Full credit is given to the above companies including the OS that this PDF file was generated!

PowerShell Get-Help on command 'Get-PcsvDevice'

PS C:\Users\wahid> Get-Help Get-PcsvDevice

NAME

Get-PcsvDevice

SYNOPSIS

Gets information about a remote hardware device.

SYNTAX

```
Get-PcsvDevice [-TargetAddress] <String> [-Credential] <PSCredential>
[-ManagementProtocol] {WSMan | IPMI} [[-Port] <UInt16>] [-AsJob]
[-Authentication {Default | Basic | Digest}] [-CimSession <CimSession[]>]
[-SkipCACheck] [-SkipCNCheck] [-SkipRevocationCheck] [-ThrottleLimit <Int32>]
[-TimeoutSec <UInt32>] [-UseSSL] [<CommonParameters>]
```

DESCRIPTION

The Get-PcsvDevice cmdlet gets information about a remote device. The cmdlet connects to a remote device, for example, a baseboard management controller, and collects hardware inventory information and information about the firmware installed on the device. The cmdlet communicates with the remote device by using the Intelligent Platform Management Interface (IPMI) or WS-Management

(WSMAN) protocols.

PARAMETERS

-AsJob [<SwitchParameter>]

Runs the cmdlet as a background job. Use this parameter to run commands that take a long time to complete.

-Authentication <Authentication>

Specifies an authentication method to use for devices managed by WS-Management. Do not specify this parameter for devices managed by using IPMI. The acceptable values for this parameter are:

- Basic

- Digest

- Default

If you specify Default for this parameter and a value of WSMAN for the ManagementProtocol parameter, the cmdlet uses Basic authentication.

-CimSession <CimSession[]>

Runs the cmdlet in a remote session or on a remote computer. Enter a computer name or a session object, such as the output of a New-CimSession (https://go.microsoft.com/fwlink/p/?LinkId=227967) or [Get-CimSession](https://go.microsoft.com/fwlink/p/?LinkId=227966)cmdlet. The default is the current session on the local computer.

-Credential <PSCredential>

Specifies a PSCredential object based on a user name and password. To obtain a PSCredential object, use the Get-Credential cmdlet. For more information, type `Get-Help Get-Credential`. This parameter specifies the credential for the remote hardware device.

-ManagementProtocol <ManagementProtocol>

Specifies a management protocol used to communicate with a device. The acceptable values for this parameter are:

- WSMAN

- IPMI

Specify WSMAN for devices that represent information by using Systems Management Architecture for Server Hardware (SMASH), Desktop and mobile Architecture for System Hardware (DASH) or Physical Computer System View (PCSV) profiles. Refer to your hardware documentation for supported management protocols.

-Port <UInt16>

Specifies a port on the remote computer to use for the management connection. If you do not specify a port, the cmdlet uses the following default ports:

- IPMI and WSMAN over HTTP. Port 623. - WSMAN over HTTPS. Port 664

-SkipCACheck [<SwitchParameter>]

Indicates that the client connects by using HTTPS without validating that a trusted CA signed the server certificate. Do not specify this parameter if you specify a value of IPMI for the ManagementProtocol parameter.

Do not specify this parameter unless you can establish trust in another way, such as if the remote computer is part of a network that is physically secure and isolated, or if the remote computer is a trusted host in a Windows Remote Management (WinRM) configuration.

-SkipCNCheck [<SwitchParameter>]

Indicates that the certificate common name of the server does not need to match the host name of the server. Do not specify this parameter if you specify a value of IPMI for the ManagementProtocol parameter.

Specify this parameter only for managing devices by using WSMAN over HTTPS. Be sure to specify this parameter only for trusted computers.

-SkipRevocationCheck [<SwitchParameter>]

Indicates that the cmdlet skips the revocation check of server certificates. Do not specify this parameter if you specify a value of IPMI for the ManagementProtocol parameter.

Be sure to specify this parameter only for trusted computers.

-TargetAddress <String>

Specifies the name or IP address of the management port on the remote hardware device. For server hardware, this is typically a dedicated BMC IP address. For other devices, like network switches, this is the IP address of their management port. For desktop and mobile devices, the BMC sometimes shares the same IP address as the computer.

-ThrottleLimit <Int32>

Specifies the maximum number of concurrent operations that can be established to run the cmdlet. If this parameter is omitted or a value of `0` is entered, then Windows PowerShellr calculates an optimum throttle limit for the cmdlet based on the number of CIM cmdlets that are running on the computer. The throttle limit applies only to the current cmdlet, not to the session or to the computer.

-TimeoutSec <UInt32>

Specifies how long to wait, in seconds, for a response from the remote hardware device. After this period, the cmdlet abandons the connection attempt.

-UseSSL [<SwitchParameter>]

Indicates that the server connects to the target computer by using SSL. WSMAN encrypts all content transmitted over the network. Specify this parameter to use the additional protection of HTTPS instead of HTTP. If you specify this parameter and SSL is not available on the connection port, the command fails.

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable, and OutVariable. For more information, see about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

----- Example 1: Get information from a remote IPMI device -----

```
PS C:\> $Credential = Get-Credential Admin
PS C:\> Get-PCSVDevice -TargetAddress "10.0.0.29" -ManagementProtocol IPMI
-Credential $Credential
TargetAddress      Manufacturer      Model           SerialNumber
EnabledState


-------------      ------------      -----           ------------
------------
10.177.231.27      DELL              PowerEdge R720     CN7016329700EH
Enabled
```

This example connects with an IPMI device and returns hardware and firmware information for the device.

The first command uses the Get-Credential cmdlet to create a credential, and then stores it in the $Credential variable. The cmdlet prompts you for a user name and password. For more information, type `Get-Help Get-Credential`.

The second command returns the hardware and firmware information from the target computer. The command connects with the remote hardware device that has the management IP address 10.0.0.29 by using the IPMI management protocol and the default port (623). The command specifies the credential object stored in the $Credential variable.

The EnabledState property indicates whether the computer is on or off or in an alternate state, such as quiesce.

---- Example 2: Get information from a remote WSMAN device ----

```
PS C:\> $Credential = Get-Credential Admin
PS C:\> Get-PcsvDevice -TargetAddress "10.0.0.30" -Credential $Credential
-ManagementProtocol WSMan -Port 664 -UseSSL -SkipCACheck -SkipCNCheck
-SkipRevocationCheck
```

This example connects with a WS-Management device by using a custom port, and returns the hardware and firmware information for the device. The remote device uses a self-signed certificate for authentication, so the Get-PcsvDevice cmdlet specifies the SkipCACheck and SkipCNCheck parameters. Specify these parameters only for connecting to trusted remote hardware devices.

The first command uses the Get-Credential cmdlet to create a credential, and then stores it in the $Credential variable. The cmdlet prompts you for a user name and password. For more information, type `Get-Help Get-Credential`.

The second command returns the hardware and firmware information from the target computer. The command connects with the target computer that has the management IP address 10.0.0.30 by using the WS-Management protocol, SSL, and port 664. The command specifies the credential object stored in the $Credential variable.

The command specifies that the client connects by using HTTPS without validating that a CA authority signed the server certificate. The command specifies that the certificate common name (CN) of the server does not need to match the host name of the server. The command specifies that the cmdlet skips the revocation check of server certificates.

Example 3: Get information from a remote WSMAN device over HTTP

```
PS C:\> Set-Item WSMan:\localhost\Client\TrustedHosts "10.0.0.30"
PS C:\> Set-Item WSMan:\localhost\Client\AllowUnencrypted true
PS C:\> $Credential = Get-Credential Admin
PS C:\> Get-PCSVDevice -TargetAddress 10.0.0.30 -ManagementProtocol WSMan
-Port 16992 -Credential $Credential -Authentication Digest
```

This example connects with a WS-Management using HTTP. Since the traffic is unencrypted, additional configuration on the management client is required.

The first two commands create the configuration that the WS-Management client on Windows requires to enable unencrypted WSMAN traffic. This is a one-time only configuration.

The third command uses the Get-Credential cmdlet to create a credential, and then stores it in the $Credential variable. The cmdlet prompts you for a user name and password. For more information, type `Get-Help Get-Credential`.

The fourth command connects with the target computer that has the management IP address 10.0.0.30 by using the WS-Management protocol and port 16992. The command specifies the credential object stored in the $Credential variable.
The command specifies the Digest authentication method for the device.

```
REMARKS
    To see the examples, type: "get-help Get-PcsvDevice -examples".
    For more information, type: "get-help Get-PcsvDevice -detailed".
    For technical information, type: "get-help Get-PcsvDevice -full".
    For online help, type: "get-help Get-PcsvDevice -online"
```