# Versionshinweise zur NetApp Console

## Release Notes

NetApp
November 06, 2026

This PDF was generated from https://docs.netapp.com/de-de/console-relnotes/index.html on November 06, 2026. Always check docs.netapp.com for the latest.

# Inhalt


Versionshinweise zur NetApp Console . . . 1
Aktuelle Änderungen in der NetApp Console . . . 2
Cloud Volumes ONTAP . . . 2
Workload Factory . . . 3
AI Data Engine . . . 8
Sicherung und Wiederherstellung . . . 9
Ransomware-Resilienz . . . 10
Ransomware-Resilienz . . . 11
Sicherung und Wiederherstellung . . . 11
Konsoleneinrichtung und -verwaltung . . . 12
Digitaler Berater . . . 12
Cloud Volumes ONTAP . . . 12
Sicherung und Wiederherstellung . . . 13
Notfallwiederherstellung . . . 14
Keystone . . . 15
Workload Factory . . . 15
Sicherung und Wiederherstellung . . . 15
Digitaler Berater . . . 16
Sicherung und Wiederherstellung . . . 17
Cloud Volumes ONTAP . . . 17
Konsoleneinrichtung und -verwaltung . . . 18
Konsoleneinrichtung und -verwaltung . . . 19
Sicherung und Wiederherstellung . . . 19
Datenklassifizierung . . . 20
Notfallwiederherstellung . . . 20
Ransomware-Resilienz . . . 21
Digitaler Berater . . . 21
Cloud Volumes ONTAP . . . 21
StorageGRID . . . 22
Notfallwiederherstellung . . . 22
Ransomware-Resilienz . . . 22
Cloud Volumes ONTAP . . . 23
Digitaler Berater . . . 23
Sicherung und Wiederherstellung . . . 23
Konsoleneinrichtung und -verwaltung . . . 24
Ransomware-Resilienz . . . 25
Digitaler Berater . . . 25
Sicherung und Wiederherstellung . . . 25
Datenklassifizierung . . . 26
Notfallwiederherstellung . . . 26
Index der Versionshinweise für NetApp Console . . . 28
Verwaltung . . . 28
Storage . . . 28

Speicher als Service . . . 28
Datendienste . . . 28
Rechtliche Hinweise für NetApp Console . . . 30
Copyright . . . 30
Marken . . . 30
Patente . . . 30
Datenschutzrichtlinie . . . 30
Open Source . . . 30

# Versionshinweise zur NetApp Console

# Aktuelle Änderungen in der NetApp Console

Informieren Sie sich über die neuesten Änderungen an den Funktionen und Datendiensten, die Teil der NetApp Console sind. Eine vollständige Versionshistorie finden Sie unter"Vollständiger Satz der Versionshinweise" für jeden einzelnen Dienst.

Die folgenden Dienste wurden eingestellt:

**Edge-Caching**
Der Edge-Caching-Dienst wurde am 7. August 2024 entfernt.

**Kubernetes**
Die Unterstützung für die Erkennung und Verwaltung von Kubernetes-Clustern wurde am 7. August 2024 entfernt.

**Migrationsberichte**
Der Dienst für Migrationsberichte wurde am 7. August 2024 entfernt.

**Betriebsstabilität**
Die Funktionen zur betrieblichen Ausfallsicherheit wurden am 22. August 2025 entfernt.

**Sanierung**
Der Sanierungsdienst wurde am 22. April 2024 entfernt.

[[02-november-2026]]
== 02. November 2026

## Cloud Volumes ONTAP

**Anleitung zum Aktualisieren von ONTAP Hotfixes für bestimmte Cloud Volumes ONTAP Versionen**

ONTAP hat die folgenden Hotfixes veröffentlicht, die mit Cloud Volumes ONTAP Versionen 9.14.1, 9.15.1, 9.16.1, 9.17.1, 9.18.1 und 9.19.1 kompatibel sind:

- 9.14.1P18HF1
- 9.15.1P20HF1
- 9.16.1P16HF1
- 9.17.1P11HF1
- 9.18.1P8HF1
- 9.19.1P3HF1

Weitere Informationen finden Sie unter "NTAP Sicherheitshinweis 20261021-0021".

Für Ihre Cloud Volumes ONTAP Systeme werden Sie möglicherweise in der NetApp Console aufgefordert, ein Upgrade auf diese Hotfixes durchzuführen. Diese Hotfixes werden jedoch nur unterstützt, wenn die Version des Console Agenten 4.12.0 oder höher ist. Wenn die Version des Console Agenten älter als 4.12.0 ist, ignorieren Sie die Aufforderung.

"Console Agent 4.12.0"

[[01-november-2026]]
== 01. November 2026

# Workload Factory

## Verbesserungen bei der Workload Factory Verwaltung

### Daten des benutzerdefinierten Dashboard überprüfen und aktualisieren

Sie können nun sehen, wann Ihre benutzerdefinierten Dashboard-Metriken zuletzt aktualisiert wurden, und sie manuell aktualisieren. Wenn Sie den Mauszeiger über **Daten aktualisieren** bewegen, werden Datum und Uhrzeit der letzten Aktualisierung angezeigt.

Mit **Daten aktualisieren** wird ein neuer Scan gestartet. Ein Banner bestätigt, dass der Scan gestartet wurde, und die Schaltfläche bleibt deaktiviert, bis der Scan abgeschlossen ist.

Wenn neue Daten verfügbar sind, kann im Benachrichtigungsbanner **Load it now** ausgewählt werden, um das Dashboard zu aktualisieren.

Sowohl **Daten aktualisieren** als auch **Jetzt laden** erzeugen Datenerfassungsereignisse in Tracker.

"Informationen zum Aktualisieren benutzerdefinierter Dashboard-Daten"

### Regionen für benutzerdefinierte Dashboards

Benutzerdefinierte Dashboards fordern nun zur Auswahl einer oder mehrerer Regionen auf, wenn diese nicht in der Anfrage enthalten sind. Die Dashboard-Daten sind auf die ausgewählten Regionen beschränkt.

"Informationen zum Erstellen eines benutzerdefinierten Dashboards"

### IAM-Richtlinie für die Erstellung von FSx for ONTAP Links

Die CloudFormation Vorlage und der Terraform Code zum Erstellen von Links verwenden nun eine IAM-Richtlinie anstelle von Inline-Lambda-Berechtigungen.

"Informationen zum Erstellen eines Links"

### Audit und Nachverfolgung von KI-Agentenaktionen

Mit Tracker können Sie jetzt Änderungen an den Einstellungen des KI-Agenten überprüfen und im Modus lesen/schreiben jede Genehmigungsanfrage einschließlich der Frage des Agenten und der Antwort des Benutzers einsehen.

Ressourcenänderungen, die über Workload Factory APIs vorgenommen werden, protokolliert der Workload Factory Dienst, der den Vorgang ausführt.

"Informationen zu Audit und Nachverfolgung von Agentenaktionen"

## Amazon FSx for NetApp ONTAP Erweiterungen

### Verbesserungen des Initiatorgruppe-Diagramms

Das Diagramm auf der Seite „Clientzugriff managen“, das Initiatorgruppen für Blockgeräte anzeigt, enthält nun mehr Details zu Hosts. Beim Bewegen des Mauszeigers über einen Host im Diagramm erscheinen Hostdetails, darunter der Hostname, die Instanz-ID, der Workload-Typ, die Region und der iSCSI Qualified

Name (IQN).

#### E-Mail-Optimierung für Well-Architected-Probleme

Das neue E-Mail-Design bietet mehr Details und Kontext zu Konfigurationsproblemen, die von Workload Factory erkannt wurden. Die E-Mail enthält die Anzahl der analysierten Ressourcen, wie viele Warnungen oder kritische Probleme aufweisen und worin diese Probleme bestehen. Die E-Mail enthält außerdem einen Link zum FSx for ONTAP Well-Architected-Dashboard, sodass Probleme umgehend behoben werden können.

#### Gut konzipierte Dashboard-Erweiterungen

### Unterstützung für ausgewählte Konfigurationsprüfungen

Sie können die Analyse für ausgewählte Konfigurationen manuell ausführen, sodass Sie nur die Konfigurationen analysieren, für die Sie sich interessieren, und die Wartezeit verkürzen.

### Neue Empfehlungen in der Well-Architected-Analyse

Workload Factory umfasst nun die folgenden Konfigurationen in der Well-Architected Analysis für FSx for ONTAP file systems:

Für Storage Workloads:

- **Host mit Failover-Knoten verbinden**: Prüft, ob Hosts in einem Aktiv/Passiv FSx for ONTAP Dateisystem zur Gewährleistung der Zuverlässigkeit mit dem Failover-Knoten verbunden sind.
- **Verbindung des Hosts mit dem bevorzugten Knoten**: Überprüft, ob Hosts über den bevorzugten Knoten mit ihren Blockgeräten verbunden sind, um eine effiziente Performance zu gewährleisten.
- **Lücke bei der ARP/AI-Mehrgeräteerkennung**: ARP/AI bietet vollen Schutz, solange an ein Volume nur ein Blockgerät angeschlossen ist. Wenn an ein Volume mehrere Blockgeräte angeschlossen sind, verschiebt Workload Factory diese auf neue Volumes, sodass jedes Volume nur noch ein Blockgerät enthält.
- **Klonbereinigung**: Prüft, ob Volume-Klone vorhanden sind, die älter als 30 Tage sind und gelöscht werden können, um die Storage-Nutzung zu optimieren und Kosten zu senken.
- **igroup OS mit Host abgleichen**: Es wird geprüft, ob das Betriebssystem der Initiatorgruppe (igroup) mit dem Betriebssystem des Hosts übereinstimmt, um E/A- oder Performance-Probleme zu vermeiden.

Für Kubernetes-Workloads:

- **QoS-Konfiguration**: Überprüft, ob Kubernetes Persistent Volumes durch eine ONTAP QoS-Richtlinie für eine effiziente Performance geschützt sind.
- **Dedizierte Kubernetes Storage-VM**: Prüft, ob das Dateisystem eine dedizierte Storage-VM für Kubernetes-Workloads verwendet, um die Isolation zu verbessern und das Storage-Management zu vereinfachen.
- **Dedizierte Kubernetes Exportrichtlinie**: Prüft, ob jedes persistente Kubernetes Volume über eine dedizierte Exportrichtlinie verfügt, die den Zugriff nur von den Worker-Knoten des Clusters aus erlaubt.
- **Bidirektionales CHAP für Kubernetes iSCSI-Backends**: Prüft, ob auf Trident iSCSI-Backends die gegenseitige CHAP-Authentifizierung aus Sicherheitsgründen aktiviert ist.
- **Deaktivieren `showmount` auf der Applikations-Storage-VM**: Prüft, ob `showmount` auf der Applikations-Storage-VM deaktiviert ist, um zu verhindern, dass Clients Exporte auflisten, auf die sie nicht zugreifen können.

Für Datenbank-Workloads:

- **SAP HANA Snapshot-Richtlinie**: Es wird geprüft, ob die Snapshot-Richtlinie für SAP HANA Volumes auf "Keine" gesetzt ist, um die Storage-Kosten zu senken und die Performance für aktive Datenbankdaten zu verbessern.
- **MySQL Snapshot-Richtlinie**: Prüft, ob die Snapshot-Richtlinie für MySQL Volumes auf "Keine" gesetzt ist, um die Storage-Kosten zu senken und die Performance für aktive Datenbankdaten zu verbessern.
- **PostgreSQL Snapshot-Richtlinie**: Prüft, ob die Snapshot-Richtlinie für PostgreSQL Volumes auf "Keine" gesetzt ist, um die Storage-Kosten zu senken und die Performance für aktive Datenbankdaten zu verbessern.

### Aktuelle und empfohlene Werte für Konfigurationen

Im Dashboard „Well-Architected“ können Sie die aktuellen und empfohlenen Werte für einige nicht optimierte Konfigurationen einsehen. Dies zeigt Ihnen, welcher Wert empfohlen wird, bevor Sie die Konfiguration korrigieren.

- Kaltdaten-Tiering
- Snapshot-Richtlinie
- SSD Kapazitätsreserve

#### Kostenoptimierungen

### Kostenprognose und Einblicke

Mit der Funktion zur Kostenprognose können Sie jetzt die Kosten Ihrer FSx for ONTAP Dateisysteme prognostizieren. Dies hilft Ihnen bei der Budgetplanung und der effizienten Ressourcennutzung. Sie erhalten außerdem Einblicke in Ihre Kosten und Nutzungsmuster, um Optimierungspotenziale zu erkennen.

### AWS Cost and Usage Reports (CUR)

Workload Factory verwendet nun AWS Cost and Usage Reports (CUR) anstelle von AWS Cost Explorer, um detaillierte Abrechnungsdatensätze in kundeneigenen S3-Buckets bereitzustellen. CUR bietet eine bessere Kostengranularität und dient als Grundlage für erweiterte FinOps-, Kostenverrechnungs- und Kostenallokations-Anwendungsfälle.

#### Verbesserungen bei der Migration von Storage VMs

Workload Factory bietet in der Benutzeroberfläche eine verbesserte Unterstützung für die Migration von Storage VMs. Dies umfasst Schritt-für-Schritt-Anleitungen und einen Testlauf vor der Übernahme der Migration in die Produktionsumgebung.

"Weitere Informationen zur Migration von Storage-VMs"

#### Verbesserung der E-Mail-Benachrichtigung bei Replikationsverzögerung

Wenn eine große Anzahl zusammenhängender Replikationsverzögerungsereignisse auftritt, fasst Workload Factory diese automatisch in einer einzigen E-Mail-Benachrichtigung zusammen, damit Sie nicht von Benachrichtigungen überflutet werden.

#### Verbesserung des automatischen Kapazitätsmanagements

Sie können jetzt automatische Benachrichtigungen zum Kapazitätsmanagement aktivieren, um die Funktion zu

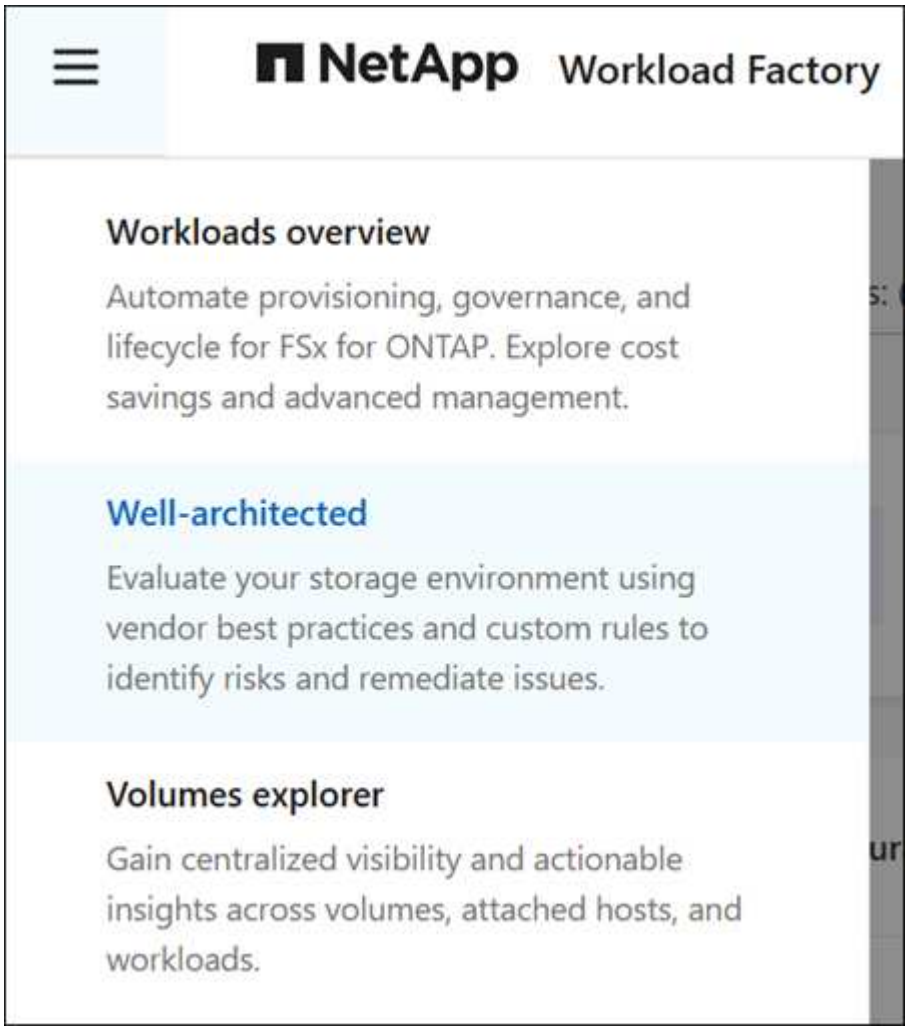
testen, bevor Sie Workload Factory mit dem automatischen Kapazitätsmanagement beauftragen. Sie werden benachrichtigt, sobald die Kapazität Ihres Dateisystems zur Neige geht.

#### Im Well-Architected Dashboard enthaltene Datenbankkonfigurationen

Das Well-Architected Dashboard enthält jetzt Empfehlungen für Ihre Datenbank-Konfigurationen, sodass Sie Ihre Einrichtung auf Grundlage von Best Practices bewerten und optimieren können. Die ersten im Dashboard enthaltenen Konfigurationen sind:

- Kaltdaten-Tiering
- Storage Effizienz
- Snapshot-Richtlinie
- SSD Kapazitätsreserve
- Blockgeräte Speicherplatzmanagement
- OS
- Betriebssystemtyp des Blockgeräts mit dem Host abgleichen
- Inaktive Blockgeräte (LUNs)
- Platzierung der Datendateien (.mdf)
- Platzierung der Protokolldateien (.ldf)
- Status von Multipath I/O
- Multipath I/O Zeitüberschreitung
- Cluster Quorum
- Compute Rightsizing

Im Hauptmenü der Workload Factory Managementplattform führt die Auswahl von **Well-architected** zum Well-Architected Dashboard.




#### Entscheidungspunkte für den Durchsatz

Sie sehen nun Empfehlungen zum Kundendurchsatz und Entscheidungspunkte für die Automatisierung. Wenn Sie den Mauszeiger über einen Entscheidungspunkt bewegen, sehen Sie Details wie die aktuelle und die empfohlene SKU oder überschrittene Kennzahlen im Zeitfenster (%).

### Erweiterungen für Google Cloud NetApp Volumes

#### Google Cloud NetApp Volumes Storage-Pools anzeigen

Sie können jetzt Ihre Storage-Pools von Google Cloud NetApp Volumes in NetApp Workload Factory anzeigen. Die Filterung kann nach Projekten, Anmeldeinformationen und Region erfolgen, und durch Auswahl des Namens eines Storage-Pools werden dessen vollständige Details angezeigt, einschließlich Zone, Replikatzone, Durchsatz, Beschreibung und Labels.

### Erweiterungen von OCI NetApp Storage Service

#### Analyse einer gut konzipierten Architektur für OCI NSS Systeme

NetApp Workload Factory umfasst die Well-Architected-Bewertung für OCI NSS-Systeme. Die Bewertung liefert Erkenntnisse, Empfehlungen und Lösungsansätze, die Ihnen dabei helfen, operative Exzellenz zu erreichen.

Für die folgenden Säulen des OCI Well-Architected Frameworks sind Konfigurationsbewertungen verfügbar:

- Zuverlässigkeit: Kapazität von Dateiobjekten, Snapshot-Richtlinie und SSD-Kapazitätspuffer
- Betriebliche Exzellenz: hostsichtbare Kapazitätsberichterstattung und Kapazitätspuffer für Volumes
- Kostenoptimierung: Kaltdaten-Tiering, Snapshot-Bereinigung und Storage-Effizienz

Weitere Informationen zu "die Well-Architected-Analyse für OCI NSS Systeme" und zu "Implementierung gut architekturierter Konfigurationen".

[[26-october-2026]]
== 26. Oktober 2026

## AI Data Engine

### AI Data Engine 1.3

AI Data Engine ist ein Metadaten-Intelligence-Service, der über NetApp Console verwaltet wird, Ihre verbundenen Systeme scannt, einen Metadatenkatalog erstellt und Ihnen die Transparenz und Tools bietet, um Storage zu optimieren und Daten in großem Maßstab zu verwalten. AI Data Engine kann als ein "AIDE Einzelknoten-Deployment", oder als AIDE Multi-Node-Deployment eingesetzt werden, wenn Ihre Umgebung Kubernetes-basierte Hochverfügbarkeit in großem Maßstab erfordert.

AI Data Engine 1.3 ist die erste allgemein verfügbare (GA) Version.

#### Deployment und Anbindung Ihrer Daten

**"In dem Umfang einsetzen, den Ihre Umgebung erfordert"**

Zur Auswahl stehen ein AIDE Single-Node-Deployment für einen schnellen Start auf einer einzelnen VM oder ein AIDE Multi-Node-Deployment auf Ihrem eigenen Kubernetes-Cluster für Hochverfügbarkeit und größere Skalierbarkeit. Falls Ihre Umgebung für den Internetzugang einen Proxy benötigt, "Informationen zu Proxys für AIDE" kann das Deployment mit einem Proxy erfolgen.

**"Ihre Daten in den Fokus rücken"**

Dateifreigaben, Datenbankserver und StorageGRID Systeme verbinden und auswählen, welche Datenressourcen gescannt werden sollen.

**"Scans in gutem Zustand halten"**

Der Systemstatus Ihres Deployments kann überwacht werden, um Probleme zu identifizieren, die den Scanvorgang unterbrechen könnten, und die Details zu erfassen, die zu deren Behebung erforderlich sind.

#### Storage optimieren und Ihre Daten analysieren

**"Speicherkapazität wiederherstellen"**

Kalte, veraltete und doppelte Daten in Ihren verbundenen Systemen werden anhand Ihrer konfigurierten Schwellenwerte identifiziert, und es wird angezeigt, welche Systeme und Dateneigentümer die höchste Konzentration dieser Daten aufweisen.

**"Kalte und veraltete Daten für Ihr Unternehmen definieren"**

Die Schwellenwerte, die festlegen, welche Daten als kalt oder veraltet eingestuft werden, sollten auf Ihre Aufbewahrungsrichtlinien abgestimmt sein.

**"Ermitteln, an wen Sie sich bezüglich der Daten wenden können"**

Im Dashboard lässt sich ermitteln, welche Dateneigentümer die höchsten Konzentrationen an kalten, veralteten oder doppelten Daten aufweisen. Anschließend lässt sich in der Untersuchungsansicht nach Eigentümer oder Gruppe filtern, um die Ergebnisse zu prüfen und festzustellen, wer zu kontaktieren ist.

**"Senkung von Kosten und Risiken"**

Verbundene Systeme können nach Zugriffszeit, Änderungsdatum, Erstellungsdatum, Dateigröße, Duplikatstatus und weiteren Kriterien gefiltert werden, um Dateien zu finden, die den Datenmanagementzielen Ihres Unternehmens entsprechen. Auf Grundlage der Ergebnisse können direkt Maßnahmen ergriffen oder die Kriterien als Richtlinie gespeichert werden.

**"Duplizierte Daten werden eliminiert"**

Dateien finden, die in Ihren verbundenen Systemen doppelt vorhanden sind. Nach dem Attribut „Duplikate“ oder nach dem Dateihash filtern, um Duplikatgruppen zu überprüfen und anschließend die doppelten Kopien zu bereinigen.

**"Zugriffsrisiken ermitteln"**

Verzeichnisse mit offenen Berechtigungen können so identifiziert werden, dass sie für eine Berechtigungsprüfung priorisiert werden können.

**"Untersuchung strukturierter Daten"**

Übergroße oder ungenutzte Datenbanktabellen auf Ihren verbundenen Datenbankservern finden.

#### Auf Basis der Daten handeln und diese im Laufe der Zeit überwachen

**"Speicherkosten senken"**

Die Datenlebenszyklusrichtlinien Ihres Unternehmens lassen sich durch Kopieren und Archivieren von Dateien auf NFS- oder SMB-Ziele, durch Kennzeichnen von Elementen zur Nachverfolgung oder durch dauerhaftes Löschen von Dateien gemäß Ihren Aufbewahrungsanforderungen durchsetzen.

**"Datenbedingungen kontinuierlich überwachen"**

Filterkriterien lassen sich als benannte Richtlinien speichern, um wiederkehrende Datenzustände im Zeitverlauf nachzuverfolgen, z. B. selten genutzte oder übergroße Dateien, und Benachrichtigungen zu erhalten, wenn sich die Anzahl der betroffenen Dateien ändert.

#### KI-Zugriff mit Governance

**"KI-Clients erhalten Governance-konformen Zugriff auf Ihre Metadaten"**

Sie können Claude Code, Claude Desktop, Cursor oder OpenCode über das Model Context Protocol (MCP) mit AI Data Engine verbinden. Sie können die Sammlungen aktivieren, die AI Clients durchsuchen können, und Microsoft Entra ID Scopes verwenden, um zu steuern, wer die einzelnen Sammlungen durchsuchen kann. AI Clients können Metadaten und Tag-Dateien durchsuchen.

#### Verwaltung

**"Zuweisung von Administrator- und Betrachterrollen"**

Sie können steuern, wer Daten untersuchen und Maßnahmen ergreifen darf, indem Sie Benutzern in Ihrer Organisation die Administrator- oder Viewer-Rolle für AI Data Engine zuweisen.

## Sicherung und Wiederherstellung

#### Kubernetes-Workloads-Erweiterungen

In dieser Version führt NetApp Backup and Recovery für Kubernetes-Workloads die folgenden Verbesserungen ein:

- **Trident Protect 26.10**: Diese Version enthält Trident Protect 26.10.
- **Unterstützung für die Treiber ontap-nas-economy und ontap-san-economy**: Sie können jetzt Persistent Volume Claims (PVCs) schützen, die vom NetApp Trident `ontap-nas-economy` Treiber

(Qtrees) und dem `ontap-san-economy` Treiber (LUNs) bereitgestellt werden. Wenn PVCs mithilfe von Economy-Treibern geschützt werden, wird das gesamte zugrunde liegende FlexVol bzw. die gesamte zugrunde liegende LUN geschützt. Einzelne PVCs können aus diesen Backups wiederhergestellt werden.

- **Kubernetes-fähige Benachrichtigungen**: Benachrichtigungen werden jetzt einmal pro Kubernetes-Applikation anstatt einmal pro Volume gesendet.
- **Unterstützung für Volume-Gruppen-Snapshots**: Beim Definieren einer Kubernetes Applikation können jetzt Volume-Gruppen erstellt werden. Volume-Gruppen ermöglichen es, mehrere Volumes gemeinsam als absturzkonsistenten Satz per Snapshot zu sichern und so die Datenkonsistenz über alle Volumes in der Gruppe hinweg zu gewährleisten.
- **Unterstützung für S3-kompatiblen Objektspeicher**: Sie können jetzt Kubernetes-Applikationsressourcen und -daten auf S3-kompatiblem Objektspeicher sichern, indem Sie Backup-Ziel-Anmeldedaten hinzufügen und Sicherungsrichtlinien konfigurieren.

Weitere Informationen zum Schutz von Kubernetes-Workloads finden Sie unter "Informationen zum Schutz von Kubernetes Workloads mit NetApp Backup and Recovery".

#### ONTAP Volumes Workloads-Verbesserungen

In dieser Version führt NetApp Backup and Recovery die folgenden Verbesserungen für ONTAP Volumes Workloads ein:

- **Schutzberichte**: NetApp Backup and Recovery unterstützt jetzt die Erstellung und das Herunterladen erweiterter Berichte für Workloads von ONTAP Volumes.
- **Backups beim Aufheben der Registrierung eines ONTAP Systems beibehalten**: Wenn Sie die Registrierung eines ONTAP Systems bei NetApp Backup and Recovery aufheben, können Sie nun festlegen, ob Sie die zuvor gesicherten Daten verwerfen oder für eine Wiederherstellung verfügbar halten möchten. Die Dokumentation zu NetApp Backup and Recovery enthält nun Anweisungen zur Verwendung der ONTAP CLI für die Wiederherstellung der beibehaltenen Daten nach Aufhebung der Registrierung des Systems.

Weitere Einzelheiten finden sich in "Backup and Recovery für ein System deregistrieren".

Weitere Informationen zum Schutz von ONTAP Volumes-Workloads finden Sie unter "Informationen zum ONTAP Volumeschutz mit NetApp Backup und Recovery".

#### Erweiterung der Oracle Database Workloads

In dieser Version bietet NetApp Backup and Recovery die folgende Erweiterung für Oracle Database Workloads:

**Wiederherstellung an einem alternativen Speicherort**: NetApp Backup and Recovery unterstützt jetzt die Wiederherstellung einer Oracle Datenbank an einem alternativen Speicherort (einem anderen registrierten Host).

Weitere Informationen zum Schutz von Oracle Database-Workloads finden Sie unter "Informationen zum Schutz von Oracle Database Workloads mit NetApp Backup and Recovery".

## Ransomware-Resilienz

#### Neuer manueller Workflow zur Erstellung eines Benutzeraktivitätsagenten

Ransomware Resilience bietet jetzt einen manuellen Workflow zur Erstellung des Benutzeraktivitätsagenten

und ermöglicht so eine präzisere Steuerung der Agentenerstellung auf Ihrer VM. Mit diesem neuen Workflow können Sie den Benutzeraktivitätsagenten direkt installieren und Proxy-Einstellungen konfigurieren, ohne VM-SSH-Schlüssel angeben zu müssen.

Weitere Informationen finden Sie unter "Erstellen Sie einen Benutzeraktivitätsagenten".

[[20-october-2026]]
== 20. Oktober 2026

## Ransomware-Resilienz

### Erweiterte Konfiguration der isolierten Wiederherstellungsumgebung

Ransomware Resilience bietet jetzt einen verbesserten Workflow zur Konfiguration isolierter Wiederherstellungsumgebungen. Der neue Workflow vereinfacht und präzisiert den Prozess zur Einrichtung einer solchen Umgebung für Cloud- oder On-Premises-Umgebungen.

Weitere Informationen finden sich unter "Eine isolierte Wiederherstellungsumgebung für eine saubere Wiederherstellung bereitstellen".

### Verbesserter Workflow zur Aktivierung der Benutzeraktivitätsüberwachung

Ransomware Resilience hat den Workflow für die Aktivierung der Benutzeraktivitätsüberwachung verbessert. Bisher testete Ransomware Resilience die Verbindung des Datensammlers jedes Mal, wenn Sie für eine Workload eine Ransomware-Schutzstrategie mit Benutzeraktivitätsüberwachung aktivierten. Mit diesem Update wird diese Prüfung nun übersprungen, wenn für die Storage VM ein Datensammler vorhanden ist und sich im Status "running" befindet, wodurch der Schutz Workflow beschleunigt wird.

Weitere Informationen finden Sie unter "Workloads schützen".

### Google Cloud NetApp Volumes Flex Service Level allgemein verfügbar

Die Unterstützung für das Flex Service Level von Google Cloud NetApp Volumes in Ransomware Resilience ist jetzt allgemein verfügbar (GA).

[[19-october-2026]]
== 19. Oktober 2026

## Sicherung und Wiederherstellung

### Erweiterung der Oracle Database Workloads

In dieser Version wird für Oracle Database-Workloads die folgende Verbesserung eingeführt:

**Unterstützung für Oracle Data Guard**: NetApp Backup and Recovery unterstützt jetzt die Verwendung von Schutzgruppen zum Schutz von primären und Standby-Datenbanken, die Oracle Data Guard für Hochverfügbarkeit verwenden.

Weitere Informationen zum Schutz von Oracle Database-Workloads finden Sie unter "Informationen zum Schutz von Oracle Database Workloads mit NetApp Backup and Recovery".

[[15-october-2026]]
== 15. Oktober 2026

## Konsoleneinrichtung und -verwaltung

### Console Agent 4.12.0

Die Version 4.12.0 unterstützt sowohl den Standardmodus als auch den eingeschränkten Modus.

Diese Version des Console-Agenten enthält Sicherheitsverbesserungen und Fehlerbehebungen.

### NetApp Console

Diese Version enthält Sicherheitsverbesserungen und Fehlerbehebungen.

## Digitaler Berater

### Unterstützung von E-Series und StorageGRID in Value Insights

Value Insights umfasst jetzt ONTAP, E-Series und StorageGRID Systeme in den Gesamtwerten für Systemstatus, Risiko, Sicherheitsrisiko und Lebenszyklus. Sie können das Dashboard nach Plattform filtern, um plattformspezifische Details anzuzeigen. Realisierte und prognostizierte Einsparungen sind weiterhin nur für ONTAP Systeme verfügbar.

"Wertvolle Einblicke im Digital Advisor entdecken".

[[14-october-2026]]
== 14. Oktober 2026

## Cloud Volumes ONTAP

### Cloud Volumes ONTAP 9.19.1 in Azure

Sie können jetzt die NetApp Console verwenden, um die Version mit allgemeiner Verfügbarkeit (GA) von Cloud Volumes ONTAP 9.19.1 in Azure einzusetzen und zu managen.

Die Console unterstützt Cloud Volumes ONTAP 9.19.1 in AWS und Google Cloud seit August 2026.

"Cloud Volumes ONTAP 9.19.1 Versionshinweise"

### Azure Verschlüsselung auf Hostebene für Cloud Volumes ONTAP

Ab Cloud Volumes ONTAP 9.19.1 GA ist die Azure-Verschlüsselung auf Hostebene standardmäßig für neue Azure-Einzelknoten- und Hochverfügbarkeits-Deployments (HA) aktiviert, die die Voraussetzungen erfüllen. Diese Funktion verschlüsselt Daten auf dem physischen Server, auf dem die VM ausgeführt wird, einschließlich des ephemeren Datenträgers und der zugehörigen Caches auf Hostebene, während die Daten auf den Host geschrieben und von ihm gelesen werden.

Vor dem Deployment von Cloud Volumes ONTAP in Azure muss Ihre Umgebung die folgenden Voraussetzungen erfüllen:

- Die `EncryptionAtHost`Funktion ist für Ihr Azure-Abonnement registriert. Weitere Informationen finden Sie unter "Microsoft-Dokumentation: Aktivierung der Verschlüsselung auf dem Host".
- Der von Ihnen ausgewählte VM-Instanz Typ unterstützt die Verschlüsselung auf dem Host in Ihrer Azure-Region. Weitere Informationen finden Sie unter "Microsoft Dokumentation: Unterstützte VM-Größen ermitteln".

Folgende Punkte sind zu beachten:

- Es ist keine zusätzliche Konfiguration erforderlich.
- Wenn diese Voraussetzungen nicht erfüllt sind, ist die Azure-Verschlüsselung auf Hostebene für Ihr Cloud Volumes ONTAP Deployment nicht aktiviert.
- Die Host-Verschlüsselung gilt nur für Azure, nicht für AWS oder Google Cloud.

Microsoft Dokumentation: "Die Ende-zu-Ende-Verschlüsselung lässt sich im Azure-Portal mithilfe der Verschlüsselung auf dem Host aktivieren"

#### Backend-Netzwerkverschlüsselung auf Cloud Volumes ONTAP Clustern in Azure und Google Cloud

Cloud Volumes ONTAP 9.19.1 und höher unterstützen die Netzwerkverschlüsselung des Backend-Clusters für HA-Konfigurationen in Azure und Google Cloud.

Die Aktivierung der Clusternetzwerkverschlüsselung kann sich auf die Cluster-Performance auswirken. Vor der Aktivierung dieser Funktion ist Vorsicht geboten, und es sollte überprüft werden, ob Ihre Umgebung den zusätzlichen Aufwand bewältigen kann.

"Backend-Netzwerkverschlüsselung auf Cloud Volumes ONTAP Clustern aktivieren"

#### Fähigkeit zur Reduzierung von Unterbrechungen während der geplanten Azure Wartung

Während geplanter Wartungsarbeiten kann Azure eine VM in einem Cloud Volumes ONTAP HA Paar kurzzeitig anhalten. ONTAP könnte die Pause als Knotenausfall interpretieren und Storage-Vorgänge auf den Partnerknoten verlagern, um sie nach dem Fortsetzen der VM wieder zurückzuverlagern (Takeover und Giveback). Dieser Vorgang kann aktive Clientverbindungen unterbrechen, selbst wenn kein Knotenausfall vorliegt.

Mit Cloud Volumes ONTAP 9.19.1 und höher lässt sich eine optionale Einstellung aktivieren, mit der das HA-Paar eine geplante Azure-Wartungssperre ohne automatisches Takeover und Giveback weiter durchlaufen kann.

Diese Funktion ist als öffentliche Vorschau mit Cloud Volumes ONTAP 9.19.1 verfügbar.

"Vermeidung von Unterbrechungen während der Azure-Wartung für Cloud Volumes ONTAP HA-Paare"

[[12-october-2026]]
== 12. Oktober 2026

## Sicherung und Wiederherstellung

#### Allgemeine NetApp Backup and Recovery-Verbesserung

In dieser Version führt NetApp Backup and Recovery die folgende Lizenzierungserweiterung für alle Workloads ein:

**Lizenzänderung**: Für Backups mit Disk-to-Disk- oder Disk-to-Disk-Fan-Out-Architekturen fallen keine Gebühren mehr an. Gebühren fallen nur für Backups auf Objekt-Storage an, einschließlich Backups mit 3-2-1- oder Disk-to-Object-Storage-Architekturen.

Weitere Informationen zur Lizenzierung finden Sie unter "Einrichtung der Lizenzierung für NetApp Backup and Recovery".

### Hyper-V-Workload-Verbesserungen

In dieser Version werden für Hyper-V-Workloads die folgenden Verbesserungen eingeführt:

- **NetApp MetroCluster support**: NetApp Backup and Recovery ermöglicht es Ihnen jetzt, Hyper-V-VMs zu schützen, die von NetApp MetroCluster gespiegelt werden.
- **Datenträgerübergreifender Schutz für SAN-VMs**: Bei CIFS- und SAN-Konfigurationen können Sie jetzt alle an jede VM in einer Schutzgruppe angeschlossenen Datenträger schützen. Dies umfasst Dateien, die über mehrere ONTAP Volumes oder ONTAP Storage Systeme verteilt sind (datenträgerübergreifende Datenträger), sowie Dateien, die auf einen einzelnen Speicherort beschränkt sind.

Weitere Informationen zum Schutz von Hyper-V-Workloads finden Sie unter "Informationen zum Schutz von Hyper-V Workloads mit NetApp Backup and Recovery".

### Erweiterung der Oracle Database Workloads

In dieser Version wird für Oracle Database-Workloads die folgende Verbesserung eingeführt:

**Automatische Archivprotokollverwaltung**: Bei Vorgängen zur Datenbankwiederherstellung und zum Klonen erkennt und mountet NetApp Backup and Recovery die erforderlichen Archivprotokolle automatisch und hängt sie nach Abschluss des Vorgangs wieder aus. Primäre, sekundäre und Objekt-Storage-Protokollquellen werden unterstützt.

Weitere Informationen zum Schutz von Oracle Database-Workloads finden Sie unter "Informationen zum Schutz von Oracle Database Workloads mit NetApp Backup and Recovery".

## Notfallwiederherstellung

### Optionale Startreihenfolge für Kubernetes Ressourcengruppen

NetApp Disaster Recovery unterstützt nun die optionale Festlegung der Startreihenfolge für Ressourcengruppen in einem Kubernetes-Replikationsplan, indem eine Prioritätsreihenfolge und eine optionale Verzögerungszeit für Ressourcen angegeben werden. Diese Option ermöglicht es, Ressourcen bei Bedarf gleichzeitig zu starten und den Start von Ressourcen zu verzögern, die von anderen abhängig sind, sodass Ihre Anwendungen ordnungsgemäß wieder online kommen.

Weitere Informationen finden Sie unter "Erstellen eines Replikationsplans".

### SnapLock Volume-Unterstützung

Disaster Recovery unterstützt jetzt SnapLock Volumes, sodass ein Failover manipulationssicherer Snapshots möglich ist. Bei einem Failback mit SnapLock Volumes muss die Option **Take snapshot now** verwendet werden, damit das Failback erfolgreich abgeschlossen wird.

Weitere Informationen sind in den Anweisungen für "Failover" und "Failback" enthalten.

### Vereinfachte Aktualisierungs- und Compliance-Ausführungen

Aktualisierungsläufe für vCenter, Replikationspläne und Compliance wurden zu einem einzigen Auftrag vereinfacht, um eine schnellere Ausführung zu ermöglichen. Um diese Änderung zu sehen, finden Sie Informationen dazu unter "Jobs überwachen".

### Kubernetes Compliance-Prüfungen

Disaster Recovery hat Compliance-Prüfungen hinzugefügt, um fehlende Arbeitsumgebungen für Kubernetes Workloads zu identifizieren. Diese Compliance-Prüfungen tragen dazu bei, den Systemstatus der Workloads sicherzustellen, damit die Integrität Ihrer Replikationspläne gewahrt bleibt.

## Keystone

Diese Keystone STaaS-Version enthält die folgenden Aktualisierungen im Keystone Dashboard in der NetApp Console.

### Generierung von Systemstatus Erkenntnissen für Keystone Abonnements

Sie können PowerPoint Berichte bei Bedarf herunterladen oder eine einmalige, wöchentliche, monatliche oder vierteljährliche Delivery unter **Storage > Keystone > Monitoring > Health reports** in der NetApp Console planen. Jeder Bericht kombiniert die Abonnementnutzung, den Systemstatus, Risiken und Schwachstellen über ausgewählte Abonnements hinweg und unterstützt Sie dabei, Probleme zu identifizieren und umsetzbare Erkenntnisse mit Empfängern zu teilen. Weitere Informationen enthält "Erstellung und Planung von Systemstatusberichten für Keystone Abonnements".

### Anzeige der ONTAP Cluster- und Aggregatkapazität

Sie können die physische Kapazität, die logische Kapazität und die Storage-Effizienz für ONTAP Cluster und deren Aggregate unter **Assets > Cluster und Aggregate** einsehen. Dies ist nur für Keystone STaaS Abonnements verfügbar, die auf Grundlage der physischen Kapazität abgerechnet werden. Weitere Informationen sind unter "Assets in Ihren Keystone-Abonnements anzeigen" und "Assets anzeigen, die mit einem Keystone-Abonnement verknüpft sind" verfügbar.

[[30-september-2026]]
== 30. September 2026

## Workload Factory

### Erstveröffentlichung von Oracle Cloud Infrastructure NetApp Storage Service für Workload Factory

Die erste Version des OCI NetApp Storage Service (OCI NSS) für Workload Factory bietet Onboarding, Systemerkennung, Anmeldeinformationsverwaltung sowie die Erstellung und Zuordnung von Links. Für die Beantragung des Zugriffs auf OCI NSS ist ein Support-Ticket bei Oracle erforderlich.

### Workload Factory Dokumentation für NetApp Console Benutzer

Detaillierte Dokumentation für Workload Factory finden Sie in der NetApp Console, einschließlich Anleitungen für Onboarding, Systemerkennung, Management von Anmeldeinformationen sowie Erstellung und Zuordnung von Links.

"Workload Factory Dokumentation für NetApp Console"

[[28-september-2026]]
== 28. September 2026

## Sicherung und Wiederherstellung

### Allgemeine NetApp Backup and Recovery-Verbesserung

In dieser Version führen KVM-, Hyper-V- und VMware-Workloads die folgende Verbesserung ein:

**Unterstützung für rollenbasierte Zugriffskontrolle (RBAC) in der Console**: Die Hyper-V-, KVM- und VMware-Workloads unterstützen jetzt das NetApp Console Framework für RBAC, sodass Sie den Zugriff auf einzelne Hyper-V-, KVM- oder VMware-Hosts verwalten können.

"Weitere Informationen zur Verwendung von RBAC in NetApp Backup and Recovery".

### ONTAP Volumes Workloads-Verbesserungen

In dieser Version führt ONTAP Volumes Workloads die folgenden Vorschauverbesserungen ein:

- **Cloud Volumes ONTAP Azure Entra ID-Unterstützung**: Microsoft Entra ID Authentifizierung kann jetzt für Azure Storage-Bucket-Konfigurationen verwendet werden, wenn für die Azure Authentifizierung nicht der Zugriffsschlüssel des Storage-Kontos verwendet werden soll. Diese Option steht für Cloud Volumes ONTAP in Azure-Systemen mit ONTAP 9.16.1 oder höher zur Verfügung.
- **Benutzerdefinierte Datumsbereichsfilterung im Job Monitor**: Sie können jetzt im Job Monitor nach Jobs aus den vergangenen 90 Tagen suchen, indem Sie in einem Kalender ein benutzerdefiniertes Start- und Enddatum auswählen.

Weitere Informationen zum Schutz von ONTAP Volumes-Workloads finden Sie unter "Informationen zum ONTAP Volumeschutz mit NetApp Backup und Recovery".

### Erweiterung für VMware Workloads

In dieser Version führt VMware Workloads die folgende Verbesserung ein:

**Google Cloud NetApp Volumes Flex Unified support**: NetApp Backup and Recovery für VMware Workloads unterstützt jetzt die Flex Unified Service Level für Google Cloud NetApp Volumes. Flex Unified wird nur im ONTAP Modus unterstützt.

Weitere Informationen zum Schutz von VMware-Workloads finden Sie unter "VMware-Workloads mit NetApp Backup and Recovery schützen".

[[25-september-2026]]
== 25. September 2026

## Digitaler Berater

### Inhaltsaktualisierung für das Value Insights Dashboard

Eine Aktualisierung der Dokumentation für das Value Insights Dashboard wurde veröffentlicht.

Weitere Informationen zu "Verwendung des Value Insights Dashboard in Digital Advisor".

### Hinweis zur Einstellung von Config Drift

Die Funktion „Konfigurationsabweichung“ wurde eingestellt und ist seit September 2026 in Digital Advisor nicht mehr verfügbar.

Bei Fragen oder zum Teilen von Feedback wenden Sie sich an das Active IQ Team.

[[21-september-2026]]
== 21. September 2026

## Sicherung und Wiederherstellung

### ONTAP Volumes Workloads-Verbesserungen

In dieser Version führt ONTAP Volumes Workloads die folgenden Vorschauverbesserungen ein:

- **Verbesserte Unterstützung für Dark Sites**: NetApp Backup and Recovery for dark sites bietet jetzt dieselben ONTAP Volumes Datenschutzfunktionen wie NetApp Backup and Recovery. Diese Verbesserung umfasst aktualisierte Backup-, Wiederherstellungs- und Job-Management-Services sowie eine neue Metadaten-Datenbank. Während eines Upgrades bleiben vorhandene Datenbankdaten erhalten und werden automatisch migriert. Nach dem Upgrade ist eine Überprüfung der Audit-Protokolle erforderlich, um sicherzustellen, dass die Migration erfolgreich abgeschlossen wurde. NetApp Backup and Recovery for dark sites unterstützt nur ONTAP Volumes Workloads.
- **Abbrechen von Volume-Wiederherstellungsaufträgen**: Laufende ONTAP Volumes-Wiederherstellungsaufträge können jetzt auf der Seite zur Auftragsüberwachung abgebrochen werden, was die Verwaltung lang laufender oder langsam ausgeführter Aufträge vereinfacht.
- **Verbesserte Statusberichterstattung zur Volume-Indizierung**: Das ONTAP Volumes Dashboard meldet den Indizierungsstatus jetzt genauer, indem der `Not Applicable`Status für Volumes und Snapshot-Kopien eingeführt wird, die nicht für die Indizierung geeignet sind. Der `Not Indexed`Status ist jetzt Volumes vorbehalten, die auf die Indizierung warten, und die Volume-Details zeigen jetzt den Indizierungsstatus pro Snapshot mit einem Hovertext an, der erklärt, warum ein Volume oder eine Snapshot-Kopie nicht indiziert wird.
- **NetApp AFX Unterstützung**: Sie können jetzt Volumes schützen, die auf 2- und 4-Knoten-NetApp AFX Clustern gehostet werden.

Weitere Informationen zum Schutz von ONTAP Volumes-Workloads finden Sie unter "Informationen zum ONTAP Volumeschutz mit NetApp Backup und Recovery".

### Kubernetes-Workloads-Erweiterungen

In dieser Version werden für Kubernetes-Workloads die folgenden Verbesserungen eingeführt:

- **Trident Protect 26.09**: Diese Version enthält Trident Protect 26.09.
- **Cluster- und Namespace-granulare rollenbasierte Zugriffskontrolle (RBAC)**: Bei der Kubernetes Cluster-Erkennung kann der Zugriff auf Ressourcen durch die Auswahl eines Projekts oder Ordners gesteuert werden, das bzw. der dem neuen Cluster zugeordnet wird. Außerdem können bestimmte Namespaces für die Zugriffskontrolle registriert werden. Dadurch wird eine granularere Zugriffskontrolle entweder auf Cluster- oder Namespace-Ebene ermöglicht.
- **Dateien und Ordner wiederherstellen**: Es ist jetzt möglich, bestimmte Dateien und Ordner aus Kubernetes VM-basierten Anwendungssicherungen wiederherzustellen oder herunterzuladen.

Weitere Informationen zum Schutz von Kubernetes-Workloads finden Sie unter "Informationen zum Schutz von Kubernetes Workloads mit NetApp Backup and Recovery".

## Cloud Volumes ONTAP

### Unterstützung für kapazitätsbasierte Lizenzen in Private-Mode-Bereitstellungen

Cloud Volumes ONTAP Systeme können jetzt im privaten Modus mit kapazitätsbasierten Lizenzen in AWS, Azure und Google Cloud bereitgestellt werden.

NetApp unterstützt nur das Essentials Paket für kapazitätsbasierte Lizenzierung im privaten Modus. Ein kapazitätsbasiertes Bring-Your-Own License (BYOL) Essentials Paket kann von NetApp erworben und während der Bereitstellung dem System zugewiesen werden. Die ersten 500 GiB verbrauchter Kapazität werden nicht auf Ihre Lizenzgebühren angerechnet. Zusätzliche Pakete können erworben werden, wenn der Bedarf an Arbeitslasten steigt.

NetApp empfiehlt die kapazitätsbasierte Lizenzierung für alle Cloud Volumes ONTAP Bereitstellungen im privaten Modus. Wenn bereits Bereitstellungen im privaten Modus mit knotenbasierten Lizenzen vorhanden sind, ist eine Umstellung auf kapazitätsbasierte Lizenzierung durch den Erwerb eines Essentials-Pakets von NetApp möglich. Diese neue Bereitstellungsfunktion, kombiniert mit der Umstellungsoption, unterstützt den Plan von NetApp, schrittweise von knotenbasierter auf kapazitätsbasierte Lizenzierung überzugehen.

**Verwandte Links**

- "Cloud Volumes ONTAP Lizenzierung"
- "Informationen zu Cloud Volumes ONTAP BYOL"
- "Ende der Verfügbarkeit knotenbasierter Lizenzen"
- "Knotenbasierte Lizenzen für Cloud Volumes ONTAP verwalten"

[[17-september-2026]]
== 17. September 2026

## Konsoleneinrichtung und -verwaltung

### Veröffentlichung im privaten Modus (4.10.0)

Eine neue Version des privaten Modus steht jetzt zum Download aus dem "NetApp Support Site" bereit.

Die Version 4.10.0 enthält Aktualisierungen der folgenden NetApp Console-Komponenten und -Dienste.

| Komponente oder Service | In dieser Version enthalten | Änderungen seit der vorherigen privaten Modus-Version |
|---|---|---|
| Konsolenagent | 4.10.0 | Gehen Sie zu "Was ist neu auf der NetApp Console-Seite" und informieren Sie sich über die Änderungen in Version 4.10.0. |
| NetApp Backup and Recovery | 5.6.2 (31. August 2026) | Gehe zu "Was ist neu auf der Seite NetApp Backup and Recovery". |
| NetApp Data Classification | 1.546.0 (10. August 2026) | Gehe zu "Was ist neu auf der Seite NetApp Klassifizierung". |

### Private mode 4.10.0 unterstützt Red Hat Enterprise Linux (RHEL) 9.6

Private mode kann jetzt auf Red Hat Enterprise Linux (RHEL) 9.6 installiert und ausgeführt werden und bietet Benutzern das neueste unterstützte Betriebssystem für mehr Sicherheit und bessere Leistung."Informationen zu den Host-Anforderungen für den privaten Modus"

[[16-september-2026]]
== 16. September 2026

## Konsoleneinrichtung und -verwaltung

### Console Agent 4.11.0

Die Version 4.11.0 unterstützt sowohl den Standardmodus als auch den eingeschränkten Modus.

Diese Version des Console-Agenten enthält Sicherheitsverbesserungen und Fehlerbehebungen.

### NetApp Console

#### Vereinfachter Agentenbereitstellungsprozess für Cloud Volumes ONTAP Abonnenten im AWS Marketplace

Wenn Sie ein neues Abonnement für eine "eigenständiges Cloud Volumes ONTAP Abonnement im AWS Marketplace" haben, vereinfacht die NetApp Console jetzt die Agentenbereitstellung. AWS-Rollen, -Richtlinien und -Anmeldeinformationen lassen sich mit weniger Schritten konfigurieren, Standardwerte werden automatisch auf einer einzigen Seite verwendet, und der Einrichtungsprozess erfolgt schneller.

## Sicherung und Wiederherstellung

### Allgemeine NetApp Backup and Recovery-Verbesserung

In dieser Version führen KVM-, Hyper-V- und VMware-Workloads die folgende Verbesserung ein:

**Auswahl der Anmeldeinformationen bei der VM-Host-Erkennung**: Bei der Erkennung eines KVM-, Hyper-V- oder VMware-Hosts können jetzt Anmeldeinformationen verwendet werden, die bereits zu Backup and Recovery hinzugefügt wurden.

### Hyper-V Workload-Verbesserung

In dieser Version wird für Hyper-V Workloads die folgende Verbesserung eingeführt:

**Datenträgerübergreifender Schutz für VMs**: Bei CIFS-Konfigurationen unterstützt NetApp Backup and Recovery jetzt den Schutz aller an jede VM in einer Datensicherungsstrategie angeschlossenen Datenträger. Dies umfasst Dateien, die über mehrere ONTAP Volumes oder ONTAP Speichersysteme verteilt sind (datenträgerübergreifende Datenträger), sowie Dateien, die sich an einem einzigen Speicherort befinden.

Weitere Informationen zum Schutz von Hyper-V-Workloads finden Sie unter "Informationen zum Schutz von Hyper-V Workloads mit NetApp Backup and Recovery".

### ONTAP Volumes Workloads-Verbesserung

In dieser Version wird für ONTAP Volumes Workloads die folgende Vorschau-Verbesserung eingeführt:

**Täglicher Bericht zum Datentransfer bei Backups**: NetApp Backup and Recovery für Volumes enthält jetzt unter der Registerkarte „Berichte“ einen täglichen Bericht zum Datentransfer bei Backups, der Einblick in die täglichen Backup- und Replikations-Datentransfers in Ihrer Umgebung bietet. Der Bericht kann für das gesamte Konto oder für ausgewählte Speichersysteme erstellt, nach Datumsbereich und Datensicherungsstrategie gefiltert und als CSV heruntergeladen werden.

Weitere Informationen zum Schutz von ONTAP Volumes-Workloads finden Sie unter "Informationen zum ONTAP Volumeschutz mit NetApp Backup und Recovery".

## Datenklassifizierung

### Allgemeine Verbesserungen

Diese Version der Datenklassifizierung beinhaltet Sicherheitsverbesserungen und Leistungsverbesserungen.

## Notfallwiederherstellung

### Kubernetes-Unterstützung in NetApp Disaster Recovery ist jetzt allgemein verfügbar (GA)

Die Unterstützung für Kubernetes-basierte Workloads in NetApp Disaster Recovery ist jetzt allgemein verfügbar (GA). Mit Unterstützung für Kubernetes-basierte Workloads können Anwendungen geschützt werden, die auf Kubernetes-Clustern ausgeführt werden, einschließlich OpenShift Virtualisierungsumgebungen. Disaster Recovery unterstützt jede von Trident Protect aktuell unterstützte Kubernetes-Version, was eine nahtlose Integration und robuste Disaster Recovery-Funktionen für containerisierte Anwendungen gewährleistet.

Um mit dem Schutz von Kubernetes-basierten Workloads zu beginnen, siehe "Kubernetes-Anforderungen für NetApp Disaster Recovery".

### Ressourcentransformationen

Disaster Recovery unterstützt nun Ressourcentransformationen, sodass jeder Aspekt einer Arbeitslast während eines Failovers angepasst werden kann. Diese Funktion bietet Flexibilität, um Arbeitslasten während eines Notfallwiederherstellungsereignisses an unterschiedliche Umgebungen und Konfigurationen anzupassen.

Ressourcentransformationen werden beim Erstellen eines Replikationsplans angewendet. Ressourcentransformationen können auf der neuen Einstellungsseite erstellt, bearbeitet und gelöscht werden. Weitere Informationen finden sich unter "Ressourcentransformationen verwalten".

### Skriptausführung

Sie können nun benutzerdefinierte Skripte in den Failover-Workflow einbinden, um das Anhalten und die Wiederaufnahme von Anwendungen zu koordinieren. Diese Funktion trägt dazu bei, dass Anwendungen vor der Replikation eines Snapshots ordnungsgemäß vorbereitet und anschließend angemessen wiederhergestellt werden, sodass der Betrieb nach einem Failover nahtlos fortgesetzt werden kann.

Informationen zum Einfügen eines benutzerdefinierten Skripts sind unter "Einen Replikationsplan erstellen" zu finden.

### Neue Workloads-Seite

NetApp Disaster Recovery hat der Benutzeroberfläche eine Workloads-Seite hinzugefügt, die einen umfassenden Überblick über alle erkannten Workloads und deren Schutzstatus bietet. Die Workloads-Seite ermöglicht eine effektivere Überwachung und Verwaltung Ihrer Workloads.

Weitere Informationen finden sich unter "Überprüfen des Gesundheits- und Schutzstatus in NetApp Disaster Recovery".

### Einstellungsseite

Disaster Recovery bietet jetzt eine Einstellungsseite zur zentralen Verwaltung von Ressourcentransformationsvorlagen und AppVaults. Diese Seite stellt eine einheitliche Schnittstelle zur

Konfiguration und Verwaltung dieser wichtigen Komponenten Ihrer Disaster-Recovery-Pläne bereit. Weitere Informationen zu den Optionen auf der Einstellungsseite finden sich unter "Ressourcentransformationen verwalten" und "Verwaltung von AppVaults".

#### Allgemeine Verbesserungen

NetApp Disaster Recovery hat erweiterte Validierungen auf der Seite zur Erstellung von Replikationsplänen eingeführt, um eine reibungslosere und fehlerfreie Benutzererfahrung sicherzustellen.

Durch die Notfallwiederherstellung wurde auch die Widerstandsfähigkeit des Dienstes erhöht, um zeitweilige Anforderungs-Timeouts zu tolerieren, wodurch die Gesamtleistung und Zuverlässigkeit der Benutzeroberfläche verbessert wurde.

## Ransomware-Resilienz

#### Unterstützung für eine saubere Wiederherstellung bei verdächtigem Benutzerverhalten und benutzerbasierten Verschlüsselungsangriffen

Saubere Wiederherstellungen sind nun nach verdächtigem Nutzerverhalten und benutzerbasierten Verschlüsselungsangriffen möglich. Diese Erweiterung ergänzt die bestehende Unterstützung für (entropiebasierte) Verschlüsselungsangriffe. Diese erweiterte Funktion ermöglicht die Nutzung des geführten Ansatzes der sauberen Wiederherstellung, wobei optimale Wiederherstellungspunkte identifiziert werden, um Datenverlust zu minimieren und die Wiederherstellung zu beschleunigen.

Weitere Informationen finden sich unter "Eine isolierte Wiederherstellungsumgebung für eine saubere Wiederherstellung bereitstellen".

[[14-september-2026]]
== 14. September 2026

## Digitaler Berater

#### Hinweis zur Einstellung der virtuellen Maschine

Die Funktion „Virtuelle Maschine“ wird im Digital Advisor im Oktober 2026 eingestellt.

Bei Fragen oder zum Teilen von Feedback wenden Sie sich an das Active IQ Team.

[[02-september-2026]]
== 02. September 2026

## Cloud Volumes ONTAP

#### Cloud Volumes ONTAP Unterstützung in Azure Secret und Top Secret Regionen (private Vorschau)

Cloud Volumes ONTAP unterstützt jetzt die Bereitstellung in Azure Government Secret und Top Secret Regionen in privater Vorschau. Diese Funktion erweitert Cloud Volumes ONTAP auf die klassifizierten Azure-Umgebungen von Microsoft, wodurch Regierungs- und Verteidigungskunden ONTAP für Datenmanagement, Datenschutz und Notfallwiederherstellung zur Unterstützung von Workloads für die nationale Sicherheit nutzen können. Für eine Teilnahme steht das NetApp Accounts-Team zur Verfügung.

Weitere Informationen sind in der Azure-Dokumentation zu finden:

- "Cloud für Missionen der US-Regierung"
- "Azure Government Secret"
- "Azure Government Top Secret"

[[01-september-2026]]
== 01. September 2026

## StorageGRID

### Unterstützung für StorageGRID 12.1

Das StorageGRID 12.1 System kann jetzt über die NetApp Console verwaltet werden.

"Informationen zur Administration von StorageGRID mithilfe der erweiterten Ansicht in der NetApp Console".

[[31-august-2026]]
== 31. August 2026

## Notfallwiederherstellung

### Verbesserte SnapMirror Snapshot-Verwaltung

Sie können nun ein Failover mithilfe des neuesten Snapshots auslösen, was die bevorzugte Methode ist, wenn kein neuer Snapshot erstellt wird.

Bei Auswahl einer bestimmten Snapshot-Baseline werden SnapMirror Transfer-Snapshots standardmäßig ausgeblendet. Dies liegt daran, dass sie während eines Failovers gelöscht werden können, was dazu führt, dass die Workload nach dem Failover aufgrund des Fehlers „Kein gemeinsamer Snapshot gefunden“ nicht wiederhergestellt werden kann. Diese Snapshots können weiterhin verwendet werden, allerdings ist eine zusätzliche Bestätigungsabfrage erforderlich, um das Risiko zu bestätigen.

Weitere Informationen finden sich unter "Failover zu einem entfernten Standort".

### Weitere Verbesserungen

- Kleinere Verbesserungen wurden vorgenommen, um die Ausfallsicherheit des Test Failover-Workflows zu erhöhen.
- Ein Validierungsfehler beim Hinzufügen eines Skripts wurde behoben.

[[25-august-2026]]
== 25. August 2026

## Ransomware-Resilienz

### SIEM-Ereignisübermittlung über den Console Agent

Ransomware Resilience unterstützt jetzt neben der bestehenden Option, Ereignisse über die NetApp Console zu übermitteln, auch die Bereitstellung von SIEM-Ereignissen über den Console-Agenten.

Wenn Sie SIEM-Ereignisse über den Console Agent übermitteln, kann die SIEM-Ereignisübermittlung innerhalb Ihrer Netzwerkgrenze bleiben. Dies vereinfacht die Bereitstellung für lokale Umgebungen mit strikten IP-Adress-Positivlisten und kann besser mit bestehenden Sicherheitskontrollen abgestimmt werden. Für die

Nutzung dieser Option muss sichergestellt sein, dass der Console Agent Ihren SIEM-Endpunkt am erforderlichen Port über alle Firewall- oder Proxy-Kontrollen hinweg auflösen und erreichen kann.

Weitere Informationen finden sich unter "Konfiguration eines SIEM-Systems".

## Cloud Volumes ONTAP

### Unterstützung für die Regionen Austria East und Belgium Central in Azure

Cloud Volumes ONTAP 9.12.1 GA und höher kann jetzt in den Azure-Regionen Austria East (austriaeast) und Belgium Central (belgiumcentral) bereitgestellt werden. Die folgenden Bereitstellungstypen werden unterstützt:

- Einzelknoten
- Hochverfügbarkeit in einer einzigen Verfügbarkeitszone unter Verwendung von lokal redundantem Storage (LRS)
- Hochverfügbarkeit in mehreren Verfügbarkeitszonen mittels zonenredundantem Speicher (ZRS)

Eine Liste aller unterstützten Regionen ist unter "Globale Regionskarte unter Azure" zu finden.

[[20-august-2026]]
== 20. August 2026

## Digitaler Berater

### Value Insights – eine Einführung

Die Funktion „Value Insights“ fasst Informationen zu Systemzustand, Einsparungen, Stabilität und Sicherheit von ONTAP Systemen zusammen. Diese Informationen ermöglichen eine Verbesserung von Systemzustand und Leistung durch eine kontinuierliche, datengestützte Betrachtung Ihrer ONTAP Umgebung.

Value Insights ist nur für ONTAP Systeme verfügbar.

Weitere Informationen zu "Value Insights".

[[17-august-2026]]
== 17. August 2026

## Sicherung und Wiederherstellung

### Hyper-V-Workload-Verbesserungen

In dieser Version wird für Hyper-V Workloads die folgende Verbesserung eingeführt:

**Objektspeichersicherung an alternativem Speicherort wiederherstellen**: Es ist jetzt möglich, Hyper-V-VMs, Dateien und Ordner aus dem Objektspeicher an einem alternativen Speicherort wiederherzustellen.

Weitere Informationen zum Schutz von Hyper-V-Workloads finden Sie unter "Informationen zum Schutz von Hyper-V Workloads mit NetApp Backup and Recovery".

### Kubernetes-Workloads-Erweiterungen

In dieser Version werden für Kubernetes-Workloads die folgenden Verbesserungen eingeführt:

- **Trident Protect 26.08**: Diese Version enthält Trident Protect 26.08.
- **Backup-Wiederholungsversuche**: Backup-Wiederholungsversuche können jetzt aktiviert und die Anzahl der Wiederholungsversuche sowie die Intervalle zwischen den Wiederholungsversuchen als erweiterte Einstellungen in Kubernetes-Schutzrichtlinien konfiguriert werden.
- **Teilweise erfolgreiche Sicherung**: Es besteht jetzt die Möglichkeit, in den Kubernetes-Schutzrichtlinien erweiterte Einstellungen zu konfigurieren, damit die Sicherung auch bei Ausfall einzelner Ressourcen fortgesetzt wird und Sicherungsaufträge als teilweise erfolgreich abgeschlossen werden können. Dadurch ist die Wiederherstellung gesicherter Ressourcen möglich, selbst wenn während des Sicherungsvorgangs einige Ressourcen ausfallen.
- **Absturzkonsistente und VM-konsistente Backups**: Der Backup and Recovery Dienst für NetApp Console unterstützt jetzt die Konfiguration von Schutzrichtlinien, die absturzkonsistente oder VM-konsistente Backups oder Snapshots erstellen. Es besteht zudem die Möglichkeit, anzupassen, wie VM-Einfrierungen während des Schutzvorgangs durchgeführt werden.
- **Wiederverbindung des Kubernetes-Clusters bei Änderung der Console-Agent-IP-Adresse**: Der Backup- und Wiederherstellungsdienst für NetApp Console ermöglicht jetzt die erneute Verbindung eines Clusters mit seinem Console-Agenten, wenn sich die IP-Adresse des Agenten ändert.
- **Cluster auf neuen Console Agent migrieren**: Der Backup and Recovery Dienst für NetApp Console ermöglicht jetzt die Migration eines Clusters auf einen neuen Console Agent, falls der ursprüngliche Agent ausfällt oder gelöscht wird, wodurch ein unterbrechungsfreier Anwendungsschutz sichergestellt wird.

Weitere Informationen zum Schutz von Kubernetes-Workloads finden Sie unter "Informationen zum Schutz von Kubernetes Workloads mit NetApp Backup and Recovery".

#### Erweiterung der Oracle Database Workloads

In dieser Version werden die folgenden Verbesserungen für Oracle Database workloads eingeführt:

- **Wiederherstellung von Pluggable Databases (PDBs)**: Es ist jetzt möglich, einzelne Pluggable Databases (PDBs) und PDB-Tablespaces wiederherzustellen, einschließlich zeitpunktgenauer Wiederherstellung.
- **Pluggable Database (PDB) Klonen**: Es ist jetzt möglich, eine einzelne PDB in eine bestehende Ziel-Containerdatenbank (CDB) zu klonen und optional PDBs auszuschließen, wenn eine komplette Containerdatenbank geklont wird.

Weitere Informationen zum Schutz von Oracle Database-Workloads finden Sie unter "Informationen zum Schutz von Oracle Database Workloads mit NetApp Backup and Recovery".

[[13-august-2026]]
== 13. August 2026

## Konsoleneinrichtung und -verwaltung

#### Console Agent 4.10.0

Die Version 4.10.0 unterstützt sowohl den Standardmodus als auch den eingeschränkten Modus.

Diese Version des Console-Agenten enthält Sicherheitsverbesserungen und Fehlerbehebungen.

##### Verbesserte Reaktionsfähigkeit und Zuverlässigkeit des Cloud Mediators

Der Dienst verarbeitet nun Cluster-Statusaktualisierungen effizienter, wodurch zeitweilige Timeouts und Ausfallzeiten reduziert und die automatische ungeplante Failover-Mediation für SMaS Beziehungen gestärkt

wird.

### NetApp Console

NetApp Console 4.10.0 Administration umfasst Sicherheits- und Fehlerbehebungen.

## Ransomware-Resilienz

### Einen Datensammler löschen

Ransomware Resilience unterstützt nun das Löschen eines Datensammlers. Der Datensammler wird automatisch erstellt, wenn die Benutzeraktivitätserkennung für Workloads aktiviert wird; falls der Datensammler veraltet ist, kann er nun manuell gelöscht werden.

Weitere Informationen finden sich unter "Einen Datensammler löschen".

[[12-august-2026]]
== 12. August 2026

## Digitaler Berater

### Hinweis zur Einstellung von Config Drift

Die Funktion „Konfigurationsabweichung“ wird im Digital Advisor im September 2026 eingestellt.

Bei Fragen oder zum Teilen von Feedback wenden Sie sich an das Active IQ Team.

[[10-august-2026]]
== 10. August 2026

## Sicherung und Wiederherstellung

### Allgemeine NetApp Backup and Recovery-Verbesserungen

- **Unterstützung für die lokale Bereitstellung der NetApp Console**: Diese Version von NetApp Backup and Recovery unterstützt die lokale Bereitstellung der NetApp Console im Vorschaustatus.
- **90 Tage Aufbewahrung von Aufträgen**: Backup and Recovery speichert Auftragsinformationen jetzt 90 Tage lang im Job Monitor.

### VMware-Workload-Verbesserungen

In dieser Version führt VMware workloads die folgenden Verbesserungen ein:

- **Unterstützung für die Wiederherstellung an einem alternativen Speicherort für SAN-VMs**: Es ist jetzt möglich, SAN-basierte VM-Backups an einem alternativen Speicherort wiederherzustellen.
- **Unterstützung für das Löschen mehrerer Backups**: Es ist jetzt möglich, mehrere Backups gleichzeitig zu löschen.

Weitere Informationen zum Schutz von VMware-Workloads finden Sie unter "Überblick über den Schutz von VMware-Workloads".

### Kubernetes-Workloads-Erweiterungen

In dieser Version werden für Kubernetes-Workloads die folgenden Verbesserungen eingeführt:

- **Vorschauunterstützung für isolierte Ressourcen**: Wenn NetApp Backup and Recovery in der lokalen NetApp Console-Bereitstellung ausgeführt wird, können isolierte Kubernetes-Ressourcen erkannt, geschützt und wiederhergestellt werden. Diese Funktion befindet sich in dieser Version in der Vorschau.

Weitere Informationen zum Schutz von Kubernetes-Workloads finden Sie unter "Übersicht zum Schutz von Kubernetes-Workloads".

### ONTAP Volumes Workloads-Verbesserungen

In dieser Version wurden für ONTAP Volumes Workloads die folgenden Verbesserungen eingeführt:

- **Wiederherstellungsaufträge gegenüber Backups priorisieren**: Es ist jetzt möglich, Wiederherstellungsaufträge gegenüber Backup-Aufträgen zu priorisieren, wenn Volumes, Dateien oder Ordner wiederhergestellt werden.
- **ONTAP Systeme und Volumes ohne Backup and Recovery Aktivierung entdecken**: Es ist jetzt möglich, Systeme und Volumes zu entdecken, ohne Backup and Recovery zu aktivieren.

Weitere Informationen zum Schutz von ONTAP Volumes-Workloads finden Sie unter "Überblick über den Schutz von ONTAP Volumes Workloads".

## Datenklassifizierung

### Registerkarte „Active scans“ zur Verbesserung der Scanverwaltung

Data Classification bietet jetzt im Konfigurationsmenü die Registerkarte **Aktive Scans**, die eine verbesserte Benutzererfahrung für die Verwaltung von Scans ermöglicht. Die Registerkarte **Aktive Scans** bietet eine Übersicht über alle Volumes, die Sie für das Scannen aktiviert haben, mit vertrauten Filtern zum Sortieren Ihrer Ressourcen. Die Registerkarte bietet außerdem einen zentralen Ort, um Scans zu priorisieren, Scans zu pausieren und Fehler zu überprüfen.

Weitere Informationen finden sich unter "Scans verwalten".

## Notfallwiederherstellung

### Verbessertes Dashboard

Das NetApp Disaster Recovery Dashboard wurde überarbeitet und bietet nun eine verbesserte Benutzeroberfläche mit einem umfassenden Überblick über Ihre gesamte NetApp Disaster Recovery Umgebung. Das neue Dashboard umfasst:

- **Einheitliche Workload-Transparenz** – Überwachung von VMware- und Kubernetes-Workloads sowie des Zustands der zugrunde liegenden Infrastruktur über eine zentrale Benutzeroberfläche.
- **Proaktive Problemerkennung** – Das Dashboard hebt jetzt automatisch Umweltprobleme hervor, wodurch eine schnellere Diagnose und kürzere Lösungszeiten ermöglicht werden.
- **Kapazitätsauslastung** – Kapazitätskennzahlen werden jetzt direkt im Dashboard angezeigt, was das Verständnis des Ressourcenverbrauchs erleichtert.

Weitere Informationen sind unter "Den Zustand Ihrer NetApp Disaster Recovery Pläne im Dashboard anzeigen" zu finden.

### Verbesserte Berichte

Die Berichtsfunktionen wurden erweitert, um einen tieferen Einblick in die NetApp Disaster Recovery-Aktivitäten in Ihrer gesamten Umgebung zu bieten:

- Berichte können auf VMware Workloads, Kubernetes Workloads oder beides bezogen werden, was die Flexibilität bietet, die Berichte auf die jeweilige Zielgruppe abzustimmen.
- Jeder Bericht liefert eine vollständige Aktivitätsübersicht für einen bestimmten Zeitraum und gewährleistet so volle Transparenz über die Ereignisse in Ihrer NetApp Disaster Recovery Umgebung.

Weitere Informationen sind unter "Berichte zur NetApp Disaster Recovery erstellen" zu finden.

### Protokollierung von Benutzeraufträgen

NetApp Disaster Recovery hat die Nachvollziehbarkeit und Prüfbarkeit von Jobs durch die benutzerbezogene Job-Protokollierung verbessert. Jeder ausgeführte Job zeichnet nun den Benutzer auf, der ihn initiiert hat, wodurch ein klarer Audit-Trail für Compliance- und Fehlerbehebungszwecke entsteht. Jobs, die automatisch von NetApp Disaster Recovery ausgelöst werden, sind als „system“ gekennzeichnet, sodass sich benutzerinitiierte und dienstinitiierte Aktivitäten leicht unterscheiden lassen.

Weitere Informationen sind unter "Überwachung von NetApp Disaster Recovery-Aufträgen" zu finden.

### Leistungs- und Ressourcenoptimierung

Es wurden diverse Verbesserungen im Hintergrund vorgenommen, um den Gesamtressourcenverbrauch des Systems zu reduzieren und die Leistung bei Disaster Recovery-Operationen zu steigern.

# Index der Versionshinweise für NetApp Console

Sehen Sie sich die vollständigen Versionshinweise zu den NetApp Console Funktionen und NetApp -Datendiensten an.

## Verwaltung

- "Einrichtung und Administration"
- "Warnungen"
- "Automatisierungskatalog"
- "Digitaler Berater"
- "Wirtschaftlichkeit"
- "Licenses and subscriptions"
- "Software-Updates"

## Storage

- "Amazon FSx für ONTAP"
- "Amazon S3-Speicher"
- "Azure Blob-Speicher"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Cloud Volumes ONTAP -Verwaltung in der NetApp Console"
- "Systeme der E-Serie"
- "Google Cloud NetApp Volumes"
- "Google Cloud-Speicher"
- "On-Premise- ONTAP Cluster"
- "StorageGRID"

## Speicher als Service

- "Keystone"

## Datendienste

- "AI Data Engine"
- "Sicherung und Wiederherstellung"
- "Datenklassifizierung"
- "Kopieren und synchronisieren"
- "Notfallwiederherstellung"
- "Ransomware-Resilienz"

- "Replikation"
- "Cloud-Tiering"
- "Volume-Caching"
- "Workload-Factory"

# Rechtliche Hinweise für NetApp Console

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

## Copyright

"https://www.netapp.com/company/legal/copyright/"

## Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

## Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

## Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

## Open Source

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

"Hinweis zur NetApp Console"

**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.