NetApp Element

PowerShell Tools Release Notes

Version 1.7

November 2020 | 215-15173_A0_UR001
doccomments@netapp.com

NetApp®

Contents

Introduction

NetApp Element PowerShell Tools is a collection of PowerShell Core functions that use Element storage API to control an Element storage system. These functions allow administrators to query for information, make changes to objects in a storage system, and develop complex scripts on a single platform. You can use this module with other modules and snap-ins, such as VMware PowerCLI to extend capabilities throughout the infrastructure.

Any user with an Element storage system and PowerShell Core can take advantage of NetApp Element PowerShell Tools. Before you use NetApp Element PowerShell Tools, you should have an understanding of PowerShell Core functions.

You can download the NetApp Element PowerShell Tools Install guide and software from the NetApp Support *Site*.

What's new in this release

Element PowerShell Tools version 1.7 contains the following improvements:

Full cmdlet support for the version 12.2 release of Element software, including security, SSH session management, IdpConfiguration, and SnapMirror support.

The following are the new Element storage cmdlets in the version 1.7 release:

- `Add-SFClusterInterfacePreference`: [Cluster] Lets you add a value to the key-value store. Works similar to a dictionary.
- `Add-SFKeyServerToProviderKmip`: [Cluster] Creates a KMIP (Key Management Interoperability Protocol) Key Provider.
- `Disable-SFIdpAuthentication`: [Cluster] Disable support for authentication using third party Identity Providers (IdP) for the cluster.
- `Disable-SFClusterSsh`: [Cluster] Disables SSH on all nodes in the cluster.
- `Disable-SFMaintenanceMode`: [Cluster] Take a node out of maintenance mode. This should be called after maintenance is complete and the node is online.
- `Disable-SFSsh`: [Node] Disables SSH on the targeted node.
- `Enable-SFIdpAuthentication`: [Cluster] Enable support for authentication using a third-party Identity Provider (IdP) for the cluster.
- `Enable-SFClusterSsh`: [Cluster] Enables SSH on all nodes in the cluster.
- `Enable-SFMaintenanceMode`: [Cluster] Prepare a node for maintenance. Maintenance includes anything that will require the node to be powered-off or restarted.
- `Enable-SFSsh`: [Node] Enables SSH on the targeted node.
- `Get-SFActiveAuthSessions`: [Cluster] Get-SFActiveAuthSessions gets a list of all active auth sessions on the cluster.
- `Get-SFActiveTlsCiphers`: [Cluster] Get-SFActiveTlsCiphers gets a list of the TLS ciphers that are currently accepted on the cluster.
- `Get-SFActiveVolume`: [Cluster] Get-SFActiveVolume gets a list of active volumes currently in the cluster.
- `Get-SFAuthSession`: [Cluster] Get-SFAuthSession gets a list of auth session on the cluster by cluster admin and user name.
- `Get-SFBinAssignmentProperties`: [Cluster] Enables you to retrieve the bin assignment properties in the database.
- `Get-SFClientCertificateSignRequest`: [Cluster] Generates a Certificate Sign Request which can be signed by a Certificate Authority to generate a client certificate for the cluster.
- `Get-SFClusterInterfacePreference`: [Cluster] Retrieves Cluster Interface Preference(s).
- `Get-SFClusterSshInfo`: [Cluster] Returns SSH status for the cluster.
- `Get-SFIdpAuthenticationState`: [Cluster] Return information regarding the state of authentication using third party Identity Providers.
- `Get-SFIdpConfiguration`: [Cluster] List configurations for third party Identity Provider(s) (IdP), optionally providing either enabledOnly flag to retrieve the currently enabled IdP configuration, or an IdP meta data UUID or IdP name to query a specific IdP configuration information.
- `Get-SFKeyProviderKmip`: [Cluster] Gets a list of KMIP (Key Management Interoperability Protocol) Key Providers on the cluster.
- `Get-SFKeyServerKmip`: [Cluster] Gets a list of KMIP (Key Management Interoperability Protocol) Key Providers on the cluster.
- `Get-SFLicenseKey`: [Cluster] Gets the current license key.

- `Get-SFNodeActiveTlsCiphers`: [Node] Get-SFNodeActiveTlsCiphers gets a list of the TLS ciphers that are currently accepted on the node.
- `Get-SFNodeFipsDrivesReport`: [Node] Reports the FipsDrives capability of a node.
- `Get-SFNodeSSLCertificate`: [Node] Gets the management node's SSL certificate.
- `Get-SFNodeSupportedTlsCiphers`: [Node] Get-SFNodeSupportedTlsCiphers gets a list of the supported TLS ciphers.
- `Get-SFProtectionDomainLayout`: [Cluster] Returns all of the Protection Domain information for the cluster.
- `Get-SFSnapMirrorAggregates`: [Cluster] `Get-SFSnapMirrorAggregates` lists all SnapMirror aggregates that are available on the remote ONTAP system. An aggregate describes a set of physical storage resources.
- `Get-SFSnapMirrorClusterIdentity`: [Cluster] `Get-SFSnapMirrorClusterIdentity` gets identity information about the ONTAP cluster.
- `Get-SFSnapMirrorEndpoints`: [Cluster] `Get-SFSnapMirrorEndpoints` lists all SnapMirror endpoints that the Element storage cluster is communicating with.
- `Get-SFSnapMirrorLuns`: [Cluster] `Get-SFSnapMirrorLuns` lists the LUN information for the SnapMirror relationship from the remote ONTAP cluster.
- `Get-SFSnapMirrorNetworkInterfaces`: [Cluster] The Element web UI uses the `ListSnapMirrorNetworkInterfaces` method to list all available SnapMirror interfaces on a remote ONTAP system.
- `Get-SFSnapMirrorNodes`: [Cluster] `Get-SFSnapMirrorNodes` lists the nodes in a remote ONTAP cluster.
- `Get-SFSnapMirrorPolicies`: [Cluster] `Get-SFSnapMirrorPolicies` lists all SnapMirror policies on a remote ONTAP system.
- `Get-SFSnapMirrorRelationships`: [Cluster] `Get-SFSnapMirrorRelationships` lists one or all SnapMirror relationships on an Element storage cluster.
- `Get-SFSnapMirrorSchedules`: [Cluster] `Get-SFSnapMirrorSchedules` lists the schedules that are available on a remote ONTAP cluster.
- `Get-SFSnapMirrorVolumes`: [Cluster] `Get-SFSnapMirrorVolumes` lists all SnapMirror volumes available on a remote ONTAP system.
- `Get-SFSnapMirrorVservers`: [Cluster] `Get-SFSnapMirrorVservers` lists all SnapMirror Vservers available on a remote ONTAP system.
- `Get-SFSshInfo`: [Node] Returns SSH status for the node.
- `Get-SFSSLCertificate`: [Cluster] Gets the cluster's SSL certificate.
- `Get-SFSupportedTlsCiphers`: [Cluster] Get-SFSupportedTlsCiphers gets a list of the supported TLS ciphers.
- `Initialize-SFSnapMirrorRelationship`: [Cluster] `Initialize-SFSnapMirrorRelationship` initializes the destination volume in a SnapMirror relationship by performing an initial baseline transfer between clusters.
- `Invoke-SFBreakSnapMirrorRelationship`: [Cluster] `Invoke-SFBreakSnapMirrorRelationship` breaks a SnapMirror relationship. When a SnapMirror relationship is broken, the destination volume is made read-write and independent, and can then diverge from the source. You can reestablish the relationship with the Start-SFResyncSnapMirrorRelationship. This method requires the ONTAP cluster to be available.
- `Invoke-SFBreakSnapMirrorVolume`: [Cluster] `Invoke-SFBreakSnapMirrorVolume` breaks the SnapMirror relationship between an ONTAP source container and SolidFire target volume. Breaking a SolidFire SnapMirror volume is useful if an ONTAP system becomes unavailable while replicating data to a SolidFire volume. This feature enables a storage administrator to take control of a SolidFire SnapMirror volume, break its relationship with the remote ONTAP system, and revert the volume to a previous snapshot.

- `Invoke-SFQuiesceSnapMirrorRelationship`: [Cluster] `Invoke-SFQuiesceSnapMirrorRelationship` disables future data transfers for a SnapMirror relationship. If a transfer is in progress, the relationship status becomes "quiescing" until the transfer is complete. If the current transfer is aborted, it will not restart. You can reenable data transfers for the relationship using the `Resume-SFSnapMirrorRelationship` commandlet.
- `New-SFIdpClusterAdmin`: [Cluster] Adds a cluster administrator user authenticated by a third-party Identity Provider (IdP).
- `New-SFIdpConfiguration`: [Cluster] Create a potential trust relationship for authentication using a third-party Identity Provider (IdP) for the cluster.
- `New-SFKeyProviderKmip`: [Cluster] Creates a KMIP (Key Management Interoperability Protocol) Key Provider.
- `New-SFKeyServerKmip`: [Cluster] Creates a KMIP (Key Management Interoperability Protocol) Key Server.
- `New-SFPublicPrivateKeyPair`: [Cluster] Create SSL public and private keys.
- `New-SFSnapMirrorEndpoint`: [Cluster] `New-SFSnapMirrorEndpoint` creates a relationship with a remote SnapMirror endpoint.
- `New-SFSnapMirrorEndpointUnmanaged`: [Cluster] New-SFSnapMirrorEndpointUnmanaged creates an unmanaged relationship with a remote SnapMirror endpoint.
- `New-SFSnapMirrorRelationship`: [Cluster] `New-SFSnapMirrorRelationship` creates a SnapMirror extended data protection relationship between a source and destination endpoint.
- `New-SFSnapMirrorVolume`: [Cluster] `New-SFSnapMirrorVolume` creates a volume on the remote ONTAP system.
- `Remove-SFAuthSession`: [Cluster] Deletes an individual auth session by SessionID, ClusterAdmin and Username.
- `Remove-SFClusterInterfacePreference`: [Cluster] Deletes an existing cluster interface preference.
- `Remove-SFIdpConfiguration`: [Cluster] Delete an existing configuration with a third party Identity Provider (IdP) for the cluster.
- `Remove-SFKeyProviderKmip`: [Cluster] Removes the specified inactive Key Provider.
- `Remove-SFKeyServerFromProviderKmip`: [Cluster] Remove the specified KMIP (Key Management Interoperability Protocol) Key Server from the provider it was assigned to.
- `Remove-SFKeyServerKmip`: [Cluster] Removes the specified inactive Key Server.
- `Remove-SFNodeSSLCertificate`: [Node] Removes the management node's SSL certificate.
- `Remove-SFSnapMirrorEndpoints`: [Cluster] `Remove-SFSnapMirrorEndpoints` deletes one or more SnapMirror endpoints from the system.
- `Remove-SFSnapMirrorRelationships`: [Cluster] `Remove-SFSnapMirrorRelationships` removes a SnapMirror relationship between a source and destination endpoint.
- `Remove-SFSSLCertificate`: [Cluster] Removes the cluster's SSL certificate.
- `Reset-SFNodeSupplementalTlsCiphers`: [Node] Reset-SFSupplementalTlsCiphers restores the supplemental ciphers to their defaults.
- `Reset-SFSupplementalTlsCiphers`: [Cluster] Reset-SFSupplementalTlsCiphers restores the supplemental ciphers to their defaults.
- `Resume-SFSnapMirrorRelationship`: [Cluster] `Resume-SFSnapMirrorRelationship` enables future transfers for a quiesced SnapMirror relationship.
- `Set-SFClusterInterfacePreference`: [Cluster] Lets you modify a value to the key-value store.
- `Set-SFKeyServerKmip`: [Cluster] Sets attributes of a KMIP (Key Management Interoperability Protocol) Key Server.

- `Set-SFLicenseKey`: [Cluster] Sets the license key for the cluster.
- `Set-SFNodeSSLCertificate`: [Node] Sets the management node's SSL certificate.
- `Set-SFNodeSupplementalTlsCiphers`: [Node] Set the list of supplemental TLS ciphers for a node.
- `Set-SFProtectionDomainLayout`: [Cluster] Used to assign nodes to user-defined **Custom Protection Domains**. The following requirements must be met, or the custom protection domain is ignored and the system returns an appropriate error:
  - Provide this protection domain information to all active nodes in the cluster. Do not provide protection domain information to any nodes that are not active.
  - Assign all nodes in each chassis to the same user-defined custom protection domain.
  - Use the same *`ProtectionDomainType`* for all nodes.
  - Do not use protection domain types that are not user-defined, such as *`Node`* and *`Chassis`*.
- `Set-SFSnapMirrorEndpoint`: [Cluster] `Set-SFSnapMirrorEndpoint` changes the name and management attributes for a SnapMirror endpoint.
- `Set-SFSnapMirrorEndpointUnmanaged`: [Cluster] Set-SFSnapMirrorEndpointUnmanaged modifies a SnapMirror endpoint.
- `Set-SFSnapMirrorRelationship`: [Cluster] `Set-SFSnapMirrorRelationship` changes the intervals at which a scheduled snapshot occurs. You can also delete or pause a schedule by using this method.
- `Set-SFSSLCertificate`: [Cluster] Sets the cluster's SSL certificate.
- `Set-SFSupplementalTlsCiphers`: [Node] Set the list of supplemental TLS ciphers.
- `Start-SFResyncSnapMirrorRelationship`: [Cluster] `Start-SFResyncSnapMirrorRelationship` establishes or reestablishes a mirror relationship between a source and destination endpoint. When you resync a relationship, the system removes snapshots on the destination volume that are newer than the common snapshot copy, and then mounts the destination volume as a data protection volume with the common snapshot copy as the exported snapshot copy.
- `Stop-SFSnapMirrorRelationship`: [Cluster] `Stop-SFSnapMirrorRelationship` stops SnapMirror transfers that have started but are not yet complete.
- `Test-SFKeyProviderKmip`: Test whether the specified KMIP (Key Management Interoperability Protocol) Key Provider is functioning normally.
- `Test-SFKeyServerKmip`: Test whether the specified KMIP (Key Management Interoperability Protocol) Key Server is functioning normally.
- `Update-SFIdpConfiguration`: [Cluster] Update an existing configuration with a third party Identity Provider (IdP) for the cluster.
- `Update-SFSnapMirrorRelationship`: [Cluster] `Update-SFSnapMirrorRelationship` makes the destination volume in a SnapMirror relationship an up-to-date mirror of the source volume.

Resolved issues

The following items have been corrected. The original ticket number is listed for reference.

Element PowerShell Tools version 1.7 contains the following corrections.

GitHub Ticket #	Description
28	Issue in `Set-SFVolumeAccessGroup` example 2.
35	`New-SFSchedule` fails when using `-Retention*` parameters.
49	Typo in `Invoke-SFShutdown` cmdlet help.
52	Incorrect `Invoke-SFShutdown` example.
54	Typo in `Set-SFClusterConfig` cmdlet help.
60	Unexpected result of `Get-SFInitiator | Add-SFInitiatorToVolumeAccessGroup`.
70	Fails to parse async delay data if populated in the json payload response to `Get-SFvolumeStats`.
72	`Test-SFPing` returns as passed -even against IPs not on network.
75	`Remove-SFInitiatorFromVolumeAccessGroup` removes the initiator from the cluster altogether (rather than just from the access group).

Where to find product documentation and other information

You can learn more about using and managing NetApp HCI and SolidFire all-flash storage from the resources available in the Documentation Centers and Resources pages for both products.

In the Documentation Centers, you can also find information about hardware installation and maintenance, additional content resources available, links to known issues and resolved issues, and the latest release notes. On the Resources pages, you can find links to data sheets, technical reports, white papers, and videos.

- *NetApp HCI Documentation*
- *NetApp HCI Documentation Center*
- *NetApp HCI Resources page*
- *SolidFire and Element 12.2 Documentation Center*
- *SolidFire and Element 12.0 Documentation Center*
- *SolidFire and Element 11.8 Documentation Center*
- *SolidFire and Element 11.7 Documentation Center*
- *SolidFire and Element 11.5 Documentation Center*
- *SolidFire Resources page*

Contact NetApp Support

If you need help with or have questions or comments about NetApp products, contact NetApp Support.

- Web:
  mysupport.netapp.com
- Phone:
  - 888.4.NETAPP (888.463.8277) (US and Canada)
  - 00.800.44.638277 (EMEA/Europe)
  - +800.800.80.800 (Asia/Pacific)

Copyright

Trademark

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277