



Management von FlexCache Volumes

ONTAP 9

NetApp
February 05, 2026

Inhalt

Management von FlexCache Volumes	1
Weitere Informationen zu ONTAP FlexCache Volumes	1
Videos	1
Unterstützte und nicht unterstützte Funktionen für ONTAP FlexCache Volumes	3
Unterstützung der ONTAP Version zwischen FlexCache Volumes und Ursprungs-Volumes	3
Unterstützte Protokolle	3
Unterstützte Funktionen	4
Richtlinien für die Größenbestimmung von ONTAP FlexCache Volumes	9
Erstellen Sie ONTAP FlexCache Volumes	9
FlexCache Write-Back	15
Erfahren Sie mehr über ONTAP FlexCache Write-Back	15
ONTAP FlexCache-Rückschreibrichtlinien	16
ONTAP FlexCache Write-Back-Architektur	18
Anwendungsfälle für die ONTAP FlexCache-Rückschreibung	22
Voraussetzungen für die ONTAP FlexCache-Zurückschreibung	24
Interoperabilität von ONTAP FlexCache-Schreibvorgängen	25
Aktivieren und Verwalten von ONTAP FlexCache Write-Back	26
Häufig gestellte Fragen zum ONTAP FlexCache-Rückschreiben	30
FlexCache-Dualität	31
Häufig gestellte Fragen zur FlexCache-Dualität	31
S3-Zugriff auf NAS-FlexCache-Volumes aktivieren	32
Managen Sie FlexCache Volumes	39
Erfahren Sie mehr über Auditing von ONTAP FlexCache Volumes	39
Synchronisieren der Eigenschaften eines ONTAP FlexCache-Volumes von einem Ursprungs-Volume ..	40
Aktualisieren Sie die Konfiguration von ONTAP FlexCache Beziehungen	41
Aktivieren Sie die Updates für die Dateizugriffszeit auf dem ONTAP FlexCache Volume	41
Globale Dateisperre auf ONTAP FlexCache Volumes	43
ONTAP FlexCache Volumes werden vorab befüllt	44
Löschen Sie ONTAP FlexCache Beziehungen	45
FlexCache für die Behebung von Hotspots	46
Beseitigung von Hot-Spotting bei hochperformanten Computing-Workloads mit ONTAP FlexCache	
Volumes	46
Architektur einer Lösung zur Behebung von ONTAP FlexCache-Hotspots	47
ONTAP FlexCache-Dichte ermitteln	50
Bestimmen Sie eine ONTAP-interne oder SVM-interne HDFA-Option	53
Konfiguration der Datenschnittstellen HDFAs und ONTAP	54
Konfigurieren Sie Clients für die Verteilung von ONTAP NAS-Verbindungen	57

Management von FlexCache Volumes

Weitere Informationen zu ONTAP FlexCache Volumes

Die NetApp FlexCache Technologie beschleunigt den Datenzugriff, reduziert WAN-Latenzen und senkt die Kosten für die WAN-Bandbreite bei leseintensiven Workloads, insbesondere, wenn die Kunden wiederholt auf dieselben Daten zugreifen müssen. Wenn Sie ein FlexCache Volume erstellen, erstellen Sie einen Remote-Cache eines bereits vorhandenen (Ursprungs-)Volumes, der nur die Daten enthält, auf die aktiv zugegriffen wird (wichtige Daten) des Ursprungs-Volume.

Wenn ein FlexCache Volume eine Leseanfrage der enthaltenen heißen Daten erhält, kann es schneller reagieren als das Ursprungs-Volume, da die Daten nicht so weit reisen müssen, bis zum Kunden. Wenn ein FlexCache Volume eine Leseanfrage für selten gelesene Daten (kalte Daten) erhält, ruft es die erforderlichen Daten vom Ursprungs-Volume ab und speichert diese dann, bevor es der Client-Anforderung dient. Nachfolgende Leseanforderungen werden dann direkt vom FlexCache Volume bedient. Nach der ersten Anfrage müssen die Daten nicht mehr über das Netzwerk übertragen oder von einem stark ausgelasteten System bedient werden. Angenommen, Sie haben Engpässe innerhalb Ihres Clusters an einem einzelnen Zugriffspunkt für häufig angeforderte Daten. FlexCache Volumes innerhalb des Clusters können mehrere Mount-Punkte für die heißen Daten bereitstellen, wodurch Engpässe reduziert und die Performance gesteigert werden. Ein weiteres Beispiel: Angenommen, Sie müssen den Netzwerk-Traffic auf ein Volume reduzieren, auf das von mehreren Clustern zugegriffen wird. Mit FlexCache Volumes können häufig benötigte Daten aus dem Ursprungs-Volume über die Cluster im Netzwerk verteilt werden. Dadurch wird der WAN-Datenverkehr reduziert, da Benutzer näher auf die Access Points zugreifen können.

Mit FlexCache Technologie lässt sich darüber hinaus die Performance in Cloud- und Hybrid-Cloud-Umgebungen steigern. Ein FlexCache Volume kann Sie dabei unterstützen, Workloads in die Hybrid Cloud zu migrieren, indem Sie Daten von einem lokalen Datacenter in die Cloud zwischenspeichern. Sie können FlexCache Volumes auch einsetzen, um Cloud-Silos zu entfernen, indem Sie die Daten von einem Cloud-Provider im Cache bei einem anderen oder zwischen zwei Regionen desselben Cloud-Providers zwischenspeichern.

Ab ONTAP 9.10.1 sind ["Globale Dateisperre aktivieren"](#) alle FlexCache Volumes übergreifend möglich. Die globale Dateisperre verhindert, dass ein Benutzer auf eine Datei zugreift, die bereits von einem anderen Benutzer geöffnet wurde. Updates des Ursprungs-Volume werden dann gleichzeitig auf alle FlexCache Volumes verteilt.

Ab ONTAP 9.9 pflegen FlexCache Volumes eine Liste mit nicht gefundenen Dateien. Dadurch wird der Netzwerkverkehr reduziert, da bei der Suche von Clients nach nicht vorhandenen Dateien mehrere Anrufe an den Ursprung gesendet werden müssen.

Eine Liste der zusätzlichen ["Funktionen, die für FlexCache Volumes und deren Ursprungs-Volumes unterstützt werden"](#), einschließlich einer Liste der unterstützten Protokolle von ONTAP-Version, ist ebenfalls verfügbar.

Mehr über die Architektur der ONTAP FlexCache-Technologie erfahren Sie in ["TR-4743: FlexCache im ONTAP"](#).

Videos

So kann FlexCache die WAN-Latenz verringern und die Lesezeiten für globale Daten verkürzen

ONTAP FlexCache
Data Access Where You Need It

Use Case

© 2020 NetApp, Inc. All rights reserved.

NetApp



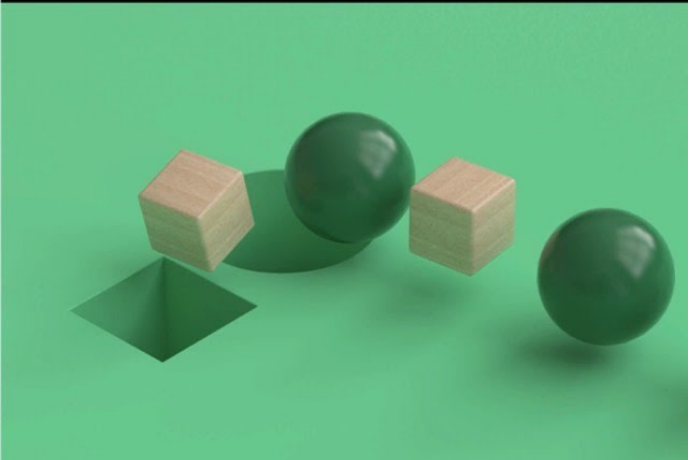
Erfahren Sie mehr über die Performance-Vorteile von ONTAP FlexCache!

ONTAP FlexCache
Data Access Where You Need It

Tech Clip

© 2020 NetApp, Inc. All rights reserved.

NetApp



Unterstützte und nicht unterstützte Funktionen für ONTAP FlexCache Volumes

Ab ONTAP 9.5 können Sie FlexCache Volumes konfigurieren. FlexVol Volumes werden als Ursprungs-Volumes unterstützt, FlexGroup Volumes werden als FlexCache Volumes unterstützt. Ab ONTAP 9.7 werden sowohl FlexVol Volumes als auch FlexGroup Volumes als Ursprungs-Volumes unterstützt. Die unterstützten Funktionen und Protokolle für das Ursprungs-Volume und das FlexCache Volume variieren.



Cache-Volumes und Ursprungs-Volumes können zusammenarbeiten, sofern beide auf einer unterstützten Version von ONTAP ausgeführt werden. Beachten Sie, dass Funktionen nur unterstützt werden, wenn sowohl der Cache als auch der Ursprung mindestens die ONTAP Version ausführen, auf der Unterstützung eingeführt wurde, oder eine neuere ONTAP Version.

Unterstützung der ONTAP Version zwischen FlexCache Volumes und Ursprungs-Volumes

Die empfohlene ONTAP-Version, die zwischen dem Ursprungs-Volume und dem Cache-Volume unterstützt wird, beträgt maximal vier Versionen vor oder vier Versionen später. Wenn im Cache beispielsweise ONTAP 9.14.1 verwendet wird, ist die früheste Version, die vom Ursprung verwendet werden kann, ONTAP 9.10.1.


Unterstützte Protokolle


Protokoll	Unterstützung auf dem Ursprungs-Volume?	Unterstützung auf dem FlexCache Volume?
NFSv3	Ja.	Ja.
NFSv4	Ja. Für den Zugriff auf Cache-Volumes mit dem NFSv4.x-Protokoll müssen sowohl der Ursprungs- als auch der Cache-Cluster ONTAP 9.10.1 oder höher verwenden. Der Ursprungs-Cluster und der FlexCache-Cluster können unterschiedliche ONTAP-Versionen aufweisen, jedoch sollten beide Versionen ONTAP 9.10.1 und höher sein, beispielsweise kann der Ursprung ONTAP 9.10.1 aufweisen, und der Cache kann ONTAP 9.11.1 aufweisen.	Ja. Unterstützt ab ONTAP 9.10.1. Für den Zugriff auf Cache-Volumes mit dem NFSv4.x-Protokoll müssen sowohl der Ursprungs- als auch der Cache-Cluster ONTAP 9.10.1 oder höher verwenden. Der Ursprungs-Cluster und der FlexCache-Cluster können unterschiedliche ONTAP-Versionen aufweisen, jedoch sollten beide Versionen ONTAP 9.10.1 und höher sein, beispielsweise kann der Ursprung ONTAP 9.10.1 aufweisen, und der Cache kann ONTAP 9.11.1 aufweisen.
NFSv4.2	Ja.	Nein


SMB	Ja.	Ja. Unterstützt ab ONTAP 9.8.
-----	-----	--------------------------------------

Unterstützte Funktionen

Funktion	Unterstützung auf dem Ursprungs-Volume?	Unterstützung auf dem FlexCache Volume?
Autonomer Ransomware-Schutz	Ja. Ab ONTAP 9.10.1 wird es für FlexVol Ursprungs-Volumes unterstützt und ab ONTAP 9.13.1 für FlexGroup Ursprungs-Volumes unterstützt. Siehe "Anwendungsfälle und Überlegungen zum autonomen Ransomware-Schutz" .	Nein
Virenschutz	Ja. Unterstützt ab ONTAP 9.7.	Keine Angabe Wenn Sie die Virenprüfung am Ursprung konfigurieren, ist sie im Cache nicht erforderlich. Die ursprüngliche (Antiviren-) Virenschutzprüfung erkennt Dateien, die mit Viren infiziert sind, bevor die Schreibvorgänge durchgeführt werden, und zwar unabhängig von der Datenquelle. Weitere Informationen zur Verwendung von Virenschutzprüfungen mit FlexCache finden Sie im "Technischer Bericht: FlexCache with ONTAP" .
Prüfung	Ja. Unterstützt ab ONTAP 9.7. Mithilfe nativer ONTAP-Prüfung können Sie NFS-Dateizugriffe in FlexCache Beziehungen prüfen. Weitere Informationen finden Sie unter Überlegungen für das Auditing von FlexCache Volumes	Ja. Unterstützt ab ONTAP 9.7. Mithilfe nativer ONTAP-Prüfung können Sie NFS-Dateizugriffe in FlexCache Beziehungen prüfen. Weitere Informationen finden Sie unter Überlegungen für das Auditing von FlexCache Volumes
Cloud Volumes ONTAP	Ja. Unterstützt ab ONTAP 9.6	Ja. Unterstützt ab ONTAP 9.6

Datenverdichtung	Ja. Unterstützt ab ONTAP 9.6	Ja. Unterstützt ab ONTAP 9.7
Komprimierung	Ja. Unterstützt ab ONTAP 9.6	Ja. Unterstützt ab ONTAP 9.6
Deduplizierung	Ja.	Ja. Die Inline-Deduplizierung wird auf FlexCache Volumes ab ONTAP 9.6 unterstützt. Die Volume-übergreifende Deduplizierung wird auf FlexCache Volumes ab ONTAP 9.7 unterstützt.
FabricPool	Ja.	Ja. Unterstützt ab ONTAP 9.7 <div>  <p>Sie können ein FlexCache Volume als Cache für ein Ursprungsvolume erstellen, bei dem FabricPool Tiering aktiviert ist, aber das FlexCache Volume selbst kann nicht getiert werden.</p> </div>
FlexCache DR	Ja.	Ja. Unterstützt ab ONTAP 9.9.1, nur mit NFSv3-Protokoll FlexCache Volumes müssen sich in separaten SVMs oder in separaten Clustern liegen.
FlexGroup Volume	Ja. Unterstützt ab ONTAP 9.7	Ja.
FlexVol Volume	Ja.	Nein

FPolicy	Ja. Unterstützt ab ONTAP 9.7	Ja. Unterstützt für NFS ab ONTAP 9.7. Unterstützt für SMB ab ONTAP 9.14.1.
MetroCluster-Konfiguration	Ja. Unterstützt ab ONTAP 9.7	Ja. Unterstützt ab ONTAP 9.7
Microsoft Offloaded Data Transfer (ODX)	Ja.	Nein
NetApp Aggregatverschlüsselung (NAE)	Ja. Unterstützt ab ONTAP 9.6	Ja. Unterstützt ab ONTAP 9.6
NetApp Volume Encryption (NVE)	Ja. Unterstützt ab ONTAP 9.6	Ja. Unterstützt ab ONTAP 9.6
ONTAP S3 NAS-Bucket	Ja. Unterstützt ab ONTAP 9.12.1	Ja. Unterstützt ab ONTAP 9.18.1
QoS	Ja.	Ja.  QoS auf Dateiebene wird für FlexCache Volumes nicht unterstützt.
Qtrees	Ja. Ab ONTAP 9.6 können Sie qtrees erstellen und ändern. Auf der Quelle erstellte qtrees können im Cache zugegriffen werden.	Nein

Kontingente	<p>Ja.</p> <p>Ab ONTAP 9.6 wird die Kontingentdurchsetzung auf FlexCache Ursprungs-Volumes für Benutzer, Gruppen und qtrees unterstützt.</p>	<p>Nein</p> <p>Im FlexCache-Schreibmodus (Standardmodus) werden Schreibvorgänge im Cache an das Ursprungs-Volumen weitergeleitet. Quotas werden am Ursprung durchgesetzt.</p> <div>  <p>Ab ONTAP 9.6 wird Remote Quoten (rquota) auf FlexCache Volumen unterstützt.</p> </div>
SMB Change Notify	<p>Ja.</p>	<p>Ja.</p> <p>Ab ONTAP 9.14.1 wird SMB Change Notify im Cache unterstützt.</p>
SnapLock Volumes	<p>Nein</p>	<p>Nein</p>
Asynchrone Beziehungen von SnapMirror*	<p>Ja.</p>	<p>Nein</p>
	<p>*FlexCache Origins:</p> <ul style="list-style-type: none"> • Sie können ein FlexCache Volume von einer Ursprungs-FlexVol verwenden • Sie können ein FlexCache Volume von einer Ursprungs-FlexGroup verwenden • Sie können ein FlexCache Volume aus einem ursprünglichen primären Volume in der SnapMirror Beziehung haben. • Ab ONTAP 9.8 kann ein sekundäres SnapMirror Volume ein Ursprungs-Volumen von FlexCache sein. Das sekundäre SnapMirror Volume muss sich ohne aktive SnapMirror Updates im Ruhezustand befinden, ansonsten schlägt die FlexCache-Erstellung fehl. 	<p>Synchrone SnapMirror Beziehungen</p>

Nein	Nein	SnapRestore
Ja.	Nein	Snapshots
Ja.	Nein	SVM DR-Konfiguration
<p>Ja.</p> <p>Unterstützt ab ONTAP 9.5. Die primäre SVM einer SVM-DR-Beziehung kann das Ursprungsvolume haben; wenn Sie jedoch eine ONTAP Version vor ONTAP 9.18.1 verwenden, muss die FlexCache Beziehung mit einem neuen Ursprungsvolume neu erstellt werden, wenn die SVM-DR-Beziehung unterbrochen wird.</p> <p>Ab ONTAP 9.18.1 werden die Caches bei einem Failover des Ursprungs-SVM automatisch auf den Ursprung am DR-Standort umgeschaltet. Manuelle Wiederherstellungsschritte entfallen.</p> <p>Erfahren Sie mehr über die Erstellung von FlexCache-Volumes.</p>	<p>Nein</p> <p>Sie können FlexCache Volumes in primären SVMs, nicht aber in sekundären SVMs vorhanden sein. Alle FlexCache Volumes in der primären SVM werden nicht als Teil der SVM-DR-Beziehung repliziert.</p>	Storage-Level Access Guard (SCHLACKE)
Nein	Nein	Thin Provisioning
Ja.	<p>Ja.</p> <p>Unterstützt ab ONTAP 9.7</p>	Klonen von Volumes
<p>Ja.</p> <p>Das Klonen eines Ursprungs-Volumes und der Dateien im Ursprungs-Volume wird ab ONTAP 9.6 unterstützt.</p>	Nein	Volume-Verschiebung
Ja.	<p>Ja (nur für Volumenkomponenten)</p> <p>Das Verschieben von Volume-Komponenten eines FlexCache Volumes wird von ONTAP 9.6 und höher unterstützt.</p>	Volume-Rehosting

Nein	Nein	VStorage API für Array Integration (VAAI)
------	------	---



In ONTAP 9 Versionen vor 9.5 können Ursprungs-FlexVol-Volumes nur Daten für FlexCache Volumes bereitstellen, die auf Systemen mit Data ONTAP 8.2.x im 7-Mode erstellt wurden. Ab ONTAP 9.5 können Ursprungs-FlexVol Volumes auch Daten für FlexCache Volumes auf ONTAP 9 Systemen bereitstellen. Informationen zur Migration von 7-Mode FlexCache zu ONTAP 9 FlexCache finden Sie unter ["Technischer Bericht 4743 zu NetApp: FlexCache in ONTAP"](#).

Richtlinien für die Größenbestimmung von ONTAP FlexCache Volumes

Die Limits für FlexCache Volumes müssen Sie beachten, bevor Sie mit der Bereitstellung der Volumes beginnen.

Die Größenbegrenzung eines FlexVol Volume gilt für ein Ursprungs-Volume. Die Größe eines FlexCache-Volumes kann kleiner als oder gleich dem Ursprungsvolumen sein. Als Best Practice für die Größe eines FlexCache-Volumes sollten mindestens 10 Prozent der Größe des Ursprungs-Volumes betragen.

Außerdem müssen Sie die folgenden zusätzlichen Limits für FlexCache Volumes beachten:

Grenze	ONTAP 9.8 und höher	ONTAP 9,7	ONTAP 9.6 – 9.5
Maximale Anzahl an FlexCache Volumes, die Sie aus einem Ursprungs-Volume erstellen können	100	10	10
Empfohlene maximale Anzahl an Ursprungs-Volumes pro Node	100	100	10
Empfohlene maximale Anzahl von FlexCache Volumes pro Node	100	100	10
Empfohlene maximale Anzahl an FlexGroup-Komponenten in einem FlexCache Volume pro Node	800	800	40
Maximale Anzahl an Komponenten pro FlexCache-Volume pro Node	32	32	32

Verwandte Informationen

- ["NetApp Interoperabilität"](#)

Erstellen Sie ONTAP FlexCache Volumes

Sie können ein FlexCache Volume im selben ONTAP-Cluster erstellen, um die Performance beim Zugriff auf ein häufig genutztes Objekt zu verbessern. Wenn Sie Rechenzentren an verschiedenen Standorten haben, können Sie FlexCache Volumes auf entfernten ONTAP-Clustern erstellen, um den Datenzugriff zu beschleunigen.

Über diese Aufgabe

- Ab ONTAP 9.18.1 können Sie den NAS S3-Bucket-Zugriff auf einem FlexCache Volume aktivieren, indem Sie die `-is-s3-enabled` Option auf `true` setzen, wenn Sie das Volume erstellen. Diese Option ist standardmäßig deaktiviert.
- Ab ONTAP 9.18.1 unterstützt FlexCache das Erstellen von Cache-Volumes für Ursprungsvolumes mit SVMs, die zu einer SVM-DR-Beziehung gehören.

Wenn Sie ONTAP 9.18.1 oder höher verwenden, muss ein Speicheradministrator die Cache-SVMs sowohl mit den primären als auch den sekundären Ursprungs-SVMs, die Teil einer SVM-DR-Beziehung sind, verbinden, bevor Cache-Volumes von Ursprungs-Volumes erstellt werden, die Teil einer SVM-DR-Beziehung sind.

- Ab ONTAP 9.14.0 können Sie ein unverschlüsseltes FlexCache-Volume aus einer verschlüsselten Quelle erstellen.
- Ab ONTAP 9.7 werden sowohl FlexVol Volumes als auch FlexGroup Volumes als Ursprungsvolumes unterstützt.
- Ab ONTAP 9.5 unterstützt FlexCache FlexVol Volumes als Ursprungs-Volumes und FlexGroup Volumes als FlexCache Volumes.

Bevor Sie beginnen

- Sie müssen ONTAP 9.5 oder höher ausführen.
- Wenn Sie ONTAP 9.6 oder früher laufen, müssen Sie ["Fügen Sie eine FlexCache-Lizenz hinzu"](#).

Für ONTAP 9.7 oder höher ist keine FlexCache Lizenz erforderlich. Ab ONTAP 9.7 ist die FlexCache-Funktionalität in ONTAP enthalten und erfordert keine Lizenz oder Aktivierung mehr.





Wenn ein HA-Paar verwendet ["Verschlüsselung von SAS- oder NVMe-Laufwerken \(SED, NSE, FIPS\)"](#), müssen Sie die Anweisungen im Thema ["Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren"](#) für alle Laufwerke innerhalb des HA-Paars befolgen, bevor Sie das System initialisieren (Startoptionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Beispiel 1. Schritte

System Manager

1. Wenn sich das FlexCache Volume in einem anderen ONTAP Cluster als das Ursprungsvolume befindet, erstellen Sie eine Cluster Peer-Beziehung:
 - a. Klicken Sie im lokalen Cluster auf **Schutz > Übersicht**.
 - b. Erweitern Sie **Intercluster Settings**, klicken Sie auf **Add Network Interfaces** und fügen Sie Cluster-Netzwerkschnittstellen hinzu.

Wiederholen Sie diesen Schritt auf dem Remote-Cluster.
 - c. Klicken Sie im Remote-Cluster auf **Schutz > Übersicht**. Klicken Sie  im Abschnitt Cluster Peers auf **Passphrase generieren**.
 - d. Kopieren Sie die generierte Passphrase, und fügen Sie sie in das lokale Cluster ein.
 - e. Klicken Sie im lokalen Cluster unter Cluster Peers auf **Peer Clusters** und führen Sie die lokalen und Remote Cluster aus.
2. SVM-Peer-Beziehung erstellen:

Klicken Sie unter Storage VM Peers auf  und dann auf **Peer Storage VMs**, um die Storage VMs zu Peer-Daten zu erstellen.
3. Wählen Sie **Storage > Volumes**.
4. Wählen Sie **Hinzufügen**.
5. Wählen Sie **More Options** und dann **Add as Cache for a Remote Volume**.



Wenn Sie ONTAP 9.8 oder höher ausführen und QoS deaktivieren oder eine benutzerdefinierte QoS-Richtlinie auswählen möchten, klicken Sie auf **Weitere Optionen**, und wählen Sie dann unter **Speicher und Optimierung Leistungsservicelevel** aus.

CLI

1. Wenn sich das zu erstellende FlexCache Volume in einem anderen Cluster befindet, erstellen Sie eine Cluster-Peer-Beziehung:
 - a. Erstellen Sie auf dem Ziel-Cluster eine Peer-Beziehung mit dem Datensicherheits-Quellcluster:

```
cluster peer create -generate-passphrase -offer-expiration
MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addr
s <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,...|*
-ipospace <ipospace_name>
```

Ab ONTAP 9.6 ist die TLS-Verschlüsselung bei der Erstellung einer Cluster-Peer-Beziehung standardmäßig aktiviert. Die TLS-Verschlüsselung wird für die Cluster-übergreifende Kommunikation zwischen den Ursprungs- und FlexCache Volumes unterstützt. Bei Bedarf können Sie auch die TLS-Verschlüsselung für die Cluster-Peer-Beziehung deaktivieren.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *
```

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: *
Intercluster LIF IP: 192.140.112.101
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.

a. Authentifizierung des Quellclusters im Quellcluster beim Ziel-Cluster:

```
cluster peer create -peer-addr <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addr
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

2. Wenn sich das FlexCache-Volume in einer anderen SVM als der Ursprungs-Volume befindet, erstellen Sie eine SVM-Peer-Beziehung mit flexcache als Applikation:

a. Wenn sich die SVM in einem anderen Cluster befindet, erstellen Sie eine SVM-Berechtigung für die Peering SVMs:

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

Das folgende Beispiel veranschaulicht die Erstellung einer SVM-Peer-Berechtigung, die für alle lokalen SVMs gilt:

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache
```

Warning: This Vserver peer permission applies to all local Vservers.
After that no explicit
"vserver peer accept" command required for Vserver peer relationship
creation request
from peer cluster "cluster2" with any of the local Vservers. Do you
want to continue? {y|n}: y

a. SVM-Peer-Beziehung erstellen:

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. FlexCache Volume erstellen:

```
volume flexcache create -vserver <cache_svm> -volume
<cache_vol_name> -auto-provision-as flexgroup -size <vol_size>
-origin-vserver <origin_svm> -origin-volume <origin_vol_name> -is-s3
-enabled true|false
```

Im folgenden Beispiel wird ein FlexCache Volume erstellt und vorhandene Aggregate für die Bereitstellung automatisch ausgewählt:

```
cluster1::> volume flexcache create -vserver vs_1 -volume fc1 -auto
-provision-as flexgroup -origin-volume vol_1 -size 160MB -origin
-vserver vs_1
[Job 443] Job succeeded: Successful
```

Im folgenden Beispiel wird ein FlexCache Volume erstellt und der Verbindungspfad festgelegt:

```
cluster1::> volume flexcache create -vserver vs34 -volume fc4 -aggr
-list aggr34,aggr43 -origin-volume origin1 -size 400m -junction-path
/fc4
[Job 903] Job succeeded: Successful
```

Das folgende Beispiel ermöglicht den S3-Zugriff auf ein FlexCache Volume:

```
cluster1::> volume flexcache create -vserver vs3 -volume
cache_vs3_vol33 -origin-volume vol33 -origin-vserver vs3 -junction
-path /cache_vs3_vol33 -is-s3-enabled true
```

4. Überprüfen Sie die FlexCache Beziehung vom FlexCache Volume und dem Ursprungs-Volume.

a. Zeigen Sie die FlexCache-Beziehung im Cluster an:

```
volume flexcache show
```

```
cluster1::> volume flexcache show
Vserver Volume      Size      Origin-Vserver Origin-Volume
Origin-Cluster
-----
vs_1      fc1          160MB      vs_1          vol_1
cluster1
```

b. Alle FlexCache-Beziehungen im Ursprungscluster anzeigen:

```
volume flexcache origin show-caches
```

```
cluster::> volume flexcache origin show-caches
Origin-Vserver Origin-Volume  Cache-Vserver  Cache-Volume
Cache-Cluster
-----
vs0            ovol1          vs1            cfg1
clusA
vs0            ovol1          vs2            cfg2
clusB
vs_1           vol_1          vs_1           fc1
cluster1
```

Ergebnis

Das FlexCache Volume wurde erfolgreich erstellt. Clients können das Volume über den Verbindungspfad des FlexCache Volume mounten.

Verwandte Informationen

["Cluster- und SVM-Peering"](#)

FlexCache Write-Back

Erfahren Sie mehr über ONTAP FlexCache Write-Back

Seit ONTAP 9.15.1 ist FlexCache Write-Back ein alternativer Betriebsmodus zum Schreiben in einen Cache. Mit Write-Back kann der Schreibvorgang auf stabilen Storage im Cache übertragen und dem Client bestätigt werden, ohne darauf zu warten, dass die Daten zum Ursprung gebracht werden. Die Daten werden asynchron an den Ursprung zurückgespült. Das Ergebnis ist ein weltweit verteiltes Filesystem, mit dem Schreibvorgänge für spezifische Workloads und Umgebungen mit nahezu lokaler Geschwindigkeit ausgeführt werden können und das mit deutlichen Performance-Vorteilen verbunden ist.



ONTAP 9.12.1 hat eine Write-Back-Funktion als öffentliche Vorschau eingeführt. Dies wird als Write-Back-Version 1 (wbv1) bezeichnet und sollte nicht als Write-Back in ONTAP 9.15.1, das als Write-Back-Version 2 (wbv2) bezeichnet wird, gedacht werden.

Write Back vs Write Around

Seit der Einführung von FlexCache in ONTAP 9.5 handelt es sich um einen Lese- und Schreibzugriff-Cache, der jedoch im Write-Around-Modus betrieben wird. Schreibvorgänge im Cache wurden an den Ursprung gesendet, um in einen stabilen Storage verschoben zu werden. Nachdem der Ursprung den Schreibvorgang erfolgreich in einen stabilen Speicher übertragen hat, hat er den Schreibvorgang in den Cache bestätigt. Der Cache bestätigt dann den Schreibvorgang an den Client. Dies führte dazu, dass bei jedem Schreibvorgang der Vorgang des Durchquerens des Netzwerks zwischen dem Cache und dem Ursprung beeinträchtigt wird. FlexCache Write-Back ändert dies.



Nach der Aktualisierung auf ONTAP 9.15.1 können Sie einen herkömmlichen Write-Around-Cache in einen Write-Back-Cache und, falls erforderlich, wieder in einen Write-Around konvertieren. Dies kann jedoch das Lesen von Diagnoseprotokollen erschweren, sollte ein Problem auftreten.

	Umschreibung	Zurückschreiben
ONTAP-Version	9,6+	9.15.1+
Anwendungsfall	Leseintensive Workload	Schreibintensive Workload
Daten werden übertragen bei	Ursprung	Cache
Kundenerfahrung	WAN-ähnlich	LAN-ähnlich
Begrenzungen	100 pro Herkunft	10 pro Herkunft
"CAP Theorem"	Verfügbar und partitiontolerant	Verfügbar und konsistent

FlexCache Write-Back-Terminologie

Verstehen Sie Schlüsselkonzepte und -Begriffe in der Arbeit mit FlexCache Write-Back.

Laufzeit	Definition
schmutzige Daten	Daten, die zwar in stabilen Speicher im Cache gespeichert wurden, aber nicht in den Ursprungsort gelöscht wurden.
Exklusiv Lock Delegation (XLD)	Eine Sperrberechtigung auf Protokollebene, die einem Cache pro Datei gewährt wird. Diese Berechtigung ermöglicht es dem Cache, exklusive Schreibsperrungen an Clients zu übergeben, ohne den Ursprung zu kontaktieren.
Shared Lock Delegation (SLD)	Eine Sperrberechtigung auf Protokollebene, die einem Cache pro Datei gewährt wird. Diese Berechtigung ermöglicht es dem Cache, freigegebene Lesesperrungen an Clients zu übergeben, ohne den Ursprung zu kontaktieren.
Rückschreiben	Dieser Modus von FlexCache-Vorgang, bei dem Schreibvorgänge in einen Cache auf stabilen Storage in diesem Cache übertragen und dem Client sofort bestätigt werden. Die Daten werden asynchron zurück in den Ursprung geschrieben.
Write-Around	Dieser Modus von FlexCache-Vorgang, bei dem Schreibvorgänge an einen Cache an den Ursprung weitergeleitet werden, um sie in stabilen Speicher zu speichern. Nach der Erstellung bestätigt der Ursprung den Schreibvorgang in den Cache, und der Cache bestätigt den Schreibvorgang an den Client.
Dirty Data Record System (DDRS)	Ein proprietärer Mechanismus, der die fehlerhaften Daten in einem Write-Back-aktivierten Cache pro Datei verfolgt.
Ursprung	Eine FlexGroup oder FlexVol, die die Quelldaten für alle FlexCache Cache Volumes enthält. Sie ist die zentrale Quelle der Wahrheit, orchestriert Sperrungen und sorgt für 100%ige Datenkonsistenz, Währung und Kohärenz.
Cache	Eine FlexGroup, die ein spärliches Cache-Volume des Ursprungs von FlexCache ist.

Konsistent, aktuell und kohärent

FlexCache ist die Lösung von NetApp, die darauf abstellt, jederzeit und überall die richtigen Daten zu haben. FlexCache ist zu 100 % konsistent, aktuell und in 100 % der Zeit kohärent:

- **Konsistent:** die Daten sind überall dort gleich, wo sie abgerufen werden.
- **Aktuell:** die Daten sind immer aktuell.
- **Kohärent:** die Daten sind korrekt/nicht beschädigt.

ONTAP FlexCache-Rückschreibrichtlinien

FlexCache Write-Back beinhaltet viele komplexe Interaktionen zwischen dem Ursprungsserver und den Caches. Für eine optimale Leistung sollten Sie sicherstellen, dass Ihre Umgebung diesen Richtlinien entspricht. Diese Richtlinien basieren auf der zum Zeitpunkt der Inhaltserstellung aktuellsten ONTAP Hauptversion (ONTAP 9.17.1.).

Als Best Practice sollten Sie Ihren Produktions-Workload in einer nicht-Produktionsumgebung testen. Das ist noch wichtiger, wenn Sie FlexCache Write-Back außerhalb dieser Richtlinien implementieren.

Die folgenden Richtlinien wurden intern bei NetApp ausführlich getestet. Es wird **stark** empfohlen, dass Sie in

ihnen bleiben. Andernfalls kann es zu unerwartetem Verhalten kommen.

- In ONTAP 9.17.1P1 wurden bedeutende Verbesserungen für FlexCache Write-Back eingeführt. Es wird **dringend** empfohlen, nach 9.17.1P1 sowohl auf dem Ursprungs- als auch auf dem Cache-Cluster die aktuell empfohlene Version auszuführen. Falls Sie die Codeline 9.17.1 nicht ausführen können, ist die neueste P-Version 9.16.1 die nächstempfohlene Version. ONTAP 9.15.1 enthält nicht alle notwendigen Korrekturen und Verbesserungen für FlexCache Write-Back und wird daher nicht für Produktionsworkloads empfohlen.
- In ihrer aktuellen Version sollten die FlexCache Write-Back-Caches mit einer einzigen Komponente für das gesamte FlexCache Volume konfiguriert werden. FlexCaches mit mehreren Bestandteilen kann zu unerwünschtem Entfernen von Daten aus dem Cache führen.
- Die Tests wurden für Dateien mit einer Größe von weniger als 100 GB und WAN-Roundtrip-Zeiten zwischen Cache und Ursprungsserver von maximal 200 ms durchgeführt. Bei Arbeitslasten außerhalb dieser Grenzen kann es zu unerwarteten Leistungseigenschaften kommen.
- Beim Schreiben in alternative SMB-Datenströme wird die Hauptdatei aus dem Cache entfernt. Alle schmutzigen Daten für die Hauptdatei müssen an den Ursprung gespült werden, bevor andere Vorgänge an dieser Datei stattfinden können. Der alternative Datenstrom wird auch an den Ursprung weitergeleitet.
- Durch Umbenennen einer Datei wird die Datei aus dem Cache entfernt. Alle schmutzigen Daten für die Datei müssen an den Ursprung gespült werden, bevor andere Vorgänge an dieser Datei stattfinden können.
- Derzeit können nur die folgenden Attribute für eine Datei auf dem schreibgeschützten FlexCache-Volume geändert oder festgelegt werden:
 - Zeitstempel
 - Modusbits
 - NT-ACLs
 - Eigentümer
 - Gruppieren
 - Größe

Alle anderen Attribute, die geändert oder gesetzt werden, werden an den Ursprung weitergeleitet, was dazu führen kann, dass die Datei aus dem Cache entfernt wird. Wenn Sie andere Attribute ändern oder im Cache einstellen müssen, bitten Sie Ihr Account Team, ein PVR zu öffnen.

- Snapshots, die am Ursprung aufgenommen wurden, verursachen den Abruf aller ausstehenden schmutzigen Daten aus jedem Rückschreibungs-aktivierten Cache, der mit diesem Ursprungsvolume verbunden ist. Dies kann mehrere Wiederholungen des Vorgangs erfordern, wenn erhebliche Write-Back-Aktivitäten ausgeführt werden, da das Entfernen dieser fehlerhaften Dateien einige Zeit in Anspruch nehmen kann.
- Opportunistische Sperren (Oplocks) für SMB-Schreibvorgänge werden auf FlexCache -Volumes mit aktiviertem Write-Back nicht unterstützt.
- Der Ursprung muss unter 80% voll bleiben. Cache-Volumes erhalten keine exklusiven Sperrdelegationen, wenn nicht mindestens 20 % des Speicherplatzes im Ursprungs-Volume verbleiben. Aufrufe zu einem Write-Back-aktivierten Cache werden in dieser Situation an den Ursprung weitergeleitet. Dadurch wird verhindert, dass der Speicherplatz am Ursprung knapp wird, was dazu führen würde, dass schmutzige Daten in einem Cache mit aktivierter Rückschreibfunktion verwaist bleiben.
- Niedrige Bandbreite und/oder verlustbehaftete Intercluster-Netzwerke können einen erheblichen negativen Einfluss auf die Write-Back-Performance von FlexCache haben. Es gibt zwar keine spezifische Bandbreitenanforderung, da diese stark von Ihrer Arbeitslast abhängt, es wird jedoch **dringend** empfohlen,

die Funktionsfähigkeit der Intercluster-Verbindung zwischen dem/den Cache(s) und dem Ursprungsserver sicherzustellen.

ONTAP FlexCache Write-Back-Architektur

FlexCache wurde unter Berücksichtigung starker Konsistenz entwickelt, einschließlich beider Schreibmodi: Write-Back und Write-Around. Sowohl der traditionelle Write-Around-Modus als auch der in ONTAP 9.15.1 eingeführte Write-Back-Modus garantieren, dass die Daten, auf die zugegriffen wird, immer 100% konsistent, aktuell und kohärent sind.

Die folgenden Konzepte beschreiben den Betrieb von FlexCache Write-Back.

Delegationen

Durch Sperren von Delegierungen und Datendelegationen kann FlexCache sowohl Write-Back- als auch Write-Around-Caches konsistent, kohärent und aktuell halten. Der Ursprung orchestriert beide Delegationen.

Delegierungen sperren

Eine Sperrdelegation ist eine Sperrbehörde auf Protokollebene, die Origin einem Cache pro Datei gewährt, um bei Bedarf Protokollsperren an Clients auszustellen. Dazu gehören [Exklusive Sperrdelegationen \(XLD\)](#) und [Gemeinsame Sperrdelegationen \(SLD\)](#).

XLD und Write-Back

Um sicherzustellen, dass ONTAP niemals einen widersprüchlichen Schreibvorgang abgleichen muss, wird ein XLD einem Cache gewährt, in dem ein Client das Schreiben in eine Datei anfordert. Wichtig ist, dass zu jeder Zeit nur ein XLD für jede Datei existieren kann, was bedeutet, dass es nie mehr als einen Writer zu einer Datei gleichzeitig geben wird.

Wenn die Anfrage zum Schreiben in eine Datei in einen schreibaktivierten Cache kommt, werden die folgenden Schritte ausgeführt:

1. Der Cache prüft, ob bereits ein XLD für die angeforderte Datei vorhanden ist. Wenn dies der Fall ist, wird dem Client die Schreibsperre gewährt, solange ein anderer Client nicht in die Datei im Cache schreibt. Wenn der Cache keine XLD für die angeforderte Datei hat, wird eine vom Ursprungsort angefordert. Dies ist ein proprietärer Anruf, der das Cluster-Netzwerk durchquert.
2. Nach dem Empfang der XLD-Anforderung aus dem Cache prüft der Origin, ob ein ausstehender XLD für die Datei in einem anderen Cache vorhanden ist. Wenn dies der Fall ist, ruft es die XLD dieser Datei auf, die eine Spülung von jedem aus diesem Cache zurück zum Ursprung auslöst [Schmutzige Daten](#).
3. Sobald die fehlerhaften Daten aus diesem Cache zurückgeleert und an einen stabilen Speicher am Ursprung übertragen wurden, wird der Ursprung die XLD für die Datei dem anfragenden Cache zuweisen.
4. Sobald der XLD der Datei empfangen wurde, gewährt der Cache dem Client die Sperre, und der Schreibvorgang beginnt.

Ein hochstufiger Ablaufplan, der einige dieser Schritte abdeckt, wird im [\[write-back-sequence-diagram\]](#) Ablaufdiagramm beschrieben.

Aus der Client-Perspektive funktioniert alle Sperrung so, als würde sie auf eine Standard-FlexVol oder FlexGroup geschrieben. Das Risiko liegt bei einer kleinen Verzögerung, wenn die Schreibsperre angefordert wird.

Wenn in der aktuellen Iteration ein Write-Back-fähiger Cache den XLD für eine Datei enthält, blockiert ONTAP *

jeden beliebigen* Zugriff auf diese Datei in anderen Caches, einschließlich READ Operationen.



Es gibt eine Grenze von 170 XLDs pro Ursprungsbestandteil.

Datendelegationen

Eine Datendelegierung ist eine dateibasierte Garantie, die einem Cache nach Herkunft zugestellt wird, dass die für diese Datei zwischengespeicherten Daten auf dem neuesten Stand sind. Solange der Cache eine Datendelegation für eine Datei hat, kann er die für die Datei zwischengespeicherten Daten für den Client bereitstellen, ohne sich mit dem Ursprung in Verbindung setzen zu müssen. Wenn der Cache keine Datendelegierung für die Datei hat, muss er sich an den Ursprung wenden, um die vom Client angeforderten Daten zu erhalten.

Im Write-Back-Modus wird die Datendelegierung einer Datei aufgehoben, wenn eine XLD für diese Datei in einem anderen Cache oder vom Ursprung genommen wird. Dadurch wird die Datei effektiv von Clients aller anderen Caches und vom Ursprung abgetrennt, auch bei Lesevorgängen. Dies ist ein Kompromiss, der getroffen werden muss, um sicherzustellen, dass auf alte Daten nie zugegriffen wird.

Lesevorgänge in einem Write-Back-aktivierten Cache arbeiten im Allgemeinen wie Lesevorgänge in einem Write-Around-Cache. Sowohl in Write-Around- als auch in Write-Back-fähigen Caches kann es zu einem ersten READ Performance-Hit kommen, wenn die angeforderte Datei über eine exklusive Schreibsperre in einem anderen Write-Back-aktivierten Cache verfügt, als wenn der Lesevorgang ausgeführt wird. Der XLD muss widerrufen werden, und die fehlerhaften Daten müssen an den Ursprung übertragen werden, bevor der Lesevorgang im anderen Cache bedient werden kann.

Unsaubere Daten werden nachverfolgt

Das Rückschreiben vom Cache zum Ursprung erfolgt asynchron. Das heißt, schmutzige Daten werden nicht sofort zurück in die ursprüngliche Quelle geschrieben. ONTAP verwendet ein System mit nicht ordnungsgemäßen Datensätzen, um schmutzige Daten pro Datei nachzuverfolgen. Jeder Dirty Data Record (DDR) stellt ungefähr 20 MB schmutzige Daten für eine bestimmte Datei dar. Wenn eine Datei aktiv geschrieben wird, beginnt ONTAP schmutzige Daten zurück zu spülen, nachdem zwei DDRs gefüllt wurden und der dritte DDR geschrieben wird. Dies führt dazu, dass während der Schreibvorgänge ungefähr 40 MB an schmutzigen Daten in einem Cache verbleiben. Bei zustandsbehafteten Protokollen (NFSv4.x, SMB) werden die verbleibenden 40 MB an Daten zurück an den Ursprung übertragen, wenn die Datei geschlossen wird. Bei zustandslosen Protokollen (NFSv3) werden die 40 MB an Daten zurückgelöscht, wenn entweder der Zugriff auf die Datei in einem anderen Cache angefordert wird oder wenn die Datei zwei oder mehr Minuten lang inaktiv ist, maximal fünf Minuten. Weitere Informationen zum Auslösen von durch Timer oder durch Speicherplatz ausgelösten schmutzigen Daten finden Sie unter [Cache-Scrubber](#).

Zusätzlich zu den DDRs und Scrubbers lösen einige Front-End NAS-Operationen auch das Spülen aller schmutzigen Daten für eine Datei aus:

- SETATTR
 - `SETATTR`s, die nur mtime, atime und/oder ctime ändern, können im Cache verarbeitet werden, um die Einbußen des WAN zu vermeiden.
- CLOSE
- OPEN In einem anderen Cache
- READ In einem anderen Cache
- REaddir In einem anderen Cache

- READDIRPLUS In einem anderen Cache
- WRITE In einem anderen Cache

Abgetrennter Modus

Wenn eine XLD für eine Datei in einem Write-Around-Cache gespeichert wird und dieser Cache vom Ursprung getrennt wird, sind Lesevorgänge für diese Datei weiterhin in den anderen Caches und im Ursprung zulässig. Dieses Verhalten unterscheidet sich, wenn ein XLD von einem Write-Back-aktivierten Cache gehalten wird. Wenn der Cache getrennt ist, hängt in diesem Fall überall der Lesezugriff auf die Datei. Dies trägt dazu bei, 100 % Konsistenz, Währung und Kohärenz aufrechtzuerhalten. Die Lesevorgänge sind im Write-Around-Modus erlaubt, da am Ursprung garantiert ist, dass alle Daten verfügbar sind, die für den Client schreibgeschützt sind. Im Write-Back-Modus während einer Trennung kann der Origin nicht garantieren, dass alle Daten, die in den Write-Back-aktivierten Cache geschrieben und vom Write-Back-aktivierten Cache bestätigt wurden, vor der Trennung auf den Ursprung gebracht wurden.

Falls ein Cache mit einem XLD für eine Datei über einen längeren Zeitraum getrennt wird, kann ein Systemadministrator den XLD am Ursprung manuell widerrufen. Dadurch kann die E/A-Datei an den verbleibenden Caches und am Ursprung wieder aufgenommen werden.



Das manuelle Zurückziehen des XLD führt zum Verlust von fehlerhaften Daten für die Datei im nicht verbundenen Cache. Das manuelle Revocieren eines XLD sollte nur im Falle einer katastrophalen Störung zwischen Cache und Ursprung erfolgen.

Cache-Scrubber

In ONTAP gibt es Scrubbers, die als Reaktion auf bestimmte Ereignisse ausgeführt werden, wie z. B. einen Timer, der abläuft oder die Schwellenwerte für die Leerräume verletzt werden. Die Scrubbers erhalten eine exklusive Sperre für die zu scrubbed Datei, effektiv Einfrieren IO auf diese Datei, bis das Scrub abgeschlossen ist.

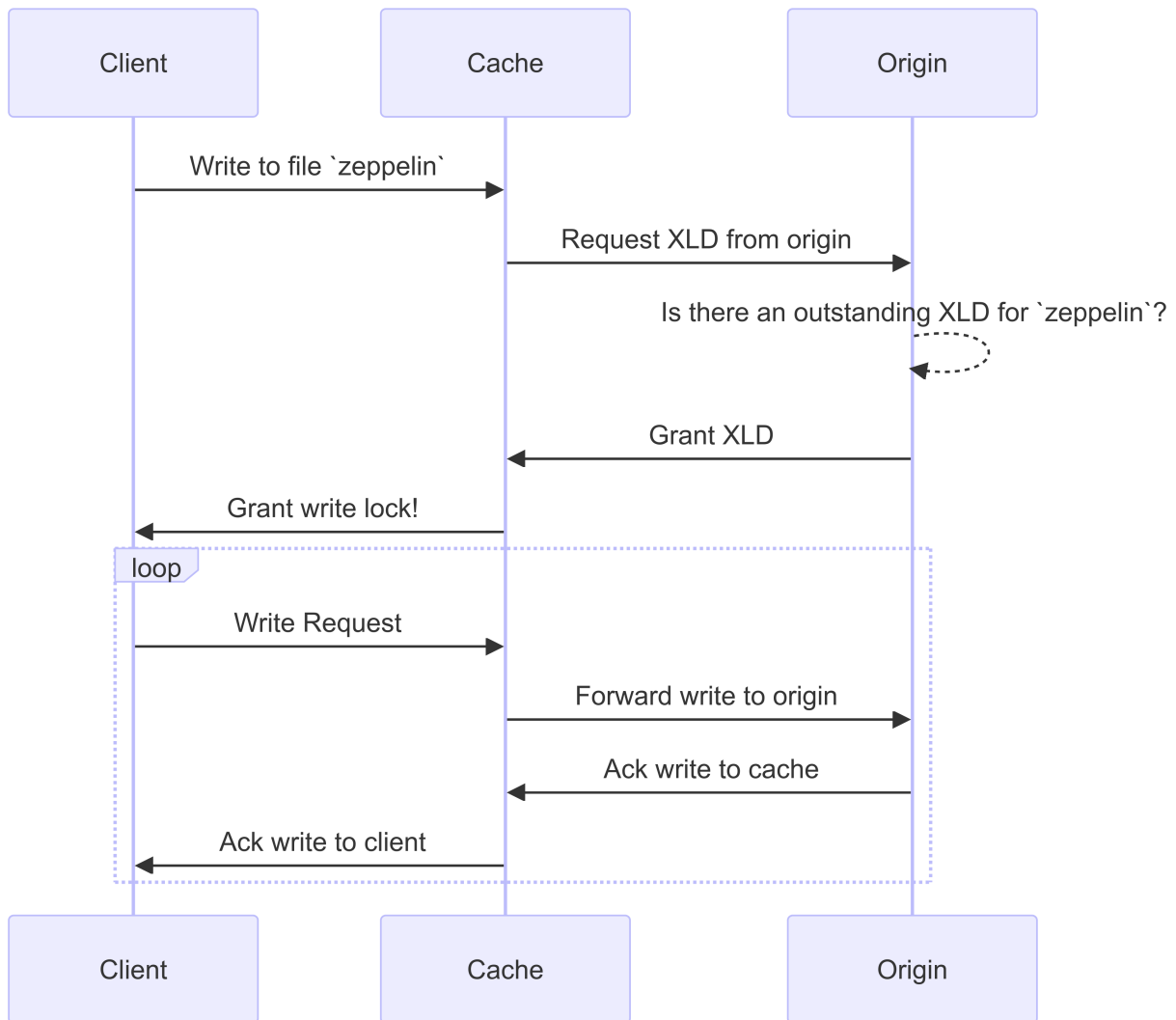
Zu den Scrubbers gehören:

- **Mtime-basierte Scrubber im Cache:** dieser Scrubber startet alle fünf Minuten und reibt jede Datei, die zwei Minuten lang unverändert sitzt. Wenn sich irgendwelche fehlerhaften Daten für die Datei noch im Cache befinden, wird die I/O-Vorgänge für diese Datei stillgelegt und ein Rückschreiben ausgelöst. Die E/A-Vorgänge werden nach Abschluss des Rückschreibens wieder aufgenommen.
- **Mtime-basierte Scrubber nach Herkunft:** ähnlich wie der mtime-basierte Scrubber im Cache läuft dieser auch alle fünf Minuten. Es reibt jedoch jede Datei, die 15 Minuten lang unverändert sitzt, und erinnert an die Delegation der Inode. Dieser Scrubber initiiert keinen Rückschreibvorgang.
- **RW-Scheuersaugmaschine auf Ursprungsbasis:** ONTAP überwacht, wie viele RW-Lock-Delegationen pro Ursprungskomponente ausgehändigt werden. Wenn diese Zahl 170 übertrifft, beginnt ONTAP mit dem Scrubbing von Write Lock-Delegationen auf LRU-Basis (Least-Recently-Used).
- **Platzbasiertes Scrubber auf dem Cache:** erreicht ein FlexCache-Volumen 90% voll, wird der Cache geschrubbt und wird auf LRU-Basis entfernt.
- **Platzbasiertes Scrubber auf der Herkunft:** erreicht ein FlexCache-Ursprungsvolumen 90% voll, wird der Cache geschrubbt und wird auf LRU-Basis entfernt.

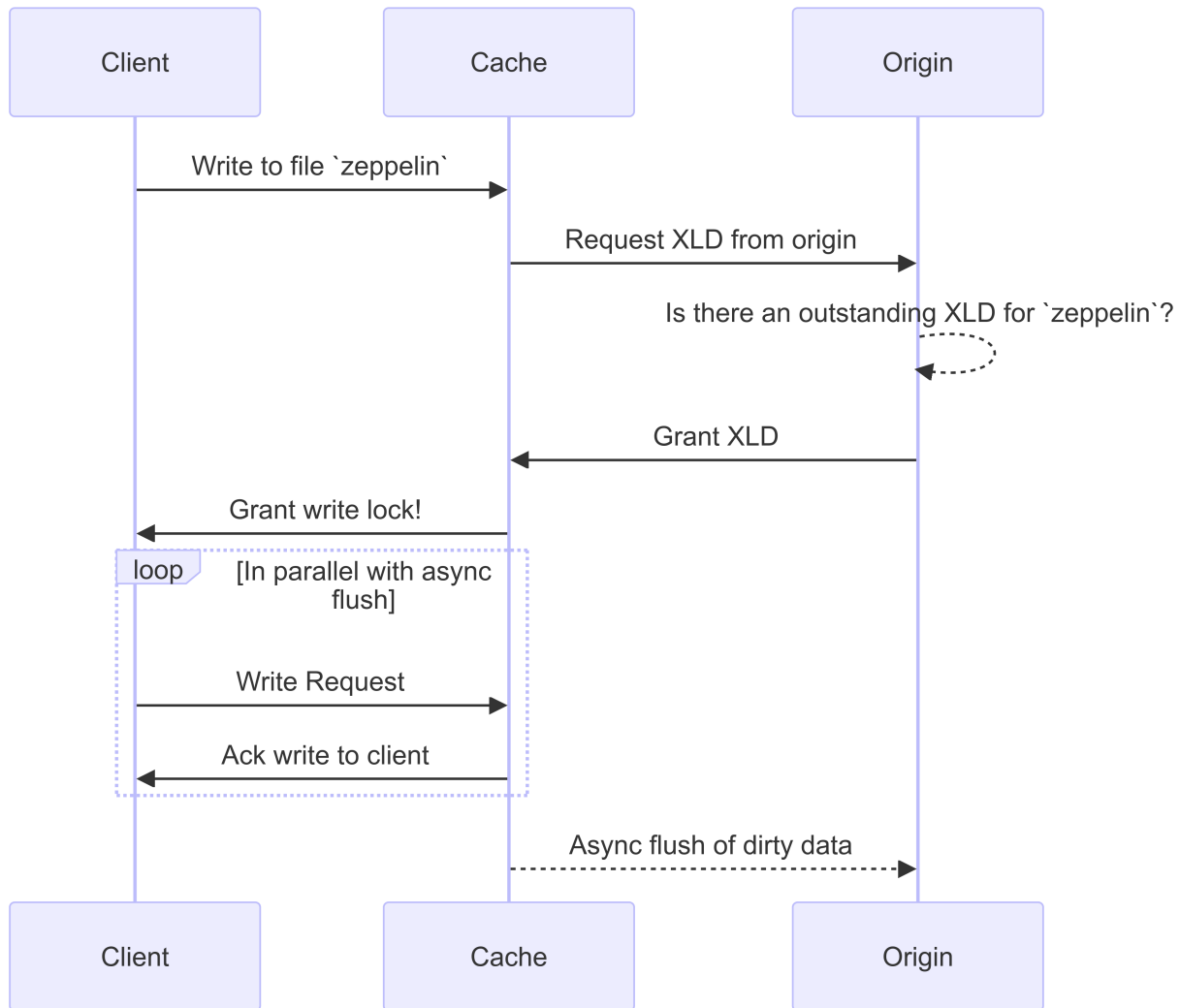
Sequenzdiagramme

Diese Sequenzdiagramme zeigen den Unterschied zwischen Write-Acknowledgement und Write-Back-Modus.

Umschreibung



Zurückschreiben



Anwendungsfälle für die ONTAP FlexCache-Rückschreibung

Dies sind Schreibprofile, die sich am besten für eine schreibBack-fähige FlexCache eignen. Sie sollten Ihren Workload testen, um festzustellen, ob Write-Back- oder Write-Around die beste Performance bietet.



Write-Back ist kein Ersatz für Write-Around. Obwohl Write-Back-Anwendungen mit schreibintensiven Workloads konzipiert sind, ist die Write-Around-Lösung immer noch die bessere Wahl für viele Workloads.

Ziel-Workloads

Dateigröße

Die Dateigröße ist weniger wichtig als die Anzahl der Schreibvorgänge, die zwischen dem und -Aufrufen für eine Datei ausgegeben `OPEN CLOSE` wurden. Kleine Dateien haben von Natur aus weniger `WRITE` Anrufe, wodurch sie weniger ideal für das Zurückschreiben sind. Große Dateien können mehr Schreibvorgänge zwischen und Aufrufen haben `OPEN CLOSE`, aber dies ist nicht garantiert.

Auf der "[FlexCache-Rückschreibrichtlinien](#)" Seite finden Sie die aktuellen Empfehlungen zur maximalen Dateigröße.

Schreibgröße

Beim Schreiben von einem Client sind andere modifizierende NAS-Anrufe außer Schreibaufrufe beteiligt. Dazu gehören unter anderem:

- CREATE
- OPEN
- CLOSE
- SETATTR
- SET_INFO

SETATTR Und SET_INFO Aufrufe, die gesetzt mtime, , , , atime ctime owner group oder size werden im Cache verarbeitet. Der Rest dieser Aufrufe muss am Ursprung verarbeitet werden und einen Rückschreibvorgang für alle schmutzigen Daten auslösen, die im schreibBack-aktivierten Cache für die Datei gesammelt werden, auf der ausgeführt wird. IO auf die Datei wird stillgelegt, bis der Schreibvorgang abgeschlossen ist.

Wenn Sie wissen, dass diese Anrufe das WAN durchlaufen müssen, können Sie Workloads identifizieren, die sich für Write-Back eignen. Je mehr Schreibvorgänge zwischen OPEN und CLOSE Aufrufen erfolgen können, ohne dass einer der oben aufgeführten Anrufe ausgegeben wird, desto besser ist die Performance-Steigerung des Rückschreibens.

Read-after-Write

Workloads mit Lese-/Schreibzugriff hatten in der Vergangenheit bei FlexCache eine schlechte Performance. Dies ist auf den Schreibmodus vor 9.15.1 zurückzuführen. Der WRITE Aufruf der Datei muss am Ursprung erfolgen, und der nachfolgende READ Aufruf müsste die Daten zurück in den Cache verschieben. Dies führt dazu, dass beide Vorgänge die WAN-Einbußen nach sich nehmen. Daher werden für FlexCache im Write-Around-Modus von Read-after-Write-Workloads abgeraten. Mit der Einführung von Write-Back im Jahr 9.15.1 werden Daten nun im Cache gespeichert und können sofort aus dem Cache gelesen werden, wodurch die WAN-Einbußen eliminiert werden. Wenn Ihr Workload auf FlexCache Volumes Lese-nach-Schreiben beinhaltet, sollten Sie den Cache für den Write-Back-Modus konfigurieren.



Wenn Read-after-write ein wichtiger Teil Ihrer Arbeitslast ist, sollten Sie Ihren Cache so konfigurieren, dass er im Write-Back-Modus arbeitet.

Write-after-Write

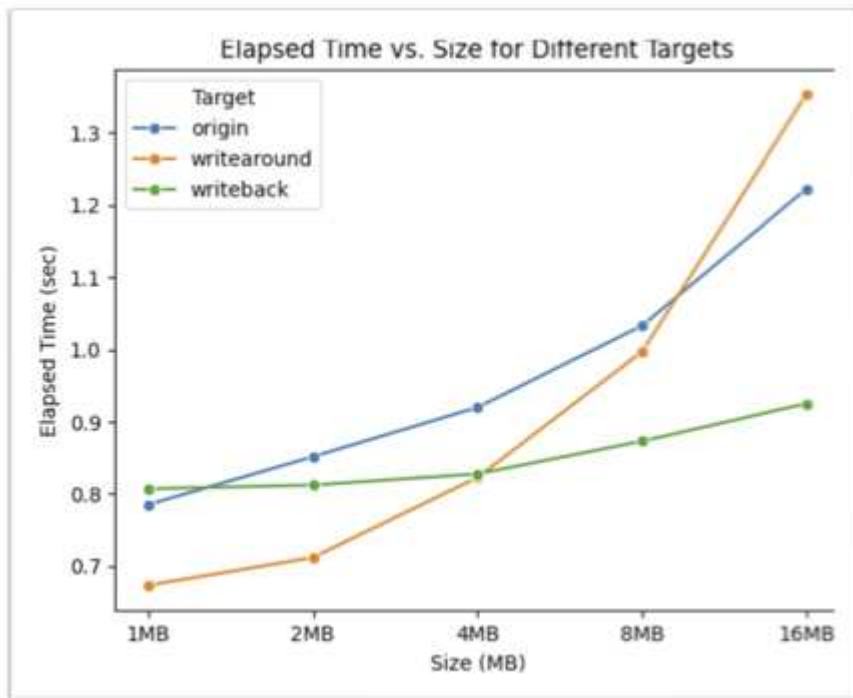
Wenn eine Datei schmutzige Daten in einem Cache akkumuliert, schreibt der Cache die Daten asynchron zurück zum Ursprung. Dies führt natürlich zu Zeiten, wenn der Client die Datei mit schmutzigen Daten schließt, die noch darauf warten, wieder an den Ursprung zurückgespült zu werden. Wenn für die gerade geschlossene Datei ein weiterer offener oder ein anderer Schreibvorgang eingeht und noch schmutzige Daten enthält, wird der Schreibvorgang unterbrochen, bis alle fehlerhaften Daten auf den Ursprung übertragen wurden.

Überlegungen zur Latenz

Wenn FlexCache im Write-Back-Modus arbeitet, ist dies für NAS-Clients mit zunehmender Latenz vorteilhafter. Es gibt jedoch einen Punkt, an dem der Overhead von Write-Back die Vorteile überwiegt, die in Umgebungen mit niedriger Latenz erzielt werden. In einigen NetApp-Tests führten die Write-Back-Ergebnisse zu einer minimalen Latenz zwischen Cache und Ursprung von 8 ms. Diese Latenz variiert je nach Workload. Stellen Sie daher sicher, dass Sie den Endpunkt Ihres Workloads kennen.

Das folgende Diagramm zeigt den Rückgabepunkt für den Rückschreibvorgang in NetApp Labortests. Die x

Achse ist die Dateigröße und die y Achse die verstrichene Zeit. Bei dem Test wurde NFSv3 verwendet, wobei ein und 256 KB und 64 ms WAN-Latenz gemountet `rsizewsize` werden. Dieser Test wurde mit einer kleinen ONTAP Select-Instanz sowohl für den Cache als auch für den Ursprungs sowie mit einem einzigen Thread-Schreibvorgang durchgeführt. Ihre Ergebnisse können variieren.



Write-Back sollte nicht für Intracluster-Caching verwendet werden. Intracluster-Caching findet statt, wenn sich Ursprung und Cache im selben Cluster befinden.

Voraussetzungen für die ONTAP FlexCache-Zurückschreibung

Stellen Sie vor der Implementierung von FlexCache im Write-Back-Modus sicher, dass Sie diese Anforderungen an Performance, Software, Lizenzierung und Systemkonfiguration erfüllt haben.

CPU und Speicher

Es wird **dringend empfohlen**, dass jeder Ursprungsclusterknoten über mindestens 128 GB RAM und 20 CPUs verfügt, um die von Caches mit aktiviertem Write-Back initiierten Write-Back-Nachrichten aufzunehmen. Dies entspricht einer A400 oder höher. Wenn der Origin-Cluster als Ursprung für mehrere Write-Back-fähige FlexCaches dient, werden mehr CPU und RAM benötigt.



Die Verwendung eines zu kleinen Ursprungs für Ihren Workload kann erhebliche Auswirkungen auf die Performance am Write Back-Enabled Cache oder am Entstehungsort haben.

ONTAP-Version

- Der Ursprung **must** wird mit ONTAP 9.15.1 oder höher ausgeführt.
- Alle Caching-Cluster, die im Write-Back-Modus arbeiten müssen **must**, werden mit ONTAP 9.15.1 oder höher ausgeführt.

- Auf jedem Caching-Cluster, der nicht im Write-Back-Modus betrieben werden muss, kann jede allgemein unterstützte ONTAP-Version ausgeführt werden.

Lizenzierung

FlexCache, einschließlich des Write-Back-Betriebsmodus, ist in Ihrem ONTAP-Kauf enthalten. Es ist keine zusätzliche Lizenz erforderlich.

Peering

- Ursprungs- und Cache-Cluster müssen sein **"Cluster-Peered"**
- Die Server Virtual Machines (SVMs) im Ursprungs- und Cache-Cluster müssen mit der Option FlexCache ausgestattet sein **"svm-Peering"**.



Sie müssen keinen Peer eines Cache-Clusters mit einem anderen Cache-Cluster erstellen. Es muss auch keine Cache-SVM mehr einer anderen Cache-SVM zugewiesen werden.

Interoperabilität von ONTAP FlexCache-Schreibvorgängen

Beachten Sie diese Interoperabilitätsüberlegungen, wenn Sie FlexCache im Write-Back-Modus bereitstellen.

ONTAP-Version

Um den Write-Back-Modus zu verwenden, müssen sowohl der Cache als auch der Ursprung *ONTAP 9.15.1 oder höher ausführen.



Auf Clustern, auf denen kein Write-Back-fähiger Cache erforderlich ist, können frühere Versionen von ONTAP ausgeführt werden, dieser Cluster kann jedoch nur im Write-Around-Modus betrieben werden.

Sie können in Ihrer Umgebung verschiedene ONTAP-Versionen verwenden.

Cluster	ONTAP-Version	Write-Back unterstützt?
Ursprung	ONTAP 9.15.1	K. A. †
Cluster 1	ONTAP 9.15.1	Ja.
Cluster 2	ONTAP 9.14.1	Nein

Cluster	ONTAP-Version	Write-Back unterstützt?
Ursprung	ONTAP 9.14.1	K. A. †
Cluster 1	ONTAP 9.15.1	Nein
Cluster 2	ONTAP 9.15.1	Nein

† Origins sind kein Cache, daher ist weder Write-Back- noch Write-Around-Unterstützung anwendbar.



In [\[example2-table\]](#) kann kein Cluster den Write-Back-Modus aktivieren, da ONTAP 9.15.1 oder höher im Ursprung nicht ausgeführt wird, was eine strikte Anforderung ist.

Client-Interoperabilität

Jeder von ONTAP allgemein unterstützte Client kann auf ein FlexCache Volume zugreifen, unabhängig davon, ob er im Write-Around- oder Write-Back-Modus arbeitet. Eine aktuelle Liste der unterstützten Clients finden Sie im Dokument NetApp ["Interoperabilitäts-Matrix"](#).

Obwohl die Client-Version speziell nicht von Bedeutung ist, muss der Client neu genug sein, um NFSv3, NFSv4.0, NFSv4.1, SMB2.x oder SMB3.x zu unterstützen. SMB1 und NFSv2 sind veraltete Protokolle und werden nicht unterstützt.

Write-Back und Write-Around

Wie in gezeigt [\[example1-table\]](#), kann FlexCache im Write-Back-Modus zusammen mit Caches im Write-Around-Modus eingesetzt werden. Es wird empfohlen, Write-Around- und Write-Back-Vergleiche mit Ihrem spezifischen Workload anzustellen.



Falls die Performance für einen Workload zwischen Write-Back und Write-Around identisch ist, verwenden Sie Write-Around.

Interoperabilität von ONTAP Funktionen

Eine aktuelle Liste der Interoperabilität von FlexCache-Funktionen finden Sie unter ["Die unterstützten und nicht unterstützten Funktionen für FlexCache Volumes"](#).

Aktivieren und Verwalten von ONTAP FlexCache Write-Back

Ab ONTAP 9.15.1 können Sie den FlexCache Write-Back-Modus auf FlexCache-Volumes aktivieren, um eine bessere Performance für Edge-Computing-Umgebungen und Caches mit schreibintensiven Workloads zu erreichen. Sie können auch bestimmen, ob Write-back auf einem FlexCache-Volume aktiviert ist, oder bei Bedarf den Write-Back-Wert auf dem Volume deaktivieren.

Wenn der Rückschreibvorgang auf dem Cache-Volume aktiviert ist, werden Schreibanforderungen an den lokalen Cache und nicht an das Ursprungs-Volume gesendet.

Bevor Sie beginnen

Sie müssen sich im erweiterten Berechtigungsmodus befinden.

Erstellen Sie ein neues FlexCache-Volume mit aktiviertem Write-Back

Schritte


Sie können ein neues FlexCache Volume mit aktivierter Write-Back-Funktion über ONTAP System Manager oder die ONTAP CLI erstellen.


System Manager

1. Wenn sich das FlexCache Volume auf einem anderen Cluster als dem Ursprungs-Volume befindet, erstellen Sie eine Cluster Peer-Beziehung:

- a. Klicken Sie im lokalen Cluster auf **Schutz > Übersicht**.
- b. Erweitern Sie **Intercluster-Einstellungen**, klicken Sie auf **Netzwerkschnittstellen hinzufügen** und fügen Sie dem Cluster Intercluster-Schnittstellen hinzu.

Wiederholen Sie dies auf dem Remote-Cluster.

- c. Klicken Sie im Remote-Cluster auf **Schutz > Übersicht**. Klicken Sie  im Abschnitt Cluster Peers auf **Passphrase generieren**.
 - d. Kopieren Sie die generierte Passphrase, und fügen Sie sie in das lokale Cluster ein.
 - e. Klicken Sie auf dem lokalen Cluster unter Cluster Peers auf **Peer Clusters**, um die lokalen und Remote-Cluster zu sehen.
2. Wenn sich das FlexCache Volume auf einem anderen Cluster als dem Ursprungs-Volume befindet, erstellen Sie eine SVM Peer-Beziehung:

Klicken Sie unter **Storage VM Peers** auf und dann auf  **Peer Storage VMs**, um die Speicher-VMs zu sehen.

Wenn sich das FlexCache Volume auf demselben Cluster befindet, können Sie mit System Manager keine SVM-Peer-Beziehung erstellen.

3. Wählen Sie **Storage > Volumes**.
4. Wählen Sie **Hinzufügen**.
5. Wählen Sie **More Options** und dann **Add as Cache for a Remote Volume**.
6. Wählen Sie **FlexCache-Rückschreibung aktivieren**.

CLI

1. Wenn sich das zu erstellende FlexCache Volume in einem anderen Cluster befindet, erstellen Sie eine Cluster-Peer-Beziehung:
 - a. Erstellen Sie auf dem Ziel-Cluster eine Peer-Beziehung mit dem Datensicherheits-Quellcluster:

```
cluster peer create -generate-passphrase -offer-expiration
MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addr
<peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,...|*
-ipospace <ipospace_name>
```

Ab ONTAP 9.6 ist die TLS-Verschlüsselung bei der Erstellung einer Cluster-Peer-Beziehung standardmäßig aktiviert. Die TLS-Verschlüsselung wird für die Cluster-übergreifende Kommunikation zwischen den Ursprungs- und FlexCache Volumes unterstützt. Bei Bedarf können Sie auch die TLS-Verschlüsselung für die Cluster-Peer-Beziehung deaktivieren.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *
```

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: *
Intercluster LIF IP: 192.140.112.101
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.

a. Authentifizierung des Quellclusters im Quellcluster beim Ziel-Cluster:

```
cluster peer create -peer-addr <peer_LIF_IPs> -ip-space <ip-space>
```

```
cluster01::> cluster peer create -peer-addr
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

2. Wenn sich das FlexCache-Volumen in einer anderen SVM als der Ursprungs-Volumen befindet, erstellen Sie eine SVM-Peer-Beziehung mit flexcache als Applikation:

a. Wenn sich die SVM in einem anderen Cluster befindet, erstellen Sie eine SVM-Berechtigung für die Peering SVMs:

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

Das folgende Beispiel veranschaulicht die Erstellung einer SVM-Peer-Berechtigung, die für alle lokalen SVMs gilt:

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache
```

Warning: This Vserver peer permission applies to all local Vservers. After that no explicit "vserver peer accept" command required for Vserver peer relationship creation request from peer cluster "cluster2" with any of the local Vservers. Do you want to continue? {y|n}: y

a. SVM-Peer-Beziehung erstellen:

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. Erstellen Sie ein FlexCache-Volume mit aktiviertem Write-Back:

```
volume flexcache create -vserver <cache_vserver_name> -volume
<cache_flexgroup_name> -aggr-list <list_of_aggregates> -origin
-volume <origin_flexgroup> -origin-vserver <origin_vserver name>
-junction-path <junction_path> -is-writeback-enabled true
```

Aktivieren Sie FlexCache Write-Back auf einem vorhandenen FlexCache-Volume

Sie können FlexCache Write-Back auf einem vorhandenen FlexCache Volume mithilfe von ONTAP System Manager oder der ONTAP CLI aktivieren.

System Manager

1. Wählen Sie **Speicher > Volumes** und wählen Sie ein vorhandenes FlexCache-Volume aus.
2. Klicken Sie auf der Übersichtsseite des Volumes oben rechts auf **Bearbeiten**.
3. Wählen Sie im Fenster **Volume bearbeiten FlexCache-Rückschreiben aktivieren** aus.

CLI

1. Write-Back auf einem vorhandenen FlexCache-Volume aktivieren:

```
volume flexcache config modify -volume <cache_flexgroup_name> -is
-writeback-enabled true
```

Überprüfen Sie, ob FlexCache Write-Back aktiviert ist

Schritte

Sie können mit System Manager oder der ONTAP-CLI bestimmen, ob das FlexCache-Zurückschreiben aktiviert ist.

System Manager

1. Wählen Sie **Speicher > Volumes** und wählen Sie ein Volume aus.
2. Suchen Sie im Volume **Übersicht FlexCache Details** und prüfen Sie, ob FlexCache Write-back auf dem FlexCache Volume auf **aktiviert** eingestellt ist.

CLI

1. Überprüfen Sie, ob FlexCache Write-Back aktiviert ist:

```
volume flexcache config show -volume <cache_flexgroup_name> -fields  
is-writeback-enabled
```

Deaktivieren Sie Write-Back auf einem FlexCache-Volume

Bevor Sie ein FlexCache-Volume löschen können, müssen Sie den FlexCache-Schreibvorgang deaktivieren.

Schritte

Sie können System Manager oder die ONTAP CLI verwenden, um FlexCache Write-Back zu deaktivieren.

System Manager

1. Wählen Sie **Speicher > Volumes** aus, und wählen Sie ein vorhandenes FlexCache-Volume aus, für das FlexCache-Rückschreiben aktiviert ist.
2. Klicken Sie auf der Übersichtsseite des Volumes oben rechts auf **Bearbeiten**.
3. Deaktivieren Sie im Fenster **Volume bearbeiten** die Option **FlexCache-Rückschreiben aktivieren**.

CLI

1. Rückschreibvorgang deaktivieren:

```
volume flexcache config modify -volume <cache_vol_name> -is  
-writeback-enabled false
```

Häufig gestellte Fragen zum ONTAP FlexCache-Rückschreiben

Diese FAQ kann Ihnen helfen, wenn Sie eine schnelle Antwort auf eine Frage suchen.

Ich möchte Rückschreiben verwenden. Welche Version von ONTAP muss ich ausführen?

Sowohl der Cache als auch der Ursprung müssen ONTAP 9.15.1 oder höher ausführen. Es wird **stark** empfohlen, die neueste P-Version auszuführen. Engineering verbessert kontinuierlich die Performance und

Funktionalität von Write-Back-Enabled Caches.

Können Clients, die auf den Ursprung zugreifen, Auswirkungen auf Clients haben, die auf den schreibaktivierten Cache zugreifen?

Ja. Der Ursprung hat das gleiche Recht auf Daten wie jeder der Caches. Wenn ein Vorgang für eine Datei ausgeführt wird, bei der die Datei aus dem Cache entfernt werden muss, oder wenn eine Sperre/Datendelegation aufgehoben werden muss, kann es vorkommen, dass der Client im Cache eine Verzögerung beim Zugriff auf die Datei sieht.

Kann ich QoS auf schreibBack-Enabled FlexCaches anwenden?

Ja. Auf jeden Cache und auf den Ursprung können unabhängige QoS-Richtlinien angewendet werden. Dies hat keine direkten Auswirkungen auf einen durch das Rückschreiben initiierten Intercluster-Datenverkehr. Indirekt können Sie durch QoS-Beschränkung des Front-End-Datenverkehrs im schreibBack-fähigen Cache den zurückschreibenden Datenverkehr verlangsamen.

Wird Multi-Protokoll-NAS bei Write-Back-Enabled FlexCaches unterstützt?

Ja. Multi-Protokoll wird bei schreibBack-fähigen FlexCaches vollständig unterstützt. Derzeit werden NFSv4.2 und S3 nicht von FlexCache unterstützt, die im Write-Around Write-Back-Modus arbeiten.

Werden alternative SMB-Datenströme in FlexCaches mit Write-Back-Funktion unterstützt?

Alternative SMB-Datenströme (ADS) werden unterstützt, jedoch nicht durch einen Schreibvorgang beschleunigt. Der Schreibvorgang auf die ADS wird an den Ursprung weitergeleitet, wodurch die WAN-Latenz beeinträchtigt wird. Der Schreibvorgang entfernt auch die Hauptdatei, zu der die ANZEIGEN gehören, aus dem Cache.

Kann ich einen Cache zwischen Write-Around- und Write-Back-Modus wechseln, nachdem er erstellt wurde?

Ja. Alles was Sie tun müssen, ist das Flag im Link:../FlexCache-writeback/FlexCache-writeback-enable-task.html[flexcache modify Befehl] umzuschalten is-writeback-enabled.

Gibt es Bandbreitenüberlegungen, die ich hinsichtlich der Intercluster-Verbindung zwischen dem/den Cache(s) und dem Ursprungsserver beachten sollte?

Ja. FlexCache Write-Back ist stark von der Intercluster-Verbindung zwischen dem/den Cache(s) und dem Ursprung abhängig. Geringe Bandbreite und/oder verlustbehaftete Netzwerke können die Leistung erheblich beeinträchtigen. Es gibt keine festgelegte Bandbreitenanforderung, da diese stark von Ihrer Arbeitslast abhängt.

FlexCache-Dualität

Häufig gestellte Fragen zur FlexCache-Dualität

Diese FAQ beantwortet häufig gestellte Fragen zur FlexCache-Dualität, die in ONTAP 9.18.1 eingeführt wurde.

Häufig gestellte Fragen

Was ist „Dualität“?

Dualität ermöglicht den einheitlichen Zugriff auf dieselben Daten sowohl über Datei- (NAS) als auch Objekt- (S3) Protokolle. Eingeführt in ONTAP 9.12.1 ohne FlexCache-Unterstützung, wurde Dualität in ONTAP 9.18.1 auf FlexCache-Volumes erweitert, sodass der S3-Protokollzugriff auf NAS-Dateien möglich ist, die in einem FlexCache-Volume zwischengespeichert sind.

Welche S3-Operationen werden für einen FlexCache S3-Bucket unterstützt?

S3-Operationen, die auf Standard-S3-NAS-Buckets unterstützt werden, sind auch auf FlexCache S3-NAS-Buckets verfügbar, mit Ausnahme der `COPY` Operation. Eine aktuelle Liste der nicht unterstützten Operationen für einen Standard-S3-NAS-Bucket finden Sie unter ["Interoperabilitätsdokumentation"](#).

Kann ich FlexCache im Write-Back-Modus mit FlexCache-Dualität verwenden?

Nein. Wenn ein FlexCache S3-NAS-Bucket auf einem FlexCache Volume erstellt wird, **muss** sich das FlexCache Volume im Write-Around-Modus befinden. Wenn Sie versuchen, einen FlexCache S3-NAS-Bucket auf einem FlexCache Volume im Write-Back-Modus zu erstellen, schlägt der Vorgang fehl.

Ich kann einen meiner Cluster aufgrund von Hardwarebeschränkungen nicht auf ONTAP 9.18.1 aktualisieren. Funktioniert die Dualität in meinem Cluster weiterhin, wenn nur der Cache-Cluster mit ONTAP 9.18.1 läuft?

Nein. Sowohl der Cache-Cluster als auch der Ursprungscluster müssen mindestens die effektive Clusterversion 9.18.1 aufweisen. Wenn Sie versuchen, einen FlexCache S3-NAS-Bucket auf einem Cache-Cluster zu erstellen, der mit einem Ursprungscluster verbunden ist, auf dem eine ONTAP Version vor 9.18.1 ausgeführt wird, schlägt der Vorgang fehl.

Ich habe eine MetroCluster-Konfiguration. Kann ich die FlexCache-Dualität nutzen?

Nein. FlexCache-Dualität wird in MetroCluster-Konfigurationen nicht unterstützt.

Kann ich den S3-Zugriff auf Dateien in einem FlexCache S3 NAS-Bucket überwachen?

Die S3-Überwachung wird durch die NAS-Überwachungsfunktionalität bereitgestellt, die FlexCache-Volumes verwenden. Weitere Informationen zur NAS-Überwachung von FlexCache-Volumes finden Sie unter ["Erfahren Sie mehr über FlexCache-Auditing"](#).

Was sollte ich erwarten, wenn das Cache-Cluster vom Origin-Cluster getrennt wird?

S3-Anfragen an einen FlexCache S3-NAS-Bucket schlagen mit einem `503 Service Unavailable` Fehler fehl, wenn der Cache-Cluster vom Ursprungscluster getrennt ist.

Kann ich mehrteilige S3-Operationen mit FlexCache Dualität verwenden?

Damit S3-Multipart-Operationen funktionieren, muss das Feld „granulare Daten“ des zugrunde liegenden FlexCache-Volumes auf „erweitert“ gesetzt sein. Dieses Feld wird auf den Wert gesetzt, der für das Ursprungsvolume festgelegt ist.

Unterstützt die Dualität von FlexCache HTTP- und HTTPS-Zugriff?

Ja. Standardmäßig ist HTTPS erforderlich. Sie können den S3-Dienst so konfigurieren, dass HTTP-Zugriff zugelassen wird, falls erforderlich.

S3-Zugriff auf NAS-FlexCache-Volumes aktivieren

Ab ONTAP 9.18.1 können Sie den S3-Zugriff auf NAS-FlexCache-Volumes aktivieren, auch als „Dualität“ bezeichnet. Dadurch können Clients auf Daten, die in einem FlexCache-Volume gespeichert sind, zusätzlich zu den herkömmlichen NAS-Protokollen wie NFS und SMB auch über das S3-Protokoll zugreifen. Sie können die folgenden Informationen verwenden, um die FlexCache-Dualität einzurichten.

Voraussetzungen

Bevor Sie beginnen, müssen Sie die folgenden Voraussetzungen erfüllen:

- Stellen Sie sicher, dass das S3-Protokoll und die gewünschten NAS-Protokolle (NFS, SMB oder beide) auf der SVM lizenziert und konfiguriert sind.

- Überprüfen Sie, ob DNS und alle anderen erforderlichen Dienste konfiguriert sind.
- Cluster und SVM Peered
- FlexCache Volume erstellen
- Data-lif erstellt



Eine ausführlichere Dokumentation zur FlexCache-Dualität finden Sie unter "[ONTAP S3 Multiprotokollunterstützung](#)".

Schritt 1: Zertifikate erstellen und signieren

Um den S3-Zugriff auf ein FlexCache-Volume zu aktivieren, müssen Sie Zertifikate für die SVM installieren, die das FlexCache-Volume hostet. In diesem Beispiel werden selbstsignierte Zertifikate verwendet, aber in einer Produktionsumgebung sollten Sie Zertifikate verwenden, die von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiert sind.

1. Erstellen einer SVM-Root-CA:

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

2. Generieren Sie eine Zertifikatsignierungsanforderung:

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

Beispielausgabe:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICzjCCABYCAQAwHzEdMBsGA1UEAxMUy2FjaGUxZy1kYXRhLm5hcy5sYWlwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCusJk07508Uh329cHI6x+BaRS2
w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK1CI2VEkrXGUg
...
vMIGN351+FgzLQ4X5lKfoMXCV70NqIakxzEmkTIUDKv7n9EVZ4b5DTTlrL03X/nK
+Bim2y2y180PaFB3NauZHTnIIzIc8zCp2IEqmFWyMDcdBjP9KS0+jNm4QhuXiM8F
D7gm3g/O70qa5OxbAEal5o4NbOl95U0T0rwqTaSzFG0XQnK2PmA1OIwS5ET35p3Z
dLU=
-----END CERTIFICATE REQUEST-----
```

Beispiel für einen privaten Schlüssel:

```

-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKYYwggSiAgEAAoIBAQCusJk07508Uh32
9cHI6x+BaRS2w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK
1CI2VEkrXGUgWbtx1K4IlrCTB829Q1aLGAQXVyWnzhQc4tS5PW/DsQ8t7olZ9zEI
...
rXGEddaqp7jQGNXUGlxbO3zcBil1/A9Hc6oalNECgYBKwe3PeZamiwhIHLY9ph7w
dJfFCshsPalMuAp2OuKIANa9l6fT9y5kf9tIbskT+t5Dth8bmV9pwe8UZaK5eC4
Svxm19jHT5Qql0DaZVUMMXFKyKoqPDdfvcDk2Eb5gMfIIb0a3TPC/jqqpDn9BzuH
TO02fuRvRR/G/HUz2yRd+A==
-----END PRIVATE KEY-----

```



Bewahren Sie eine Kopie Ihrer Zertifikatsanforderung und Ihres privaten Schlüssels für zukünftige Referenz auf.

3. Signieren Sie das Zertifikat:

Das root-ca ist diejenige, die Sie in [Erstellen Sie eine SVM-Root-CA](#) erstellt haben.

```

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

```

4. Fügen Sie die in [Generieren Sie eine Zertifikatsignierungsanforderung](#) generierte Zertifikatsignierungsanforderung (CSR) ein.

Beispiel:

```

-----BEGIN CERTIFICATE REQUEST-----
MIICzjCCAbYCAQAwHzEdMBsGA1UEAxMUy2FjaGUxZy1kYXRhLm5hcy5sYWlwgGEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCusJk07508Uh329cHI6x+BaRS2
w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK1CI2VEkrXGUg
...
vMIGN351+FgzLQ4X5lKfoMXCV70NqIakxzEmkTIUDKv7n9EVZ4b5DTTlrL03X/nK
+Bim2y2y180PaFB3NauZHTnIIzIc8zCp2IEqmFWyMDcdBjP9KS0+jNm4QhuXiM8F
D7gm3g/O70qa50xbAEal5o4NbOl95U0T0rwqTaSzFG0XQnK2PmA1OIwS5ET35p3Z
dLU=
-----END CERTIFICATE REQUEST-----

```

Dadurch wird ein signiertes Zertifikat auf der Konsole ausgegeben, ähnlich wie im folgenden Beispiel.

Beispiel für ein signiertes Zertifikat:

```

-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIIGHolbgv5DPowDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMwY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjIxNTU0WhcNMjYxMTIwMjIxNTU0WjAfMR0wGwYDVQQDEXRjYWNoZTFnLWRhdGEu
...
qS7zhj3ikWE3Gp9s+QijKWXx/0HDD1UuGqy0QZNqNm/M0mqVnokJNk5F4fBFxMiR
1o63BxL8xGIRdtTCjjb2Gq2Wj7EC1Uw6CykEkxAcVk+XrRtArGkNtcYdtHfUsKVE
wswvv0rNydrNnWhJLhS18TW5Tex+OMyTXgk9/3K8kB0mAMrtxxYjt8tm+gztkivf
J0eoluDJhaNxqwEZRzFyGaa4k1+56oFzRfTc
-----END CERTIFICATE-----

```

5. Kopieren Sie das Zertifikat für den nächsten Schritt.

6. Installieren Sie das Serverzertifikat auf der SVM:

```

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

```

7. Fügen Sie das signierte Zertifikat von [Signieren Sie das Zertifikat](#) ein.

Beispiel:

```

Please enter Certificate: Press <Enter> [twice] when done
-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIIGHolbgv5DPowDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMwY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjIxNTU0WhcNMjYxMTIwMjIxNTU0WjAfMR0wGwYDVQQDEXRjYWNoZTFnLWRhdGEu
bmFzLmxhYjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK6wmTTvk7xS
...
qS7zhj3ikWE3Gp9s+QijKWXx/0HDD1UuGqy0QZNqNm/M0mqVnokJNk5F4fBFxMiR
1o63BxL8xGIRdtTCjjb2Gq2Wj7EC1Uw6CykEkxAcVk+XrRtArGkNtcYdtHfUsKVE
wswvv0rNydrNnWhJLhS18TW5Tex+OMyTXgk9/3K8kB0mAMrtxxYjt8tm+gztkivf
J0eoluDJhaNxqwEZRzFyGaa4k1+56oFzRfTc
-----END CERTIFICATE-----

```

8. Fügen Sie den privaten Schlüssel, der in [Generieren Sie eine Zertifikatsignierungsanforderung](#) generiert wurde, ein.

Beispiel:

```
Please enter Private Key: Press <Enter> [twice] when done
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKYYwggSiAgEAAoIBAQCusJk07508Uh32
9cHI6x+BaRS2w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK
1CI2VEkrXGUgwBtx1K4I1rCTB829Q1aLGAQXVyWnzhQc4tS5PW/DsQ8t7olZ9zEI
W/gaEIajgpXIwGNWZ+weKQK+yoolxC+gy4IUE7WvnEUiezaIdoqzyPhYq5GC4XWf
0johpQugOPe0/w2nVFRWJoFQp3ZP3NZAXc8H0qkRB6SjaM243XV2jnuEzX2joXvT
wHHH+IBAQ2JDs7s1TY0I20e49J2Fx2+HvUxDx4BHao7CCHA1+MnmEl+9E38wTaEk
NLsU724ZAgMBAAECggEABHUY06wxcIk5h03S9Ik1FDZV3JWzsu5gGdLSQOHRd5W+
...
rXGEEdDaqp7jQGNXUGlxb03zcBil1/A9Hc6oalNECgYBKwe3PeZamiwhIHLy9ph7w
dJfFCshsPalMuAp2OuKIANa9l6ft9y5kf9tIbskT+t5Dth8bmV9pwe8UZaK5eC4
Svxm19jHT5QqloDaZVUmMXFKyKoqPDdfvcDk2Eb5gMfIIb0a3TPC/jqqpDn9BzuH
TO02fuRvRR/G/HUz2yRd+A==
-----END PRIVATE KEY-----
```

9. Geben Sie die Zertifikate der Zertifizierungsstellen (CA) ein, die die Zertifikatskette des Serverzertifikats bilden.

Dies beginnt mit dem ausstellenden CA-Zertifikat des Serverzertifikats und kann bis zum Root-CA-Zertifikat reichen.

```
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. Ermitteln Sie den öffentlichen Schlüssel für die SVM-Root-CA:

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

```
-----BEGIN CERTIFICATE-----
```

```
MIIDgTCCAmgAwIBAgIIGHokTnbsHKEwDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMwY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjE1NTIzWhcNMjYxMTIxMjE1NTIzWjAuMR8wHQYDVQDEExZjYWN0ZS0xNjRnLXN2
bS1yb290LWNhMQswCQYDVQGEwJVUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
```

```
...
```

```
DoOL7vZFFt44xd+rp0DwafhSnLH5HNhdIAfa2JvZW+eJ7rgevH9wmOzyc1vaihl3
Ewtb6cz1a/mtESSYRNBMGkIGM/SFCy5v1ROZXCzF96XPbYQN4cW0AYI3AHYBZP0A
HlNzDR8iml4k9IuKf6BHLFA+VwLTJJZKrdf5Jvjgh0trGAbQGI/Hp2Bjuiopkui+
n4aa5Rz0JFQopqQddAYnMuvqc10CyNn7S0vF/XLd3fJaprH8kQ==
```

```
-----END CERTIFICATE-----
```



Dies ist erforderlich, um den Client so zu konfigurieren, dass er den von der SVM-Root-CA signierten Zertifikaten vertraut. Der öffentliche Schlüssel wird in der Konsole ausgegeben. Kopieren und speichern Sie den öffentlichen Schlüssel. Die Werte in diesem Befehl sind die gleichen wie die, die Sie in [Erstellen Sie eine SVM-Root-CA](#) eingegeben haben.

Schritt 2: Konfigurieren Sie den S3-Server

1. S3-Protokollzugriff aktivieren:

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



S3 ist auf SVM-Ebene standardmäßig zulässig.

2. Eine vorhandene Richtlinie klonen:

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

3. Fügen Sie S3 zur geklonten Richtlinie hinzu:

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

4. Fügen Sie die neue Richtlinie der Daten-LIF hinzu:

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



Die Änderung der Dienstrichtlinie eines bestehenden LIF kann zu Störungen führen. Dazu muss das LIF heruntergefahren und anschließend mit einem Listener für den neuen Dienst neu gestartet werden. TCP sich davon zwar schnell erholen, dennoch sollten mögliche Auswirkungen beachtet werden.

5. Erstellen Sie den S3-Objektspeicherserver auf der SVM:

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

6. S3-Funktionalität auf dem FlexCache-Volume aktivieren:

Die `flexcache config` Option `-is-s3-enabled` muss auf `true` gesetzt werden, bevor Sie einen Bucket erstellen können. Sie müssen außerdem die Option `-is-writeback-enabled` auf `false` setzen.

Der folgende Befehl ändert eine bestehende FlexCache:

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

7. Erstellen Sie einen S3-Bucket:

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

8. Erstellen Sie eine Bucket-Richtlinie:

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

9. Erstellen Sie einen S3-Benutzer:

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

Beispielausgabe:


```
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. Schlüssel für den Root-Benutzer neu generieren:

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

Beispielausgabe:

```
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.
```

Schritt 3: Client einrichten

Es gibt viele S3-Clients. Ein guter Ausgangspunkt ist die AWS CLI. Weitere Informationen finden Sie unter ["Installation der AWS CLI"](#).

Managen Sie FlexCache Volumes

Erfahren Sie mehr über Auditing von ONTAP FlexCache Volumes

Ab ONTAP 9.7 können Sie NFS-Dateizugriff-Ereignisse in FlexCache Beziehungen mit nativem ONTAP-Auditing und Datei-Richtlinien-Management mit FPolicy prüfen.

Ab ONTAP 9.14.1 wird FPolicy für FlexCache-Volumes mit NFS oder SMB unterstützt. Zuvor wurde FPolicy nicht für FlexCache Volumes mit SMB unterstützt.

Native Audits und FPolicy werden mit denselben CLI-Befehlen konfiguriert und gemanagt, die für FlexVol Volumes verwendet werden. Jedoch gibt es ein paar verschiedene Verhaltensweisen mit FlexCache-Volumes.

- * Native Auditing*
 - Sie können ein FlexCache Volume nicht als Ziel für Prüfprotokolle verwenden.
 - Wenn Sie Lese- und Schreibvorgänge auf FlexCache-Volumes prüfen möchten, müssen Sie sowohl für die Cache-SVM als auch für die Ursprungs-SVM prüfen.

Der Grund dafür ist, dass Dateisystemvorgänge dort geprüft werden, wo sie verarbeitet werden. Das heißt, Lesevorgänge werden auf der Cache-SVM geprüft und Schreibvorgänge werden auf der ursprünglichen SVM geprüft.

- Um den Ursprung von Schreibvorgängen zu verfolgen, werden die SVM-UUID und MSID im Audit-Protokoll angehängt, um das FlexCache-Volume zu identifizieren, aus dem der Schreibvorgang stammt.

• FPolicy

- Obwohl Schreibvorgänge auf ein FlexCache Volume auf dem Ursprungs-Volume ausgeführt werden, überwachen FPolicy Konfigurationen die Schreibvorgänge auf dem Cache-Volume. Dies unterscheidet sich vom nativen Audit, bei dem die Schreibvorgänge auf das Ursprungs-Volume geprüft werden.
- Während ONTAP nicht die gleiche FPolicy Konfiguration auf Cache und Ursprungs-SVMs erfordert, wird jedoch empfohlen, dass Sie zwei ähnliche Konfigurationen implementieren. Dies ist möglich, indem Sie eine neue FPolicy für den Cache erstellen, die wie die der ursprünglichen SVM konfiguriert ist, aber mit dem Umfang der neuen Richtlinie auf die Cache-SVM beschränkt ist.
- Die Größe der Erweiterungen in einer FPolicy Konfiguration ist auf 20 KB (20480 Byte) beschränkt. Wenn die Größe der in einer FPolicy-Konfiguration auf einem FlexCache-Volume verwendeten Erweiterungen 20 KB überschreitet, wird die EMS-Meldung `nblade.fpolicy.extn.failed` ausgelöst.

Synchronisieren der Eigenschaften eines ONTAP FlexCache-Volumes von einem Ursprungs-Volume

Einige der Volume-Eigenschaften des FlexCache Volume müssen immer mit denen des Ursprungs-Volume synchronisiert werden. Wenn die Volume-Eigenschaften eines FlexCache-Volumes nicht automatisch synchronisiert werden, nachdem die Eigenschaften am Ursprungs-Volume geändert wurden, können Sie die Eigenschaften manuell synchronisieren.

Über diese Aufgabe

Die folgenden Volume-Eigenschaften eines FlexCache Volume müssen immer mit denen des Ursprungs-Volume synchronisiert werden:

- Sicherheitsstil (`-security-style`)
- Volume-Name (`-volume-name`)
- Maximale Verzeichnisgröße (`-maxdir-size`)
- Mindestvorlesbarkeit (`-min-readahead`)

Schritt

1. Synchronisieren Sie auf dem FlexCache Volume die Volume-Eigenschaften:

```
volume flexcache sync-properties -vserver svm_name -volume flexcache_volume
```

```
cluster1::> volume flexcache sync-properties -vserver vs1 -volume fc1
```

Aktualisieren Sie die Konfiguration von ONTAP FlexCache Beziehungen

Nach Ereignissen wie Volume-Verschiebung, Aggregatverschiebung oder Storage Failover werden die Volume-Konfigurationsinformationen auf das Ursprungs-Volume und das FlexCache Volume automatisch aktualisiert. Falls die automatischen Updates fehlschlagen, wird eine EMS-Nachricht generiert und dann müssen Sie die Konfiguration für die FlexCache-Beziehung manuell aktualisieren.

Wenn sich das Ursprungs-Volume und das FlexCache-Volume im getrennten Modus befinden, müssen Sie möglicherweise einige zusätzliche Operationen durchführen, um eine FlexCache-Beziehung manuell zu aktualisieren.

Über diese Aufgabe

Wenn Sie die Konfigurationen eines FlexCache-Volumes aktualisieren möchten, müssen Sie den Befehl aus dem ursprünglichen Volume ausführen. Wenn Sie die Konfigurationen eines Ursprungs-Volumes aktualisieren möchten, müssen Sie den Befehl aus dem FlexCache-Volume ausführen.

Schritt

1. Aktualisieren Sie die Konfiguration der FlexCache-Beziehung:

```
volume flexcache config-refresh -peer-vserver peer_svm -peer-volume  
peer_volume_to_update -peer-endpoint-type [origin | cache]
```

Aktivieren Sie die Updates für die Dateizugriffszeit auf dem ONTAP FlexCache Volume

Ab ONTAP 9.11.1 können Sie das `-atime-update` Feld auf dem FlexCache Volume aktivieren, um Zeitaktualisierungen für den Dateizugriff zuzulassen. Sie können auch einen Aktualisierungszeitraum für `-atime-update-period` die Zugriffszeit mit dem Attribut festlegen. Das `-atime-update-period` Attribut steuert, wie oft Updates der Zugriffszeit stattfinden können und wann sie auf das Ursprungs-Volume übertragen werden können.

Überblick

ONTAP bietet ein Feld auf Volume-Ebene namens `-atime-update`, zur Verwaltung von Updates der Zugriffszeit auf Dateien und Verzeichnisse, die mit LESE-, READLINK- und READDIR gelesen werden. Atime kommt bei Entscheidungen über den Daten-Lebenszyklus für Dateien und Verzeichnisse zum Einsatz, auf die selten zugegriffen wird. Die Dateien, auf die selten zugegriffen wird, werden zu Archiv-Storage migriert und oft später auf Tape verlagert.

Das Feld `atime-Update` ist bei vorhandenen und neu erstellten FlexCache-Volumes standardmäßig deaktiviert. Wenn Sie FlexCache Volumes mit ONTAP Versionen vor 9.11.1 verwenden, sollten Sie das Feld `atime-Update` deaktiviert lassen, damit Caches nicht unnötig entfernt werden, wenn auf dem Ursprungs-Volume ein Lesevorgang durchgeführt wird. Bei großen FlexCache Caches verwenden Administratoren jedoch spezielle Tools für das Datenmanagement und helfen sicherzustellen, dass „heiße“ Daten im Cache verbleiben und „kalte“ Daten gelöscht werden. Dies ist nicht möglich, wenn das `atime-Update` deaktiviert ist. Ab ONTAP 9.11.1 können Sie jedoch `-atime-update -atime-update-period`, die für das Management der zwischengespeicherten Daten erforderlichen Tools aktivieren und verwenden.

Bevor Sie beginnen

- Alle FlexCache Volumes müssen ONTAP 9.11.1 oder höher ausführen.
- Sie müssen den Berechtigungsmodus verwenden `advanced`.

Über diese Aufgabe

Die Einstellung `-atime-update-period` auf 86400 Sekunden ermöglicht nicht mehr als eine Aktualisierung der Zugriffszeit pro 24-Stunden-Zeitraum, unabhängig von der Anzahl der leseähnlichen Vorgänge, die für eine Datei durchgeführt werden.

Wenn Sie den `-atime-update-period` auf 0 setzen, werden für jeden Lesezugriff Nachrichten an den Ursprung gesendet. Der Ursprung informiert jedes FlexCache Volume darüber, dass das `atime` veraltet ist, was die Performance beeinträchtigt.

Schritte

1. Stellen Sie den Berechtigungsmodus auf `advanced`:

```
set -privilege advanced
```

2. Aktivieren Sie die Zeitaktualisierung des Dateizugriffs, und legen Sie die Aktualisierungshäufigkeit fest:

```
volume modify -volume vol_name -vserver <SVM name> -atime-update true -atime-update-period <seconds>
```

Das folgende Beispiel aktiviert `-atime-update` und setzt `-atime-update-period` auf 86400 Sekunden oder 24 Stunden:

```
c1: volume modify -volume origin1 vs1_c1 -atime-update true -atime-update-period 86400
```

3. Vergewissern Sie sich, dass `-atime-update` aktiviert ist:

```
volume show -volume vol_name -fields atime-update,atime-update-period
```

```
c1::*> volume show -volume cachel_origin1 -fields atime-update,atime-update-period
vserver volume          atime-update atime-update-period
-----
vs2_c1  cachel_origin1 true          86400
```

4. Nachdem `-atime-update` aktiviert ist, können Sie angeben, ob die Dateien auf einem FlexCache-Volume automatisch geschrubbt werden können und ein Scrubbing-Intervall:

```
volume flexcache config modify -vserver <SVM name> -volume <volume_name> -is-atime-scrub-enabled <true|false> -atime-scrub-period <integer>
```

Erfahren Sie mehr über `-is-atime-scrub-enabled` Parameter in der ["ONTAP-Befehlsreferenz"](#).

Globale Dateispernung auf ONTAP FlexCache Volumes

Ab ONTAP 9.10.1 kann die globale Dateispernung angewendet werden, um Lesevorgänge für alle im Cache gespeicherten Dateien zu vermeiden.

Wenn die globale Dateispernung aktiviert ist, werden Änderungen am Ursprungs-Volume ausgesetzt, bis alle FlexCache Volumes online sind. Sie sollten die globale Dateispernung nur aktivieren, wenn Sie die Zuverlässigkeit der Verbindungen zwischen Cache und Ursprung aufgrund von Suspensionen und möglichen Timeouts bei Offline-FlexCache-Volumes kontrollieren.

Bevor Sie beginnen

- Für die globale Dateispernung müssen die Cluster, die den Ursprung und alle zugehörigen Caches enthalten, ONTAP 9.9.1 oder höher ausführen. Die globale Dateispernung kann auf neuen oder bestehenden FlexCache Volumes aktiviert werden. Der Befehl kann auf einem Volume ausgeführt werden und gilt für alle zugehörigen FlexCache Volumes.
- Sie müssen sich in der erweiterten Berechtigungsebene befinden, um die globale Dateispernung zu aktivieren.
- Wenn Sie auf eine Version von ONTAP vor Version 9.9 zurücksetzen, muss die globale Dateispernung zunächst für den Ursprung und die zugehörigen Caches deaktiviert werden. Führen Sie zum Deaktivieren vom Ursprungs-Volume aus: `volume flexcache prepare-to-downgrade -disable-feature -set 9.10.0`
- Der Prozess zum Aktivieren der globalen Dateispernung hängt davon ab, ob der Ursprung über vorhandene Caches verfügt:
 - [\[enable-gfl-new\]](#)
 - [\[enable-gfl-existing\]](#)

Globale Dateispernung auf neuen FlexCache Volumes ermöglichen

Schritte

1. FlexCache Volume erstellen mit `-is-global-file-locking` set to true:

```
volume flexcache create volume volume_name -is-global-file-locking-enabled true
```



Der Standardwert von `-is-global-file-locking` ist „false“. Wenn nachfolgende `volume flexcache create` Befehle auf einem Volume ausgeführt werden, müssen sie mit `-is-global-file-locking enabled` Satz auf „true“ übergeben werden.

Globale Dateispernung auf vorhandenen FlexCache Volumes ermöglichen

Schritte

1. Die globale Dateispernung muss vom Ursprungsvolume festgelegt werden.
2. Der Ursprung kann keine anderen bestehenden Beziehungen haben (z. B. SnapMirror). Bestehende Beziehungen müssen distanziert werden. Alle Caches und Volumes müssen zum Zeitpunkt der Ausführung des Befehls verbunden sein. Um den Verbindungsstatus zu überprüfen, führen Sie folgende Schritte aus:

```
volume flexcache connection-status show
```

Der Status für alle aufgeführten Volumes sollte wie angezeigt werden `connected`.. Weitere Informationen finden Sie unter ["Anzeigen des Status einer FlexCache-Beziehung"](#) oder ["Eigenschaften eines FlexCache-Volumes von einem Ursprung synchronisieren"](#).

3. Globale Dateispernung in den Caches aktivieren:

```
volume flexcache origin config show/modify -volume volume_name -is-global-file  
-locking-enabled true
```

Verwandte Informationen

- ["ONTAP-Befehlsreferenz"](#)

ONTAP FlexCache Volumes werden vorab befüllt

Sie können ein FlexCache Volume vor dem Auffüllen vorladen, um den Zugriff auf im Cache gespeicherte Daten zu beschleunigen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator auf der erweiterten Berechtigungsebene sein
- Die Pfade, die Sie für die Vorbefüllung übergeben haben, müssen vorhanden sein oder der Voreinfüllen-Vorgang schlägt fehl.

Über diese Aufgabe

- Vorbefüllen liest nur Dateien und durchsucht Verzeichnisse
- Das `-isRecursion` Flag gilt für die gesamte Liste der an Prepopulate übergebenen Verzeichnisse

Schritte

1. Vorbefüllen eines FlexCache Volume:

```
volume flexcache prepopulate -cache-vserver vs1 -cache-volume -path  
-list path_list -isRecursion true|false
```

- Der `-path-list` Parameter gibt den relativen Verzeichnispfad an, den Sie ab dem Stammverzeichnis „Origin“ vorbelegen möchten. Wenn beispielsweise das Stammverzeichnis `-path-list dir1, dir2 -path-list /dir1, /dir2 " /origin"` lautet und die Verzeichnisse `/origin/dir1` und `/origin/dir2` enthält, können Sie die Pfadliste wie folgt angeben: Oder.
- Der Standardwert des `-isRecursion` Parameters ist `TRUE`.

In diesem Beispiel wird ein einzelner Verzeichnispfad vorausgefüllt:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache  
-volume fg_cachevol_1 -path-list /dir1  
(volume flexcache prepopulate start)  
[JobId 207]: FlexCache prepopulate job queued.
```

In diesem Beispiel werden Dateien aus mehreren Verzeichnissen vorausgefüllt:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1,/dir2,/dir3,/dir4
(volume flexcache prepopulate start)
[JobId 208]: FlexCache prepopulate job queued.
```

In diesem Beispiel wird eine einzelne Datei vorgefüllt:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1/file1.txt
(volume flexcache prepopulate start)
[JobId 209]: FlexCache prepopulate job queued.
```

In diesem Beispiel werden alle Dateien vom Ursprung vorausgefüllt:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list / -isRecursion true
(volume flexcache prepopulate start)
[JobId 210]: FlexCache prepopulate job queued.
```

Dieses Beispiel enthält einen ungültigen Pfad für die Vorbefüllung:

```
cluster1::*> flexcache prepopulate start -cache-volume
vol_cache2_vs3_c2_vol_origin1_vs1_c1 -cache-vserver vs3_c2 -path-list
/dir1, dir5, dir6
(volume flexcache prepopulate start)

Error: command failed: Path(s) "dir5, dir6" does not exist in origin
volume
      "vol_origin1_vs1_c1" in Vserver "vs1_c1".
```

2. Anzahl der gelesenen Dateien anzeigen:

```
job show -id job_ID -ins
```

Verwandte Informationen

- ["Jobanzeigen"](#)

Löschen Sie ONTAP FlexCache Beziehungen

Sie können eine FlexCache-Beziehung und das FlexCache-Volume löschen, wenn Sie das FlexCache-Volume nicht mehr benötigen.

Schritte

1. Versetzen Sie das FlexCache Volume in den Offline-Modus von dem Cluster, der das FlexCache Volume aufweist:

```
volume offline -vserver svm_name -volume volume_name
```

2. Löschen Sie das FlexCache Volume:

```
volume flexcache delete -vserver svm_name -volume volume_name
```

Die Details zur FlexCache Beziehung werden aus dem Ursprungs-Volume und dem FlexCache Volume entfernt.

FlexCache für die Behebung von Hotspots

Beseitigung von Hot-Spotting bei hochperformanten Computing-Workloads mit ONTAP FlexCache Volumes

Hotspot ist ein häufiges Problem bei vielen High-Performance-Computing-Workloads wie Animations-Rendering oder EDA. Hotspotting ist eine Situation, die auftritt, wenn ein bestimmter Teil des Clusters oder Netzwerks im Vergleich zu anderen Bereichen eine deutlich höhere Last aufweist, was zu Leistungsengpässen und einer verringerten Gesamteffizienz aufgrund des an diesem Standort konzentrierten übermäßigen Datenverkehrs führt. Beispielsweise ist eine oder mehrere Dateien eine große Nachfrage nach den ausgeführten Jobs. Dies führt zu einem Engpass bei der CPU, der für die Erfüllung von Anforderungen (über eine Volume-Affinität) an diese Datei verwendet wird. FlexCache kann dazu beitragen, diesen Engpass zu beseitigen, er muss jedoch ordnungsgemäß eingerichtet werden.

In dieser Dokumentation wird erklärt, wie FlexCache zur Behebung von Hotspotting eingerichtet wird.



Ab Juli 2024 wurden die Inhalte aus zuvor als PDFs veröffentlichten technischen Berichten in die ONTAP Produktdokumentation integriert. Dieser technische Bericht zur Behebung von ONTAP-Hotspots ist zum Zeitpunkt der Veröffentlichung vollkommen neu und wurde in keinem früheren Format erstellt.

Schlüsselkonzepte

Bei der Planung der Hotspot-Sanierung ist es wichtig, diese wesentlichen Konzepte zu verstehen.

- **High-Density FlexCache (HDF):** Ein FlexCache, der so wenige Knoten überspannt ist, wie es die Cache-Kapazitätsanforderungen erlauben
- **HDF Array (HDFA):** Eine Gruppe von HDFS, die Caches gleichen Ursprungs sind und über den Cluster verteilt sind
- **Inter-SVM HDFA:** Ein HDF aus der HDFA pro Server Virtual Machine (SVM)
- **Intra-SVM HDFA:** Alle HDFS im HDFA in einer SVM
- **Ost-West-Verkehr:** Cluster-Backend-Verkehr, der aus indirektem Datenzugriff generiert wird

Wie es weiter geht

- "Erfahren Sie, wie Sie mithilfe von hochdichten FlexCache Lösungen die Hot Spotting-Probleme beheben können"
- "Entscheiden Sie sich für die FlexCache Array-Dichte"
- "Bestimmen Sie die Dichte Ihres HDFS, und entscheiden Sie, ob Sie über NFS mit Inter-SVM HDFAs und Intra-SVM HDFAs auf HDFS zugreifen"
- "Konfiguration von HDFA und den Daten-LIFs, um die Vorteile des Intracluster Caching mit der ONTAP Konfiguration auszuschöpfen"
- "Erfahren Sie, wie Sie Clients konfigurieren, um ONTAP-NAS-Verbindungen mit der Client-Konfiguration zu verteilen"

Architektur einer Lösung zur Behebung von ONTAP FlexCache-Hotspots

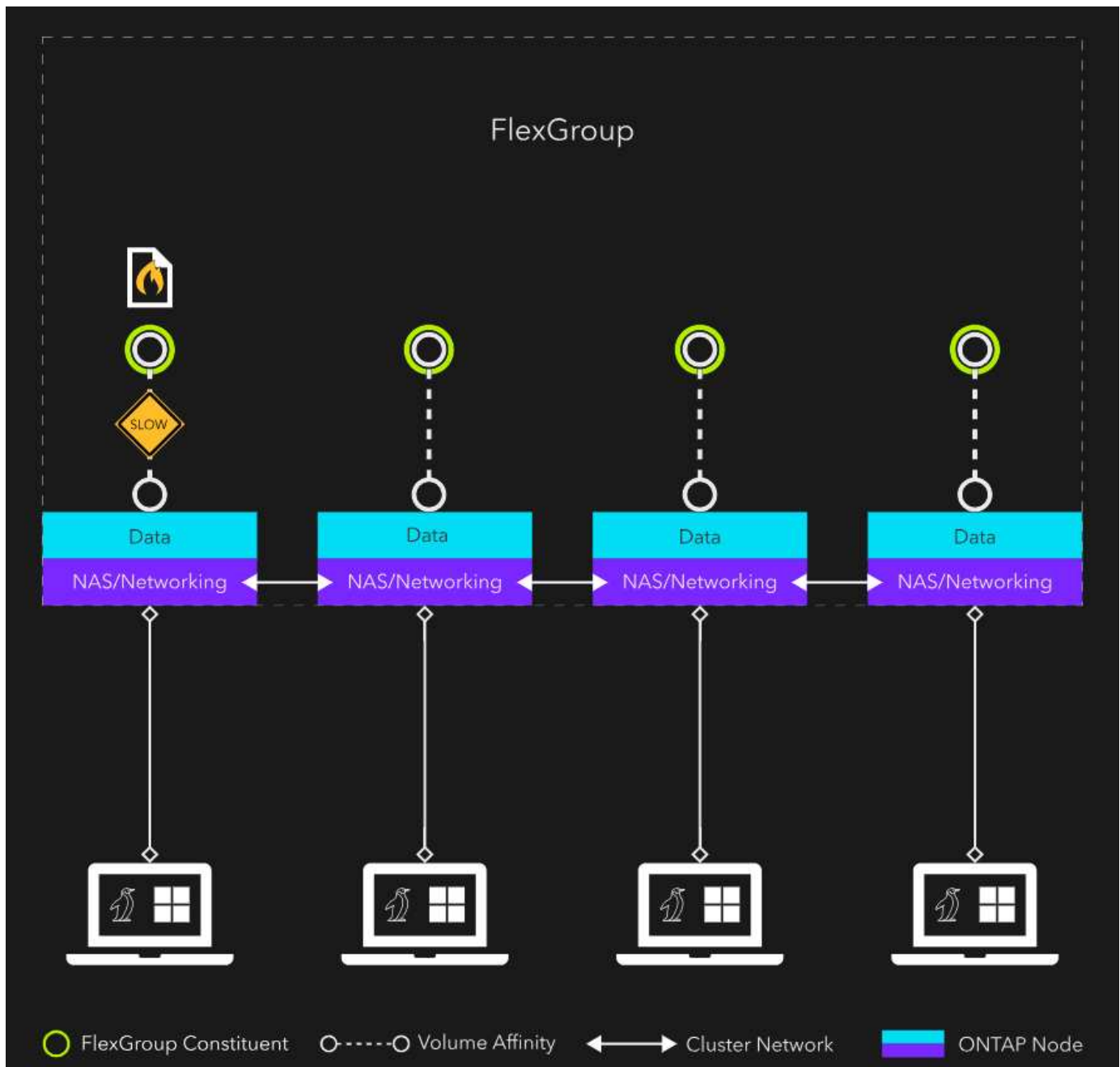
Untersuchen Sie zur Beseitigung von Hotspots die zugrunde liegenden Ursachen von Engpässen, warum FlexCache mit automatischer Bereitstellung nicht ausreicht und die technischen Details, die für eine effektive Entwicklung einer FlexCache Lösung erforderlich sind. Durch das Verständnis und die Implementierung von High-Density-FlexCache-Arrays (HDSA) können Sie die Performance optimieren und Engpässe bei High-Demand-Workloads beseitigen.

Engpassverständnis

Im Folgenden [Bild](#) wird ein typisches Hotspotting-Szenario mit einer Datei dargestellt. Das Volume ist eine FlexGroup mit einer einzelnen Komponente pro Node, und die Datei befindet sich auf Node 1.

Wenn Sie alle Netzwerkverbindungen der NAS-Clients auf verschiedene Nodes im Cluster verteilen, wird der Engpass auf der CPU weiterhin so verursacht, dass die Volume-Affinität dort bereitgestellt wird, wo sich die Hot File befindet. Außerdem führen Sie Cluster-Netzwerkverkehr (Ost-West-Datenverkehr) zu den Anrufen von Clients ein, die mit anderen Knoten als dem Speicherort der Datei verbunden sind. Der Overhead für Ost-West-Datenverkehr ist normalerweise klein, aber bei hochperformanten Computing-Workloads zählt jedes Bit.

Abbildung 1: FlexGroup-Hotspot-Szenario mit einer einzigen Datei

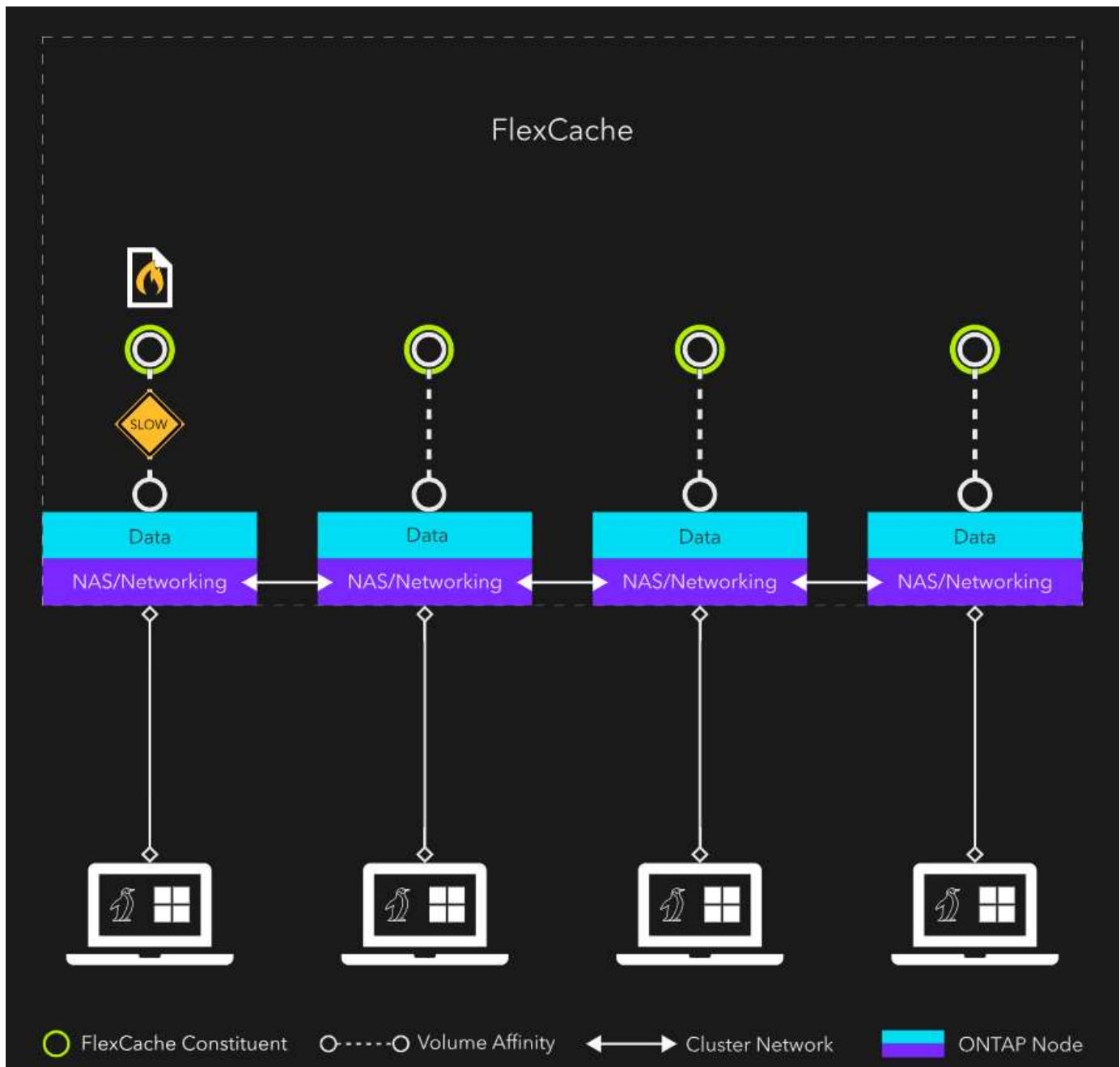


Warum ist eine FlexCache mit automatischer Bereitstellung nicht die Lösung

Um Hotspotting zu beheben, beseitigen Sie den CPU-Engpass und vorzugsweise auch den Ost-West-Verkehr. FlexCache kann Ihnen bei ordnungsgemäßer Einrichtung helfen.

Im folgenden Beispiel wird FlexCache automatisch mit System Manager, NetApp Console oder Standard-CLI-Argumenten bereitgestellt. [Abbildung 1](#) und [Abbildung 2](#) Auf den ersten Blick scheinen sie gleich zu sein: Beide sind NAS-Container mit vier Knoten und einem Bestandteil. Der einzige Unterschied besteht darin, dass der NAS-Container in [Abbildung 1](#) eine FlexGroup und der NAS-Container in [Abbildung 2](#) ein FlexCache ist. Jede Abbildung stellt denselben Engpass dar: die CPU von Knoten 1 für die Volume-Affinität, die den Zugriff auf die Hot-File bedient, und den Ost-West-Verkehr, der zur Latenz beiträgt. Ein automatisch bereitgestellter FlexCache hat den Engpass nicht beseitigt.

Abbildung 2: FlexCache-Szenario mit automatischer Bereitstellung



Anatomie eines FlexCache

Um eine FlexCache für die Behebung von Hotspots effektiv zu entwickeln, müssen Sie einige technische Details zu FlexCache verstehen.

FlexCache ist immer ein spärlicher FlexGroup. Ein FlexGroup besteht aus mehreren FlexVols. Diese FlexVols werden FlexGroup-Komponenten genannt. In einem Standard-FlexGroup-Layout gibt es eine oder mehrere Komponenten pro Node im Cluster. Die Bestandteile werden unter einer Abstraktionsschicht „zusammengenäht“ und dem Client als einzelner großer NAS-Container präsentiert. Wenn eine Datei in eine FlexGroup geschrieben wird, bestimmen Ingest Heuristics, auf welcher Komponente die Datei gespeichert werden soll. Es kann sich um eine Komponente handeln, die die NAS-Verbindung des Clients enthält, oder um einen anderen Node. Der Standort ist irrelevant, da alles unter der Abstraktionsebene läuft und für den Kunden unsichtbar ist.

Wenden wir nun dieses Verständnis von FlexGroup auf FlexCache an. Da FlexCache auf einer FlexGroup

basiert, verfügen Sie standardmäßig über eine einzelne FlexCache mit Komponenten auf allen Nodes im Cluster, wie in dargestellt. [Abbildung 1](#) In den meisten Fällen ist das eine großartige Sache. Sie nutzen alle Ressourcen in Ihrem Cluster.

Für die Behebung von Hot Files ist dies jedoch aufgrund der zwei Engpässe nicht ideal: CPU für eine einzelne Datei und Ost-West-Datenverkehr. Wenn Sie eine FlexCache mit Komponenten auf jedem Node für eine Hot File erstellen, bleibt diese Datei nur auf einer der Komponenten gespeichert. Das bedeutet, es gibt eine CPU, die den gesamten Zugriff auf die Hot File bedienen kann. Sie möchten auch die Menge des Ost-West-Verkehrs begrenzen, die erforderlich ist, um die Hot File zu erreichen.

Die Lösung besteht aus einer Reihe von FlexCaches mit hoher Dichte.

Anatomie eines hochdichten FlexCache

Eine High-Density FlexCache (HDF) verfügt über Komponenten auf so wenigen Knoten, wie die Kapazitätsanforderungen für die zwischengespeicherten Daten zulassen. Das Ziel besteht darin, dass Ihr Cache auf einem einzigen Knoten verwendet wird. Wenn Kapazitätsanforderungen das unmöglich machen, können stattdessen nur Komponenten auf wenigen Nodes verwendet werden.

Ein Cluster mit 24 Nodes könnte beispielsweise drei FlexCaches mit hoher Dichte aufweisen:

- Einer, der die Nodes 1 bis 8 umfasst
- Eine Sekunde, die die Nodes 9 bis 16 umfasst
- Ein Drittel, der die Knoten 17 bis 24 umfasst

Diese drei HDFS würden ein High-Density-FlexCache-Array (HDFA) bilden. Wenn die Dateien gleichmäßig in jedem HDF verteilt sind, besteht die Chance, dass die vom Client angeforderte Datei lokal an der Front-End-NAS-Verbindung gespeichert ist. Wenn 12 HDFS nur zwei Nodes umfassen, ergibt sich eine Wahrscheinlichkeit von 50 %, dass die Datei lokal gespeichert wird. Wenn Sie die HDF auf einen einzelnen Knoten reduzieren und 24 davon erstellen können, wird sichergestellt, dass die Datei lokal ist.

Diese Konfiguration beseitigt den gesamten Ost-West-Datenverkehr und bietet, was am wichtigsten ist, 24 CPUs/Volume-Affinitäten für den Zugriff auf die Hot File.

Was kommt als Nächstes?

["Entscheiden Sie sich für die FlexCache Array-Dichte"](#)

Verwandte Informationen

["Dokumentation zu FlexGroup und TRs"](#)

ONTAP FlexCache-Dichte ermitteln

Ihre erste Entscheidung für das Design zur Behebung von Hotspots ist die FlexCache-Dichte. Die folgenden Beispiele sind Cluster mit vier Nodes. Angenommen, die Dateianzahl wird gleichmäßig auf alle Komponenten in jedem HDF verteilt. Gehen Sie auch von einer gleichmäßigen Verteilung von Frontend-NAS-Verbindungen über alle Nodes aus.

Obwohl diese Beispiele nicht die einzigen Konfigurationen sind, die Sie verwenden können, sollten Sie das Leitprinzip verstehen, um so viele HDFS zu erstellen, wie Ihre Speicherplatzanforderungen und verfügbaren Ressourcen zulassen.

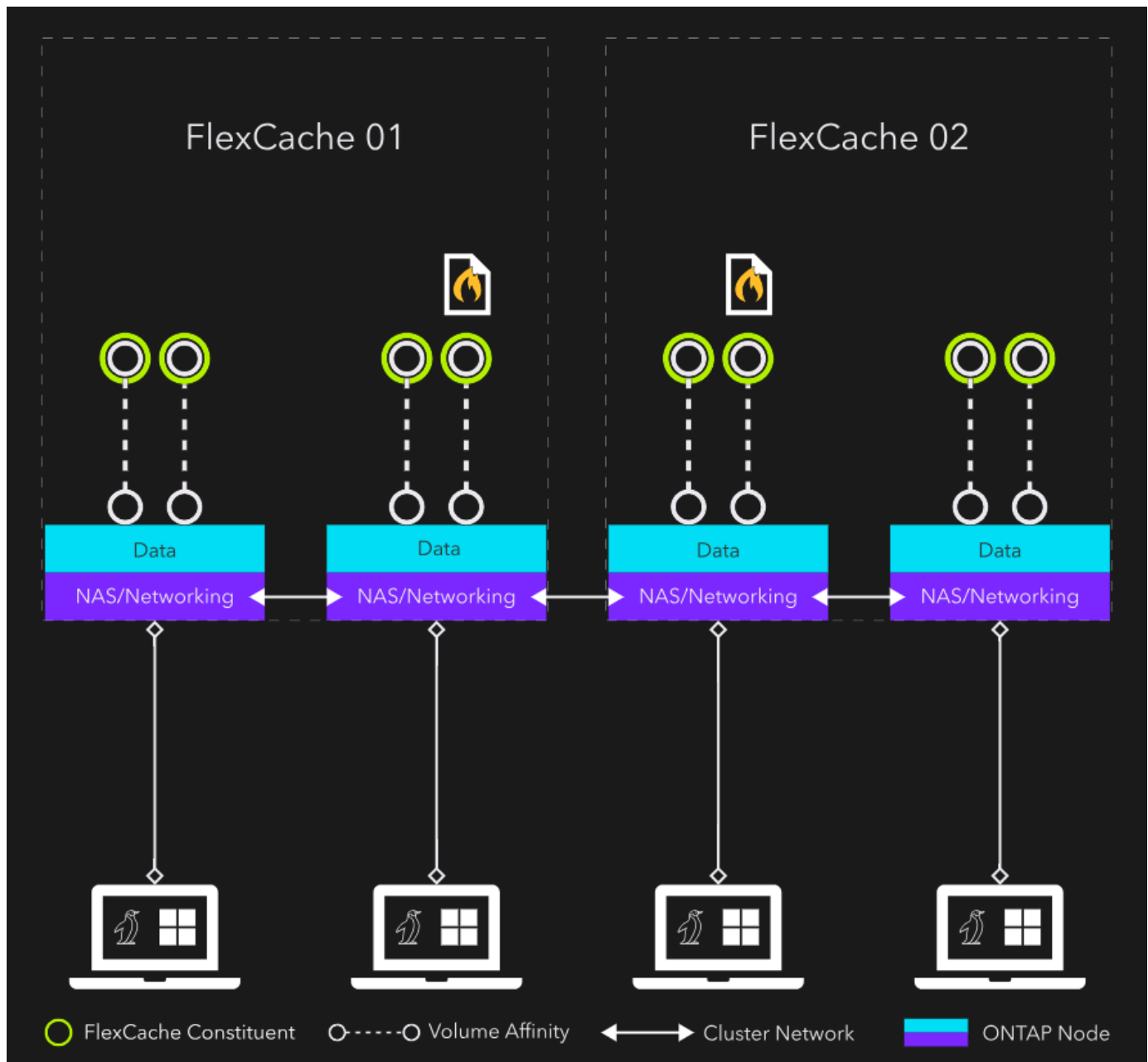


HDFAs werden mit folgender Syntax dargestellt: HDFs per HDFA x nodes per HDF x constituents per node per HDF

2x2 HDFA-Konfiguration

Abbildung 1 Zeigt ein Beispiel für eine 2x2 HDFA-Konfiguration: Zwei HDFS, die jeweils zwei Nodes abdecken und jeder Node zwei zusammengehörige Volumes enthält. In diesem Beispiel hat jeder Client eine Chance von 50 %, direkten Zugriff auf die Hot File zu haben. Zwei der vier Clients verfügen über Ost-West-Datenverkehr. Wichtig ist jedoch, dass es jetzt zwei HDFS gibt, was zwei unterschiedliche Caches der Hot File bedeutet. Es gibt jetzt zwei CPUs/Volume-Affinitäten, die den Zugriff auf die Hot File ermöglichen.

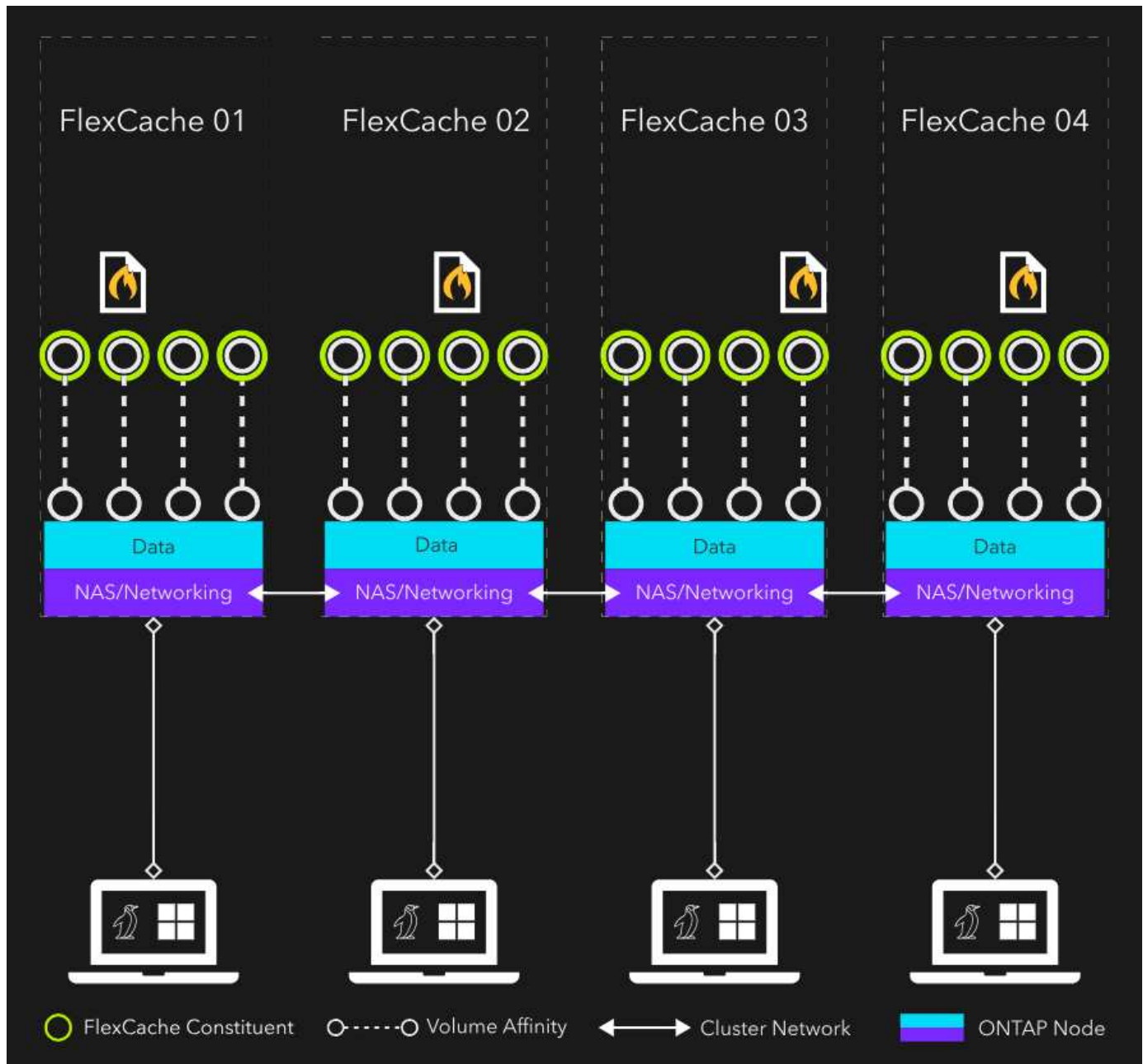
Abbildung 1: 2x2 HDFA-Konfiguration



4 x 1 x 4 HDFA-Konfiguration

Abbildung 2 Stellt eine optimale Konfiguration dar. Dies ist ein Beispiel für eine 4 x 1 x 4 HDFA-Konfiguration: Vier HDFS, jeweils in einem einzelnen Node enthalten, und jeder Node enthält vier Komponenten. In diesem Beispiel hat jeder Client garantiert direkten Zugriff auf einen Cache der Hot File. Da vier gecachte Dateien auf vier verschiedenen Nodes vorhanden sind, unterstützen vier verschiedene CPUs/Volume-Affinitäten den Zugriff auf die Hot File. Zusätzlich wird kein Ost-West-Verkehr erzeugt.

Abbildung 2: 4x1x4 HDFA-Konfiguration



Wie es weiter geht

Nachdem Sie festgelegt haben, wie dicht Sie Ihr HDFS erstellen möchten, müssen Sie eine weitere Designentscheidung treffen, wenn Sie mit NFS auf das HDFS zugreifen "[Inter-SVM HDFAs und Intra-SVM HDFAs](#)".

Bestimmen Sie eine ONTAP-interne oder SVM-interne HDFA-Option

Nachdem Sie die Dichte Ihres HDFS ermittelt haben, entscheiden Sie, ob Sie über NFS auf HDFS zugreifen, und erhalten Sie weitere Informationen zu den HDFA- und HDFA-Optionen zwischen SVMs und Intra-SVM.



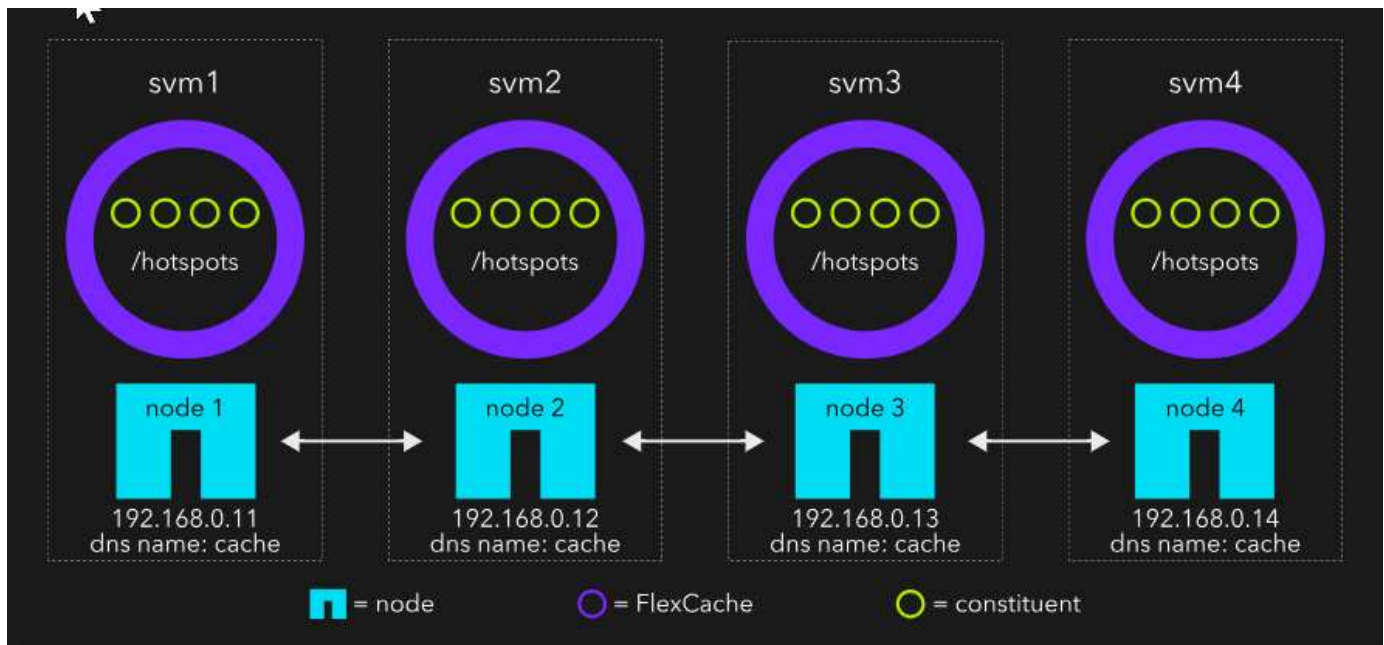
Wenn nur SMB-Clients auf HDFS zugreifen, sollten Sie alle HDFS in einer einzigen SVM erstellen. Informationen zur Verwendung von DFS-Zielen für den Lastausgleich finden Sie in der Windows-Clientkonfiguration.

SVM-interne HDFA-Implementierung

Für eine Inter-SVM HDFA muss für jeden HDF in der HDFA eine SVM erstellt werden. Dadurch können alle HDFS innerhalb der HDFA über denselben Verbindungspfad verfügen, was eine einfachere Konfiguration auf der Client-Seite ermöglicht.

In diesem [Abbildung 1](#) Beispiel befindet sich jeder HDF in einer eigenen SVM. Dies ist eine SVM-interne HDFA-Implementierung. Jeder HDF verfügt über einen Verbindungspfad von /Hotspots. Außerdem hat jede IP einen DNS-Eintrag mit Hostnamen-Cache. Diese Konfiguration nutzt DNS-Round-Robin, um Load-Balancing-Mounts über die verschiedenen HDFS durchzuführen.

Abbildung 1: 4x1x4 Inter-SVM HDFA-Konfiguration



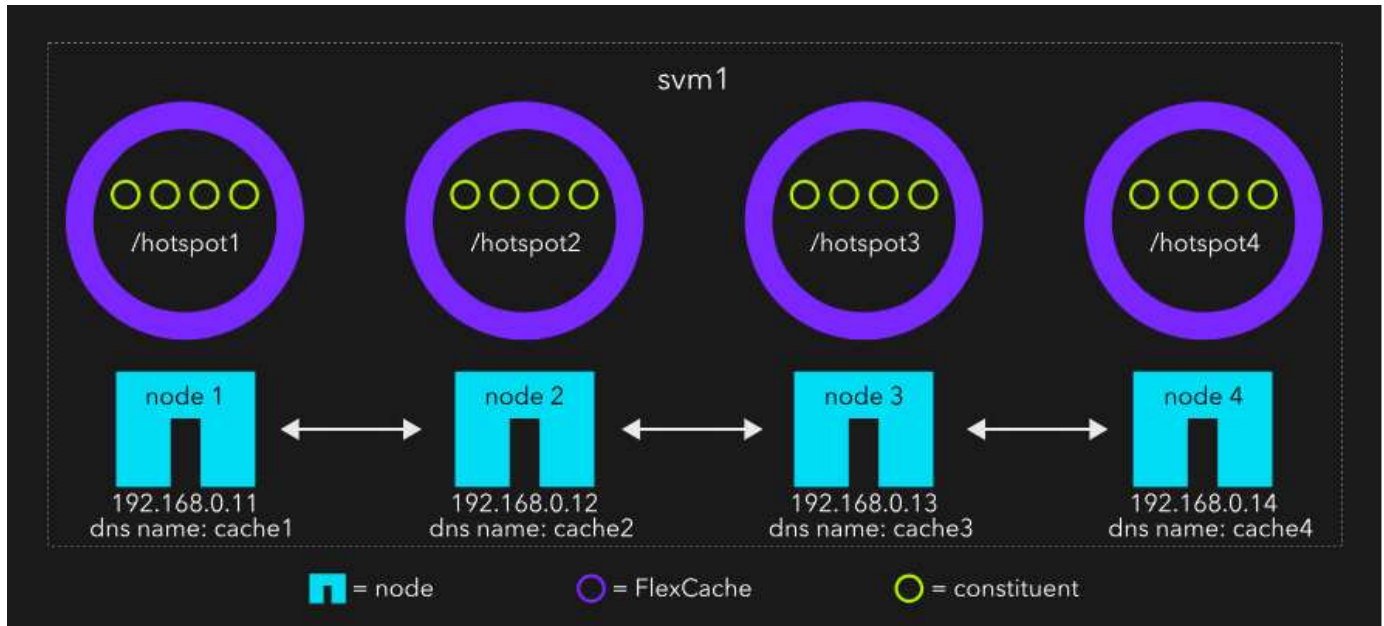
SVM-interne HDFA-Implementierung

Bei einer internen SVM muss für jede HDF ein eindeutiger Verbindungspfad vorhanden sein, doch alle HDFS befinden sich in einer SVM. Dieses Setup ist in ONTAP einfacher, da nur eine SVM benötigt wird, jedoch eine erweiterte Konfiguration auf Linux-Seite mit und eine LIF-Platzierung der Daten in ONTAP erforderlich `autoifs` ist.

Im [Abbildung 2](#) Beispiel befindet sich jede HDF in derselben SVM. Hierbei handelt es sich um eine SVM-interne HDFA-Implementierung, für die die Verbindungspfade eindeutig sein müssen. Damit der Lastausgleich ordnungsgemäß funktioniert, müssen Sie für jede IP einen eindeutigen DNS-Namen erstellen und die von dem Hostnamen auflöst Daten-LIFs nur auf den Nodes platzieren, auf denen sich der HDF befindet. Sie müssen

auch mit mehreren Einträgen konfigurieren `autofs`, wie in behandelt "[Linux-Client-Konfiguration](#)".

Abbildung 2: 4 x 1 x 4 intra-SVM-HDFA-Konfiguration



Wie es weiter geht

Jetzt haben Sie eine Vorstellung davon, wie Sie Ihre HDFAs einsetzen möchten, "[Stellen Sie die HDFA bereit, und konfigurieren Sie die Clients für den dezentralen Zugriff](#)".

Konfiguration der Datenschnittstellen HDFAs und ONTAP

Sie müssen HDFA und die Daten-LIFs entsprechend konfigurieren, um die Vorteile dieser Lösung zur Behebung von Hotspots nutzen zu können. Bei dieser Lösung werden Intracluster-Caching mit Ursprung und HDFA im selben Cluster verwendet.

Im Folgenden sind zwei HDFA-Beispielkonfigurationen aufgeführt:

- 2x2 x 2 Inter-SVM HDFA
- 4 x 1 x 4 intra-SVM HDFA

Über diese Aufgabe

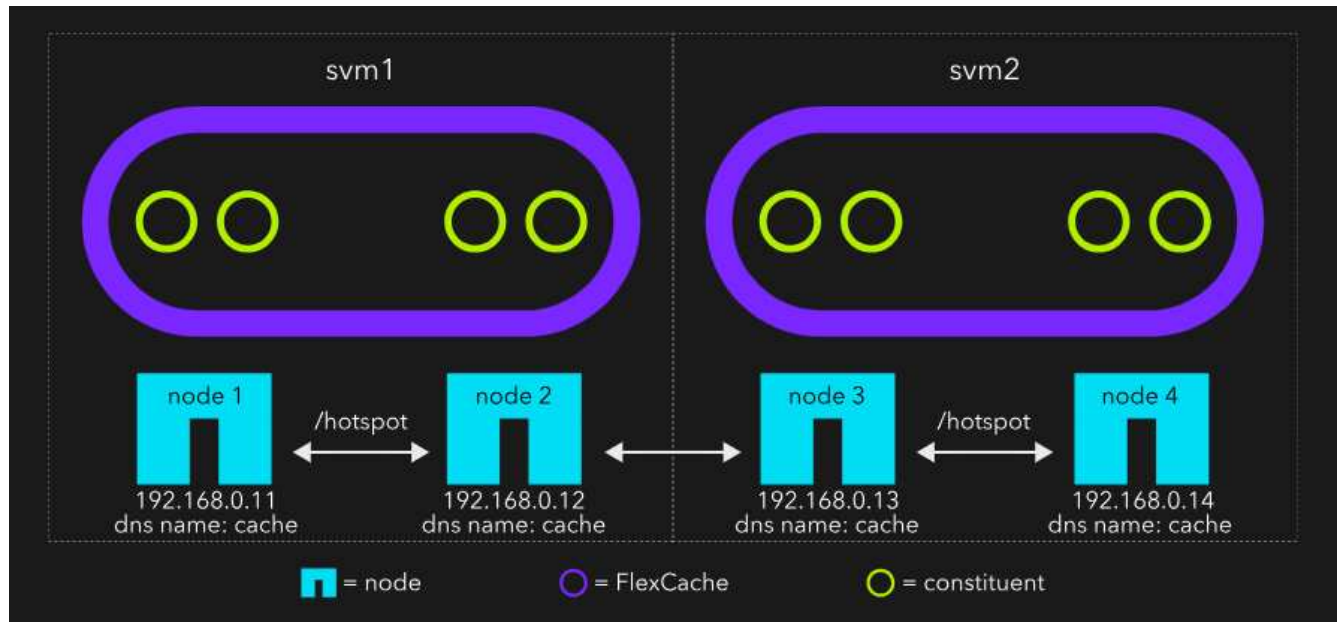
Führen Sie diese erweiterte Konfiguration mithilfe der ONTAP-CLI durch. Sie müssen im Befehl zwei Konfigurationen verwenden `flexcache create`, und eine Konfiguration, die Sie sicherstellen müssen, dass sie nicht konfiguriert ist:

- `-aggr-list`: Stellt ein Aggregat oder eine Liste von Aggregaten zur Verfügung, die sich auf dem Knoten oder Untergruppe von Knoten befinden, auf die Sie die HDF beschränken möchten.
- `-aggr-list-multiplier`: Bestimmen Sie, wie viele Bestandteile pro in der Option aufgelisteten Aggregat erstellt werden `aggr-list`. Wenn Sie zwei Aggregate aufgelistet haben, und setzen Sie diesen Wert auf 2, werden Sie am Ende mit vier Komponenten. NetApp empfiehlt bis zu 8 Komponenten pro Aggregat, aber auch 16.
- `-auto-provision-as`: Wenn Sie ausklinken, wird die CLI versuchen, `autofill` und setzen Sie den Wert auf `flexgroup`. Stellen Sie sicher, dass dies nicht konfiguriert ist. Löschen Sie die Datei, wenn sie angezeigt wird.

Erstellen Sie eine 2x2x2-Inter-SVM-HDFA-Konfiguration

- Um die Konfiguration eines 2x2x2 Inter-SVM HDFA wie in Abbildung 1 dargestellt zu unterstützen, füllen Sie ein Vorbereitungsblatt aus.

Abbildung 1: 2x2 Inter-SVM HDFA-Layout



SVM	Knoten pro HDF	Aggregate	Komponenten pro Node	Verbindungspf ad	Daten-LIF-IPs
svm1	node1, node2	aggr1, aggr2	2	/Hotspot	192.168.0.11, 192.168.0.12
svm2	node3, node4	aggr3, aggr4	2	/Hotspot	192.168.0.13, 192.168.0.14

- Erstellen Sie das HDFA. Führen Sie den folgenden Befehl zweimal für jede Zeile im Vorbereitungsblatt aus. Stellen Sie sicher, dass Sie die `vserver` Werte und `aggr-list` für die zweite Iteration anpassen.

```
cache::> flexcache create -vserver svm1 -volume hotspot -aggr-list
aggr1,aggr2 -aggr-list-multiplier 2 -origin-volume <origin_vol> -origin
-vserver <origin_svm> -size <size> -junction-path /hotspot
```

- Erstellung der Daten-LIFs. Führen Sie den Befehl viermal aus und erstellen Sie zwei Daten-LIFs pro SVM auf den im Vorbereitungsblatt aufgeführten Nodes. Stellen Sie sicher, dass Sie die Werte für jede Iteration entsprechend anpassen.

```
cache::> net int create -vserver svm1 -home-port e0a -home-node node1
-address 192.168.0.11 -netmask-length 24
```

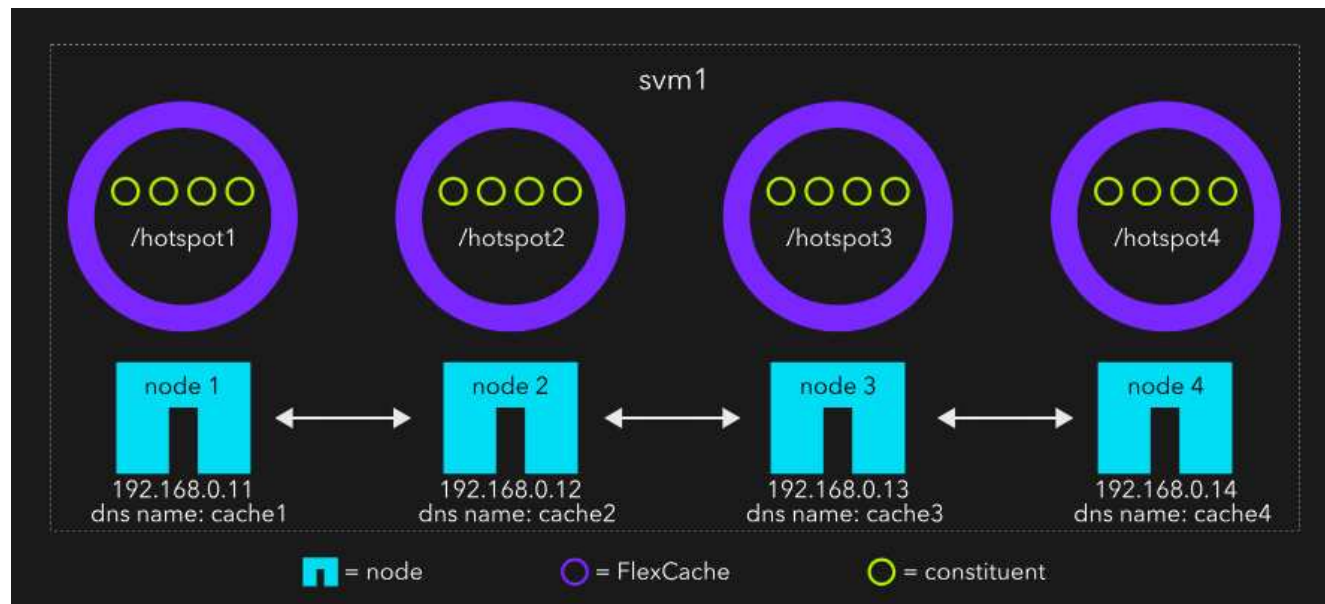
Wie es weiter geht

Jetzt müssen Sie Ihre Clients so konfigurieren, dass sie den HDFA entsprechend nutzen können. Siehe

Erstellen Sie ein 4 x 1 x 4-intra-SVM-HDFA

- Um die Konfiguration eines 4x1x4 Inter-SVM HDFA wie in Abbildung 2 dargestellt zu unterstützen, füllen Sie ein Vorbereitungsblatt aus.

Abbildung 2: 4 x 1 x 4 HDFA-Layout innerhalb einer SVM



SVM	Knoten pro HDF	Aggregate	Komponenten pro Node	Verbindungspf ad	Daten-LIF-IPs
svm1	node1	Aggr1	4	/Hotspot1	192.168.0.11
svm1	node2	aggr2	4	/Hotspot2	192.168.0.12
svm1	node3	aggr3	4	/Hotspot3	192.168.0.13
svm1	node4	aggr4	4	/Hotspot4	192.168.0.14

- Erstellen Sie das HDFS. Führen Sie den folgenden Befehl vier Mal für jede Zeile im Vorbereitungsblatt aus. Stellen Sie sicher, dass Sie die aggr-list Werte und junction-path für jede Iteration anpassen.

```
cache::> flexcache create -vserver svm1 -volume hotspot1 -aggr-list
aggr1 -aggr-list-multiplier 4 -origin-volume <origin_vol> -origin
-vserver <origin_svm> -size <size> -junction-path /hotspot1
```

- Erstellung der Daten-LIFs. Führen Sie den Befehl viermal aus und erstellen Sie insgesamt vier Daten-LIFs in der SVM. Pro Node sollte eine Daten-LIF vorhanden sein. Stellen Sie sicher, dass Sie die Werte für jede Iteration entsprechend anpassen.

```
cache::> net int create -vserver svm1 -home-port e0a -home-node node1
-address 192.168.0.11 -netmask-length 24
```

Wie es weiter geht

Jetzt müssen Sie Ihre Clients so konfigurieren, dass sie den HDFA entsprechend nutzen können. Siehe ["Client-Konfiguration"](#).

Konfigurieren Sie Clients für die Verteilung von ONTAP NAS-Verbindungen

Um das Hotspotting zu beheben, konfigurieren Sie den Client ordnungsgemäß, damit er seinen Teil zur Vermeidung von CPU-Engpässen verwendet.

Linux-Client-Konfiguration

Unabhängig davon, ob Sie sich für eine SVM- oder SVM-interne HDFA-Implementierung entscheiden, sollten Sie in Linux verwenden `autofs`, um sicherzustellen, dass die Clients über die verschiedenen HDFS verteilt werden. Die `autofs` Konfiguration unterscheidet sich je nach SVM und innerhalb der SVM.

Bevor Sie beginnen

Sie benötigen `autofs` und die entsprechenden Abhängigkeiten installiert. Hilfe hierzu finden Sie in der Linux-Dokumentation.

Über diese Aufgabe

Bei den beschriebenen Schritten wird eine Beispieldatei mit dem folgenden Eintrag verwendet
`/etc/auto_master`:

```
/flexcache auto_hotspot
```

Dadurch wird konfiguriert `autofs`, nach einer Datei zu suchen, die im `/etc` Verzeichnis aufgerufen `auto_hotspot` wird, wenn ein Prozess versucht, auf das Verzeichnis zuzugreifen `/flexcache`. Der Inhalt der `auto_hotspot` Datei bestimmt, welcher NFS-Server und welcher Verbindungspfad innerhalb des Verzeichnisses gemountet werden sollen `/flexcache`. Die beschriebenen Beispiele sind unterschiedliche Konfigurationen für die `auto_hotspot` Datei.

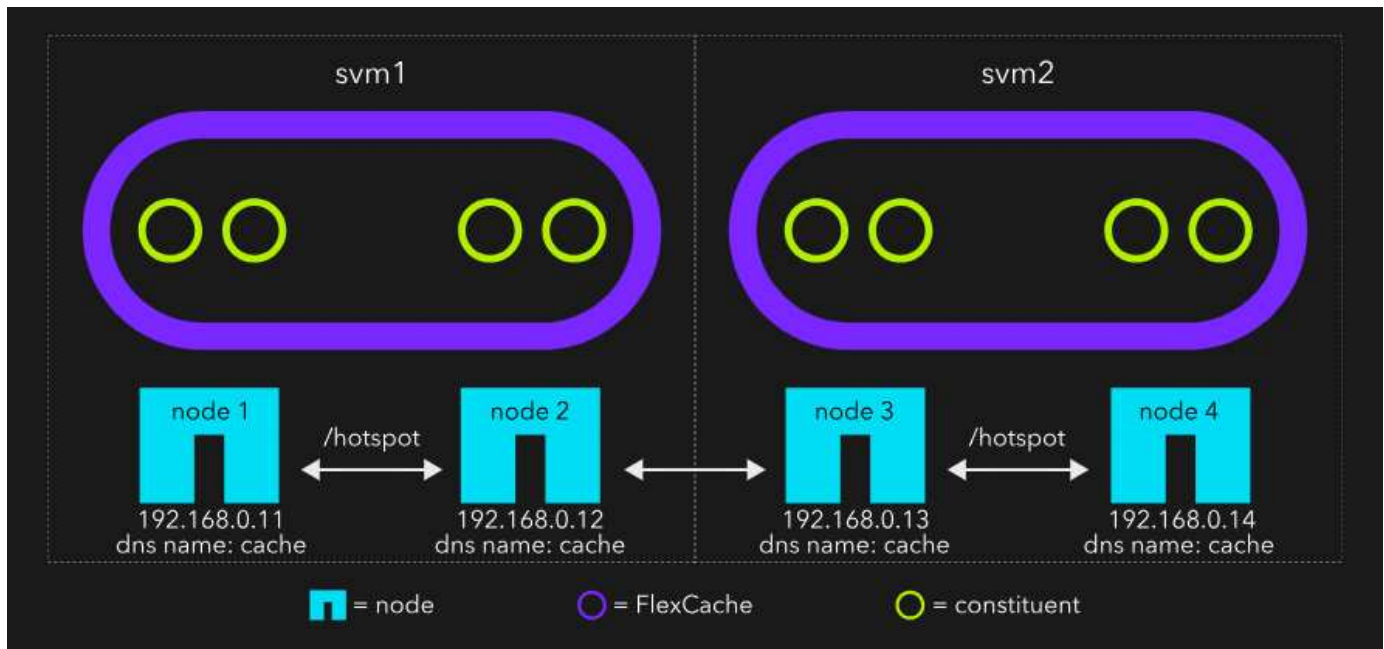
Autofs-Konfiguration der internen SVM-HDFA

Im folgenden Beispiel erstellen wir eine `autofs` Karte für das Diagramm in [Abbildung 1](#). Da jeder Cache denselben Verbindungspfad hat und der Hostname `cache` vier DNS A-Einträge enthält, benötigen wir nur eine Zeile:

```
hotspot cache:/hotspot
```

Diese eine einfache Zeile führt dazu, dass der NFS-Client eine DNS-Suche nach Hostnamen durchführt `cache`. DNS ist so eingerichtet, dass die IPs im Round-Robin-Verfahren zurückgegeben werden. Dies führt zu einer gleichmäßigen Verteilung von Front-End-NAS-Verbindungen. Nachdem der Client die IP empfangen hat, wird der Junction-Path unter `/flexcache/hotspot` gemountet `/hotspot`. Es könnte mit SVM1, SVM2, SVM3 oder SVM4 verbunden werden, aber die besondere SVM spielt keine Rolle.

Abbildung 1: 2x2 Inter-SVM HDFA



Autofs-Konfiguration der internen SVM-HDFA

Im folgenden Beispiel erstellen wir eine `autofs` Karte für das Diagramm in [Abbildung 2](#). Wir müssen sicherstellen, dass die NFS-Clients die IPs mounten, die Teil der HDF-Verbindungspfadimplementierung sind. Mit anderen Worten, wir wollen nicht mit etwas anderem als IP 192.168.0.11 mounten. `/hotspot1` Dazu können wir alle vier IP/Junction-Path-Paare für eine lokale Mount-Position in der Karte auflisten `auto_hotspot`.



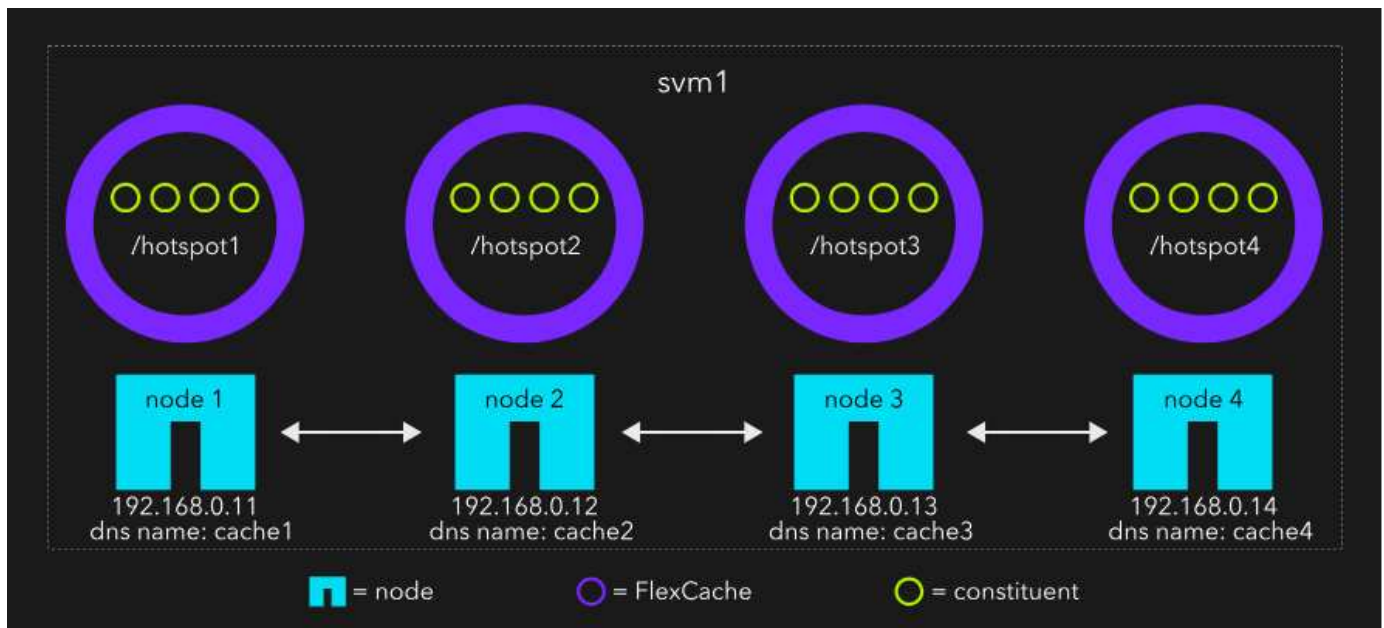
Der Backslash (\) im folgenden Beispiel setzt den Eintrag in die nächste Zeile fort und macht es leichter zu lesen.

```
hotspot    cache1:/hotspot1 \
           cache2:/hotspot2 \
           cache3:/hotspot3 \
           cache4:/hotspot4
```

Wenn der Client versucht, auf zuzugreifen `/flexcache/hotspot`, `autofs` wird eine Forward-Lookup für alle vier Hostnamen durchgeführt. Wenn alle vier IPs entweder im gleichen Subnetz wie der Client oder in einem anderen Subnetz sind, `autofs` gibt es einen NFS Null Ping zu jeder IP aus.

Für diesen Null-Ping muss das Paket vom NFS-Service von ONTAP verarbeitet werden, aber es benötigt keinen Festplattenzugriff. Der erste Ping-Befehl wird die IP sein und der Junction-Path wird `autofs` mounten.

Abbildung 2: 4 x 1 x 4 intra-SVM HDFA



Windows-Client-Konfiguration

Bei Windows-Clients sollten Sie eine intra-SVM-HDFA verwenden. Um einen Lastenausgleich über die verschiedenen HDFS in der SVM durchzuführen, müssen Sie jedem HDF einen eindeutigen Freigabennamen hinzufügen. Befolgen Sie anschließend die Schritte unter "[Microsoft-Dokumentation](#)", um mehrere DFS-Ziele für denselben Ordner zu implementieren.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.