



Pure Storage FlashArray Management Extension For Microsoft SQL Server Management Studio

Tuesday, November 02, 2021 14:32

Contents

Chapter 1: Introduction	5
Overview	5
Features	5
Audience	9
Chapter 2: Best Practices	10
Metadata Files	10
Back up Extension Metadata and Configuration Data	10
Configuration	10
Administrators	11
Runtime	12
Limitations in this Release	12
Chapter 3: Setup	14
Before You Begin	14
Download and Install the Microsoft SSMS Application	15
Download and Install the Pure Storage FA SSMS Extension	16
Chapter 4: Using the FA SSMS Extension GUI	17
Overview of Using the Pure Storage FA SSMS Extension	17
Open the Pure Storage FA SSMS Extension Context Menu	17
Manage Credentials	18
Backup Configurations	24
Backups	31
Extension Settings	37
Chapter 5: Considerations with FlashArray Replication	38
Recovery in ActiveCluster Environments	38
Recovery with ActiveDR Arrays	38
Chapter 6: The Pure Storage PowerShell Backup SDK	40
SDK Overview	40
Installation and Import	40
Cmdlets List, Cmdlets Help, and Cmdlet Equivalents	40
Using the PowerShell Backup SDK Cmdlets	43
Utility Cmdlets	49
PowerShell TroubleShooting	50

Appendix A: Example of Configuring a Database Hosted on a FlashArray Volume	52
Appendix B: Troubleshooting	56
Issue: Attach Database Failed	56
Issue: Connecting to the Remote Server Failed	57
Issue: Backup Output Error	57
Issue: Creating a Backup Configuration Times Out	58
Issue: Permissions Errors	58
Issue: VSS PureProvider service is not compatible	59
Issue: VSS_E_NOT_SUPPORTED Error	59
Issue: VMware PowerCLI Error log4net.dll Missing	60
Appendix C: Resources	61
Pure Storage Documentation	61
Documentation Feedback	62
Appendix D: Copyright and Notices	63
End User Agreement	63
Copyrights and Licenses	63

Chapter 1. Introduction

Overview

The Pure Storage FlashArray Management Extension for Microsoft SQL Server Management Studio (the FA SSMS Extension) is a host-based integration that executes on the Windows Server™ to manage SQL Server backup and restore operations. The Extension supports creating application-consistent snapshots using the Pure Storage Volume Shadow Copy Service (VSS) Hardware Provider. The Extension can be used from the FA SSMS GUI or automated using the Pure Storage Backup SDK Windows PowerShell module. Database administrators can manage backup and restore operations on local and remote databases from a centralized SSMS deployment.

The included Pure Storage Backup SDK provides automation of application-consistent SQL backup and restore operations, which can greatly help administrators learn and accomplish their tasks easily while avoiding common mistakes.

Microsoft® SQL Server™ Management Studio (SSMS) is an easy to use GUI provided by Microsoft as part of the SQL Server product. SSMS is based on the Visual Studio™ Shell, which can be extended using plugins.

The Pure Storage® FlashArray™ system is an ideal storage platform for performance intensive workloads. Pure's fast and highly available storage enables enterprise database applications to achieve top notch performance. Pure Storage strives for usage simplicity and provides management UIs and tools to help database administrators accomplish daily tasks easily.

Features

The Pure Storage FA SSMS Extension supports following backup and restore operations:

- Create and edit a backup configuration
- Perform backups based on named backup configurations
- Search and filter the backup history
- Remove a backup from the backup history
- Restore from a backup
- Mount or dismount a backup

Full and copy-only backups are supported:

- **Full backup** -- Backs up the entire database, including part of the transaction log so that the full database can be recovered after a full database backup is restored. A full database backup represents the database at the time the backup finished.
- **Copy-only backup** -- Provides the ability to use a database for scenarios such as development, test, and QA. A copy-only backup is independent of the sequence of conventional SQL Server backups.

Contrast this with a full backup, in which case the database is alerted and which affects how later backups are restored. This is not the case with copy-only backups.

Note: Administrators are responsible for ensuring point-in-time recovery when copy-only backups are used.

The following database restore use cases are supported:

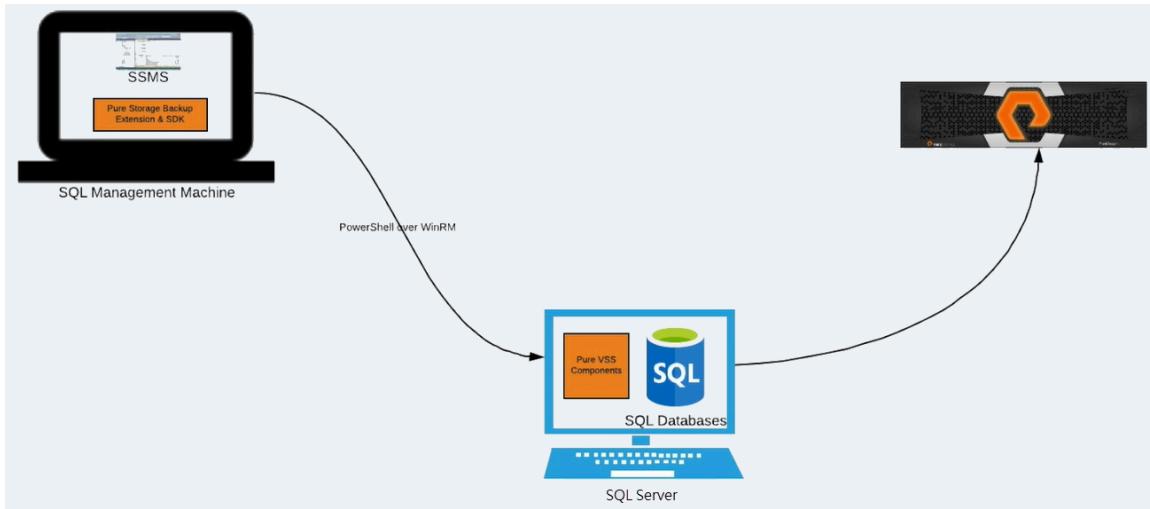
- **Database restore** -- Import a backup (snapshot), then restore a database to the original location. This operation performs an overwrite of the original database volumes in place by restoring Pure Volumes that hold database or transaction log files. Other data, including other SQL data files located on those Pure Volumes, are also impacted by this point-in-time restore.
When some volumes are missing a snapshot, the Allow Partial Restore option supports a restore for those volumes for which snapshots exist.
- **Database restore with No-Recovery** -- Import a backup (snapshot), then restore a database in No-Recovery Mode. The restored database is left in the *Recovering* state. This option provides support for point-in-time recovery. Additional transaction logs can be applied manually.
- **Database mount** -- Import a backup (snapshot), then restore a database to a different drive letter or mount point on the original or a different server, using the **Mount** option.
The database files can be copied to the original location, or the database can be directly attached. If attached to the original server, be sure to make the **Attach as** name unique.

The Pure Storage FA SSMS Extension also supports following related features:

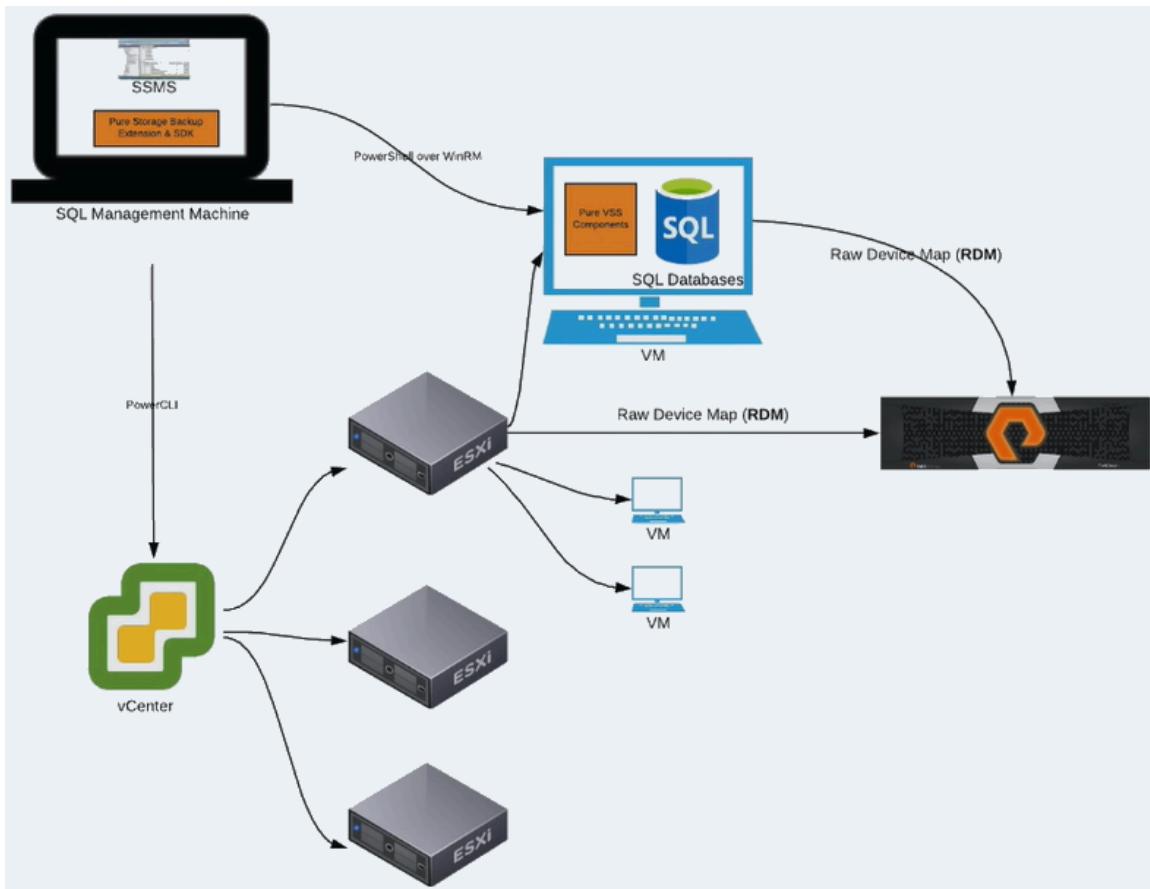
- Backups on running databases, without bringing the databases offline
- Automation through the Pure Storage PowerShell Backup SDK
- Application-consistent snapshots using the VSS Hardware Provider
- Microsoft SQL Server physical deployments
- VMware ESXi™ physical raw device maps (pRDMS)
- Scheduling administrative tasks using SQL Server Agent jobs with the **CmdExec** proxy option
- Managing databases running on the Pure Cloud Block Store™ virtual appliance
- A centralized installation to back up multiple databases (both local and remote)

The following diagram shows a simple scenario:

- The SQL database is hosted on the FlashArray.
- The Pure Storage FA SSMS Extension is installed on the SQL Management Machine with the Microsoft SSMS application.
- The Extension communicates with the SQL Server with PowerShell over WinRM.
- Multiple SQL Servers and multiple FlashArrays are also supported (not shown).

Figure 1.1:


The following diagram shows a scenario in which the SQL Server is hosted on an ESXi VM:

Figure 1.2:


Components

The following components are included with the FA SSMS Extension:

- The FA SSMS Extension for SQL Server Management Studio
- The Pure Storage Volume Shadow Copy Service (VSS) hardware provider
- The Pure Storage Backup SDK Windows PowerShell module for automation of all operations supported in the FA SSMS Extension

Named Backup Configurations

The FA SSMS Extension uses named backup configurations that define the databases to be backed up, along with other information such as credentials.

Each configuration has a name that you provide. The name is like an alias for the backup job and allows the configuration to be reused conveniently.

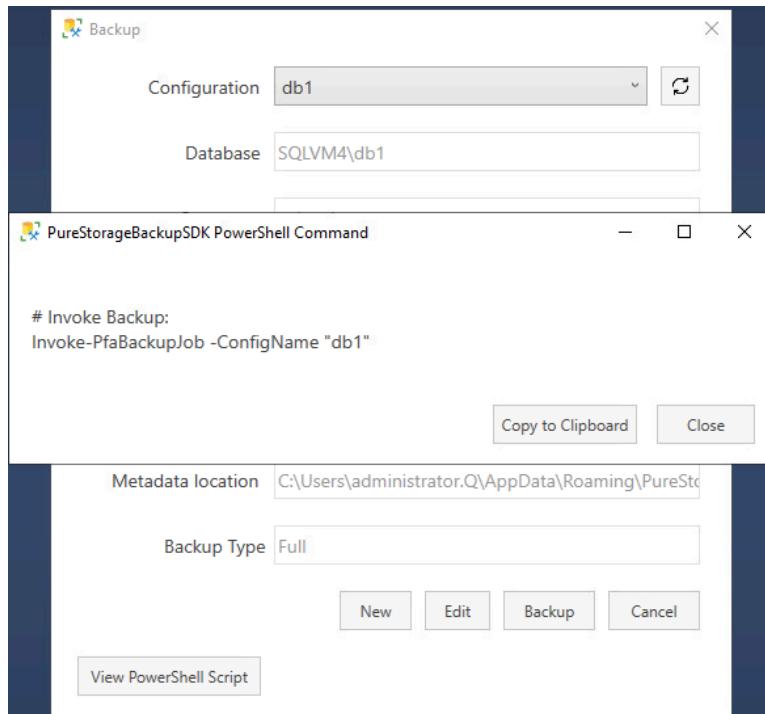
Automation

The FA SSMS Extension includes the Pure Storage Backup SDK, which offers scripting for all of the Extension's backup, restore, and history functions.

PowerShell scripts use the backup configuration name to automate your backup jobs.

As a convenience, FA SSMS Extension GUI screens provide a **View PowerShell Script** button that provides the equivalent PowerShell CLI script to each GUI operation.

Figure 1.3:



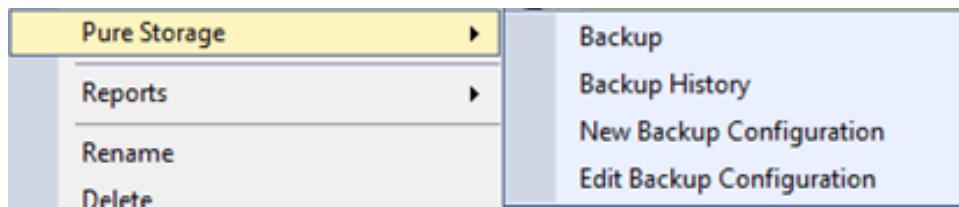
The FA SSMS Extension is also compatible with automation through SQL Server Agent jobs scheduling.

Access in the SQL Server Studio

The FA SSMS Extension appears in the Microsoft SQL Server Management Studio as an individual database context menu ("Pure Storage Snapshot Management") and also as a top level menu item ("Pure Storage").

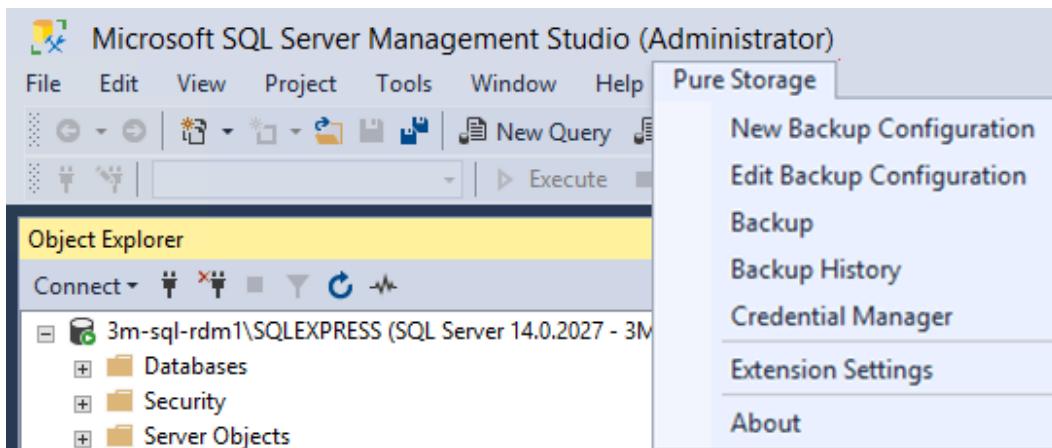
In a database context menu:

Figure 1.4:



In the SSMS top-level tool bar:

Figure 1.5:



Audience

This guide describes how to install, configure, and use the Pure Storage FlashArray SSMS Extension to provide application-consistent backup and restore of SQL databases with Microsoft SQL Server Management Studio and the Pure Storage VSS Hardware Provider.

The intended audiences for this guide include database administrators and SSMS administrators, who configure and support database backup and restore.

This guide assumes familiarity with storage, application-consistent snapshots, and Microsoft SSMS administration.

Chapter 2. Best Practices

Metadata Files

The FA SSMS Extension uses metadata to track backup information along with information about the database. Each backup run generates metadata that is required to successfully restore from the backup.

The Extension saves this metadata as XML files in a central location of your choosing so that the required information can be found during a restore. While the central location of the metadata files is configurable, after a backup has been made, it is extremely important to not move, edit, rename, or in any way modify a metadata file. To do so would make a restore of that backup impossible.

 **Important:** Do NOT move, modify, or rename a backup's metadata file after a backup or snapshot has been created.

It is impossible to mount or restore a snapshot through the Extension if the metadata file is been modified or cannot be located. A manual volume copy (with or without overwrite) is required to access the data, provided that the snapshots still exist.

The default location for the Extension's metadata files is `C:\Users\<username>\AppData\Roaming`.

Back up Extension Metadata and Configuration Data

Important: We recommend that you regularly backup the following directories on the SQL management machine:

- The Extension's metadata files directory.
The default location for the Extension's metadata files is `C:\Users\<username>\AppData\Roaming`. However, a different location could be specified during installation.
- The Extension's configuration data directory, `%PROGRAMDATA%\PureStorage\PureStorageBackupSDK`.

Configuration

Volume design principles

 **Critical information**

- Consider assigning each database its own FlashArray volume. This practice makes restore operations safer, by being less likely to unintentionally overwrite other software.
A restore operation affects the entire drive where the database resides. In addition to database files, any other files placed in that drive would be restored as well.
- Consider assigning each database its own volume that is not also the operating system volume.

- Ensure that no database to be backed up is directly on the same volume as the operating system or the SQL Server.

Databases to be backed up cannot be in the system drive (c:) and cannot be on the same drive(s) as other SQL Server databases including the SQL Server system databases `master`, `tempdb`, `model`, and `msdb`.

Remote connectivity

With PowerShell remoting and Windows™ systems, ensure that the admin level of TrustedHosts is correctly set.

For more information, see [Windows PowerShell Remoting](#) and [Trusted Hosts](#) in the [Setup](#) chapter.

Databases as LUNs on the FlashArray

The databases hosted on Microsoft SQL Server can be on one or more disks. The recommendation from Pure Storage is that each of these disks be configured as a LUN (Logical Unit of storage) in a single partition (NTFS or (Re)FS) on the FlashArray.

Multiple partitions on a single Pure volume are not supported.

For example, if a database named `testDB` contains `testDB.mdf` and `testDB_log.ldf`, both can reside on `E:\` and `F:\` drives respectively. Note that `E:\` and `F:\` drives correspond to two LUNs on the Pure Storage FlashArray.

When the Pure Storage Backup SDK takes a backup of a database, that operation creates a Pure Storage snapshot for the set of LUNs that correspond to the input database.

For SQL Servers that are workstations

Both domain accounts and local user accounts are supported.

Users may have to set appropriate security policies to enable PowerShell remoting.

With SQL Server Availability Groups

The current release does not support seeding a database in order to join a database into an existing SQL Server Availability Group. Application consistent and crash consistent snapshots can be used for databases or volumes that participate in a SQL Server Availability Group, to be mounted as a standalone database outside of the SQL Server Availability Group.

As a workaround, add the database to the availability group after the database is restored.

With a Windows Server Failover Cluster

When deploying a database, the database should be isolated onto its own clustered disk and not be included with the SQL Server master, model, or msdb databases. Master, model, and msdb are typically installed on the root drive (C:\) but will be installed on the shared disk assigned to the SQL Server role for the SQL instance in a SQL Failover Cluster Instance. The new user database disk must be added to the cluster, added to the SQL role, and then made dependent of the SQL Server resource.

Administrators

FA SSMS Extension administrators require the following:

- Must be an administrator in the SQL instance.

- Must be added to the local server Administrators Group.

Runtime

Run SSMS only as administrator

Run the SSMS application with administrator credentials for the machine the SSMS application is hosted on.

Mounting a backup in a failover cluster

When performing a mount operation in a Microsoft failover cluster, mount the database node outside of the current failover cluster, in order to avoid a signature collision.

Restoring volumes that contain multiple databases

When restoring a volume that contains multiple databases, do not perform an overwrite (an in-place restore).

An in-place restore effectively reverts all databases on the volume back to the time of the backup.

Following this practice makes restore operations safer and less likely to unintentionally overwrite other software.

Run management operations on the SSMS machine only

Run the backup, restore, and mount management operations only from the machine where SSMS is deployed.

Avoid manual operations on the SQL Servers

Manual operations on the SQL Servers are not recommended.

Operations to be avoided on the SQL Servers include masking (removing a shadow copy or snapshot), importing a snapshot, mounting a snapshot, and dismounting a snapshot.

Read-only Partitions after Restoring a Snapshot

When a snapshot with the `vss` suffix where the provider took the snapshot is copied manually (outside of FA SSMS Extension or the Pure Storage Backup SDK), the restored content will be hidden and read only.

For instance, if a VSS snapshot is the source and is either restored to a live file system or copied to another Pure Storage volume, the partition on each volume is hidden and read only.

For steps to make the partitions writable, see [Issue: Attach Database Failed](#).

Limitations in this Release

Mounting on the Backup Machine

Mounting is only supported on the same physical SQL machine that was backed up. Mounting to a VM or to a different physical machine is not supported in this release.

SQL Servers Hosted on VMs

Only VMware ESXi virtual machines configured with the raw device mapping (RDM) storage access method are supported. On virtual SQL Server machines, mounting is supported only to virtual machines on the same hypervisor machine.

Manual Cleanup after Removing a Backup History Entry

In this release, by default, when an entry is removed from the Backup History listing, the Extension does not delete either the backup snapshots or volumes on the FlashArray or associated items in the VSS history or cache.

When deleting an entry from the backup history, the snapshot on the FlashArray can also be destroyed if the **Destroy Snapshots on FlashArray** GUI check box is checked, or if the switch **-DestroySnapshot** is used in the **Remove-PfaBackupHistory** cmdlet in the Pure Storage Backup SDK.

If the snapshot is not marked for destruction during the removal of the entry from the backup history, clean up of these associated items has to be done manually.

Support for SQL Servers Hosted on a Virtual Volume (vVol)

In this release, vVol support is in beta and is not available for general release. We expect to remove this limitation in a subsequent release.

The Backup Configuration dialog accepts the selection of **vvol** but any backups attempted with that configuration fail.

Volumes in Multiple Protection Groups

The FA SSMS Extension does not support volumes that are members of more than one protection group.

Choose one of the following workarounds if you have one or more volumes in multiple protection groups:

- Rearrange protection group membership so that each volume is a member of at most one protection group.
OR,
- Change the Pure Storage VSS Hardware Provider to take volume snapshots instead of protection group snapshots.

The following command to change to volume snapshots. Run this command on each SQL Server host:

```
pureproviderconfig.exe volumesnapshotonly --enable
```

The full path might be required for this command. At the default installation location, the command (to be entered as one line) is:

```
C:\program files\pure storage\vss\provider\pureproviderconfig.exe
volumesnapshotonly --enable
```

Note: This change affects all FA SSMS Extension snapshots.

Renaming a Protection Group

Renaming a FlashArray protection group is not supported.

To do so would also rename all snapshots that have previously been created for the protection group and would cause the FlashArray SSMS Extension not to find, mount, restore, or delete those snapshots.

Chapter 3. Setup

Before You Begin

Review the Release Notes

If you have not already done so, please review the release notes. See the Releases section of [Pure Storage FlashArray Management Extension for Microsoft SQL Server Management Studio](https://support.purestorage.com/Solutions/Microsoft_Platform_Guide/bbb_Microsoft_Integration_Releases/Pure_Storage_FlashArray_Management_Extension_for_Microsoft_SQL_Server_Management_Studio#Releases). [https://support.purestorage.com/Solutions/Microsoft_Platform_Guide/bbb_Microsoft_Integration_Releases/Pure_Storage_FlashArray_Management_Extension_for_Microsoft_SQL_Server_Management_Studio#Releases]

Verify System Requirements and Compatibility

Verify that your system meets the minimum requirements to run the FA SSMS Extension.

Software	Minimum Version
Microsoft SQL Server (Supported only on Windows Server 2012r2, 2016, 2019, or 2022, or on Windows 10)	2012R2
Microsoft SQL Server Management Studio (SSMS)	18.x
PowerShell (Must be installed manually on Windows Server 2012R2)	5.0
PowerCLI (If the SQL Server is hosted on a VMware ESXi VM, PowerCLI is required on the SSMS host and must be installed in <code>C:\Program Files\WindowsPowerShell\Modules</code>)	The most recent release
.NET	4.5
Purity//FA	5.3.0 or later
Purity REST API	1.7
All Windows systems	64-bit operating system

The following sections describe additional requirements in certain environments.

For SQL Servers Hosted on VMs

The following are required when a SQL Server is hosted on a VM:

- VMware vCenter Server 6.0 or higher
- PowerCLI on the SSMS host

Windows PowerShell Remoting

PowerShell remoting must be enabled on the SQL Server machine.

For steps to enable PowerShell remoting, please see Microsoft PowerShell documentation. At the time of this writing, the link is [Enable-PSRemoting](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-7) [<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-7>].

The Extension installer includes the Pure Storage PowerShell Backup SDK and the Pure Storage VSS Hardware Provider. When Windows PowerShell remoting is enabled and running on the SSMS machine, the Extension automatically installs the Pure Storage PowerShell Backup SDK and the Pure Storage VSS Hardware Provider on SQL Server machines when required.

Windows PowerShell remoting is a prerequisite for this feature.

See also the Microsoft article [Installation and Configuration for Windows Remote Management](https://docs.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management) [<https://docs.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management>].

Trusted Hosts

If the environment includes hosts for the SSMS application or the SQL Servers that are not in the same Active Directory domain, manually add those hosts that are not within the SSMS application host's domain to the TrustedHosts list on the SSMS application host.

Example command to add a SQL Server to the TrustedHosts list:

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Value <SQL Server host address>
```

The SQL Server host's fully-qualified domain name (FQDN) can be used in place of the address.

You may need to restart the WinRM service for the new settings to take effect.

```
Restart-Service WinRM
```

Run the following command to test the remote functionality of the WinRM by attempting to connect to the SQL Server (where `sqlserver` is the SQL Server name):

```
winrm id -r:sqlserver
```

See [PowerShell Troubleshooting](#) for an example of an error message seen due to TrustedHost issues.

Download and Install the Microsoft SSMS Application

If you have not already done so, download and install Microsoft's stand-alone SSMS application before installing the Pure Storage FA SSMS Extension.

Download the Microsoft SSMS 18.x or later installer from one of the following links:

- The Microsoft SSMS download page is [Download SQL Server Management Studio](https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15) [<https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15>].
- This link begins the download of the SSMS installer executable directly (no landing page): [go.microsoft.com](https://go.microsoft.com/fwlink/?linkid=2108895&clcid=0x409) [<https://go.microsoft.com/fwlink/?linkid=2108895&clcid=0x409>].

Links are subject to change. Follow Microsoft SSMS documentation for installation instructions.

Download and Install the Pure Storage FA SSMS Extension

Install the Extension on the Microsoft SQL Server Management Studio machine. The FA SSMS Extension needs to be installed only once and that is on the SSMS application host machine.

The installer is hosted on both github.com [<https://github.com>] and [Pure1 Support](https://support.purestorage.com) [<https://support.purestorage.com>]. Please see the release notes for the download locations.

Run the FA SSMS Extension installer, `PureSSMSInstaller.msi`, and follow the prompts.

Note: If you do not select the default location for the Extension's metadata files, make a note of the new location in order to back up the metadata files regularly. See [Back up Extension Metadata and Configuration Data](#).

Chapter 4. Using the FA SSMS Extension GUI

Overview of Using the Pure Storage FA SSMS Extension

The first step is to create a backup configuration, which is the definition of what a backup should do. (See [Create a New Backup Configuration](#).)

You can create multiple backup configurations, which can be used to run a backup on demand and can be automated through the Pure Storage PowerShell Backup SDK.

Open the Pure Storage FA SSMS Extension Context Menu

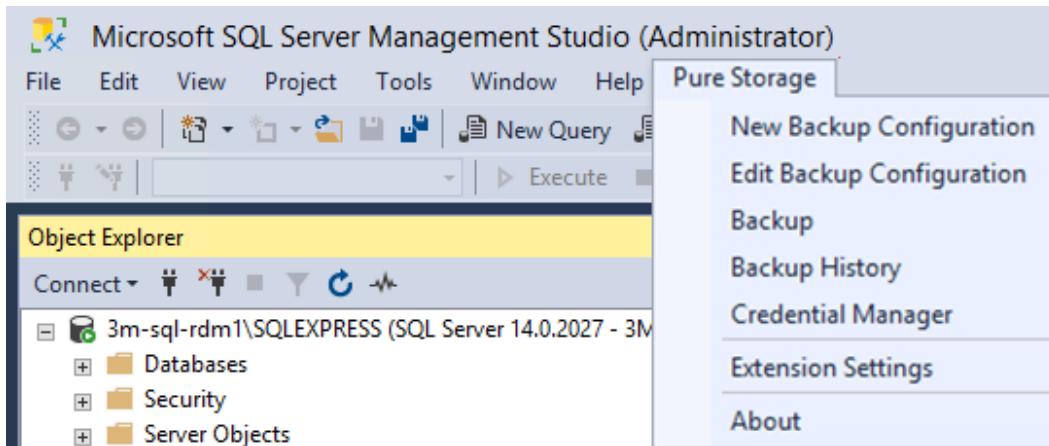
There are two ways to open the FA SSMS Extension content menu, from the SSMS tool bar or from a database selected in the Object Explorer.

The Pure Storage tab in the SSMS tool bar provides the full FA SSMS Extension content menu, which applies to SQL databases that are backed up by the Extension. The Extension content menu opened from a specific database offers actions only on that database and its backups.

From the SSMS Tool Bar

To open the Extension menu from the SSMS tool bar, select the **Pure Storage** tab:

Figure 4.1:



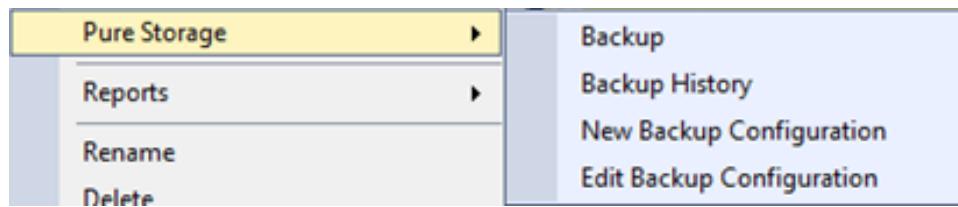
From the Context Menu for a Database

Note: the first time you open a database's context menu, if the Extension is still initializing, the Pure Storage menu does not appear. If that happens, please close the menu and reopen it.

To open the FA SSMS Extension menu from a specific database:

1. In the Object Explorer, select the database.
2. Right click the database and select an action for that specific database.

Figure 4.2:

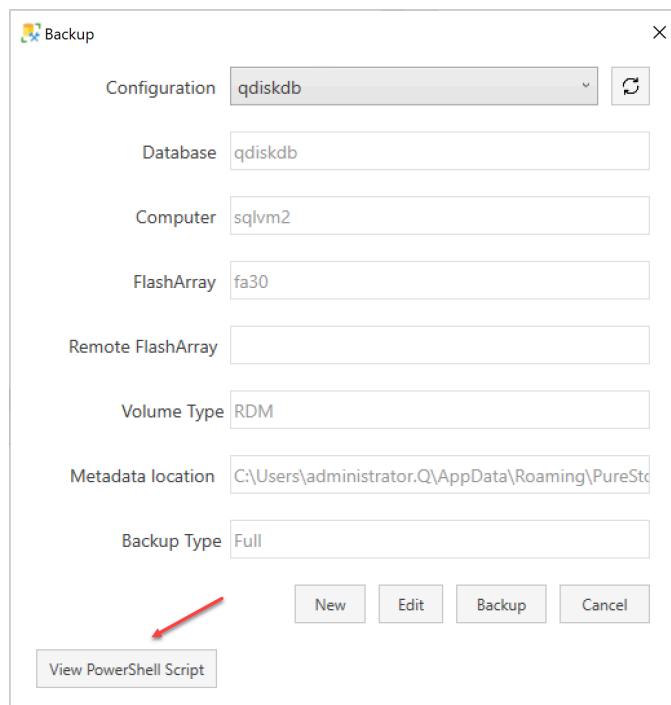


Note about the View PowerShell Script Button

Many FA SSMS Extension dialogs include a `View PowerShell Script` button, which displays the PowerShell Backup SDK commands equivalent to the dialog's action.

Use this button *after* you have filled out the dialog's information. For example:

Figure 4.3:



See also [Cmdlets List](#), [Cmdlets Help](#), and [Cmdlet Equivalents](#).

Manage Credentials

The backup and restore process involves accessing several distinct entities such as the Microsoft SQL Server Management Studio machine, the protected FlashArray, the vCenter Server, the SQL Server, and the VM or computer hosting the SQL Server.

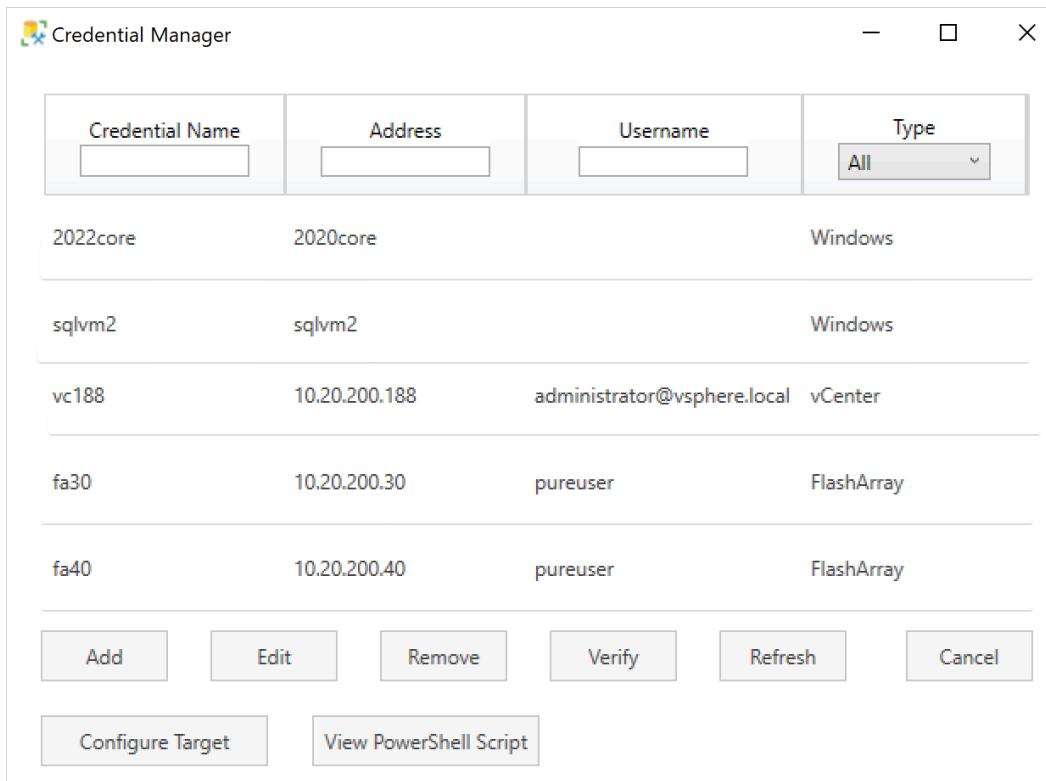
The FA SSMS Extension Credential Manager provides a convenient way to enter, verify, and manage these credentials. Credentials are protected with the Windows ProtectedData class to encrypt credentials. For more information, see the Microsoft article [**ProtectedData Class**](#)

[<https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.protecteddata?view=windowsdesktop-5.0>].

Use of the Credential Manager is optional. Credentials can also be entered in the Backup Configuration dialog when you create or edit a configuration.

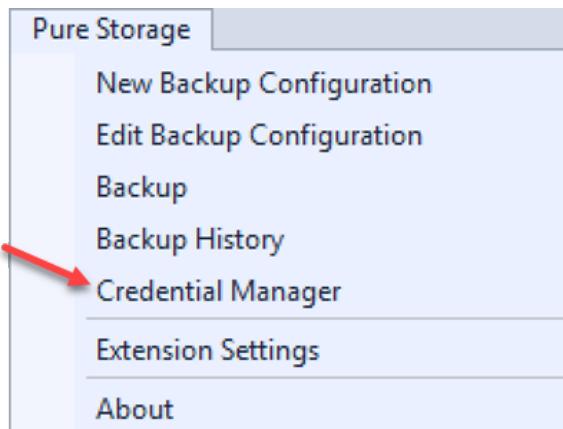
The following is an example of a completed Credential Manager dialog.

Figure 4.4:



To access the Credential Manager, in the SSMS tool bar, select **Pure Storage > Credential Manager**.

Figure 4.5:



Add a Credential

Adding a credential creates a name or nickname by which the credential can be used in your backup configurations.

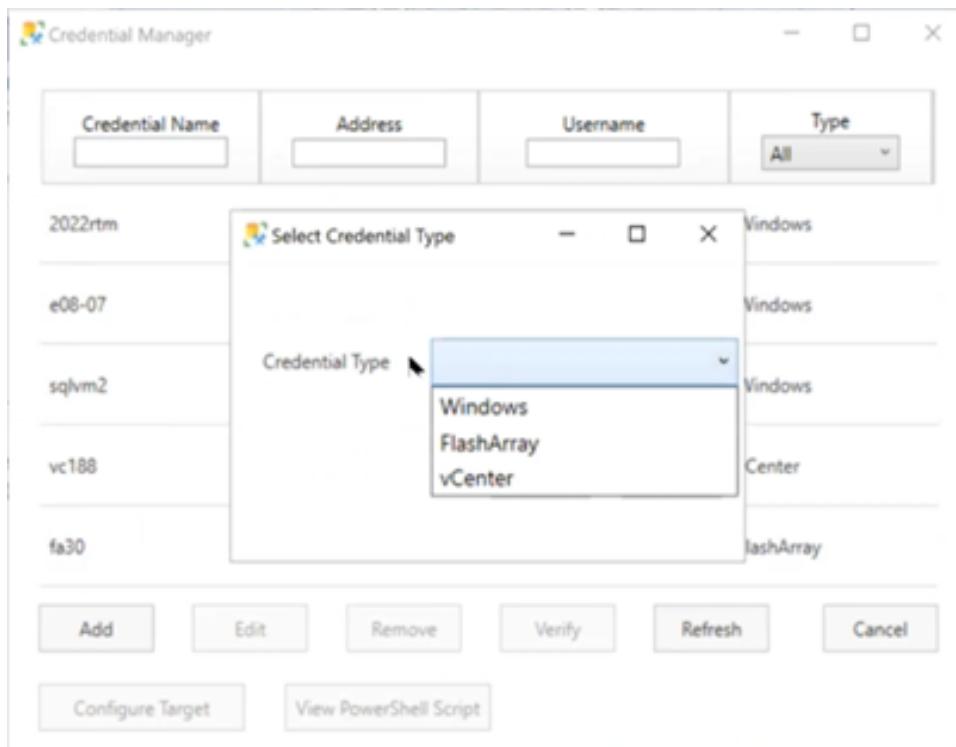
To add a credential:

1. In the SSMS tool bar, select **Pure Storage > Credential Manager**.

Click **Add**.

The Select Credential Type dialog opens.

Figure 4.6:



Select the Credential Type based on the type of machine the new credential is for.

2. A New Credential dialog opens for the selected type.
Complete the dialog with the information for that credential type.

For a Windows credential:

Field	Entry
Computer Label	Enter the name of the machine or VM hosting the SQL Server. This name can be the actual machine name or a nickname used only within the Extension.
Address	Enter the fully-qualified domain name or IP address of the machine hosting the SQL Server. For VMs on ESXi using SQL

Field	Entry
	Failover Cluster Instance, this name must be the SQL Server Network Name. Otherwise, the backup will fail if the role is running on another VM in the cluster.
Use credential for current machine	Enable this check box if the Extension is running on the SQL Server host.
Username	Enter an administrator for the machine hosting the SQL Server.
Password	Enter that administrator's password.

For a FlashArray credential:

Field	Entry
FlashArray Label	Enter the name of the FlashArray hosting the SQL database. This name can be the actual machine name or a nickname used only within the Extension.
Address	Enter the fully-qualified domain name or IP address of the FlashArray hosting the SQL database.
Username	Enter a FlashArray administrator, whose credentials will be used to connect to the array. Array Admin or Storage Admin privileges are required.
Password	Enter that administrator's password.

For a vCenter credential:

Field	Entry
vCenter Label	Enter the name of the vCenter. This name can be the actual vCenter name or a nickname used only within the Extension.
Address	Enter the fully-qualified domain name or IP address of the vCenter.
Username	Enter an administrator for <i>the machine hosting the vCenter</i> .
Password	Enter that administrator's password.

Verify a Credential

To verify a credential:

1. Select the row containing the credential.
2. Click **Verify**.

Remove a Credential

Removing a credential removes the configured name or nickname from the FA SSMS Extension..

To remove a credential:

1. Select the row containing the credential.
2. Click **Remove**.

Refresh

To refresh the Credential Manager:

1. Click **Refresh**.

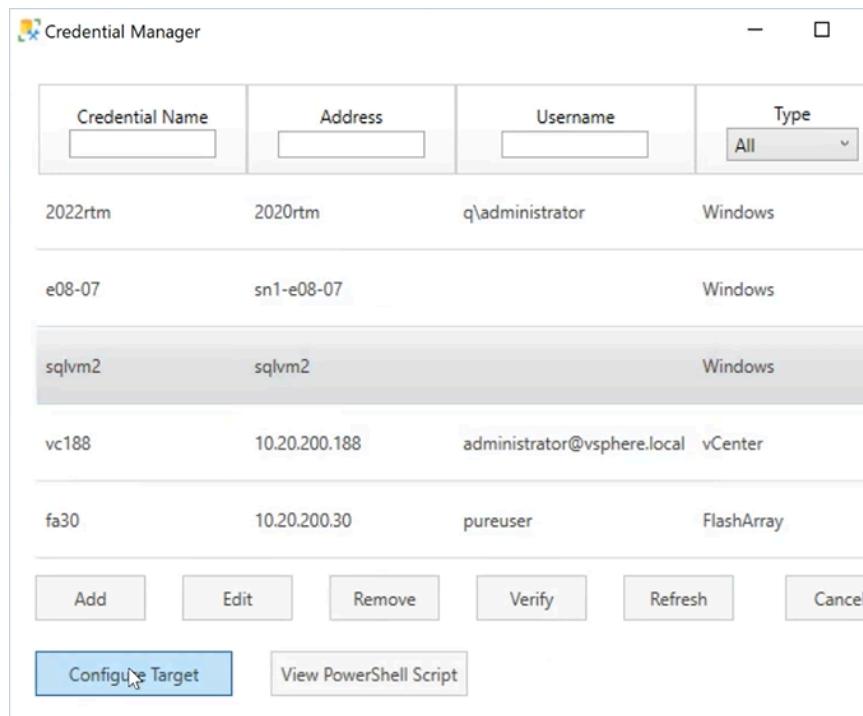
Search or Filter Credentials

Optionally use the **Credential Name**, **Address**, **Username**, and **Type** fields along the top to search for a credential or to filter the displayed credentials.

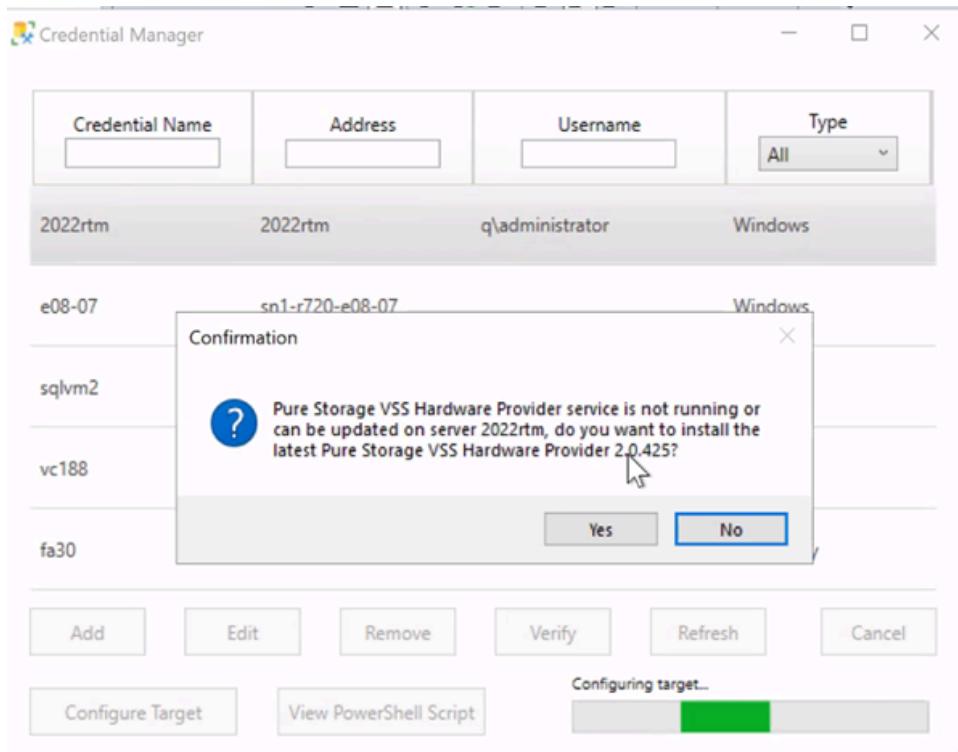
Update the VSS Provider on a Remote Machine

The Credential Manager also supports verifying the VSS Provider of the target and installing or upgrading the VSS Provider on the target. With a Windows entity selected, select the **Configure Target** button.

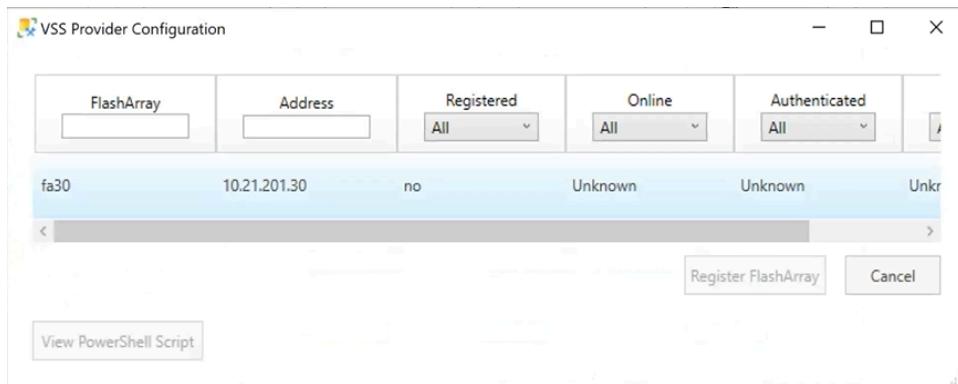
Figure 4.7:



For Windows targets (Microsoft SSMS Servers), the FA SSMS Extension checks if the VSS Provider on that target is up to date, and offers to install or upgrade the VSS Provider on the target when necessary.

Figure 4.8:


The following example shows the VSS Provider is up to date and connects with the FlashArray named **fa30**.

Figure 4.9:


Backup Configurations

Creating a backup configuration is the first step to protecting your database.

A backup configuration is required before a backup can be performed.

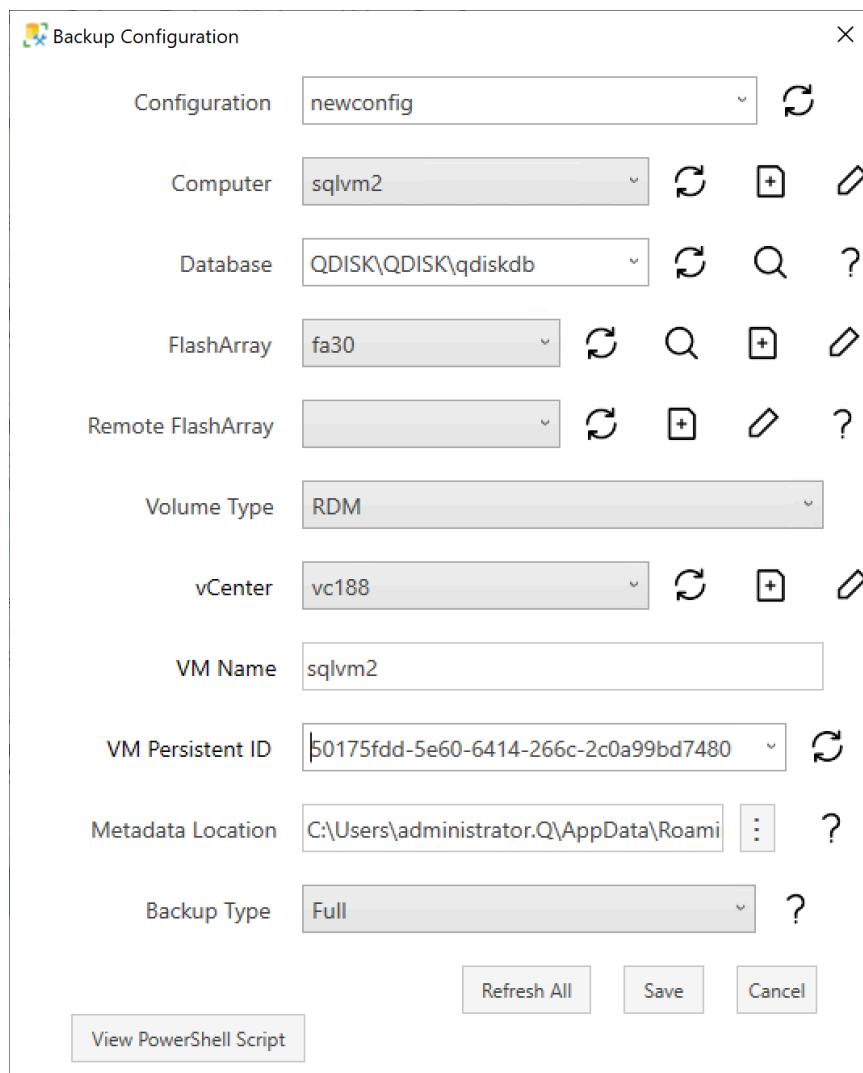
Create a New Backup Configuration

A backup configuration includes the information needed to perform the backup, including database name, whether the database is on a physical machine or on a virtual machine hosted on ESXi and configured in VMware raw device mapping (RDM) mode, whether the backup is full or copy only, and various credentials.

Backup configurations are named, which allows automating backups and reusing configurations by referencing the configuration name.

The following is an example of a completed Backup Configuration dialog.

Figure 4.10:



Notes:

- PowerCLI must be installed on the Microsoft SQL Server Management Studio host before you can create a backup configuration for a SQL Server that is hosted on a VMware ESXi VM.
- When creating a backup configuration, enter the Computer, Computer Credential, Database, FlashArray, and FlashArray Credential fields in exactly the order shown in the Backup Configuration dialog.

After you specify the SQL Server ("Computer"), the Extension discovers which databases are hosted on that server and presents them in the database dropdown menu. Similarly, after the database is selected, the Extension can discover which FlashArray provides storage for that database.

These instructions describe the steps to create the first backup configuration. When subsequent configurations are created, host names and FlashArray names are available in the dropdown menus and credentials do not have to be re-entered.

Notes about the icons on the Backup Configuration dialog:

- The New Credential icon  is used to specify a new SQL Server, FlashArray, or vCenter Server, as well as administrator credentials for that server or array.
- The Edit icon  is used to change an administrator's password or to supply a different administrator account. The Edit icon is used when editing an existing backup configuration, not when creating a new backup configuration.
- The Discover icon  identifies the specific FlashArray that hosts the SQL database in the backup configuration and puts that array name in the FlashArray field.

Notes:

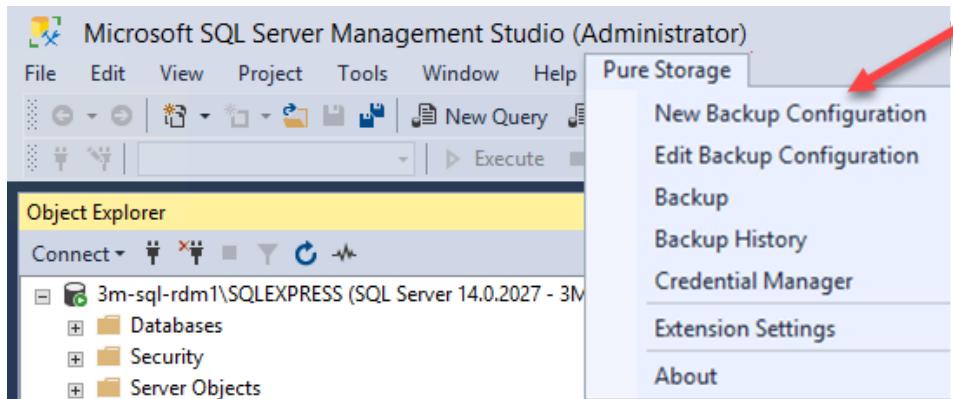
- Discovery may take a few moments.
- The FA SSMS Extension makes its best effort to discover the FlashArray but in some cases cannot do so.
In that case, manually select the FlashArray credential that contains the SQL database files intended for backup.
- The Refresh icon  repopulates the field, bringing in any change made outside of the Backup Configuration window.
- The Tip icon  provides a brief explanation of the field.

To create a new backup configuration:

Note: Enter the Computer, Computer Credential, Database, FlashArray, and FlashArray Credential fields in exactly the order shown in the Backup Configuration dialog.

1. In the SSMS tool bar, select **Pure Storage > New Backup Configuration**.

Figure 4.11:



The Backup Configuration screen opens.

2. In the **Configuration** field, enter a descriptive name for the new configuration.
On-demand backups in the GUI and backup automation scripts will reference this name.
3. In the **Computer** row, specify the SQL Server that hosts the database to be backed up.
If you have configured credentials for the SQL Server in the Credential Manager, enter that credential name in the **Computer** field.
If credentials for the SQL Server host are not already configured:
 - a. Click the **Create a new computer credential**  icon.
 - b. The New Computer Credential dialog opens.
Enter the following information:

Field	Entry
Computer Label	Enter the name of the machine or VM hosting the SQL Server. This name can be the actual machine name or a nickname used only within the Extension.
Address	Enter the fully-qualified domain name or IP address of the machine hosting the SQL Server. For VMs on ESXi using SQL Failover Cluster Instance, this name must be the SQL Server Network Name. Otherwise, the backup will fail if the role is running on another VM in the cluster.
Use credential for current machine	Enable this check box if the Extension is running on the SQL Server host.
Username	Enter an administrator for the machine hosting the SQL Server.

Field	Entry
Password	Enter that administrator's password.

When you save the credentials dialog, the Extension confirms that it can reach the specified SQL Server host with those credentials.

The Extension also discovers the server's SQL databases that are hosted on FlashArrays.

4. Back on the Backup Configuration dialog, select the SQL Server in the Computer dropdown menu.
5. In the **Database** row, select the database to be backed up.
6. In the **FlashArray** row, specify the FlashArray hosting the database.

If you have configured credentials for the FlashArray in the Credential Manager, enter that credential name in the **FlashArray** field.

If credentials for the FlashArray are not already configured:

- a. Click the **Create a new FlashArray credential**  icon.
- b. The New FlashArray Credential dialog opens.

Enter the following information:

Field	Entry
FlashArray Label	Enter the name of the FlashArray hosting the SQL database. This name can be the actual machine name or a nickname used only within the Extension.
Address	Enter the fully-qualified domain name or IP address of the FlashArray hosting the SQL database.
Username	Enter a FlashArray administrator, whose credentials will be used to connect to the array. Array Admin or Storage Admin privileges are required.
Password	Enter that administrator's password.

7. Back on the Backup Configuration dialog, select that FlashArray in the FlashArray dropdown menu.
8. For replication environments, enter the replication target FlashArray in the Remote FlashArray field.
The Remote FlashArray is used during recovery operations. (See [Recovery with ActiveDR Arrays](#).)
9. In the **Volume Type** row, specify the type of volume hosting the SQL database:

Physical

Is physically hosted on the FlashArray.

vVol

Not supported in this release. Do not use. If **vVol** is selected, backups performed with the backup configuration will fail.

We expect to add this support in a future release.

RDM

Is a virtual machine hosted on ESXi and configured in VMware physical raw device mapping (pRDM) mode for datastore.

10. For RDM volume types, specify the vCenter in the **vCenter** row.

If you have configured credentials in the Credential Manager for the machine hosting the vCenter, enter that credential name in the **vCenter** field.

If credentials for the vCenter host are not already configured:

- a. Click the **Create a new vCenter credential**  icon.
- b. The New vCenter Credential dialog opens.

Enter the following information:

Field	Entry
vCenter Label	Enter the name of the vCenter. This name can be the actual vCenter name or a nickname used only within the Extension.
Address	Enter the fully-qualified domain name or IP address of the vCenter.
Username	Enter an administrator for <i>the machine hosting the vCenter</i> .
Password	Enter that administrator's password.

11. If the SQL Server is hosted on a VM, enter its VM Name as configured in vCenter.

12. The Extension will fill in the **VM Persistent ID** field.

If the field is not populated within a short time, click the  refresh icon on the **VM Persistent ID** row.

The FA SSMS Extension uses the VM Persistent ID to connect to the correct VM even if the VM has been renamed in vCenter.

13. The **Metadata Location** field shows the location of the backup metadata files.

Do not change the **Metadata Location** field if any backup has already been made. To do so would make the Extension unable to restore those backups.

Please see the warnings in [Metadata Files](#).

14. In the **Type** field, select the backup type, either **Full** or **Copy only**.

See [Microsoft SQL Server documentation](https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/backup-overview-sql-server) [<https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/backup-overview-sql-server>] for a description of backup types.

15. Click **Save.**

Your backup configuration is available to use. Reference the configuration name entered in the Configuration field at the top of the Backup Configuration dialog.

Edit an Existing Backup Configuration

Refer to [Create a New Backup Configuration](#) for explanations of the fields and instructions.

However, when editing an existing backup configuration, host names and FlashArray names are available in the dropdown menus and credentials do not have to be re-entered.

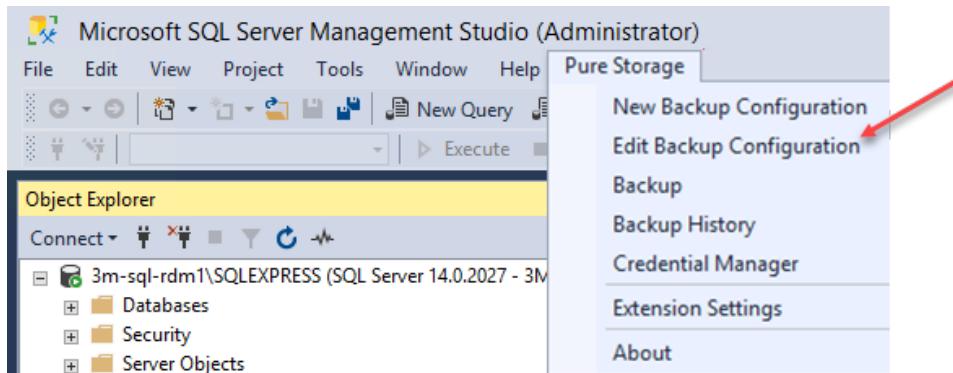
To change an administrator account or password:

1. In the SSMS tool bar, select **Pure Storage > Edit Backup Configuration**.
The Backup Configuration screen opens.
2. To change an administrator or administrator's password, click the  icon in the row for that system.
In the popup, enter the new account information.
3. When you have made your changes, click **Save**.

To edit an existing backup configuration:

1. In the SSMS tool bar, select **Pure Storage > Edit Backup Configuration**.

Figure 4.12:



2. The Backup Configuration screen opens.

If necessary, use the **Configuration** dropdown menu to select the correct backup configuration, and the **Database** dropdown menu to select the correct database.

3. Make the necessary changes.

However, do not change the **Metadata Location** field if any backup has already been made. To do so would make the Extension unable to restore those backups.

Please see the warnings in [Metadata Files](#).

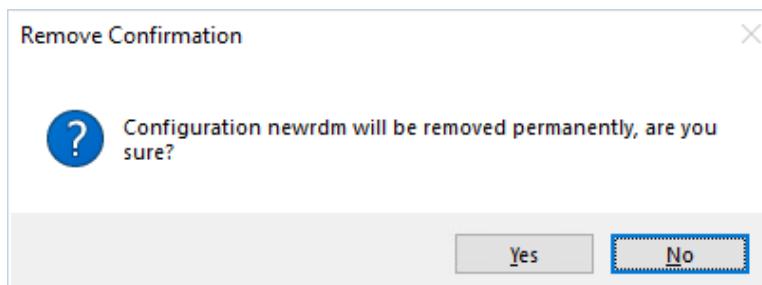
4. When you have made your changes, click **Save**.

Delete a Backup Configuration

To delete an existing backup configuration:

1. In the SSMS tool bar, select **Pure Storage > Edit a Backup Configuration**.
2. In the Edit a Backup Configuration screen, use the Configuration drop-down menu to select the configuration that is to be deleted.
If you are sure the correct configuration is selected, click **Remove**.
3. In the confirmation dialog, click **Pure Storage > Edit a Backup Configuration**.

Figure 4.13:



If you are sure the correct configuration is selected, click **Yes**.

Backups

These sections describe working with backups.

Backup Using an Existing Configuration

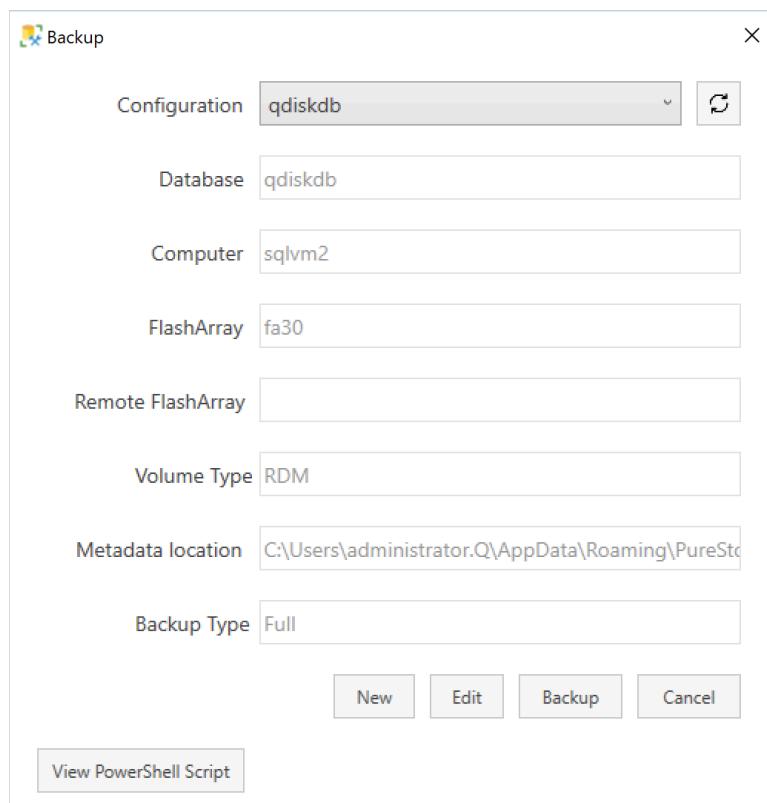
This section describes how to run an on-demand backup.

These steps require that an appropriate named backup configuration has already been created (see [Create a New Backup Configuration](#)).

To perform a backup using an existing configuration:

1. In the SSMS tool bar, select **Pure Storage > Backup**, or in the Object Explorer, select the database to be backed up, right click, and select **Pure Storage > Backup**.
2. The Backup dialog opens.
If necessary, use the **Configuration** dropdown menu to select the correct backup configuration.

Figure 4.14:



3. Confirm that the correct configuration is selected in the Configuration menu.
Then click **Backup** to start the backup.

Use the **New** or **Edit** buttons to create a new backup configuration or to edit the selected backup configuration, if necessary.

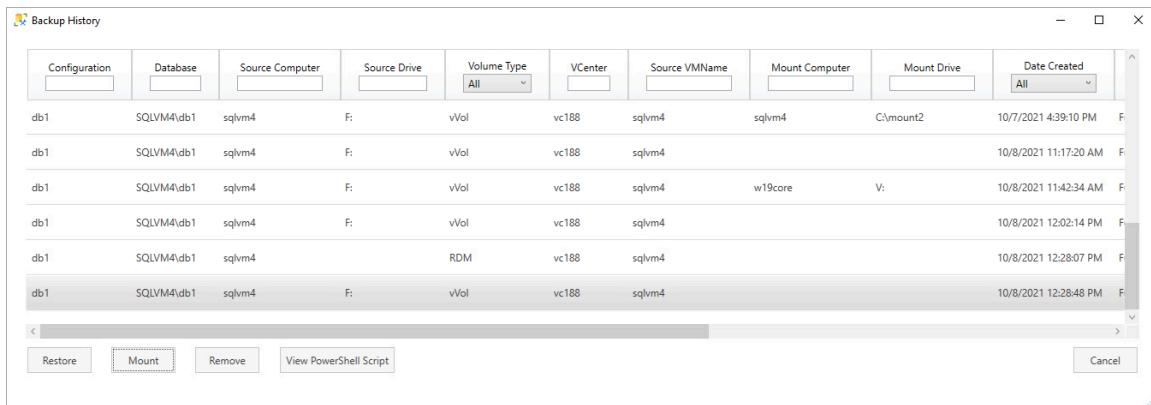
View the Backup History

The backup history lists backups that are available to restore, mount, dismount, or remove.

To view the backup history:

1. In the SSMS tool bar, select **Pure Storage > Backup History**, or in the Object Explorer, select the database to be backed up, right click, and select **Pure Storage > Backup History**.
2. The Backup History listing opens.

Figure 4.15:



Configuration	Database	Source Computer	Source Drive	Volume Type	VCenter	Source VMName	Mount Computer	Mount Drive	Date Created
db1	SQLVM4\dbo1	sqlvm4	F:	vVol	vc188	sqlvm4	sqlvm4	C:\mount2	10/7/2021 4:39:10 PM
db1	SQLVM4\dbo1	sqlvm4	F:	vVol	vc188	sqlvm4			10/8/2021 11:17:20 AM
db1	SQLVM4\dbo1	sqlvm4	F:	vVol	vc188	sqlvm4	w19core	V:	10/8/2021 11:42:34 AM
db1	SQLVM4\dbo1	sqlvm4		RDM	vc188	sqlvm4			10/8/2021 12:02:14 PM
db1	SQLVM4\dbo1	sqlvm4	F:	vVol	vc188	sqlvm4			10/8/2021 12:28:07 PM
db1	SQLVM4\dbo1	sqlvm4	F:	vVol	vc188	sqlvm4			10/8/2021 12:28:48 PM

Notes:

- To search or filter the history, enter a keyword in any of the filter boxes (Configuration, Database, etc.).
- To sort the listing, click a column header.
- Select a specific backup entry to enable the Restore, Mount, and Remove buttons.
Select a mounted backup entry to enable the Dismount button.
- The View PowerShell Script button displays the command to remove the selected backup.
To view the Restore or Mount commands, select that button and complete the dialog, then select View PowerShell Script in Restore or Mount dialog.

See also [Dismount a Backup](#), [Mount a Backup](#), [Remove a Backup History Entry](#), and [Restore a Backup](#).

Restore a Backup

Caution: Be very careful when restoring, that the correct backup is selected. Restoring from an incorrect backup will overwrite data.

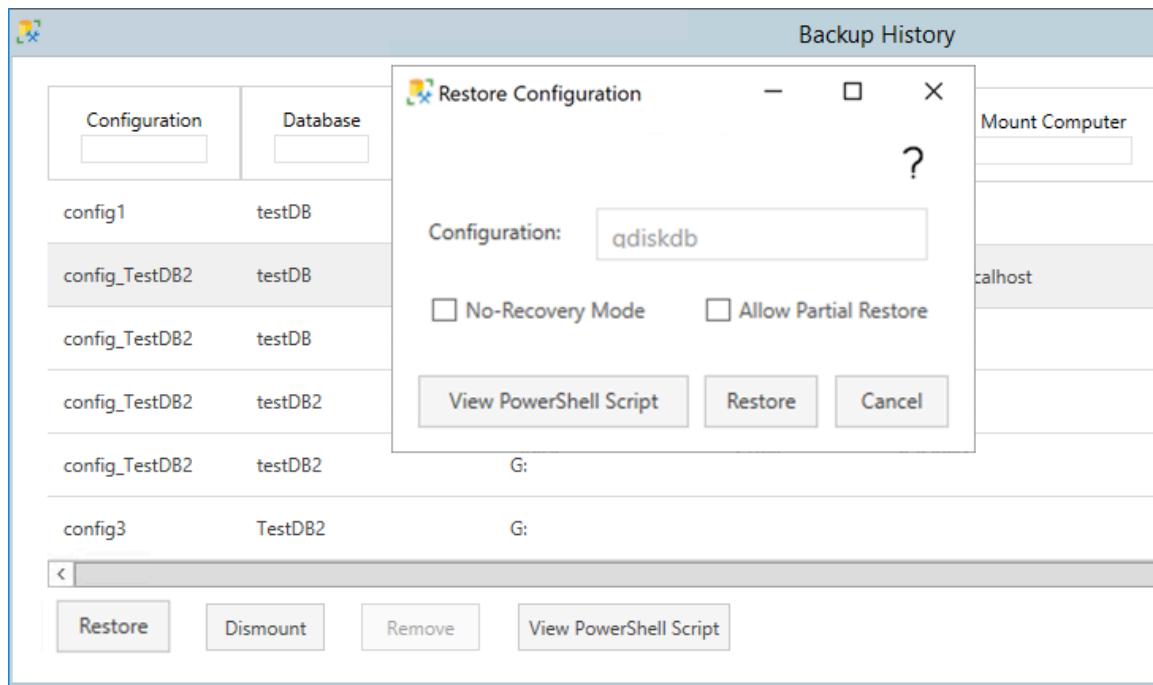
Note: When restoring a SQL Failover Cluster Instance VM, the SQL Role must be online on the VM that is the source computer in the backup history. Otherwise the restore will fail.

To restore from a backup:

1. In the SSMS tool bar, select **Pure Storage > Backup History**, or in the Object Explorer, select the database to be backed up, right click, and select **Pure Storage > Backup History**.
2. If required, search or filter the list to locate the specific backup.
Select the backup and click **Restore**.

The Restore Configuration dialog opens.

Figure 4.16:



3. In the Restore Configuration dialog:

- a. Optionally enable the **No Recovery** check box.

Please see Microsoft SQL Server documentation for the effect of the **No Recovery** option.

- b. Optionally enable the **Allow Partial Restore** check box.

Normally, a restore operation fails if 1 or more of the Pure Storage volumes is missing the snapshot. With the **Allow Partial Restore** box checked, the restore completes on those volumes where the snapshots exist.

If failures occur during an Allow Partial restore, the database will not be online and has to be fixed manually.

- c. To view the equivalent PowerShell command, first complete the Restore Configuration dialog fields, then click **View PowerShell Script** (optional).
- d. Double-check that the correct backup is selected.
If you are sure, click **Restore**.

Mount a Backup

The mount operation imports a backup to the SQL Server machine, where a database administrator can inspect it.

For physical SQL Server machines, mounting is only supported on the same SQL machine that was backed up. For virtual SQL Server machines, mounting is supported only to virtual machines on the same hypervisor machine.

Snapshots from volumes that are part of a pod are mounted inside of that pod.

Notes on SQL Server Failover Cluster Instances:

- A Failover Cluster Instances cannot mount a snapshot with the same disk signature. Such a mount attempt fails.
- As a workaround, mount the snapshot to a server or VM outside of the cluster, then change the disk signature.
- After the disk signature is changed, the snapshot can be manually mounted to the host group, or in the case of VMs, the snapshot can be added as RDM/Existing disk.
- See [Using FlashProtect Snapshots and Cluster Shared Volumes](https://support.purestorage.com/Solutions/Microsoft_Platform_Guide/Failover_Clustering/Using_FlashProtect_Snapshots_and_Cluster_Shared_Volumes) [https://support.purestorage.com/Solutions/Microsoft_Platform_Guide/Failover_Clustering/Using_FlashProtect_Snapshots_and_Cluster_Shared_Volumes] for more information.

To mount a backup:

1. In the SSMS tool bar, select **Pure Storage > Backup History**, or in the Object Explorer, select the database to be backed up, right click, and select **Pure Storage > Backup History**.
If necessary, search or filter the list to locate the specific backup.
2. Select the backup and click **Mount**.
3. Enter the following information in the Mount Drive Selection dialog:

Mount Computer

A friendly name of mount destination computer

Accept the suggestion in the **Mount computer** dropdown menu.

Mount Directory

Path to the mounted database backup on the destination computer

The path can be a drive name (such as D:) or a mount path (such as D:\Database).

Multiple paths are supported, for a database that resides on multiple source drives.

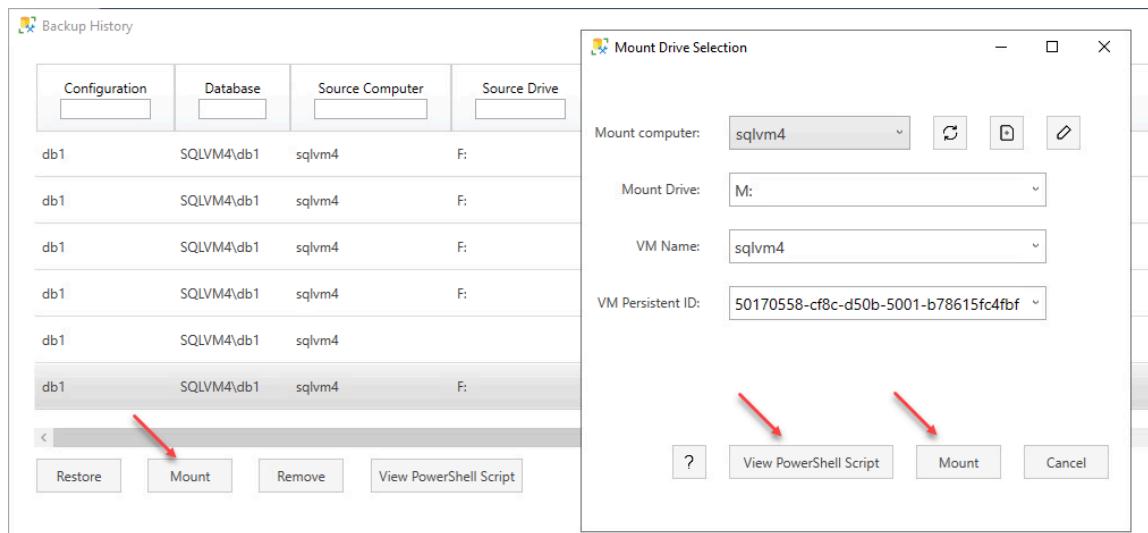
VM Name

For a SQL Server that is running on an ESXi host managed by vCenter, enter the VM Name of that computer in vCenter.

VM Persistent ID

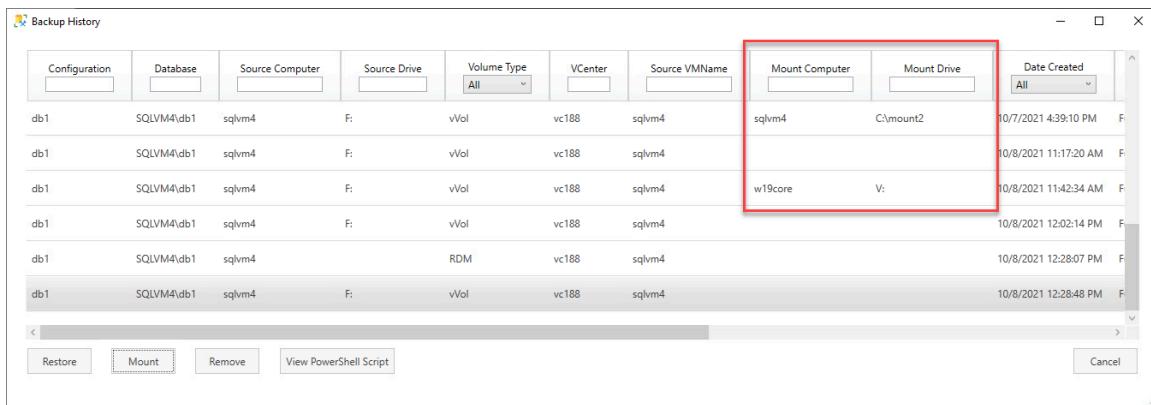
The FA SSMS Extension populates this field.

Figure 4.17:



4. To view the equivalent PowerShell command, first complete the Mount Configuration dialog fields, then click **View PowerShell Script** (optional).
5. Double-check that the correct backup is selected.
If you are sure, click **Mount**.

On success, a completed message is shown and the mount is shown in the Backup History listing, with entries in the **Mount Computer** and **Mount Drive** columns.

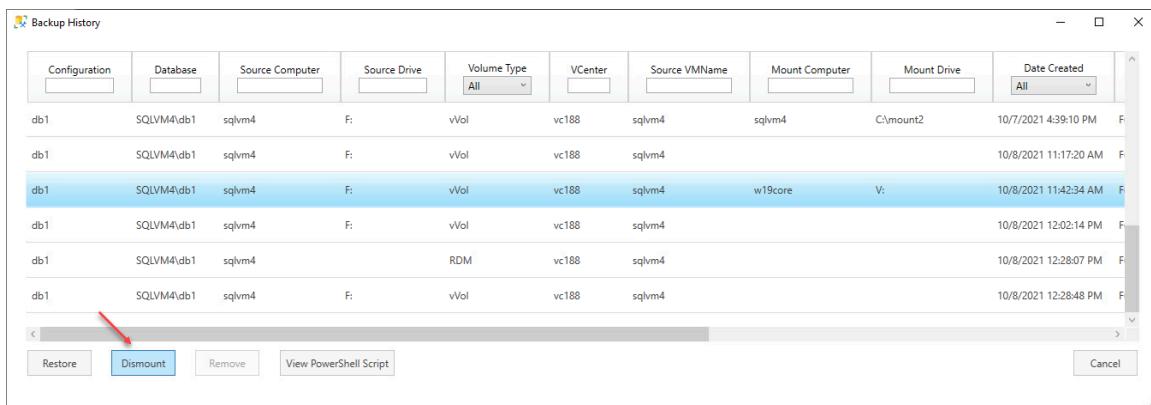
Figure 4.18:


Dismount a Backup

Note: Dismounting a backup completely removes the mount drive and all its content. Any volume copies or other changes made on mounted backups are not persisted once a dismount is performed.

To dismount a backup, specify an existing backup history that is already mounted to a mount destination. The **Dismount** button is only available when a mounted backup is selected.

1. In the SSMS tool bar, select **Pure Storage > Backup History**, or in the Object Explorer, select the database to be backed up, right click, and select **Pure Storage > Backup History**. Search or filter the list to locate the specific backup.
2. Select the correct backup.

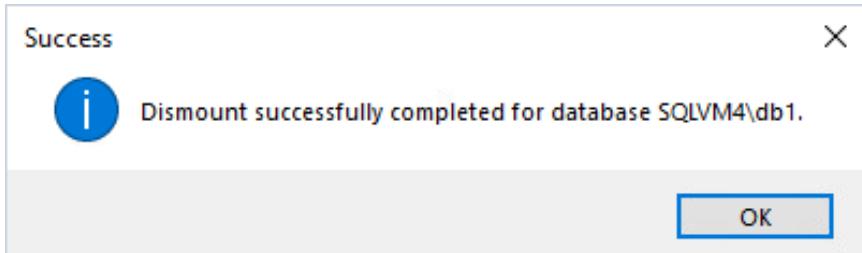
Figure 4.19:


If you are sure the correct backup is selected, click **Dismount**.

The dismount begins immediately, without a confirmation question.

3. A success message is shown and the Mount Computer and Mount Drive information is removed from the Backup History listing.

Figure 4.20:



Remove a Backup History Entry

This section describes removing an entry from the Backup History listing.

Notes:

- When a backup is mounted, its entry cannot be removed.
- The destroy snapshot option only destroys, not eradicates, the backup snapshots.

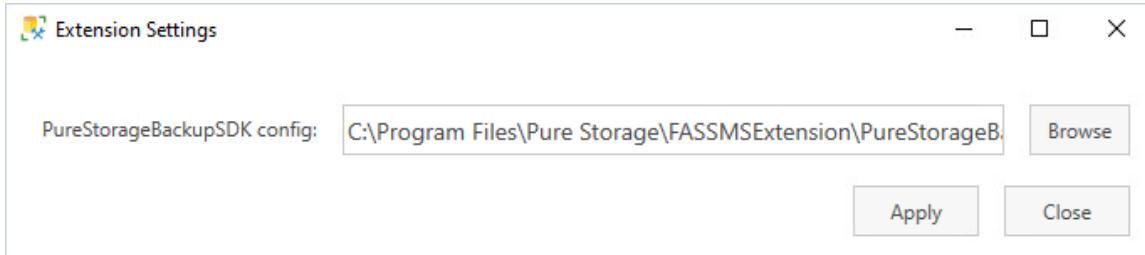
To remove a backup entry:

1. In the SSMS tool bar, select **Pure Storage > Backup History**, or in the Object Explorer, select the database to be backed up, right click, and select **Pure Storage > Backup History**. If necessary, search or filter the list to locate the specific backup.
2. Select the backup and click the **Remove** button.
3. In the confirmation dialog, optionally select the **Destroy Snapshots on FlashArray** check box to also destroy the backup snapshots on the FlashArray.
This option destroys but does not eradicate the snapshots.
4. Click **Remove** in the Remove Backup History Configuration confirmation dialog.

Extension Settings

The Extension Settings dialog shows the location of the Pure Storage Backup SDK. We recommend not changing this field.

Figure 4.21:



Chapter 5. Considerations with FlashArray Replication

Recovery in ActiveCluster Environments

With ActiveCluster configured for synchronous replication, add both FlashArrays to the backup configuration. Then, no matter which FlashArray the SQL Database is live on, snapshots can be taken. Since the FlashArrays are in a synchronous relationship, the snapshots are created on both simultaneously. In the event of an outage, backups can continue to run. Once both FlashArrays return to a healthy state, restore and mount functionality are enabled.

In the configuration:

1. In the Credential Manager, add a credential for the peer FlashArray.
2. In the Backup Configuration, enter the peer FlashArray in the Remote FlashArray field.

For information on ActiveCluster, see the FlashArray User Guide and the Knowledge Base articles at **Knowledge Base ActiveCluster Articles** [<http://support.purestorage.com/FlashArray/PurityFA/Protect/ActiveCluster>]

Recovery with ActiveDR Arrays

ActiveDR with Replication to the DR Site

With ActiveDR, it is common to deploy independent infrastructure in each site, and have the FlashArrays continuously replicate between the sites. If the production site SQL Server host resources have storage fabric access to the DR site and then the production FlashArray has an outage, the production SQL Server host resources can connect to the DR FlashArray and manipulate prior snapshots.

In the configuration:

1. In the Credential Manager, add a credential for the DR FlashArray.
2. In the Backup Configuration, enter the DR FlashArray in the Remote FlashArray field.

ActiveDR with Independent Sites

The most common deployment scenario for ActiveDR involves the FlashArray and SQL Server in the DR site being independent from the FlashArray and SQL Server in the production site. In this scenario, the FA SSMS Extension can create volume or protection group snapshots in production, and these snapshots will be continuously replicated to the DR FlashArray. In the event of a failure, the FA SSMS Extension in the production site cannot be used to manipulate snapshots that were replicated to the DR site. Any manipulation of older snapshots has to be handled through the FlashArray UI or the Pure Storage PowerShell SDK. If the DR site will run the production workload for an extended period of time, a new FA SSMS Extension can be configured in the DR site to take future snapshots, which can be mounted or restored in the DR Site.

To recover:

1. First promote the pod.
In most cases, promoting the pod is sufficient.
2. If restoring the DR snapshots is required, use the PowerShell SDK or the Purity//FA GUI (the FlashArray management GUI).

For information on ActiveDR, see the FlashArray User Guide and the Knowledge Base articles at **Knowledge Base ActiveDR Articles** [<http://support.purestorage.com/FlashArray/PurityFA/Protect/ActiveDR>].

Chapter 6. The Pure Storage PowerShell Backup SDK

SDK Overview

Pure Storage® provides the PowerShell Backup SDK to perform and automate operations supported by the Pure Storage FA SSMS Extension, including creating SQL backups and restoring from backups.

The SDK orchestrates the work flow required for database backup, restore, mount, and dismount for Microsoft SQL Servers.

The Backup SDK connects the SQL Server™ host and FlashArray™ (FA) connected to the SQL Server host and orchestrates the required operations needed to backup, restore, mount, and dismount.

Installation and Import

The PowerShell Backup SDK is installed during the FA SSMS Extension installation. Its default location is:

```
%PROGRAMFILES%\Pure Storage\FASSMSExtension\PureStorageBackupSDK
```

In order to use the Backup SDK, open the Windows PowerShell app, select Run as Administrator, and run the following PowerShell command from the install directory:

```
Import-Module -Name PureStorageBackupSDK
```

Cmdlets List, Cmdlets Help, and Cmdlet Equivalents

The following PowerShell command lists the available cmdlets:

```
Get-Command -Module PureStorageBackupSDK
```

The output is:

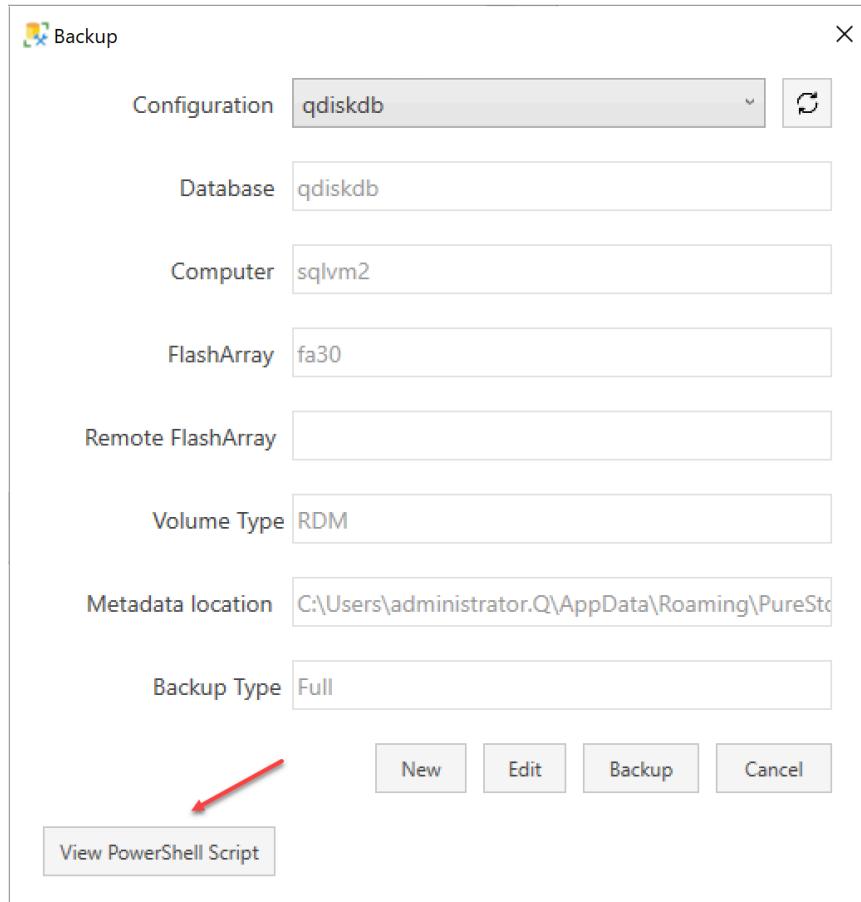
CommandType	Name	Version	Source
-----	-----	-----	-----
Function	Add-PfaBackupCred	2.0.433	PureStorageBackupSDK
Function	Add-PfaBackupJob	2.0.433	PureStorageBackupSDK
Function	Connect-PfaVMHardDisk	2.0.433	PureStorageBackupSDK
Function	Dismount-PfaDrive	2.0.433	PureStorageBackupSDK
Function	Get-AvailableVM	2.0.433	PureStorageBackupSDK
Function	Get-ESXiDetails	2.0.433	PureStorageBackupSDK
Function	Get-PfaAvailableDBNames	2.0.433	PureStorageBackupSDK
Function	Get-PfaBackupAvailableDrives	2.0.433	PureStorageBackupSDK
Function	Get-PfaBackupCred	2.0.433	PureStorageBackupSDK
Function	Get-PfaBackupCredList	2.0.433	PureStorageBackupSDK
Function	Get-PfaBackupHistory	2.0.433	PureStorageBackupSDK

Function	Get-PfaBackupJobs	2.0.433	PureStorageBackupSDK
Function	Get-PfaBackupSnapshot	2.0.433	PureStorageBackupSDK
Function	Get-PfaConnectedFlashArray	2.0.433	PureStorageBackupSDK
Function	Get-PfaVerboseDiskInfo	2.0.433	PureStorageBackupSDK
Function	Get-PfaVMPersistentId	2.0.433	PureStorageBackupSDK
Function	Get-PfaVSSInstallerVersion	2.0.433	PureStorageBackupSDK
Function	Get-PfaVSSProvider	2.0.433	PureStorageBackupSDK
Function	Get-PfaVSSVersion	2.0.433	PureStorageBackupSDK
Function	Install-VSS	2.0.433	PureStorageBackupSDK
Function	Invoke-PfaBackupJob	2.0.433	PureStorageBackupSDK
Function	Mount-PfaBackupJob	2.0.433	PureStorageBackupSDK
Function	Register-PfaVSSProvider	2.0.433	PureStorageBackupSDK
Function	Remove-PfaBackupCred	2.0.433	PureStorageBackupSDK
Function	Remove-PfaBackupHistory	2.0.433	PureStorageBackupSDK
Function	Remove-PfaBackupJob	2.0.433	PureStorageBackupSDK
Function	Remove-PfaVMHardDisk	2.0.433	PureStorageBackupSDK
Function	Restore-PfaBackupJob	2.0.433	PureStorageBackupSDK
Function	Test-PfaBackupCred	2.0.433	PureStorageBackupSDK
Function	Test-PfaVSSProvider	2.0.433	PureStorageBackupSDK
Function	Test-PfaVSSVersion	2.0.433	PureStorageBackupSDK

Use the `Get-Help` command for a detailed explanation of each cmdlet:

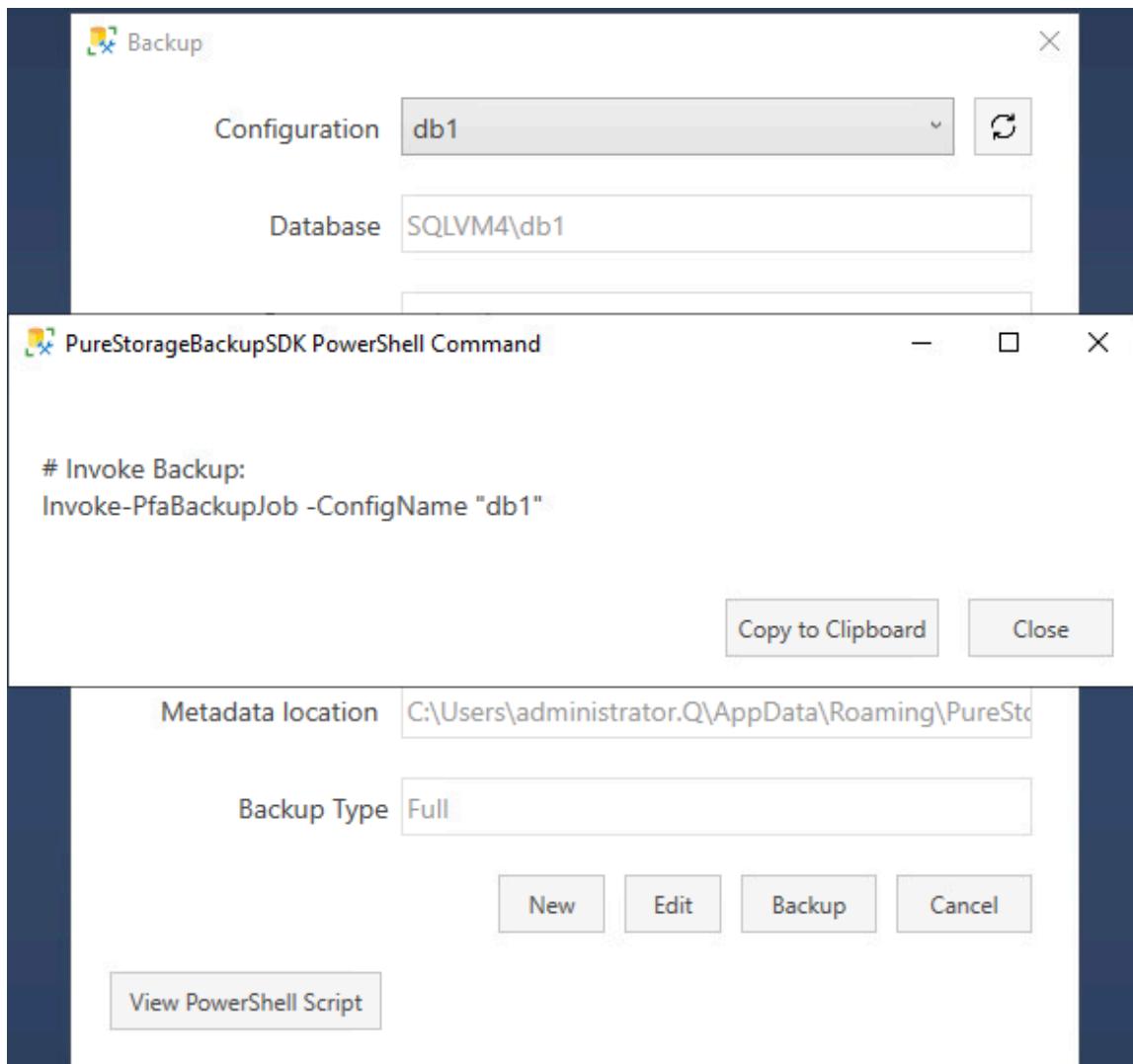
```
Get-Help <cmdlet> -Detailed
```

The FA SSMS Extension GUI provides a **PowerShell Script** that lists the Backup SDK cmdlets equivalent to the operations provided in the GUI. For example:

Figure 6.1:

The equivalent Backup SDK cmdlets are displayed in a pop-up. For example:

Figure 6.2:



In the Backup History dialog, the **PowerShell Script** provides the cmdlet equivalent for the Remove button. To see the cmdlet equivalents for the Restore and Mount buttons, click them and complete the subsequent popups, then click the **PowerShell Script** on the completed popup.

Using the PowerShell Backup SDK Cmdlets

The following are examples of typical tasks performed with SDK cmdlets:

1. [Adding SQL Server Host Computer Credential](#)
2. [Adding FlashArray Credentials](#)
3. [Adding VMware vCenter Credentials](#)
4. [Creating a Backup Job Configuration](#)
5. [Invoking a Backup Job Configuration](#)

6. [*Listing Backup Job Configurations*](#)
7. [*Retrieving a Historical Backup*](#)
8. [*Restoring a Database from a Snapshot*](#)
9. [*Mounting a Backup Snapshot*](#)
10. [*Dismounting a Mounted Drive*](#)
11. [*Removing an Entry from the Backup History*](#)

You need to input the SQL Server host computer credentials and the Pure Storage FlashArray credentials when creating a backup configuration.

Adding SQL Server Host Computer Credential

Enter the following command (all on one line):

```
Add-PfaBackupCred -CredentialName "mySqlServer" -Address <sql-server-name>
-CredentialType Windows -Credential (Get-Credential)
```

CredentialName is a friendly name to identify the Windows server.

Use **Get-PfaBackupCred** to check the credential that is added into the Pure Storage Backup SDK:

```
Get-PfaBackupCred -CredentialName mySqlServer -CredentialType Windows
```

As part of adding the credential to the Pure Storage Backup SDK, we do ensure that the server is alive and the credentials are accurate. This is also true when adding credentials for FlashArray and vCenter below.

If there is an issue, the cmdlet throws an exception.

Please ensure that the server is connected via network to this client machine where the credentials are being added and that the PowerShell remoting is enabled and operational.

The credentials are stored in the client computer at the following location:

```
%PROGRAMDATA%\PureStorage\PureStorageBackupSDK\<username>\
```

Adding FlashArray Credentials

Enter the following command (all on one line):

```
Add-PfaBackupCred -CredentialName "myFlashArray" -Address <flasharray-name>
-CredentialType FlashArray -Credential (Get-Credential)
```

CredentialName is a friendly name to identify the FlashArray.

Use **Get-PfaBackupCred** to check the credential that is added into PureStorage Backup SDK.

```
Get-PfaBackupCred -CredentialName myFlashArray -CredentialType FlashArray
```

The credentials are stored in the client computer at the following location:

```
%PROGRAMDATA%\PureStorage\PureStorageBackupSDK\<username>\
```

Adding VMware vCenter Credentials

If the SQL Server host computer is a VMware virtual machine hosted on ESXi and the backing datastore is configured as RDM (raw device mapping), vCenter credentials are required to configure the ESXi host to update the backing datastore.

Enter the following command (all on one line):

```
Add-PfaBackupCred -CredentialName myVCenter -CredentialType vCenter -Address <vcenter-machine-name> -Credential (Get-Credential)
```

The credentials are stored in the client computer at the following location:

```
%PROGRAMDATA%\PureStorage\PureStorageBackupSDK\<username>\
```

Creating a Backup Job Configuration

We define a backup job that encompasses the details required to perform a backup. The configuration includes the SQL Server host computer name, the SQL Server instance name, and the database name.

If the SQL Server host is a virtual machine configured as RDM, then the vCenterName and VMName are also included.

```
Add-PfaBackupJob -ConfigName "myTestBackupConfig" -ComputerName "mySqlServer" -FAName "myFlashArray" -Component testDB
```

Use the following command to define a backup job configuration for a SQL Server host computer that is a virtual machine configured as RDM:

```
Add-PfaBackupJob -ConfigName "myTestBackupConfig" -ComputerName "mySqlServer" -FAName "myFlashArray" -VCenterName "myVCenter" -VMName "virtualMachineName" -Component testDB
```

Notes:

- It is mandatory to add the correct FlashArray details when creating a backup job configuration. Adding a FlashArray that is not the backing storage for the SQL Server host will interfere with backup, restore, and mount commands.
- The **ComputerName** and **FAName** here are the friendlyName configured in the **Add-PfaBackupCred** as **CredentialName**.

This helper function identifies the FlashArray corresponding to a SQL Server database. This takes the list of FlashArray friendly names previously configured using **Add-PfaBackupCred**. This command returns the FlashArray that corresponds to this database.

```
Get-PfaConnectedFlashArray -ComputerName mySqlServer -FAName myFlashArray,correctFlashArray -DBName testDB
```

Important: All database-related files for the above-mentioned component **testDB** must reside on the Pure Storage FlashArray disks.

Invoking a Backup Job Configuration

The command to take a backup uses the friendly configuration name given when the configuration was created.

Run the following command to perform a backup:

```
Invoke-PfaBackupJob -ConfigName "myTestBackupConfig"
```

This creates a Pure Storage snapshot on the FlashArray for the volume corresponding to the database specified in the backup job configuration.

Note that the database may belong to multiple disk drives on SQL Server host computer, in which case each disk drive corresponds to a FlashArray volume (also known as a FlashArray LUN).

When a backup is performed, a snapshot is taken of all volumes. The Pure Storage Backup SDK orchestrates between the client computer where the Backup SDK is installed and the SQL Server host computer (and vCenter and VM, if virtual) and FlashArray to create the snapshot. The metadata associated with this snapshot is created by the Pure Storage VSS Hardware Provider running on the SQL Server host computer.

This metadata is copied to the SSMS computer and stored in the default location of `C:\Users\<username>\AppData\Roaming\`.

You can override the path at which the metadata file is copied using the `-MetadataDir` argument to the `Add-PfaBackupJob` cmdlet.

This metadata file is important as it is required for a restore or a mount of the snapshot. If a backup's metadata file is not provided for a restore, the restore operation fails.

The result of invoking a backup job is stored in the `history.json` file, located at `%PROGRAMDATA%\PureStorage\PureStorageBackupSDK\<username>\history.json`.

Listing Backup Job Configurations

The `Get-PfaBackupJobs` command lists the existing backup configurations.

This example shows two backup configurations, `config1` and `config2`.

```
Get-PfaBackupJobs

ConfigName      : config1
ComputerName    : localhost
FAName         : vss-purity-vm
vCenterName    :
VMName         :
Component      : testDB
Path           :
CopyOnly       : False
Metadata       :
MetadataDir    : C:\Users\Administrator\AppData\Roaming
MetadataOverwrite : False
```

```

ConfigName      : config2
ComputerName    : localhost
FAName          : vss-purity-vm
vCenterName     :
VMName          :
Component       : testDB
Path             :
CopyOnly         : True
Metadata         :
MetadataDir     : C:\Users\Administrator\AppData\Roaming
MetadataOverwrite : False

```

Retrieving a Historical Backup

The `Get-PfaBackupHistory` command lists backup history.

```

Get-PfaBackupHistory

HistoryId : 0
ConfigName : myTestBackupConfig
Path : E:
Component : testDB
Metadata : Metadata_SQL-RDM_20190930141943
MetadataDir : C:\Users\Administrator\AppData\Roaming\
MetadataFullPath : C:\Users\Administrator\AppData\Roaming\Metadata_SQL-RDM_20200...
Status : Succeeded
TimeCreated : 09/30/2019 14:19:45
BackupType : Full
ComputerName : mySqlServer
FAName : myFlashArray
VCenterName : myVCenter
VMName : sql-rdm
MountComputer :
MountDrive :

```

Each invocation of the backup job using `Invoke-BackupJob` creates an entry into the backup history file. Each entry has a unique `HistoryId` and corresponding `Status` denoting Successful/Failed.

If the snapshot is successful, the `HistoryId` can be used to restore the database to that instance of the data.

Restoring a Database from a Snapshot

The `Restore-PfaBackupJob` cmdlet restores a database. First run the following cmdlet to determine the `HistoryId` of the appropriate backup:

```
Get-PfaBackupHistory | Format-Table AutoSize
```

Run the following cmdlet to restore the database to the point of the snapshot:

```
Restore-PfaBackupJob -HistoryId 0
```

With **-AllowPartial**, a restore operation does not fail if a volume is missing its snapshot. Instead, the restore completes on those volumes for which a snapshot exists.

```
Restore-PfaBackupJob -HistoryId 0 -AllowPartial
```

Using **-NoRecovery**, the database is restored in no recovery mode.

```
Restore-PfaBackupJob -HistoryId 0 -NoRecovery
```

The restore operation causes all changes since the point the backup was made to be lost.

Mounting a Backup Snapshot

The **Mount-PfaBackupJob** command mounts a backup snapshot onto one or more Windows drive letters or mount points.

Example command:

```
Mount-PfaBackupJob -HistoryId 0 -DriveLetter "E:"
```

Replace "E:" with a valid available drive letter.

Multiple drives are supported, if the source involves multiple drives. Separate multiple drive letters with a comma (no spaces) and enclose them with double quotes. For example: "**E: ,F:**".

Use **-MountComputer** <computer credential name> of the computer where you want to mount the snapshot. If this argument is not used, then we mount on the SQL Server host computer where the database belongs.

Use **-MountVMPersistentID** to use the PersistentId (also referred to as the InstanceUuid or MoRef) of the virtual machine.

Use **-MountVMName** if the **-MountComputer** is a virtual machine hosted on ESXi. **MountVMName** is the credential name of the VM previously configured using **Add-PfaBackupCred**.

The **Mount-PfaBackupJob** argument creates a new drive on the MountComputer or SQL Server host with the copy of the data at the point of snapshot taken with HistoryId 0.

The result of the mounted drive letter and whether it was successful is stored in the history configuration.

Dismounting a Mounted Drive

Dismounts a database snapshot from an existing mounted drive.

```
Dismount-PfaDrive -HistoryId 0
```

The history configuration identifies the drive letter that mounted the HistoryId 0 and the mount computer. This information is used to dismount.

Removing an Entry from the Backup History

Removes an entry from the backup history, without deleting the backup snapshots.

```
Remove-PfaBackupHistory -HistoryId 0
```

Removes an entry from the backup history and also deletes the backup snapshots.

```
Remove-PfaBackupHistory -HistoryId 0 -DeleteSnapshot
```

The **-All** option removes *all* entries from the backup history.

Removes the entire backup history, without deleting the backup snapshots.

```
Remove-PfaBackupHistory -All
```

Removes the entire backup history and also deletes the backup snapshots.

```
Remove-PfaBackupHistory -All -DeleteSnapshot
```

Utility Cmdlets

Install-VSS

This cmdlet installs the VSS Hardware Provider on the SQL Server host computer.

Use **-ForceUpgrade** to upgrade or reinstall VSS.

Get-AvailableVM

This cmdlet returns the virtual machine names managed by specified vCenter that match the specified SQL Server.

Get-ESXiDetails

This cmdlet returns the ESXi that hosts the specified VM name.

Get-PfaAvailableDBNames

This cmdlet finds databases that exist on the SQL Server host computer.

Connect-PfaVMHardDisk

This cmdlet can be used to connect a volume (given a volume serial number) to a virtual machine computer that is hosted on ESXi using raw device mapping (RDM).

Note: The ESXi should be connected to the FlashArray using RDM configuration.

Example:

```
Connect-PfaVMHardDisk -VolumeSerial AC02BDF1FF54147900012197 -VMName sql-rdm  
-VCenterName test-vcenter
```

Remove-PfaVMHardDisk

This cmdlet disconnects a volume from a virtual machine computer that is hosted on an ESXi using raw device mapping (RDM) configuration.

Get-PfaBackupAvailableDrives

This cmdlet gets a list of available drive letters on the SQL Server host computer.

Get-PfaBackupCredList

This cmdlet gets the credential list for a vCenter, FlashArray, or Windows machine.

Remove-PfaBackupCred

This cmdlet removes a credential from the Extension's list of known credentials.

Remove-PfaBackupHistory

This cmdlet removes an entry from the backup history list or deletes all entries from the backup history list.

Remove-PfaBackupJob

This cmdlet removes a backup configuration or deletes all backup configurations.

Get-PfaConnectedFlashArray

This cmdlet identifies the connected FlashArray to a SQL Server host computer. This cmdlet takes a list of FlashArray credential names (the credential names previously configured using **Add-PfaBackupCred**).

Get-PfaVSSInstallerVersion

This cmdlet identifies the VSS Hardware Provider version number on the SQL Server host computer.

PowerShell TroubleShooting

Debug logs on the client and server machines are stored at %PROGRAMDATA%\PureStorage\.

Client Machine Logs

This log contains the Pure Storage Backup SDK debug messages that are crucial to understanding a failure:

```
<username>_PureStorageBackupSDK.log
```

SQL Server Host Computer Logs

The following log files are stored on the SQL Server host computer and are crucial in debugging:

```
PureSQLSnap.log
```

PureVSSHardwareProvider.log

Error Messages Related to TrustedHosts Issues

Error messages similar to the following indicate that the remote SQL Server has not been added to your local TrustedHosts list:

```
The running command stopped because the preference variable "ErrorActionPreference"
or common parameter is set to Stop: [10.01.01.01] Connecting to remote server
10.01.01.01 failed with the following error message : The WinRM client cannot
process the request.

Default authentication may be used with an IP address under the following conditions:
the transport is HTTPS or the destination is in the TrustedHosts list, and explicit
credentials are provided.

Use winrm.cmd to configure TrustedHosts.

Note that computers in the TrustedHosts list might not be authenticated.

For more information on how to set TrustedHosts run the following command:
winrm help config.

For more information, see the about_Remote_Troubleshooting Help topic.
```

Appendix A. Example of Configuring a Database Hosted on a FlashArray Volume

This section describes how to configure a SQL Server database that is hosted on a FlashArray volume. This example shows configuration with an iSCSI initiator. However, both Fibre Channel and iSCSI are supported.

1. **On the FlashArray, create a host for the SQL database:**

- a. First, find a port on the SQL Server host.

On the SQL Server, in PowerShell run `Get-InitiatorPort`.

Figure 29:

```
PS C:\Users\admin> Get-InitiatorPort
InstanceName          NodeAddress          PortAddress      ConnectionType
-----              -----
ROOT\ISCSIPRT\0000_0  iqn.vsstest.com:test1 ISCSI ANY PORT iSCSI

PS C:\Users\admin>
```

- b. Copy the text under `NodeAddress`.

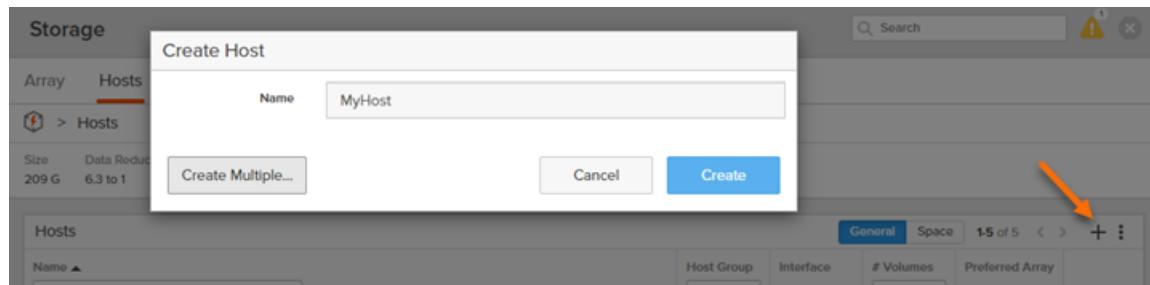
(The `NodeAddress` is `iqn.vsstest.com:test1` in this example.)

2. **Create a host on the FlashArray:**

- a. On the FlashArray, go to **Storage > Hosts**.

Click the plus icon `+` to create a new host.

Figure 30:



- b. Give the host a name and click **Create**.

- c. Click on the newly created host.

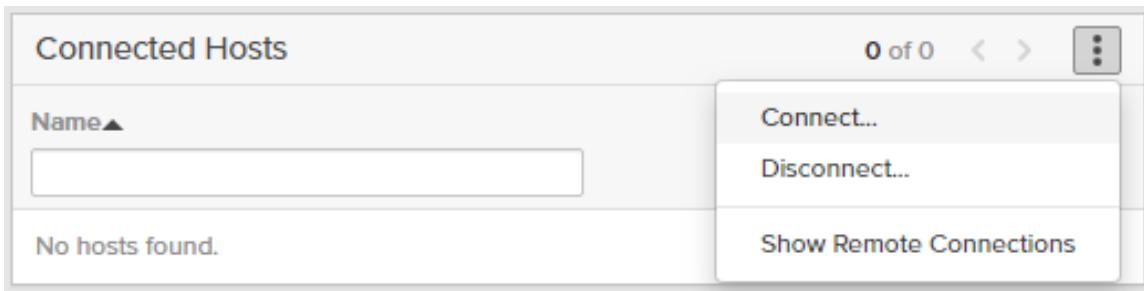
Under Host Ports, select **Configure IQNs**.

Figure 31:


Enter the **NodeAddress** from the PowerShell step above.

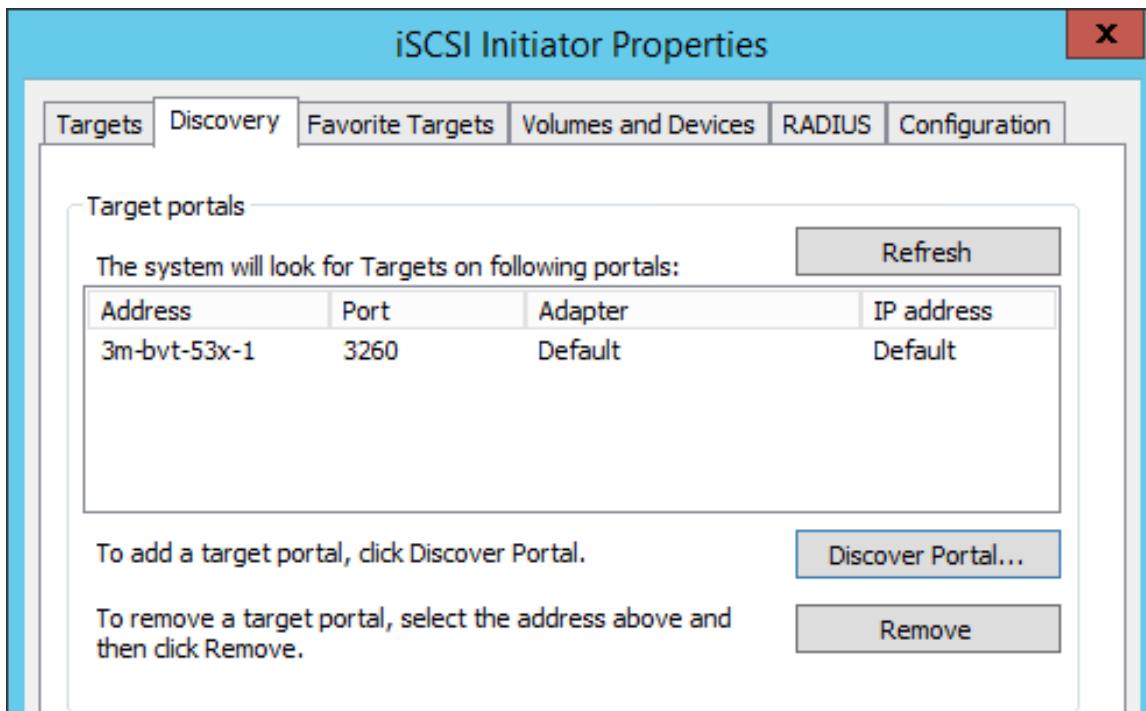
3. Create a volume on the FlashArray:

- On the FlashArray, go to **Storage > Volumes**
 Click the plus icon + to create a new volume.
- Click on the newly created volume.
- In the Connected Hosts pane, connect the host you created above.

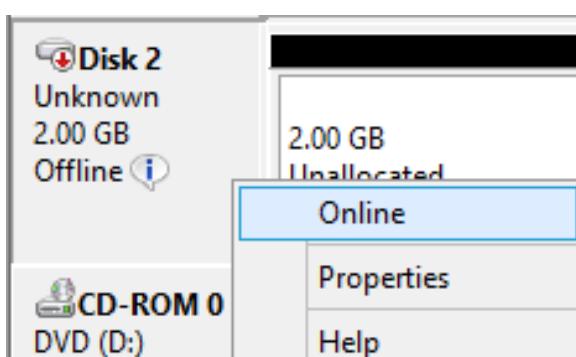
Figure 32:


4. On the SQL Server, connect to the FlashArray:

- On the SQL Server, run **ISCSI Initiator**.
- Under Discovery, click **Discover Portal**.

Figure 33:


- c. Enter the hostname of the FlashArray
 - d. In iSCSI Initiator, under Targets, click **Connect**.
5. **Create a volume on the SQL Server:**
- a. Go to **Disk Management**.
 - b. Select the new volume, right click it, and bring it online.

Figure 34:


- c. Right click again and click **Initialize Disk**.
- d. Right click in the partition space and create a new volume.
- e. Format the new volume.

6. Create the new database on the Pure Volume on the SQL Server:

- a. In Microsoft SQL Server Management Studio, right-click on **Databases > New Database**.
- b. Edit the path of the new database to be on the newly-created volume on the FlashArray.

Appendix B. Troubleshooting

Issue: Attach Database Failed

Objective

To recover from an operation that results in media being write-protected, making its volumes and file systems appear as read only. To be able to copy a snapshot and mount its database.

Recovery Process Using the FlashArray SSMS Extension

If the disaster recovery (DR) FlashArray is available to the primary computer resources (the server hosting Microsoft SSMS), the FA SSMS Extension can manage the DR snapshots for a recovery, in the event the primary FlashArray experiences a failure.

To recover using the FlashArray SSMS Extension:

1. Take a VSS backup.
2. Open the Backup History and mount the snapshot on the appropriate SQL instance.
3. Attach to the database.

Recovery Process Not Using the FA SSMS Extension

If the VSS snapshot is the source for a new or overwritten volume, before the database can be attached and brought online, the following flags must be removed from the Windows partition: **readonly**, **shadowcopy**, and **hidden**.

In order to attach the database:

1. Open DiskPart.
2. List and then select the disk.
3. List and then select the partition.
4. List the partition attributes with: **attribute volume**
5. Clear readonly with: **attribute volume clear readonly**
6. Clear shadowcopy with: **attribute volume clear shadowcopy**
7. Clear hidden with: **attribute volume clear hidden**
8. List the partition attributes with: **attribute volume**

After clearing the flags, the partition will be writable and the database can be attached and brought online.

Issue: Connecting to the Remote Server Failed

Symptoms

Adding a computer to a backup configuration receives the following error:

```
Connecting to the remote server failed with the following error message:  
WinRM cannot process the request
```

The error is also seen in the following scenarios:

- When manually attempting to open a remote PowerShell session to the localhost.
- When attempting to add the local server where the SSMS extension is installed.

Cause

The server time is off by more than 5 minutes from the domain controller.

Resolution

Ensure the domain controllers and the SQL Servers are in sync with the same NTP server.

Issue: Backup Output Error

Some of the database files are not on the backup drives.

Symptoms

Backup fails with an error: `Some of the database files are not on the backup drives.`

Cause

The database named in the backup configuration determines which drives are part of the backup set. All drives that contain any of the database files (all MDF, NDF, LDF, and custom extensions files) are part of the backup set.

However, the SQL Writer queries all disks in the backup set for other SQL databases. If another database also has any files on those backup drives, this failure is seen if that second database has any files outside of the backup set.

Resolution

Either move other databases off the drives that are part of the backup set, to other Pure drives, or move the offending files that are outside of the backup set, to drives that are part of the backup set.

Additional Information

This is SQL Server VSS writer behavior. Databases do not need to be isolated. However, all databases must be entirely on the drives that are part of the backup set.

Issue: Creating a Backup Configuration Times Out

Symptom

Time outs are seen when creating a backup configuration or when performing a backup.

Recommendations

- Use the Credential Manager and verify each credential before configuring or performing backups.
- Check that you can ping the FlashArray.
- Login to the FlashArray and check the network.
- Ensure the correct management IP is used, preferably the virtual management IP.

Issue: Permissions Errors

New Administrators

New FA SSMS Extension administrators need the following memberships:

- Need to be added to the SQL instance as an admin.
- Need to be added to the local server Administrators Group.

Permissions Errors

- Error message:

```
Error: Exception calling "Protect" with "3" argument(s): "The requested operation cannot be completed. The computer must be trusted for delegation and the current user account must be configured to allow delegation."
```

If you have entered a remote PowerShell session and try to add a FlashArray or Windows credential for the first time, adding the credential fails. Run the first config while logged in locally to the SSMS Server or use RDP.

- Error message:

```
Error: [Invoke-TestAndInstallVSSProvider]:Connecting to remote server localhost failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.
```

If you have entered a remote PowerShell session and try to run the cmdlet `add-pfabackupjob` for the first time, the operation will check for the VSS provider and fail. Run the first config while logged in locally to the SSMS Server or use RDP.

- Error message:

```
Error: New-PSSession : [localhost] Connecting to remote server localhost failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.
```

When logged in interactively through KVM or RDP, you see the above error when attempting to create a new configuration. Open a new PowerShell window by right clicking and selecting **Run as Administrator**.

Issue: VSS PureProvider service is not compatible

VSS PureProvider service is not compatible. Use Install-VSS to install.

Symptom

When attempting to backup a database for the first time on a server, the backup fails because the VSS Provider is not installed or is an older version lower than 1.7.

Resolution

Use the **Configure Target** feature of the [Manage Credentials](#) to update the VSS Provider on SSMS machines.

Issue: VSS_E_NOT_SUPPORTED Error

Symptoms

The following error is seen:

```
ERROR: one or more backup volumes not supported by the Pure VSS hardware provider.
```

```
ERROR: VSS_E_NOT_SUPPORTED
```

Cause

The Pure Hardware Provider only supports physical RDM on VMs in vSphere and physical disks that are directly exposed to the operating system.

For example, FC or iSCSI LUNs connected to HBAs on a server, or iSCSI initiator directly connecting to the FlashArray from a VM.

Virtual hard disks are not supported (VMDK/VHDX), nor are virtual RDMs on vSphere.

To Resolve or Avoid the Error

Ensure that all of the database files, log and database, are placed on physical disks or pRDM disks.

Additional Information

See the user guide in the download package for each release for more details. The download package available in the [GitHub repository](#) [<https://github.com/PureStorage-Connect/FlashArray-SQLServer-SSMS-Extension/releases/>]

Issue: VMware PowerCLI Error log4net.dll Missing

Symptoms

An error mentioning `log4net.dll` is seen with the following import command, even though the file `log4net.dll` is present at that location.

```
import-module vmware.vimautomation.core
import-module : Could not load file or assembly 'file:///c:\Program
Files\WindowsPowerShell\Modules\VMware.VimAutomation.Sdk\net45\log4net.dll' or one
of its dependencies. Operation is not supported.
```

Background

VMware PowerCLI is a prerequisite for the FA SSMS Extension.

Attempts to run an Extension command that depends on PowerCLI get an error if PowerCLI is not installed correctly.

Resolution

1. Remove all `VMware*` folders under `C:\Program Files\WindowsPowerShell\Modules`.
2. First, attempt to manually import the module, with either of the following methods:
 - The PowerShell command `Install-Module -Name VMware.PowerCLI`
OR,
 - Manually download and extract the zip file:
 - a. Download the latest zip file from [VMware PowerCLI](https://code.vmware.com/web/tool/12.4/vmware-powercli) [<https://code.vmware.com/web/tool/12.4/vmware-powercli>].
 - b. Using a third-party extraction tool, extract the zipped files to `c:\Program Files\windowspowershell\modules`.
We have verified extraction with [7-Zip](https://www.7-zip.org/) [<https://www.7-zip.org/>].
Do not use Windows Explorer extraction for this zip file.

- c. Retry the `import-module vmware.vimautomation.core` command.

Appendix C. Resources

Links are subject to change without notice.

Pure Storage Documentation

The following Purity resources are available at [**Pure Technical Services**](#) [<http://support.purestorage.com>] (registration and login are required).

Pure Storage solutions for the Microsoft platform:

- [**Pure Storage FlashArray Management Extension for Microsoft SQL Server Management Studio Release Notes**](#) [https://support.purestorage.com/Solutions/Microsoft_Platform_Guide/bbb_Microsoft_Integration_Releases/Pure_Storage_FlashArray_Management_Extension_for_Microsoft_SQL_Server_Management_Studio#Release_Notes]
This section provides our recommendations for SQL Server databases hosted on Pure Storage FlashArrays.
- [**Pure Storage Microsoft Platform Guide**](#) [http://support.purestorage.com/Solutions/Microsoft_Platform_Guide]
This section provides details on best practices for configuring Microsoft Windows Server with a Pure Storage FlashArray.
- [**Best Practices: Microsoft SQL Server**](#) [https://support.purestorage.com/Solutions/Microsoft_Platform_Guide/Microsoft_SQL_Server/001_Microsoft_SQL_Server_Quick_Reference]
This section provides our recommendations for SQL Server databases hosted on Pure Storage FlashArrays.
- [**Volume Shadow Copy Service \(VSS\)**](#) [[http://support.purestorage.com/Solutions/Microsoft_Platform_Guide/L_Volume_Shadow_Copy_Service_\(VSS\)/Volume_Shadow_Copy_Service_\(VSS\)](http://support.purestorage.com/Solutions/Microsoft_Platform_Guide/L_Volume_Shadow_Copy_Service_(VSS)/Volume_Shadow_Copy_Service_(VSS))]
The Pure Storage VSS Hardware Provider is an integration that provides the ability to take application-consistent snapshots for Microsoft SQL Server.
- [**Troubleshooting the Volume Shadow Copy Service \(VSS\)**](#) [[http://support.purestorage.com/Solutions/Microsoft_Platform_Guide/L_Volume_Shadow_Copy_Service_\(VSS\)/Troubleshooting_the_Volume_Shadow_Copy_Service_\(VSS\)](http://support.purestorage.com/Solutions/Microsoft_Platform_Guide/L_Volume_Shadow_Copy_Service_(VSS)/Troubleshooting_the_Volume_Shadow_Copy_Service_(VSS))]
Troubleshooting information for the Pure Storage VSS Hardware Provider.

FlashArray information:

- [**Purity FlashArray User Guides**](#) [http://support.purestorage.com/FlashArray/PurityFA/FlashArray_User_Guide]
This page contains PDFs of the FlashArray User Guide for current and past releases, and an HTML version of the guide for the most recent Purity//FA release.
Instructions for configuring volumes, hosts, and LUNs are included in the FlashArray User Guide.

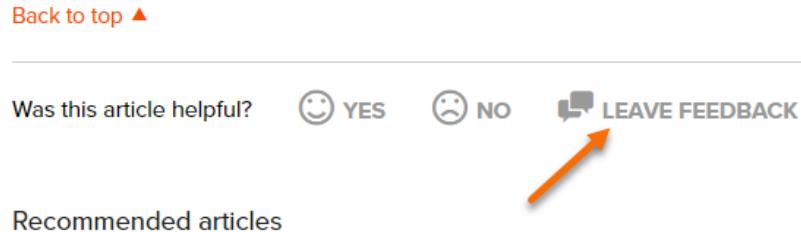
- **Knowledge Base ActiveCluster Articles** [<http://support.purestorage.com/FlashArray/PurityFA/Protect/ActiveCluster>]
This site contains Knowledge Base articles on FlashArray ActiveCluster replication.
- **Knowledge Base ActiveDR Articles** [<http://support.purestorage.com/FlashArray/PurityFA/Protect/ActiveDR>]
This site contains Knowledge Base articles on FlashArray ActiveDR replication.
- **REST API PDF Reference Guides** [http://support.purestorage.com/FlashArray/PurityFA/Purity_FA_REST_API/Reference/REST_API_PDF_Reference_Guides]
This page contains PDFs of the REST API Reference Guide for current and past releases and an HTML version of the most recent REST API release.

Documentation Feedback

Feedback on Pure Technical Services pages

The Microsoft Platform Guide and other Pure Technical Services pages include a feedback link at the bottom of the page.

Figure 35: Pure Technical Services Feedback Link



Your feedback is registered as sent by the email address associated with your Pure Technical Services login.

You can optionally give permission to be contacted by email about your comments. (The default is not to contact you.)

Feedback Through Email

We welcome your feedback about Pure Storage documentation and encourage you to send your questions and comments to <DocumentFeedback@purestorage.com>. We would love to hear from you.

Appendix D. Copyright and Notices

End User Agreement

End User Agreement [http://www.purestorage.com/agreements/Pure_enduser_agreement.pdf]

Copyrights and Licenses

Copyright© 2021 Pure Storage, Inc. All rights reserved. Pure Storage and the P Logo are trademarks or registered trademarks of Pure Storage, Inc., in the U.S. and other countries.

Microsoft, Windows, Windows Server, SQL Server, and Visual Studio are trademarks or registered trademarks of Microsoft Corporation in the United States, other countries, or both.

VMware, vCenter, and ESXi are trademarks or registered trademarks of VMware Corporation in the United States, other countries, or both.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

The Pure Storage products and programs described in this documentation are distributed under a license agreement restricting the use, copying, distribution, and decompilation/reverse engineering of the products. No part of this documentation may be reproduced in any form by any means without prior written authorization from Pure Storage, Inc. and its licensors, if any. Pure Storage may make improvements and/or changes in the Pure Storage products and/or the programs described in this documentation at any time without notice.

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. PURE STORAGE SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Pure Storage, Inc.
650 Castro Street
Mountain View, CA 94041



Pure Storage, Inc.

Twitter: @purestorage

650 Castro Street, Suite 200

Mountain View, CA 94041

800-379-7873

Sales: sales@purestorage.com

Support: support@purestorage.com

Media: pr@purestorage.com

General: info@purestorage.com