Firewall Group Policies*
- *Windows 2008: Configuring Windows Credentials in Zenoss*

This procedure requires the PowerShell script *zenoss-lpu.ps1*, available from the Zenoss support site.

Creating the Script GPO

1. Create your service account configuration script (or edit, as appropriate, the sample script referenced above the section titled *About Windows Authentication for WinRM Monitoring*).

2. Copy your configuration script to an appropriate folders shared on the network, for example:

   ```
   \\[yourdomain]\SYSVOL\[yourdomain]\SCRIPTS
   ```

3. Open Group Policy Management, from the *Server Manager Console*, click **Tools > Group Policy Management**

4. Create a new policy.

   i. In the left pane, navigate to:

   ```
   Forest: yourdomain > Domains > yourdomain > Group Policy Objects
   ```

   For example:

   Forest: *doctest.loc* **> Domains >** *doctest.loc* **> Group Policy Objects**

   ii. Right click *Group Policy Objects* and select **New** to display the *NEW GPO* dialog.
   iii. Name your policy, for example *zenoss-sa*
   iv. Click **OK** to save and exit the *New Policy* window.

5. Edit your new policy. In the left pane, navigate to your new Group Policy Object.
   For example:

   Forest: *doctest.loc* **> Domains >** *doctest.loc* **> Group Policy Objects >** *zenoss-sa*

   i. Right click the policy and select **Edit** to display the *Group Policy Management Editor*.
   ii. In the left pane of the *Group Policy Management* window, navigate to:

   ```
   Computer Configuration\Policies\Windows Settings\Scripts
   (Startup/Shutdown)
   ```

   iii. Click **Scripts (Startup/Shutdown)**.
   iv. In the right pane (*Scripts (Startup/Shutdown*), double-click **Startup** to launch the *Startup Properties* dialog.
   v. In the *Startup Properties* dialog box, select the **PowerShell Scripts** tab.
   vi. Click **Add** to display the *Add a Script* dialog box:

   a. Specify the script name and path. In the *Script Name* field, enter the path to the script, or click **Browse** to locate the script file you copied in step 2 above.

   b. Select the script and click **Open**.

   c. In the *Script Parameters* box, enter the domain logon information for your service account user in the form of:
   -u yourusername@yourdomain for a domain user
   or *-u yourusername* for a local user.

   d. Click **OK** to save the information and exit the *Add a Script* window.

   e. If you have multiple scripts and want them to run in a particular order, use the **Up** and **Down** buttons in the *Startup Properties* window to set their run order.

   f. Click **OK** to exit the *Startup Properties* window.

6. Exit the Local Group Policy Editor:

   File > Exit

7. Link your new GPO to one or more Organizational Units (OU) containing servers to which you want the policies applied. Alternatively, you can apply the policies to all Windows servers in the domain by linking the new GPO to the domain itself. To link the GPO to the domain, complete the following process.

   Note: Substitute a specific OU for the domain if you want to link only to a subset of servers.

   i. Right-click your domain in the left pane of the *Group Policy Management* window.
   ii. Choose **Link an Existing GPO...**
   iii. Select your new GPO from the list that displays.
   iv. Click **OK** to complete the process.

8. Exit the Group Policy Management window:

   Select **File > Exit**

9. Manually refresh Group Policy from the command prompt of target servers:

```
gpupdate /force
```

10. Reboot your member servers to pick up the script changes.

Windows 2003 SP2 Standard Edition

The following sections describe how to configure Windows 2003 SP2 Standard Edition.

Prerequisites

The following prerequisites are specific to Windows Server 2003 SP2 Standard Edition:

- Patched (up to date) Windows 2003 Server SP2
- .NET Framework 2.0 SP1
  `(NetFx20SP1_x86.exe)`
- Windows Management Framework Core package
  `(WindowsServer2003-KB968930-x86-ENG.exe)`
- Group Policy Management Console with Service Pack 1
  `(gpmc.msi)`
- Windows Server 2003 Enterprise Edition (only required to use SSL with WinRM & WinRS)

Configuring Windows Server 2003 Using Group Policy (Basic Authentication, no Encryption)

Windows Remote Management (winrm) is one component of the Windows Hardware Management features. These enable management of server hardware both locally and remotely.

Note: Windows firewall must allow incoming ICMP (ping).

Note: All windows computers must have WinRM installed and enabled on them for WinRS to work and retrieve information from the remote system.

Perform the following procedure to configure Windows server for basic authentication without encryption:

1. Log on to a domain controller as a user with 'Domain Admin' privileges.
2. Create a new policy.
   Note: If you need to install the *Group Policy Management Console (GPMC)*, use the instructions provided at: http://technet.microsoft.com/en-us/library/cc757728%28v=ws.10%29.aspx

   Note: It is recommended that you create a new Group Policy Object instead of editing your *Default Domain Policy*.

   i. Open the **Group Policy Management** dialog:

      Start > Administrative Tools > Group Policy Management

   ii. In the **Group Policy Management** window, Navigate to
      Domains >*YourDomain* **> Group Policy Objects**.

   iii. Select (highlight) **Group Policy Objects**.

   iv. Right click and select **New**.

   v. Enter a useful name for the policy, for example, *WinRM_Monitored*.

   vi. Click **OK**.

3. Edit the new *Group Policy Object* (or *Default Domain Policy* , if you did not create a new one):

   i. In the **Group Policy Management** window, highlight the policy (for example *WinRM_Monitored*.

   ii. Right click and select **Edit** to display the *Group Policy Object Editor* window for your new policy.

   iii. In the **Group Policy Object Editor** window, expand the **Computer Configuration** section of the tree and navigate the tree to:
      Administrative Templates\Windows Components\Windows Remote Management(WinRM)

   Note: If the *\Windows Remote Management(WinRM)* folder does not display, you must add the policy:

   a. Right click **Administrative Templates** in the left pane.
   b. Select **Add/Remove Templates** to display the *Add/Remove Templates* dialog.
   c. Click **Add**.
   d. Select ***windowsremotemanagement.adm***.
   e. Click **Open** to select that template.
   f. Repeat this process for *windowsremoteshell.adm*.
   g. Click **Close** to exit the *Add/Remove Templates* dialog.

4. Enable remote server management:
    1. Navigate to **Administrative Templates\Windows Components\Windows Remote Management (WinRM)** in the left pane to access the *WinRM Service Group Policy* settings in the right pane.
    2. Click on **WinRM Service** in the right pane.
    3. In the right pane, double-click the **Allow automatic configuration of listeners** property.
    4. Click the **Enabled** radio button.
    5. Place an asterisk as a wildcard (' * ') in the *IPv4 filer* and *IPv6 fields* or specify a range of IP addresses for WinRM to listen on.
    6. Click **OK** at the bottom to submit the form.
5. Enable authentication:
    1. Double-click the **Allow Basic authentication** property in the right pane.
    2. Select the **Enabled** radio button.
    3. Click **OK** at the bottom to submit the form.
6. Specify unencrypted traffic:
    1. Double-click the **Allow unencrypted traffic** property.
    2. Select the **Enabled** radio button.
    3. Click **OK** at the bottom to submit the form.
7. Click on **Windows Remote Shell** in the left pane to display the *Windows Remote Shell* settings in the right pane. This is located in the group policy tree at (which might be located right below *WinRM* service in the tree):

    ```
    Computer Configuration\Administrative Templates\Windows
    Components\Windows Remote Shell
    ```

8. Configure remote shell access:
    1. In the right pane, double-click **Allow Remote Shell Access**.
    2. Select the **Enabled** radio button.
    3. Click **OK** at the bottom to submit the form.
9. Configure shell processes:
    1. In the right pane, double-click **Specify maximum number of processes per Shell**.
    2. Select the **Enabled** radio button.
    3. Enter the value 9999 (this is the maximum allowable value) in the *MaxProcessPerShell* field.
    4. Click **OK** at the bottom to submit the form.
10. Configure shell timeout value:
    1. In the Right pane, double-click **Specify Shell Timeout**.
    2. Select the **Enabled** radio button.
    3. Enter the value 9999 (this is the maximum allowable value) in the **ShellTimeOut field**.
    4. Click **OK** at the bottom to submit the form.
11. Configure the number of remote shells:
    1. In the right pane, double-click **Specify maximum number of remote shells per user**.

ii. Select the **Enabled** radio button.

iii. Enter the value 9999 (this is the maximum allowable value) in the *MaxShellsPerUser* field.

iv. Click **OK** at the bottom to submit the form.

Windows 2003: Configuring Firewall Group Policies

This section assumes you already administer the firewalls through Group Policy. These instructions are for adding additional WinRM port exceptions.

The port WinRM listens on depends on whether encryption is used or not:

- No encryption = Port 5985
- Encryption = Port 5986

The appropriate ports must be opened on the firewalls of monitored servers. You can use Group Policy to open these ports on all servers across the organization.

Note: Windows Server 2003 uses the Windows firewall settings to control local port usage and Group Policy to administer firewalls across the servers. It is important to note that the setting for *Allow Remote Administration* in Windows Server 2013 opens ports 135 & 145, not the required 5985 and 5986.

1. In the **Group Policy Object Editor** for your new policy, navigate to:
   `Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile`
2. In the right *Setting* pane:

   i. Double click **Windows Firewall: Define port exceptions**.

   a. Select **Enabled**.
   b. Click **Show**.
   c. Add two new rules for the 5985 and 5986 ports. For example, to open port 5985, enter the following:

   ```
   5985:TCP:localsubnet:enabled:somename
   ```

   d. Click **OK** to close the rules window.
   e. Click **OK** to close the *Define port exceptions Properties* window.

   ii. Double click **Windows Firewall: Allow ICMP exceptions**.

   a. Click **Enabled**.
   b. Check **Allow inbound echo request**
   c. Click **OK** to close the *Windows Firewall: Allow ICMP exceptions Properties* window

3. Link your new GPO to one or more Organizational Units (OU) containing servers to which you want to have the policies applied. Alternatively, you can apply the policies to all Windows servers in the domain by linking the new GPO to the domain itself. To link the GPO to the entire domain, complete the following process.

   Note: Substitute a specific OU for the domain if you want to link only to a subset of servers.

   i. Right-click your domain in the left pane of the *Group Policy Management* window.

   ii. Choose **Link an Existing GPO...**

   iii. Select your new GPO from the list that displays, *WinRM_Monitoring*, for example.

   iv. Click **OK** to complete the process.

4. Exit the *Group Policy Management Editor*:

   Select **File > Exit**

5. Before adding servers to Zenoss for monitoring, wait a sufficient amount of time for Group Policy to automatically refresh on the server(s). Alternatively, you can manually refresh Group Policy from the command prompt of target servers using the command:

```
gpupdate /force
```

Windows 2003: Configuring Zenoss at the Device Class Level

When one or more servers are ready for addition to Zenoss, perform the following steps in the Zenoss web interface:

1. Navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class.
3. Click the **Details** icon.
4. Click **Configuration Properties** in the left pane.
5. In the right pane, set the configuration properties for *zWinRMUser* and *zWinRMPassword*, supplying the appropriate Windows credentials.

Note: As this Knowledge Base article goes to press, only the *domain administrator* or *local administrator* accounts for each system can serve as the *zWinRMUser* variable. Zenoss engineers are currently working to document a method to substitute a different, less privileged account for this purpose in the future.

6. Click **See All**.
7. Add windows servers using the web interface or `ZenBatchload`.

Windows 2003: Improving Security - Specify Kerberos to Encrypt Credentials at the Device Class Level

The Zenoss master and / or any collectors tasked with monitoring Windows servers that use Kerberos must have Kerberos also installed on the host operating system.

1. Log in to the host as *root*, or as a user with *superuser* privileges.
2. Determine whether the Kerberos authentication package is installed:

   ```
   # rpm -qa | grep -i krb5-workstation
   ```

3. If the command returns a result, Kerberos authentication is installed and no additional action is necessary.

   If the command does not return a result, install Kerberos:

   ```
   # yum -y install krb5-workstation
   ```

The Kerberos authentication process requires an available ticket granting server. In the Microsoft Active Directory (AD) environment the AD Server also acts as the Key Distribution Center (KDC). The *zWinKDC* configuration property in Zenoss must be set to the IP address of the AD Server. Each collector used to monitor Windows servers must be able to send Kerberos packets to this server. To specify the ticket granting server in Zenoss, perform the following steps:

1. In the Zenoss web UI, navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class in the left pane.
3. Click the **Details** icon.
4. Click **Configuration Properties** in the left pane.
5. Edit the configuration property in the right pane for *zWinKDC*. Double click **zWinKDC** and specify the IP address of your Active Directory Server.
6. Edit the value for *zWinRMUser* name to be the *complete domain name* of the user, for example, *administrator@test.loc*.

Note: A *zWinRMUser* name value in the form of *user@domain* is the trigger for Zenoss to use Kerberos encryption for credentials. When the value of *zWinRMUser* name takes the form of *user*[only] instead of *user@domain,* Zenoss will not use Kerberos.

Note: The Zenoss server and collectors must be able to resolve the target server's pointer records (PTR) to their Active Directory fully qualified domain name. Administrators can meet this requirement by either configuring the Zenoss server to access the Windows DNS server for its DNS resolutions, or by manually entering PTR records for each server in the `/etc/hosts` file.
For example, the server *r2d2.example.com* at the IP address **77.77.77.77** has the following PTR record:
77.77.77.77 r2d2.example.com

Windows 2003: Configuring WinRM and WinRS on Individual Servers (Basic Authentication, no Encryption)

Perform the following steps to configure WinRM and WinRS:

1. Log on to the target server as a user with *Domain Admin* or local *Admin* privileges.
2. Press the **Start** button.
3. Launch **Windows PowerShell**:
   - Navigate to **Start > All Programs > Accessories > Windows PowerShell > Windows PowerShell**

   or

   - Type `powershell` at the command line.
4. Within Windows PowerShell:

   i. Configure the system to accept WS-Management requests from other systems. Enter the following at the command prompt:

   ```
   winrm quickconfig
   ```

   ii. Specify *http* instead of *https* (SSL) connections. Enter the following command:

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

   iii. Configure the *maximum number of concurrent operations per user*. Use the following command:

   ```
   winrm s winrm/config/service
   '@{MaxConcurrentOperationsPerUser="4294967295"}'
   ```

   iv. Configure *the maximum number of shells per user*. Enter the following command:

   ```
   winrm s winrm/config/winrs '@{MaxShellsPerUser="2147483647"}'
   ```

   Note: If this setting is controlled by policy, the command returns an error. You must use the policy editor to change the default setting to the new value of *Not Configured* and retry the command.

   v. Configure the *idle timeout*. Enter the following command:

   ```
   winrm s winrm/config/winrs '@{IdleTimeout="7200000"}'
   ```

   vi. Specify Basic Authentication. Enter the following command:

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

   vii. Exit PowerShell:

   ```
   exit
   ```

5. Configure the firewall to allow connections on ports 5985 and 5986:

   Note: Follow this process to configure the required firewall port exceptions only if you are using the windows firewall. If you are not using the firewall, it is NOT necessary to configure it. WinRM does not require the windows firewall to function.

   i. Navigate **Start > Control Panel > Windows Firewall** to display the *Windows Firewall* window.
   ii. Click the **Exceptions** tab:
      a. Click **Add Port.**
      b. Input a name for the exception, *WinRM*, for example.
      c. Add the Port number *5985.*
      d. Verify the **TCP** radio button is selected.

e. Click **OK** to close the *Add a port* dialog.

iii. Click the **Advanced** tab:

a. In the *ICMP* section select **Settings**
b. Verify **Allow incoming echo request** is selected.
c. Click **OK** to close the *ICMP* dialog.
d. Click **OK** to exit the *Windows Firewall* dialog.

6. Configure Zenoss to monitor the server. Perform the following steps within the Zenoss web interface:

i. Navigate to the **Infrastructure** page.

ii. Select the **Server/Microsoft/Windows** device class.

iii. Click the **Details** icon.

iv. Click **Configuration Properties** in the left pane.

v. In the right pane, confirm that the configuration properties for *zWinRMUser* and *zWinRMPassword* are correct for the target server - this means the appropriate Windows credentials.

vi. If the credentials listed are correct, click **See All** and add the server to Zenoss.

vii. If the credentials listed are not appropriate to the target server, the server must be added and the server's individual *zWinRMUser* and *zWinRMPassword* configuration properties must be set. Perform the following steps to add the server information:

a. Add the server to the **Server/Microsoft/Windows** device class, but opt out of modeling the device when adding as follows:

- If you are adding via the web interface, leave the **Model Device:** box unchecked.
- If you are adding via the `zenbatchload` command, be sure the device has the --*nomodel* flag set.

b. When the device displays in the device list, click on its name.

c. Click on **Configuration Properties**, and set the configuration properties for *zWinRMUser* and *zWinRMPassword*, supplying the appropriate Windows credentials..

d. Model the device by clicking the Action Wheel (gear-shaped) icon in the lower left and select **Model Device...**

Windows 2003: Improving Security for Individual Devices - Specify Kerberos to Encrypt Credentials

The Zenoss master and / or any collectors tasked with monitoring Windows servers with Kerberos must have Kerberos installed on the host operating system.

1. Log in to the host as *root*, or as a user with *superuser* privileges.
2. Determine whether the Kerberos authentication package is installed:

```
# rpm -qa | grep -i krb5-workstation
```

If the command returns a result, Kerberos authentication is installed and no additional action is necessary.

3. If the command does not return a result, install Kerberos:

```
# yum -y install krb5-workstation
```

The Kerberos authentication process requires an available ticket granting server. In the Microsoft Active Directory (AD) environment, the AD Server also acts as the Key Distribution Center (KDC). The *zWinKDC* configuration property in Zenoss must be set to the IP address of the AD Server. Each collector that monitors Windows servers must be able to send Kerberos packets to this server. To specify the ticket granting server in Zenoss, perform the following steps:

1. In the Zenoss web UI, navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class.
3. Click **Details**.
4. Edit the configuration property for *zWinKDC* to specify the IP address of your Active Directory Server.
5. Edit the value for *zWinRMUserName* to be the complete domain name of the user, for example, *administrator@test.loc*.

Note: A *zWinRMUserName* value in the form of *user@domain* is the trigger for Zenoss to use Kerberos encryption for credentials. When the value of *zWinRMUsername* takes the form of *user*[only] instead of *user@domain,* Zenoss will not use Kerberos.

Note: The Zenoss server and collectors must be able to resolve the target server's pointer records (PTR) to their Active Directory fully qualified domain name. Administrators can meet this requirement by either configuring the Zenoss server to access the Windows DNS server for its DNS resolutions, or by manually entering PTR records for each server in the `/etc/hosts` file.
For example, the server *r2d2.example.com* at the IP address **77.77.77.77** has the following PTR record:
77.77.77.77 r2d2.example.com

Windows 2003: Improving Individual Server Security - Specify SSL for WinRM & WinRS

To successfully encrypt the payload between Resource Manager and Windows clients, you must install a *Server Authentication* certificate on each monitored server. This process includes duplicating the *Web Server* certificate template, editing it for your specific use and then issuing it. This process requires Windows Server 2003 Enterprise Edition. To create certificates on Windows 2003 Enterprise Edition, consult the relevant sections from the Windows 2008 section of this document and amend as necessary for Windows 2003.

Note: Due to a limited set of pre-defined certificates available in Windows 2003 Standard Edition, this process cannot be accomplished using Windows 2003 Standard Edition.