

Carbonite[®] Recover

Gewährleisten Sie für Top-Tier-Systeme mittels Ausfallsicherung auf Knopfdruck einen höheren Grad an Verfügbarkeit.

Die Uhr beginnt zu ticken, sobald ein kritisches Geschäftssystem ausfällt. Wenn die Umsatzverluste zunehmen und die Produktivität sinkt, ist die Wiederaufnahme des normalen Betriebs von größter Bedeutung.

Der schnellste Weg zur Wiederherstellung besteht in der Migration des Workloads zu einem anderen Server, häufig an einem sekundären Standort. Für die meisten Unternehmen sind redundante Hardware, Serverplatz und zusätzliche Humanressourcen jedoch viel zu kostspielig, um dies zu einer tragfähigen Option zu machen. Angesichts potenziell verheerender Ausfälle leben viele IT-Abteilungen einfach mit dem Risiko oder geben sich mit kostengünstigeren Sicherungsoptionen für kritische Workloads zufrieden.

Die Lösung ist Carbonite Recover – eine von Carbonite gehostete Disaster-Recovery-Lösung. Durch die sichere Replikation kritischer Systeme aus Ihrer primären Umgebung zur Cloud stellt Carbonite Recover sicher, dass jederzeit eine aktuelle sekundäre Kopie für den Failover verfügbar ist, wodurch Ausfallzeiten und Kosten minimiert werden.

Während weniger kritische Workloads durch herkömmliche Sicherungen gesichert werden, sorgt Carbonite Recover für die Verfügbarkeit von Systemen, die für kritische Geschäftsvorgänge unerlässlich sind, unabhängig davon, was an der Quelle geschieht.

Echtzeitreplikation und Ausfallzeiten nahe null

Mit Carbonite Recover erfolgt die Replikation vom primären Server zur Cloud kontinuierlich auf Byte-Ebene. Die Replikation am sekundären Cloud-Standort wird ständig mit der Quelle synchronisiert, um die Aktualität der Daten sicherzustellen. Zu dieser Cloud-basierten Replikation ist ein sofortiger Failover möglich, wenn der Fehlerschwellenwert erreicht wurde. Die gesamte Ausfallzeit (oder RTO) wird in Minuten gemessen. Das Wiederherstellungsziel (RPO) beträgt nur wenige Sekunden, wodurch geschäftliche Auswirkungen des Ausfalls praktisch ausgeschlossen werden.

Für komplexe IT-Umgebungen entwickelt

Das Failover eines einzelnen Servers ist ziemlich einfach. Die meisten Systeme bestehen jedoch aus voneinander abhängigen mehrschichtigen Anwendungen. Carbonite Recover unterstützt die wichtigsten Anforderungen komplexer IT-Umgebungen, darunter:

- **Orchestrierung** – Mehrschichtige Anwendungen haben häufig eine bestimmte Startreihenfolge und stellen zusätzliche Anforderungen in Bezug auf eine benutzerdefinierte Automatisierung, damit die Anwendung ordnungsgemäß wiederhergestellt wird. Die in Carbonite Recover integrierte Orchestrierung und Automatisierung unterstützen zusammen mit benutzerdefinierten Skriptpunkten diese komplexen Anwendungsfälle über mehrere Servergruppen hinweg.
- **Leistung und Bandbreite** – Durch die kontinuierliche Übertragung winziger Datenmengen minimiert Carbonite Recover die Auswirkungen auf die Leistung, sowohl für die Server, die geschützt werden, als auch für das Netzwerk.
- **Sicherheit** – Alle Daten werden während der Übertragung und im Ruhezustand durch AES-256-Verschlüsselung gesichert.



Wichtigste Vorteile

- Wiederherstellungszeiten und Wiederherstellungspunkte gemessen in Minuten oder Sekunden
- Orchestrierung für mehrschichtige Anwendungen mit Startreihenfolge, Skripterstellung und automatisierter Erkennung der Systeme in Ihrer Umgebung
- Unterbrechungsfreie Self-Service-Tests
- Bandbreitenoptimierung zur Begrenzung der Auswirkungen auf das Netzwerk
- Integrierte Verschlüsselung im Ruhezustand und während der Übertragung
- Technischer Support von Carbonite von der anfänglichen Bereitstellung über Tests bis zu Failover und Failback
- Unterstützung für exotische Plattformen wie iSeries und AIX mit unserer Carbonite[®] Disaster Recovery-Lösung

Unterstützte Plattformen

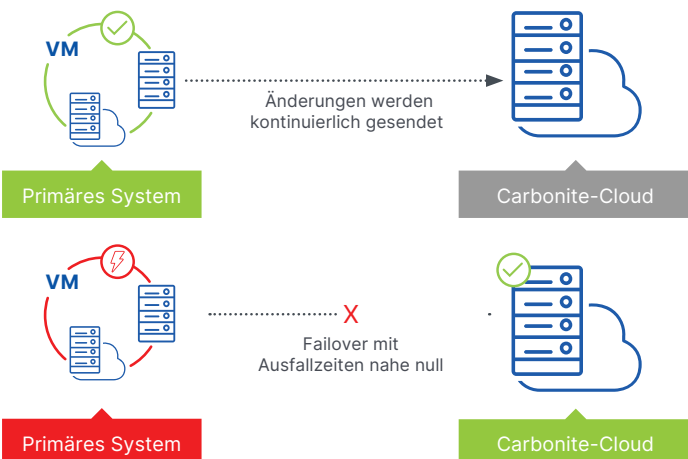
- Windows
- Red Hat Enterprise Linux
- CentOS
- VMware und Hyper-V

- **DNS** – Nach dem Failover Ihrer Systeme automatisiert Carbonite Recover DNS-Updates, um Ihre Benutzer nahtlos zu den neuen Systemen umzuleiten.
- **Optimierte Verwaltung** zum Anzeigen und Bearbeiten des Auftragsstatus und zum Erstellen von Ausschlussrichtlinien zur Optimierung der Schutzleistung.
- **Vorinstalliertes VPN** – Durch die Aufrechterhaltung einer VPN-Verbindung zu Ihrem Produktionsnetzwerk werden die Schritte zum Herstellen einer Verbindung zu Ihren Cloud-Workloads bei einem Ausfall vereinfacht.

Tests, die Vertrauen schaffen

Bei einem Ausfall oder einer Katastrophe ist das Vertrauen in Ihre Datenschutzsysteme von kritischer Bedeutung. Ohne sie lösen viele Organisationen keine Katastrophenverfahren aus, wodurch sie exponiert bleiben.

Der beste Weg, dies zu mildern, sind regelmäßige Tests, die jederzeit mit Carbonite Recover ausgeführt werden können. Diese Self-Service-Tests unterbrechen den Betrieb nicht. Außerdem steht unser Kundensupport-Team zur Verfügung, um auftretende Probleme zu untersuchen. Carbonite Recover kann einen Failover-Bericht generieren, der den Echtzeitstatus und den Erfolg von Live- und Test-Failovers bereitstellt und zeigt, dass die Wiederherstellungsumgebung wie erwartet funktioniert. Die besten Geschäftskontinuitätspläne werden einmal pro Quartal getestet. Daher haben wir die Lösung so entwickelt, dass regelmäßige Tests nach Ihren Wünschen unterstützt werden.



Funktionsweise

Zunächst melden Sie sich bei der Konsole an. Anschließend überträgt die Lösung die Agenten, die die Replikation ausführen, auf die zu schützenden Systeme. Anschließend wird der Dienst konfiguriert. Nach der Konfiguration senden Ihre Systeme kontinuierlich Daten an die Carbonite-Cloud. Da dies auf Byte-Ebene erfolgt, werden die Auswirkungen auf die Leistung der Systeme oder des Netzwerks minimiert.

Bei einem Ausfall können Sie einen Failover über die Carbonite-Konsole auslösen. Innerhalb weniger Minuten werden die sekundären Systeme in der Cloud gestartet und sind einsatzbereit. Die Daten auf ihnen sind nur wenige Sekunden alt. Die meisten Benutzer bemerken noch nicht einmal eine Dienstunterbrechung.

Sobald Sie bereit sind, einen Failback zu Ihren primären Systemen auszuführen, kann der Prozess leicht umgekehrt werden. Carbonite Recover wird von unserem herausragenden technischen Team unterstützt, das die Funktionsfähigkeit Ihres Datenschutzplans sicherstellt und Sie bei einem Ausfall unterstützt.

Carbonite® Recover mit Carbonite® Managed Disaster Recover Service

Unternehmen, die einen stärker verwalteten Service-Ansatz benötigen, können Carbonite Recover mit dem Carbonite Managed Disaster Recovery-Dienst kombinieren. Dieser White-Glove-Dienst umfasst nicht nur die anfängliche Einrichtung und die Bereitstellung der Software, sondern unterstützt auch die kontinuierliche Verwaltung und Validierung der ordnungsgemäßen Funktion der Disaster-Recovery-Lösung, um sicherzustellen, dass das Unternehmen im Katastrophenfall online geschaltet werden kann.

Nehmen Sie Kontakt mit uns auf, um mehr zu erfahren – Carbonite EMEA

E-Mail: carb-salesemea@opentext.com

Telefon: Frankreich: +33 1 47 96 55 41 | Deutschland: +49 2162 91980 20 | Niederlande: +31 73 648 1400 | UK: +44 333 1234 200

Für alle anderen Länder wählen Sie bitte: +44 333 1234 200

Über Carbonite und Webroot

Carbonite und Webroot, beides OpenText-Unternehmen, nutzen die Cloud und künstliche Intelligenz, um Unternehmen, einzelnen Personen und Managed Services-Anbietern umfassende Lösungen für eine größere Cyberresilienz anzubieten. Cyberresilienz bedeutet, dass Systeme trotz Cyberangriffen und Datenverlusten jederzeit aktiv und betriebsbereit sind. Mit diesem Ziel haben wir unsere Kräfte gebündelt, um Endpunktschutz, Netzwerkschutz, Schulungen zur Steigerung des Sicherheitsbewusstseins, Datensicherungs- und Notfallwiederherstellungslösungen sowie Threat-Intelligence-Services bereitzustellen, die von marktführenden Technologieanbietern weltweit verwendet werden. Webroot nutzt die Leistungsstärke des Machine Learning für den Schutz von Millionen von Unternehmen und Einzelpersonen und sichert die vernetzte Welt. Carbonite und Webroot sind weltweit in Nordamerika, Europa, Australien und Asien tätig. Unter carbonite.com und webroot.com erfahren Sie mehr über Cyberresilienz.