FlexCache duality

ONTAP 9

NetApp
February 06, 2026

Table of Contents

FlexCache duality

FAQ about FlexCache duality

This FAQ answers common questions about FlexCache duality introduced in ONTAP 9.18.1.

Frequently asked questions

What is "duality?"

Duality enables unified access to the same data using both file (NAS) and object (S3) protocols. Introduced in ONTAP 9.12.1 without FlexCache support, duality was extended in ONTAP 9.18.1 to include FlexCache volumes, allowing S3 protocol access to NAS files cached in a FlexCache volume.

What S3 operations are supported on a FlexCache S3 bucket?

S3 operations supported on standard S3 NAS buckets are supported on FlexCache S3 NAS buckets, with the exception of the `COPY` operation. For an up-to-date list of unsupported operations for a standard S3 NAS bucket, visit the interoperability documentation.

Can I use FlexCache in write-back mode with FlexCache duality?

No. If a FlexCache S3 NAS bucket is created on a FlexCache volume, the FlexCache volume **must** be in write-around mode. If you attempt to create a FlexCache S3 NAS bucket on a FlexCache volume in write-back mode, the operation will fail.

I can’t upgrade one of my clusters to ONTAP 9.18.1 because of hardware limitations. Will duality still work in my cluster if only the cache cluster is running ONTAP 9.18.1?

No. Both the cache cluster and origin cluster must have a minimum effective cluster version of 9.18.1. If you attempt to create a FlexCache S3 NAS bucket on a cache cluster peered with an origin running an ONTAP version earlier than 9.18.1, the operation will fail.

I have a MetroCluster configuration. Can I use FlexCache duality?

No. FlexCache duality is not supported in MetroCluster configurations.

Can I audit S3 access to files in a FlexCache S3 NAS bucket?

S3 auditing is provided by the NAS auditing functionality FlexCache volumes use. For more information about NAS auditing of FlexCache volumes, see Learn more about FlexCache auditing.

What should I expect if the cache cluster becomes disconnected from the origin cluster?

S3 requests to a FlexCache S3 NAS bucket will fail with a `503 Service Unavailable` error if the cache cluster is disconnected from the origin cluster.

Can I use multipart S3 operations with FlexCache duality?

For multipart S3 operations to work, the underlying FlexCache volume must have the granular-data field set to 'advanced'. This field is set to whatever value is set for the origin volume.

Does FlexCache duality support HTTP and HTTPS access?

Yes. By default, HTTPS is required. You can configure the S3 service to allow HTTP access if needed.

Enable S3 access to NAS FlexCache volumes

Beginning in ONTAP 9.18.1, you can enable S3 access to NAS FlexCache volumes, also referred to as "duality." This allows clients to access data stored in a FlexCache volume using the S3 protocol, in addition to traditional NAS protocols like NFS and SMB. You can use the following information to set up FlexCache duality.

Prerequisites

Before you begin, you must ensure you complete the following prerequisites:

- Make sure the S3 protocol and desired NAS protocols (NFS, SMB, or both) are licensed and configured on the SVM.
- Verify that DNS and any other required services are configured.
- Cluster and SVM Peered
- FlexCache Volume create
- Data-lif created

ⓘ For more thorough documentation on FlexCache duality, see ONTAP S3 multiprotocol support.

Step 1: Create and sign certificates

To enable S3 access to a FlexCache volume, you need to install certificates for the SVM that hosts the FlexCache volume. This example uses self-signed certificates, but in a production environment, you should use certificates signed by a trusted Certificate Authority (CA).

1. Create an SVM root CA:

```
security certificate create -vserver <svm> -type root-ca -common-name
<arbitrary_name>
```

2. Generate a Certificate Signing Request:

```
security certificate generate-csr -common-name <dns_name_of_data_lif>
-dns-name <dns_name_of_data_lif> -ipaddr <data_lif_ip>
```

Example output:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICzjCCAbYCAQAwHzEdMBsGA1UEAxMUY2FjaGUxZy1kYXRhLm5hcy5sYWIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCusJk075O8Uh329cHI6x+BaRS2
w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK1CI2VEkrXGUg
...
vMIGN351+FgzLQ4X5lKfoMXCV70NqIakxzEmkTIUDKv7n9EVZ4b5DTTlrL03X/nK
+Bim2y2y180PaFB3NauZHTnIIzIc8zCp2IEqmFWyMDcdBjP9KS0+jNm4QhuXiM8F
D7gm3g/O70qa5OxbAEal5o4NbOl95U0T0rwqTaSzFG0XQnK2PmA1OIwS5ET35p3Z
dLU=
-----END CERTIFICATE REQUEST-----
```

Private key example:

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCusJk075O8Uh32
9cHI6x+BaRS2w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK
1CI2VEkrXGUgwBtx1K4IlrCTB829Q1aLGAQXVyWnzhQc4tS5PW/DsQ8t7olZ9zEI
...
rXGEdDaqp7jQGNXUGlbxO3zcBil1/A9Hc6oalNECgYBKwe3PeZamiwhIHLy9ph7w
dJfFCshsPalMuAp2OuKIAnNa9l6fT9y5kf9tIbskT+t5Dth8bmV9pwe8UZaK5eC4
Svxm19jHT5QqloDaZVUmMXFKyKoqPDdfvcDk2Eb5gMfIIb0a3TPC/jqqpDn9BzuH
TO02fuRvRR/G/HUz2yRd+A==
-----END PRIVATE KEY-----
```

Keep a copy of your certificate request and private key for future reference.

3. Sign the certificate:

   The `root-ca` is the one you created in Create an SVM root CA.

   ```
   certificate sign -ca <svm_root_ca> -ca-serial <svm_root_ca_sn> -expire
   -days 364 -format PEM -vserver <svm>
   ```

4. Paste the Certificate Signing Request (CSR) generated in Generate a Certificate Signing Request.

   Example:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICzjCCAbYCAQAwHzEdMBsGA1UEAxMUY2FjaGUxZy1kYXRhLm5hcy5sYWIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCusJk075O8Uh329cHI6x+BaRS2
w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK1CI2VEkrXGUg
...
vMIGN351+FgzLQ4X5lKfoMXCV70NqIakxzEmkTIUDKv7n9EVZ4b5DTTlrL03X/nK
+Bim2y2y180PaFB3NauZHTnIIzIc8zCp2IEqmFWyMDcdBjP9KS0+jNm4QhuXiM8F
D7gm3g/O70qa5OxbAEal5o4NbOl95U0T0rwqTaSzFG0XQnK2PmA1OIwS5ET35p3Z
dLU=
-----END CERTIFICATE REQUEST-----
```

This prints a signed certificate to the console, similar to the following example.

Signed Certificate example:

```
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIIGHolbgv5DPowDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMWY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjIxNTU4WhcNMjYxMTIwMjIxNTU4WjAfMR0wGwYDVQQDExRjYWNoZTFnLWRhdGEu
...
qS7zhj3ikWE3Gp9s+QijKWXx/0HDd1UuGqy0QZNqNm/M0mqVnokJNk5F4fBFxMiR
1o63BxL8xGIRdtTCjjb2Gq2Wj7EClUw6CykEkxAcVk+XrRtArGkNtcYdtHfUsKVE
wswvv0rNydrNnWhJLhSl8TW5Tex+OMyTXgk9/3K8kB0mAMrtxxYjt8tm+gztkivf
J0eo1uDJhaNxqwEZRzFyGaa4k1+56oFzRfTc
-----END CERTIFICATE-----
```

5. Copy the certificate for the next step.
6. Install the server certificate on the SVM:

```
certificate install -type server -vserver <svm> -cert-name flexcache-duality
```

7. Paste the signed certificate from Sign the certificate.

   Example:

```
Please enter Certificate: Press <Enter> [twice] when done
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIIGHolbgv5DPowDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMWY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjIxNTU4WhcNMjYxMTIwMjIxNTU4WjAfMR0wGwYDVQQDExRjYWNoZTFnLWRhdGEu
bmFzLmxhYjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK6wmTTvk7xS
...
qS7zhj3ikWE3Gp9s+QijKWXx/0HDd1UuGqy0QZNqNm/M0mqVnokJNk5F4fBFxMiR
1o63BxL8xGIRdtTCjjb2Gq2Wj7EClUw6CykEkxAcVk+XrRtArGkNtcYdtHfUsKVE
wswvv0rNydrNnWhJLhSl8TW5Tex+OMyTXgk9/3K8kB0mAMrtxxYjt8tm+gztkivf
J0eo1uDJhaNxqwEZRzFyGaa4k1+56oFzRfTc
-----END CERTIFICATE-----
```

8. Paste the private key generated in Generate a Certificate Signing Request.

   Example:

```
Please enter Private Key: Press <Enter> [twice] when done
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCusJk075O8Uh32
9cHI6x+BaRS2w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK
1CI2VEkrXGUgwBtx1K4IlrCTB829Q1aLGAQXVyWnzhQc4tS5PW/DsQ8t7olZ9zEI
W/gaEIajgpXIwGNWZ+weKQK+yoolxC+gy4IUE7WvnEUiezaIdoqzyPhYq5GC4XWf
0johpQugOPe0/w2nVFRWJoFQp3ZP3NZAXc8H0qkRB6SjaM243XV2jnuEzX2joXvT
wHHH+IBAQ2JDs7s1TY0I20e49J2Fx2+HvUxDx4BHao7CCHA1+MnmEl+9E38wTaEk
NLsU724ZAgMBAAECggEABHUy06wxcIk5hO3S9Ik1FDZV3JWzsu5gGdLSQOHRd5W+
...
rXGEdDaqp7jQGNXUGlbxO3zcBil1/A9Hc6oalNECgYBKwe3PeZamiwhIHLy9ph7w
dJfFCshsPalMuAp2OuKIAnNa9l6fT9y5kf9tIbskT+t5Dth8bmV9pwe8UZaK5eC4
Svxm19jHT5QqloDaZVUmMXFKyKoqPDdfvcDk2Eb5gMfIIb0a3TPC/jqqpDn9BzuH
TO02fuRvRR/G/HUz2yRd+A==
-----END PRIVATE KEY-----
```

9. Enter certificates of certification authorities (CA) which form the certificate chain of the server certificate.

   This starts with the issuing CA certificate of the server certificate and can range up to the root CA certificate.

```
Do you want to continue entering root and/or intermediate certificates
{y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.

The installed certificate's CA and serial number for reference:
CA: cache-164g-svm-root-ca
serial: 187A256E0BF90CFA
```

10. Get the public key for the SVM root CA:

```
security certificate show -vserver <svm> -common-name <root_ca_cn> -ca
<root_ca_cn> -type root-ca -instance

-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIIGHokTnbsHKEwDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMWY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjE1NTIzWhcNMjYxMTIxMjE1NTIzWjAuMR8wHQYDVQQDExZjYWNoZS0xNjRnLXN2
bS1yb290LWNhMQswCQYDVQQGEwJVUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
...
DoOL7vZFFt44xd+rp0DwafhSnLH5HNhdIAfa2JvZW+eJ7rgevH9wmOzyc1vaihl3
Ewtb6cz1a/mtESSYRNBmGkIGM/SFCy5v1ROZXCzF96XPbYQN4cW0AYI3AHYBZP0A
HlNzDR8iml4k9IuKf6BHLFA+VwLTJJZKrdf5Jvjgh0trGAbQGI/Hp2Bjuiopkui+
n4aa5Rz0JFQopqQddAYnMuvcq10CyNn7S0vF/XLd3fJaprH8kQ==
-----END CERTIFICATE-----
```

This is needed to configure the client to trust the certificates signed by the SVM root-ca. The public key is printed to the console. Copy and save the public key. The values in this command are the same ones you entered in Create an SVM root CA.

Step 2: Configure the S3 server

1. Enable S3 protocol access:

```
vserver show -vserver <svm> -fields allowed-protocols
```

S3 is allowed at the SVM level by default.

2. Clone an existing policy:

```
network interface service-policy clone -vserver <svm> -policy default-
data-files -target-vserver <svm> -target-policy <any_name>
```

3. Add S3 to the cloned policy:

   ```
   network interface service-policy add-service -vserver <svm> -policy
   <any_name> -service data-s3-server
   ```

4. Add the new policy to the data lif:

   ```
   network interface modify -vserver <svm> -lif <data_lif> -service-policy
   duality
   ```

   Modifying the service policy of an existing LIF can be disruptive. It requires the LIF to be taken down and brought back up with a listener for the new service. TCP **should** recover from this quickly, but be aware of potential impact.

5. Create the S3 object store server on the SVM:

   ```
   vserver object-store-server create -vserver <svm> -object-store-server
   <dns_name_of_data_lif> -certificate-name flexcache-duality
   ```

6. Enable S3 capability on FlexCache volume:

   The `flexcache config` option `-is-s3-enabled` must be set to `true` before you can create a bucket. You must also set the option `-is-writeback-enabled` to `false`.

   The following command modifies an existing FlexCache:

   ```
   flexcache config modify -vserver <svm> -volume <fcache_vol> -is
   -writeback-enabled false -is-s3-enabled true
   ```

7. Create an S3 bucket:

   ```
   vserver object-store-server bucket create -vserver <svm> -bucket
   <bucket_name> -type nas -nas-path <flexcache_junction_path>
   ```

8. Create a bucket policy:

```
vserver object-store-server bucket policy add-statement -vserver <svm>
-bucket <bucket_name> -effect allow
```

9. Create an S3 user:

```
vserver object-store-server user create -user <user> -comment ""
```

Example output:

```
    Vserver: <svm>>
       User: <user>>
 Access Key: WCOT7...Y7D6U
 Secret Key: 6143s...pd__P
    Warning: The secret key won't be displayed again. Save this key for
future use.
```

10. Regenerate keys for the root user:

```
vserver object-store-server user regenerate-keys -vserver <svm> -user
root
```

Example output:

```
    Vserver: <svm>>
       User: root
 Access Key: US791...2F1RB
 Secret Key: tgYmn...8_3o2
    Warning: The secret key won't be displayed again. Save this key for
future use.
```

Step 3: Set up the client

There are many S3 clients available. A good place to start is with the AWS CLI. For more information, see Installing the AWS CLI.

Copyright information

Trademark information