cockpit
IT Service Manager

Monitoring - Windows system access

FAQ document

Table of contents

Introduction

The aim of this document is to help technicians to configure access on Windows systems in order to monitor them remotely using the Cockpit IT Service Manager engine. This access also allows configuration audits to be carried out on the servers automatically.

We recommend that you use the WinRM protocol to monitor and/or audit systems running Windows 2003 or above. A range of authentication modes are available, depending on the particular operating system installed on the server in question, and whether or not that server is attached to a domain. Three authentication modes are described in this document. The table below indicates the various authentication modes that are compatible with various architectures: you must however select an authentication mode that is compatible with your particular architecture.

Cockpit IT Service Manager Engine		**Target Windows Server**	**Compatibility with authentication mode**		
			SPNEGO	**Basic Unencrypted**	**Basic encrypted**
Linux		-	No	Yes	Yes
Windows	Within the domain	Within the domain	Yes	Yes	Yes
		Outside the domain	No	Yes	Yes
	Outside the domain	Within the domain	No	Yes	Yes
		Outside the domain	Yes	Yes	Yes

Notes:

- “SPNEGO” authentication is the simplest to implement, but it does not work in certain environments (most notably when the Cockpit IT Service Manager engine is installed on a Linux server).
- “Basic Unencrypted” authentication works in all environments, but it is not recommended because data is transferred over an unencrypted network.
- “Basic Encrypted” authentication is the preferred choice, because it works in all environments, and provides a level of encryption and security.

Quick deployment

To carry out a quick deployment of WinRM access on a Windows system that you wish to monitor, you can follow the steps below:

1. Log in to the server to be monitored
2. Open a command prompt (the standard cmd.exe)
3. Run the three commands below (answering 'y' to the first prompt, if a response is required)

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

WinRM access is via the open port 5985. This access is unencrypted, and if you prefer to deploy an encrypted solution, follow the procedure as set out below.

Warning: Ensure that the port used by WinRM is indeed available. (For some Windows versions, the default ports are 80 or 443). We recommend that you use port 5985 in non-SSL mode, and 5986 in SSL mode. You can check which port is in use by running the following command.

winrm e winrm/config/listener

```
Listener
        Address = *
        Transport = HTTP
        Port = 5985
```

Specific configuration

I. Service configuration

Whichever authentication mode is selected, the “Windows Remote Management (WS-Management)” service must be configured.

Log in to the target server using the administrator account: it is vital that this account is used to configure the service.

Open a command prompt, running it as an administrator.

Configure WinRM by running the following command.

winrm get winrm/config/service

If the command returns a list of configuration settings (as shown in the example below), this confirms that the WinRM service is already running. In this case, simply move on to the next step.

```
Service
        RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
        MaxConcurrentOperations = 4294967295
        MaxConcurrentOperationsPerUser = 15
…
```

If the command returns an error message, configure and then start the WinRM service by running the following command. This command starts the “Windows Remote Management (WS-Management)” service and configures it to run automatically. It also configures an open HTTP port (port 5985) and updates the firewall rules to grant access.

winrm quickconfig

II. “SPNEGO” authentication

No configuration is required; this method of WinRM authentication works with the default configuration.

Run the following command to check the configuration status.

winrm get winrm/config/service/auth

Check the “Kerberos” setting: it should be set to “true.”

```
Auth
        Basic = false
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
```

If this value is not set to “true”, run the following command.

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

III. “Basic/Unencrypted” authentication

Run the following command in order to enable “Basic” authentication.

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

Run the following command in order to enable unencrypted authentication.

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

IV. “Basic/Encrypted” authentication

A. Installing the certificate

1. Using a certificate server

If you have access to a certificate server, use the guide published by Microsoft at http://support.microsoft.com/kb/2019527 to install the certificate on the server to be monitored.

2. Manually creating a certificate

If you do not have access to a certificate server, a manually-generated certificate is required. Once generated, this certificate must be installed on the server to be monitored.

Installing selfssl.exe

The “selfssl.exe” utility is required to create the certificate.

This utility forms part of Microsoft’s IIS 6.0 resource kit, which is described at http://support.microsoft.com/kb/840671/

If the resource kit is installed on the server to monitored, the utility will be located in one of the following folders:

- C:\Program Files (x86)\IIS Resources\SelfSSL\selfssl.exe
- C:\Program Files\IIS Resources\SelfSSL\selfssl.exe

Creating the certificate

Run “selfssl.exe” from a command prompt.

cd {répertoire de selfssl}
selfssl.exe /V:365 /T

Confirm:

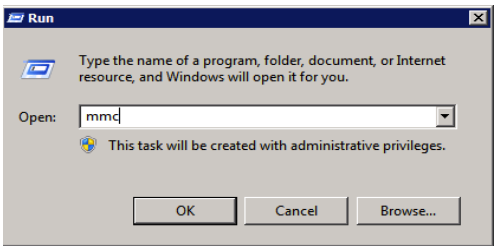
Y

> Note: Don't pay any attention to the error message (it is generated if the full resource kit is not installed).

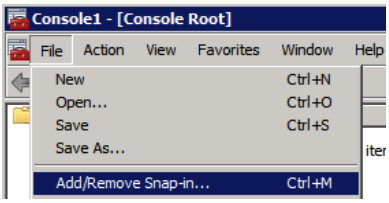
Retrieving thumbprint data

Open the "Start" menu and select "Run."

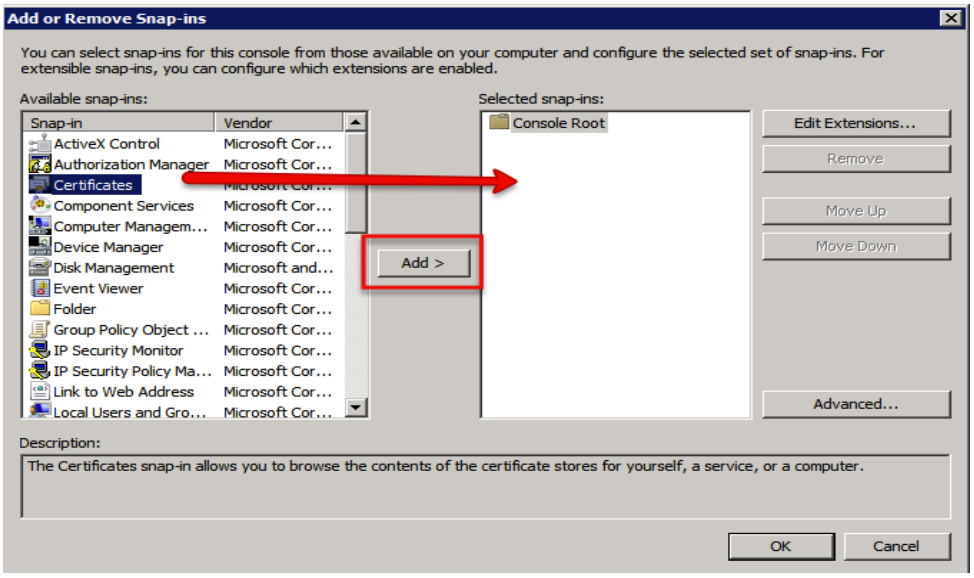
Star the MMC console.



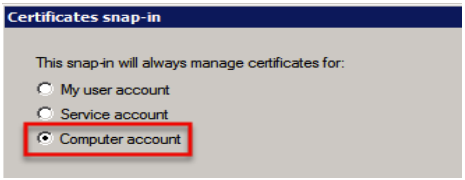
Open the "Add/Remove Snap-in" menu.



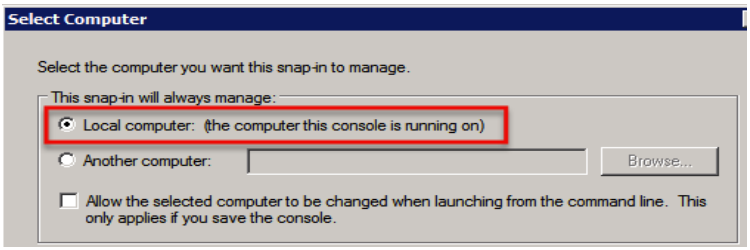
Select the "Certificates" "Snap-in".



Select “Computer account”.



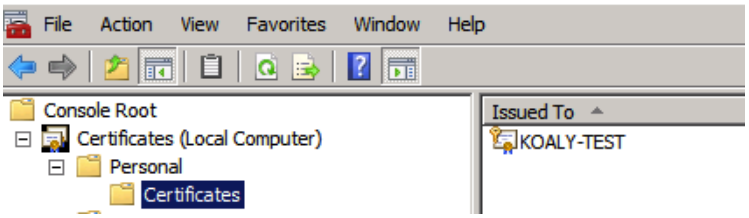
Select “Local computer”.



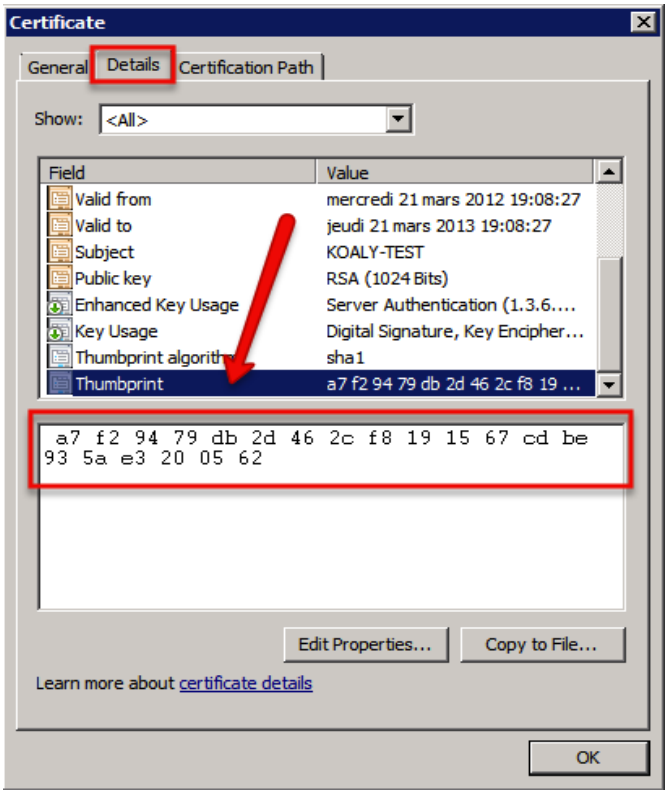
The newly created certificate will be located in the hierarchy at “Certificates/Personal/Certificates”.

The name of this certificate will match that of the server.

Open the certificate by double clicking.



Within the “Details” tab, select the “Thumbprint” and copy the value displayed in the field shown below the list.



Creating the WinRM HTTPS listener

From a command prompt, run the following command by replacing the items between “<>“.

winrm create winrm/config/listener?Address=+Transport=HTTPS @{Hostname="<nom du serveur>";CertificateThumbprint="<valeur de thumbprint sans les espaces>"}*

Example command:

winrm create winrm/config/listener?Address=+Transport=HTTPS @{Hostname="HOST-TEST";CertificateThumbprint="a7f29479db2d462cf8191567cdbe935ae3200562"}*

Note: You must ensure that the thumbprint value does not contain any spaces.

Run the following command to manage the listener.

winrm e winrm/config/listener

Specify the underlined items, and ensure that the thumbprint matches up with the certificate that has been created.

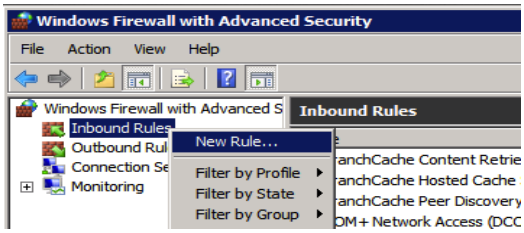
```
Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = HOST-TEST
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = a7f29479db2d462cf8191567cdbe935ae3200562
```

ListeningOn = 127.0.0.1, 172.16.42.226, ::1, 2001:0:5ef5:73b8:142c:140:53ef:d51d,fe80::5efe:172.16.42.226%13, fe80::142c:140:53ef:d51d%11#

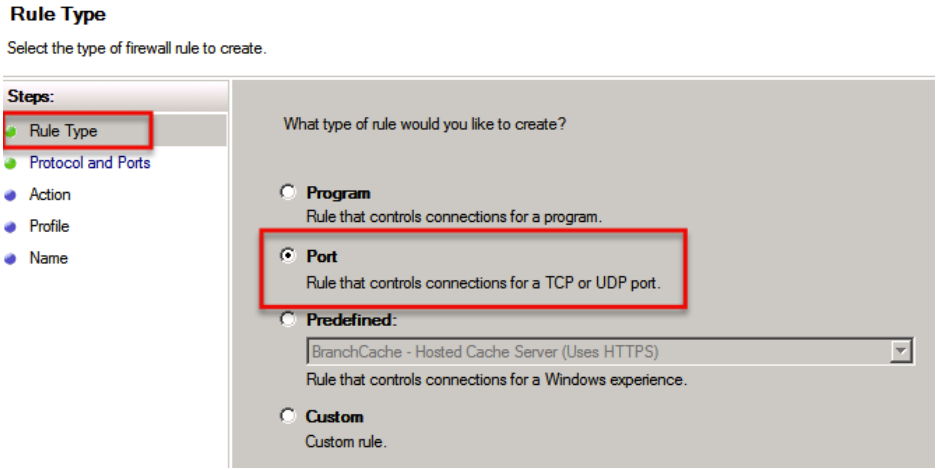
Configuring the firewall

Open the Windows firewall manager (Control Panel → System and Security → Windows Firewall → Advanced Settings).

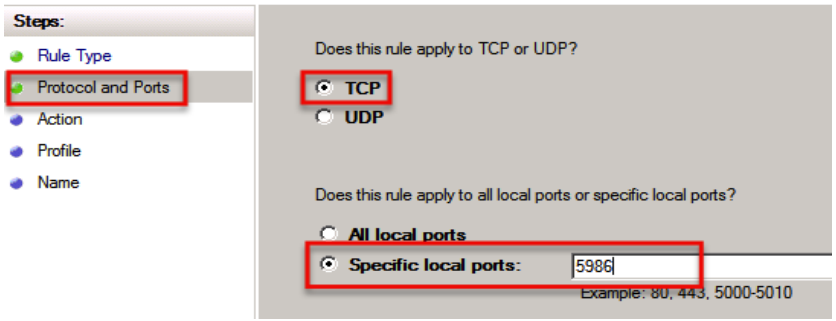
Create a new inbound authorization rule.



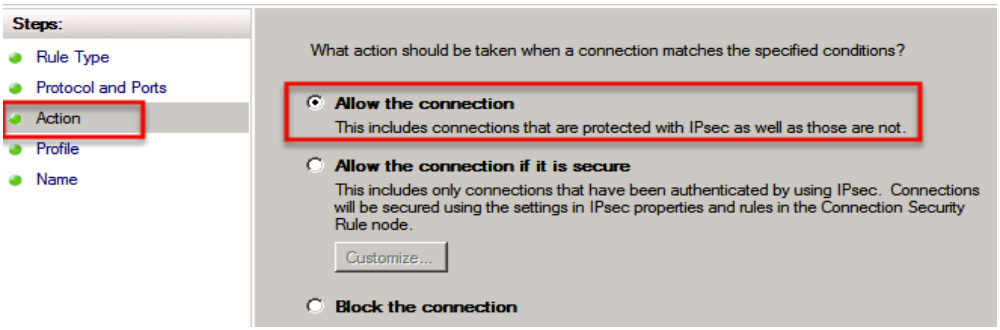
Select the “Port” type.



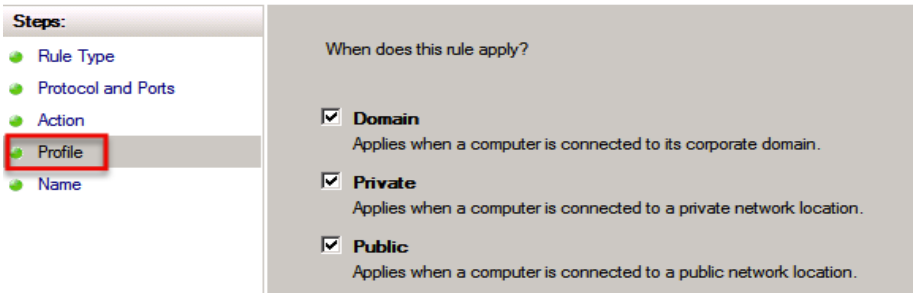
Select the “TCP” protocol and specify port “5986”



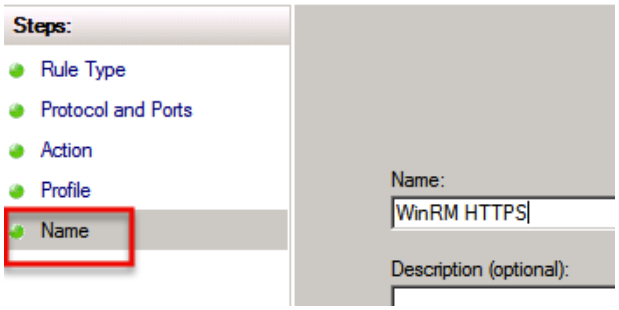
Enable connections.



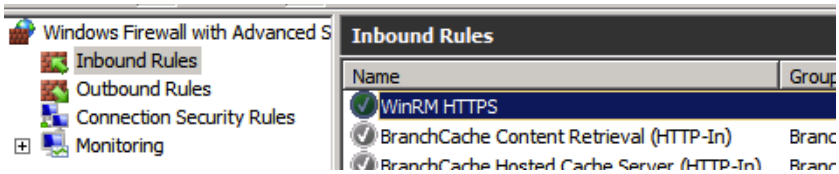
Enable all networks.



Give a name to the rule.

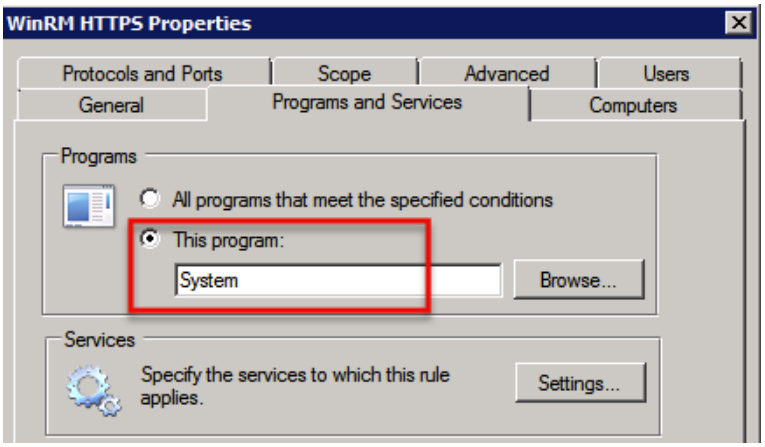


Edit the rule.



Open the “Programs and Services” tab.

Select the “System” program and then save the settings.



B. Enabling “Basic” authentication

Run the following command to enable “Basic” authentication.

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

Run the following command to check the configuration.

winrm get winrm/config/service

Specify the settings that are underlined.

```
Service
        RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
        ...
        MaxPacketRetrievalTimeSeconds = 120
        AllowUnencrypted = false
        Auth
                Basic = true
                Kerberos = true
                Negotiate = true
                Certificate = false
                CredSSP = false
                CbtHardeningLevel = Relaxed
        DefaultPorts
                HTTP = 5985
                HTTPS = 5986
```

C. Force the use of a specific authentication mode

The “Negotiate = true” authentification setting allows Windows to automatically select the correct connection mode.

However if you encounter connection problems, you can test a connection mode by forcing its use.

For example, switch the “Basic” mode to “false” to force the use of the “Kerberos” mode with the following command.

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

Run the following command to check the configuration.

winrm get winrm/config/service

Specify the settings that are underlined, in this example the “Kerberos” authentication mode is used.

```
Service
        RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
        ...
        MaxPacketRetrievalTimeSeconds = 120
        AllowUnencrypted = false
        Auth
                Basic = false
                Kerberos = true
                Negotiate = true
                Certificate = false
                CredSSP = false
                CbtHardeningLevel = Relaxed
        DefaultPorts
                HTTP = 5985
                HTTPS = 5986
```

D. Deleting the HTTP listener

To delete the HTTP listener (for instance, because you are using the HTTPS listener), use the following command.

winrm delete winrm/config/listener?Address=+Transport=HTTP*

You can obtain a list of listeners by running the following command.

winrm e winrm/config/listener

Issues under Windows XP/Server 2003

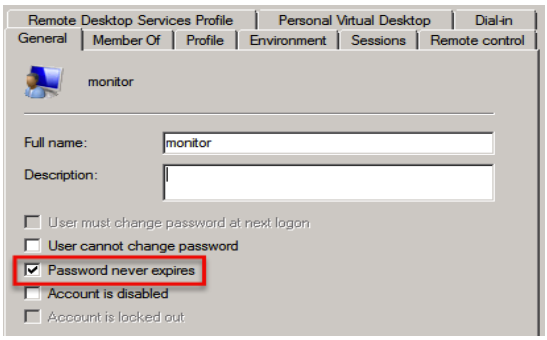
WinRM connections to machines running Windows XP/Server 2003 require the following components to be installed on the target hardware.

- Installer .NET framework 3.5
- Visual C++ 2012 redistributable
- WS-Management v1.1 package: http://support.microsoft.com/kb/936059
- Windows Management Framework Core http://support.microsoft.com/kb/968930

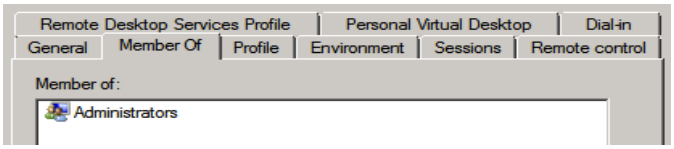
System user

I. Required settings

Create a system user for the specific server to be monitored, with an associated password that never expires.

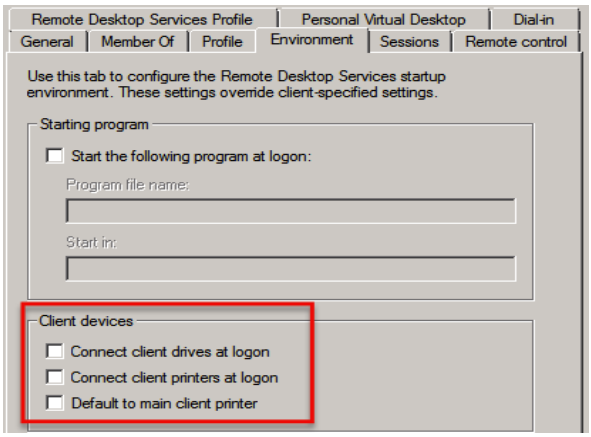


The user must be a member of the “Administrators” group.

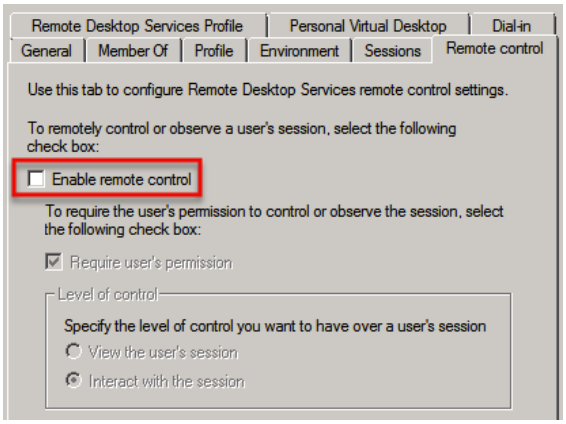


II. Optional settings

Do not connect any peripherals.



Disable remote control of the machine using “Remote Desktop Services”.



Ports

The port to be opened depends on the authentication method:

Authentication mode	Port
SPNEGO	5985
Basic Unencrypted	5985
Basic Encrypted	5986

Warning: Ensure that the port used by WinRM is indeed available. (For some Windows versions, the default ports are 80 or 443). We recommend that you use port 5985 in non-SSL mode, and 5986 in SSL mode. You can check which port is in use by running the following command.

winrm e winrm/config/listener

```
Listener
    Address = *
    Transport = HTTP
    Port = 5985
```

Or

```
Listener
    Address = *
    Transport = HTTPS
    Port = 5986
```

Tests

Connectivity tests in relation to the server to be monitored must be run from a machine with a Windows operating system (Vista, 7, Server 2008 or higher).

I. Unsecured connection: “SPNEGO” or “Basic Unencrypted”

Open a command prompt, running it as an administrator.
Run the following command; the target server must require the user’s password.
winrm g winrm/config/service -r:http://<serveur cible>:5985 -u:<utilisateur>

II. Secure connection: “Basic Encrypted”

Open a command prompt, running it as an administrator.
Run the following command; the target server must require the user’s password.
winrm g winrm/config/service -r:https://<serveur cible>:5986 -u:<utilisateur> -skipCAcheck

Portal configuration

Enter server login information by following the procedure as set out below on the Cockpit IT Service Manager portal.

1. Go to the “Infrastructure/Hardware/Management” menu
2. Open the target server in editing mode
3. Fill out the following fields in the “Monitoring” tab.

Field	Comments
DNS Name	
Cluster	Check this box if the server is a logical node within a cluster If this box is checked, the monitor will not use persistent connections
User	
Password	
Connection type	WinRM
Port	5985 (SPNEGO authentication) 5985 (Basic Unencrypted authentication) 5986 (Basic Encrypted authentication)
SSL	Check this box to select “Basic Encrypted” authentication
Connection time	10 seconds by default; increase this value if the connection to the server is slow

4. Save

Document end