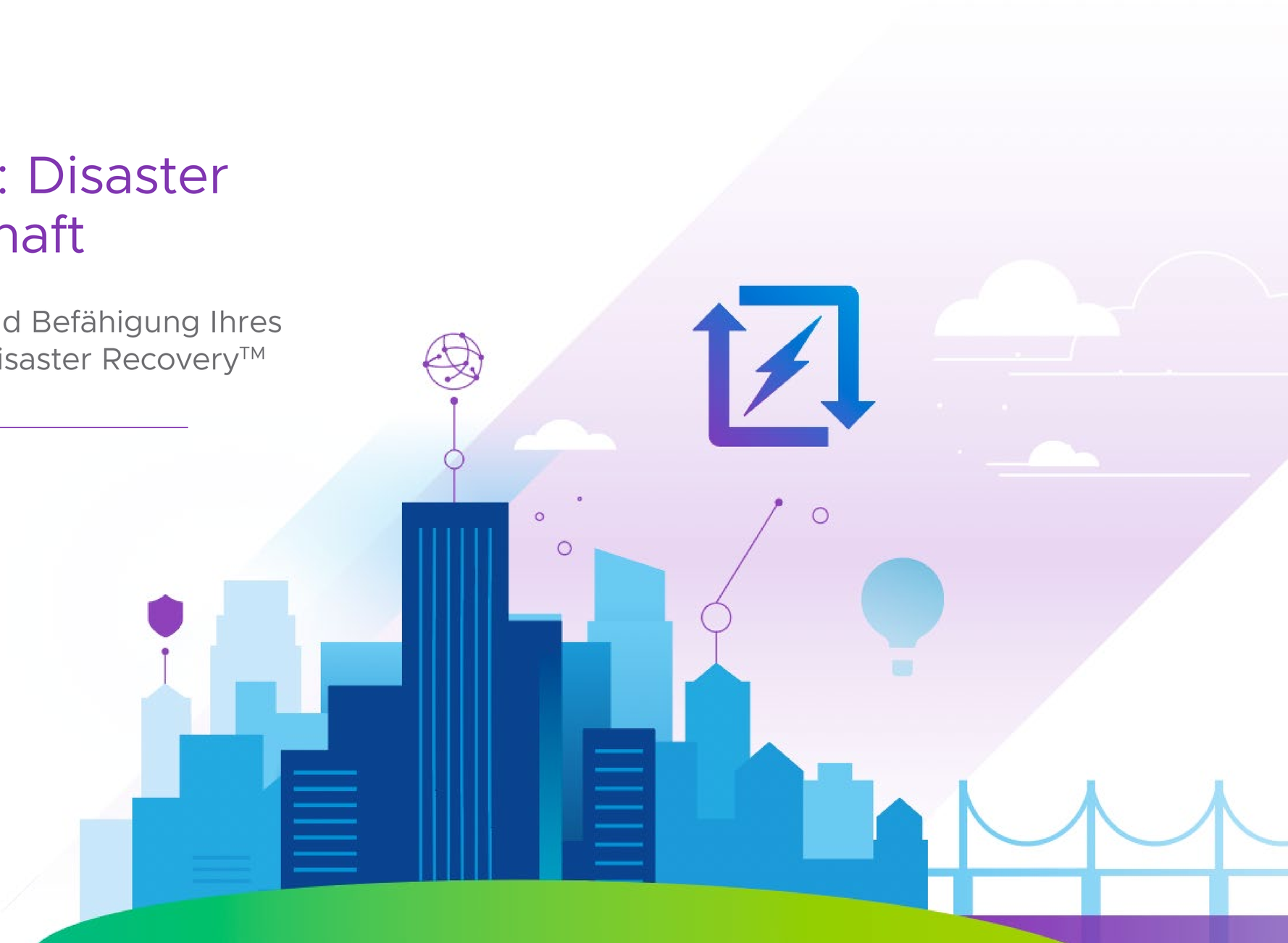
VMware-Leitfaden: Disaster Recovery-Bereitschaft

Schnellere Disaster Recovery und Befähigung Ihres DR-Teams mit VMware Cloud Disaster Recovery™



ERSTE SCHRITTE

Aufstieg von Disaster Recovery: Ist es das Gebot der Stunde?

In der heutigen Zeit ist es wichtig, im Hinblick auf Daten auf Unvorhergesehenes vorbereitet zu sein. Doch langfristige Probleme lassen sich nicht mit kurzfristigen Lösungen beheben. Datenschutz ist zu einer gemeinsamen Verantwortung geworden und Disaster Recovery ist die letzte Verteidigungslinie, wenn alles andere versagt. Als solche sollte sie als eine Geschäftsentscheidung behandelt werden, die die Zukunft Ihres Unternehmens beeinflussen kann.

Ist Disaster Recovery für Sie erfreuliche Realität oder bereitet sie Ihnen schlaflose Nächte? Hier erfahren Sie, warum Sie über Disaster Recovery nachdenken sollten:

Schon gewusst?

250.000 USD
pro Stunde kosten Unternehmen Ausfallzeiten im Durchschnitt.[1]

76%
haben in den vergangenen zwei Jahren einen Vorfall gemeldet, der einen DR-Plan erforderte.[2]

75%
haben ihre Strategien für Datensicherheit und Recovery aufgrund von COVID-19 geändert.[3]

Nach einem Angriff ist die Anspannung groß und je weniger spontane Überlegungen angestellt werden müssen, desto besser.

1. Enterprise IT Infrastructure Survey von IDC: „Insights on End-User 2021 IT Infrastructure Priorities and Adoption of Data Protection/Disaster Recovery Services and Solutions“, 4. Quartal 2020
2. Gartner: „Survey Analysis: IT Disaster Recovery Trends and Benchmarks“, J. Rozeman, R. Blair, 30. April 2020
3. Enterprise IT Infrastructure Survey von IDC: „Insights on End-User 2021 IT Infrastructure Priorities and Adoption of Data Protection/Disaster Recovery Services and Solutions“, 4. Quartal 2020

DRaaS oder herkömmliche DR: Fundierte Entscheidungsfindung

Disaster Recovery as a Service (DRaaS) oder herkömmliche On-Premises-DR?

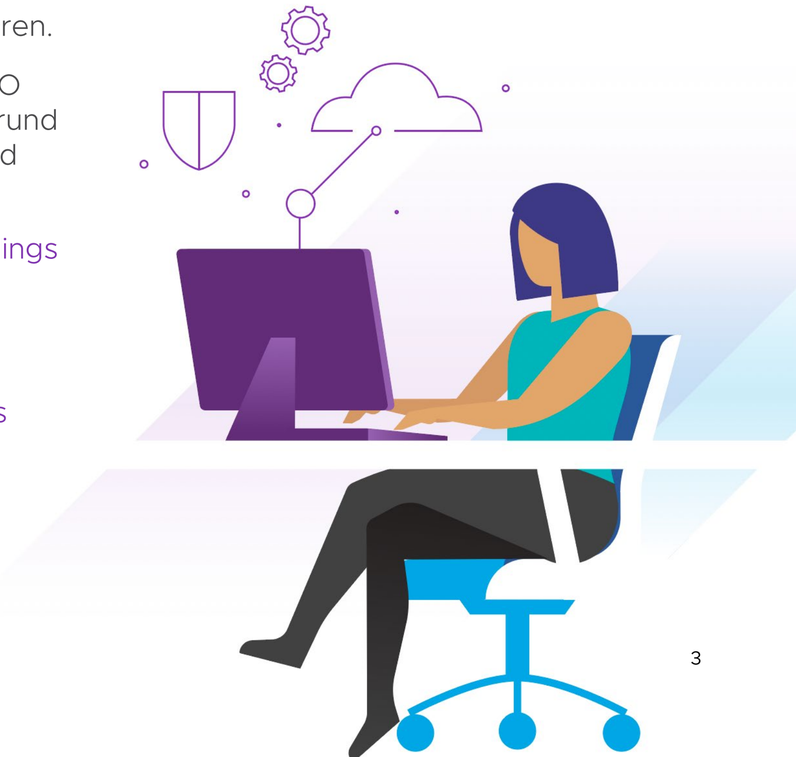
Angesichts der rasanten Entwicklung der Disaster Recovery ist ein getesteter und bewährter DR-Plan von entscheidender Bedeutung, damit Unternehmen ihre Geschäftstätigkeit aufrechterhalten können. Informieren Sie sich über die Unterschiede zwischen DRaaS und herkömmlicher DR, um die für Ihre Anforderungen geeignete Entscheidung zu treffen.

DRaaS (Disaster Recovery as a Service)

- OpEx-intensiv: Keine Erstinvestition in Hardware
- Kein Lebenszyklusmanagement: Automatische Aktualisierung ohne manuelle Eingriffe und ohne komplizierte Erneuerungen
- Unterbrechungsfreie Tests: Optimierte DR-Abläufe und mehr Vertrauen in Recovery
- Bis zu 60% niedrigere TCO im Vergleich zu herkömmlicher DR *Weitere Informationen*
- Erfüllt die meisten SLA-Anforderungen für Workloads.
- SaaS-basierter Service abstrahiert die Komplexität von DR-Betriebs- und Wartungsaufgaben.
- Vom Anbieter verwaltete Lösungen reduzieren die für den Betrieb erforderlichen IT-Ressourcen auf ein Minimum.

Herkömmliche DR (On-Premises)

- CapEx-intensiv: Erfordert Vorabinvestitionen in Hardware, die sich dann im Laufe der Zeit amortisieren.
- Ist für Workloads mit strengsten SLAs (RTO und RPO unter 5 Minuten) geeignet oder für solche, die aufgrund von Compliance-Vorschriften noch nicht in der Cloud gespeichert werden können.
- Kann nahezu sofortiges RPO und RTO bieten, allerdings zu einem erhöhten Preis. *Weitere Informationen*
- Zum Testen muss der Produktionsstandort heruntergefahren werden, um einen Failover durchzuführen. Dies erhöht die Belastung durch das Testen und führt zu geringerer Testhäufigkeit – ein maßgeblicher Problembereich bei der DR-Implementierung.
- Vom Kunden verwaltete Lösungen sind u.U. sehr arbeitsaufwendig.

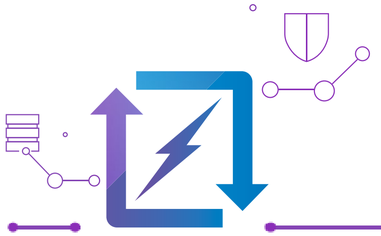


DRaaS oder herkömmliche DR: Fundierte Entscheidungsfindung

Sie müssen nicht nur über eine DR-Strategie verfügen, sondern diese muss auch funktionieren. Vielleicht haben Sie bereits einen Plan implementiert, aber wie oft testen Sie ihn? Wie sicher sind Sie sich, dass Sie Daten nach einem Zwischenfall wiederherstellen können?

Expertentipps

Einfache, unterbrechungsfreie Tests sind ein unverzichtbarer Bestandteil bei der Datenwiederherstellung. Erstellen Sie einen Plan und testen Sie ihn häufig. Wenn Sie Ihre DR-Vorgänge planen und testen, können Sie Ihre Daten im Bedarfsfall nahtlos wiederherstellen.



Erfahren Sie, wie sich die Kosteneffizienz von VMware Cloud DR auf Ihre Umgebung auswirkt. Sehen Sie sich unser TCO-Tool an.

Die fünf entscheidenden Schritte zur DR-Bereitschaft

Schon gewusst?

Nur 38%

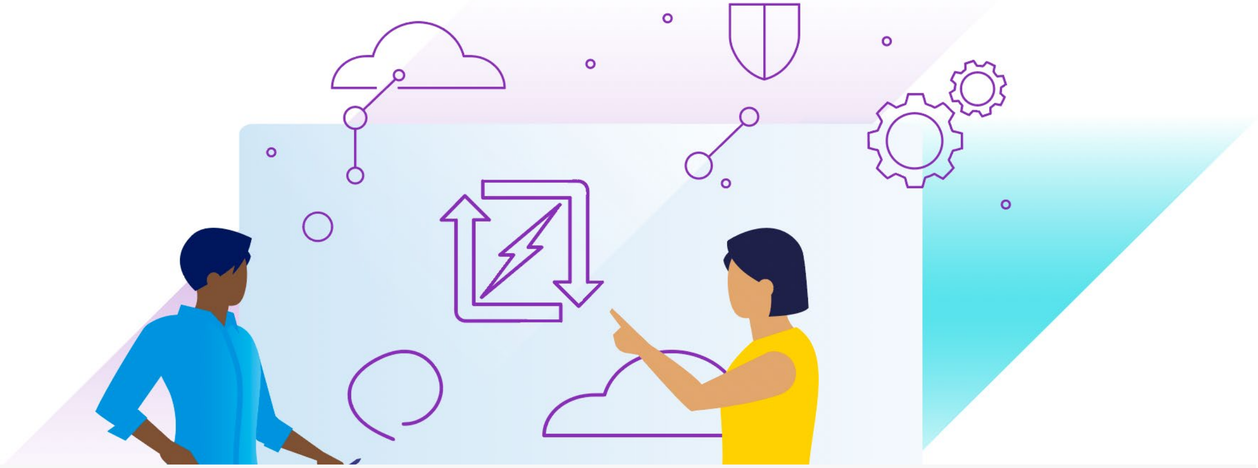
testen ihren DR-Plan öfter als zweimal pro Jahr.[1]

1. Umfrage „Voice of the Enterprise“ zu Disaster Recovery von 451 Research, 2021

Tag 1: Planen

Der erste Schritt zur DR-Bereitschaft: Planen. Am Anfang steht das Verständnis Ihres Datenbestands. Was Sie nicht sehen, können Sie nicht schützen. In diesem Schritt ordnen Sie Anwendungen zu, wählen SLAs aus und katalogisieren Ihre On-Premises-Infrastruktur. Wenn Sie dies richtig machen, sparen Sie später Zeit und Ressourcen.

Nicht alle Ihre Anwendungen haben dieselben SLA- oder Aufbewahrungsanforderungen. Aus diesem Grund ist dieser Vorgang iterativ und auf VM-Ebene anpassbar, basierend auf den von Ihnen erstellten Schutzgruppen und den entsprechenden Recovery-Zeiten. Dies ist auch eine Business-Entscheidung: Welchen Schutz benötigen Ihre Workloads und wie können Sie die Ressourcen, die Sie Ihren DR-Abläufen zuweisen, ohne Abstriche bei der Zuverlässigkeit optimieren? Hier erweist sich eine anpassbare Lösung als vorteilhaft.



Expertentipps

Legen Sie fest, was Sie schützen wollen. Ordnen Sie dazu Ihre Anwendungen zu und organisieren Sie Ihre On-Premises-Infrastruktur. Stellen Sie sich dann folgende Fragen:

- Über welche kritischen Anwendungen verfügen Sie?
- Welche Anwendungen stellen Sie wieder her?
- Welche Anwendungsabhängigkeiten bestehen?
- Wie oft muss jede VM auf den Cloud-basierten Service repliziert werden?
- Wie lange müssen unveränderliche, Cloud-basierte Snapshots aufbewahrt werden?
- Welche SLAs benötigen Sie für verschiedene Workload-Stufen? Geringere RPO- und RTO-Anforderungen wirken sich direkt auf die Kosten aus. Daher sollten Sie hier die von Ihrem Unternehmen benötigten SLAs mit den TCO abstimmen und Ihren Workloads den Schutz zuweisen, der erforderlich ist, um den Wert Ihrer DR-Lösung zu maximieren. Wie wird das erreicht? Mit einem mehrstufigen DR-Ansatz

Tag 2: Definieren

Es ist an der Zeit, den Umfang Ihrer DR-Pläne zu definieren. Jetzt haben Sie Ihre Infrastruktur katalogisiert, Ihre kritischen Anwendungen identifiziert und wissen, welche Abhängigkeiten bestehen. Im nächsten Schritt erstellen Sie DR-Standorte über die intuitive webbasierte UI auf, indem Sie auf die entsprechende Registerkarte zugreifen. Anschließend erstellen Sie Schutzgruppen. Wählen Sie die VMs aus, die Sie schützen möchten, indem Sie eine nahtlose tagbasierte Suche durchführen. Richten Sie eine Testschutzgruppe ein (hierbei sind die SLAs, die Sie an Tag 1 ausgewählt haben, von entscheidender Bedeutung). Sobald Sie sich vergewissert haben, dass Ihre Testschutzgruppe funktioniert, beginnen Sie damit, manuelle Snapshots aller verbleibenden Schutzgruppen zu erstellen – die sogenannte Datenreplikation. Dies ist der erste Schritt in Richtung einer erfolgreichen Recovery.

Expertentipps

Stellen Sie sich die folgenden Fragen, wenn Sie Ihre Schutzgruppen definieren möchten:

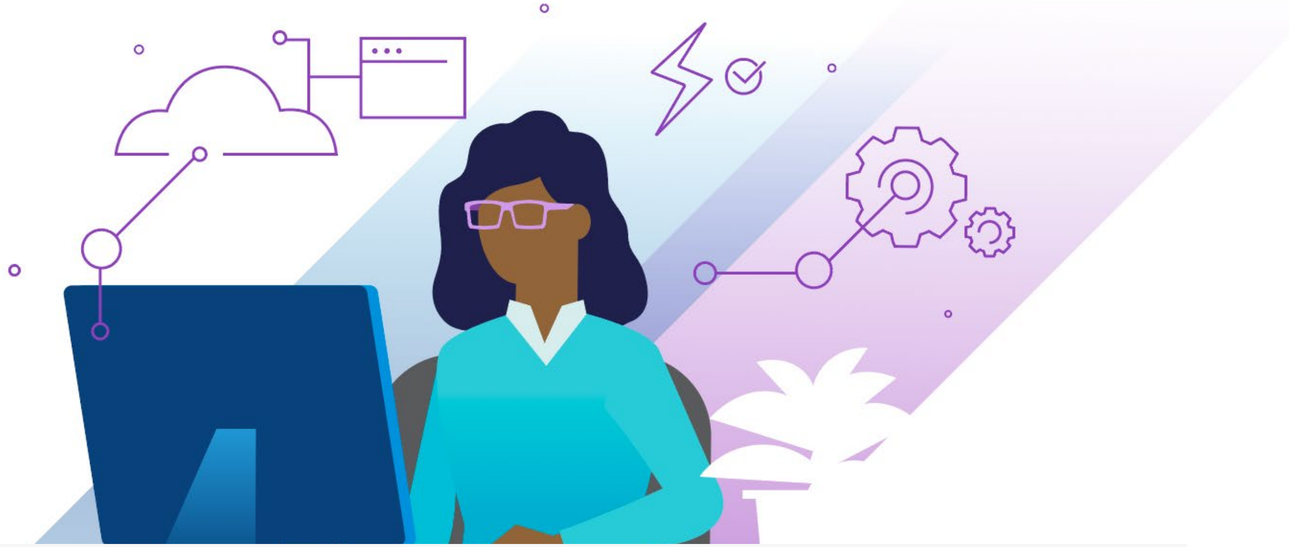
- Richten Sie Ihre Schutzgruppen an den Recovery-Zielen aus. Benötigen Sie eine detaillierte Recovery?
- Wie sieht Ihr Schutzzeitplan aus?
- Wie lange werden die geschützten Daten aufbewahrt? (Dies wirkt sich auf Ihre TCO aus.)

Tag 3: Konfigurieren

Ein DR-Plan wurde erarbeitet und Ihre Schutzgruppen wurden erstellt. Was nun? Sie benötigen einen Standort für den Failover, daher besteht der nächste Schritt darin, das Recovery-SDDC zu erstellen. Sobald dies geschehen ist, führen Sie einen Cloud-Test durch. Richten Sie den Produktions- und den DR-Standort so ein, dass Sie über einheitliche, vertraute Abläufe verfügen, was in der Regel als Abgleich der Standorte bezeichnet wird.

Nachdem nun beide Standorte bereitgestellt sind, erstellen und testen Sie Ihre DR-Pläne. Wählen Sie die Schutzgruppen aus und legen Sie den vCenter-Ordner, die Computing-Ressourcen und die virtuellen Netzwerkzuordnungen fest. Das Tool bietet eine Anleitung, sodass keine IT-Kenntnisse erforderlich sind.

Sobald Schutzgruppen erstellt und an Ihre DR-Pläne angepasst sind, sind Sie bereit für Tag 4.



Expertentipps

- Wenn Sie Pläne erstellen und Zuordnungen vornehmen, testen Sie diese zunächst gründlich in einer kleinen SDDC-Umgebung.
- Mehrstufiger DR-Ansatz: Falls Sie RTO minimieren möchten, nutzen Sie den Pilot Light-Modus. Sie müssen dann nicht mehr darauf warten, dass das DR-SDDC bereitgestellt wird.
- Um den Ransomwareschutz zu verbessern, richten Sie ein isoliertes Netzwerk in Ihrem SDDC ein. So können Sie alle Backup-Snapshots unter Quarantäne stellen und testen, bevor Sie Failover durchführen. Auf diese Weise können Sie Ihre Snapshots in einer abgeschirmten Umgebung sicher auf Malware testen, bevor Sie ein Failover Ihrer gesamten Umgebung durchführen.
- Dokumentieren Sie Ihre Zuordnungen und bewahren Sie diese Informationen zusammen mit Ihren Runbooks und Konfigurationstest-Reports auf.

Tag 4: Testen

Sobald Schutzgruppen erstellt sind, ist es an der Zeit, den Failover durchzuführen. Doch zunächst müssen Sie Ihre Pläne testen. Das Testen ist einfach, unterbrechungsfrei und bildet den Eckpfeiler Ihrer DR-Strategie. Wenn Sie den Test ausführen, wird das Recovery-SDDC mit Anwendungen gefüllt. Nachdem der Test korrekt durchgeführt wurde, bereinigt der SaaS-Orchestrator die Testumgebung. Greifen Sie über die UI auf Ihre DR-Test-Reports zu und stellen Sie Ihre DR-Failover-Pläne unterbrechungsfrei bereit.

Expertentipps

- Beim Bereitstellen im Pilot Light-Modus ist diese Vorgehensweise schneller, da nicht gewartet werden muss, bis das Failover-SDDC bereitgestellt wird. Für kritische Anwendungen sollten Sie daher Pilot Light als Teil Ihres mehrstufigen DR-Konzepts in Betracht ziehen.
- Sie können VMs und Dateien im Cloud-Dateisystem belassen, falls Sie Ihre Pläne nur testen wollen, ohne einen vollständigen Failover durchzuführen.
- Hier validieren Sie Ihre Schutzgruppen und optimieren Detailgenauigkeit und Häufigkeit der Replikation auf den Cloud-basierten Service. Wiederholen Sie diesen Vorgang, bis Ihre Schutzgruppen Ihren DR-Anforderungen entsprechen.

Tag 5: Betreiben

Sie haben Tag 5 erreicht! Dies sind Ihre heutigen Aufgaben, damit Sie für den Betrieb gerüstet sind.

Überprüfen Sie den Fortschritt der Schutzgruppen und stellen Sie sicher, dass alles ordnungsgemäß läuft. Als nächstes greifen Sie auf das Überwachungs-Dashboard zu und überprüfen die allgemeinen DR-Bedingungen. Zu guter Letzt erstellen Sie Reports über die Audit-Compliance. Diese dienen als Nachweis, dass Ihre DR-Pläne getestet und korrekt ausgeführt werden.

Expertentipps

- Löschen Sie das SDDC, das Sie für Ihre Tests bereitgestellt haben, um eine maximale Kostenoptimierung zu erreichen. Falls Sie den Pilot Light-Modus verwenden, können Sie diese SDDCs auch für andere Zwecke einsetzen, um den Nutzen Ihrer Cloud-Umgebung zu maximieren.
- Überprüfen Sie Ihre DR-Reports und gleichen Sie sie mit Ihren erforderlichen SLAs ab. Möglicherweise müssen Sie Ihre Schutzgruppen ändern oder Anpassungen vornehmen.

Ausschöpfen des DRaaS-Potenzials mit VMware Cloud DR

Nutzen Sie bedarfsorientierte Disaster Recovery als SaaS-Lösung mit Cloud-Ökonomie. Erfahren Sie, wie Sie dank VMware Cloud DR Ihr Unternehmenswachstum mit intelligenter DR vorantreiben können.

Vergleichen Sie DRaaS und herkömmliche DR für Ihre Umgebung mit unserem TCO-Tool

Flexible Bereitstellungsoptionen

Sie können flexibel zwischen verschiedenen Bereitstellungsoptionen wählen und Failover-Kapazitäten zu 100% bedarfsorientiert oder mit geringem Ressourcenbedarf über den Pilot Light-Modus einrichten.

Optimierte Kosten

Nutzen Sie die Elastizität und Zuverlässigkeit der Cloud, um wirksame DR-Abläufe und optimierte IT-Ressourcenzuweisung miteinander in Einklang zu bringen und so bis zu 60% niedrigere Gesamtbetriebskosten zu erzielen.

Einheitliche Abläufe dank VMware

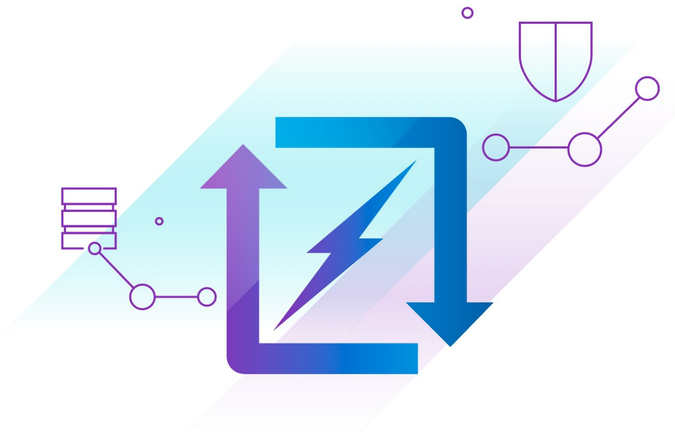
Optimale Anwenderfreundlichkeit: Nutzen Sie einheitliche Abläufe On-Premises und in der Cloud durch Automatisierung von Failover und Failback.

Funktionen

Optimieren Sie Ihre Disaster Recovery-Pläne mit VMware Cloud Disaster Recovery-Lösungen:

- **Pilot Light:** Stellen Sie einen kleinen Teil der Failover-Kapazität in der Cloud bereit und skalieren Sie bedarfsorientiert.
- **Instant Power-on:** Wenn Sie Ihre DR-Pläne testen oder orchestrieren, können Sie Ihre VMs in der Cloud sofort einschalten.
- **Unveränderliche Snapshots:** Schützen Sie Ihre Daten mithilfe eines umfassenden Verlaufs unveränderlicher Snapshots vor Malware.
- **Kontinuierliche DR-Systemdiagnosen:** DR-Systemdiagnosen sind für die Recovery nach Ransomware unerlässlich und werden alle 30 Minuten ausgeführt.
- **Deltabasierter Failback:** Minimieren Sie Egress-Gebühren für Cloud-Daten und optimieren Sie DR-Betriebskosten.
- **Detaillierte DR-Reports:** Erbringen Sie den Nachweis, dass DR-Pläne getestet und ordnungsgemäß ausgeführt werden.

Modernisieren Sie Ihre bestehende DR, optimieren Sie Betriebskosten und beschleunigen Sie die Recovery von Ransomware mit **VMware Cloud DR**.



Schneller zu Disaster Recovery mit VMware

Beim Definieren und Implementieren Ihrer DRaaS-Strategie gibt es viele Variablen, daher ist ein gezieltes Vorgehen erforderlich. Sie benötigen die entsprechenden Ressourcen (Personal und Zeit), um Ihre Lösung bereitzustellen und zu überprüfen.

VMware Professional Services können Sie dabei unterstützen, Ihre DRaaS-Implementierung zu optimieren und zu beschleunigen. Wir können eine umfassende Disaster Recovery-Strategie erstellen und implementieren, die Ihre RPO- und RTO-Ziele erfüllt, den Zeitraum bis zum Schutz verkürzt und DR-Abläufe vereinfacht. Wir verwenden einen bewährten, skalierbaren und wiederholbaren Ansatz, um die Wirksamkeit Ihrer Implementierung sicherzustellen, und bieten kontinuierliche Prozesse, mit denen Sie DR-Pläne fortlaufend überprüfen und Konfigurationsabweichungen mit einer hohen Erfolgsquote beheben können.

VMware Professional Services

Jetzt durchstarten

Annahmen

1. Unter der Annahme, dass eine 1-Gbit/s-Verbindung zu AWS eine Datenrate von etwa 10 TB/Tag bietet, können maximal ungefähr 20 TB in 2 – 3 Tagen geschützt werden, um den Schutz der zu testenden VMs zu erzielen.
2. Beinhaltet keine umfassende Überarbeitung des Standorts mit dem Ziel, Anwendungen in einer Hybrid Cloud-Umgebung auszuführen. Betrifft eher NSX/HCX/VMC/AWS und liegt außerhalb des Rahmens dieses Angebots.
3. Es wird davon ausgegangen, dass Netzwerkverbindungen zwischen On-Premises und Cloud hergestellt wurden und dass das Team über alle erforderlichen Berechtigungen und den nötigen Zugriff verfügt, um Aufgaben durchzuführen.
4. Beinhaltet keine Änderungen der Kerninfrastruktur mit dem Ziel, den hybriden oder reinen Cloud-Betrieb zu unterstützen (z.B. DNS, DHCP, Lastausgleich, VPN, Firewalls usw.).
5. Beinhaltet keine Anpassungen der Skript-VM für den DR-Plan. Beispiel: Eine Skript-VM kann in die Vorbereitungs- und Testphase aufgenommen werden.

Jetzt durchstarten

Erfahren Sie mehr darüber, wie Sie Ihre Cloud-basierte Disaster Recovery-Strategie dank VMware Cloud DRaaS Services schneller erstellen und implementieren können.

Weitere Informationen