FlexCache 二元性

ONTAP 9

NetApp
February 05, 2026

目录

FlexCache 二元性

关于 FlexCache 二元性的常见问题

此常见问题解答回答了有关 ONTAP 9.18.1 中引入的 FlexCache 二元性的常见问题。

常见问题解答

什么是"二元性"?

Duality 支持使用文件 (NAS) 和对象 (S3) 协议统一访问相同的数据。在 ONTAP 9.12.1 中引入时不支持 FlexCache，duality 在 ONTAP 9.18.1 中得到扩展以包括 FlexCache 卷，允许 S3 协议访问 FlexCache 卷中缓存的 NAS 文件。

在 **FlexCache S3** 存储桶上支持哪些 **S3** 操作?

标准 S3 NAS 存储区上支持的 S3 操作在 FlexCache S3 NAS 存储区上受支持，但 `COPY` 操作除外。有关标准 S3 NAS 存储区不支持的操作的最新列表，请访问 "互操作性文档"。

我可以在具有 **FlexCache** 二元性的回写模式下使用 **FlexCache** 吗?

不可以。如果在 FlexCache 卷上创建了 FlexCache S3 NAS 存储桶，则该 FlexCache 卷*必须*处于写入绕过模式。如果尝试在回写模式的 FlexCache 卷上创建 FlexCache S3 NAS 存储桶，则操作将失败。

由于硬件限制，我无法将其中一个集群升级到 **ONTAP 9.18.1**。如果只有缓存集群运行 **ONTAP 9.18.1**，我的集群中的双重性是否仍然有效?

否。缓存集群和原始集群都必须具有最低有效集群版本 9.18.1。如果尝试在缓存集群上创建一个 FlexCache S3 NAS 存储桶，该集群与运行早于 9.18.1 的 ONTAP 版本的原始集群对等，则操作将失败。

我有 **MetroCluster** 配置。我可以使用 **FlexCache** 二元性吗?

不，MetroCluster 配置中不支持 FlexCache 的双重性。

我可以审核 **S3** 对 **FlexCache S3 NAS** 存储桶中文件的访问权限吗?

S3 审核由 NAS 审核功能 FlexCache 卷使用提供。有关 FlexCache 卷的 NAS 审核的详细信息，请参见 "详细了解 FlexCache 审核"。

如果缓存集群与原始集群断开连接，我应该期待什么?

如果缓存集群与原始集群断开连接，则对 FlexCache S3 NAS 存储桶的 S3 请求将失败并出现 `503 Service Unavailable`错误。

我可以将多部分 **S3** 操作与 **FlexCache** 双重性一起使用吗?

要使多部分 S3 操作正常工作，底层 FlexCache 卷必须将 granular-data 字段设置为 'advanced'。此字段设置为源卷设置的任何值。

FlexCache 双重性是否支持 **HTTP** 和 **HTTPS** 访问?

是。默认情况下，HTTPS 是必需的。如果需要，您可以将 S3 服务配置为允许 HTTP 访问。

启用 S3 对 NAS FlexCache 卷的访问

从 ONTAP 9.18.1 开始，您可以启用 S3 对 NAS FlexCache 卷的访问，也称为"双重性"。

这允许客户端使用 S3 协议访问存储在 FlexCache 卷中的数据，以及 NFS 和 SMB 等传统 NAS 协议。您可以使用以下信息设置 FlexCache 双重性。

前提条件

在开始之前，您必须确保完成以下先决条件：

- 确保在 SVM 上许可并配置了 S3 协议和所需的 NAS 协议（NFS、SMB 或两者）。
- 验证是否已配置 DNS 和任何其他必需服务。
- 集群和 SVM 已建立对等关系
- FlexCache 卷创建
- 已创建 Data-lif

有关 FlexCache 二元性的更全面的文档，请参见 "ONTAP S3 多协议支持"。

步骤 1：创建并签署证书

要启用对 FlexCache 卷的 S3 访问，需要为托管 FlexCache 卷的 SVM 安装证书。此示例使用自签名证书，但在生产环境中，应使用由受信任的证书颁发机构 (CA) 签名的证书。

1. 创建 SVM 根 CA：

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

2. 生成证书签名请求：

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

输出示例：

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

私钥示例：

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

保留证书请求和私钥的副本，以备将来参考。

3. 签署证书：

`root-ca` 是您在 <<anchor1-step,创建 SVM 根 CA>> 中创建的。

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

4. 粘贴在 生成证书签名请求 中生成的证书签名请求 (CSR)。

示例

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

此操作会将签名证书打印到控制台，类似于以下示例。

签名证书示例：

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

5. 复制证书以供下一步使用。
6. 在 SVM 上安装服务器证书：

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

7. 从 签署证书 粘贴签名的证书。

   示例

```
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. 粘贴在 生成证书签名请求 中生成的专用密钥。

   示例

```
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. 输入构成服务器证书的证书链的证书颁发机构 (CA) 的证书。

   这从颁发服务器证书的 CA 证书开始，范围可达根 CA 证书。

```
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. 获取 SVM 根 CA 的公钥：

```
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-----
```

这是配置客户端信任由 SVM root-ca 签名的证书所必需的。公钥会输出到控制台。复制并保存公钥。此命令中的值与您在 创建 SVM 根 CA 中输入的值相同。

步骤 2：配置 S3 服务器

1. 启用 S3 协议访问：

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

默认情况下，S3 在 SVM 级别是允许的。

2. 克隆现有策略：

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

3. 将 S3 添加到已克隆的策略：

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

4. 将新策略添加到 data lif：

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

修改现有 LIF 的服务策略可能会造成中断。它要求将 LIF 取下，并使用新服务的侦听器重新启动。TCP *应该*能够快速从中恢复，但要注意潜在的影响。

5. 在 SVM 上创建 S3 对象存储服务器：

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

6. 在 FlexCache 卷上启用 S3 功能：

   该 `flexcache config`选项 `-is-s3-enabled`必须设置为 `true`，然后才能创建存储桶。您还必须将选项 `-is-writeback-enabled`设置为 `false`。

   以下命令将修改现有 FlexCache：

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

7. 创建 S3 存储桶：

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

8. 创建存储桶策略：

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

9. 创建 S3 用户：

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

   输出示例：

```
    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. 为 root 用户重新生成密钥：

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

输出示例：

```
    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.
```

步骤 3：设置客户端

有许多 S3 客户端可用。AWS CLI 是一个很好的起点。有关详细信息，请参见 "安装 AWS CLI"。