cockpit
IT Service Manager

Monitoring - Windows system access

FAQ document

Table of contents

Introduction

The aim of this document is to configure access on Windows systems in order to monitor, inventory, collect metrics using the Cockpit IT Service Manager engine.

We recommend that you use the WinRM protocol to monitor and/or audit systems running Windows.
A range of authentication modes are available, 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.**

Secured connection (recommended)

The following procedure explains how to configure an access with a "Basic Encrypted" authentication mode.

I. Remote Management Service

On the Windows service management console, the "Windows Remote Management (WS-Management)" service must be active and must be started automatically (normally, it is by default).

II. Certificate creation

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.
Create a certificate by executing the following command (replace <COMPUTERNAME> with the full DNS name of the server, case sensitive).
new-SelfSignedCertificate -DnsName "<COMPUTERNAME>" -CertStoreLocation Cert:\LocalMachine\My

Copy the Thumbprint value generated by the command.

```
Directory: Microsoft.PowerShell.Security\Certificate::LocalMachine\My


Thumbprint                                Subject
----------                                -------
BB30999234AE9CE7D1C631F6052428136CD23333  CN=WIN-UHEPFOLN33D
```

III. WinRM configuration

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

In order to configure access with a "Basic Encrypted" authentication mode, execute the following commands (replace <COMPUTERNAME> with the full DNS name of the server and <THUMBPRINT> with the one that was generated).

winrm create winrm/config/listener?Address=+Transport=HTTPS ‘@{Hostname="<COMPUTERNAME>";CertificateThumbprint="<THUMBPRINT>"}’*

winrm set winrm/config/service/auth ‘@{Basic="true"}’
winrm set winrm/config/client ‘@{TrustedHosts=""}’*

IV. Check the configuration

Execute the command and check the values of the highlighted parameters.

winrm get winrm/config/service

```
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 1500
    EnumerationTimeoutms = 240000
    MaxConnections = 300
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = false
    Auth
        Basic = true
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    IPv4Filter = *
    IPv6Filter = *
    EnableCompatibilityHttpListener = false
    EnableCompatibilityHttpsListener = false
    CertificateThumbprint
    AllowRemoteAccess = true
```

Execute the command and check the values of the highlighted parameters.

winrm get winrm/config/client

```
Client
    NetworkDelayms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
        Basic = true
        Digest = true
        Kerberos = true
        Negotiate = true
        Certificate = true
        CredSSP = false
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    TrustedHosts = *
```

Execute the command and check the values of the highlighted parameters.

winrm e winrm/config/listener

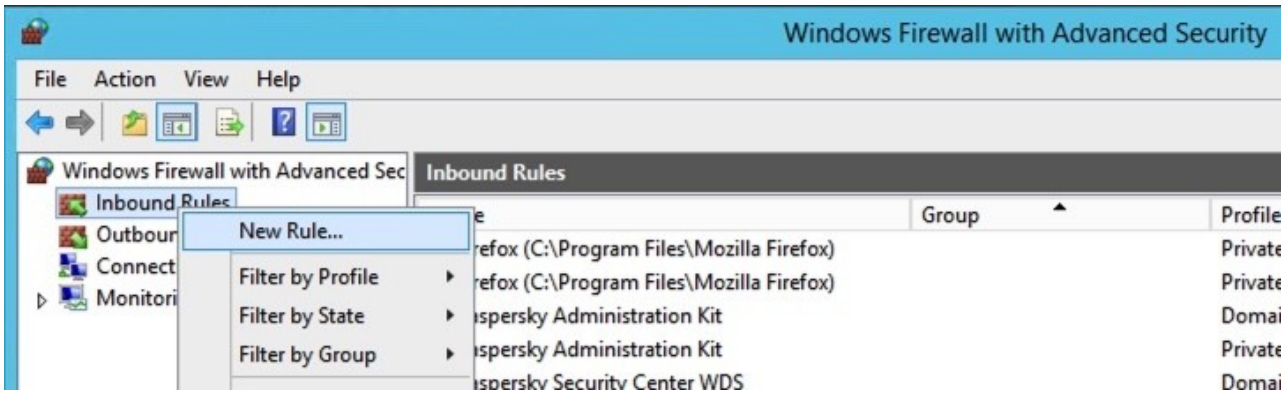
Check the thumbprint value.

```
Listener
        Address = *
        Transport = HTTPS
        Port = 5986
        Hostname = WIN-UHEPFOLN33D
        Enabled = true
        URLPrefix = wsman
        CertificateThumbprint = BB30999234AE9CE7D1C631F6052428136CD23333
        ListeningOn = 127.0.0.1, 172.16.42.226, ::1, 2001:0:5ef5:73b8:142c:140:53ef:d51d,fe80::5efe:172.1
        6.42.226%13, fe80::142c:140:53ef:d51d%11#
```

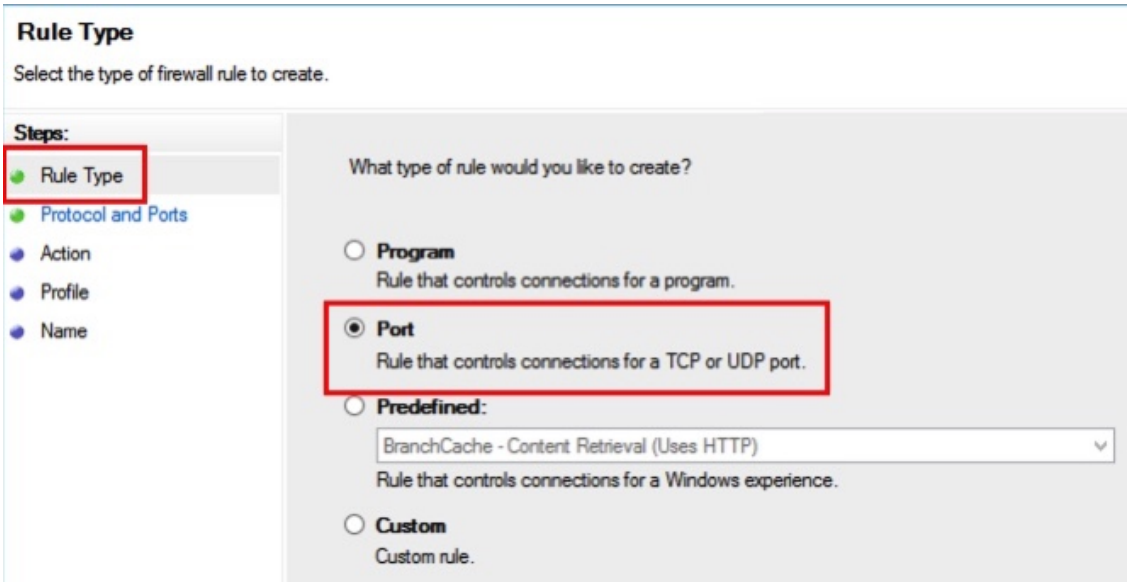
V. Configuring the firewall

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

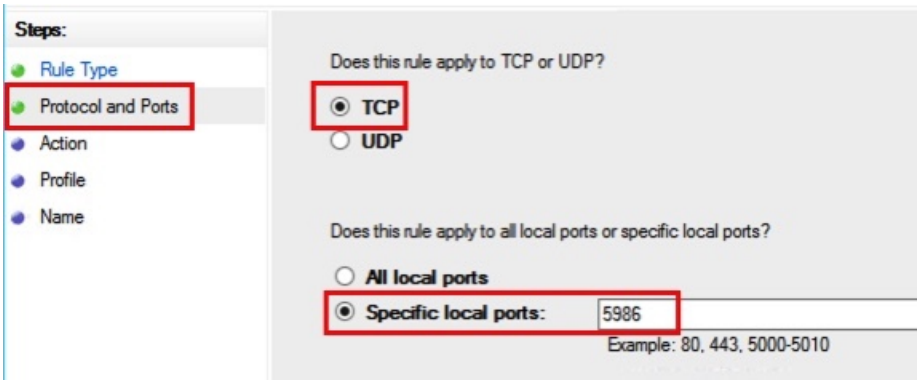
Create a new inbound authorization rule.



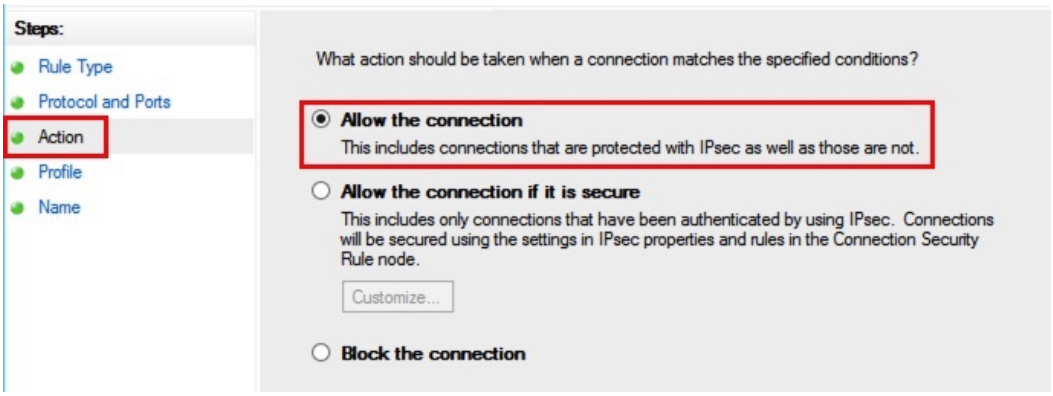
Select the “Port” type.



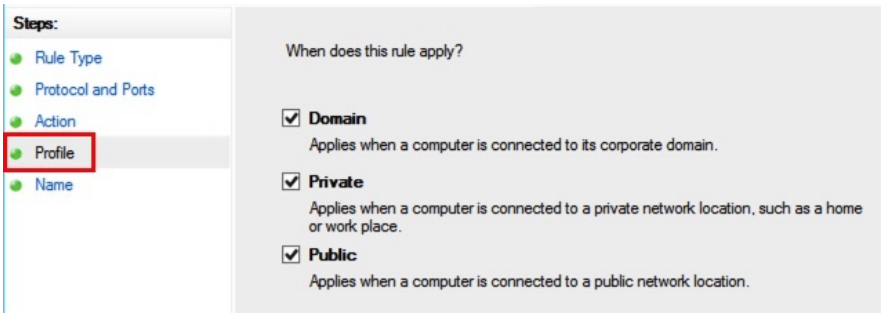
Select the “TCP” protocol and specify port “5986”



Enable connections.

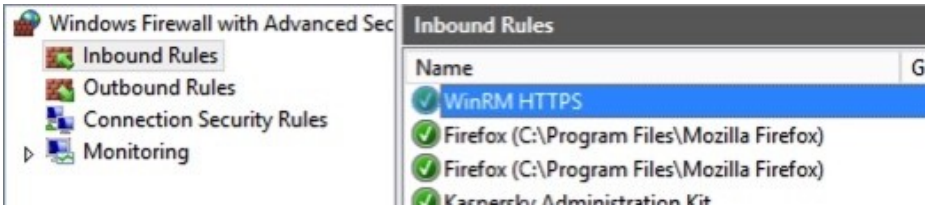


Enable all networks.



Give a name to the rule.

Edit the rule.



VI. Tests

From a remote Windows workstation (which accesses the server to be monitored), 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

VII. Additional configuration (optional)

A. 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
```

B. 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

Unsecured connection (not recommended)

The following procedure describes how to configure access with a "Basic Unencrypted" authentication mode.

I. Remote Management Service

On the Windows service management console, the "Windows Remote Management (WS-Management)" service must be active and must be started automatically (normally, it is by default).

II. WinRM configuration

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

In order to configure access with a "Basic Encrypted" authentication mode, execute the following commands.

winrm set winrm/config/service/auth ‘@{Basic="true"}’
winrm set winrm/config/service ‘@{AllowUnencrypted="true"}’
winrm set winrm/config/client ‘@{TrustedHosts=""}’*

III. Check the configuration

Execute the command and check the values of the highlighted parameters.

winrm get winrm/config/service

```
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
    EnumerationTimeoutms = 240000
    MaxConnections = 300
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = true
    Auth
        Basic = true
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    IPv4Filter = *
    IPv6Filter = *
    EnableCompatibilityHttpListener = false
    EnableCompatibilityHttpsListener = false
    CertificateThumbprint
    AllowRemoteAccess = true
```

Execute the command and check the values of the highlighted parameters.

winrm get winrm/config/client

```
Client
    NetworkDelayms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
        Basic = true
        Digest = true
        Kerberos = true
        Negotiate = true
        Certificate = true
        CredSSP = false
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    TrustedHosts = *
```

IV. Tests

From a remote Windows workstation (which accesses the server to be monitored), 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>

“SPNEGO” authentication

The following procedure describes how to configure access with a "SPNEGO" authentication mode.

I. Remote Management Service

On the Windows service management console, the "Windows Remote Management (WS-Management)" service must be active and must be started automatically (normally, it is by default).

II. WinRM configuration

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. Tests

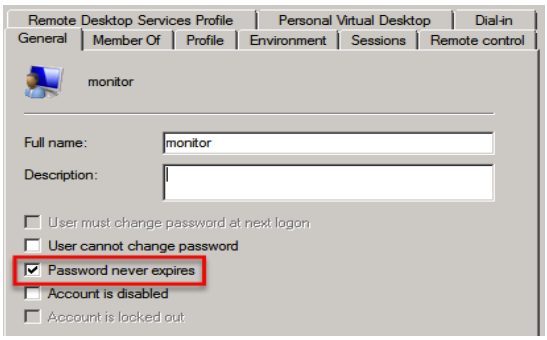
From a remote Windows workstation (which accesses the server to be monitored), open a command prompt, running it as an administrator.
Run the following command; the target server must require the user’s password.

winrm g winrm/config/service -r:http://<serveur cible>:5985 -u:<utilisateur>

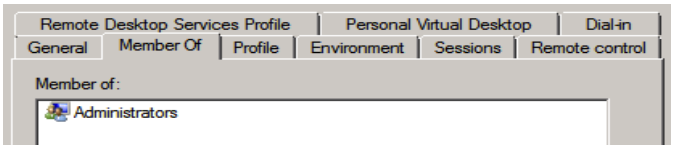
System user

I. Required settings

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

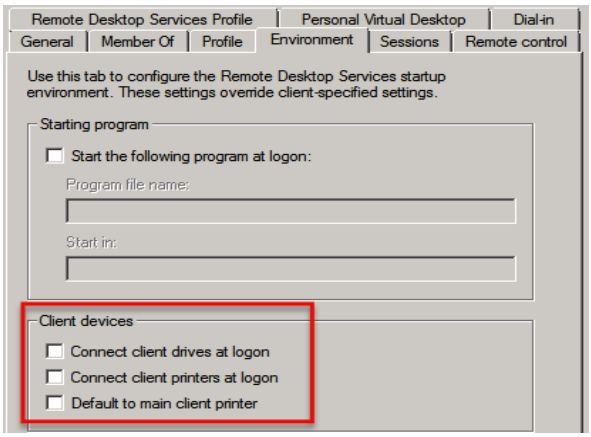


The user must be a member of the “Administrators” group.

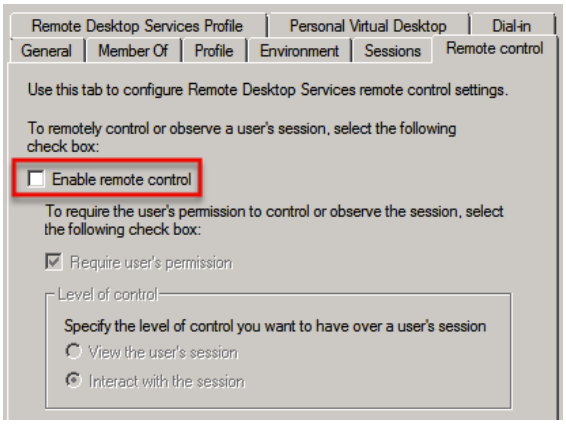


II. Optional settings

Do not connect any peripherals.



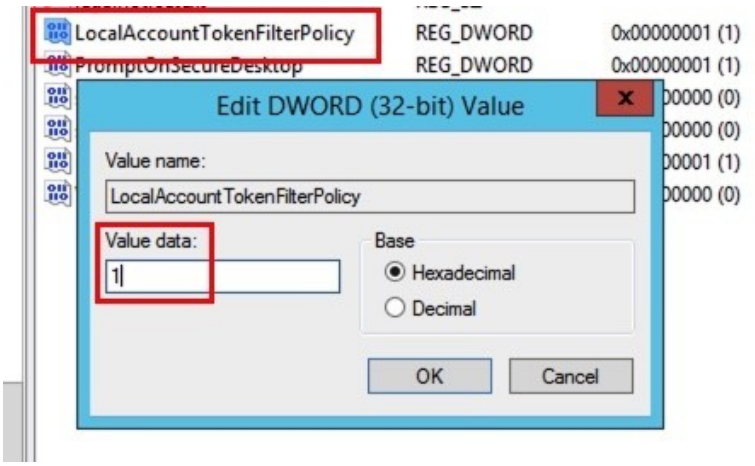
Disable remote control of the machine using “Remote Desktop Services”.



In the case the monitored equipment is not in the domain where the monitoring engine is located, it may be necessary to set the following entry in the registry:

Path: [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

Value name: LocalAccountTokenFilterPolicy = 1 (REG_DWORD)



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
```

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 “Parameters” tab.

Field	Comments
DNS Name	Name of the equipment as it is identified on the network and used for connections For secured connections, use the server name that has been specified to generate the certificate.
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	Domain user: fill in “Domain\user”. Local user: fill in “user”. In case the monitored equipment is not in the domain where the monitoring engine is located, it may necessary to indicate the name of the monitored equipment in the domain: “Hostname\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