


PowerShell Cmdlets for SQL Diagnostic Manager

The following cmdlets help you automate the administration of your SQL Diagnostic Manager deployment.

 To use SQL Diagnostic Manager snapin, you have to [enable the provider and register the SQLDM drive](#).

Cmdlet Name	Description	Examples
Escape-SQLdmName	Allows you to specify server names containing special characters such as ?/<>[]:*	<pre>Escape-SQLdmName Server\Instance</pre> <ul style="list-style-type: none"> Escapes the instance name Server\Instance. <pre>Escape-SQLdmName Server\Instance1,Server\Instance2</pre> <ul style="list-style-type: none"> Escapes the array of instance names. <pre>Escape-SQLdmName Server\Instance Escape-SQLdmName -undo</pre> <ul style="list-style-type: none"> Escapes the instance name Server\Instance and then undo the operation. <pre>Set-SQLdmMonitoredInstance (Escape-SQLName Server\Instance1) -WindowsAuthentication</pre> <ul style="list-style-type: none"> Escapes the instance name for a Windows user.
Get-SQLServers	Retrieves a list of SQL Servers on the network	<pre>Get-SQLServers</pre> <ul style="list-style-type: none"> Returns a list of all known SQL Servers. <pre>Get-SQLServers -localonly</pre> <ul style="list-style-type: none"> Returns a list of SQL Servers running on the local machine.
Grant-SQLdmPermissions	Grants SQL Diagnostic Manager permissions on a server	<pre>Grant-SQLdmPermission -Path dm:\appsecurity\AUser\AServer -Permission View</pre> <ul style="list-style-type: none"> Grants View permissions to instance 'AServer' to user 'AUser'. <pre>Grant-SQLdmPermission -Path("dm:\appsecurity\" + (Escape-SQLdmName -Name MyDomain\AUser)) -Name AServer -Permission Modify</pre> <ul style="list-style-type: none"> Grants Modify permissions to instance 'AServer' to Windows user 'MyDomain\AUser'. <pre>Grant-SQLdmPermission -Path dm:\appsecurity\AUser -Tag Prod -Permission Modify</pre> <ul style="list-style-type: none"> Grants a user permissions to instances tagged as Prod.
New-SQLdmAlertTemplate	Associates a template to a monitored instance or a tag	<pre>New-SQLdmAlertTemplate</pre> <ul style="list-style-type: none"> Enter the following parameters when using this command: TemplateName, DataSource, and RepositoryName or Tag.
New-SQLdmDrive	Creates a drive for connecting to the SQLdm Repository	<pre>New-SQLdmDrive dm MYSQLDMSERVER SQLdmRepository</pre> <ul style="list-style-type: none"> Creates a new SQL Diagnostic Manager drive called 'dm' that is connected to the SQLdmRepository database on the MYSQLDMSERVER SQL Server using Windows Authentication. <pre>New-SQLdmDrive dm MYSQLDMSERVER SQLdmRepository -Credential sa</pre> <ul style="list-style-type: none"> Creates a new SQL Diagnostic Manager drive called 'dm' that is connected to the SQLdmRepository database on the MYSQLDMSERVER SQL Server using SQL Authentication. Note that Powershell will prompt for the password.

<p>New-SQLdmMonitoredInstance</p>	<p>Adds a SQL Server Instance to monitor in SQL Diagnostic Manager</p>	<pre>New-SQLdmMonitoredInstance -Path Instance1 -WindowsAuthentication -tags production,finance,critical</pre> <ul style="list-style-type: none"> • Adds a new instance named Instance1 to SQL Diagnostic Manager. <pre>New-SQLdmMonitoredInstance -Path (Escape-SQLdmName -Name ServerA\Instance1) -Credential sa</pre> <ul style="list-style-type: none"> • Adds a new instance named ServerA\Instance1 to SQL Diagnostic Manager.
<p>New-SQLdmUser</p>	<p>Creates a new SQL Diagnostic Manager user</p>	<pre>New-SQLdmUser -Path fred -SQLLogin -Password xxxx -Comment "Fred is an admin"</pre> <ul style="list-style-type: none"> • Creates a new user called fredthat uses SQL Authentication . Note that if the password is not specified, PowerShell will prompt for the password. <pre>New-SQLdmUser (Escape-SQLdmName -Name mydomain\fred) -WindowsUser</pre> <ul style="list-style-type: none"> • Creates a new user called mydomain\fred that uses Windows Authentication.
<p>Remove-SQLdmMonitoredInstance</p>	<p>Removes a SQL Server Instance from SQL Diagnostic Manager monitoring</p>	<pre>Remove-SQLdmMonitoredInstance -Path \Instances\ServerA</pre> <ul style="list-style-type: none"> • Removes the instance named ServerA from SQL Diagnostic Manager. <pre>Remove-SQLdmMonitoredInstance (Escape-SQLdmName -Name ServerA\Instance1) -retaindata</pre> <ul style="list-style-type: none"> • Removes the instance named ServerA from SQL Diagnostic Manager but retains its data for reporting.
<p>Remove-SQLdmUser</p>	<p>Removes an existing SQL Diagnostic Manager user</p>	<pre>Remove-SQLdmUser -Path /AppSecurity/fred</pre> <ul style="list-style-type: none"> • Removes user fredfrom SQL Diagnostic Manager. <pre>Remove-SQLdmUser (Escape-SQLdmName -Name MyDomain\AUser)</pre> <ul style="list-style-type: none"> • Removes Windows user MyDomain\AUser from SQL Diagnostic Manager.
<p>Revoke-SQLdmPermission</p>	<p>Revokes SQL Diagnostic Manager permissions on a server</p>	<pre>Revoke-SQLdmPermission -Path \AppSecurity\fred\ServerA</pre> <ul style="list-style-type: none"> • Revokes user fred's permissions to instance ServerA. <pre>Revoke-Permission -Path /AppSecurity/fred -Name ServerA</pre> <ul style="list-style-type: none"> • Revokes user fred's permissions to instance ServerA. <pre>Revoke-Permission -Path /AppSecurity/fred -Tag Prod</pre> <ul style="list-style-type: none"> • Revokes user fred's permissions to instances tagged as Prod. <pre>Revoke-SQLdmPermission -Path ("dm:\AppSecurity\" + (Escape-SQLdmName -Name MyDomain\UserA)) -Name (Escape-SQLdmName -Name ServerA\Instance1)</pre> <ul style="list-style-type: none"> • Revokes Windows user MyDomain\UserA permission to ServerA\Instance1.
<p>Set-SQLdmAppSecurity</p>	<p>Enables or disables Application Security for SQL Diagnostic Manager</p>	<pre>Set-SQLdmAppSecurity \AppSecurity -Enabled</pre> <ul style="list-style-type: none"> • Enables SQL Diagnostic Manager Application Security. <pre>Set-SQLdmAppSecurity \AppSecurity -Disabled</pre> <ul style="list-style-type: none"> • DisablesSQL Diagnostic Manager Application Security.
<p>Set-SQLdmLogging</p>	<p>Sets the logging level of the SQL Diagnostic Manager provider</p>	<div style="border: 1px solid red; padding: 5px;">  Use Set-SQLdmLogging for debugging purposes only. This cmdlet should be used at the request of IDERA Technical Support. </div>

<p>Set-SQLdmMonitoredInstance</p>	<p>Configures options on your SQL Server Instance</p>	<pre>Set-SQLdmMonitoredInstance -Path Instance1,Instance2,Instance3 -Credential sa</pre> <ul style="list-style-type: none"> • Updates the credentials used for Instance1,Instance2, and Instance3 to use SQL Authentication and sets a new login and password. Note that PowerShell will prompt for the password. <pre>Set-SQLdmMonitoredInstance (Escape-SQLdmName -Name ServerA\Instance1) -WindowsAuthentication</pre> <ul style="list-style-type: none"> • Updates the credentials used for ServerA\Instance1 to use Windows Authentication.
<p>Set-SQLdmUser</p>	<p>Set the properties of an existing SQL Diagnostic Manager user</p>	<pre>Set-SQLdmUser -path \AppSecurity\bozo -Disabled -Comment "Bozo is disabled."</pre> <ul style="list-style-type: none"> • Disables the Set SQL Diagnostic Manager user bozo. <pre>Set-SQLdmUser fred -Enabled -Administrator</pre> <ul style="list-style-type: none"> • Enables SQL Diagnostic Manager user fred and gives him administrator rights. <pre>Set-SQLdmUser (Escape-SQLdmName -Name mydomain\fred) -Disabled</pre> <ul style="list-style-type: none"> • Disables the SQL Diagnostic Manager user mydomain\fred.