



Datensicherung und Systemverfügbarkeit an dezentralen Standorten

Bennett Klein, Sr. Director Product Marketing

Für die Sicherung von Daten und die Verfügbarkeit in Zweigniederlassungen gibt es viele Ansätze. Dieses White Paper befasst sich mit den Best Practices bei der Verwendung der heute verfügbaren Technologien für den Schutz, die Wiederherstellung und die Verfügbarkeit von Systemen, Anwendungen und Daten an dezentralen Standorten oder in Zweigniederlassungen.

ARCserve®
Mehr als Backup

Inhaltsverzeichnis

Herausforderungen.....	2
Schutz von Daten	2
Wachsende Speicheranforderungen	2
Schutz virtueller und physischer Server	2
Disaster-Recovery-Planung	2
Service-Level-Agreements/Systemverfügbarkeit	3
Technologieoptionen	3
Kommerzielle Software für Backups auf Bändern	3
Backups/Snapshots auf Festplatten	3
Replikation über WAN	4
RAID (Redundant Array of Independent Disks)	4
Schutz und Verfügbarkeit von Systemen	5
Bare-Metal-Recovery	5
Software für hohe Verfügbarkeit	5
Hochverfügbarkeitscluster	5
Anwendungsvirtualisierung	5
Zusammenfassung.....	6
Die CA ARCserve®-Produktfamilie	6
Zusammenfassung.....	9
Nächste Schritte	9



HERAUSFORDERUNGEN

IT-Organisationen sehen sich bei der Unterstützung dezentraler Niederlassungen zahlreichen Herausforderungen gegenüber. Dazu gehören die Bereitstellung physischer und virtueller Server, das Management und die Maintenance vieler verschiedener Betriebssysteme und Anwendungen, die Überwachung unterschiedlicher Speicherlösungen wie DAS, NAS und SAN sowie das immer anspruchsvollere Management der IT-Sicherheit. Sobald die IT-Kerninfrastruktur eingerichtet ist, entstehen noch schwierigere IT-Herausforderungen, die den Schutz der Daten, die Systemverfügbarkeit und die Disaster-Recovery betreffen, insbesondere, wenn geografisch verteilte Niederlassungen einbezogen werden müssen, die im Allgemeinen eine vielfältige IT-Umgebung unterstützen.

Schutz von Daten

Studien von Branchenanalysten zeigen, dass sich heute über 70 % der Daten außerhalb des Unternehmensrechenzentrums befinden, wobei natürlich auch der Schutz dieser Daten sichergestellt werden muss. Viele Unternehmen, Behörden und Hochschulen sehen sich heute vor der schwierigen Aufgabe, die Informationen und Systeme an dezentralen Standorten oder in Zweigniederlassungen zu schützen. Umfragen haben gezeigt, dass mindestens 30 % der kleinen und mittleren Organisationen nicht einmal Backups der Daten in Niederlassungen erstellen, da ihnen die Kosten- oder Ressourcenanforderungen zu hoch sind.

Organisationen, die Backups in Zweigniederlassungen erstellen, verwenden im Allgemeinen herkömmliche Softwarelösungen mit Bandmedien. Bei dieser Strategie muss jemand das Backup durchführen und die Medien (wie Bänder) verwalten. Dies kann ein IT-Administrator sein, der sich zur Niederlassung begibt, ein Reseller oder Service-Provider vor Ort, der die Organisation unterstützt, oder im schlechtesten Fall ein Mitarbeiter der Niederlassung, der nicht der IT-Abteilung angehört. Die meisten Organisationen erstellen tägliche oder wöchentliche Backups, abhängig von ihren Zielsetzungen für Recoverypunkte (Recovery Point Objectives, RPOs), d. h. der Menge an Daten, deren Verlust sie zwischen den regelmäßigen Backups zu riskieren bereit sind.

Diese Strategie stellt die Organisationen vor zahlreiche Herausforderungen. Erstens fallen die Kosten für einen Backup-Server, Festplattenspeicher, ein Bandlaufwerk oder einen Bandwechsler und Medien in jeder Niederlassung an. Zweitens verursacht ein IT-Administrator Kosten, der vom Rechenzentrum zu den Niederlassungen reist, um das Backup durchzuführen und auf fehlgeschlagene Backup-Jobs zu reagieren, die durch einen Hardware-, Software- oder Medienausfall verursacht werden können. Selbst wenn die IT-Mitarbeiter den Backup- oder Wiederherstellungsjob auf einem Server in der Niederlassung mithilfe einer Fernzugriffslösung durchführen, können Probleme auftreten, wenn das erforderliche Medium sich nicht im Laufwerk befindet. Jemand muss dann nach dem richtigen Band suchen und es einlegen. Den Backup-Job an einen örtlichen Reseller oder Service-Provider auszulagern, verursacht deutliche Zusatzkosten.

Wachsende Speicheranforderungen

Wenn ein Unternehmen eine herkömmliche festplattenbasierte Backuplösung verwendet, muss es etwas gegen das exponentielle Datenwachstum unternehmen, das die Speicheranforderungen und die zugehörigen Kosten immer weiter in die Höhe treibt. Viele Hersteller bieten Deduplikationstechnologien an, um die Speicherkosten für Backups zu senken. Wenn eine solche Technologie separat erworben wird, kann sie jedoch teuer sein, was ihre finanziellen Vorteile teilweise zunichte macht.

Schutz virtueller und physischer Server

Heute haben viele Organisationen bereits virtuelle Server in Niederlassungen bereitgestellt oder ziehen die Servervirtualisierung in Erwägung, um Kosten zu senken und die betriebliche Effizienz zu erhöhen. Einige IT-Organisationen verwenden sogar unterschiedliche Backuplösungen, eine für physische Server und eine für virtuelle, obwohl es Backuplösungen mit Festplatten oder Bändern gibt, die für beides verwendet werden können. Zwei separate Backuplösungen bereitzustellen, zu verwalten und zu warten macht die Aufgaben der IT komplexer, zeitaufwändiger und teurer.

Disaster-Recovery-Planung

Im Interesse der Sicherheit und der Disaster-Recovery ziehen es die meisten Organisationen vor, eine Kopie ihrer Backups an einem zentralen Standort aufzubewahren, etwa in ihrem Rechenzentrum, in ihrer Hauptniederlassung oder an einem Disaster-Recovery-Standort. Hierfür müssen sie Kopien auf Bändern anfertigen und einen Kurierdienst oder, was noch unerfreulicher ist, einen Mitarbeiter jeder Niederlassung damit beauftragen, die Bänder nach jeder Backuperstellung an den zentralen Standort zu bringen. Der Transport physischer Bänder bedeutet zusätzliche Komplexität, Zeitaufwand und das Risiko beschädigter, verlorener oder gestohlener Bänder. Und wie bekommen Organisationen, die Backups von Festplatte auf Festplatte ziehen, ein Exemplar des Backups an einen anderen Standort, um sich für den Fall zu wappnen, dass der lokalen Niederlassung etwas zustößt, wie Feuer, Hochwasser, Erdbeben, Tornado oder Chemieunfall?

Service-Level-Agreements/Systemverfügbarkeit

Die dritte Frage schließlich ist: Wie können IT-Organisationen strikte Service-Level-Agreements und Business Continuity-Ziele für dezentrale Standorte einhalten? Backups schützen nur die Daten, nicht jedoch die Betriebsfähigkeit von Systemen und Anwendungen. Server-Clustering und Datenbankspiegelung können hier helfen, sind für kleine IT-Organisationen jedoch häufig zu komplex oder zu teuer in der Bereitstellung, Verwaltung und Wartung.

TECHNOLOGIEOPTIONEN

Es gibt viele unterschiedliche Ansätze für den Schutz von Daten und die Wahrung der Systemverfügbarkeit in Niederlassungen, bei denen unterschiedliche bereits verfügbare Technologien verwendet werden.

Kommerzielle Software für Backups auf Bändern

Viele Unternehmen verwenden an dezentralen Standorten seit langer Zeit einfache Backuptechnologien mit Bändern. Eine solche Softwarelösung ist einfach bereitzustellen und zu verwalten, aber das Management der Bänder/Medien ist die Herausforderung. Wer soll sicherstellen, dass an jedem dezentralen Standort das richtige Band in das Bandlaufwerk oder den Bandwechsler eingelegt ist? Wer soll Kopien der Bänder anfertigen, um sie ans Rechenzentrum oder an einen anderen Disaster-Recovery-Standort zu senden? Backups auf Bändern bringen viele Risiken mit sich, einschließlich der berühmten Medienausfälle. Daher erfüllen einfache Backups auf Bändern die heutigen hohen Anforderungen von Unternehmen und Organisationen an den Schutz ihrer Daten nicht.

Eine Möglichkeit besteht darin, Daten mit kommerzieller Backup-Software über das WAN (Wide Area Network) in das Rechenzentrum oder die Hauptniederlassung zu sichern oder zu kopieren. Dies ermöglicht einen zentralen Schutz der Daten, wobei die Backup- und Wiederherstellungsvorgänge von geschulten, erfahrenen IT-Mitarbeitern durchgeführt werden können. Viele Unternehmen, vor allem kleine und mittelgroße, stehen jedoch vor der Schwierigkeit, dass die Übertragung der großen Datenmengen über das WAN zu lange dauern würde, da viele nicht über Hochgeschwindigkeitsverbindungen (wie Standleitungen oder direkte Anbindungen an den Backbone) zwischen den einzelnen Niederlassungen und dem Rechenzentrum verfügen. Selbst wenn es technisch möglich ist, ein Backup über das WAN zu übertragen, erfüllt dies allein noch nicht die Zielsetzungen für Recoverypunkte, die viele Organisationen erfüllen müssen, um die Risiken versehentlicher Löschungen, böswilliger Angriffe über das Internet sowie Naturkatastrophen und von Menschen verursachter Katastrophen zu mindern. Organisationen, die nicht über einen eigenen Disaster-Recovery-Standort verfügen, können auf Wunsch auch eine cloudbasierte Backuplösung wählen, die das Rechenzentrum eines eigenständigen Service-Providers nutzt. Diese Lösung stellt sie jedoch vor die gleichen Herausforderungen.

Backups/Snapshots auf Festplatten

Eine zweite Möglichkeit besteht darin, in jeder Niederlassung eine Lösung zu verwenden, die Backups auf Festplatten erstellt. Bei dieser Lösung entfallen die Risiken von Backups auf Bändern, wie Laufwerk- und Medienausfälle, sowie das mühselige Medienmanagement, das im Allgemeinen von Mitarbeitern durchgeführt wird, die nicht zum IT-Personal gehören. Heute sind wesentlich bessere Technologien als Festplattenbackups erhältlich, mit denen insbesondere Backup und Wiederherstellung beschleunigt und der Bedarf an Festplattenspeicher wesentlich gesenkt werden. Die erste dieser Technologien heißt "unbegrenzte inkrementelle Backups". Ihre Besonderheit liegt darin, dass IT-Organisationen nur einmal ein vollständiges Backup ausführen müssen und alle darauf folgenden Backups inkrementell sein können. Mit dieser Lösung sind nicht nur schnellere Backups möglich, sondern auch schnellere Wiederherstellungen mit differenzierteren Recoverypunkten in Abständen von bis zu 15 Minuten. Außerdem wird für die Backups weniger Festplattenspeicher benötigt. Dies führt zu Kosteneinsparungen. Eine andere verbreitete Technologie wird als Datendeduplikation bezeichnet. Dabei werden Daten während des Backups („gleichzeitige Verarbeitung“) oder nach der Erstellung der Sicherung („nachgelagerte Verarbeitung“) verglichen, und redundante Daten werden entfernt, im Allgemeinen auf Blockebene. Mit der Datendeduplikation können die Anforderungen an den Festplattenspeicher um bis zu 95 % reduziert werden, abhängig von den zu sichernden Daten. Wie können Sie jedoch bei Durchführung von Backups auf Festplatten Kopien der Backups an einen anderen Standort bringen, um sie für die Disaster-Recovery nutzen zu können? Einige IT-Organisationen kopieren Backups dezentraler Niederlassungen auf Bänder und transportieren diese physisch ins Datenzentrum oder an einen anderen entfernten Standort. Auch diese Strategie ist zeitaufwändig, teuer und risikoreich. Bänder können während des Transports zum entfernten Aufbewahrungsort beschädigt, verloren oder gestohlen werden. Datenreplikationstechnologien, die für Übertragungen über das WAN optimiert sind, können sich als bessere Lösung erweisen, da Kopien auf Band und physische Transporte wegfallen. Die meisten Replikationslösungen übertragen (nach Abschluss des jeweiligen Backups) nur die kleinen Änderungen, die an Dateien und Datenbanken vorgenommen wurden, über das WAN. Daher können die meisten Organisationen zwischen den einzelnen Niederlassungen und dem Disaster-Recovery-Standort oder dem Standort des primären Rechenzentrums Verbindungen mit geringer Bandbreite verwenden. Um maximale Effizienz zu erzielen, muss die verwendete Replikationslösung sowohl unbegrenzte inkrementelle Backups als auch Backups mit Datendeduplikation unterstützen.

Replikation über WAN

Für manche Organisationen kann eine dritte Option darin bestehen, zuerst mit einer Datenreplikationslösung, die für die Echtzeitübertragung über WAN optimiert ist, die Daten aller Niederlassungen im Rechenzentrum oder am Disaster-Recovery-Standort zu konsolidieren. Replikationstechnologien sind in Form hostbasierter Software erhältlich, bei der die Replikationssoftware auf jedem Anwendungsserver in der Niederlassung installiert wird, oder als hardwarebasierte Lösung im Rahmen eines Speicherarrays in einer Appliance oder einem SAN (Storage Area Network). Hardwarebasierte Replikationslösungen sind teurer, da nicht die Replikationstechnologie das Wesentliche ist, sondern das Gerät, wie etwa ein SAN-basiertes Festplattenarray. Softwarebasierte Replikationslösungen bieten mehrere Vorteile: Sie sind im Allgemeinen kostengünstiger, können anwendungsorientiert arbeiten, um Transaktionsintegrität für Anwendungen wie Datenbanken bereitzustellen, ermöglichen die Speicherreplikation mit beliebigen Quellen und Zielen zur Senkung von Speicherkosten, und sind leichter zu implementieren und zu verwalten, vor allem für kleine und mittlere Organisationen mit begrenztem IT-Personal. Außerdem können Unternehmen mit den meisten Softwarereplikationslösungen zwischen der kontinuierlichen Replikation und der zeitplanbasierten/regelmäßigen Replikation wählen, um ein Gleichgewicht zwischen der Auslastung von Netzwerkressourcen und dem gewünschten Schutzniveau zu schaffen. Natürlich bietet eine kontinuierliche Replikation besseren Schutz als eine periodische Replikation, da die Daten fortlaufend an einen anderen Standort kopiert werden. So können Unternehmen auch strikere Zielsetzungen für Recoverypunkte erfüllen.

Im Allgemeinen arbeiten alle hostbasierten Softwarereplikationslösungen auf die gleiche Weise. Zuerst wird jeder zu schützende Server/Speicher (der Produktionsserver) in jeder Niederlassung über das WAN oder anderweitig mit einem genauso konfigurierten physischen oder virtuellen Server (dem Replikatserver) im Rechenzentrum oder am Disaster-Recovery-Standort synchronisiert. Sobald der Produktionsserver und der Replikatserver synchronisiert sind, werden nur noch die kleinen Änderungen der Daten auf dem Produktionsserver auf Byteebene in Echtzeit über das WAN übertragen. Dies ermöglicht eine effiziente Übertragung über Verbindungen mit begrenzter Bandbreite zwischen den Niederlassungen und dem Rechenzentrum. Bei der kontinuierlichen Replikation werden der Produktionsserver und der Replikatserver fortlaufend synchronisiert. Dies entspricht fast einer Spiegelungsmethode. Die Replikation wird jedoch asynchron ausgeführt, um die Anforderungen an die WAN-Bandbreite möglichst gering zu halten und die Leistung zu verbessern. Die meisten Replikationslösungen schließen außerdem eine Komprimierungstechnologie ein, um die Anforderungen an die Bandbreite zu minimieren.

Nachdem die Daten aus allen Zweigniederlassungen in das Rechenzentrum repliziert wurden, können IT-Mitarbeiter das Backup vom lokalen Replikatserver ausführen, um Protokolldaten zu schützen, Daten zu archivieren und Vorschriften einzuhalten. In diesem Szenario hat die Ausführung des Backups keine Auswirkungen auf die Produktionsserver in den Zweigniederlassungen, weil das Backup stattdessen von den Failover-Servern aus ausgeführt wird. Daher wird die Produktivität in den Niederlassungen nicht beeinträchtigt, und die Einschränkungen durch Backupzeitfenster, die heute in den meisten Organisationen ein Problem darstellen, werden überwunden. Mit dieser Lösung werden außerdem mehrere Probleme gelöst, die bei dezentralen Backups auf Band auftreten, wie die Notwendigkeit, IT-Mitarbeiter in die Niederlassungen zu senden (oder einen lokalen Service-Provider unter Vertrag zu nehmen). Außerdem fallen weniger Kosten und Wartungsaufwand für Backup-Server, Bandlaufwerke, Bandwechsler und Medien in den einzelnen Zweigniederlassungen an. Zusätzlich wird ein zentraler, sicherer Schutz von Daten im Rechenzentrum oder in der Hauptniederlassung sichergestellt.

Umfassendere hostbasierte Softwarereplikationslösungen besitzen weitere Leistungsmerkmale, wie den kontinuierlichen Schutz der Daten (Continuous Data Protection, CDP), bei dem der IT-Administrator schnell und einfach einen Rücklauf (Rewind) der Daten auf dem Failover-Server bis zu einem bekannten fehlerfreien Zustand durchführen kann, wenn Daten auf dem Produktionsserver in der Zweigniederlassung aus Versehen oder durch einen Angriff verloren gegangen sind oder beschädigt wurden. Die wiederhergestellten Dateien oder Datenbanken können dann wieder auf dem Produktionsserver bereitgestellt werden.

RAID (Redundant Array of Independent Disks)

RAID ist eine Technologie, die durch Redundanz eine zuverlässigere Speicherung ermöglicht. Dabei werden mehrere kostengünstige, weniger zuverlässige Festplatten zu einer logischen Einheit kombiniert. Alle Festplatten im Array hängen voneinander ab. RAID-Speichergeräte sind im Laufe der Zeit bekannter und preisgünstiger geworden. Heute ist diese Speicherlösung auch für kleinere Organisationen erschwinglich. Für RAID sind drei Konzepte wichtig: Die Spiegelung, bei der mehrere Festplatten identische Daten enthalten; das Striping, bei dem sequenzielle Datenblöcke auf mehrere Festplatten aufgeteilt werden, und die Fehlerkorrektur, bei der redundante Paritätsinformationen gespeichert werden, damit Probleme erkannt und soweit möglich behoben werden können (auch als Fehlertoleranz bezeichnet). Bei erhältlichen RAID-Schemata werden abhängig von den Systemanforderungen eine oder mehrere dieser Techniken verwendet. RAID wird verwendet, um die Zuverlässigkeit und Verfügbarkeit von Daten zu verbessern und somit sicherzustellen, dass wichtige Daten bei einem Hardwareausfall nicht beschädigt werden, und/oder um die Geschwindigkeit der Ein-/Ausgabe in Dateien zu erhöhen. Die Bereitstellung und das Management von RAID-Geräten können jedoch komplexer sein, und RAID-Geräte alleine bieten noch keinen Schutz gegen versehentliche oder böswillige Datenverluste und -schäden, Naturkatastrophen und von Menschen verursachte Katastrophen – oder auch nur gegen Diebstahl des Geräts. In Verbindung mit anderen Technologien hingegen bietet RAID einen robusten Schutz gegen Ausfälle lokaler Festplatten.

Schutz und Verfügbarkeit von Systemen

- **Bare-Metal-Recovery**

Einige Backuplösungen schließen eine Technologie ein, die als Bare-Metal-Restore/Recovery (BMR) bezeichnet wird und mit der die IT-Abteilung nach einem ungeplanten Absturz oder Ausfall schneller und leichter einen gesamten Server wiederherstellen kann, einschließlich des Betriebssystems, der Anwendungen und der Daten. Im Allgemeinen gehören zu den gesicherten Daten die erforderlichen Betriebssystem-, Anwendungs- und Datenkomponenten, mit denen das gesicherte System auf einer anderen Hardware eingerichtet oder wiederhergestellt werden kann. Bei einigen Konfigurationen muss die Hardware, auf der das System wiederhergestellt wird, genau die gleiche Konfiguration aufweisen wie die Hardware, die Quelle des Backups war. Bei einigen BMR-Lösungen ist eine Bare-Metal-Wiederherstellung auf einer Hardwarekonfiguration möglich, die von der ursprünglichen Hardware abweicht (dies wird als BMR auf abweichender Hardware bezeichnet). Die Recovery mit BMR ist wesentlich schneller als eine Neuinstallation des Betriebssystems und der Anwendungen auf einem neuen oder reparierten Server.

- **Software für hohe Verfügbarkeit**

Für eher kritische Server und Anwendungen kann sogar die BMR-Technologie zu zeitintensiv sein. Viele Datenreplikationslösungen bieten Optionen für die Serverüberwachung sowie für das automatisierte Failover und Failback. So wird eine Hochverfügbarkeitsumgebung für sehr kritische und kritische Systeme, Anwendungen und Daten bereitgestellt, mit der jede Zweigniederlassung den Schutz von Daten, die Business Continuity und die Disaster-Recovery mithilfe einer einzelnen Lösung sicherstellen kann. Um eine optimale Risikominderung zu ermöglichen, enthalten einige Hochverfügbarkeits-Replikationslösungen außerdem automatisierte Wiederherstellungstests ohne Betriebsunterbrechungen, mit denen sichergestellt wird, dass die Failoverumgebung im Rechenzentrum oder an einem anderen entfernten Standort bereit ist, wenn für die Zweigstelle ein Failover notwendig wird. Einige Lösungen bieten zusätzlich ein manuell auszulösendes Failover. Dieses kann vor einer bevorstehenden Katastrophe wie einem Hurrikan verwendet werden. Außerdem kann es genutzt werden, um Server und Betriebssysteme zu aktualisieren und zu migrieren, ohne die Arbeitsumgebung zu stören und ohne dass Mitarbeiter nachts oder am Wochenende arbeiten müssen, um die Hauptarbeitszeiten zu vermeiden.

- **Hochverfügbarkeitscluster**

Eine andere Technologie für die Systemverfügbarkeit ist der Hochverfügbarkeitscluster (auch als High-Availability-Cluster, HA-Cluster oder Failover-Cluster bezeichnet). Hierbei handelt es sich um einen Server-Cluster, der vor allem zu dem Zweck implementiert wird, die hohe Verfügbarkeit der vom Cluster bereitgestellten Services zu erreichen. In Hochverfügbarkeitsclustern werden redundante Computer oder Knoten verwendet, sodass die Services beim Ausfall einzelner Systemkomponenten weiter bereitgestellt werden können. Wenn in einem Szenario ohne hohe Verfügbarkeit ein Server mit einer bestimmten Anwendung abstürzt, ist die Anwendung so lange nicht verfügbar, bis der Server repariert wird. In einem Hochverfügbarkeitscluster hingegen werden Hardware-/Softwarefehler erkannt, und die Anwendung wird sofort auf einem anderen System gestartet, ohne dass menschliches Eingreifen erforderlich ist. Dieser Prozess wird als Failover bezeichnet. Die Bereitstellung und das Management von Hochverfügbarkeitsclustern können jedoch komplexer sein als Software für Replikation und Hochverfügbarkeit, und sie bieten selbst keinen Schutz von Daten, da sie im Allgemeinen gemeinsam genutzten Speicher wie ein NAS oder SAN verwenden. Daher werden im Allgemeinen zusätzlich weitere Schutztechnologien für Daten benötigt, wie Backups, Replikation und kontinuierlicher Schutz der Daten (CDP).

Anwendungsvirtualisierung

Abschließend sei die Möglichkeit genannt, mithilfe einer Anwendungsvirtualisierungslösung alle Anwendungen sowie die Speicherung für die Niederlassungen in das Rechenzentrum zu verlagern. Dort können die Systeme, Anwendungen und Daten zusammen mit der restlichen Infrastruktur des Rechenzentrums zentral geschützt werden. Bei Anwendungsvirtualisierungslösungen werden Client/Server- und Desktopanwendungen in einer Serverfarm im Rechenzentrum ausgeführt, und nur die grafische Benutzeroberfläche (GUI) wird über das Netzwerk übertragen. Dies ermöglicht sicheren Fernzugriff sogar über langsame WAN-Verbindungen. Nachdem die IT-Abteilung alle Systeme, Anwendungen und Daten in das Rechenzentrum verlagert hat, kann sie jede Kombination der oben beschriebenen Backup-, Replikations- und Hochverfügbarkeitstechnologien auf alle Ressourcen im Rechenzentrum anwenden.

ZUSAMMENFASSUNG

Der Schutz von Systemen, Anwendungen und Daten in Niederlassungen ist genauso wichtig wie der Schutz von Ressourcen im Rechenzentrum. Mit den heute verfügbaren Technologien können auch kleine und mittlere Unternehmen und Organisationen ihre Ziele in diesem Bereich mithilfe kosteneffizienter und benutzerfreundlicher Lösungen erreichen.

Selbstverständlich sollten in jeder Organisation Backups auf Festplatten oder Bändern erstellt werden, um einen grundlegenden Schutz der Daten sicherzustellen. Mit Festplatten sind Backups und Wiederherstellung schneller möglich als mit Bändern, und unvermeidliche Risiken der Speicherung auf Bändern werden vermieden. Mit Replikationslösungen können Backups zu Disaster-Recovery-Zwecken an einen anderen Standort kopiert werden, Daten der Niederlassungen können zum Zweck zentraler Backups konsolidiert werden, und jede Backuplösung kann durch einen kontinuierlichen Schutz der Daten ergänzt werden. Hochverfügbarkeitslösungen sind für wichtige Server, Systeme und Anwendungen bestimmt, bei denen Ausfallzeiten schwerwiegende Konsequenzen für den Umsatz, den Service, die Produktivität, den guten Ruf des Unternehmens und die Einhaltung von Vorschriften haben.

Kleine und mittlere Organisationen, denen die Mitarbeiter oder das Wissen für Bereitstellung, Management und Maintenance derartiger Systeme fehlen, können das Wissen und die Erfahrung eines vertrauenswürdigen Beraters nutzen, indem sie einen serviceorientierten Channel-Partner oder Reseller heranziehen. Außerdem können Sie sich nach einem Anbieter von Managed Services umsehen, der SAS-basierte Softwarelösungen sowie Hosting- und Management-Services anbietet. Solche Services können Sie aus dem Betriebskostenbudget (OPEX) statt dem Investitionsbudget (CAPEX) bezahlen.

DIE CA ARCSERVE®-PRODUKTFAMILIE

Mit der CA ARCserve®-Produktfamilie behalten Sie die Kontrolle über sich verändernde Geschäftsanforderungen, denn sie bietet umfassenden Schutz, Wiederherstellung und Verfügbarkeit für Ihre Server, Anwendungen und Daten in dezentralen Niederlassungen. Die CA ARCserve-Produktfamilie ist die einzige Lösung für die hohe Verfügbarkeit, die ein Komplettpaket von der Bare-Metal-Recovery bis zum vollautomatischen Failover umfasst. Sie erhalten eine vollständige Strategie für das Management von Backups, Wiederherstellung und Verfügbarkeit in dezentralen Niederlassungen und in Rechenzentren.

CA ARCserve D2D ermöglicht die schnelle und mühelose Erstellung von Backups auf Festplatten und ist die einzige Windows-basierte Backuplösung, die die I²-Technologie für unbegrenzte inkrementelle Snapshots auf Blockebene bietet. Mit dieser neuen Backupmethode werden Backup und Wiederherstellung wesentlich beschleunigt, und die durch Bandgeräte und -medien verursachten Risiken werden vermieden. Mit der I²-Technologie werden außerdem die Speicheranforderungen für Backups und die damit verbundenen Kosten wesentlich reduziert, sodass die Gesamtbetriebskosten gesenkt werden können. Mit differenzierter Wiederherstellung und Bare-Metal-Recovery (auf gleicher oder anderer Hardware) können Sie verlorene oder beschädigte Daten schneller und leichter wiederherstellen und beschädigte Server in Niederlassungen von einem beliebigen Ort aus über die webgestützte Managementkonsole neu einrichten. Fertige Backups dezentraler Standorte können mithilfe von CA ARCserve Replication mühelos an einen anderen Ort übertragen werden, sodass sie im Bedarfsfall für die Disaster-Recovery zur Verfügung stehen. Nach der anfänglichen Synchronisierung zwischen dem CA ARCserve D2D-Repository in der Niederlassung und dem Replikatserver im Rechenzentrum, in der Hauptniederlassung oder am Disaster-Recovery-Standort werden nur noch Änderungen auf Byteebene in den unbegrenzten inkrementellen Backups über das WAN übertragen. Somit wird das Netzwerk nur minimal beansprucht. Funktionen für die Replikation nach Zeitplan sowie die Bandbreitenoptimierung ermöglichen eine Nutzung von Zeiträumen, in denen das Netzwerk weniger ausgelastet ist, damit die WAN-Bandbreite nicht erhöht werden muss. Diese Lösung ermöglicht Unternehmen eine schnelle Wiederherstellung von lokalen Festplatten, sowie (im Fall eines Problems in der lokalen Niederlassung) auch von entfernten Festplatten.

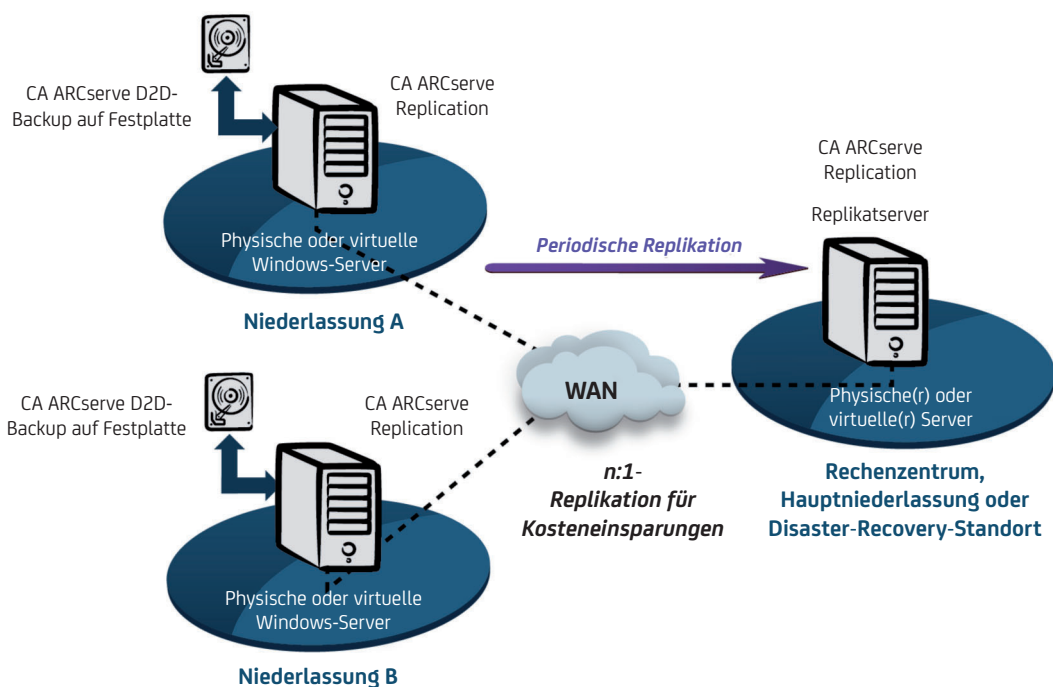


Abbildung 1. Festplattenbasierte Backups für Niederlassungen mit CA ARCserve D2D und CA ARCserve Replication über das WAN an einen anderen Standort zum Schutz von Daten und für die Disaster-Recovery.

Alternativ können Sie mit CA ARCserve Replication unter Windows, Linux und UNIX Daten von Niederlassungen replizieren, um alle Daten an einem zentralen Standort zu aggregieren. Vom dortigen Replikatserver aus können Sie dann mithilfe von CA ARCserve Backup oder CA ARCserve D2D Backups auf Festplatte oder Band erstellen, ohne dass Auswirkungen auf die Server und die Mitarbeiter in der Niederlassung entstehen. CA ARCserve Backup unterstützt Windows, Linux und UNIX, schließt eine integrierte Datenduplikation ein, mit der die Speicheranforderungen um bis zu 95 % gesenkt werden können, und ermöglicht Backups wahlweise auf Festplatte oder auf Band. CA ARCserve Backup und CA ARCserve D2D unterstützen physische und virtuelle Server. In diesem Szenario kann festgelegt werden, dass die Replikation kontinuierlich ausgeführt wird. Dies bedeutet noch besseren Schutz der Daten und stellt eine noch bessere Vorbereitung für den Fall der Disaster-Recovery dar. Sie können jedoch auch einen Zeitplan für die regelmäßige Replikation festlegen, den Sie als geeignet erachten. Mit dieser Lösung können Unternehmen eine schnelle Datenwiederherstellung von dezentralen Festplatten durchführen und die Daten der Niederlassungen langfristig speichern, um Unternehmensrichtlinien und Vorschriften einzuhalten.

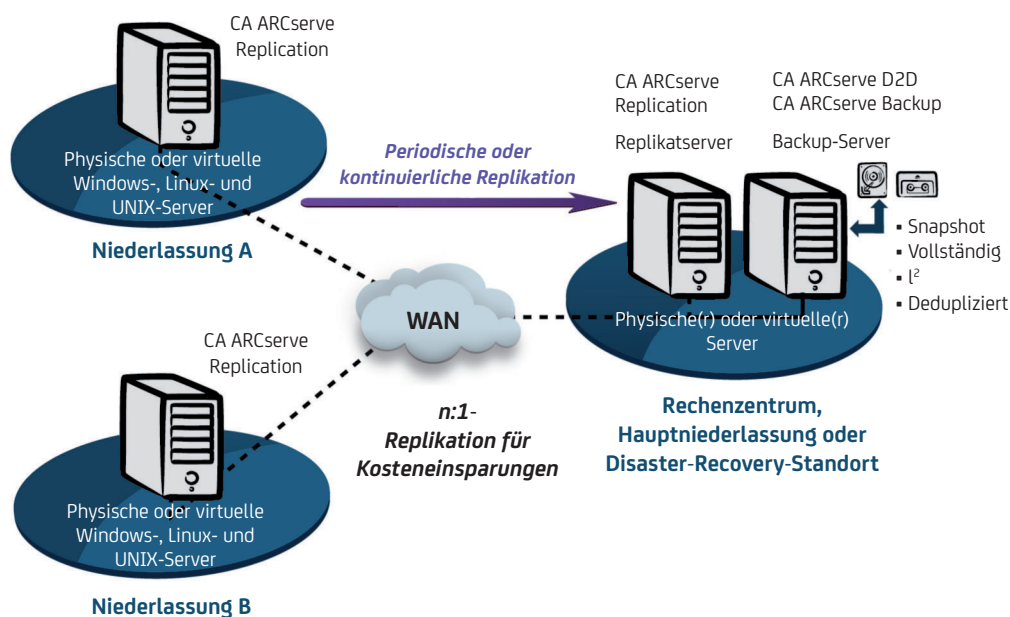


Abbildung 2. CA ARCserve Replication über das WAN an einen anderen Standort zur Aggregation der Daten aller Niederlassungen zur zentralen Erstellung von Festplatten- oder Bandbackups ohne Betriebsunterbrechungen mit CA ARCserve Backup oder CA ARCserve D2D für den Schutz der Daten und die Disaster-Recovery.

CA ARCserve Replication schließt die Data-Rewind-Technologie ein, mit der die Datenwiederherstellung nach einem versehentlichen oder böswilligen Verlust oder Schaden ganz einfach ist. Ebenfalls eingeschlossen ist CA ARCserve Assured Recovery für automatisierte Wiederherstellungstests ohne Betriebsunterbrechung, mit denen sichergestellt werden kann, dass der Replikatserver, die Anwendung und die Daten verfügbar sind, wenn sie gebraucht werden.

CA ARCserve High Availability sollte statt CA ARCserve Replication verwendet werden, wenn die Replikation, der kontinuierliche Schutz der Daten sowie die hohe Verfügbarkeit von Systemen, Anwendungen und Daten erforderlich sind, um anspruchsvolle Service-Level-Agreements einzuhalten und Disaster-Recovery-Strategien umzusetzen. Mit CA ARCserve High Availability werden alle kontinuierlichen oder regelmäßigen Replikationsvorgänge für den Schutz der Daten in Niederlassungen durchgeführt, und es wird eine Überwachung der Server und Anwendungen in Echtzeit bereitgestellt. Durch einen automatisch oder manuell ausgelösten Failover kann sichergestellt werden, dass die Ressourcen in den Niederlassungen kontinuierlich verfügbar sind. Wie CA ARCserve Replication schließt auch CA ARCserve High Availability die Technologien Data-Rewind und Assured Recovery ein. CA ARCserve Replication und CA ARCserve High Availability unterstützen Windows, Linux und UNIX auf physischen und virtuellen Servern.

Ganz gleich, welche Strategie Sie für den Schutz Ihrer Daten und die Wahrung der Systemverfügbarkeit verwenden: Die CA ARCserve-Produktfamilie bietet vollständigen Schutz, Wiederherstellung und Verfügbarkeit für Ihre Niederlassungen und Ihre Rechenzentren.

ZUSAMMENFASSUNG

Sie können entscheiden, ob Sie in den einzelnen Niederlassungen schnelle Backups auf Festplatten durchführen und sie zum Zweck der Disaster-Recovery an einen anderen Standort replizieren möchten, oder ob Sie zuerst die Daten aller Niederlassungen an einen zentralen Standort replizieren und dann dort ein Backup ohne Betriebsunterbrechungen durchführen möchten. Für beide Vorgehensweisen stehen zahlreiche Technologien zur Verfügung, mit denen Sie Ihre dezentralen Standorte genauso schützen können wie die Hauptniederlassung oder das Rechenzentrum. Mit Lösungen für die Bare-Metal-Recovery und die hohe Verfügbarkeit können Sie für Systeme und Anwendungen das Risiko von Ausfallzeiten minimieren, die den Betrieb, die Produktivität und die Services beeinträchtigen würden. Mit der CA ARCserve-Produktfamilie ist dies leicht zu erreichen, denn sie bietet umfassenden Schutz, Wiederherstellung und Verfügbarkeit für Ihre Server, Anwendungen und Daten in Niederlassungen und im Rechenzentrum.

NÄCHSTE SCHRITTE

Lesen Sie mehr über die CA ARCserve-Produktfamilie unter arcserve.com/products. Für die gesamte oben beschriebene Software der CA ARCserve-Produktfamilie sind kostenfreie 30-tägige Testversionen erhältlich. Bitte wenden Sie sich an Ihren örtlichen Reseller, oder besuchen Sie arcserve.com/partners, um einen autorisierten Partner in Ihrer Region zu finden.

Copyright ©2010 CA Technologies. Alle Rechte vorbehalten. Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern. UNIX ist eine eingetragene Marke von The Open Group in den USA und/oder anderen Ländern. Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Alle anderen erwähnten Marken, Handelsnamen, Dienstleistungsmarken und Logos sind Eigentum der jeweiligen Unternehmen.