



Paralleles NFS

ONTAP 9

NetApp
January 08, 2026

Inhalt

- Paralleles NFS 1
 - Einführung 1
 - Erfahren Sie mehr über paralleles NFS (pNFS) in ONTAP..... 1
 - Lernen Sie die pNFS-Architektur in ONTAP kennen..... 2
 - pNFS-Anwendungsfälle in ONTAP 9
 - pNFS-Bereitstellungsstrategie in ONTAP 13
 - Planen 15
 - Plan für die pNFS-Implementierung 15
 - pNFS-Optimierung und Leistungsoptimierung – Best Practices 17
 - pNFS-Befehle, Statistiken und Ereignisprotokolle 22

Paralleles NFS

Einführung

Erfahren Sie mehr über paralleles NFS (pNFS) in ONTAP.

Parallel NFS wurde im Januar 2010 als RFC-Standard unter RFC-5661 eingeführt, um Clients den direkten Zugriff auf Dateidaten auf NFSv4.1-Servern zu ermöglichen, indem Metadaten- und Datenpfade getrennt werden. Dieser direkte Zugriff bietet Leistungsvorteile durch Datenlokalisierung, CPU-Effizienz und Parallelisierung von Operationen. Ein späterer RFC wurde im Jahr 2018 verfasst, der die pNFS-Layouttypen abdeckt (RFC-8434) und Standards für Datei-, Block- und Objekt-Layouts definiert. ONTAP nutzt den Dateilayouttyp für pNFS-Operationen.



Ab Juli 2024 werden Inhalte aus technischen Berichten, die zuvor als PDFs veröffentlicht wurden, in die ONTAP Produktdokumentation integriert. Die ONTAP NFS-Speicherverwaltungsdokumentation enthält nun Inhalte aus *TR-4063: Parallel Network File System (pNFS) in NetApp ONTAP*.

Jahrelang war NFSv3 die Standardversion des NFS-Protokolls, die für nahezu alle Anwendungsfälle verwendet wurde. Allerdings wies das Protokoll Einschränkungen auf, wie etwa fehlende Zustandsverwaltung, ein rudimentäres Berechtigungsmodell und grundlegende Sperrfunktionen. NFSv4.0 (RFC 7530) führte eine Reihe von Verbesserungen gegenüber NFSv3 ein und wurde mit den nachfolgenden Versionen NFSv4.1 (RFC 5661) und NFSv4.2 (RFC 7862) weiter verbessert, die Funktionen wie paralleles NFS (pNFS) hinzufügten.

Vorteile von NFSv4.x

NFSv4.x bietet gegenüber NFSv3 folgende Vorteile:

- Firewall-freundlich, da NFSv4 für seine Operationen nur einen einzigen Port (2049) verwendet.
- Fortschrittliches und aggressives Cache-Management, wie z. B. Delegationen in NFSv4.x
- Starke RPC-Sicherheitsoptionen, die Kryptografie einsetzen
- Internationalisierung von Zeichen
- Verbundoperationen
- Funktioniert nur mit TCP
- Zustandsbehaftetes Protokoll (nicht zustandslos wie NFSv3)
- Vollständige Kerberos-Integration für effiziente Authentifizierungsmechanismen
- NFS-Überweisungen
- Unterstützung von Zugriffskontrollsystemen, die mit UNIX und Windows kompatibel sind
- Zeichenkettenbasierte Benutzer- und Gruppenkennungen
- pNFS (NFSv4.1)
- Erweiterte Attribute (NFSv4.2)
- Sicherheitslabels (NFSv4.2)
- Sparse-File-Operationen (FALLOCATE) (NFSv4.2)

Weitere Informationen zu NFSv4.x im Allgemeinen, einschließlich Best Practices und Details zu den Funktionen, finden Sie unter ["NetApp Technical Report 4067: NFS Best Practice and Implementation Guide"](#)Die

Verwandte Informationen

- ["Übersicht über die NFS-Konfiguration"](#)
- ["NFS-Verwaltungsübersicht"](#)
- ["Management von FlexGroup Volumes"](#)
- ["Übersicht über NFS Trunking"](#)
- <https://www.netapp.com/pdf.html?item=/media/19370-tr-4523.pdf>
- ["Technischer Bericht von NetApp 4616: NFS Kerberos im ONTAP mit Microsoft Active Directory"](#)

Lernen Sie die pNFS-Architektur in ONTAP kennen.

Die pNFS-Architektur besteht aus drei Hauptkomponenten: einem NFS-Client, der pNFS unterstützt, einem Metadatenserver, der einen dedizierten Pfad für Metadatenoperationen bereitstellt, und einem Datenserver, der lokalisierte Pfade zu Dateien bereitstellt.

Der Clientzugriff auf pNFS erfordert eine Netzwerkverbindung zu den auf dem NFS-Server verfügbaren Daten- und Metadatenpfaden. Wenn der NFS-Server Netzwerkschnittstellen enthält, die von den Clients nicht erreichbar sind, kann der Server dem Client Datenpfade ankündigen, die nicht zugänglich sind, was zu Ausfällen führen kann.

Metadatenserver

Der Metadatenserver in pNFS wird eingerichtet, wenn ein Client eine Einbindung mit NFSv4.1 oder höher initiiert, sofern pNFS auf dem NFS-Server aktiviert ist. Sobald dies geschehen ist, wird der gesamte Metadatenverkehr über diese Verbindung gesendet und bleibt für die Dauer des Mountvorgangs auf dieser Verbindung, selbst wenn die Schnittstelle auf einen anderen Knoten migriert wird.

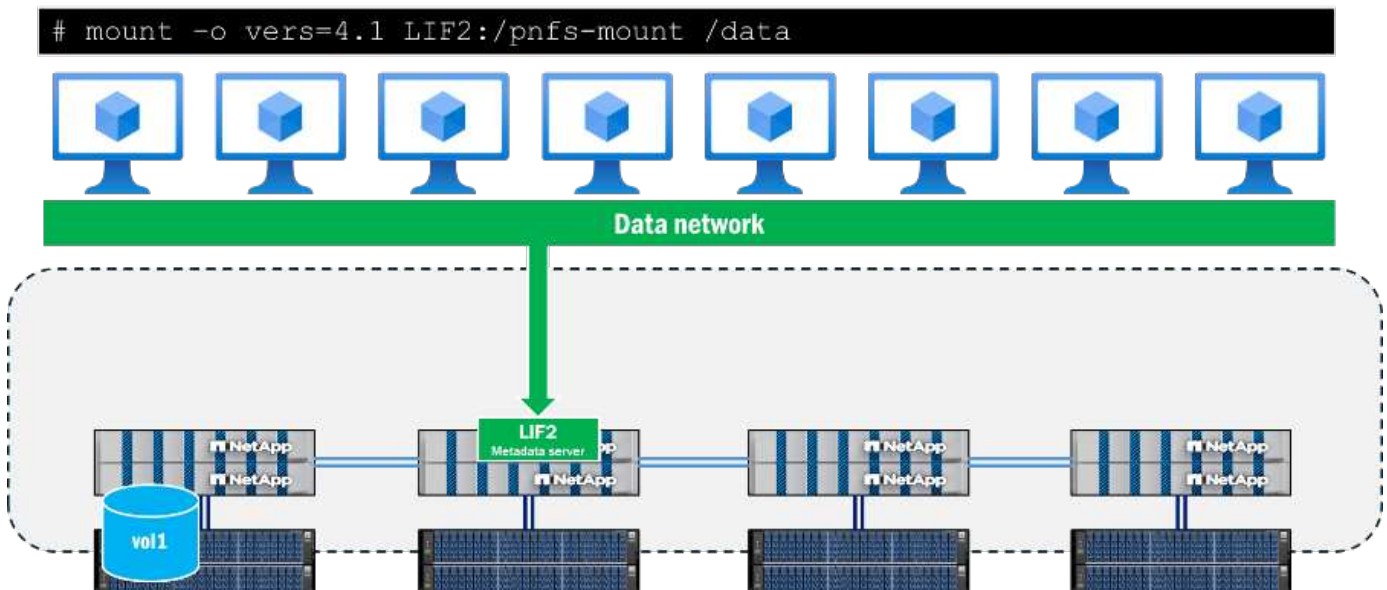


Abbildung 1. Richten Sie den Metadatenserver in pNFS in ONTAP ein.

Die pNFS-Unterstützung wird während des Mount-Aufrufs, insbesondere in den EXCHANGE_ID-Aufrufen, ermittelt. Dies kann in einer Paketerfassung unterhalb der NFS-Operationen als Flag gesehen werden. Wenn

die pNFS-Flags EXCHGID4_FLAG_USE_PNFS_DS Und EXCHGID4_FLAG_USE_PNFS_MDS Wenn der Wert auf 1 gesetzt ist, kann die Schnittstelle sowohl für Daten- als auch für Metadatenoperationen in pNFS verwendet werden.

```

  Operations (count: 1)
    Opcode: EXCHANGE_ID (42)
      Status: NFS4_OK (0)
      clientid: 0x004050a97100001c
      seqid: 0x00000001
    flags: 0x00060100, EXCHGID4_FLAG_USE_PNFS_DS, EXCHGID4_FLAG_USE_PNFS_MDS, EXCHGID4_FLAG_BIND_PRINC
      0... .. = EXCHGID4_FLAG_CONFIRMED_R: Not set
      .0.. .. = EXCHGID4_FLAG_UPD_CONFIRMED_REC_A: Not set
      ....1.. .. = EXCHGID4_FLAG_USE_PNFS_DS: Set
      ....1.. .. = EXCHGID4_FLAG_USE_PNFS_MDS: Set
      ....0.. .. = EXCHGID4_FLAG_USE_NON_PNFS: Not set
      ....1.. .. = EXCHGID4_FLAG_BIND_PRINC_STATEID: Set
      ....0.. .. = EXCHGID4_FLAG_SUPP_MOVED_MIGR: Not set
      ....0.. .. = EXCHGID4_FLAG_SUPP_MOVED_REFER: Not set

```

Abbildung 2. Paketerfassung für pNFS-Mount

Metadaten in NFS bestehen im Allgemeinen aus Datei- und Ordnerattributen wie Dateihandles, Berechtigungen, Zugriffs- und Änderungszeiten sowie Eigentümerinformationen. Metadaten können auch Erstellungs- und Löschaufufe, Verknüpfungs- und Aufhebungsaufufe sowie Umbenennungen umfassen.

In pNFS gibt es außerdem eine Teilmenge von Metadatenaufrufen, die spezifisch für die pNFS-Funktion sind und in [Referenz einfügen] detaillierter beschrieben werden. "[RFC 5661](#)"Die Diese Anrufe dienen dazu, pNFS-fähige Geräte zu ermitteln, Geräte Datensätzen zuzuordnen und weitere erforderliche Informationen zu erhalten. Die folgende Tabelle zeigt eine Liste dieser pNFS-spezifischen Metadatenoperationen.

Betrieb	Beschreibung
LAYOUTGET	Ruft die Datenserver-Zuordnung vom Metadatenserver ab.
LAYOUTCOMMIT	Die Server speichern das Layout und aktualisieren die Metadatenzuordnungen.
LAYOUTRETURN	Gibt das Layout oder, falls die Daten geändert wurden, das neue Layout zurück.
GEBÄUDEINFORMATIONEN	Der Client erhält aktualisierte Informationen von einem Datenserver im Speichercluster.
GERÄTELISTE	Der Client fordert die Liste aller Datenserver an, die am Speichercluster beteiligt sind.
CB_LAYOUTRECALL	Der Server ruft das Datenlayout vom Client ab, wenn Konflikte festgestellt werden.
CB_RECALL_ANY	Gibt alle Layouts an den Metadatenserver zurück.
CB_NOTIFY_DEVICEID	Meldet Änderungen der Geräte-ID.

Datenpfadinformationen

Sobald der Metadatenserver eingerichtet ist und die Datenoperationen beginnen, beginnt ONTAP mit der Verfolgung der Geräte-IDs, die für pNFS-Lese- und Schreibvorgänge geeignet sind, sowie der Gerätezuordnungen, die die Volumes im Cluster den lokalen Netzwerkschnittstellen zuordnen. Dieser Vorgang findet statt, wenn im Mount eine Lese- oder Schreiboperation durchgeführt wird. Metadatenaufrufe, wie z. B.

GETATTR. wird diese Gerätezuordnungen nicht auslösen. Daher ist das Betreiben eines `ls` Ein Befehl innerhalb des Mountpunkts aktualisiert die Zuordnungen nicht.

Geräte und Zuordnungen können mit der ONTAP CLI in erweiterten Berechtigungen angezeigt werden, wie unten dargestellt.

```
::*> pnfs devices show -vserver DEMO
(vserver nfs pnfs devices show)
Vserver Name      Mapping ID      Volume MSID      Mapping Status
Generation
-----
DEMO              16             2157024470      available      1

::*> pnfs devices mappings show -vserver SVM
(vserver nfs pnfs devices mappings show)
Vserver Name      Mapping ID      Dsid             LIF IP
-----
DEMO              16             2488             10.193.67.211
```



In diesen Befehlen sind die Volumennamen nicht vorhanden. Stattdessen werden die numerischen IDs verwendet, die diesen Datenträgern zugeordnet sind: die Master-Set-ID (MSID) und die Data-Set-ID (DSID). Um die den Zuordnungen zugeordneten Datenträger zu finden, können Sie Folgendes verwenden: `volume show -dsid [dsid_numeric]` oder `volume show -msid [msid_numeric]` mit erweiterten Berechtigungen der ONTAP CLI.

Wenn ein Client versucht, eine Datei auf einem Knoten zu lesen oder zu beschreiben, der nicht mit dem Metadatenserver verbunden ist, handelt pNFS die entsprechenden Zugriffspfade aus, um die Datenlokalität für diese Operationen zu gewährleisten, und der Client wird zum angekündigten pNFS-Gerät umgeleitet, anstatt zu versuchen, das Clusternetzwerk zu durchlaufen, um auf die Datei zuzugreifen. Dies trägt dazu bei, die CPU-Auslastung und die Netzwerklatenz zu reduzieren.

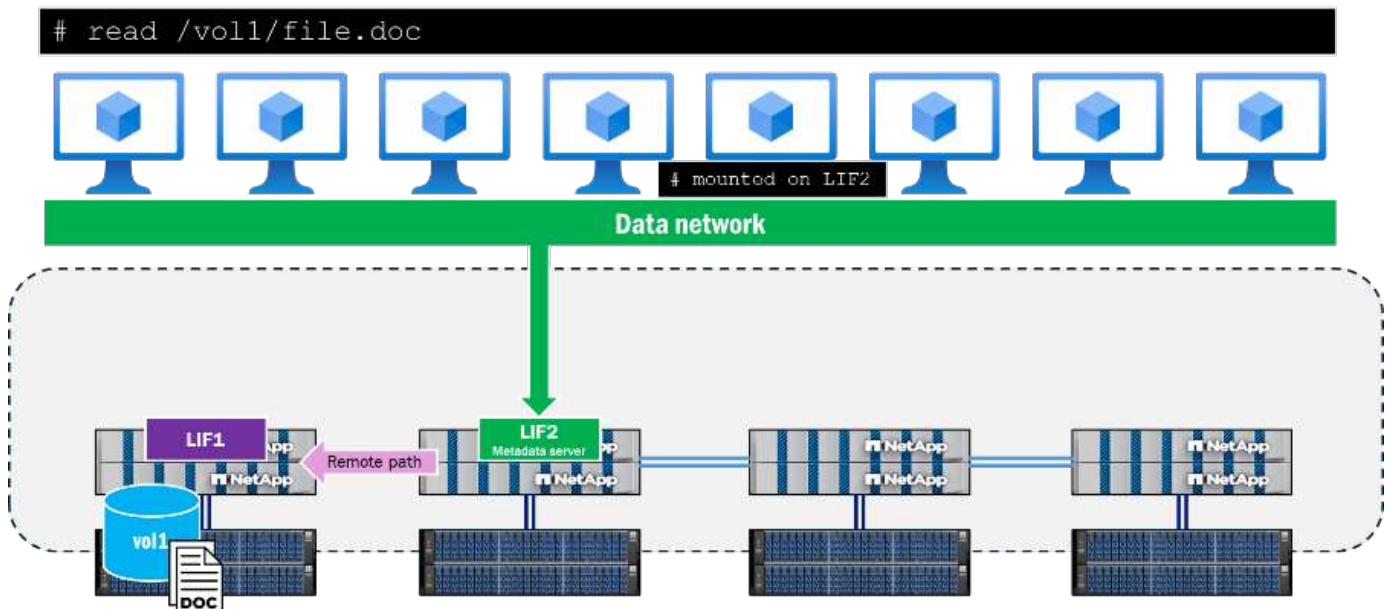


Abbildung 3. Remote-Lese pfad über NFSv4.1 ohne pNFS

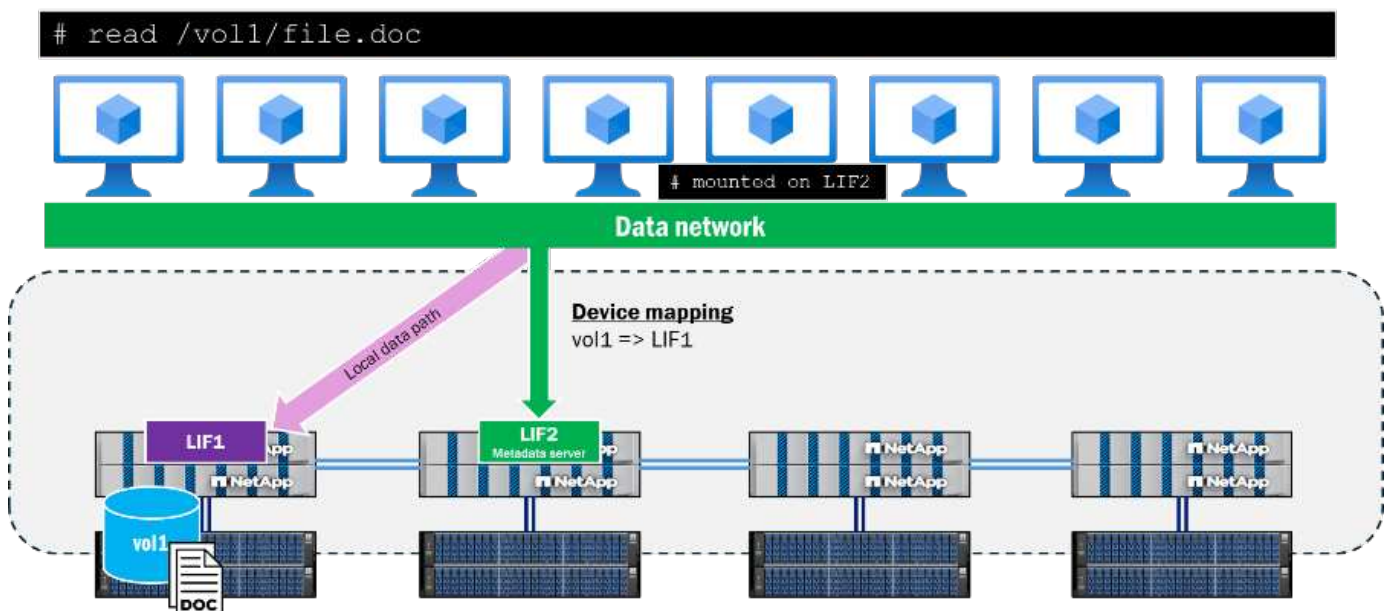


Abbildung 4. Lokalisierter Lese pfad mit pNFS

pNFS-Steuerpfad

Zusätzlich zu den Metadaten- und Datenanteilen von pNFS gibt es auch einen pNFS-Kontrollpfad. Der Kontrollpfad wird vom NFS-Server verwendet, um Dateisysteminformationen zu synchronisieren. In einem ONTAP Cluster wird das Backend-Cluster-Netzwerk regelmäßig repliziert, um sicherzustellen, dass alle pNFS-Geräte und Gerätezuordnungen synchronisiert sind.

pNFS-Gerätebesiedlungs-Workflow

Im Folgenden wird beschrieben, wie ein pNFS-Gerät in ONTAP angezeigt wird, nachdem ein Client eine Anfrage zum Lesen oder Schreiben einer Datei in einem Volume gestellt hat.

1. Der Client fordert einen Lese- oder Schreibvorgang an; es wird ein OPEN-Befehl ausgeführt und der Dateihandle abgerufen.

2. Sobald der OPEN-Vorgang ausgeführt wurde, sendet der Client den Dateihandle über die Metadatenserververbindung in einem LAYOUTGET-Aufruf an den Speicher.
3. LAYOUTGET gibt Informationen über das Layout der Datei zurück, wie z. B. die Status-ID, die Streifengröße, das Dateisegment und die Geräte-ID, an den Client.
4. Der Client nimmt dann die Geräte-ID und sendet einen GETDEVINFO-Aufruf an den Server, um die zugehörige IP-Adresse des Geräts abzurufen.
5. Der Speicher sendet eine Antwort mit der Liste der zugehörigen IP-Adressen für den lokalen Zugriff auf das Gerät.
6. Der Client setzt die NFS-Kommunikation über die lokale IP-Adresse fort, die vom Speicher zurückgesendet wird.

Interaktion von pNFS mit FlexGroup -Volumina

FlexGroup Volumes in ONTAP stellen Speicher als FlexVol volume -Bestandteile dar, die sich über mehrere Knoten in einem Cluster erstrecken. Dies ermöglicht es einer Arbeitslast, mehrere Hardware-Ressourcen zu nutzen und gleichzeitig einen einzigen Mountpoint beizubehalten. Da mehrere Knoten mit mehreren Netzwerkschnittstellen mit der Arbeitslast interagieren, ist es ein natürliches Ergebnis, dass der Remote-Datenverkehr das Backend-Cluster-Netzwerk in ONTAP durchläuft.

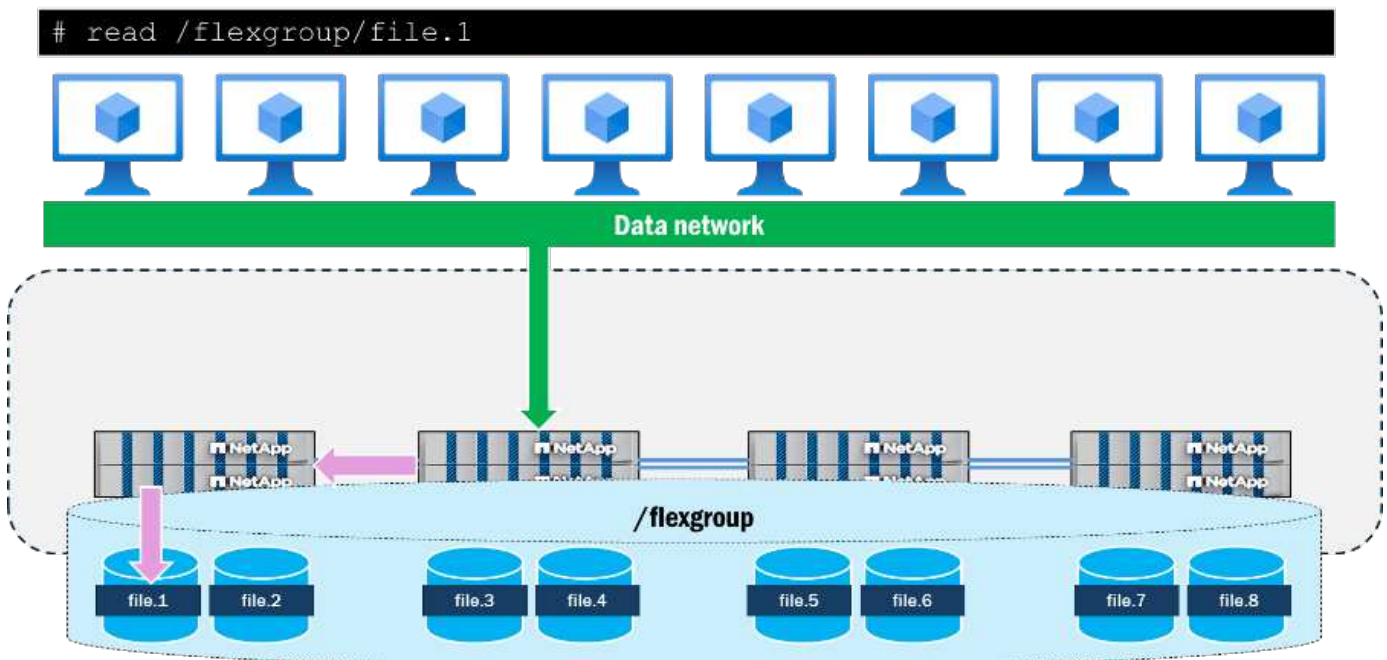


Abbildung 5. Einzeldateizugriff in einem FlexGroup -Volume ohne pNFS

Bei Verwendung von pNFS verfolgt ONTAP die Datei- und Volumenlayouts des FlexGroup -Volumes und ordnet sie den lokalen Datenschnittstellen im Cluster zu. Befindet sich beispielsweise ein Teilvolume, das eine Datei enthält, auf die zugegriffen wird, auf Knoten 1, so benachrichtigt ONTAP den Client, den Datenverkehr auf die Datenschnittstelle auf Knoten 1 umzuleiten.

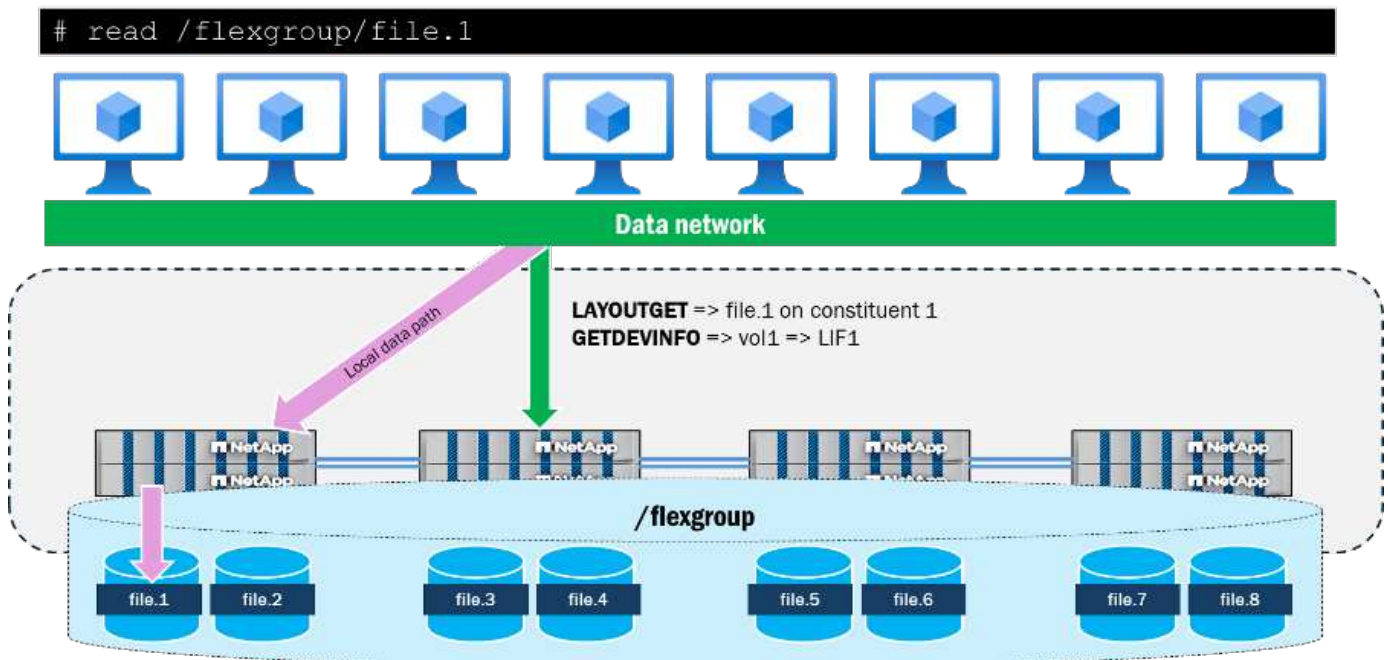


Abbildung 6. Einzeldateizugriff in einem FlexGroup -Volume mit pNFS

pNFS ermöglicht auch die Darstellung paralleler Netzwerkpfade zu Dateien von einem einzelnen Client aus, was NFSv4.1 ohne pNFS nicht ermöglicht. Wenn ein Client beispielsweise gleichzeitig auf vier Dateien vom selben Mountpunkt über NFSv4.1 ohne pNFS zugreifen möchte, wird für alle Dateien derselbe Netzwerkpfad verwendet, und der ONTAP Cluster sendet stattdessen Remote-Anfragen an diese Dateien. Der Mount-Pfad kann zu einem Flaschenhals für die Operationen werden, da alle Operationen einem einzigen Pfad folgen und an einem einzigen Knoten ankommen, der neben den Datenoperationen auch Metadatenoperationen bedient.

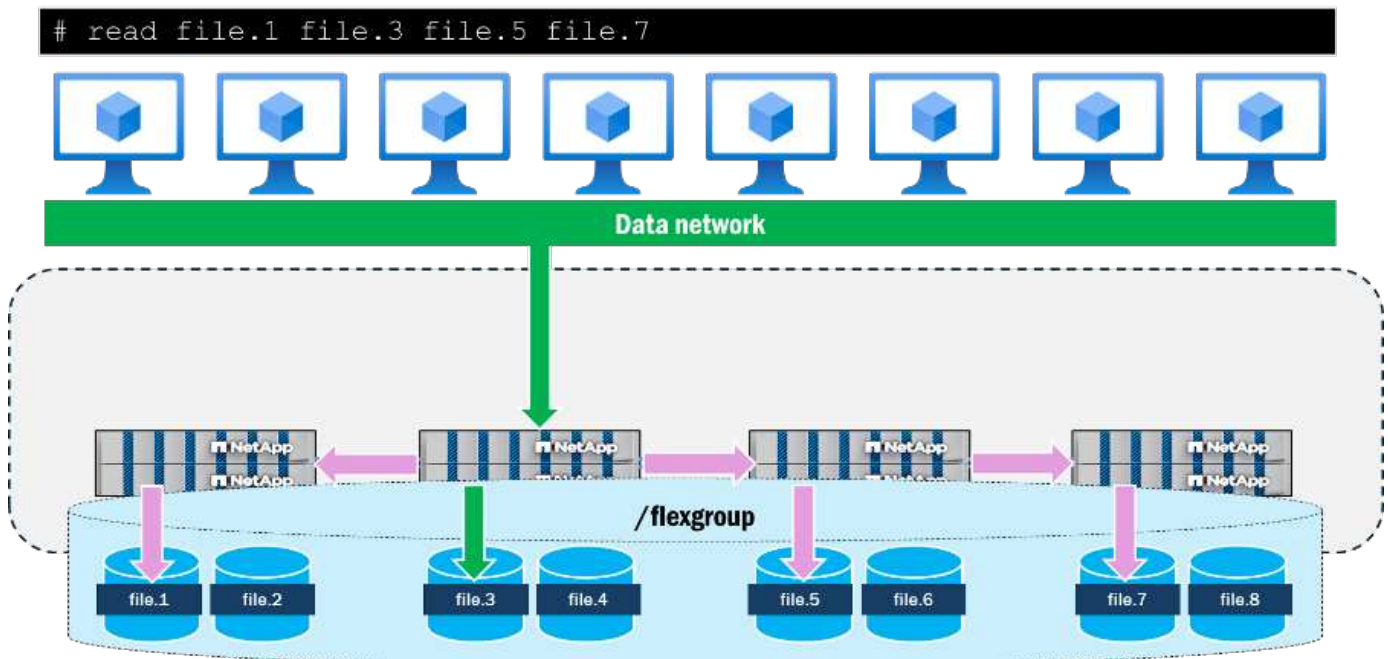


Abbildung 7. Mehrere gleichzeitige Dateizugriffe in einem FlexGroup -Volume ohne pNFS

Wenn pNFS verwendet wird, um von einem einzigen Client gleichzeitig auf dieselben vier Dateien zuzugreifen, verhandeln Client und Server lokale Pfade zu jedem Knoten mit den Dateien und verwenden mehrere TCP-Verbindungen für die Datenoperationen, während der Mount-Pfad als Speicherort für alle Metadatenoperationen dient. Dies bietet Vorteile hinsichtlich der Latenz durch die Verwendung lokaler Pfade zu den Dateien, kann aber auch Vorteile hinsichtlich des Durchsatzes durch die Verwendung mehrerer

Netzwerkschnittstellen bieten, vorausgesetzt, die Clients können genügend Daten senden, um das Netzwerk auszulasten.

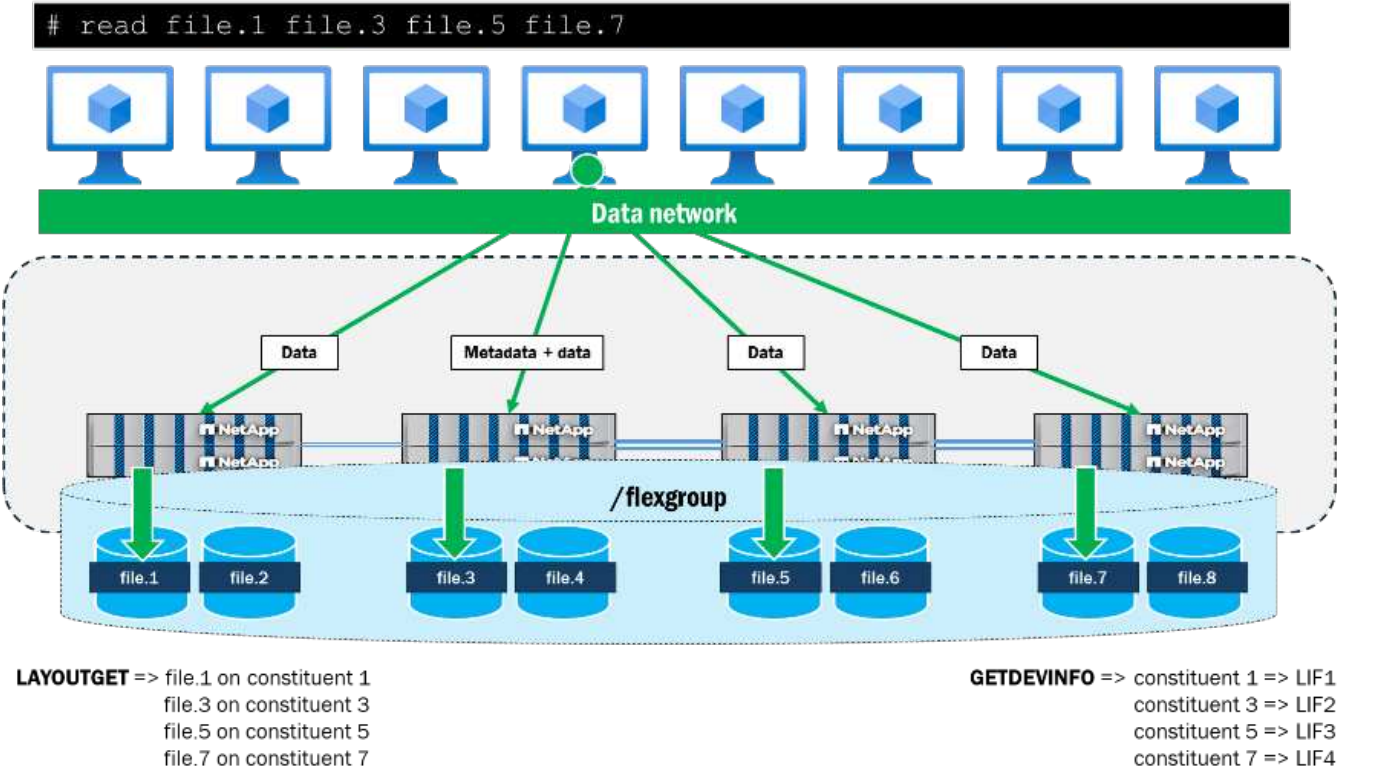


Abbildung 8. Mehrere gleichzeitige Dateizugriffe in einem FlexGroup -Volume mit pNFS

Nachfolgend werden die Ergebnisse eines einfachen Testlaufs auf einem einzelnen RHEL 9.5-Client dargestellt, bei dem vier 10 GB große Dateien (die sich alle auf verschiedenen Teilvolumes auf zwei ONTAP Clusterknoten befinden) parallel mit dd gelesen werden. Bei Verwendung von pNFS wurde für jede Datei der Gesamtdurchsatz und die Bearbeitungszeit verbessert. Bei Verwendung von NFSv4.1 ohne pNFS war der Leistungsunterschied zwischen Dateien, die sich lokal am Mountpunkt befanden, und entfernten Dateien größer als mit pNFS.

Prüfen	Durchsatz pro Datei (MB/s)	Bearbeitungszeit pro Datei
NFSv4.1: kein pNFS	<ul style="list-style-type: none">• Datei 1–228 (lokal)• Datei 2–227 (lokal)• Datei 3–192 (remote)• Datei 4–192 (remote)	<ul style="list-style-type: none">• Datei 1–46 (lokal)• Datei 2–46.1 (lokal)• Datei 3–54.5 (remote)• Datei 4–54.5 (remote)
NFSv4.1: mit pNFS	<ul style="list-style-type: none">• Datei 1–248 (lokal)• Datei 2–246 (lokal)• Datei.3–244 (lokal über pNFS)• Datei.4–244 (lokal über pNFS)	<ul style="list-style-type: none">• Datei 1–42.3 (lokal)• Datei 2–42.6 (lokal)• Datei 3–43 (lokal über pNFS)• Datei 4–43 (lokal über pNFS)

Verwandte Informationen

- "Management von FlexGroup Volumes"
- "NetApp Technischer Bericht 4571: FlexGroup Best Practices"

pNFS-Anwendungsfälle in ONTAP

pNFS kann mit verschiedenen ONTAP -Funktionen verwendet werden, um die Leistung zu verbessern und zusätzliche Flexibilität für NFS-Workloads zu bieten.

pNFS mit nconnect

Mit einigen neueren Clients und Servern wurde von NFS eine neue Mount-Option eingeführt, die es ermöglicht, mehrere TCP-Verbindungen unter Verwendung einer einzigen IP-Adresse bereitzustellen. Dies ermöglicht eine bessere Parallelisierung von Operationen, um Einschränkungen von NFS-Servern und -Clients zu umgehen und potenziell die Gesamtleistung bestimmter Workloads zu steigern. nconnect wird in ONTAP 9.8 und höher unterstützt, sofern der Client nconnect unterstützt.

Bei Verwendung von nconnect mit pNFS werden die Verbindungen mithilfe der nconnect-Option über jedes vom NFS-Server angekündigte pNFS-Gerät parallelisiert. Wenn beispielsweise nconnect auf vier eingestellt ist und vier geeignete Schnittstellen für pNFS vorhanden sind, beträgt die Gesamtzahl der erstellten Verbindungen bis zu 16 pro Mountpunkt (4 nconnect x 4 IP-Adressen).

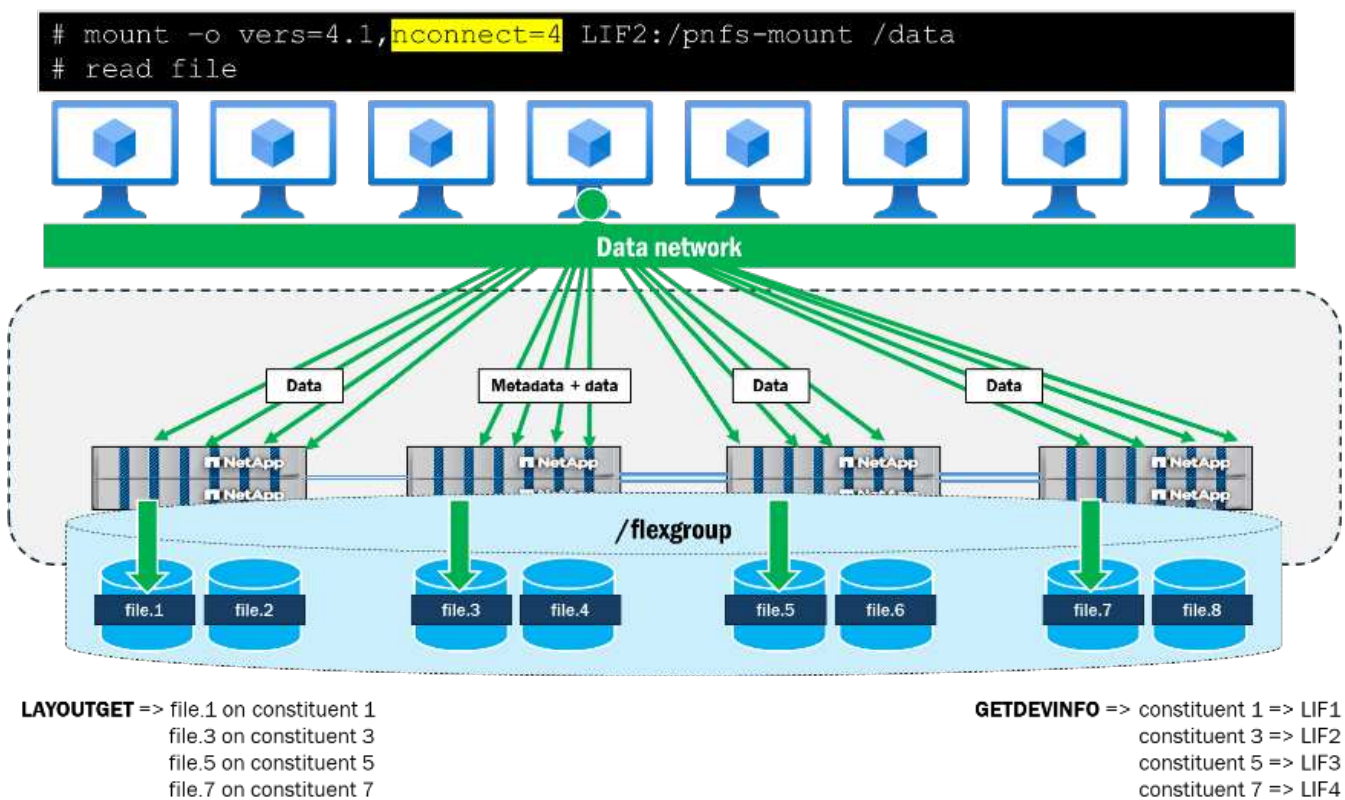


Abbildung 9. pNFS mit nconnect auf 4 eingestellt

"Erfahren Sie mehr über die ONTAP Unterstützung für NFSv4.1"

pNFS mit NFSv4.1 Session Trunking

NFSv4.1 Session-Trunking ("RFC 5661, Abschnitt 2.10.5") ist die Verwendung mehrerer TCP-Verbindungen zwischen einem Client und einem Server, um die Geschwindigkeit der Datenübertragung zu erhöhen. Die Unterstützung für NFSv4.1 Session Trunking wurde in ONTAP 9.14.1 hinzugefügt und muss mit Clients

verwendet werden, die ebenfalls Session Trunking unterstützen.

In ONTAP kann Session Trunking über mehrere Knoten in einem Cluster genutzt werden, um zusätzlichen Durchsatz und Redundanz über die Verbindungen hinweg zu gewährleisten.

Session-Trunking kann auf verschiedene Arten eingerichtet werden:

- **Automatische Erkennung über Mount-Optionen:** Session Trunking kann bei den meisten modernen NFS-Clients über Mount-Optionen eingerichtet werden (siehe Dokumentation Ihres Betriebssystemherstellers), die dem NFS-Server signalisieren, Informationen über Session Trunks an den Client zurückzusenden. Diese Informationen erscheinen über ein NFS-Paket als `fs_location4` Anruf.

Die verwendete Mount-Option hängt von der Betriebssystemversion des Clients ab. Beispielsweise verwenden Ubuntu Linux-Varianten im Allgemeinen `max_connect=n` um zu signalisieren, dass ein Sitzungs-Trunk verwendet werden soll. In RHEL-Linux-Distributionen, `trunkdiscovery` Die Montageoption wird verwendet.

Ubuntu-Beispiel

```
mount -o vers=4.1,max_connect=8 10.10.10.10:/pNFS /mnt/pNFS
```

RHEL-Beispiel

```
mount -o vers=4.1,trunkdiscovery 10.10.10.10:/pNFS /mnt/pNFS
```



Wenn Sie versuchen zu verwenden `max_connect` Bei RHEL-Distributionen wird es stattdessen als `nconnect` behandelt, und Session Trunking funktioniert nicht wie erwartet.

- **Manuelle Einrichtung:** Sie können Session-Trunking manuell einrichten, indem Sie jede einzelne IP-Adresse dem gleichen Exportpfad und Mountpunkt zuordnen. Wenn Sie beispielsweise zwei IP-Adressen auf demselben Knoten haben (10.10.10.10 und 10.10.10.11) für einen Exportpfad von `/pNFS` Sie führen den Mount-Befehl zweimal aus:

```
mount -o vers=4.1 10.10.10.10:/pNFS /mnt/pNFS
mount -o vers=4.1 10.10.10.11:/pNFS /mnt/pNFS
```

Wiederholen Sie diesen Vorgang für alle Schnittstellen, die am Trunk teilnehmen sollen.



Jeder Knoten erhält seinen eigenen Sitzungsstrang. Trunks durchlaufen keine Knoten.



Bei Verwendung von pNFS sollten Sie ausschließlich Session Trunking *oder* `nconnect` verwenden. Die Verwendung beider Methoden führt zu unerwünschtem Verhalten, beispielsweise dass nur die Metadatenserververbindung die Vorteile von `nconnect` nutzt, während die Datenserver eine einzige Verbindung verwenden.


```
# mount -o vers=4.1, trunkdiscovery PNFS:/pnfs-mount /data
```

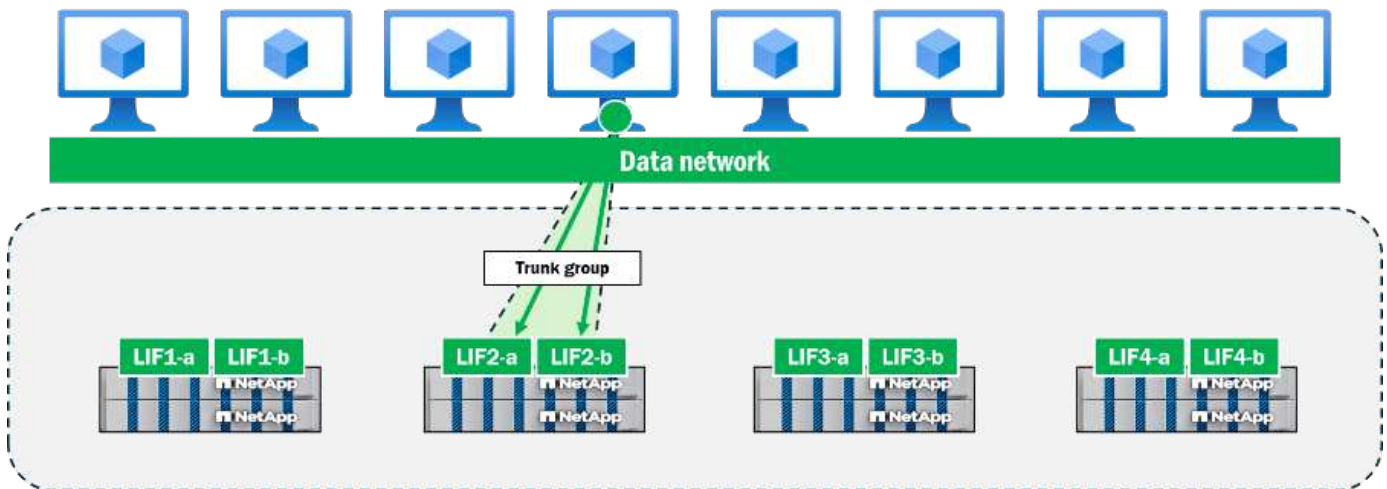
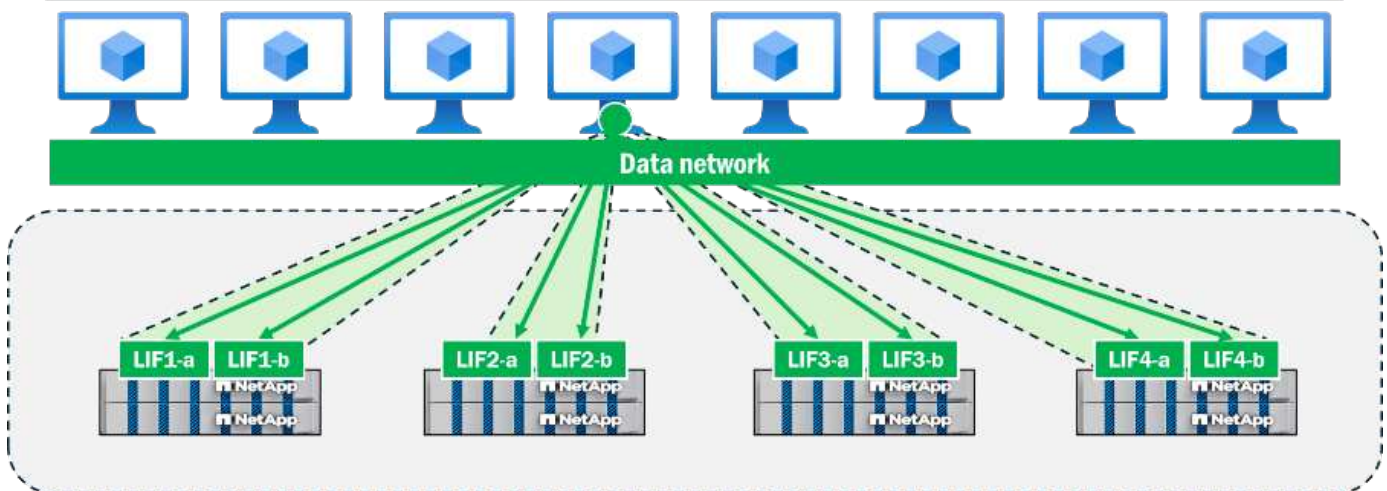


Abbildung 10. NFSv4.1 Session Trunking in ONTAP

pNFS kann einen lokalen Pfad zu jedem teilnehmenden Knoten in einem Cluster bereitstellen, und in Verbindung mit Session Trunking kann pNFS einen Session Trunk pro Knoten nutzen, um den Durchsatz für den gesamten Cluster zu maximieren.

```
# mount -o vers=4.1, trunkdiscovery PNFS:/pnfs-mount /data
```



Wann **trunkdiscovery** wird verwendet, wird ein zusätzlicher GETATTR-Aufruf (FS_Locations) für die aufgelisteten Session-Trunk-Schnittstellen auf dem NFS-Serverknoten genutzt, auf dem sich die Mount-Schnittstelle befindet. Sobald diese zurückgesendet sind, werden weitere Mounts an die zurückgesendeten Adressen vorgenommen. Dies lässt sich bei einer Paketerfassung während der Einbindung beobachten.

198	1.219372			NFS	246	V4	Call (Reply In 199)	GETATTR	FH: 0x787f5cf1
199	1.219579			NFS	238	V4	Reply (Call In 198)	GETATTR	


```

  ✓ Opcode: SEQUENCE (53)
    Status: NFS4_OK (0)
    sessionid: 7100001e004090a90000000000000409
    seqid: 0x00000009
    slot id: 0
    high slot id: 63
    target high slot id: 63
  > status flags: 0x00000000
  ✓ Opcode: PUTFH (22)
    Status: NFS4_OK (0)
  ✓ Opcode: GETATTR (9)
    Status: NFS4_OK (0)
  ✓ Attr mask: 0x01000100 (FSID, FS_Locations)
    ✓ reqd_attr: FSID (8)
      > fattr4_fsid
    ✓ reco_attr: FS_Locations (24)
      ✓ fattr4_fs_locations
        pathname components: 0
      ✓ fs_location4
        num: 1
      ✓ fs_location4
        ✓ servers
          num: 1
          ✓ server: 
            length: 14
            contents: 
            fill bytes: opaque data
        pathname components: 0

```

Abbildung 11. NFS-Sitzungstrunk-Erkennung während der Einbindung: Paketerfassung

["Erfahren Sie mehr über NFS-Trunking."](#)

pNFS- versus NFSv4.1-Überweisungen

NFSv4.1-Verweise bieten eine Methode zur anfänglichen Umleitung des Mount-Pfads, die einen Client bei einer Mount-Anforderung zum Speicherort der Volumes leitet. NFSv4.1-Verweise funktionieren innerhalb einer einzelnen SVM. Diese Funktion versucht, die NFS-Einbindung auf einer Netzwerkschnittstelle zu lokalisieren, die sich auf demselben Knoten wie das Datenvolume befindet. Wird diese Schnittstelle oder dieses Volume auf einen anderen Knoten verschoben, während es an einen Client angebunden ist, dann ist der Datenpfad nicht mehr lokalisiert, bis eine neue Anbindung hergestellt wird.

pNFS versucht nicht, einen Mount-Pfad zu lokalisieren. Stattdessen wird ein Metadatenserver mithilfe eines Mount-Pfads eingerichtet und der Datenpfad dann bei Bedarf dynamisch lokalisiert.

NFSv4.1-Verweise können mit pNFS verwendet werden, diese Funktionalität ist jedoch nicht erforderlich. Die Aktivierung von Überweisungen mit pNFS wird keine merklichen Ergebnisse zeigen.

["NFSv4-Verweise aktivieren oder deaktivieren"](#)

Interaktion von pNFS mit fortschrittlichem Kapazitätsausgleich

["Erweiterter Kapazitätsausgleich"](#) ONTAP schreibt Teile von Dateidaten über die einzelnen Volumes eines FlexGroup -Volumes (wird bei einzelnen FlexVol -Volumes nicht unterstützt). Wenn eine Datei größer wird, entscheidet ONTAP, die Daten in einen neuen Multipart-Inode auf einem anderen Teilvolume zu schreiben, das sich auf demselben Knoten oder auf einem anderen Knoten befinden kann. Schreib-, Lese- und Metadatenoperationen an diesen Multi-Inode-Dateien sind transparent und beeinträchtigen die Clients nicht.

Durch eine fortschrittliche Kapazitätsverteilung wird das Raummanagement innerhalb der FlexGroup-Komponenten optimiert, was zu einer gleichmäßigeren Leistung führt.

pNFS kann die Daten-E/A auf einen lokalen Netzwerkpfad umleiten, abhängig von den im NFS-Server gespeicherten Dateilayoutinformationen. Wenn eine einzelne große Datei in Teilen über mehrere Teilvolumes erstellt wird, die sich potenziell über mehrere Knoten im Cluster erstrecken können, kann pNFS in ONTAP dennoch lokalisierten Datenverkehr zu jedem Dateiteil bereitstellen, da ONTAP auch die Dateilayoutinformationen für alle Dateiteile verwaltet. Beim Lesen einer Datei wird die Datenpfadlokalität nach Bedarf geändert.

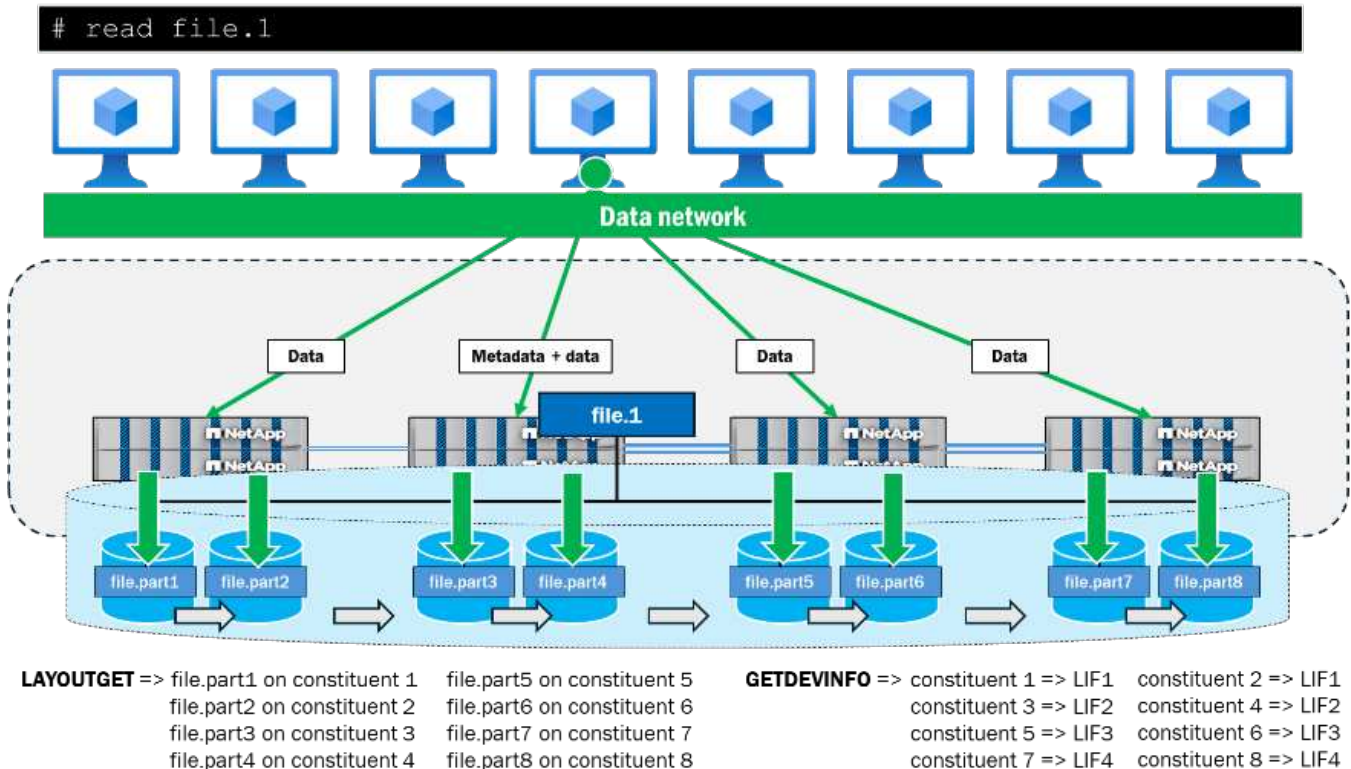


Abbildung 12. Erweiterter Kapazitätsausgleich mit pNFS

Verwandte Informationen

- ["FlexGroup Volume-Konfiguration"](#)

pNFS-Bereitstellungsstrategie in ONTAP

pNFS wurde eingeführt, um das traditionelle NFS zu verbessern, indem Metadaten- und Datenpfade getrennt, Datenlokalisierung ermöglicht und parallele Operationen erlaubt werden.

Herausforderungen der traditionellen NFS und Vorteile der pNFS

Die folgende Tabelle zeigt die Herausforderungen des traditionellen NFS und erklärt, wie pNFS in ONTAP diese angeht.

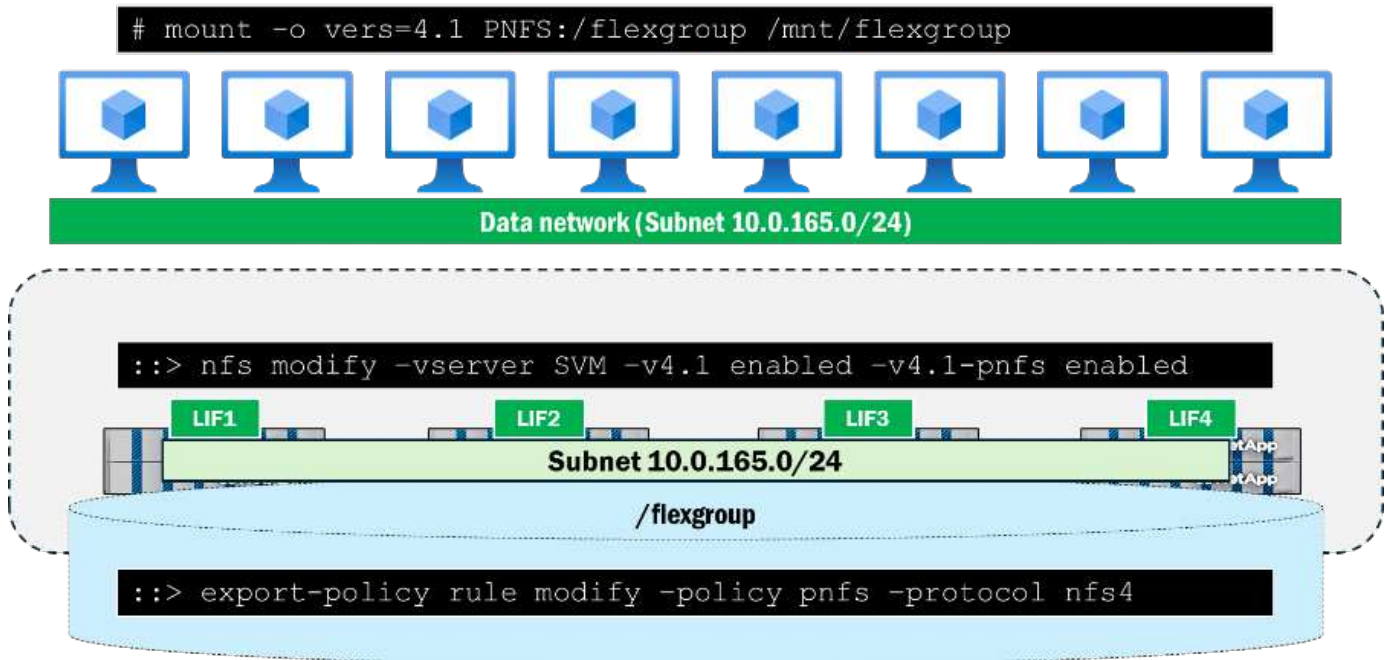
Herausforderung	pNFS-Nutzen
Derselbe Pfad für Metadaten und Daten Bei herkömmlichem NFS durchlaufen Metadaten und Daten denselben Pfad, was sowohl das Netzwerk als auch die CPU auslasten kann, da ein einzelner Pfad an einen einzelnen Hardwareknoten im Cluster angebunden wird. Dies wird noch verschärft, wenn viele Benutzer versuchen, auf denselben NFS-Export zuzugreifen.	Metadaten- und Datenpfade sind getrennt, Datenpfade werden parallelisiert Durch die Trennung der Metadaten- und Datenpfade für den NFS-Verkehr und die Bereitstellung mehrerer Netzwerkpfade für Datenpfade werden die CPU- und Netzwerkressourcen in einem ONTAP Cluster maximiert, wodurch eine verbesserte Skalierbarkeit für Workloads erreicht wird.
Herausforderungen bei der Workload-Verteilung In einem ONTAP NAS-Cluster können Sie bis zu 24 Knoten haben, von denen jeder über eigene Datenvolumes und Netzwerkschnittstellen verfügen kann. Jedes Volume kann seine eigene Arbeitslast oder eine Teilmenge einer Arbeitslast hosten, und mit einem FlexGroup -Volume kann diese Arbeitslast über mehrere Knoten verteilt sein, die zur Vereinfachung auf einen einzigen Namespace zugreifen. Wenn ein Client einen NFS-Export einbindet, wird der Netzwerkverkehr auf einem einzigen Knoten aufgebaut. Wenn sich die abgerufenen Daten auf einem separaten Knoten im Cluster befinden, entsteht Remote-Datenverkehr, was zu Latenzzeiten bei der Arbeitslast und zu Komplexität bei der Administration führen kann.	Lokale, parallele Pfade zu Datenstrukturen Da pNFS die Datenpfade von den Metadaten trennt und mehrere parallele Datenpfade je nach Lokalität des Volumes im Cluster bereitstellt, kann die Latenz durch Verringerung der Distanz des Netzwerkverkehrs im Cluster sowie durch die Nutzung mehrerer Hardware-Ressourcen in einem Cluster reduziert werden. Da pNFS in ONTAP den Datenverkehr automatisch umleitet, müssen Administratoren weniger mehrere Exportpfade und -orte verwalten.
Verschiebung von NFS-Mountpunkten Sobald ein Mountpunkt eingerichtet ist, würde das Aushängen und erneute Einhängen des Volumes zu Störungen führen. ONTAP bietet die Möglichkeit, Netzwerkschnittstellen zwischen Knoten zu migrieren, dies führt jedoch zu einem erhöhten Verwaltungsaufwand und ist für zustandsbehaftete NFS-Verbindungen mit NFSv4.x störend. Einige Gründe für die Verlegung eines Mount-Punktes hängen mit den Herausforderungen der Datenlokalität zusammen.	Automatische Pfadumleitung Mit pNFS verwaltet der NFS-Server eine Tabelle mit den Speicherorten der Netzwerkschnittstellen und Volumes. Wenn eine Datenstruktur von einem Client über den Metadatenpfad in pNFS angefordert wird, liefert der Server einen optimierten Netzwerkpfad an den Client, der diesen Pfad dann für Datenoperationen verwendet. Dies reduziert den Verwaltungsaufwand für Arbeitslasten drastisch und kann in einigen Fällen die Leistung verbessern.

Konfigurationsanforderungen

Die Konfiguration von pNFS in NetApp ONTAP erfordert Folgendes:

- Ein NFS-Client, der pNFS unterstützt und mit NFSv4.1 oder höher eingebunden ist.
- NFSv4.1 auf dem NFS-Server in ONTAP aktiviert (`nfs modify -v4.1 enabled` (Standardmäßig deaktiviert))

- pNFS ist auf dem NFS-Server in ONTAP aktiviert. (`nfs modify -v4.1-pnfs enabled` (Standardmäßig deaktiviert))
- Mindestens eine Netzwerkschnittstelle pro Knoten, die zu den NFS-Clients routen kann.
- Datenvolumes in der SVM, die Exportrichtlinien und -regeln haben, die NFSv4 zulassen



Sobald die oben genannten Konfigurationsvoraussetzungen erfüllt sind, funktioniert pNFS von selbst.

Verwandte Informationen

- ["NFS-Konfiguration"](#)
- ["ONTAP -Unterstützung für NFSv4.1"](#)
- ["Netzwerkschnittstellenkonnektivität für pNFS"](#)

Planen

Plan für die pNFS-Implementierung

Bevor Sie pNFS in Ihrer Umgebung einsetzen, stellen Sie sicher, dass Sie die Voraussetzungen erfüllen und die Interoperabilitätsanforderungen sowie die Konfigurationsgrenzen verstehen.

Voraussetzungen

Bevor Sie pNFS in ONTAP aktivieren und verwenden, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- NFSv4.1 oder höher ist auf dem NFS-Server aktiviert.
- Mindestens einer ["Daten-LIF existieren pro Knoten"](#) im Cluster für die SVM, die den NFS-Server hostet
- Alle ["Daten-LIFs im SVM sind routenfähig"](#) zu NFS-Clients
- NFS-Clients unterstützen pNFS (die meisten modernen Linux-Distributionen ab 2014).

- Die Netzwerkverbindung zwischen Clients und allen Daten-LIFs im SVM ist funktionsfähig.
- Die DNS-Auflösung (bei Verwendung von Hostnamen) ist für alle Daten-LIFs ordnungsgemäß konfiguriert.
- ["FlexGroup Volumes"](#) sind konfiguriert (empfohlen für beste Ergebnisse)
- ["NFSv4.x ID-Domänen stimmen überein"](#) zwischen Kunden und ONTAP
- ["NFS Kerberos"](#) (falls verwendet) ist für alle Daten-LIFs im SVM aktiviert.

Zusammenfassung bewährter Verfahren

Bei der Implementierung von pNFS in Ihrer Umgebung sollten Sie folgende Best Practices beachten:

- Verwenden ["FlexGroup Volumes"](#) für optimale Leistung und Kapazitätsskalierung
- Stellen Sie sicher, dass alle ["Die Netzwerkschnittstellen in der SVM sind routingfähig"](#) für Kunden
- ["Deaktivieren Sie NFSv4.0"](#) um sicherzustellen, dass Clients NFSv4.1 oder höher verwenden
- Verteilen Sie die Mountpunkte über mehrere Netzwerkschnittstellen und Knoten.
- Verwenden Sie Round-Robin-DNS für ["Load-Balancing-Metadatenserver"](#)
- Verifizieren ["NFSv4.x ID-Domänen stimmen überein"](#) auf Clients und Servern
- Benehmen ["Migrationen von Netzwerkschnittstellen"](#) Und ["Speicherausfälle"](#) während der Wartungsfenster
- Aktivieren ["NFS Kerberos"](#) auf allen Daten-LIFs, wenn Kerberos-Sicherheit verwendet wird
- Vermeiden Sie die Verwendung ["NFSv4.1-Überweisungen"](#) bei Verwendung von pNFS
- Prüfen ["nconnect-Einstellungen"](#) sorgfältig darauf achten, die TCP-Verbindungslimits nicht zu überschreiten
- In Betracht ziehen ["Sitzungsbündelung"](#) als Alternative zu ["Nconnect"](#) (Verwenden Sie nicht beide gleichzeitig)
- Verifizieren ["Unterstützung durch den Client-Betriebssystemanbieter"](#) für pNFS vor der Bereitstellung

Interoperabilität

pNFS in ONTAP ist für die Zusammenarbeit mit RFC-konformen NFS-Clients ausgelegt. Folgende Überlegungen sind zu beachten:

- Die modernsten ["Linux-Distributionen ab 2014"](#) Unterstützung für pNFS (RHEL 6.4, Fedora 17 und höher)
- Vergewissern Sie sich bei Ihrem Betriebssystemanbieter, dass pNFS unterstützt wird.
- pNFS funktioniert sowohl mit FlexVol als auch mit ["FlexGroup Volumes"](#)
- pNFS wird mit NFSv4.1 unterstützt und ["NFSv4.2"](#)
- pNFS kann verwendet werden mit ["NFS Kerberos"](#) (krb5, krb5i, krb5p), die Leistung könnte jedoch beeinträchtigt sein
- pNFS kann zusammen mit ["Nconnect"](#) oder ["Sitzungsbündelung"](#) (aber nicht beides gleichzeitig)
- pNFS funktioniert nicht über ["NFSv4.0"](#)

Begrenzungen

Für pNFS in ONTAP gelten folgende Beschränkungen:

- ["TCP-Verbindungslimits"](#) Die Anzahl der Knoten variiert je nach Plattform (die genauen Grenzwerte finden Sie im NetApp Hardware Universe).

- Maximale Dateigröße: Abhängig vom Datenträgertyp und der ONTAP Version
- Maximale Dateianzahl: Bis zu 200 Milliarden Dateien mit ["FlexGroup Volumes"](#)
- Maximale Kapazität: Bis zu 60 PB mit ["FlexGroup Volumes"](#)
- ["Anzahl der Netzwerkschnittstellen"](#) Mindestens ein Daten-LIF pro Knoten ist erforderlich; für den Lastausgleich können weitere erforderlich sein.

Bei Verwendung ["nconnect mit pNFS"](#) Beachten Sie, dass sich die Anzahl der TCP-Verbindungen schnell vervielfacht:

- Jede Client-Einbindung mit nconnect erstellt mehrere TCP-Verbindungen pro Daten-LIF.
- Da viele Clients hohe nconnect-Werte verwenden, ["TCP-Verbindungslimits"](#) kann überschritten werden
- Wenn die TCP-Verbindungslimits überschritten werden, werden keine neuen Verbindungen hergestellt, bis bestehende Verbindungen freigegeben werden.

Verwandte Informationen

- ["Netzwerkschnittstellenkonnektivität für pNFS"](#)
- ["Aktivieren oder Deaktivieren von NFSv4.1"](#)
- ["ONTAP -Unterstützung für NFSv4.1"](#)
- ["ONTAP -Unterstützung für NFSv4.2"](#)
- ["NetApp Hardware Universe"](#)

pNFS-Optimierung und Leistungsoptimierung – Best Practices

Bei der Verwendung von pNFS in ONTAP sollten Sie diese Hinweise und bewährten Vorgehensweisen beachten, um optimale Ergebnisse zu erzielen.

Empfehlungen zum Volumentyp

pNFS in ONTAP funktioniert sowohl mit FlexVol -Volumes als auch mit FlexGroup -Volumes, aber für die besten Gesamtergebnisse sollten FlexGroup -Volumes verwendet werden.

FlexGroup Volumes bieten:

- Ein einzelner Mountpunkt, der sich über mehrere Hardware-Ressourcen in einem Cluster erstrecken kann und gleichzeitig pNFS die Lokalisierung des Datenverkehrs ermöglicht.
- Enorme Speicherkapazität (bis zu 60 PB) und hohe Dateianzahl (bis zu 200 Milliarden Dateien)
- Unterstützung für mehrteilige Dateien zur Kapazitätsverteilung und potenziellen Leistungsverbesserungen
- Paralleler Zugriff auf Volumes und Hardware zur Unterstützung einer einzelnen Arbeitslast

["Erfahren Sie mehr über das Volumenmanagement von FlexGroup."](#)

Kundenempfehlungen

Nicht alle NFS-Clients unterstützen pNFS, die meisten modernen Clients jedoch schon. RHEL 6.4 und Fedora 17 waren die ersten Clients mit pNFS-Unterstützung (etwa 2014), daher kann man davon ausgehen, dass Clientversionen der letzten Jahre diese Funktion vollständig unterstützen. ONTAP verfolgt in Bezug auf NFS den Ansatz: „Wenn der Client die Funktion unterstützt und RFC-konform ist und wir die Funktion unterstützen, dann wird die Kombination unterstützt.“ Es empfiehlt sich jedoch, sicherzustellen, dass pNFS vom Hersteller

des Client-Betriebssystems unterstützt wird.

Volumenbewegungen

ONTAP bietet die Möglichkeit, Datenvolumen unterbrechungsfrei zwischen Knoten oder Aggregaten im selben Cluster zu verschieben, um eine flexible Balance zwischen Kapazität und Leistung zu gewährleisten. Wenn in ONTAP eine Volume-Verschiebung stattfindet, werden die pNFS-Gerätezuordnungen automatisch aktualisiert, um Clients gegebenenfalls über die Verwendung der neuen Volume-zu-Schnittstelle-Beziehung zu informieren.

["Erfahren Sie mehr über das Verschieben eines Volumens"](#)

Migration der Netzwerkschnittstelle

ONTAP bietet die Möglichkeit, Netzwerkschnittstellen zwischen Knoten innerhalb desselben Clusters zu verschieben, um ein ausgewogenes Leistungsverhältnis und Flexibilität bei der Wartung zu gewährleisten. Ähnlich wie bei Volume-Verschiebungen werden bei einer Migration der Netzwerkschnittstelle in ONTAP die pNFS-Gerätezuordnungen automatisch aktualisiert, um Clients gegebenenfalls über die Verwendung der neuen Volume-zu-Schnittstelle-Beziehung zu informieren.

Da NFSv4.1 jedoch ein zustandsbehaftetes Protokoll ist, kann eine Migration der Netzwerkschnittstelle zu Störungen bei Clients führen, die die NFS-Freigabe aktiv nutzen. Es empfiehlt sich, Netzwerkschnittstellenmigrationen in einem Wartungsfenster durchzuführen und die Kunden über mögliche Netzwerkstörungen zu informieren.

Speicherausfälle/Speicherrückgaben

pNFS berücksichtigt bei der Speicherausfallsicherung dieselben Aspekte wie NFSv4.1. Diese werden ausführlich behandelt in ["NetApp Technical Report 4067: NFS Best Practice and Implementation Guide"](#) Generell sollten alle Speicherausfälle/Speicherrückgaben im Zusammenhang mit pNFS in einem Wartungsfenster durchgeführt werden, wobei aufgrund der Zustandsabhängigkeit des Protokolls mit potenziellen Speicherunterbrechungen zu rechnen ist.

Metadaten-Workloads

Metadatenoperationen sind klein, können aber je nach Arbeitslast in großer Zahl auftreten (Erstellen Sie eine große Anzahl von Dateien?). Führen Sie "find"-Befehle aus?) und die Gesamtzahl der Dateien. Daher können Arbeitslasten mit vielen Metadatenabfragen die CPU des NFS-Servers stark belasten und potenziell zu einem Flaschenhals über eine einzelne Verbindung führen. pNFS (und NFSv4.x im Allgemeinen) ist für leistungskritische Arbeitslasten mit hohem Metadatenaufkommen nicht geeignet, da die Zustandsverwaltung, die Sperrmechanismen und einige Sicherheitsfunktionen dieser Protokollversion die CPU-Auslastung und Latenz negativ beeinflussen können. Diese Workload-Typen (wie z. B. hohe GETATTR- oder SETATTR-Werte) kommen im Allgemeinen mit NFSv3 besser zurecht.

Metadatenserver

Der Metadatenserver in pNFS wird beim ersten Mounten eines NFS-Exports eingerichtet. Sobald der Mountpunkt eingerichtet ist, bleibt er so lange an seinem Platz, bis er neu eingebunden oder die Datenschnittstelle verschoben wird. Aus diesem Grund ist es eine bewährte Vorgehensweise, sicherzustellen, dass mehrere Clients, die auf dasselbe Volume zugreifen, auf unterschiedlichen Knoten und Datenschnittstellen innerhalb des SVM eingebunden werden. Dieser Ansatz ermöglicht eine gleichmäßige Verteilung der Metadatenserver auf die Knoten und CPU-Ressourcen und maximiert gleichzeitig die Anzahl der Netzwerkschnittstellen im Cluster. Eine Möglichkeit, dies zu erreichen, besteht in der Einrichtung eines Round-Robin-DNS-Systems, das im Folgenden beschrieben wird. ["NetApp Technischer Bericht 4523: DNS-Lastverteilung in ONTAP"](#) Die

NFSv4.x ID-Domänen

NFSv4.x bietet Sicherheitsfunktionen auf vielfältige Weise (ausführlich beschrieben in ["NetApp Technical Report 4067: NFS Best Practice and Implementation Guide"](#)). NFSv4.x ID-Domänen sind eine dieser Methoden, bei der Client und Server sich auf die ID-Domänen einigen müssen, wenn sie versuchen, Benutzer und Gruppen in einem NFS-Export zu authentifizieren. Eine mögliche Folge einer Diskrepanz zwischen Benutzer-ID und Domäne wäre, dass der Benutzer oder die Gruppe als anonymisierter Benutzer (im Wesentlichen unterdrückt) angezeigt wird, um unerwünschten Zugriff zu verhindern. Bei NFSv4.x (und auch pNFS) ist es ratsam, sicherzustellen, dass die NFSv4.x-ID-Domänen auf Client und Server übereinstimmen.

Nconnect

Wie bereits erwähnt, kann nconnect in ONTAP bei einigen Arbeitslasten zur Leistungsverbesserung beitragen. Bei pNFS ist es wichtig zu verstehen, dass nconnect zwar die Leistung verbessern kann, indem es die Gesamtzahl der TCP-Verbindungen zum Speichersystem erheblich erhöht, aber auch Probleme verursachen kann, wenn viele Clients die Mount-Option nutzen, indem sie die TCP-Verbindungen zum Speicher überlasten. Das NetApp Hardware Universe umfasst die TCP-Verbindungslimits pro Knoten.

Wenn die TCP-Verbindungsgrenzen eines Knotens überschritten werden, werden keine neuen TCP-Verbindungen zugelassen, bis bestehende Verbindungen freigegeben werden. Dies kann in Gebieten, in denen es zu heftigen Stürmen kommen kann, zu Komplikationen führen.

Die folgende Tabelle zeigt, wie pNFS mit nconnect die TCP-Verbindungsgrenzen überschreiten könnte:

Kundenzahl	nconnect-Wert	Gesamtzahl potenzieller TCP-Verbindungen pro Mountpunkt, pro Knoten
1	4	4
100	4	400
1000	8	8000
10000	8	80000
10000	16	160000 ¹

¹ Überschreitet die meisten TCP-Verbindungsgrenzen von ONTAP für einzelne Knoten.

NFSv4.1 Session-Trunking

Session Trunking in ONTAP kann verwendet werden, um den Durchsatz und die Pfadausfallsicherheit für NFSv4.x-Mounts zu erhöhen. Bei Verwendung mit pNFS kann jeder Knoten in einem Cluster einen Session-Trunk aufbauen. Allerdings benötigen Session Trunks mindestens zwei Schnittstellen pro Knoten, und pNFS benötigt mindestens eine Schnittstelle pro Knoten, um wie vorgesehen zu funktionieren. Darüber hinaus müssen alle Schnittstellen in der SVM für die NFS-Clients erreichbar sein. Session Trunking und pNFS funktionieren nicht ordnungsgemäß, wenn gleichzeitig nconnect genutzt wird. Betrachten Sie nconnect und Session Trunking als sich gegenseitig ausschließende Funktionen.

["Erfahren Sie mehr über NFS-Trunking."](#)

Netzwerkschnittstellenkonnektivität

Für die ordnungsgemäße Funktion von pNFS ist eine routingfähige Netzwerkschnittstelle auf jedem Knoten eines Clusters erforderlich. Falls in derselben SVM wie der NFS-Server, auf dem pNFS gehostet wird, andere Netzwerkschnittstellen vorhanden sind, die für NFS-Clients nicht routingfähig sind, kündigt ONTAP diese

Schnittstellen dennoch in der Gerätezuordnung für Clients an. Wenn der NFS-Client versucht, über die Schnittstellen in einem anderen Subnetz auf Daten zuzugreifen, kann keine Verbindung hergestellt werden, und es kommt zu einem Ausfall. Es empfiehlt sich, bei der Verwendung von pNFS nur Netzwerkschnittstellen in einer SVM zuzulassen, auf die Clients zugreifen können.



Standardmäßig verlangt pNFS, dass alle Daten-LIFs im SVM über Schnittstellen auf den NFS-Clients routbar sind, da pNFS-Gerätelisten mit allen Daten-LIFs im SVM gefüllt werden. Als Folge davon könnten nicht routingfähige Daten-LIFs ausgewählt werden, was zu Ausfallszenarien führen kann. Als bewährte Vorgehensweise sollten routingfähige Daten-LIFs nur bei Verwendung von pNFS konfiguriert werden.

Ab ONTAP 9.18.1 RC1 und späteren Versionen können Sie pro Subnetz festlegen, welche Schnittstellen für pNFS-Datenverkehr geeignet sind, wodurch eine Mischung aus routingfähigen und nicht routingfähigen Schnittstellen möglich ist. Wenden Sie sich an den NetApp Support, um Informationen zu den Befehlen zu erhalten.

NFSv4.0

NFSv4.0 ist eine Option, die auf einem ONTAP -NFS-Server neben NFSv4.1 aktiviert werden kann. Allerdings funktioniert pNFS nicht mit NFSv4.0. Wenn NFSv4.0 auf dem NFS-Server aktiviert ist, können Clients diese Protokollversion möglicherweise unwissentlich einbinden und pNFS nicht nutzen. Daher ist es ratsam, NFSv4.0 bei der Verwendung von pNFS explizit zu deaktivieren. NFSv4.1 muss weiterhin aktiviert sein und kann unabhängig von NFSv4.0 funktionieren.

NFSv4.1-Überweisungen

NFSv4.1-Verweise lokalisieren den Mount-Pfad vom Client zur Netzwerkschnittstelle des Knotens, dem das Volume gehört. pNFS lokalisiert den Datenpfad, und der Mount-Pfad fungiert als Metadatenserver.

Obwohl die beiden Funktionen grundsätzlich zusammen verwendet werden können, kann die Verwendung von NFSv4.1-Verweisen mit pNFS zu dem unerwünschten Effekt führen, dass mehrere Metadatenserver auf demselben Knoten gestapelt werden und die Möglichkeit, Metadatenserver über mehrere Clusterknoten zu verteilen, eingeschränkt wird. Wenn Metadatenserver bei der Verwendung von pNFS nicht gleichmäßig über einen Cluster verteilt sind, kann die CPU eines einzelnen Knotens mit Metadatenanfragen überlastet werden und einen Leistungsengpass verursachen.

Daher empfiehlt es sich, bei der Verwendung von pNFS auf NFSv4.1-Verweise zu verzichten. Verteilen Sie stattdessen die Mount-Punkte auf mehrere Netzwerkschnittstellen und Knoten im Cluster.

["Erfahren Sie mehr über das Aktivieren oder Deaktivieren von NFSv4-Verweisen."](#)

NFS Kerberos

Mit NFS Kerberos ist es möglich, die Authentifizierung mit krb5 zu verschlüsseln und zusätzlich Datenpakete mit krb5i und krb5p zu verschlüsseln. Dies wird in einer SVM pro Netzwerkschnittstelle aktiviert und ausführlich beschrieben in ["Technischer Bericht von NetApp 4616: NFS Kerberos im ONTAP mit Microsoft Active Directory"](#) Die

Da pNFS den Datenverkehr über Knoten und Netzwerkschnittstellen in der SVM umleiten kann, muss NFS Kerberos auf jeder Netzwerkschnittstelle in der SVM aktiviert und funktionsfähig sein. Wenn eine Netzwerkschnittstelle in der SVM nicht für Kerberos aktiviert ist, kann pNFS beim Zugriff auf Datenvolumes auf diesen Schnittstellen nicht ordnungsgemäß funktionieren.

Wenn man beispielsweise einen Lesetest mit parallel dd auf einer pNFS-fähigen SVM mit zwei

Netzwerkschnittstellen durchführt (von denen nur eine für Kerberos aktiviert ist), funktionieren die Dateien auf der Kerberos-fähigen Schnittstelle einwandfrei, während die Dateien auf dem Knoten mit der Schnittstelle ohne aktiviertes Kerberos ihre Lesevorgänge nie abschließen konnten. Nachdem Kerberos auf beiden Schnittstellen aktiviert wurde, funktionierten alle Dateien wie erwartet.

NFS Kerberos kann mit pNFS verwendet werden, vorausgesetzt, NFS Kerberos ist auf allen Netzwerkschnittstellen in der SVM aktiviert. Beachten Sie, dass NFS Kerberos aufgrund der Verschlüsselung/Entschlüsselung der Pakete zu Leistungseinbußen führen kann. Daher empfiehlt es sich, pNFS mit NFS Kerberos gründlich mit Ihren Workloads zu testen, um sicherzustellen, dass etwaige Leistungseinbußen die Workload nicht übermäßig beeinträchtigen.

Nachfolgend ein Beispiel für die Leistung beim parallelen Lesen bei Verwendung von krb5 (Authentifizierung) und krb5p (Ende-zu-Ende-Verschlüsselung) mit pNFS auf einem RHEL 9.5-Client. Krb5p verzeichnete in diesem Test einen Leistungsabfall von 70%.

Kerberos-Geschmack	MB/s	Fertigstellungszeit
Krb5	<ul style="list-style-type: none"> • File1-243 • File2-243 • File3-238 • File4-238 	<ul style="list-style-type: none"> • File1-43 • File2-43,1 • File3-44 • File4-44,1
krb5p	<ul style="list-style-type: none"> • File1-72,9 • File2-72,8 • File3-71,4 • File4-71,2 	<ul style="list-style-type: none"> • File1-143,9 • File2-144,1 • File3-146,9 • File4-147,3

["Erfahren Sie mehr über Kerberos mit NFS für starke Sicherheit."](#)

NFSv4.2

NFSv4.2 wurde in ONTAP 9.8 hinzugefügt und ist die neueste verfügbare NFSv4.x-Version (RFC-7862). NFSv4.2 bietet keine explizite Option zum Aktivieren/Deaktivieren. Stattdessen wird es zusammen mit NFSv4.1 aktiviert/deaktiviert. (-4.1 enabled). Wenn ein Client NFSv4.2 unterstützt, handelt er während des Mount-Befehls die höchste unterstützte NFS-Version aus, sofern nicht anders angegeben. `minorversion=2` Montageoption.

NFSv4.2 in ONTAP unterstützt die folgenden Funktionen:

- Sicherheitsetiketten (MAC-Etiketten)
- Erweiterte Attribute
- Operationen mit dünnbesetzten Dateien (FALLOCATE)

pNFS wurde mit NFSv4.1 eingeführt, wird aber auch mit NFSv4.2 sowie den dazugehörigen Funktionen unterstützt.

["Erfahren Sie mehr über die ONTAP-Unterstützung für NFSv4.2"](#)

pNFS-Befehle, Statistiken und Ereignisprotokolle

Diese ONTAP CLI-Befehle beziehen sich speziell auf pNFS. Sie können damit konfigurieren, Fehler beheben und Statistiken erfassen.

Aktivieren Sie NFSv4.1

```
nfs modify -vserver SVM -v4.1 enabled
```

Aktivieren Sie pNFS

```
nfs modify -vserver SVM -v4.1-pnfs enabled
```

pNFS-Geräte anzeigen (erweiterte Berechtigungen)

```
pnfs devices show -vserver SVM
```

Vserver Name Generation	Mapping ID	Volume MSID	Mapping Status	
-----	-----	-----	-----	
SVM	17	2157024470	notavailable	2
SVM	18	2157024463	notavailable	2
SVM	19	2157024469	available	3
SVM	20	2157024465	available	4
SVM	21	2157024467	available	3
SVM	22	2157024462	available	1

pNFS-Gerätezuordnungen anzeigen (erweiterte Berechtigungen)

```
pnfs devices mappings show -vserver SVM
```

Vserver Name	Mapping ID	Dsid	LIF IP
-----	-----	-----	-----
SVM	19	2449	10.x.x.x
SVM	20	2512	10.x.x.y
SVM	21	2447	10.x.x.x
SVM	22	2442	10.x.x.y

pNFS-spezifische Leistungsindikatoren erfassen (erweiterte Berechtigungen)

```
statistics start -object nfsv4_1 -vserver SVM -sample-id [optional-name]
```

pNFS-spezifische Leistungsindikatoren anzeigen (erweiterte Berechtigungen)

```
statistics show -object nfsv4_1 -vserver SVM
```

Liste der pNFS-spezifischen Zähler anzeigen (erweiterte Berechtigungen)

```
statistics catalog counter show -object nfsv4_1 -counter *layout*|*device*
```

Object: nfsv4_1

Counter	Description
-----	-----
getdeviceinfo_avg_latency	Average latency of NFSv4.1 GETDEVICEINFO operations.
getdeviceinfo_error	The number of failed NFSv4.1 GETDEVICEINFO operations.
getdeviceinfo_percent	Percentage of NFSv4.1 GETDEVICEINFO operations.
getdeviceinfo_success	The number of successful NFSv4.1 GETDEVICEINFO operations.
getdeviceinfo_total	Total number of NFSv4.1 GETDEVICEINFO operations.
getdevicelist_avg_latency	Average latency of NFSv4.1 GETDEVICELIST operations.
getdevicelist_error	The number of failed NFSv4.1 GETDEVICELIST operations.
getdevicelist_percent	Percentage of NFSv4.1 GETDEVICELIST operations.
getdevicelist_success	The number of successful NFSv4.1 GETDEVICELIST operations.
getdevicelist_total	Total number of NFSv4.1 GETDEVICELIST operations.
layoutcommit_avg_latency	Average latency of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_error	The number of failed NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_percent	Percentage of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_success	The number of successful NFSv4.1 LAYOUTCOMMIT operations.

layoutcommit_total	Total number of NFSv4.1 LAYOUTCOMMIT operations.
layoutget_avg_latency	Average latency of NFSv4.1 LAYOUTGET operations.
layoutget_error	The number of failed NFSv4.1 LAYOUTGET operations.
layoutget_percent	Percentage of NFSv4.1 LAYOUTGET operations.
layoutget_success	The number of successful NFSv4.1 LAYOUTGET operations.
layoutget_total	Total number of NFSv4.1 LAYOUTGET operations.
layoutreturn_avg_latency	Average latency of NFSv4.1 LAYOUTRETURN operations.
layoutreturn_error	The number of failed NFSv4.1 LAYOUTRETURN operations.
layoutreturn_percent	Percentage of NFSv4.1 LAYOUTRETURN operations.
layoutreturn_success	The number of successful NFSv4.1 LAYOUTRETURN operations.
layoutreturn_total	Total number of NFSv4.1 LAYOUTRETURN operations.

Aktive Netzwerkverbindungen für NFS anzeigen

Sie können mit folgendem Befehl überprüfen, ob mehrere TCP-Verbindungen zur SVM hergestellt werden:
`network connections active show` **Befehl.**

Wenn Sie beispielsweise NFS-Sitzungs-Trunks anzeigen möchten, suchen Sie nach Verbindungen von denselben Clients über verschiedene Schnittstellen pro Knoten:

```
cluster::*> network connections active show -node cluster-0* -vserver PNFS
```

	Vserver	Interface	Remote	
CID Ctx Name	Name:Local	Port	Host:Port	
Protocol/Service				
-----	---	-----	-----	-----

Node: node-01				
2304333128 14 PNFS	data1:2049		ubuntu22-224:740	TCP/nfs
2304333144 10 PNFS	data3:2049		ubuntu22-224:864	TCP/nfs
2304333151 5 PNFS	data1:2049		ubuntu22-226:848	TCP/nfs
2304333167 15 PNFS	data3:2049		ubuntu22-226:684	TCP/nfs
Node: node-02				
2497668321 12 PNFS	data2:2049		ubuntu22-224:963	TCP/nfs
2497668337 18 PNFS	data4:2049		ubuntu22-224:859	TCP/nfs
2497668344 14 PNFS	data2:2049		ubuntu22-226:675	TCP/nfs
2497668360 7 PNFS	data4:2049		ubuntu22-226:903	TCP/nfs

NFS-Versionsinformationen für verbundene Clients anzeigen

Sie können NFS-Verbindungen auch mit dem anzeigen `nfs connected-clients show` Befehl. Beachten Sie, dass die angezeigte Liste nur Clients umfasst, die in den letzten 48 Stunden aktiven NFS-Datenverkehr hatten. Im Leerlauf befindliche NFS-Clients (selbst wenn sie noch eingebunden sind) werden möglicherweise erst angezeigt, wenn auf die Einbindung zugegriffen wird. Sie können diese filtern, um nur die zuletzt aufgerufenen Clients anzuzeigen, indem Sie die folgenden Angaben machen: `-idle-time` Besonderheit.

Um beispielsweise Clients mit Aktivität in den letzten 10 Minuten für die pNFS SVM anzuzeigen:

```
cluster::*> nfs connected-clients show -vserver PNFS -idle-time <10m>

Node: node-01

Vserver: PNFS Data-IP: 10.x.x.x Local Remote Client-IP Protocol Volume
Policy Idle-Time Reqs Reqs Trunking

10.x.x.a nfs4.2 PNFS_root default 9m 10s 0 149 false 10.x.x.a nfs4.2
FG_0001 default 9m 10s 135847 0 false 10.x.x.b nfs4.2 PNFS_root default 8m
12s 0 157 false 10.x.x.b nfs4.2 FG_0001 default 8m 12s 52111 0 false
```

Verwandte Informationen

- ["Erfahren Sie mehr über paralleles NFS \(pNFS\) in ONTAP."](#)

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.