S3-Client-Zugriff auf NAS-Daten bereitstellen

ONTAP 9

NetApp
November 05, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/s3-multiprotocol/index.html on November 05, 2026. Always check docs.netapp.com for the latest.

Inhalt

S3-Client-Zugriff auf NAS-Daten bereitstellen . . . 1
Informationen zur Multiprotokollunterstützung von ONTAP S3 . . . 1
Wie die Multiprotokollunterstützung von S3 funktioniert . . . 1
Datenschutz für S3 NAS Buckets . . . 2
Überwachung von S3 NAS Buckets . . . 2
Objekt-Multipart-Upload . . . 2
S3 und NAS Interoperabilität . . . 3
Informationen zu den NAS-Datenanforderungen für den ONTAP S3-Clientzugriff . . . 4
S3-Protokollzugriff auf NAS-Daten auf einer ONTAP SVM aktivieren . . . 5
Einen ONTAP S3 NAS Bucket erstellen . . . 7
ONTAP S3-Clientbenutzer aktivieren . . . 10

S3-Client-Zugriff auf NAS-Daten bereitstellen

Informationen zur Multiprotokollunterstützung von ONTAP S3

Ab ONTAP 9.12.1 ist es möglich, Clients, die das S3-Protokoll verwenden, den Zugriff auf dieselben Daten zu ermöglichen, die auch Clients mit den Protokollen NFS und SMB zur Verfügung stehen, ohne dass eine Neuformatierung erforderlich ist. Diese Funktion ermöglicht es, NAS-Daten weiterhin für NAS-Clients bereitzustellen, während Objektdaten für S3-Clients mit S3-Anwendungen (wie Data Mining und künstlicher Intelligenz) präsentiert werden.

Die Multiprotokoll-Funktionalität von S3 deckt zwei Anwendungsfälle ab:

1. Zugriff auf vorhandene NAS-Daten mithilfe von S3-Clients

   Wenn Ihre vorhandenen Daten mit herkömmlichen NAS-Clients (NFS oder SMB) erstellt wurden und sich auf NAS-Volumes (FlexVol oder FlexGroup Volumes) befinden, können analytische Tools auf S3-Clients verwendet werden, um auf diese Daten zuzugreifen.

2. Backend-Speicher für moderne Clients, die E/A mit sowohl NAS- als auch S3-Protokollen ausführen können

   Sie können integrierten Zugriff für Anwendungen wie Spark und Kafka bereitstellen, die dieselben Daten sowohl über die NAS- als auch über die S3-Protokolle lesen und schreiben können.

Wie die Multiprotokollunterstützung von S3 funktioniert

ONTAP Multiprotokollunterstützung ermöglicht die Darstellung desselben Datensatzes als Dateihierarchie oder als Objekte in einem Bucket. Dazu erstellt ONTAP „S3 NAS Buckets“, die es S3-Clients ermöglichen, Dateien im NAS-Speicher mithilfe von S3-Objektanfragen zu erstellen, zu lesen, zu löschen und aufzulisten. Diese Zuordnung entspricht der NAS-Sicherheitskonfiguration, wobei Datei- und Verzeichniszugriffsberechtigungen beachtet werden und bei Bedarf Einträge im Sicherheitsaudit-Protokoll erfolgen.

Diese Zuordnung erfolgt durch die Darstellung einer bestimmten NAS-Verzeichnishierarchie als S3-Bucket. Jede Datei in der Verzeichnishierarchie wird als S3-Objekt dargestellt, dessen Name relativ vom zugeordneten Verzeichnis abwärts ist, wobei Verzeichnisgrenzen durch das Schrägstrichzeichen ('/')

ONTAP-definierte S3-Benutzer können auf diesen Speicher zugreifen, wie durch die für den Bucket, der dem NAS-Verzeichnis zugeordnet ist, definierten Bucket-Richtlinien festgelegt. Damit dies möglich ist, müssen Zuordnungen zwischen den S3-Benutzern und den SMB/NFS-Benutzern definiert werden. Die Anmeldeinformationen des SMB/NFS-Benutzers werden für die NAS-Berechtigungsprüfung verwendet und in allen Audit-Protokollen aufgeführt, die aus diesen Zugriffen resultieren.

Wenn eine Datei von SMB- oder NFS-Clients erstellt wird, wird sie sofort in einem Verzeichnis abgelegt und ist daher für Clients sichtbar, bevor Daten hineingeschrieben werden. S3-Clients erwarten eine andere Semantik, bei der das neue Objekt im Namensraum erst sichtbar ist, nachdem alle seine Daten geschrieben wurden. Diese Zuordnung von S3 zu NAS-Speicher erstellt Dateien gemäß der S3-Semantik und hält die Dateien extern unsichtbar, bis der S3-Erstellungsbefehl abgeschlossen ist.

Datenschutz für S3 NAS Buckets

S3 NAS „buckets“ sind lediglich Zuordnungen von NAS-Daten für S3-Clients, sie sind keine Standard-S3-buckets. Daher besteht keine Notwendigkeit, S3 NAS buckets mit NetApp SnapMirror S3-Funktionalität zu schützen. Stattdessen können Volumes, die S3 NAS buckets enthalten, mit SnapMirror asynchroner Volume-Replikation geschützt werden. SnapMirror synchron und SVM-Desaster Recovery werden nicht unterstützt.

Ab ONTAP 9.14.1 werden S3 NAS Buckets in gespiegelten und ungespiegelten Aggregaten für MetroCluster IP- und FC-Konfigurationen unterstützt.

Informationen dazu "SnapMirror asynchron".

Überwachung von S3 NAS Buckets

Da S3 NAS Buckets keine herkömmlichen S3 Buckets sind, kann die S3 Audit Funktion nicht so konfiguriert werden, dass der Zugriff darauf protokolliert wird. Weitere Informationen zu "S3 Audit".

Dennoch können die in S3 NAS-Buckets abgebildeten NAS-Dateien und -Verzeichnisse mithilfe herkömmlicher ONTAP Auditverfahren auf Zugriffsereignisse geprüft werden. S3-Operationen können daher NAS Audit-Ereignisse auslösen, mit folgenden Ausnahmen:

- Wird der Zugriff eines S3-Clients durch die S3-Richtlinienkonfiguration (Gruppen- oder Bucket-Richtlinie) verweigert, wird keine NAS-Auditierung für das Ereignis initiiert. Dies ist darauf zurückzuführen, dass die S3-Berechtigungen geprüft werden, bevor SVM-Audit-Prüfungen erfolgen können.
- Wenn die Zieldatei einer S3 Get-Anfrage die Größe 0 hat, wird der Get-Anfrage der Inhalt 0 zurückgegeben und der Lesezugriff wird nicht protokolliert.
- Wenn sich die Zieldatei einer S3-Get-Anfrage in einem Ordner befindet, für den der Benutzer keine Traverse-Berechtigung besitzt, schlägt der Zugriffsversuch fehl und das Ereignis wird nicht protokolliert.

Informationen dazu "Überwachung von NAS-Ereignissen auf SVMs".

Objekt-Multipart-Upload

Ab ONTAP 9.16.1 wird der Multipart-Upload von Objekten in S3 NAS-Buckets unterstützt, wenn "fortschrittlicher Kapazitätsausgleich" auf dem zugrunde liegenden FlexGroup Volume aktiviert ist.

Der mehrteilige Upload von Objekten auf NAS-Dateispeicher ermöglicht einem S3-Protokollclient, ein großes Objekt als kleinere Teile hochzuladen. Der mehrteilige Upload von Objekten bietet folgende Vorteile:

- Es ermöglicht das parallele Hochladen von Objekten.
- Im Falle eines Upload-Fehlers oder einer Pause müssen nur die Teile, die noch nicht hochgeladen wurden, hochgeladen werden. Der Upload des gesamten Objekts muss nicht neu gestartet werden.
- Wenn die Größe des Objekts nicht im Voraus bekannt ist (zum Beispiel wenn ein großes Objekt noch geschrieben wird), können Clients sofort mit dem Hochladen von Teilen des Objekts beginnen und den Upload abschließen, nachdem das gesamte Objekt erstellt wurde.

> Mehrteilige Objekte in S3 NAS-Buckets müssen in ganzen Größen und nicht in Teilgrößen ausgerichtet sein. Zum Beispiel kann ein Teil 4MB oder 4GB oder eine ähnliche Größe haben. Ein Teil kann keine Teil- oder Unter-MB-Größen wie 4.5MB oder 4000.5MB verwenden.

Der Multipart Upload unterstützt die folgenden S3-Aktionen:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject (beginnend mit ONTAP 9.17.1)
- CreateMultipartUpload

  Ab ONTAP 9.17.1 unterstützt CreateMultipartUpload Tagging und Benutzer-Metadaten-Schlüssel/Wert-Paare.

- ListMultipartUploads
- UploadPart

> GET nach Teilenummer ("partNumber=xx") wird in S3 NAS Buckets nicht unterstützt. Stattdessen wird das vollständige Objekt zurückgegeben.

S3 und NAS Interoperabilität

ONTAP S3 NAS Buckets unterstützen die Standard-NAS- und S3-Funktionalität, außer wie hier aufgeführt.

NAS-Funktionalität wird von S3 NAS Buckets derzeit nicht unterstützt.

FabricPool Kapazitätsstufe

S3 NAS Buckets können nicht als Kapazitätsebene für FabricPool konfiguriert werden.

S3-Aktionen und Funktionen, die derzeit von S3 NAS Buckets nicht unterstützt werden

Aktionen

- ByPassGovernanceRetention
- CopyObject wird in SnapLock Volumes nicht unterstützt
- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- GetBucketObjectLockConfiguration
- GetBucketVersioning
- GetObjectRetention
- ListBucketVersioning
- ListObjectVersions
- PutBucketLifecycleConfiguration
- PutBucketVersioning
- PutObjectLockConfiguration
- PutObjectRetention

> Diese S3-Aktionen werden bei der Verwendung von S3 in S3 NAS-Buckets nicht unterstützt. Bei der Verwendung nativer S3-Buckets sind diese Aktionen "wie gewohnt unterstützt".

AWS-Benutzermetadaten

- Ab ONTAP 9.17.1 besteht Unterstützung für Metadaten mit Multipart-Objekten.

- Ab ONTAP 9.16.1 besteht Unterstützung für Metadaten mit einteiligen Objekten.
- Bei ONTAP 9.15.1 und früher werden die als Teil der S3-Benutzermetadaten empfangenen Schlüssel-Wert-Paare nicht zusammen mit den Objektdaten auf der Festplatte gespeichert.
- Bei ONTAP 9.15.1 und früher werden Anforderungsheader mit dem Präfix "x-amz-meta" ignoriert.

AWS Tags

- Ab ONTAP 9.17.1 besteht Unterstützung für Tags mit Multipart-Objekten.
- Ab ONTAP 9.16.1 besteht Unterstützung für Tags mit einteiligen Objekten.
- Bei ONTAP 9.15.1 und früher auf PUT-Objekt- und Multipart-Initiate-Anfragen werden Header mit dem Präfix "x-amz-tagging" ignoriert.
- Bei ONTAP 9.15.1 und früher werden Anfragen zum Aktualisieren von Tags auf einer bestehenden Datei (Put, Get und Delete Anfragen mit der Abfragezeichenfolge ?tagging) mit einem Fehler abgelehnt.

Versionierung

In der Bucket-Mapping-Konfiguration kann keine Versionierung angegeben werden.

- Anfragen, die nicht-null Versionsangaben enthalten (die versionId=xyz Abfragezeichenfolge), erhalten Fehlermeldungen.
- Anfragen zur Änderung des Versionierungsstatus eines Buckets werden mit Fehlermeldungen zurückgewiesen.

Informationen zu den NAS-Datenanforderungen für den ONTAP S3-Clientzugriff

Es ist wichtig zu verstehen, dass es bei der Zuordnung von NAS-Dateien und -Verzeichnissen für den S3-Zugriff zu gewissen Inkompatibilitäten kommen kann. Es kann erforderlich sein, die NAS-Dateihierarchien anzupassen, bevor sie mit S3 NAS-Buckets bereitgestellt werden.

Ein S3 NAS-Bucket bietet S3-Zugriff auf ein NAS-Verzeichnis, indem dieses Verzeichnis mithilfe der S3-Bucket-Syntax abgebildet wird, und die Dateien im Verzeichnisbaum werden als Objekte betrachtet. Die Objektnamen sind die durch Schrägstriche getrennten Pfadnamen der Dateien relativ zu dem in der S3-Bucket-Konfiguration angegebenen Verzeichnis.

Diese Zuordnung bringt einige Anforderungen mit sich, wenn Dateien und Verzeichnisse über S3 NAS Buckets bereitgestellt werden:

- S3-Namen sind auf 1024 Bytes begrenzt, daher sind Dateien mit längeren Pfadnamen über S3 nicht zugänglich.
- Datei- und Verzeichnisnamen sind auf 255 Zeichen beschränkt, daher darf ein Objektname nicht mehr als 255 aufeinanderfolgende Nicht-Schrägstrich-Zeichen („/“) enthalten.
- Ein SMB-Pfadname, der durch Backslash-Zeichen ('\') begrenzt ist, erscheint in s3 stattdessen als Objektname, der Forward-Slash-Zeichen ('/') enthält.
- Manche Paare gültiger S3-Objektnamen können nicht gleichzeitig im zugeordneten NAS-Verzeichnisbaum existieren. Beispielsweise entsprechen die gültigen S3-Objektnamen „part1/part2“ und „part1/part2/part3“ Dateien, die nicht gleichzeitig im NAS-Verzeichnisbaum existieren können, da „part1/part2“ im ersten Namen eine Datei und im anderen ein Verzeichnis ist.

- Wenn "part1/part2" eine vorhandene Datei ist, schlägt eine S3-Erstellung von "part1/part2/part3" fehl.
- Falls "part1/part2/part3" eine vorhandene Datei ist, schlägt eine S3-Erstellung oder -Entfernung von "part1/part2" fehl.
- Die Erstellung eines S3-Objekts, dessen Name mit dem eines bestehenden Objekts übereinstimmt, ersetzt dieses (in nicht versionierten Buckets); das gilt auch für NAS, erfordert jedoch eine exakte Übereinstimmung. Die obigen Beispiele führen nicht zur Entfernung des bestehenden Objekts, da die Namen zwar kollidieren, aber nicht übereinstimmen.

Ein Objektspeicher ist zwar darauf ausgelegt, eine sehr große Anzahl beliebiger Namen zu unterstützen, doch kann es bei einer NAS-Verzeichnisstruktur zu Leistungsproblemen kommen, wenn sehr viele Namen in einem Verzeichnis abgelegt werden. Insbesondere Namen ohne Schrägstrich (‘/’) werden alle im Stammverzeichnis des NAS-Mappings abgelegt. Anwendungen, die häufig Namen verwenden, die nicht „NAS-freundlich“ sind, wären besser in einem tatsächlichen Objektspeicher-Bucket als in einem NAS-Mapping aufgehoben.

S3-Protokollzugriff auf NAS-Daten auf einer ONTAP SVM aktivieren

Die Aktivierung des S3-Protokollzugriffs besteht darin, sicherzustellen, dass eine NAS-fähige SVM die gleichen Anforderungen erfüllt wie ein S3-fähiger Server, einschließlich des Hinzufügens eines Objektspeicherservers sowie der Überprüfung der Netzwerk- und Authentifizierungsanforderungen.

Bei neuen ONTAP-Installationen wird empfohlen, den S3-Protokollzugriff auf eine SVM zu aktivieren, nachdem diese für die Bereitstellung von NAS-Daten an Clients konfiguriert wurde. Weitere Informationen zur NAS-Protokollkonfiguration finden sich unter:

- "NFS-Konfiguration"
- "SMB-Konfiguration"

Bevor Sie beginnen

Folgendes muss konfiguriert werden, bevor das S3-Protokoll aktiviert wird:

- Das S3-Protokoll und die gewünschten NAS-Protokolle, NFS, SMB oder beide, sind lizenziert.
- Eine SVM ist für die gewünschten NAS-Protokolle konfiguriert.
- NFS- und/oder SMB-Server sind vorhanden.
- DNS und alle anderen erforderlichen Dienste sind konfiguriert.
- NAS-Daten werden exportiert oder für Clientsysteme freigegeben.

Über diese Aufgabe

Um HTTPS-Datenverkehr von S3-Clients zur S3-fähigen SVM zu ermöglichen, ist ein Zertifikat einer Zertifizierungsstelle (CA-Zertifikat) erforderlich. CA-Zertifikate können von drei Quellen verwendet werden:

- Ein neues selbstsigniertes ONTAP Zertifikat auf der SVM.
- Ein vorhandenes selbstsigniertes ONTAP Zertifikat auf der SVM.
- Ein Zertifikat eines Drittanbieters.

Sie können dieselben Daten-LIFs für den S3/NAS-Bucket verwenden, die Sie auch für die Bereitstellung von NAS-Daten nutzen. Falls spezifische IP-Adressen erforderlich sind, siehe "Daten-LIFs erstellen". Eine S3-

Service-Datenrichtlinie ist erforderlich, um den S3-Datenverkehr auf LIFs zu ermöglichen; die bestehende Service-Richtlinie der SVM kann angepasst werden, um S3 einzuschließen.

Beim Erstellen des S3-Objektservers sollten Sie darauf vorbereitet sein, den S3-Servernamen als vollqualifizierten Domänennamen (FQDN) einzugeben, den Clients für den S3-Zugriff verwenden. Der FQDN des S3-Servers darf nicht mit einem Bucket-Namen beginnen.

System Manager (ONTAP 9.16.1 und früher)

1. S3 kann auf einer Storage-VM mit konfigurierten NAS-Protokollen aktiviert werden.
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie eine NAS-fähige Speicher-VM aus, klicken Sie auf **Einstellungen** und dann unter **Protokolle > S3** auf ⚙ S3.
   b. Wählen Sie den Zertifikatstyp aus. Unabhängig davon, ob ein systemgeneriertes Zertifikat oder ein eigenes ausgewählt wird, ist es für den Clientzugriff erforderlich.
   c. Die Netzwerkschnittstellen eingeben.
2. Wenn das systemgenerierte Zertifikat ausgewählt wurde, werden die Zertifikatsinformationen angezeigt, sobald die Erstellung der neuen Storage-VM bestätigt ist. **Herunterladen** kann ausgewählt und das Zertifikat für den Clientzugriff gespeichert werden.
   ◦ Der geheime Schlüssel wird nicht erneut angezeigt.
   ◦ Falls Sie die Zertifikatsinformationen erneut benötigen: **Speicher > Speicher-VMs** auswählen, die Speicher-VM auswählen und auf **Einstellungen** klicken.

System Manager (ONTAP 9.17.1 und höher)

1. S3 kann auf einer Storage-VM mit konfigurierten NAS-Protokollen aktiviert werden.
   a. Klicken Sie auf **Cluster > Storage VMs**, wählen Sie eine NAS-fähige Storage VM aus, klicken Sie auf **Einstellungen** und anschließend unter **Protokolle > S3** auf ⚙.
   b. Wählen Sie den Zertifikatstyp aus. Unabhängig davon, ob ein systemgeneriertes Zertifikat oder ein eigenes ausgewählt wird, ist es für den Clientzugriff erforderlich.
   c. Die Netzwerkschnittstellen eingeben.
2. Wenn das systemgenerierte Zertifikat ausgewählt wurde, werden die Zertifikatsinformationen angezeigt, sobald die Erstellung der neuen Storage-VM bestätigt ist. **Herunterladen** kann ausgewählt und das Zertifikat für den Clientzugriff gespeichert werden.
   ◦ Der geheime Schlüssel wird nicht erneut angezeigt.
   ◦ Falls Sie die Zertifikatsinformationen erneut benötigen: Klicken Sie auf **Cluster > Storage VMs**, wählen Sie die Storage VM aus und klicken Sie auf **Einstellungen**.

CLI

1. Es sollte überprüft werden, ob das S3-Protokoll auf der SVM zugelassen ist:
   `vserver show -fields allowed-protocols`
2. Das öffentliche Schlüsselzertifikat für diese SVM ist zu notieren. + Falls ein neues selbstsigniertes ONTAP Zertifikat benötigt wird, siehe "Ein CA-Zertifikat auf der SVM erstellen und installieren".
3. Die Dienstdatenrichtlinie aktualisieren
   a. Die Dienstdatenrichtlinie für die SVM
   `network interface service-policy show -vserver svm_name` wird angezeigt.

   Weitere Informationen zu `network interface service-policy show` finden sich in der "ONTAP-Befehlsreferenz".

b. Fügen Sie das `data-core` und `data-s3-server services` hinzu, falls sie nicht vorhanden sind.
`network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`

4. Es sollte überprüft werden, ob die Daten-LIFs auf der SVM den Anforderungen entsprechen:
`network interface show -vserver svm_name`

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

5. Den S3-Server erstellen:
`vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

Zusätzliche Optionen können beim Erstellen des S3-Servers oder jederzeit später angegeben werden.

- HTTPS ist standardmäßig auf Port 443 aktiviert. Sie können die Portnummer mit der Option -secure -listener-port ändern. + Wenn HTTPS aktiviert ist, sind CA-Zertifikate für die korrekte Integration mit SSL/TLS erforderlich. Ab ONTAP 9.15.1 wird TLS 1.3 mit S3 Objektspeicher unterstützt.
- HTTP ist standardmäßig deaktiviert; wenn es aktiviert ist, lauscht der Server auf Port 80. HTTP kann mit der Option -is-http-enabled aktiviert oder die Portnummer mit der Option -listener-port geändert werden. + Wenn HTTP aktiviert ist, werden alle Anfragen und Antworten unverschlüsselt über das Netzwerk gesendet.

  1. Es sollte überprüft werden, ob S3 wie gewünscht konfiguriert ist:
  `vserver object-store-server show`

Beispiel + Der folgende Befehl überprüft die Konfigurationswerte aller Objektspeicherserver:
`cluster1::> vserver object-store-server show`

```
Vserver: vs1

                     Object Store Server Name: s3.example.com
                         Administrative State: up
                       Listener Port For HTTP: 80
                Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
            Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Verwandte Informationen

- "network interface service-policy add-service"

Einen ONTAP S3 NAS Bucket erstellen

Ein S3 NAS Bucket ist eine Zuordnung zwischen einem S3 Bucket-Namen und einem

NAS-Pfad. S3 NAS Buckets ermöglichen S3-Zugriff auf jeden Teil eines SVM-Namensraums mit vorhandenen Volumes und Verzeichnisstruktur.

Bevor Sie beginnen

- Ein S3-Objektserver ist in einer SVM konfiguriert, die NAS-Daten enthält.
- Die NAS-Daten entsprechen dem "Anforderungen für den S3-Clientzugriff".

Über diese Aufgabe

Sie können S3 NAS-Buckets so konfigurieren, dass beliebige Dateien und Verzeichnisse innerhalb des Stammverzeichnisses der SVM angegeben werden.

Sie können auch Bucket-Richtlinien festlegen, die den Zugriff auf NAS-Daten basierend auf einer beliebigen Kombination dieser Parameter erlauben oder verbieten:

- Dateien und Verzeichnisse
- Benutzer- und Gruppenberechtigungen
- S3 Operationen

Beispielsweise möchten Sie möglicherweise eine Bucket-Richtlinie einrichten, die einer großen Gruppe von Benutzern nur Lesezugriff auf Daten gewährt, und eine andere Bucket-Richtlinie, die es einer begrenzten Gruppe erlaubt, Operationen an einer Teilmenge dieser Daten durchzuführen.

Ab ONTAP 9.18.1 können Sie S3 NAS Buckets erstellen, die Anwendungen den Zugriff über das S3-Protokoll auf Daten in FlexCache Volumes ermöglichen. Bevor Sie über das S3-Protokoll auf ein FlexCache Volume zugreifen können, müssen Sie die `-is-s3-enabled`Option auf `true` "auf dem FlexCache Volume" setzen. Der Parameter ist standardmäßig auf `false` gesetzt.

Ab ONTAP 9.20.1 werden S3 NAS-Buckets auf FlexCache Volumes unterstützt, wenn das Ursprungsvolume ein FlexVol Volume ist.

In ONTAP 9.18.1 und 9.19.1 werden S3 NAS Buckets auf FlexCache Volumes nur unterstützt, wenn das FlexCache Ursprungsvolume ein FlexGroup Volume ist. Ab ONTAP 9.17.1 ist Folgendes möglich:

- die direkte Verknüpfung eines S3 NAS Bucket mit einem Volume anstatt mit dem Verbindungspfad. Standardmäßig ist ein S3 Bucket auf einem NAS Volume mit einem Verbindungspfad verknüpft, der von einem ONTAP Administrator jederzeit geändert werden kann. Diese Änderungen können den Betrieb des S3 Bucket beeinträchtigen.
- In der ONTAP CLI dient die `-is-nas-path-mutable false` Option mit dem `vserver object-store-server bucket create` Befehl zum Aktivieren der Verknüpfung des S3 NAS Buckets mit einem Volume. Standardmäßig ist `-is-nas-path-mutable` auf `true` gesetzt.

Da es sich bei S3 NAS "buckets" um Mappings und nicht um S3 buckets handelt, gelten die folgenden Eigenschaften von Standard S3 buckets nicht für S3 NAS buckets.

- **aggr-list \ aggr-list-multiplier \ storage-service-level \ volume \ size \ exclude-aggr-list \ qos-policy-group** + Beim Konfigurieren von S3 NAS Buckets werden keine Volumes oder Qtrees erstellt.
- **role \ is -protected \ is -protected-on-ontap \ is -protected-on-cloud** + S3 NAS Buckets werden nicht mit SnapMirror S3 geschützt oder gespiegelt, sondern nutzen stattdessen den regulären SnapMirror-Schutz auf Volume-Granularität.
- **Versionsstatus** + NAS-Volumes verfügen üblicherweise über Snapshot-Technologie zum Speichern verschiedener Versionen. Allerdings ist die Versionierung in S3 NAS-Buckets derzeit nicht verfügbar.

- **logical-used \ object-count** + Entsprechende Statistiken sind für NAS-Volumes über die Volume-Befehle verfügbar.
- **Multipart-Objekte** + Ab ONTAP 9.16.1 werden Multipart-Objekte in S3-NAS-Buckets unterstützt, wenn "fortschrittlicher Kapazitätsausgleich" auf dem zugrunde liegenden FlexGroup Volume aktiviert ist. Erweitertes Kapazitätsbalancing kann nur auf FlexGroup Volumes aktiviert werden. Auf FlexVol Volumes kann es nicht aktiviert werden.

  Ab ONTAP 9.20.1 wird der Zugriff auf S3 NAS Buckets auch für FlexCache Volumes mit FlexVol Ursprüngen unterstützt. Multipart Upload Vorgänge werden für S3 NAS Buckets auf FlexCache Volumes mit FlexVol Ursprüngen nicht unterstützt, da FlexVol Volumes Granular Data Distribution nicht unterstützen. Das Kopieren von Objekten innerhalb desselben FlexCache NAS Buckets ist möglich, wenn das Ursprungsvolume ein FlexVol Volume ist.

Schritte

Sie können den System Manager oder die ONTAP CLI verwenden, um einen NAS Bucket zu erstellen.

System Manager

Fügen Sie einen neuen S3 NAS-Bucket auf einer NAS-fähigen Storage-VM hinzu.

1. Klicken Sie auf **Speicher > Buckets** und anschließend auf **Hinzufügen**.
2. Geben Sie einen Namen für den S3 NAS-Bucket ein und wählen Sie die Storage-VM aus, geben Sie keine Größe ein, und klicken Sie dann auf **Weitere Optionen**.
3. Geben Sie einen gültigen Pfadnamen ein oder klicken Sie auf „Durchsuchen“, um aus einer Liste gültiger Pfadnamen auszuwählen. + Bei Eingabe eines gültigen Pfadnamens werden Optionen, die für die S3 NAS Konfiguration nicht relevant sind, ausgeblendet.
4. Wenn Sie bereits S3-Benutzer NAS-Benutzern zugeordnet und Gruppen erstellt haben, können Sie deren Berechtigungen konfigurieren und dann auf **Speichern** klicken. + Die S3-Benutzer müssen bereits NAS-Benutzern zugeordnet sein, bevor in diesem Schritt Berechtigungen konfiguriert werden.

Andernfalls auf **Speichern** klicken, um die S3 NAS-Bucket-Konfiguration abzuschließen.

CLI

1. Erstellen eines S3 NAS-Buckets in einer SVM, die NAS-Dateisysteme enthält.
   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -type nas -nas-path <junction_path> -is-nas-path-mutable
   true|false [-comment <text>]
   ```

   Beispiel 1: Erstellen eines S3 NAS Buckets

   ```
   cluster1::> vserver object-store-server bucket create -bucket testbucket
   -type nas -path /vol1
   ```

   Beispiel 2: Erstellen eines S3 NAS-Buckets und Verknüpfen des Buckets mit einem Volume

   ```
   vserver object-store-server bucket create -vserver vs1 -bucket nasbucket1
   -type nas -nas-path /pathA/dir1 -is-nas-path-mutable false
   ```

ONTAP S3-Clientbenutzer aktivieren

Um S3-Clientbenutzern den Zugriff auf NAS-Daten zu ermöglichen, müssen S3-Benutzernamen entsprechenden NAS-Benutzern zugeordnet und ihnen anschließend mithilfe von Bucket-Service-Richtlinien die Berechtigung zum Zugriff auf die NAS-Daten erteilt werden.

Bevor Sie beginnen

Benutzernamen für den Clientzugriff (LINUX/UNIX, Windows und S3-Clientbenutzer) müssen bereits vorhanden sein.

Sie sollten sich darüber im Klaren sein, dass einige S3 Funktionen "wird von S3 NAS Buckets nicht unterstützt".

Über diese Aufgabe

Durch die Zuordnung eines S3-Benutzernamens zu einem entsprechenden LINUX/UNIX- oder Windows-Benutzer werden Autorisierungsprüfungen für die NAS-Dateien beim Zugriff durch S3-Clients berücksichtigt. S3-zu-NAS-Zuordnungen werden durch Angabe eines S3-Benutzernamens *Muster*, der als einzelner Name oder als POSIX-Regulärer Ausdruck angegeben werden kann, und eines LINUX/UNIX- oder Windows-Benutzernamens *Ersatz* festgelegt.

Falls keine Namenszuordnung vorhanden ist, wird die Standard-Namenszuordnung verwendet, wobei der S3-Benutzername selbst als UNIX-Benutzername und Windows-Benutzername verwendet wird. Die Standardzuordnungen für UNIX- und Windows-Benutzernamen können mit dem `vserver object-store-server modify` Befehl angepasst werden.

Es wird nur die lokale Namenszuordnung unterstützt; LDAP wird nicht unterstützt.

Nachdem S3-Benutzer NAS-Benutzern zugeordnet wurden, können Benutzern Berechtigungen erteilt werden, indem die Ressourcen (Verzeichnisse und Dateien) angegeben werden, auf die sie Zugriff haben, sowie die Aktionen, die ihnen dort erlaubt oder nicht erlaubt sind.

System Manager

1. Lokale Namenszuordnungen für UNIX- oder Windows-Clients (oder beide) erstellen.
   a. **Speicher > Buckets** auswählen und anschließend die S3/NAS-fähige Storage-VM auswählen.
   b. Wählen Sie **Einstellungen** und klicken Sie dann auf →**Namenszuordnung** (unter **Hostbenutzer und -gruppen**).
   c. In den Kacheln **S3 zu Windows** oder **S3 zu UNIX** (oder beiden) auf **Hinzufügen** klicken, dann die gewünschten **Muster** (S3) und **Ersatz** (NAS) Benutzernamen eingeben.
2. Erstellen Sie eine Bucket-Richtlinie, um Clientzugriff zu gewähren.
   a. Klicken Sie auf **Speicher > Buckets**, klicken Sie auf ⋮ neben dem gewünschten S3-Bucket und dann auf **Bearbeiten**.
   b. **Hinzufügen** auswählen und die gewünschten Werte angeben.
      - **Principal** - S3-Benutzernamen angeben oder die Standardeinstellung (alle Benutzer) verwenden.
      - **Auswirkung** – **Zulassen** oder **Verweigern** auswählen.
      - **Aktionen** – Aktionen für diese Benutzer und Ressourcen eingeben. Die Menge der Ressourcenoperationen, die der Objektspeicherserver derzeit für S3 NAS Buckets unterstützt,

umfasst: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBucketVersioning, PutBucketVersioning und ListBucketVersions. Platzhalter sind für diesen Parameter zulässig.

- **Ressourcen** – Ordner- oder Dateipfade angeben, in denen die Aktionen erlaubt oder verweigert sind, oder die Standardeinstellungen verwenden (Stammverzeichnis des Buckets).

CLI

1. Lokale Namenszuordnungen für UNIX- oder Windows-Clients (oder beide) erstellen.
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` - Prioritätsnummer für die Kartenauswertung; 1 oder 2 eingeben.
   - `-pattern` - ein S3-Benutzername oder ein regulärer Ausdruck
   - `-replacement` - ein Windows- oder Unix-Benutzername

Beispiele

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1 vserver name-mapping create -direction s3-unix
-position 2 -pattern s3_user_1 -replacement unix_user_1
```

1. Erstellen Sie eine Bucket-Richtlinie, um Clientzugriff zu gewähren.
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` - legt fest, ob der Zugriff erlaubt oder verweigert wird, wenn ein Benutzer eine Aktion anfordert.
   - `-action <Action>, …` gibt an, welche Ressourcenoperationen zulässig oder verboten sind. Die Ressourcenoperationen, die der Objektspeicherserver aktuell für S3 NAS Buckets unterstützt, sind: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl und GetBucketLocation. Platzhalter sind für diesen Parameter zulässig.
   - `-principal <Objectstore Principal>, …` - prüft den Benutzer, der den Zugriff anfordert, anhand der in diesem Parameter angegebenen Benutzer oder Gruppen des Objektspeicherservers.
     - Eine Objektspeicher Servergruppe wird durch Hinzufügen des Präfixes group/ zum Gruppennamen angegeben.
     - `-principal` - (der Bindestrich) gewährt allen Benutzern Zugriff.
   - `-resource <text>, …` - Gibt den Bucket, Ordner oder das Objekt an, für das Berechtigungen erlaubt oder verweigert werden. Platzhalter sind für diesen Parameter zulässig.
   - `[-sid <SID>]` - gibt einen optionalen Textkommentar für die Objektspeicher Bucket-Richtlinienanweisung des Objektspeicherservers an.

Beispiele

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"
```

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

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 IRGENDEINER 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.