FlexCache の二重性

ONTAP 9

NetApp
February 05, 2026

目次

FlexCache の二重性

FlexCache の二重性に関するよくある質問

このFAQでは、ONTAP 9.18.1で導入されたFlexCacheデュアリティに関するよくある質問にお答えします。

よくある質問

「二重性」とは何でしょうか？

Duality により、ファイル（NAS）プロトコルとオブジェクト（S3）プロトコルの両方を使用して同じデータへの統合アクセスが可能になります。ONTAP 9.12.1でFlexCacheサポートなしで導入されたduality は、ONTAP 9.18.1でFlexCacheボリュームを含むように拡張され、FlexCacheボリュームにキャッシュされたNASファイルへのS3プロトコル アクセスが可能になりました。

FlexCache S3 バケットでサポートされている **S3** 操作は何ですか？

標準S3 NASバケットでサポートされているS3操作は、FlexCache S3 NASバケットでサポートされていますが、 `COPY`操作は除きます。標準S3 NASバケットでサポートされていない操作の最新リストについては、"相互運用性ドキュメント"を参照してください。

FlexCache デュアリティで **FlexCache** をライトバック モードで使用できますか。

いいえ。FlexCache S3 NASバケットがFlexCacheボリュームに作成される場合、FlexCacheボリュームはライトアラウンドモードになっている*必要があります*。FlexCache S3 NASバケットをライトバックモードのFlexCacheボリュームに作成しようとすると、操作は失敗します。

ハードウェアの制限により、クラスタの **1** つを **ONTAP 9.18.1** にアップグレードできません。キャッシュクラスタのみが **ONTAP 9.18.1** を実行している場合でも、クラスタ内で二重性は機能しますか？

いいえ。キャッシュ クラスターとオリジン クラスターの両方で、最低有効クラスター バージョンは 9.18.1 である必要があります。9.18.1 より前の ONTAP バージョンを実行しているオリジンとピア接続されたキャッシュ クラスターで FlexCache S3 NAS バケットを作成しようとすると、操作は失敗します。

私は**MetroCluster**構成を持っています。**FlexCache**デュアリティを使用できますか？

いいえ。FlexCache の二重性は MetroCluster 構成ではサポートされていません。

FlexCache S3 NAS バケット内のファイルへの **S3** アクセスを監査できますか？

S3監査は、FlexCacheボリュームが使用するNAS監査機能によって提供されます。FlexCacheボリュームのNAS監査の詳細については、"FlexCache 監査の詳細"を参照してください。

キャッシュ クラスタが元のクラスタから切断された場合、何が起こるでしょうか？

FlexCache S3 NASバケットへのS3リクエストは、キャッシュ クラスターが元のクラスターから切断されている場合、 `503 Service Unavailable`エラーで失敗します。

マルチパート **S3** オペレーションを **FlexCache** デュアリティで使用できますか？

マルチパートS3オペレーションが機能するには、基盤となるFlexCacheボリュームのgranular-dataフィールドを「advanced」に設定する必要があります。このフィールドは、元のボリュームに設定されている値に設定されます。

FlexCache の二重性は **HTTP** および **HTTPS** アクセスをサポートしますか？

はい。デフォルトでは、HTTPS が必須です。必要に応じて、HTTP アクセスを許可するように S3 サービスを設定できます。

NAS FlexCache ボリュームへのS3アクセスを有効にする

ONTAP 9.18.1以降では、NAS FlexCacheボリュームへのS3アクセスを有効にすることができます。これは「デュアリティ」とも呼ばれます。これにより、クライアントは、NFSやSMBなどの従来のNASプロトコルに加えて、S3プロトコルを使用してFlexCacheボリュームに格納されたデータにアクセスできます。以下の情報を使用して、FlexCacheデュアリティを設定できます。

前提条件

開始する前に、次の前提条件を満たしていることを確認する必要があります：

- S3 プロトコルと必要な NAS プロトコル（NFS、SMB、またはその両方）が SVM でライセンスされ、設定されていることを確認します。
- DNS およびその他の必要なサービスが設定されていることを確認します。
- クラスタと SVM のピア関係を確立
- FlexCache ボリュームの作成
- データ LIF が作成されました

FlexCache の二重性に関するより詳細なドキュメントについては、"ONTAP S3 マルチプロトコル サポート"を参照してください。

ステップ1：証明書を作成して署名する

S3アクセスをFlexCacheボリュームに対して有効にするには、FlexCacheボリュームをホストするSVMの証明書をインストールする必要があります。この例では自己署名証明書を使用していますが、本番環境では、信頼できる証明機関（CA）によって署名された証明書を使用する必要があります。

1. SVM ルート CA を作成します：

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

2. 証明書署名要求を生成する：

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

出力例：

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

秘密鍵の例：

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

ⓘ 将来の参照用に証明書要求と秘密キーのコピーを保管してください。

3. 証明書に署名します：

`root-ca`は、<<anchor1-step,SVMルートCAを作成する>>で作成したものです。

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

4. 証明書署名要求を生成するで生成された証明書署名要求（CSR）を貼り付けます。

例：

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

これにより、次の例のように、署名された証明書がコンソールに出力されます。

署名された証明書の例：

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

5. 次のステップのために証明書をコピーします。
6. SVM にサーバー証明書をインストールします：

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

7. 証明書に署名するから署名された証明書を貼り付けます。

   例：

```
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. 証明書署名要求を生成するで生成された秘密鍵を貼り付けます。

   例：

```
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. サーバー証明書の証明書チェーンを形成する認証局（CA）の証明書を入力します。

   これは、サーバー証明書の発行 CA 証明書から始まり、ルート CA 証明書までの範囲になります。

```
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. SVM ルート CA の公開キーを取得します：

```
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-----
```

これは、SVM ルート CA によって署名された証明書をクライアントが信頼するように設定するために必要です。公開鍵はコンソールに表示されます。公開鍵をコピーして保存します。このコマンドの値は、SVMルートCAを作成するで入力したものと同じです。

ステップ2：S3サーバーを構成する

1. S3 プロトコル アクセスを有効にする：

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

デフォルトでは、S3 は SVM レベルで許可されます。

2. 既存のポリシーを複製します：

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

3. クローンされたポリシーに S3 を追加します：

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

4. 新しいポリシーをデータ LIF に追加します：

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

> 既存の LIF のサービス ポリシーを変更すると、混乱が生じる可能性があります。LIF を停止し、新しいサービスのリスナーを使用して再起動する必要があります。TCP はすぐに回復するはずですが、潜在的な影響に注意してください。

5. SVM 上に S3 オブジェクト ストア サーバーを作成します：

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

6. FlexCacheボリュームでS3機能を有効にする：

`flexcache config`オプション `-is-s3-enabled`を`true`に設定してから、バケットを作成する必要があります。また、 `-is-writeback-enabled`オプションを `false`に設定する必要があります。

次のコマンドは、既存のFlexCacheを変更します：

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

7. S3 バケットを作成します：

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

8. バケットポリシーを作成します：

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

9. S3ユーザを作成します。

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

出力例：

```
    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. ルートユーザーのキーを再生成します：

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

出力例：

```
    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.
```

ステップ3：クライアントを設定する

利用可能な S3 クライアントは多数あります。始めるには AWS CLI が適しています。詳細については、"AWS CLI のインストール"を参照してください。

著作権に関する情報

商標に関する情報