Erste Schritte

NetApp Disaster Recovery

NetApp
February 04, 2026

Inhalt

Erste Schritte

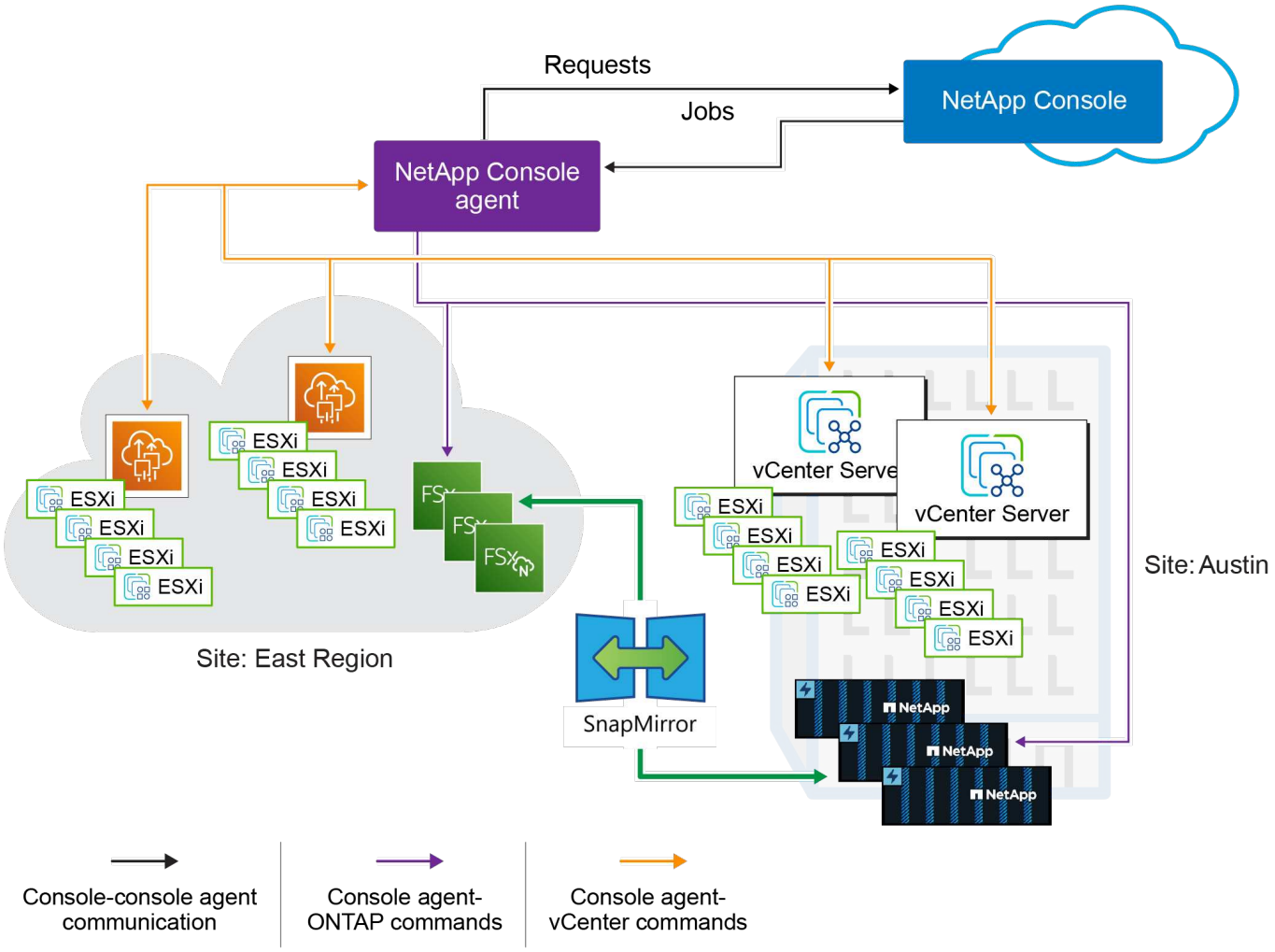
Erfahren Sie mehr über NetApp Disaster Recovery für VMware

Die Notfallwiederherstellung in der Cloud ist eine robuste und kostengünstige Möglichkeit, Workloads vor Standortausfällen und Datenbeschädigungen zu schützen. Mit NetApp Disaster Recovery für VMware können Sie Ihre lokalen VMware-VM- oder Datastore-Workloads mit ONTAP -Speicher in ein softwaredefiniertes VMware-Rechenzentrum in einer öffentlichen Cloud mit NetApp Cloud-Speicher oder in eine andere lokale VMware-Umgebung mit ONTAP -Speicher als Disaster-Recovery-Site replizieren. Sie können Disaster Recovery auch verwenden, um VM-Workloads von einem Standort zu einem anderen zu migrieren.

NetApp Disaster Recovery ist ein Cloud-basierter Disaster-Recovery-Dienst, der Disaster-Recovery-Workflows automatisiert. Mit NetApp Disaster Recovery können Sie Ihre lokalen, NFS-basierten Workloads und VMware vSphere Virtual Machine File System (VMFS)-Datenspeicher für iSCSI und FC mit NetApp -Speicher auf einem der folgenden Systeme schützen:

- Amazon Elastic VMware Service (EVS) mit Amazon FSx for NetApp ONTAP Weitere Informationen finden Sie unter"Einführung von NetApp Disaster Recovery mit Amazon Elastic VMware Service und Amazon FSx for NetApp ONTAP" .
- VMware Cloud (VMC) auf AWS mit Amazon FSx for NetApp ONTAP
- Azure VMware Solution (AVS) mit NetApp Cloud Volumes ONTAP (iSCSI) (Private Vorschau)
- Google Cloud VMware Engine (GCVE) mit Google Cloud NetApp Volumes
- Eine weitere lokale NFS- und/oder VMFS-basierte (iSCSI/FC) VMware-Umgebung mit ONTAP Speicher

NetApp Disaster Recovery verwendet die ONTAP SnapMirror -Technologie mit integrierter nativer VMware-Orchestrierung, um VMware-VMs und die zugehörigen On-Disk-Betriebssystemimages zu schützen und gleichzeitig alle Speichereffizienzvorteile von ONTAP beizubehalten. Disaster Recovery verwendet diese Technologien als Replikationstransport zum Disaster Recovery-Standort. Dies ermöglicht die branchenweit beste Speichereffizienz (Komprimierung und Deduplizierung) an primären und sekundären Standorten.



NetApp Console

Auf NetApp Disaster Recovery kann über die NetApp Console zugegriffen werden.

Die NetApp Console ermöglicht eine zentrale Verwaltung von NetApp -Speicher- und Datendiensten in lokalen und Cloud-Umgebungen auf Unternehmensebene. Die Konsole ist für den Zugriff auf und die Nutzung der NetApp -Datendienste erforderlich. Als Verwaltungsschnittstelle ermöglicht es Ihnen, viele Speicherressourcen über eine Schnittstelle zu verwalten. Konsolenadministratoren können den Zugriff auf Speicher und Dienste für alle Systeme innerhalb des Unternehmens steuern.

Sie benötigen weder eine Lizenz noch ein Abonnement, um die NetApp Console zu verwenden. Es fallen nur dann Kosten an, wenn Sie Konsolenagenten in Ihrer Cloud bereitstellen müssen, um die Konnektivität zu Ihren Speichersystemen oder NetApp -Datendiensten sicherzustellen. Einige NetApp -Datendienste, auf die über die Konsole zugegriffen werden kann, sind jedoch lizenz- oder abonnementbasiert.

Erfahren Sie mehr über die "NetApp Console" .

Vorteile der Verwendung von NetApp Disaster Recovery für VMware

NetApp Disaster Recovery bietet die folgenden Vorteile:

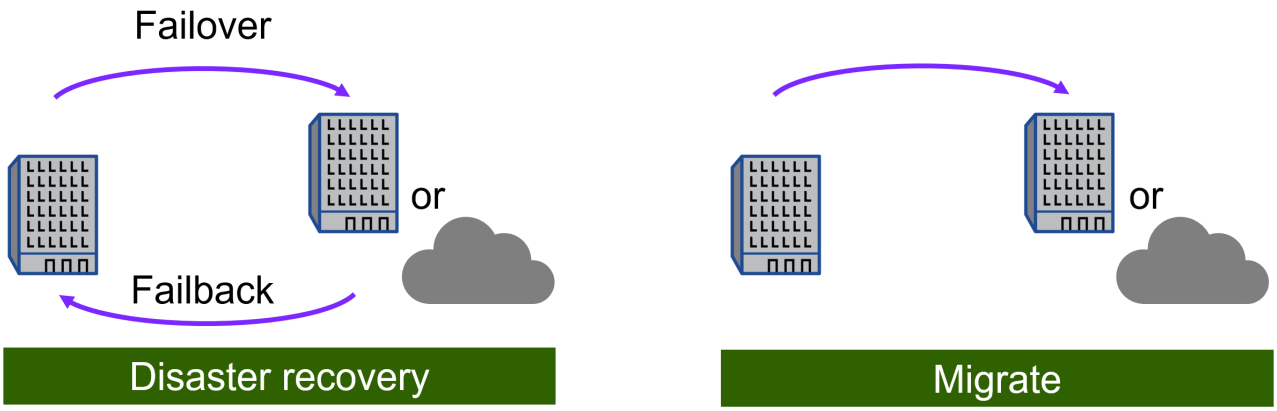
- Vereinfachte Benutzererfahrung für die vCenter-Erkennung und -Wiederherstellung von Anwendungen mit mehreren zeitpunktbezogenen Wiederherstellungsvorgängen.

- Niedrigere Gesamtbetriebskosten durch reduzierte Betriebskosten und die Möglichkeit, Notfallwiederherstellungspläne mit minimalem Ressourcenaufwand zu erstellen und anzupassen.
- Kontinuierliche Notfallwiederherstellungsbereitschaft mit virtuellen Failover-Tests, die den Betrieb nicht unterbrechen. Sie können Ihre DR-Failover-Pläne regelmäßig testen, ohne die Produktionsarbeitslast zu beeinträchtigen.
- Schnellere Wertschöpfung durch dynamische Änderungen in Ihrer IT-Umgebung und die Möglichkeit, diese in Ihren Notfallwiederherstellungsplänen zu berücksichtigen.
- Möglichkeit, sowohl die Speicher- als auch die virtuellen Ebenen durch Backend-Orchestrierung von ONTAP und VMware gleichzeitig zu verwalten, ohne dass virtuelle Server-Appliances (VSAs) bereitgestellt und gewartet werden müssen.
- DR-Lösungen für VMware können ressourcenintensiv sein. Viele DR-Lösungen replizieren VMs auf der virtuellen VMware-Ebene mithilfe von VSAs, was mehr Rechenressourcen verbrauchen und zu einem Verlust der wertvollen Speichereffizienz von ONTAP führen kann. Da Disaster Recovery die ONTAP SnapMirror -Technologie verwendet, kann es mithilfe unseres inkrementellen Replikationsmodells mit allen nativen Datenkomprimierungs- und Deduplizierungseffizienzen von ONTAP Daten von Produktionsdatenspeichern zum DR-Standort replizieren.

Was Sie mit NetApp Disaster Recovery für VMware tun können

NetApp Disaster Recovery bietet Ihnen die volle Nutzung mehrerer NetApp -Technologien, um die folgenden Ziele zu erreichen:

- Replizieren Sie VMware-Apps auf Ihrem lokalen Produktionsstandort mithilfe der SnapMirror -Replikation an einen Remote-Standort zur Notfallwiederherstellung in der Cloud oder vor Ort.
- Migrieren Sie VMware-Workloads von Ihrem ursprünglichen Standort zu einem anderen Standort.
- Führen Sie einen Failover-Test durch. Wenn Sie dies tun, erstellt der Dienst temporäre virtuelle Maschinen. Disaster Recovery erstellt aus dem ausgewählten Snapshot ein neues FlexClone Volume und ein temporärer Datenspeicher, der durch das FlexClone -Volume gesichert ist, wird den ESXi-Hosts zugeordnet. Dieser Prozess verbraucht keine zusätzliche physische Kapazität auf dem lokalen ONTAP -Speicher oder FSx für NetApp ONTAP -Speicher in AWS. Das ursprüngliche Quellvolume wird nicht geändert und Replikationsaufträge können auch während der Notfallwiederherstellung fortgesetzt werden.
- Führen Sie im Katastrophenfall bei Bedarf ein Failover Ihres primären Standorts auf den Disaster Recovery-Standort durch. Dabei kann es sich um VMware Cloud auf AWS mit Amazon FSx for NetApp ONTAP oder eine lokale VMware-Umgebung mit ONTAP handeln.
- Nachdem der Notfall behoben wurde, führen Sie bei Bedarf ein Failback vom Notfallwiederherstellungsstandort zum primären Standort durch.
- Gruppieren Sie VMs oder Datenspeicher für eine effiziente Verwaltung in logische Ressourcengruppen.



Die Konfiguration des vSphere-Servers erfolgt außerhalb von NetApp Disaster Recovery im vSphere-Server.

Kosten

NetApp berechnet Ihnen keine Gebühren für die Nutzung der Testversion von NetApp Disaster Recovery.

NetApp Disaster Recovery kann entweder mit einer NetApp -Lizenz oder einem jährlichen Abonnementplan über Amazon Web Services verwendet werden.

Einige Versionen enthalten eine Technologievorschau. NetApp berechnet Ihnen keine Kosten für die in der Vorschau angezeigte Workload-Kapazität. Sehen"Was ist neu bei NetApp Disaster Recovery ?" für Informationen zu den neuesten Technologievorschauen.

Lizenzierung

Sie können die folgenden Lizenztypen verwenden:

- Melden Sie sich für eine 30-tägige kostenlose Testversion an.
- Erwerben Sie ein Pay-as-you-go-Abonnement (PAYGO) über den Amazon Web Services (AWS) Marketplace oder den Microsoft Azure Marketplace. Mit dieser Lizenz können Sie eine Lizenz mit fester, geschützter Kapazität ohne langfristige Bindung erwerben.
- Bringen Sie Ihre eigene Lizenz (BYOL) mit. Dabei handelt es sich um eine NetApp Lizenzdatei (NLF), die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten. Sie können die Seriennummer der Lizenz verwenden, um BYOL in der NetApp Console zu aktivieren.

Lizenzen für alle NetApp -Datendienste werden über Abonnements in der NetApp Console verwaltet. Nachdem Sie Ihr BYOL eingerichtet haben, können Sie in der Konsole eine aktive Lizenz für den Dienst sehen.

Die Lizenzierung des Dienstes erfolgt auf Grundlage der auf geschützten ONTAP Volumes gehosteten Datenmenge. Der Dienst ermittelt, welche Volumes für Lizenzierungszwecke berücksichtigt werden sollten, indem er geschützte VMs ihren vCenter-Datenspeichern zuordnet. Jeder Datenspeicher wird auf einem ONTAP Volume oder LUN gehostet. Die von ONTAP für dieses Volume oder LUN gemeldete genutzte Kapazität wird für Lizenzierungsbestimmungen verwendet.

Geschützte Volumes können viele VMs hosten. Einige sind möglicherweise nicht Teil einer NetApp Disaster Recovery -Ressourcengruppe. Unabhängig davon wird der von allen VMs auf diesem Volume oder LUN verbrauchte Speicher auf die maximale Lizenzkapazität angerechnet.

> Die Gebühren für NetApp Disaster Recovery basieren auf der genutzten Kapazität der Datenspeicher am Quellstandort, wenn mindestens eine VM über einen Replikationsplan verfügt. Die Kapazität für einen ausgefallenen Datenspeicher ist nicht in der Kapazitätszuteilung enthalten. Wenn bei einem BYOL die Daten die zulässige Kapazität überschreiten, sind die Vorgänge im Dienst eingeschränkt, bis Sie eine zusätzliche Kapazitätslizenz erwerben oder die Lizenz in der NetApp Console aktualisieren.

Einzelheiten zum Einrichten der Lizenzierung für NetApp Disaster Recovery finden Sie unter"Einrichten der NetApp Disaster Recovery -Lizenzierung" .

30 Tage kostenlos testen

Sie können NetApp Disaster Recovery mit einer 30-tägigen kostenlosen Testversion ausprobieren.

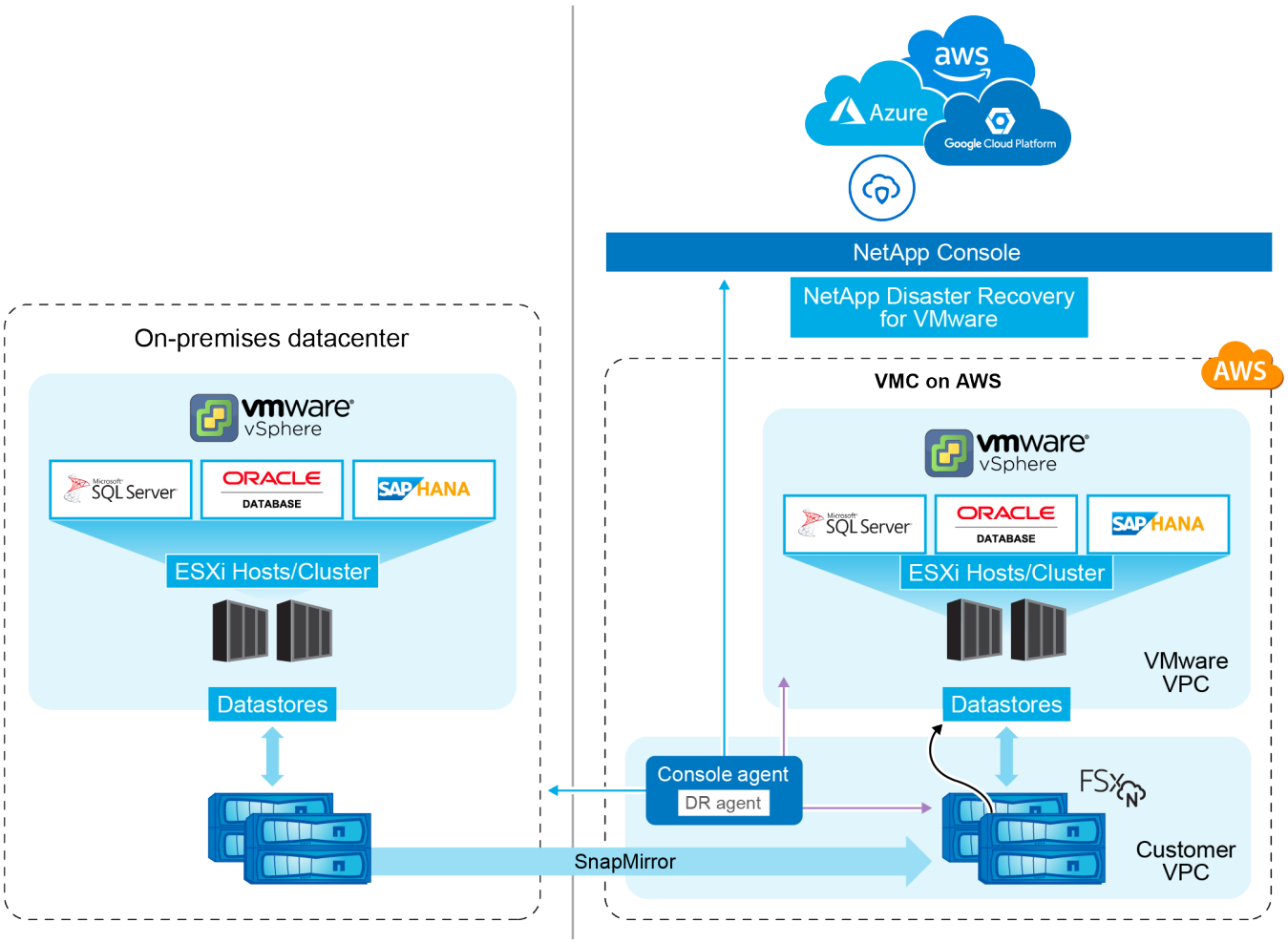
Um nach der 30-tägigen Testphase fortzufahren, müssen Sie ein Pay-as-you-go-Abonnement (PAYGO) von Ihrem Cloud-Anbieter erwerben oder eine BYOL-Lizenz von NetApp kaufen.

Sie können jederzeit eine Lizenz erwerben und es fallen erst nach Ablauf der 30-tägigen Testphase Kosten für Sie an.

So funktioniert NetApp Disaster Recovery

NetApp Disaster Recovery ist ein Dienst, der in der NetApp Console -Software als Serviceumgebung (SaaS) gehostet wird. Disaster Recovery kann Workloads wiederherstellen, die von einem lokalen Standort auf Amazon FSx for ONTAP oder einen anderen lokalen Standort repliziert wurden. Dieser Service automatisiert die Wiederherstellung von der SnapMirror -Ebene über die Registrierung virtueller Maschinen in VMware Cloud auf AWS bis hin zu Netzwerkzuordnungen direkt auf der VMware-Netzwerkvirtualisierungs- und Sicherheitsplattform NSX-T. Diese Funktion ist in allen Virtual Machine Cloud-Umgebungen enthalten.

NetApp Disaster Recovery verwendet die ONTAP SnapMirror -Technologie, die eine hocheffiziente Replikation ermöglicht und die Effizienz der inkrementellen Snapshots von ONTAP für immer bewahrt. Die SnapMirror Replikation stellt sicher, dass anwendungskonsistente Snapshot-Kopien immer synchron sind und die Daten nach einem Failover sofort nutzbar sind.



Im Katastrophenfall unterstützt Sie dieser Dienst bei der Wiederherstellung virtueller Maschinen in der anderen lokalen VMware-Umgebung oder VMC, indem er die SnapMirror -Beziehungen auflöst und die Zielsite aktiviert.

- Mit dem Dienst können Sie außerdem ein Failback virtueller Maschinen auf den ursprünglichen Quellspeicherort durchführen.
- Sie können den Failover-Prozess für die Notfallwiederherstellung testen, ohne die ursprünglichen virtuellen Maschinen zu unterbrechen. Der Test stellt virtuelle Maschinen in einem isolierten Netzwerk wieder her, indem ein FlexClone des Volumes erstellt wird.
- Für den Failover- oder Test-Failover-Prozess können Sie den neuesten (Standard) oder ausgewählten Snapshot auswählen, von dem aus Ihre virtuelle Maschine wiederhergestellt werden soll.

Komponenten der Notfallwiederherstellung

Disaster Recovery verwendet die folgenden Komponenten, um die Notfallwiederherstellung für VMware-Workloads bereitzustellen:

- * NetApp Console*: Die Benutzeroberfläche zum Verwalten Ihrer Notfallwiederherstellungspläne. Mit der NetApp Console können Sie Replikationspläne, Ressourcengruppen und Failover-Vorgänge in Ihren lokalen und Cloud-Umgebungen erstellen und verwalten.
- **Konsolenagent**: Eine leichtgewichtige Softwarekomponente, die in Ihrem Cloud-gehosteten Netzwerk oder Ihrer lokalen VMware-Umgebung ausgeführt wird. Es kommuniziert mit der NetApp Console und verwaltet die Datenreplikation zwischen Ihrer lokalen Umgebung und dem Disaster-Recovery-Standort. Der Konsolenagent wird auf einer virtuellen Maschine in Ihrer VMware-Umgebung installiert.

- * ONTAP -Speichercluster*: Die ONTAP -Speichercluster sind die primären Speichersysteme, die Ihre VMware-Workloads hosten. Die ONTAP Speichercluster stellen die zugrunde liegende Speicherinfrastruktur für Ihre Notfallwiederherstellungspläne bereit. Disaster Recovery verwendet ONTAP Speicher-APIs zum Verwalten von ONTAP Speicherclustern wie lokalen Arrays und Cloud-basierten Lösungen wie Amazon FSx for NetApp ONTAP.
- **vCenter-Server**: Das VMware vCenter ist der Verwaltungsserver für Ihre VMware-Umgebung. Es verwaltet die ESXi-Hosts und die zugehörigen Datenspeicher. Der Konsolenagent kommuniziert mit dem VMware vCenter, um die Datenreplikation zwischen Ihrer lokalen Umgebung und dem Notfallwiederherstellungsstandort zu verwalten. Dazu gehört das Registrieren von ONTAP -LUNs und -Volumes als Datenspeicher, das Neukonfigurieren von VMs sowie das Starten und Stoppen von VMs.

Der Disaster Recovery-Schutz-Workflow

Wenn einer Ressourcengruppe ein Replikationsplan zugewiesen wird, führt Disaster Recovery eine Erkennungsprüfung aller Komponenten in der Ressourcengruppe und im Plan durch, um sicherzustellen, dass der Plan aktiviert werden kann.

Wenn diese Prüfung erfolgreich ist, führt Disaster Recovery die folgenden Initialisierungsschritte durch:

1. Identifizieren Sie für jede VM in der Zielressourcengruppe den VMware-Hostdatenspeicher.
2. Identifizieren Sie für jeden gefundenen VMware-Datenspeicher das Host ONTAP FlexVol volume oder die LUN.
3. Stellen Sie für jedes gefundene ONTAP Volume und LUN fest, ob eine vorhandene SnapMirror Beziehung zwischen den Quellvolumes und einem Zielvolume am Zielstandort besteht.
    a. Wenn keine SnapMirror -Beziehung vorhanden ist, erstellen Sie alle neuen Zielvolumes und erstellen Sie eine neue SnapMirror -Beziehung zwischen jedem ungeschützten Quellvolume.
    b. Wenn bereits eine SnapMirror -Beziehung besteht, verwenden Sie diese Beziehung, um alle Replikationsvorgänge durchzuführen.

Nachdem Disaster Recovery alle Beziehungen erstellt und initialisiert hat, führt der Dienst bei jeder geplanten Sicherung die folgenden Schritte zum Datenschutz aus:

1. Verwenden Sie für jede als „anwendungskonsistent“ gekennzeichnete VM VMtools, um die unterstützte Anwendung in einen Sicherungszustand zu versetzen.
2. Erstellen Sie einen neuen Snapshot aller ONTAP -Volumes, die geschützte VMware-Datenspeicher hosten.
3. Führen Sie einen SnapMirror Aktualisierungsvorgang durch, um diese Snapshots auf den Ziel ONTAP -Cluster zu replizieren.
4. Stellen Sie fest, ob die Anzahl der aufbewahrten Snapshots die im Replikationsplan definierte maximale Snapshot-Aufbewahrung überschritten hat, und löschen Sie alle überflüssigen Snapshots sowohl vom Quell- als auch vom Zielvolume.

Unterstützte Schutzziele und Datenspeichertypen

Unterstützte Datenspeichertypen NetApp Disaster Recovery unterstützt die folgenden Datenspeichertypen:

- NFS-Datenspeicher, die auf ONTAP FlexVol -Volumes gehostet werden, die sich auf ONTAP Clustern befinden.
- VMware vSphere Virtual Machine File System (VMFS)-Datenspeicher mit dem iSCSI- oder FC-Protokoll

Unterstützte Schutzziele

- VMware Cloud (VMC) auf AWS mit Amazon FSx for NetApp ONTAP
- Eine weitere lokale, NFS-basierte VMware-Umgebung mit ONTAP Speicher oder eine lokale FC/iSCSI-VMSF
- Amazon Elastic VMware Service
- Azure VMware Solution (AVS) mit NetApp Cloud Volumes ONTAP (iSCSI) (Private Vorschau)
- Google Cloud VMware Engine (GCVE) mit Google Cloud NetApp Volumes

Begriffe, die Ihnen bei NetApp Disaster Recovery helfen könnten

Es kann für Sie von Vorteil sein, einige Begriffe im Zusammenhang mit der Notfallwiederherstellung zu verstehen.

- **Datenspeicher**: Ein VMware vCenter-Datencontainer, der ein Dateisystem zum Speichern von VMDK-Dateien verwendet. Typische Datenspeichertypen sind NFS, VMFS, vSAN oder vVol. Disaster Recovery unterstützt NFS- und VMFS-Datenspeicher. Jeder VMware-Datenspeicher wird auf einem einzelnen ONTAP Volume oder LUN gehostet. Disaster Recovery unterstützt NFS- und VMFS-Datenspeicher, die auf FlexVol Volumes gehostet werden, die sich auf ONTAP Clustern befinden.
- **Replikationsplan**: Ein Satz von Regeln darüber, wie oft Sicherungen durchgeführt werden und wie mit Failover-Ereignissen umgegangen wird. Pläne werden einer oder mehreren Ressourcengruppen zugewiesen.
- **Recovery Point Objective (RPO)**: Der maximale Datenverlust, der im Katastrophenfall akzeptabel ist. RPO wird in der Häufigkeit der Datenreplikation oder im Replikationszeitplan des Replikationsplans definiert.
- **Recovery Time Objective (RTO)**: Die maximal akzeptable Zeitspanne für die Wiederherstellung nach einem Desaster. RTO ist im Replikationsplan definiert und ist die Zeit, die für das Failover zum DR-Standort und den Neustart aller VMs benötigt wird.
- **Ressourcengruppe**: Ein logischer Container, der es Ihnen ermöglicht, mehrere VMs als eine Einheit zu verwalten. Eine VM kann sich jeweils nur in einer Ressourcengruppe befinden. Sie können für jede Anwendung oder Arbeitslast, die Sie schützen möchten, eine Ressourcengruppe erstellen.
- **Site**: Ein logischer Container, der normalerweise mit einem physischen Rechenzentrum oder Cloud-Standort verknüpft ist, der einen oder mehrere vCenter-Cluster und ONTAP Speicher hostet.

Voraussetzungen für NetApp Disaster Recovery

Bevor Sie NetApp Disaster Recovery verwenden, stellen Sie sicher, dass Ihre Umgebung die Anforderungen an ONTAP -Speicher, VMware vCenter-Cluster und NetApp Console erfüllt.

Softwareversionen

Komponente	Mindestversion
Amazon FSx for NetApp ONTAP	Neuste verfügbare Version
Google Cloud VMware Engine mit Google Cloud NetApp Volumes	Neuste verfügbare Version

Komponente	Mindestversion
ONTAP Software	ONTAP 9.10.0 oder höher
VMware Cloud für AWS	Neuste verfügbare Version
VMware vCenter vor Ort	7.0u3 oder höher

Voraussetzungen und Überlegungen für Google Cloud

Bei der Notfallwiederherstellung auf Google Cloud VMware Engine mit Google Cloud NetApp Volumes müssen Sie sicherstellen, dass Sie die richtigen Berechtigungen konfigurieren und die genannten Hinweise beachten.

- Wenden Sie sich an das Google SRE-Team, um die folgenden Dienste auf die Whitelist setzen zu lassen:
  - Synchronisierungs-API zum Übertragen von Snapshots vom lokalen Speicher in Google Cloud NetApp Volumes.
  - Das Google-Projekt mit der VMware-Engine zum Erstellen, Einbinden und Ausbinden von Datenspeichern.
- Du musst"Stellen Sie einen Antrag, um Ihre Volumes für die Hybridreplikation auf die Zulassungsliste setzen zu lassen." Die
- Seien Sie sich der folgenden Punkte bewusst:"Google Cloud NetApp Volumes Kontingente und Limits" Die
- Einem Replikationsplan kann nur ein Volume oder Datenspeicher hinzugefügt werden.
- Überprüfen Sie die"Einschränkungen" Die

Überlegungen zum Ausfallmanagement

- Failover wird nur mit dem neuesten Snapshot unterstützt. Falls erforderlich, können Sie während des Failovers einen neuen Snapshot erstellen (das heißt, die Option für selektive Snapshots muss deaktiviert sein).
- Nach einem Failover kann kein neuer Snapshot erstellt werden.
- Snapshots können nach einem Failover nicht beibehalten und abgeglichen werden.

Ausfallüberlegungen

- Ein Failback ist nur mit der Option „Selektiver Snapshot“ möglich. Ein Failback kann nicht durch Erstellen eines neuen Snapshots durchgeführt werden.
- Wenn Sie das Cluster-Peering zwischen lokalem Speicher und Google Cloud NetApp Volumes -Speicherclustern entfernen, müssen Sie den Cluster- und Speicher-VM-Peering-Eintrag im lokalen Cluster manuell löschen. Weitere Informationen finden Sie unter "Eine vServer-Peer-Beziehung löschen".

Google Cloud-Berechtigungen

Dem Dienstprinzipal in Google Cloud sollten die folgenden Rollen oder gleichwertige Berechtigungen zugewiesen werden:

- "Rolle als Computeradministrator"
- "Google Cloud-Berechtigungen für die NetApp Console"

- "Google Cloud NetApp Volumes Admin"
- "VMware Engine-Dienstadministrator"

NetApp Console

Der NetApp Console Konsolenbenutzer muss über folgende Rollen verfügen:

- "Google Cloud NetApp Volumes Administrator"
- "SnapCenter -Administrator"
- "Disaster Recovery-Failover-Administrator"

ONTAP -Speichervoraussetzungen

Diese Voraussetzungen gelten entweder für ONTAP oder Amazon FSX für NetApp ONTAP Instanzen.

- Quell- und Zielcluster müssen eine Peer-Beziehung haben.
- Die SVM, die die Disaster-Recovery-Volumes hostet, muss auf dem Zielcluster vorhanden sein.
- Zwischen Quell-SVM und Ziel-SVM muss eine Peer-Beziehung bestehen.
- Bei der Bereitstellung mit Amazon FSx for NetApp ONTAP gilt die folgende Voraussetzung:
  - In Ihrer VPC muss eine Amazon FSx for NetApp ONTAP -Instanz zum Hosten von VMware DR-Datenspeichern vorhanden sein. Um loszulegen, siehe"die Amazon FSx für ONTAP -Dokumentation" Die

Voraussetzungen für VMware vCenter-Cluster

Diese Voraussetzungen gelten sowohl für lokale vCenter-Cluster als auch für das softwaredefinierte Rechenzentrum (SDDC) von VMware Cloud für AWS.

- Rezension"vCenter-Berechtigungen" erforderlich für NetApp Disaster Recovery.
- Alle VMware-Cluster, die von NetApp Disaster Recovery verwaltet werden sollen, verwenden ONTAP Volumes zum Hosten aller VMs, die Sie schützen möchten.
- Alle VMware-Datenspeicher, die von NetApp Disaster Recovery verwaltet werden sollen, müssen eines der folgenden Protokolle verwenden:
  - NFS
  - VMFS mit dem iSCSI- oder FC-Protokoll
- VMware vSphere Version 7.0 Update 3 (7.0v3) oder höher
- Wenn Sie VMware Cloud SDDC verwenden, gelten diese Voraussetzungen.
  - Verwenden Sie in der VMware Cloud Console die Dienstrollen „Administrator“ und „NSX Cloud-Administrator“. Verwenden Sie den Organisationseigentümer auch für die Organisationsrolle. Siehe "Dokumentation zur Verwendung von VMware Cloud Foundations mit AWS FSx für NetApp ONTAP" .
  - Verknüpfen Sie das VMware Cloud SDDC mit der Amazon FSx for NetApp ONTAP Instanz. Siehe "VMware Cloud auf AWS-Integration mit Amazon FSx for NetApp ONTAP -Bereitstellungsinformationen" .

Voraussetzungen für die NetApp Console

Erste Schritte mit der NetApp Console

Falls Sie dies noch nicht getan haben, "Melden Sie sich bei der NetApp Console an und erstellen Sie eine Organisation" Die

Sammeln Sie Anmeldeinformationen für ONTAP und VMware

- Die Anmeldeinformationen für Amazon FSx for ONTAP und AWS müssen im NetApp Console Projekt, das NetApp Disaster Recovery verwaltet, zum System hinzugefügt werden.
- Für NetApp Disaster Recovery sind vCenter-Anmeldeinformationen erforderlich. Sie geben die vCenter-Anmeldeinformationen ein, wenn Sie eine Site in NetApp Disaster Recovery hinzufügen.

  Eine Liste der erforderlichen vCenter-Berechtigungen finden Sie unter"Für NetApp Disaster Recovery erforderliche vCenter-Berechtigungen" . Anweisungen zum Hinzufügen einer Site finden Sie unter"Hinzufügen einer Site" .

Erstellen Sie den NetApp Console Agenten

Der Konsolenagent ist eine Softwarekomponente, die es der Konsole ermöglicht, mit Ihrem ONTAP Speicher und Ihren VMware vCenter-Clustern zu kommunizieren. Es ist erforderlich, damit die Notfallwiederherstellung ordnungsgemäß funktioniert. Der Agent befindet sich in Ihrem privaten Netzwerk (entweder in einem lokalen Rechenzentrum oder in einer Cloud-VPC) und kommuniziert mit Ihren ONTAP Speicherinstanzen sowie allen weiteren Server- und Anwendungskomponenten. Für die Notfallwiederherstellung ist dies der Zugriff auf Ihre verwalteten vCenter-Cluster.

In der NetApp Console muss ein Konsolenagent eingerichtet werden. Wenn Sie den Agenten verwenden, enthält er die entsprechenden Funktionen für den Disaster Recovery-Dienst.

- NetApp Disaster Recovery funktioniert nur mit der Agent-Bereitstellung im Standardmodus. Sehen "Erste Schritte mit der NetApp Console im Standardmodus" .
- Stellen Sie sicher, dass sowohl der Quell- als auch der Ziel-vCenter-Cluster denselben Console-Agenten verwenden.
- Benötigter Konsolenagenttyp:
  - **On-Premises-zu-On-Premises-Disaster-Recovery**: Installieren Sie den On-Premises-Console-Agenten am Disaster-Recovery-Standort. Mit dieser Methode verhindert ein Ausfall des primären Standorts nicht, dass der Dienst Ihre virtuellen Ressourcen am DR-Standort neu startet. Siehe "Installieren und Einrichten des Konsolen-Agenten vor Ort".

    Disaster Recovery unterstützt auch die Verwendung mehrerer Konsolenagenten mit lokalen Konfigurationen. In diesem Szenario leiten die Console-Agenten Aktionen an vCenter- und ONTAP -Array-Cluster weiter, wobei Quelle und Ziel jeweils über einen eigenen Console-Agenten verfügen. Es wird empfohlen, mehrere Console-Agenten zu verwenden, um die Latenz zu verringern und die Wiederherstellungszeit zu verbessern, falls ein Console-Agent oder eine Site ausfällt.

  - **Vor Ort zu AWS**: Installieren Sie den Konsolenagenten für AWS in Ihrem AWS VPC. Siehe "Installationsoptionen für Konsolenagenten in AWS" .

Verwenden Sie für die lokale Übertragung den lokalen Konsolenagenten. Verwenden Sie für die lokale Verbindung zu AWS den AWS-Konsolenagenten, der Zugriff auf das lokale Quell-vCenter und das lokale Ziel-vCenter hat.

    - Der installierte Konsolenagent muss auf alle VMware vCenter-Clusterinstanzen und ESXi-Hosts zugreifen können, die von diesen vCenter-Clustern verwaltet werden und die von Disaster Recovery verwaltet werden.

- Alle ONTAP Arrays, die von NetApp Disaster Recovery verwaltet werden sollen, müssen zu jedem System innerhalb des NetApp Console -Projekts hinzugefügt werden, das zur Verwaltung von NetApp Disaster Recovery verwendet wird.

  Sehen "Entdecken Sie lokale ONTAP -Cluster" .

- Informationen zum Einrichten eines intelligenten Proxys für NetApp Disaster Recovery finden Sie unter"Richten Sie Ihre Infrastruktur für NetApp Disaster Recovery ein" .

Workload-Voraussetzungen

Um sicherzustellen, dass die Prozesse zur Anwendungskonsistenz erfolgreich sind, müssen Sie die folgenden Voraussetzungen erfüllen:

- Stellen Sie sicher, dass VMware-Tools (oder Open VM-Tools) auf den zu schützenden VMs ausgeführt werden.
- Bei Windows-VMs, auf denen Microsoft SQL Server, Oracle Database oder beides ausgeführt wird, müssen die VSS Writer der Datenbanken aktiviert sein.
- Bei Oracle-Datenbanken, die auf einem Linux-Betriebssystem laufen, muss die Betriebssystem-Benutzerauthentifizierung für die Oracle-Datenbank-SYSDBA-Rolle aktiviert sein.

Weitere Informationen

- Erforderliche vCenter Privilegien
- Voraussetzungen für Amazon EVS mit NetApp Disaster Recovery

Schnellstart für NetApp Disaster Recovery

Hier finden Sie eine Übersicht über die erforderlichen Schritte für den Einstieg in NetApp Disaster Recovery. Über die Links in den einzelnen Schritten gelangen Sie zu einer Seite mit weiteren Einzelheiten.

Überprüfen der Voraussetzungen

"Stellen Sie sicher, dass Ihr System diese Anforderungen erfüllt" .

Einrichten von NetApp Disaster Recovery

- "Einrichten der Infrastruktur für den Dienst" .
- "Einrichten der Lizenzierung" .

Wie geht es weiter?

Nachdem Sie den Dienst eingerichtet haben, können Sie als Nächstes Folgendes tun.

- "Fügen Sie Ihre vCenter-Sites zu NetApp Disaster Recovery" .
- "Erstellen Sie Ihre erste Ressourcengruppe" .
- "Erstellen Sie Ihren ersten Replikationsplan" .
- "Replizieren von Anwendungen auf eine andere Site" .
- "Failover von Anwendungen auf einen Remote-Standort" .
- "Failback von Anwendungen auf die ursprüngliche Quellsite" .
- "Verwalten von Sites, Ressourcengruppen und Replikationsplänen" .
- "Überwachen von Notfallwiederherstellungsvorgängen" .

Richten Sie Ihre Infrastruktur für NetApp Disaster Recovery ein

Um NetApp Disaster Recovery zu verwenden, führen Sie einige Schritte aus, um es sowohl in Amazon Web Services (AWS) als auch in der NetApp Console einzurichten.

Rezension"Voraussetzungen" um sicherzustellen, dass Ihr System bereit ist.

Sie können NetApp Disaster Recovery in folgenden Infrastrukturen verwenden:

- Hybrid Cloud DR, das ein lokales VMware plus ONTAP -Rechenzentrum in eine AWS DR-Infrastruktur repliziert, die auf VMware Cloud on AWS und Amazon FSx for NetApp ONTAP basiert.
- Private Cloud-DR, die ein lokales VMware plus ONTAP vCenter auf ein anderes lokales VMware plus ONTAP vCenter repliziert.

Hybrid Cloud mit VMware Cloud und Amazon FSx for NetApp ONTAP

Diese Methode besteht aus einer lokalen vCenter-Produktionsinfrastruktur mit Datenspeichern, die auf ONTAP FlexVol -Volumes mithilfe eines NFS-Protokolls gehostet werden. Die DR-Site besteht aus einer oder mehreren VMware Cloud SDDC-Instanzen, die Datenspeicher verwenden, die auf FlexVol -Volumes gehostet werden, die von einer oder mehreren FSx for ONTAP -Instanzen mithilfe eines NFS-Protokolls bereitgestellt werden.

Die Produktions- und DR-Standorte sind über eine AWS-kompatible sichere Verbindung verbunden. Gängige Verbindungstypen sind ein sicheres VPN (privat oder von AWS bereitgestellt), AWS Direct Connect oder andere genehmigte Verbindungsmethoden.

Für die Notfallwiederherstellung mit AWS-Cloud-Infrastruktur müssen Sie den Konsolenagenten für AWS verwenden. Der Agent sollte im selben VPC wie die FSx for ONTAP -Instanz installiert werden. Wenn zusätzliche FSx for ONTAP -Instanzen in anderen VPCs bereitgestellt wurden, muss die VPC, die den Agenten hostet, Zugriff auf die anderen VPCs haben.

AWS-Verfügbarkeitszonen

AWS unterstützt die Bereitstellung von Lösungen in einer oder mehreren Verfügbarkeitszonen (AZ) innerhalb einer bestimmten Region. Disaster Recovery verwendet zwei von AWS gehostete Dienste: VMware Cloud für AWS und AWS FSx für NetApp ONTAP.

- **VMware Cloud für AWS**: Unterstützt die Bereitstellung in einer Single-AZ- oder in einer Dual-AZ-Stretch-Cluster-SDDC-Umgebung. Disaster Recovery unterstützt eine Single-AZ-SDDC-Bereitstellung nur für

Amazon VMware Cloud für AWS.

- **AWS FSx für NetApp ONTAP**: Wenn dies in einer Dual-AZ-Konfiguration bereitgestellt wird, gehört jedes Volume einem einzelnen FSx-System. Jedes Volume gehört einem einzelnen FSx-System. Die Daten des Volumes werden auf das zweite FSx-System gespiegelt. Die FSx für ONTAP -Systeme können entweder in Single- oder Dual-AZ-Bereitstellungen eingesetzt werden. Disaster Recovery unterstützt sowohl Single- als auch Multi-AZ-FSx für FSx für ONTAP Bereitstellungen.

BEST PRACTICE: Für die AWS DR-Site-Konfiguration empfiehlt NetApp die Verwendung von Single-AZ-Bereitstellungen sowohl für VMware Cloud als auch für AWS FSx für ONTAP -Instanzen. Da AWS für DR verwendet wird, bietet die Einführung mehrerer AZs keinen Vorteil. Mehrere AZs können die Kosten und die Komplexität erhöhen.

Von On-Premises zu AWS

AWS bietet die folgenden Methoden zum Verbinden privater Rechenzentren mit der AWS-Cloud. Jede Lösung hat ihre Vorteile und Kostenaspekte.

- **AWS Direct Connect**: Dies ist eine AWS-Cloud-Verbindung, die sich im selben geografischen Gebiet wie Ihr privates Rechenzentrum befindet und von einem AWS-Partner bereitgestellt wird. Diese Lösung bietet eine sichere, private Verbindung zwischen Ihrem lokalen Rechenzentrum und der AWS-Cloud, ohne dass eine öffentliche Internetverbindung erforderlich ist. Dies ist die direkteste und effizienteste Verbindungsmethode, die von AWS angeboten wird.
- **AWS Internet Gateway**: Dies bietet öffentliche Konnektivität zwischen AWS-Cloud-Ressourcen und externen Rechenressourcen. Dieser Verbindungstyp wird normalerweise verwendet, um externen Kunden Serviceangebote bereitzustellen, beispielsweise HTTP/HTTPS-Dienste, bei denen Sicherheit keine Voraussetzung ist. Es gibt keine Kontrolle der Dienstqualität, Sicherheit oder Konnektivitätsgarantie. Aus diesem Grund wird diese Verbindungsmethode nicht für die Verbindung eines Produktionsrechenzentrums mit der Cloud empfohlen.
- **AWS Site-Site VPN**: Diese virtuelle private Netzwerkverbindung kann verwendet werden, um sichere Zugriffsverbindungen zusammen mit einem öffentlichen Internetdienstanbieter bereitzustellen. Das VPN verschlüsselt und entschlüsselt alle Daten, die zur und von der AWS-Cloud übertragen werden. VPNs können entweder software- oder hardwarebasiert sein. Für Unternehmensanwendungen sollte der öffentliche Internetdienstanbieter (ISP) Qualitätsgarantien bieten, um sicherzustellen, dass für die DR-Replikation ausreichend Bandbreite und Latenz zur Verfügung stehen.

BEST PRACTICE: Für die AWS DR-Site-Konfiguration empfiehlt NetApp die Verwendung von AWS Direct Connect. Diese Lösung bietet höchste Leistung und Sicherheit für Unternehmensanwendungen. Wenn dies nicht möglich ist, sollte eine leistungsstarke öffentliche ISP-Verbindung zusammen mit einem VPN verwendet werden. Stellen Sie sicher, dass der ISP kommerzielle QoS-Dienstlevel anbietet, um eine angemessene Netzwerkleistung sicherzustellen.

VPC-zu-VPC-Verbindungen

AWS bietet die folgenden Arten von VPC-zu-VPC-Verbindungen an. Jede Lösung hat ihre Vorteile und Kostenaspekte.

- **VPC-Peering**: Dies ist eine private Verbindung zwischen zwei VPCs. Es ist die direkteste und effizienteste Verbindungsmethode, die von AWS angeboten wird. VPC-Peering kann verwendet werden, um VPCs in derselben oder in verschiedenen AWS-Regionen zu verbinden.
- **AWS Internet Gateway**: Dies wird normalerweise verwendet, um Verbindungen zwischen AWS VPC-Ressourcen und Nicht-AWS-Ressourcen und -Endpunkten bereitzustellen. Der gesamte Datenverkehr folgt einem „Haarnadelpfad“, bei dem VPC-Datenverkehr, der für eine andere VPC bestimmt ist, die AWS-Infrastruktur über das Internet-Gateway verlässt und über dasselbe oder ein anderes Gateway zur AWS-

Infrastruktur zurückkehrt. Dies ist kein geeigneter VPC-Verbindungstyp für VMware-Unternehmenslösungen.

- **AWS Transit Gateway**: Dies ist ein zentralisierter, routerbasierter Verbindungstyp, der es jedem VPC ermöglicht, eine Verbindung zu einem einzigen, zentralen Gateway herzustellen, das als zentraler Hub für den gesamten VPC-zu-VPC-Verkehr fungiert. Dies kann auch mit Ihrer VPN-Lösung verbunden werden, um lokalen Rechenzentrumsressourcen den Zugriff auf von AWS VPC gehostete Ressourcen zu ermöglichen. Für die Implementierung dieser Verbindungsart fallen in der Regel zusätzliche Kosten an.

BEST PRACTICE: Für DR-Lösungen mit VMware Cloud und einem einzelnen FSx für ONTAP VPC empfiehlt NetApp die Verwendung der VPC-Peer-Verbindung. Wenn mehrere FSx für ONTAP VPCs bereitgestellt werden, empfehlen wir die Verwendung eines AWS Transit Gateway, um den Verwaltungsaufwand mehrerer VPC-Peer-Verbindungen zu reduzieren.

Machen Sie sich bereit für den On-Premises-to-Cloud-Schutz mit AWS

Um NetApp Disaster Recovery für den On-Premises-to-Cloud-Schutz mit AWS einzurichten, müssen Sie Folgendes einrichten:

- AWS FSx für NetApp ONTAP einrichten
- Einrichten von VMware Cloud on AWS SDDC

AWS FSx für NetApp ONTAP einrichten

- Erstellen Sie ein Amazon FSx for NetApp ONTAP -Dateisystem.
  - Stellen Sie FSx für ONTAP bereit und konfigurieren Sie es. Amazon FSx for NetApp ONTAP ist ein vollständig verwalteter Service, der äußerst zuverlässigen, skalierbaren, leistungsstarken und funktionsreichen Dateispeicher bietet, der auf dem NetApp ONTAP Dateisystem basiert.
  - Folgen Sie den Schritten in "Technischer Bericht 4938: Mounten Sie Amazon FSx ONTAP als NFS-Datenspeicher mit VMware Cloud auf AWS" Und "Schnellstart für Amazon FSx for NetApp ONTAP" FSx für ONTAP bereitstellen und konfigurieren.
- Fügen Sie dem System Amazon FSx for ONTAP hinzu und fügen Sie AWS-Anmeldeinformationen für FSx for ONTAP hinzu.
- Erstellen oder überprüfen Sie Ihr Ziel ONTAP SVM in AWS FSx für die ONTAP Instanz.
- Konfigurieren Sie die Replikation zwischen Ihrem lokalen ONTAP Quellcluster und Ihrer FSx for ONTAP Instanz in der NetApp Console.

Siehe "So richten Sie ein FSx für ONTAP -System ein" für detaillierte Schritte.

Einrichten von VMware Cloud on AWS SDDC

"VMware Cloud auf AWS"bietet eine Cloud-native Erfahrung für VMware-basierte Workloads im AWS-Ökosystem. Jedes VMware-Software-Defined Data Center (SDDC) läuft in einer Amazon Virtual Private Cloud (VPC) und bietet einen vollständigen VMware-Stack (einschließlich vCenter Server), NSX-T-Software-Defined Networking, vSAN-Software-Defined Storage und einen oder mehrere ESXi-Hosts, die den Workloads Rechen- und Speicherressourcen bereitstellen.

Um eine VMware Cloud-Umgebung auf AWS zu konfigurieren, befolgen Sie die Schritte in "Bereitstellen und Konfigurieren der Virtualisierungsumgebung auf AWS" Ein Pilotlichtcluster kann auch für die Notfallwiederherstellung verwendet werden.

Private Cloud

Sie können NetApp Disaster Recovery verwenden, um VMware-VMs zu schützen, die auf einem oder mehreren vCenter-Clustern gehostet werden, indem Sie VM-Datenspeicher auf einen anderen vCenter-Cluster replizieren, entweder im selben privaten Rechenzentrum oder in einem entfernten privaten oder am selben Standort befindlichen Rechenzentrum.

Installieren Sie den Konsolenagenten für On-Premises-Situationen an einem der physischen Standorte.

Disaster Recovery unterstützt die Site-to-Site-Replikation über Ethernet und TCP/IP. Stellen Sie sicher, dass ausreichend Bandbreite zur Verfügung steht, um die Datenänderungsraten auf den VMs des Produktionsstandorts zu unterstützen, sodass alle Änderungen innerhalb des RPO-Zeitrahmens (Recovery Point Objective) auf den DR-Standort repliziert werden können.

Machen Sie sich bereit für den On-Premises-zu-On-Premises-Schutz

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie NetApp Disaster Recovery für den On-Premises-zu-On-Premises-Schutz einrichten:

- ONTAP-Speicher
  - Stellen Sie sicher, dass Sie über ONTAP Anmeldeinformationen verfügen.
  - Erstellen oder überprüfen Sie Ihre Disaster-Recovery-Site.
  - Erstellen oder überprüfen Sie Ihr Ziel ONTAP SVM.
  - Stellen Sie sicher, dass Ihre Quell- und Ziel ONTAP -SVMs per Peering verbunden sind.
- vCenter-Cluster
  - Stellen Sie sicher, dass die VMs, die Sie schützen möchten, auf NFS-Datenspeichern (mithilfe von ONTAP NFS-Volumes) oder VMFS-Datenspeichern (mithilfe von NetApp iSCSI LUNs) gehostet werden.
  - Rezension"vCenter-Berechtigungen" erforderlich für NetApp Disaster Recovery.
  - Erstellen Sie ein Benutzerkonto für die Notfallwiederherstellung (nicht das standardmäßige vCenter-Administratorkonto) und weisen Sie dem Konto die vCenter-Berechtigungen zu.

Intelligente Proxy-Unterstützung

Der NetApp Console Agent unterstützt intelligente Proxys. Intelligent Proxy ist eine einfache, sichere und effiziente Möglichkeit, Ihre lokale Umgebung mit der NetApp Console zu verbinden. Es bietet eine sichere Verbindung zwischen Ihrem System und dem Konsolendienst, ohne dass ein VPN oder direkter Internetzugang erforderlich ist. Diese optimierte Proxy-Implementierung entlastet den API-Verkehr innerhalb des lokalen Netzwerks.

Wenn ein Proxy konfiguriert ist, versucht NetApp Disaster Recovery, direkt mit VMware oder ONTAP zu kommunizieren und verwendet den konfigurierten Proxy, wenn die direkte Kommunikation fehlschlägt.

Die Implementierung des NetApp Disaster Recovery -Proxys erfordert eine Kommunikation über Port 443 zwischen dem Konsolenagenten und allen vCenter-Servern und ONTAP Arrays unter Verwendung eines HTTPS-Protokolls. Der NetApp Disaster Recovery -Agent innerhalb des Konsolen-Agenten kommuniziert bei der Durchführung von Aktionen direkt mit VMware vSphere, dem VC oder ONTAP .

Weitere Informationen zur allgemeinen Proxy-Einrichtung in der NetApp Console finden Sie unter "Konfigurieren des Konsolenagenten zur Verwendung eines Proxyservers" Die

Zugriff auf NetApp Disaster Recovery

Sie verwenden die NetApp Console , um sich beim NetApp Disaster Recovery -Dienst anzumelden.

Zum Anmelden können Sie Ihre Anmeldeinformationen für die NetApp Support-Site verwenden oder sich mit Ihrer E-Mail-Adresse und einem Kennwort für eine NetApp Cloud-Anmeldung registrieren. "Erfahren Sie mehr über die Anmeldung" .

Bestimmte Aufgaben erfordern bestimmte Benutzerrollen. "Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

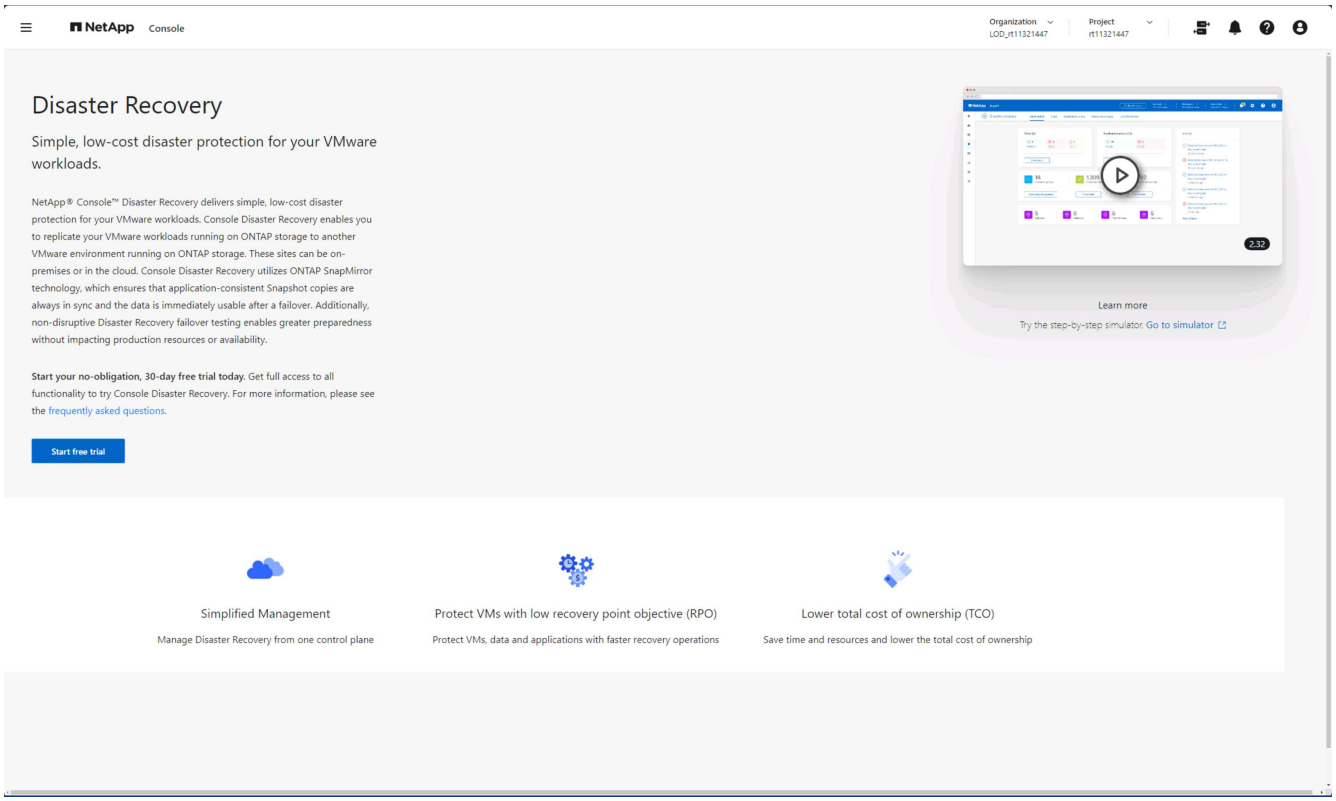
Schritte

1. Öffnen Sie einen Webbrowser und gehen Sie zu "NetApp Console" .

   Die Anmeldeseite der NetApp Console wird angezeigt.

2. Melden Sie sich bei der NetApp Console an.
3. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.

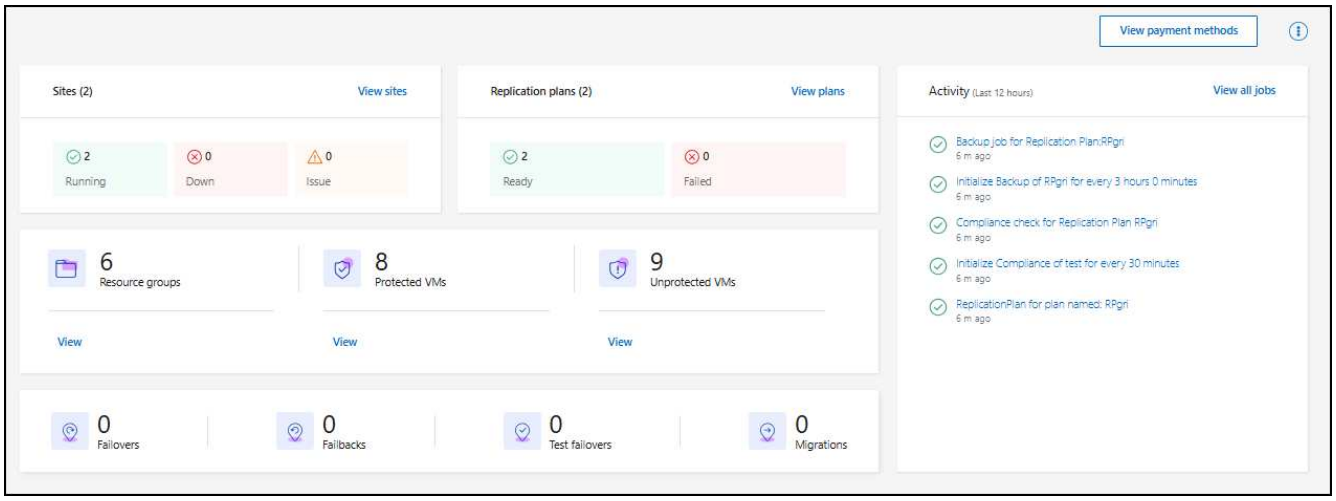
   Wenn Sie sich zum ersten Mal bei diesem Dienst anmelden, wird die Zielseite angezeigt und Sie können sich für eine kostenlose Testversion anmelden.



Andernfalls wird das NetApp Disaster Recovery Dashboard angezeigt.

- Wenn Sie noch keinen NetApp Console Agenten hinzugefügt haben, müssen Sie einen hinzufügen. Um den Agenten hinzuzufügen, siehe "Erfahren Sie mehr über Konsolenagenten" Die

- Wenn Sie ein NetApp Console mit einem vorhandenen Agenten sind und „Notfallwiederherstellung“ auswählen, wird eine Meldung zur Anmeldung angezeigt.
- Wenn Sie den Dienst bereits verwenden und „Notfallwiederherstellung“ auswählen, wird das Dashboard angezeigt.



Einrichten der Lizenzierung für NetApp Disaster Recovery

Mit NetApp Disaster Recovery können Sie verschiedene Lizenzierungspläne nutzen, darunter eine kostenlose Testversion, ein Pay-as-you-go-Abonnement oder die Nutzung Ihrer eigenen Lizenz.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator oder Notfallwiederherstellungsanwendungsadministrator.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über Zugriffsrollen für alle Dienste".

Lizenzierungsoptionen Sie können die folgenden Lizenzierungsoptionen nutzen:

- Melden Sie sich für eine 30-tägige kostenlose Testversion an.
- Erwerben Sie ein Pay-as-you-go-Abonnement (PAYGO) für den Amazon Web Services (AWS) Marketplace oder den Microsoft Azure Marketplace.
- Bringen Sie Ihre eigene Lizenz (BYOL) mit. Dabei handelt es sich um eine NetApp Lizenzdatei (NLF), die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten. Sie können die Seriennummer der Lizenz verwenden, um BYOL in der NetApp Console zu aktivieren.

> Die Gebühren für NetApp Disaster Recovery basieren auf der genutzten Kapazität der Datenspeicher am Quellstandort, wenn mindestens eine VM über einen Replikationsplan verfügt. Die Kapazität für einen ausgefallenen Datenspeicher ist nicht in der Kapazitätszuteilung enthalten. Wenn bei einem BYOL die Daten die zulässige Kapazität überschreiten, sind die Vorgänge im Dienst eingeschränkt, bis Sie eine zusätzliche Kapazitätslizenz erwerben oder die Lizenz in der NetApp Console aktualisieren.

"Mehr über Abonnements erfahren".

Nach Ablauf der kostenlosen Testversion oder der Lizenz können Sie im Dienst weiterhin Folgendes tun:

- Zeigen Sie beliebige Ressourcen an, beispielsweise eine Arbeitslast oder einen Replikationsplan.
- Löschen Sie beliebige Ressourcen, beispielsweise eine Arbeitslast oder einen Replikationsplan.
- Führen Sie alle geplanten Vorgänge aus, die während der Testphase oder unter der Lizenz erstellt wurden.

Probieren Sie es mit einer 30-tägigen kostenlosen Testversion aus

Sie können NetApp Disaster Recovery mit einer 30-tägigen kostenlosen Testversion ausprobieren.

Während der Testphase gelten keine Kapazitätsbeschränkungen.

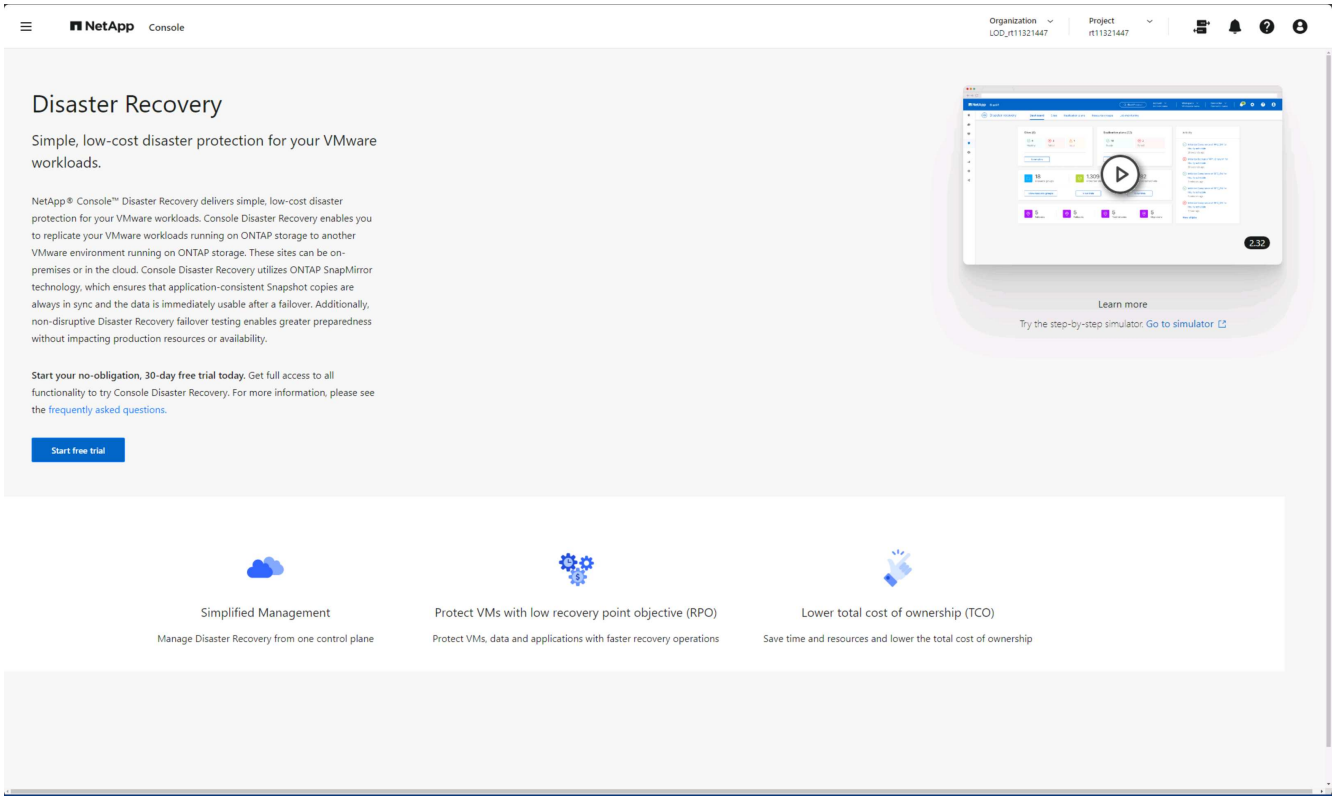
Um nach der Testphase fortzufahren, müssen Sie eine BYOL-Lizenz oder ein PAYGO-AWS-Abonnement erwerben. Sie können jederzeit eine Lizenz erwerben und es entstehen Ihnen erst nach Ablauf der Testphase Kosten.

Während der Testphase steht Ihnen die volle Funktionalität zur Verfügung.

Schritte

1. Melden Sie sich an bei "NetApp Console" .
2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.

   Wenn Sie sich zum ersten Mal bei diesem Dienst anmelden, wird die Zielseite angezeigt.



3. Wenn Sie noch keinen Konsolenagenten für andere Dienste hinzugefügt haben, fügen Sie einen hinzu.

   Informationen zum Hinzufügen eines Konsolenagenten finden Sie unter "Erfahren Sie mehr über Konsolenagenten" Die

4. Nachdem Sie den Agenten eingerichtet haben, ändert sich auf der Zielseite von NetApp Disaster Recovery

die Schaltfläche zum Hinzufügen des Agenten in eine Schaltfläche zum Starten einer kostenlosen Testversion. Wählen Sie **Kostenlose Testversion starten**.

5. Beginnen Sie mit dem Hinzufügen von vCenters.

   Weitere Informationen finden Sie unter "vCenter-Sites hinzufügen" .

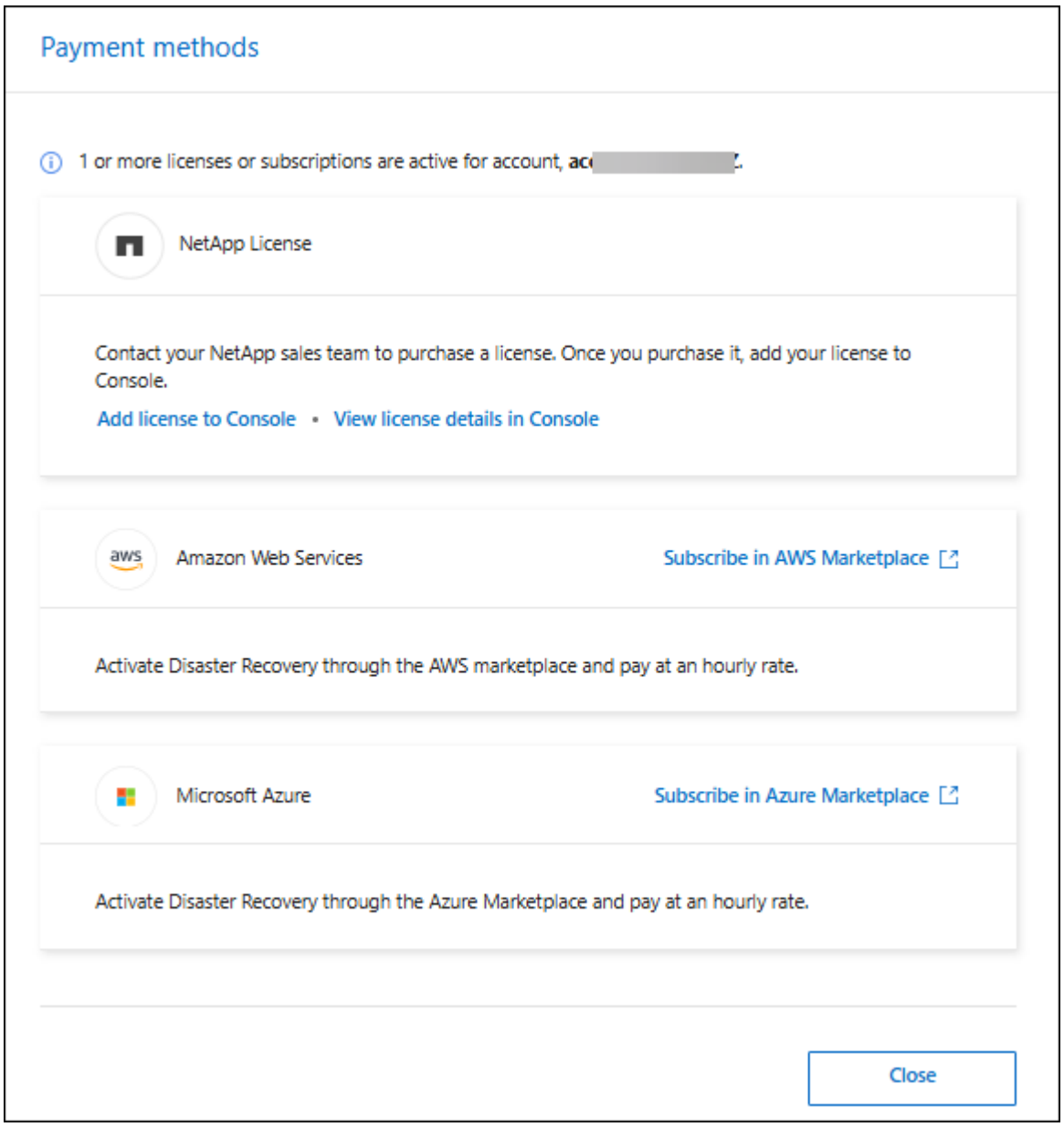
Nach Ablauf der Testphase abonnieren Sie über einen der Marketplaces

Nach Ablauf der kostenlosen Testversion können Sie entweder eine Lizenz von NetApp erwerben oder ein Abonnement über AWS Marketplace oder Microsoft Azure Marketplace abschließen. Dieses Verfahren bietet einen allgemeinen Überblick darüber, wie Sie sich direkt bei einem der Marktplätze anmelden können.

Schritte

1. In NetApp Disaster Recovery wird eine Meldung angezeigt, dass die kostenlose Testversion abläuft. Wählen Sie in der Nachricht **Abonnieren oder Lizenz kaufen** aus.

   Oder wählen Sie im die Option **Zahlungsmethoden anzeigen** aus.



2. Wählen Sie **Im AWS Marketplace abonnieren** oder **Im Azure Marketplace abonnieren**.
3. Verwenden Sie AWS Marketplace oder Microsoft Azure Marketplace, um * NetApp Disaster Recovery* zu abonnieren.
4. Wenn Sie zu NetApp Disaster Recovery zurückkehren, wird eine Meldung angezeigt, dass Sie abonniert sind.

   Sie können Abonnementdetails auf der Abonnementseite der NetApp Console anzeigen. "Erfahren Sie mehr über die Verwaltung von Abonnements mit der NetApp Console".

Nach Ablauf der Testphase können Sie über NetApp eine BYOL-Lizenz erwerben.

Nach Ablauf der Testphase können Sie über Ihren NetApp Vertriebsmitarbeiter eine Lizenz erwerben.

Wenn Sie Ihre eigene Lizenz mitbringen (BYOL), umfasst die Einrichtung den Kauf der Lizenz, das Abrufen der NetApp -Lizenzdatei (NLF) und das Hinzufügen der Lizenz zur NetApp Console.

Fügen Sie die Lizenz zur NetApp Console hinzu. * Nachdem Sie Ihre NetApp Disaster Recovery -Lizenz von einem NetApp Vertriebsmitarbeiter erworben haben, können Sie die Lizenz in der Konsole verwalten.

"Erfahren Sie mehr über das Hinzufügen von Lizenzen mit der NetApp Console".

Aktualisieren Sie Ihre Lizenz, wenn sie abläuft

Wenn sich Ihre Lizenzlaufzeit dem Ablaufdatum nähert oder Ihre lizenzierte Kapazität das Limit erreicht, werden Sie in der NetApp Disaster Recovery Benutzeroberfläche benachrichtigt. Sie können Ihre NetApp Disaster Recovery -Lizenz vor Ablauf aktualisieren, sodass Ihr Zugriff auf die gescannten Daten ohne Unterbrechung möglich ist.

Diese Meldung erscheint auch in der NetApp Console und in "Benachrichtigungen" Die

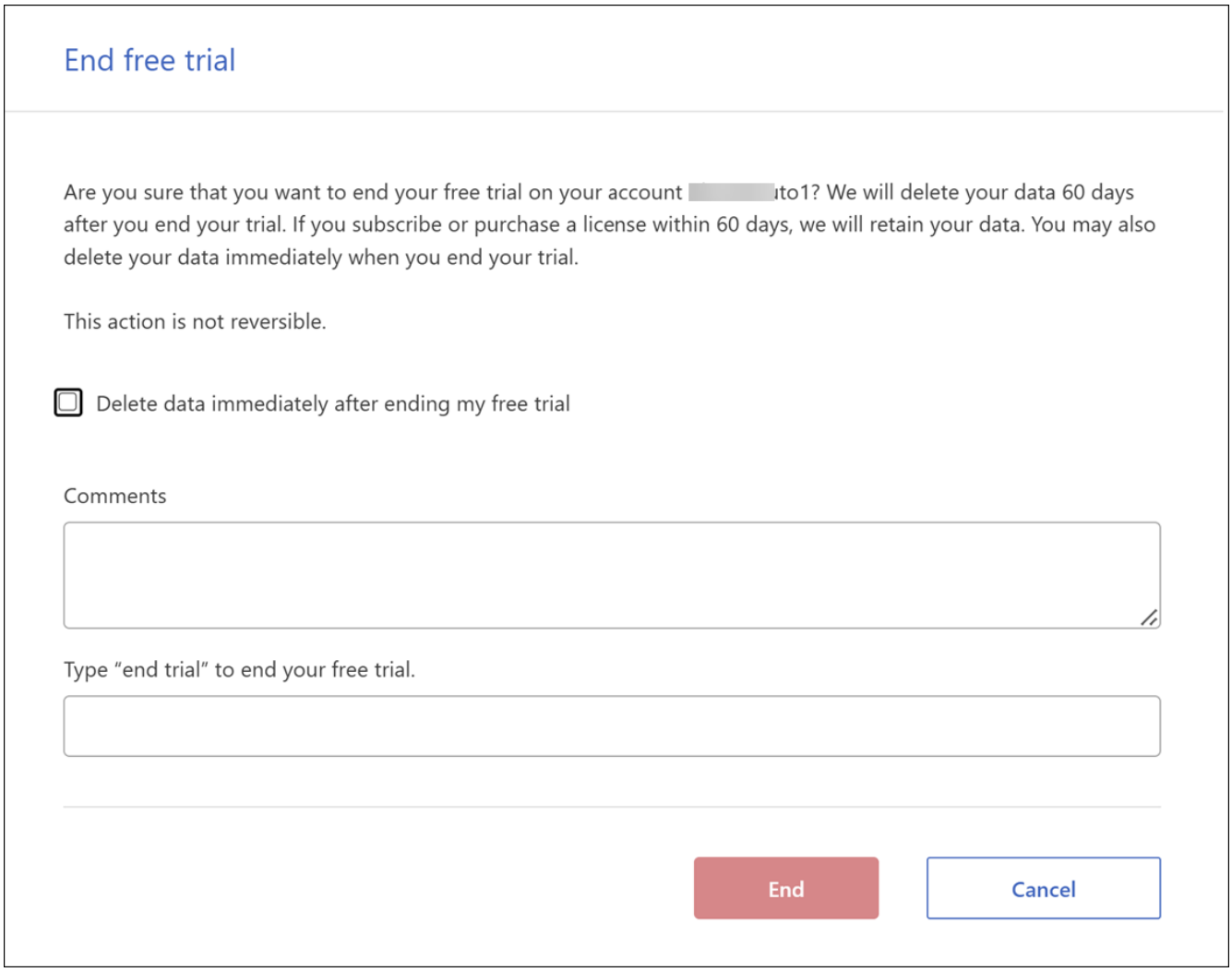
"Erfahren Sie mehr über die Aktualisierung von Lizenzen mit der NetApp Console".

Kostenlose Testversion beenden

Sie können die kostenlose Testversion jederzeit beenden oder warten, bis sie abläuft.

Schritte

1. Wählen Sie in NetApp Disaster Recovery*Kostenlose Testversion – Details anzeigen* aus.
2. Wählen Sie in den Dropdown-Details **Kostenlose Testversion beenden** aus.



3. Wenn Sie alle Daten löschen möchten, aktivieren Sie **Daten sofort nach Beendigung meiner kostenlosen Testversion löschen**.

   Dadurch werden alle Zeitpläne, Replikationspläne, Ressourcengruppen, vCenter und Sites gelöscht. Prüfdaten, Betriebsprotokolle und Auftragsverläufe werden bis zum Ende der Produktlebensdauer aufbewahrt.

   Wenn Sie die kostenlose Testversion beenden, keine Datenlöschung angefordert haben und keine Lizenz oder kein Abonnement erwerben, löscht NetApp Disaster Recovery 60 Tage nach Ablauf der kostenlosen Testversion alle Ihre Daten.

4. Geben Sie „Testversion beenden“ in das Textfeld ein.
5. Wählen Sie **Ende**.