snapmirror object-store commands

Command reference

NetApp
July 17, 2026

Table of Contents

snapmirror object-store commands

snapmirror object-store config create

Define the configuration for a SnapMirror object store

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `snapmirror object-store config create` command is used by a cluster administrator to tell ONTAP how to connect to an object store. Following pre-requisites must be met before creating an object store configuration in ONTAP.

- A valid data bucket or container must be created with the object store provider. This assumes that the user has valid account credentials with the object store provider to access the data bucket.
- The ONTAP node must be able to connect to the object store. This includes
- Fast, reliable connectivity to the object store.
- An inter-cluster LIF (Logical Interface) must be configured on the cluster.
- If SSL/TLS authentication is required, then valid certificates must be installed.

An object-store configuration once created must not be reassociated with a different object-store or container. See snapmirror object-store config modify command for more information.

Parameters

`-vserver <vserver name>` - Vserver Name

This parameter specifies the vserver on which the object store configuration needs to be created.

`-object-store-name <text>` - Object Store Configuration Name

This parameter specifies the name that will be used to identify the object store configuration. The name can contain the following characters: "*", "-", A-Z, a-z, and 0-9. The first character must be one of the following: '*"*', A-Z, or a-z.

`-usage {data|metadata}` - Object Store Use

This parameter specifies the usage for an object store configuration.

`-provider-type <providerType>` - Type of the Object Store Provider

This parameter specifies the type of object store provider that will be attached to the aggregate. Valid options are: AWS_S3 (Amazon S3 storage), Azure_Cloud (Microsoft Azure Cloud), SGWS (StorageGrid WebScale), IBM_COS (IBM Cloud Object Storage), AliCloud (Alibaba Cloud Object Storage Service), GoogleCloud (Google Cloud Storage) and ONTAP_S3.

`-server <Remote InetAddress>` - Fully Qualified Domain Name of the Object Store Server

This parameter specifies the Fully Qualified Domain Name (FQDN) of the remote object store server. For Amazon S3, server name must be an AWS regional endpoint in the format s3.amazonaws.com or s3-<region>.amazonaws.com, for example, s3-us-west-2.amazonaws.com. The region of the server and the bucket must match. For more information on AWS regions, refer to 'Amazon documentation on AWS regions and endpoints'. For Azure, if the `-server` is a "blob.core.windows.net" or a

"blob.core.usgovcloudapi.net", then a value of `-azure-account` followed by a period will be added in front of the server.

[-is-ssl-enabled {true|false}] - Is SSL/TLS Enabled

This parameter indicates whether a secured SSL/TLS connection will be used during data access to the object store. The default value is `true` .

[-port <integer>] - Port Number of the Object Store

This parameter specifies the port number on the remote server that ONTAP will use while establishing connection to the object store.

-container-name <text> - Data Bucket/Container Name

This parameter specifies the data bucket or container that will be used for read and write operations.

This name cannot be modified once a configuration is created.

[-access-key <text>] - Access Key ID for S3 Compatible Provider Types

This parameter specifies the access key (access key ID) required to authorize requests to the AWS S3, SGWS, IBM COS object stores and ONTAP_S3. For an Azure object store see `-azure-account.`

[-ipspace <IPspace>] - IPspace to Use in Order to Reach the Object Store

This optional parameter specifies the IPspace to use to connect to the object store. Default value: *`Default`* .

[-use-iam-role {true|false}] - (DEPRECATED)-Use IAM Role for AWS Cloud Volumes ONTAP

This optional parameter is deprecated. Use `-auth-type` instead. Note, that `-auth-type EC2-IAM` is an equivalent of `-use-iam-role true` , and `-auth-type key` is an equivalent of `-use-iam-role false` .

[-secret-password <text>] - Secret Access Key for S3 Compatible Provider Types

This parameter specifies the password (secret access key) to authenticate requests to the AWS S3, SGWS, IBM COS object stores and ONTAP_S3. If the `-access-key` is specified but the `-secret-password` is not, then one will be asked to enter the `-secret-password` without echoing the input.

[-is-certificate-validation-enabled {true|false}] - Is SSL/TLS Certificate Validation Enabled

This parameter indicates whether an SSL/TLS certificate of an object store server is validated whenever an SSL/TLS connection to an object store server is established. This parameter is only applicable when `is-ssl-enabled` is `true` . The default value is `true` . It is recommended to use the default value to make sure that ONTAP connects to a trusted object store server, otherwise identities of an object store server are not verified.

[-azure-account <text>] - Azure Account

This parameter specifies the account required to authorize requests to the Azure object store. For other object store providers see access-key.

The value of this field cannot be modified once a configuration is created.

[-ask-azure-private-key {true|false}] - Ask to Enter the Azure Access Key without Echoing

If this parameter is true then one will be asked to enter `-azure-private-key` without echoing the input. Default value: *true* .

[-azure-private-key <text>] - Azure Access Key

This parameter specifies the access key required to authenticate requests to the Azure object store. See also `ask-azure-private-key` . For other object store providers see `-secret-password` .

[-server-side-encryption {none | SSE-S3}] - Encryption of Data at Rest by the Object Store Server

This parameter specifies if AWS or other S3 compatible object store server must encrypt data at rest. The available choices depend on provider-type. `none` encryption (no encryption required) is supported by all types of S3 (non-Azure) object store servers. `SSE-S3` encryption is supported by and is a default for all types of S3 (non-Azure) object store servers except ONTAP_S3. This is an advanced property. In most cases it is best not to change default value of "sse_s3" for object store servers which support SSE-S3 encryption. The encryption is in addition to any encryption done by ONTAP at a volume or at an aggregate level.

[-url-style {path-style | virtual-hosted-style}] - URL Style Used to Access S3 Bucket

This parameter specifies the URL style used to access S3 bucket. This option is only available for non-Azure object store providers. The available choices and default value depend on provider-type.

[-iamra-session-token <text>] - IAMRA Session Token for Authentication

This parameter specifies a temporary token for S3 SnapMirror which will expire periodically. This will increase security.

[-azure-msi-token <text>] - Azure MSI Token for Authentication

This optional parameter specifies the Managed Service Identity (MSI) token required to authenticate to the Azure object store. This form of authentication is only supported on Azure NetApp Files.

Examples

The following example creates a cluster scoped object store configuration named *objectStoreName.*

```
cluster1::*> snapmirror object-store config create
        -object-store-name objectStoreName -usage data -owner snapmirror
        -provider-type SGWS -server objectStoreServer.com
        -container-name containerName -is-ssl-enabled true
        -is-certificate-validation-enabled false
        -ipspace Default -access-key userAccessKey
        -secret-password userSecretPassWord
```

Related Links

- snapmirror object-store config modify

snapmirror object-store config delete

Delete SnapMirror object store configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `snapmirror object-store config delete` command removes an existing object store configuration in ONTAP.

Parameters

`-vserver <vserver name>` - Vserver Name

This parameter specifies the vserver name on which the object store configuration has been configured.

`-object-store-name <text>` - Object Store Configuration Name

This parameter specifies the object store configuration to be deleted.

Examples

The following example deletes an object store configuration named *`objectStoreName`*.

```
cluster1::*> snapmirror object-store config delete
        -object-store-name objectStoreName
```

snapmirror object-store config modify

Modify SnapMirror object store configuration attributes

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The storage aggregate object-store config modify command is used to update one or more of object store configuration parameters.

Parameters

`-vserver <vserver name>` - Vserver Name

This parameter specifies the vserver on which the object store configuration needs to be created.

`-object-store-name <text>` - Object Store Configuration Name

This parameter identifies the configuration to be modified.

`[-usage {data|metadata}]` - Object Store Use

This parameter specifies the usage for an object store configuration.

[-new-object-store-name <text>] - Object Store Configuration New Name

This optional parameter specifies the new name for the object store configuration.

[-server <Remote InetAddress>] - Fully Qualified Domain Name of the Object Store Server

This optional parameter specifies the new Fully Qualified Domain Name (FQDN) of the same object store server. For Amazon S3, server name must be an AWS regional endpoint in the format s3.amazonaws.com or s3-<region>.amazonaws.com, for example, s3-us-west-2.amazonaws.com. The region of the server and the bucket must match. For more information on AWS regions, refer to 'Amazon documentation on AWS regions and endpoints'. For Azure, if the `-server` is a "blob.core.windows.net" or a "blob.core.usgovcloudapi.net", then the value of azure-account in the configuration followed by a period will be added in front of the server. Note that the value of `azure-account` cannot be modified.

[-is-ssl-enabled {true|false}] - Is SSL/TLS Enabled

This optional parameter indicates whether a secured SSL/TLS connection will be used during data access to the object store.

[-port <integer>] - Port Number of the Object Store

This optional parameter specifies a new port number to connect to the object store server indicated in the `-server` parameter.

[-access-key <text>] - Access Key ID for S3 Compatible Provider Types

This optional parameter specifies a new access key (access key ID) for the AWS S3, SGWS, IBM COS object stores and ONTAP S3.

[-ipspace <IPspace>] - IPspace to Use in Order to Reach the Object Store

This optional parameter specifies new ipspace values for the configuration.

[-use-iam-role {true|false}] - (DEPRECATED)-Use IAM Role for AWS Cloud Volumes ONTAP

This optional parameter is deprecated. Use `-auth-type` instead. Note, that `-auth-type EC2-IAM` is an equivalent of `-use-iam-role true` , and `-auth-type key` is an equivalent of `-use-iam-role false` .

[-secret-password <text>] - Secret Access Key for S3 Compatible Provider Types

This optional parameter specifies a new password (secret access key) for the AWS S3, SGWS, IBM COS object stores and ONTAP S3. For an Azure object store see `-azure-private-key` . If the `-access-key` is specified but the `-secret-password` is not then one will be asked to enter the `-secret-password` without echoing the input.

[-is-certificate-validation-enabled {true|false}] - Is SSL/TLS Certificate Validation Enabled

This optional parameter indicates whether an SSL/TLS certificate of an object store server is validated whenever an SSL/TLS connection to an object store server is established. This parameter is only applicable when `is-ssl-enabled` is `true` . It is recommended to keep the default value which is `true` to make sure that ONTAP connects to a trusted object store server, otherwise identities of an object store server are not verified.

[-ask-azure-private-key {true|false}] - Ask to Enter the Azure Access Key without Echoing

If this optional parameter is true then one will be asked to enter the `-azure-private-key` without echoing the input.

[-azure-private-key <text>] - Azure Access Key

This optional parameter specifies a new access key for Azure object store. For other object store providers see `secret-password` . See also `ask-azure-private-key` .

[-server-side-encryption {none | SSE-S3}] - Encryption of Data at Rest by the Object Store Server

This parameter specifies if AWS or other S3 compatible object store server must encrypt data at rest. The available choices depend on provider-type. `none` encryption (no encryption required) is supported by all S3 (non-Azure) object store servers. `SSE-S3` encryption is supported by all S3 (non-Azure) object store servers except ONTAP_S3. This is an advanced property. In most cases it is best not to change default value of "sse_s3" for object store servers which support SSE-S3 encryption. The encryption is in addition to any encryption done by ONTAP at a volume or at an aggregate level. Note that changing this option does not change encryption of data which already exist in the object store.

[-url-style {path-style | virtual-hosted-style}] - URL Style Used to Access S3 Bucket

This parameter specifies the URL style used to access S3 bucket. This option is only available for non-Azure object store providers. The available choices and default value depend on provider-type.

[-iamra-session-token <text>] - IAMRA Session Token for Authentication

This parameter specifies a temporary token for S3 SnapMirror which will expire periodically. This will increase security.

[-azure-msi-token <text>] - Azure MSI Token for Authentication

This optional parameter specifies the new Managed Service Identity (MSI) token required to authenticate to the Azure object store. This form of authentication is only supported on Azure NetApp Files.

Examples

The following example modifies an object-store configuration named *`objectStoreName`* to a new name *`newName.`*

```
cluster::*> snapmirror object-store config modify
        -object-store-name objectStoreName
        -new-object-store-name newName
```

Related Links

- storage aggregate object-store config modify

snapmirror object-store config show

Display a list of SnapMirror object store configurations

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `snapmirror object-store config show` command displays information about all existing object store configurations in the cluster.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name

If this parameter is specified, the command displays information only about object store configurations which are configured within this vserver.

[-object-store-name <text>] - Object Store Configuration Name

If this parameter is specified, the command displays information only about object store configurations whose name matches the specified names.

[-usage {data|metadata}] - Object Store Use

Specifies what this objectc store configuration is used for.

[-vsUuid <UUID>] - Vserver UUID

Vserver UUId.

[-config-id <integer>] - Object Store Configuration ID

If this parameter is specified, the command displays information only about object store configurations whose configuration ID matches the specified value.

[-provider-type <providerType>] - Type of the Object Store Provider

If this parameter is specified, the command displays information only about object store configurations whose provider type matches the specified value.

[-server <Remote InetAddress>] - Fully Qualified Domain Name of the Object Store Server

If this parameter is specified, the command displays information only about object store configurations whose server name matches the specified value. The server name is specified as a Fully Qualified Domain Name (FQDN).

[-is-ssl-enabled {true|false}] - Is SSL/TLS Enabled

If this parameter is specified, the command displays information only about object store configurations whose status about the use of secured communication over the network matches the specified value.

[-port <integer>] - Port Number of the Object Store

If this parameter is specified, the command displays information only about object store configurations whose port numbers matches the specified value.

[-container-name <text>] - Data Bucket/Container Name

If this parameter is specified, the command displays information only about object store configurations whose container name matches the specified value. ONTAP uses this container name or object store data bucket while accessing data from the object store.

[-access-key <text>] - Access Key ID for S3 Compatible Provider Types

If this parameter is specified, the command displays information only about AWS S3, SGWS, IBM COS object store configurations and ONTAP S3 whose access key matches the specified value. ONTAP requires the access key for authorized access to the object store.

[-ipspace <IPspace>] - IPspace to Use in Order to Reach the Object Store

If this parameter is specified, the command displays information only about object store configurations whose IPspace matches the specified value. ONTAP uses the IPspace value to connect to the object store.

[-use-iam-role {true|false}] - (DEPRECATED)-Use IAM Role for AWS Cloud Volumes ONTAP

If this parameter is specified, the command displays information only about object store configurations whose IAM role status flag matches the specified value. The `-iam-role` and `-use-iam-role` parameters are relevant only in the context of AWS object store and indicates whether IAM role must be used for accessing it. The IAM credentials can be obtained only through AWS Cloud Volumes ONTAP.

[-is-certificate-validation-enabled {true|false}] - Is SSL/TLS Certificate Validation Enabled

If this parameter is specified, the command displays information only about object store configurations whose status about the validation of SSL/TLS certificate matches the specified value.

[-azure-account <text>] - Azure Account

If this parameter is specified, the command displays information only about Azure object store configurations whose account matches the specified value. ONTAP requires the Azure account for authorized access to the Azure object store.

[-server-side-encryption {none | SSE-S3}] - Encryption of Data at Rest by the Object Store Server

If this parameter is specified, the command displays information only about object store configurations whose server-side encryption matches the specified value.

[-url-style {path-style | virtual-hosted-style}] - URL Style Used to Access S3 Bucket

If this parameter is specified, the command displays information only about object store configurations whose URL style matches the specified value.

Examples

The following example displays information about all existing object store configurations in the cluster.

```
cluster1::*> snapmirror object-store config show
```

Copyright information

Trademark information