



Versionshinweise

Cloud Backup

NetApp
January 09, 2023

Inhaltsverzeichnis

- Was ist neu bei Cloud Backup 1
 - 9 Januar 2023 1
 - Bis 19. Dezember 2022 1
 - Bis 6. Dezember 2022 2
 - November 2022 3
 - 28. September 2022 4
 - 19. September 2022 5
 - 18. August 2022 6
 - 13 Juli 2022 7
 - 14. Juni 2022 8
 - Mai 2022 9
 - 4. April 2022 10
 - 3 März 2022 10
 - 14 Februar 2022 10
 - Januar 2022 11

Was ist neu bei Cloud Backup

Alles zum Thema Cloud Backup:

9 Januar 2023

Möglichkeit, ältere Backup-Dateien in AWS S3 Archiv-Storage von StorageGRID Systemen zu verschieben

Jetzt können Sie ältere Backup-Dateien von StorageGRID Systemen auf Archiv-Storage in AWS S3 verschieben. So können Sie auf Ihren StorageGRID Systemen Speicherplatz freigeben und Kosten sparen, indem Sie eine kostengünstige Storage-Klasse für alte Backup-Dateien verwenden. Zudem stehen für das Tiering von Backups AWS S3 Glacier oder S3 Glacier Deep Archive Storage zur Verfügung.

Diese Funktion ist verfügbar, wenn Ihr Cluster ONTAP 9.12.1 oder höher verwendet und Ihr StorageGRID System mindestens 11.3 verwendet. ["Hier erfahren Sie mehr"](#).

Möglichkeit, Ihre eigenen vom Kunden gemanagten Schlüssel zur Datenverschlüsselung auf Google Cloud auszuwählen

Beim Backup von Daten aus Ihren ONTAP-Systemen auf Google Cloud Storage können Sie nun im Aktivierungsassistenten Ihre eigenen, vom Kunden gemanagten Schlüssel zur Datenverschlüsselung auswählen und nicht die von Google gemanagten Standardschlüssel verwenden. Legen Sie zuerst die von Kunden gemanagten Schlüssel fest und geben Sie bei der Aktivierung von Cloud Backup Details ein.

Die Rolle „Storage-Admin“ wird für das Servicekonto zur Erstellung von Backups in Google Cloud Storage nicht mehr benötigt

In früheren Versionen war die Rolle „Storage Admin“ für das Service-Konto erforderlich, mit dem Cloud Backup auf Google Cloud Storage Buckets zugreifen kann. Jetzt können Sie eine benutzerdefinierte Rolle mit einem reduzierten Satz von Berechtigungen erstellen, die dem Servicekonto zugewiesen werden sollen. ["So bereiten Sie Ihren Google Cloud Storage auf Backups vor"](#).

Die Seite Ergebnisse der Jobüberwachung kann als CSV-Bericht heruntergeladen werden

Nachdem Sie die Seite Jobüberwachung gefiltert haben, um die gewünschten Jobs und Aktionen anzuzeigen, können Sie nun eine .csv-Datei dieser Daten generieren und herunterladen. Anschließend können Sie die Informationen analysieren oder den Bericht an andere Personen in Ihrem Unternehmen senden. ["Erfahren Sie, wie Sie einen Bericht zur Jobüberwachung erstellen"](#).

Bis 19. Dezember 2022

Erweiterungen für Cloud Backup für Applikationen

- SAP HANA Datenbanken
 - Unterstützung für richtlinienbasiertes Backup und Restore von SAP HANA Datenbanken in Azure NetApp Files (ANF)
 - Unterstützt benutzerdefinierte Richtlinien

- Oracle Datenbanken
 - Hosts hinzufügen und Plug-in automatisch implementieren
 - Unterstützt benutzerdefinierte Richtlinien
 - Unterstützung von richtlinienbasierten Backups, Restores und Klonen von Oracle Datenbanken auf Cloud Volumes ONTAP
 - Unterstützung von richtlinienbasiertem Backup und Restore von Oracle Datenbanken in Amazon FSX für NetApp ONTAP
 - Unterstützt die Wiederherstellung von Oracle Datenbanken mithilfe von Connect-and-Copy-Methode
 - Unterstützt Oracle 21c
 - Das Klonen von Cloud-nativer Oracle Database wird unterstützt

Verbesserungen bei Cloud Backup für Virtual Machines

- Virtual Machines
 - Backup von Virtual Machines aus sekundärem On-Premises-Storage
 - Unterstützt benutzerdefinierte Richtlinien
 - Unterstützt Google Cloud Platform (GCP) für den Backup von einem oder mehreren Datastores
 - Unterstützt kostengünstigen Cloud-Storage wie Glacier, Deep Glacier und Azure Archive

Bis 6. Dezember 2022

Erforderliche Änderungen am Endpunkt für ausgehende Internetzugriffe für Connector

Aufgrund der Änderung im Cloud-Backup müssen die folgenden Connector-Endpunkte für einen erfolgreichen Cloud-Backup-Betrieb geändert werden:

Alter Endpunkt	Neuer Endpunkt
https://cloudmanager.cloud.netapp.com	https://api.bluelxp.netapp.com
https://*.cloudmanager.cloud.netapp.com	https://*.api.bluelxp.netapp.com

Hier finden Sie die vollständige Liste der Endpunkte für Ihr "AWS", "Google Cloud", Oder "Azure" Cloud-Umgebung.

Unterstützung für die Auswahl des Google Archivspeicherclasses in der UI

Sicherungsdateien werden zunächst in der Speicherklasse Google Standard erstellt. Jetzt können Sie über die Benutzeroberfläche von Cloud Backup ältere Backups nach einer bestimmten Anzahl von Tagen auf Google Archiv-Storage verschieben, um die Kosten weiter zu optimieren.

Diese Funktion wird derzeit für ONTAP-Cluster vor Ort mit ONTAP 9.12.1 oder höher unterstützt. Dieses Angebot ist derzeit nicht für Cloud Volumes ONTAP Systeme verfügbar.

Unterstützung für FlexGroup Volumes

Cloud Backup unterstützt jetzt Backups und Restores von FlexGroup Volumes. Bei Verwendung von ONTAP

9.12.1 oder neuer können Sie FlexGroup Volumes in Public- und Private-Cloud-Storage sichern. Wenn Sie über funktionierende Umgebungen mit FlexVol- und FlexGroup-Volumes verfügen, können Sie nach der Aktualisierung der ONTAP Software jedes der FlexGroup-Volumes auf diesen Systemen sichern.

["Die vollständige Liste der unterstützten Volume-Typen finden Sie unter"](#).

Möglichkeit zur Wiederherstellung von Daten aus Backups in einem bestimmten Aggregat auf Cloud Volumes ONTAP Systemen

In älteren Versionen könnten Sie das Aggregat nur auswählen, wenn Sie Daten in On-Premises-ONTAP-Systemen wiederherstellen. Diese Funktion ist jetzt auch für die Wiederherstellung von Daten auf Cloud Volumes ONTAP Systemen geeignet.

November 2022

Möglichkeit, ältere Snapshot Kopien in die Basis-Backup-Dateien zu exportieren

Wenn es lokale Snapshot-Kopien für Volumes in Ihrer Arbeitsumgebung gibt, die Ihren Backup-Schedule-Etiketten (z. B. täglich, wöchentlich usw.) entsprechen, können Sie diese historischen Snapshots als Backup-Dateien in den Objekt-Storage exportieren. Damit können Sie Ihre Backups in die Cloud initialisieren, indem Sie ältere Snapshot-Kopien in die Basis-Backup-Kopie verschieben.

Diese Option ist bei der Aktivierung von Cloud Backup für Ihre Arbeitsumgebungen verfügbar. Sie können diese Einstellung auch später im ändern ["Seite „Erweiterte Einstellungen“"](#).

Cloud Backup kann nun für die Archivierung von Volumes verwendet werden, die Sie nicht mehr auf dem Quellsystem benötigen

Nun können Sie die Backup-Beziehung für ein Volume löschen. Auf diese Weise erhalten Sie einen Archivierungsmechanismus, wenn Sie die Erstellung neuer Backup-Dateien beenden und das Quell-Volume löschen möchten, aber alle vorhandenen Backup-Dateien behalten möchten. So können Sie das Volume bei Bedarf später aus der Backup-Datei wiederherstellen und gleichzeitig Speicherplatz aus dem Quell-Storage-System löschen. ["Erfahren Sie, wie"](#).

Unterstützung wurde hinzugefügt, um Cloud Backup-Benachrichtigungen per E-Mail und im Notification Center zu erhalten

Cloud Backup wurde in den BlueXP Notification Service integriert. Sie können Cloud-Backup-Benachrichtigungen anzeigen, indem Sie in der Menüleiste von BlueXP auf die Benachrichtigungsglocke klicken. Sie können BlueXP auch so konfigurieren, dass Benachrichtigungen per E-Mail als Benachrichtigungen gesendet werden, damit Sie auch dann über wichtige Systemaktivitäten informiert werden können, wenn Sie nicht im System angemeldet sind. Die E-Mail kann an alle Empfänger gesendet werden, die auf Backup- und Wiederherstellungsaktivitäten achten müssen. ["Erfahren Sie, wie"](#).

Mit der neuen Seite „Erweiterte Einstellungen“ können Sie Backup-Einstellungen auf Cluster-Ebene ändern

Auf dieser neuen Seite können Sie viele Backup-Einstellungen auf Cluster-Ebene ändern, die Sie bei der Aktivierung von Cloud Backup für jedes ONTAP System festgelegt haben. Sie können auch einige Einstellungen ändern, die als „Standard“-Backup-Einstellungen angewendet werden. Die vollständigen Backup-Einstellungen, die Sie ändern können, umfassen:

- Die Storage-Schlüssel, die Ihrem ONTAP System Zugriff auf Objekt-Storage gewähren
- Die Netzwerkbandbreite, die dem Hochladen von Backups in den Objektspeicher zugewiesen ist
- Die automatische Backup-Einstellung (und -Richtlinie) für zukünftige Volumes
- Die Archiv-Storage-Klasse (nur AWS)
- Gibt an, ob historische Snapshot-Kopien in den ersten Basis-Backup-Dateien enthalten sind
- Gibt an, ob „jährliche“ Snapshots aus dem Quellsystem entfernt werden
- ONTAP-IPspace, der mit dem Objekt-Storage verbunden ist (bei falscher Auswahl während der Aktivierung)

["Weitere Informationen zum Managen von Backup-Einstellungen auf Cluster-Ebene".](#)

Sie können jetzt Backup-Dateien mithilfe von Search & Restore wiederherstellen, wenn Sie einen On-Premises Connector verwenden

In der vorherigen Version wurde beim Einsatz des Connectors in Ihrer Umgebung Unterstützung beim Erstellen von Backup-Dateien in der Public Cloud erhalten. In dieser Version wurde mithilfe von Search & Restore weiterhin Unterstützung für die Wiederherstellung von Backups von Amazon S3 oder Azure Blob ermöglicht, wenn der Connector in Ihrer lokalen Umgebung implementiert wird. Search & Restore unterstützt jetzt auch die Wiederherstellung von Backups aus StorageGRID Systemen in ONTAP Systemen vor Ort.

Derzeit muss der Connector in der Google Cloud Platform bereitgestellt werden, wenn Sie Search & Restore verwenden, um Backups von Google Cloud Storage wiederherzustellen.

Die Seite Job-Überwachung wurde aktualisiert

Die folgenden Aktualisierungen wurden an der vorgenommenen ["Seite Job-Überwachung"](#):

- Es steht eine Spalte für „Workload“ zur Verfügung, damit Sie die Seite filtern können, um Jobs für die folgenden Backup-Services anzuzeigen: Volumes, Applikationen, Virtual Machines und Kubernetes.
- Sie können neue Spalten für „Benutzername“ und „Jobtyp“ hinzufügen, wenn Sie diese Details für einen bestimmten Backup-Job anzeigen möchten.
- Auf der Seite Jobdetails werden alle untergeordneten Jobs angezeigt, die ausgeführt werden, um den Hauptjob abzuschließen.
- Die Seite wird automatisch alle 15 Minuten aktualisiert, sodass Sie immer die aktuellsten Ergebnisse des Jobstatus sehen. Und Sie können auf die Schaltfläche **Aktualisieren** klicken, um die Seite sofort zu aktualisieren.

Kontoübergreifende Backup-Verbesserungen für AWS

Wenn Sie ein anderes AWS Konto für Ihre Cloud Volumes ONTAP-Backups verwenden möchten als für die Quell-Volumes, müssen Sie die Zielanmeldeinformationen für AWS-Konto in BlueXP hinzufügen, und Sie müssen die Berechtigungen "s3:PutBucketPolicy" und "s3:PutBucketEigntümershipControls" zur IAM-Rolle hinzufügen, die BlueXP mit Berechtigungen versorgt. In der Vergangenheit mussten Sie zahlreiche Einstellungen in der AWS Console konfigurieren – dieser Wunsch brauchen Sie nicht mehr.

28. September 2022

Erweiterungen für Cloud Backup für Applikationen

- Unterstützt Google Cloud Platform (GCP) und StorageGRID, um applikationskonsistente Snapshots zu erstellen
- Erstellen benutzerdefinierter Richtlinien
- Unterstützung von Archiv-Storage
- SAP HANA-Applikationen sichern
- Sichern Sie Oracle und SQL Applikationen auf VMware Umgebungen
- Backup von Applikationen aus lokalem Sekundär-Storage
- Backups deaktivieren
- SnapCenter-Server nicht registrieren

Verbesserungen bei Cloud Backup für Virtual Machines

- Unterstützt StorageGRID für das Backup von einem oder mehreren Datastores
- Erstellen benutzerdefinierter Richtlinien

19. September 2022

DataLock und Ransomware-Schutz können für Backup-Dateien in StorageGRID Systemen konfiguriert werden

In der letzten Version wurden *DataLock und Ransomware Protection* für Backups eingeführt, die in Amazon S3 Buckets gespeichert sind. Diese Version erweitert den Support für Backup-Dateien, die in StorageGRID Systemen gespeichert sind. Wenn Ihr Cluster ONTAP 9.11.1 oder höher verwendet und auf Ihrem StorageGRID System Version 11.6.0.3 oder höher ausgeführt wird, ist diese neue Backup-Policy-Option verfügbar. ["Erfahren Sie mehr darüber, wie Sie mit DataLock- und Ransomware-Schutz Ihre Backups schützen können"](#).

Beachten Sie, dass Sie einen Connector mit Version 3.9.22 oder neuer verwenden müssen. Der Connector muss in Ihrem Haus installiert werden und kann auf einer Website mit oder ohne Internetzugang installiert werden.

Die Wiederherstellung auf Ordner Ebene ist jetzt über Ihre Sicherungsdateien verfügbar

Jetzt können Sie einen Ordner aus einer Sicherungsdatei wiederherstellen, wenn Sie Zugriff auf alle Dateien in diesem Ordner benötigen (Verzeichnis oder Freigabe). Das Wiederherstellen eines Ordners ist wesentlich effizienter als das Wiederherstellen eines gesamten Volumes. Diese Funktion steht für Wiederherstellungsvorgänge mit der Methode „Durchsuchen und Wiederherstellen“ und der Methode „Suchen und Wiederherstellen“ bei Verwendung von ONTAP 9.11.1 oder höher zur Verfügung. Zu diesem Zeitpunkt können Sie nur einen einzigen Ordner auswählen und wiederherstellen, und nur Dateien aus diesem Ordner werden wiederhergestellt - keine Unterordner oder Dateien in Unterordnern, wiederhergestellt.

Restores auf Dateiebene stehen nun für Backups zur Verfügung, die in Archiv-Storage verschoben wurden

Früher war es möglich, Volumes nur von Backup-Dateien wiederherzustellen, die in Archiv-Storage verschoben wurden (nur AWS und Azure). Sie können nun einzelne Dateien aus diesen archivierten Backup-

Dateien wiederherstellen. Diese Funktion steht für Wiederherstellungsvorgänge mit der Methode „Durchsuchen und Wiederherstellen“ und der Methode „Suchen und Wiederherstellen“ bei Verwendung von ONTAP 9.11.1 oder höher zur Verfügung.

Wiederherstellung auf Dateiebene bietet jetzt die Möglichkeit, die ursprüngliche Quelldatei zu überschreiben

In der Vergangenheit wurde eine auf das ursprüngliche Volume wiederhergestellte Datei immer als neue Datei mit dem Präfix "Restore_<file_Name>" wiederhergestellt. Nun können Sie die ursprüngliche Quelldatei überschreiben, wenn Sie die Datei an den ursprünglichen Speicherort auf dem Volume wiederherstellen. Diese Funktion steht für Wiederherstellungsvorgänge sowohl mit der Methode Durchsuchen und Wiederherstellen als auch mit der Methode Suchen und Wiederherstellen zur Verfügung.

Per Drag-and-Drop können Sie Cloud-Backups in StorageGRID-Systemen aktivieren

Wenn der "StorageGRID" Ziel für Ihre Backups ist als Arbeitsumgebung auf dem Canvas vorhanden, Sie können Ihre On-Prem ONTAP Arbeitsumgebung auf das Ziel ziehen, um den Cloud Backup-Setup-Assistenten zu starten.

18. August 2022

Der Schutz von Cloud-nativen Applikationsdaten wurde durch zusätzliche Unterstützung hinzugefügt

Cloud Backup für Applikationen ist ein SaaS-basierter Service mit Datensicherungsfunktionen für Applikationen, die auf NetApp Cloud Storage ausgeführt werden. Cloud Backup für Applikationen in BlueXP ermöglicht effizientes, applikationskonsistentes, richtlinienbasiertes Backup und Restore von Oracle Datenbanken in Amazon FSX für NetApp ONTAP.<https://docs.netapp.com/us-en/cloud-manager-backup-restore/concept-protect-cloud-app-data-to-cloud.html>["Weitere Informationen ."]].

Die Suche & Wiederherstellung wird jetzt auch für Backup-Dateien in Azure Blob unterstützt

Die Suchmethode zur Wiederherstellung von Volumes und Dateien steht jetzt für Benutzer zur Verfügung, die ihre Backup-Dateien in Azure Blob Storage speichern. ["Erfahren Sie, wie Sie Ihre Volumes und Dateien mithilfe von Search Restore wiederherstellen wiederherstellen wiederherstellen wiederherstellen"](#).

Beachten Sie, dass in der Rolle Connector zusätzliche Berechtigungen erforderlich sind, um diese Funktion nutzen zu können. Ein Connector, der mit Software der Version 3.9.21 (August 2022) bereitgestellt wird, umfasst diese Berechtigungen. Wenn Sie den Connector mit einer früheren Version bereitgestellt haben, müssen Sie die Berechtigungen manuell hinzufügen. ["Lesen Sie, wie Sie diese Berechtigungen hinzufügen, falls erforderlich"](#).

Wir haben die Möglichkeit hinzugefügt, Ihre Backup-Dateien vor Löschungen und Ransomware-Angriffen zu schützen

Cloud Backup unterstützt jetzt Objekt-Lock-Support für Ransomware-sichere Backups. Wenn Ihr Cluster ONTAP 9.11.1 oder höher verwendet und Ihr Backup-Ziel Amazon S3 ist, steht jetzt eine neue Backup-Policy-Option namens *DataLock und Ransomware Protection* zur Verfügung. DataLock schützt Ihre Backup-Dateien vor Änderungen oder Löschung. Ransomware-Schutz scannt Ihre Backup-Dateien, um nach einem Ransomware-Angriff auf Ihre Backup-Dateien zu suchen. ["Erfahren Sie mehr darüber, wie Sie mit DataLock-](#)

und Ransomware-Schutz Ihre Backups schützen können".

Beachten Sie, dass in der Rolle Connector zusätzliche Berechtigungen erforderlich sind, um diese Funktion nutzen zu können. Ein Connector, der mit der Software Version 3.9.21 bereitgestellt wird, enthält diese Berechtigungen. Wenn Sie den Connector mit einer früheren Version bereitgestellt haben, müssen Sie die Berechtigungen manuell hinzufügen. ["Lesen Sie, wie Sie diese Berechtigungen hinzufügen, falls erforderlich"](#).

Cloud Backup unterstützt jetzt Richtlinien, die mithilfe benutzerdefinierter SnapMirror Labels erstellt werden

Zuvor unterstützte Cloud Backup nur vordefinierte SnapMirror Labels wie stündlich, täglich, wöchentlich, stündlich oder jährlich. Jetzt kann Cloud Backup SnapMirror Richtlinien erkennen, die über individuelle SnapMirror-Labels verfügen, die Sie mit System Manager oder der CLI erstellt haben. Diese neuen Bezeichnungen werden der Cloud Backup-UI ausgesetzt. Damit können Sie Volumes mit dem SnapMirror Label Ihrer Wahl in der Cloud sichern.

Zusätzliche Verbesserung der Backup-Richtlinien für ONTAP Systeme

Einige Seiten der Backup-Richtlinien wurden neu gestaltet, um alle für Volumes in jedem ONTAP Cluster verfügbaren Backup-Richtlinien einfacher anzuzeigen. Dadurch sind die Details der verfügbaren Richtlinien einfacher abrufbar, damit Sie die besten Richtlinien auf Ihren Volumes anwenden können.

Aktivieren Sie Cloud Backup per Drag-and-Drop in Azure Blob und Google Cloud Storage

Wenn der ["Azure Blob"](#) Oder ["Google Cloud Storage"](#) Ziel für Ihre Backups ist als Arbeitsumgebung auf dem Canvas vorhanden. Sie können Ihre On-Prem ONTAP oder Cloud Volumes ONTAP Arbeitsumgebung (installiert in Azure oder GCP) auf das Ziel ziehen, um den Backup-Setup-Assistenten zu starten.

Für Amazon S3 Buckets ist diese Funktion bereits vorhanden.

13 Juli 2022

SnapLock Enterprise Volumes werden jetzt zusätzlich unterstützt

Mit Cloud Backup lassen sich jetzt SnapLock Enterprise Volumes in Public und Private Clouds sichern. Für diese Funktion muss auf Ihrem ONTAP System ONTAP 9.11.1 oder höher ausgeführt werden. SnapLock Compliance Volumes werden derzeit jedoch nicht unterstützt.

Bei Verwendung eines On-Premises-Connectors können Sie jetzt Backup-Dateien in der Public Cloud erstellen

Früher mussten Sie den Connector im selben Cloud-Provider implementieren, als wo Sie Backup-Dateien erstellt haben. Mit einem Connector, der in Ihrem Standort implementiert ist, können Sie jetzt Backup-Dateien von On-Premises-ONTAP-Systemen über Amazon S3, Azure Blob und Google Cloud Storage erstellen. (Bei der Erstellung von Sicherungsdateien auf StorageGRID Systemen war immer ein On-Prem-Connector erforderlich.)

Wenn Backup-Richtlinien für ONTAP Systeme erstellt werden, sind zusätzliche Funktionen verfügbar

- Das Backup steht nun gemäß jährlicher Planung zur Verfügung. Der Standardwert für die Aufbewahrung ist

1 für jährliche Backups. Sie können diesen Wert jedoch ändern, wenn Sie auf die Backup-Dateien vieler Jahre zugreifen möchten.

- Sie können Ihre Backup-Richtlinien benennen, damit Sie Ihre Richtlinien mit beschreibenden Text identifizieren können.

14. Juni 2022

Es wurde Unterstützung für das Backup von On-Premises-ONTAP-Cluster-Daten an Standorten ohne Internetzugang hinzugefügt

Wenn Ihr ONTAP-Cluster vor Ort an einem Standort ohne Internetzugang – auch als „Dark Site“ oder „Offline“ bezeichnet – gespeichert ist, können Sie mit Cloud Backup Volumes-Daten auf einem NetApp StorageGRID-System am selben Standort sichern. Für diese Funktionalität muss auch der BlueXP Connector (Version 3.9.19 oder höher) auf der Offline-Website bereitgestellt werden.

["Lesen Sie, wie Sie den Connector in Ihrer Offline-Website installieren"](https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-backup-onprem-private-cloud.html).<https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-backup-onprem-private-cloud.html>["Erfahren Sie, wie Sie ONTAP Daten in StorageGRID auf Ihrer Offline-Website sichern"].

Cloud Backup für Virtual Machines 1.1.0 ist jetzt allgemein verfügbar

Durch die Integration des SnapCenter Plug-ins für VMware vSphere in BlueXP können Sie Daten auf Ihren virtuellen Maschinen schützen. Sie können Datastores in der Cloud sichern und Virtual Machines problemlos im lokalen SnapCenter Plug-in für VMware vSphere wiederherstellen.

["Erfahren Sie mehr über die Sicherung von Virtual Machines in der Cloud"](#).

Für die ONTAP Browse & Restore-Funktion ist keine Cloud Restore-Instanz erforderlich

Für Suchvorgänge und Restores auf Dateiebene von S3 und Blob-Storage wurde eine separate Cloud Restore-Instanz/Virtual Machine benötigt. Diese Instanz wurde heruntergefahren, wenn sie nicht verwendet wird – aber es hat immer noch Zeit und Kosten für die Wiederherstellung von Dateien hinzugefügt. Diese Funktion wurde durch einen kostenfrei bereitgestellten Container ersetzt, der bei Bedarf auf dem Connector bereitgestellt wird. Es bietet folgende Vorteile:

- Keine zusätzlichen Kosten für Restore-Vorgänge auf Dateiebene
- Schnellere Restore-Vorgänge auf Dateiebene
- Unterstützung für Browse & Restore-Vorgänge für Dateien aus der Cloud, wenn der Connector vor Ort installiert ist

Beachten Sie, dass die Cloud Restore-Instanz/VM automatisch entfernt wird, wenn Sie sie zuvor verwendet haben. Ein Cloud-Backup-Prozess wird einmal am Tag ausgeführt, um alle alten Cloud Restore-Instanzen zu löschen. Diese Änderung ist völlig transparent - es gibt keine Auswirkungen auf Ihre Daten, und Sie werden keine Änderungen an Ihren Backup- oder Restore-Jobs bemerken.

Unterstützung für Dateien aus Google Cloud- und StorageGRID-Storage finden Sie unter Durchsuchen und Wiederherstellen

Durch Hinzufügen des Containers für Browse & Restore (wie oben beschrieben) lassen sich nun Datei-wiederherstellungsvorgänge aus Backup-Dateien durchführen, die in Google Cloud- und StorageGRID-Systemen gespeichert sind. Mit Browse & Restore können Dateien jetzt bei allen Public-Cloud-Providern und

von StorageGRID wiederhergestellt werden. ["Erfahren Sie, wie Sie „Browse Restore“ verwenden, um Volumes und Dateien aus Ihren ONTAP-Backups wiederherzustellen"](#).

Per Drag-and-Drop ist Cloud-Backup im S3-Storage möglich

Wenn das Amazon S3 Ziel für Ihre Backups als Arbeitsumgebung auf dem Canvas existiert, können Sie Ihr On-Prem ONTAP-Cluster oder Cloud Volumes ONTAP-System (installiert in AWS) auf die Amazon S3-Arbeitsumgebung ziehen, um den Setup-Assistenten zu initiieren.

Automatische Anwendung einer Backup-Richtlinie auf neu erstellte Volumes in Kubernetes Clustern

Falls Sie nach Aktivierung von Cloud Backup neue persistente Volumes zu Ihren Kubernetes Clustern hinzugefügt haben, mussten Sie in der Vergangenheit auch daran denken, Backups für diese Volumes zu konfigurieren. Sie können nun eine Richtlinie auswählen, die automatisch auf neu erstellte Volumes angewendet wird ["Klicken Sie auf der Seite „Backup Settings“ auf „"](#) Für Cluster, die bereits Cloud Backup aktiviert haben.

Cloud Backup APIs sind jetzt für das Management von Backup- und Restore-Vorgängen verfügbar

Die APIs sind unter verfügbar <https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html>.
Siehe ["Auf dieser Seite"](#) Für eine Übersicht der APIs.

Mai 2022

Search & Restore wird jetzt mit Sicherungsdateien in Google Cloud Storage unterstützt

Im April wurde die Such- & Restore-Methode zur Wiederherstellung von Volumes und Dateien für Benutzer eingeführt, die ihre Backup-Dateien in AWS speichern. Jetzt ist die Funktion für Anwender verfügbar, die ihre Backup-Dateien in Google Cloud Storage speichern. ["Erfahren Sie, wie Sie Ihre Volumes und Dateien mithilfe von Search Restore wiederherstellen wiederherstellen wiederherstellen wiederherstellen"](#).

Backup-Richtlinie konfigurieren, die automatisch auf neu erstellte Volumes in Kubernetes Clustern angewendet wird

Falls Sie nach Aktivierung von Cloud Backup neue persistente Volumes zu Ihren Kubernetes Clustern hinzugefügt haben, mussten Sie in der Vergangenheit auch daran denken, Backups für diese Volumes zu konfigurieren. Sie können nun eine Richtlinie auswählen, die automatisch auf neu erstellte Volumes angewendet wird. Diese Option ist im Setup-Assistenten verfügbar, wenn Sie Cloud Backup für ein neues Kubernetes-Cluster aktivieren.

Cloud Backup erfordert jetzt eine Lizenz, bevor sie für eine Arbeitsumgebung aktiviert wird

Die Implementierung der Lizenzierung mit Cloud Backup hat einige Änderungen:

- Sie müssen sich für ein PAYGO Marketplace Abonnement bei Ihrem Cloud-Provider anmelden oder eine BYOL-Lizenz von NetApp erwerben, bevor Sie Cloud Backup aktivieren können.
- Die 30-Tage-kostenlose Testversion steht nur bei Nutzung eines PAYGO Abonnements von Ihrem Cloud-Provider zur Verfügung. Diese ist bei Verwendung der BYOL-Lizenz nicht verfügbar.

- Die kostenlose Testversion startet den Tag, an dem das Marketplace-Abonnement beginnt. Wenn Sie beispielsweise die kostenlose Testversion aktivieren, nachdem Sie 30 Tage lang ein Marketplace-Abonnement für ein Cloud Volumes ONTAP-System verwendet haben, steht die Cloud Backup-Testversion nicht zur Verfügung.

["Erfahren Sie mehr über die verfügbaren Lizenzmodelle".](#)

4. April 2022

Cloud Backup für Applikationen 1.1.0 (unterstützt von SnapCenter) ist jetzt allgemein verfügbar

Mit der neuen Cloud Backup für Applikationen können Sie vorhandene applikationskonsistente Snapshots (Backups) für Oracle und Microsoft SQL vom primären Storage vor Ort in den Cloud-Objekt-Storage in Amazon S3 oder Azure Blob auslagern.

Bei Bedarf können diese Daten aus der Cloud in On-Premises-Umgebungen wiederhergestellt werden.

["Weitere Informationen zum Schutz von On-Premises-Applikationsdaten in der Cloud".](#)

Neue Such- und Wiederherstellungsfunktion zur Suche nach Volumes oder Dateien in allen ONTAP Backup-Dateien

Jetzt können Sie nach einem Volume oder einer Datei über **alle ONTAP Backup-Dateien** nach einem Teil- oder Volldateinamen, einem partiellen oder vollständigen Dateinamen, einem Größenbereich und zusätzlichen Suchfiltern suchen. Dies ist eine großartige neue Möglichkeit, die wiederherzustellenden Daten zu finden, falls Sie nicht sicher sind, welches Cluster oder Volume die Quelle für die Daten war. ["Erfahren Sie, wie Sie suchen Restore verwenden".](#)

3 März 2022

Möglichkeit für das Backup persistenter Volumes von den GKE Kubernetes-Clustern auf Google Cloud Storage

Wenn im GKE-Cluster NetApp Astra Trident installiert ist und Cloud Volumes ONTAP für GCP als Backend-Storage für den Cluster verwendet wird, können Sie Ihre persistenten Volumes in und aus dem Google Cloud Storage sichern und wiederherstellen. ["Weitere Informationen finden Sie hier".](#)

Die Beta-Funktion zur Verwendung von Cloud Data Sense zum Scannen Ihrer Cloud Backup-Dateien wurde in dieser Version eingestellt

14 Februar 2022

Nun können Sie Backup-Richtlinien einzelnen Volumes in einem einzigen Cluster zuweisen

Früher konnten alle Volumes in einem Cluster nur eine einzelne Backup-Richtlinie zugewiesen werden. Sie können nun mehrere Backup-Richtlinien für ein einzelnes Cluster erstellen und unterschiedliche Richtlinien auf verschiedene Volumes anwenden. ["Hier erfahren Sie, wie Sie neue Backup-Richtlinien für ein Cluster erstellen und diesen ausgewählten Volumes zuweisen".](#)

Über eine neue Option können Sie automatisch eine standardmäßige Backup-Richtlinie auf neu erstellte Volumes anwenden

In der Vergangenheit mussten Sie neue Volumes, die nach Aktivierung von Cloud Backup in einer Arbeitsumgebung erstellt wurden, manuell eine Backup-Richtlinie anwenden. Unabhängig davon, ob das Volume in BlueXP, System Manager, der CLI oder mithilfe von APIs erstellt wurde, entdeckt Cloud Backup das Volume und wendet die als Standardrichtlinie ausgewählte Backup-Richtlinie an.

Diese Option steht zur Verfügung, wenn Sie das Backup in einer neuen Arbeitsumgebung aktivieren oder über die Seite „*Volumes* verwalten“ für vorhandene Arbeitsumgebungen.

Neuer Job Monitor ist verfügbar, um den Prozessstatus aller Backup- und Wiederherstellungsaufträge anzuzeigen

Der Job Monitor kann sehr hilfreich sein, wenn Sie eine Operation gegen mehrere Volumes eingeleitet haben, z. B. das Ändern der Backup-Richtlinie oder das Löschen von Backups, so dass Sie sehen können, wann der Vorgang auf allen Volumes abgeschlossen ist. "[Lesen Sie, wie Sie den Job Monitor verwenden](#)".

Januar 2022

Möglichkeit zur Sicherung persistenter Volumes von AKS Kubernetes-Clustern auf Azure Blob Storage

Wenn in Ihrem AKS Cluster NetApp Astra Trident installiert ist und Cloud Volumes ONTAP für Azure als Back-End-Storage für den Cluster genutzt wird, können Sie Volumes mit Backups und Restores von und aus dem Azure Blob-Storage durchführen. "[Weitere Informationen finden Sie hier](#)".

In dieser Version wurden die Cloud Backup Service-Gebühren geändert, um sich stärker an die Branchenstandards anzupassen

Anstatt NetApp für die Kapazität auf Basis der Größe der Backup-Dateien zu bezahlen, zahlen Sie jetzt nur für die gesicherten Daten, berechnet anhand der verwendeten logischen Kapazität (vor der ONTAP-Effizienz) der zu sichernden ONTAP Quell-Volumes. Diese Kapazität wird auch als Front-End Terabyte (FETB) bezeichnet.

Copyright-Informationen

Copyright © 2023 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.