Kapitel 1 – Sicherungs- und Wiederherstellungsdesign

(Engl. Originaltitel: Chapter 1 – Backup and Restore Design)

Dieses Kapitel ist Teil der englischsprachigen Dokumentation Backup and Restore Solution for Windows 2000–based Data Centers.

Zusammenfassung

In diesem Kapitel wird die Sicherungs- und Wiederherstellungslösung für Microsoft® Internet Data Center beschrieben. Erläutert werden die Sicherungsprinzipien und -strategien für Rechenzentren sowie Methoden zur Beurteilung, was in einer IDC-Umgebung gesichert werden sollte. Die empfohlene Sicherungs- und Wiederherstellungslösung verwendet CommVault Galaxy-Software in allen virtuellen lokalen IDC-Netzwerken (Virtual Local-Area Networks oder VLANs). Die Funktionen der Galaxy-Software werden erläutert und das Design der Lösung beschrieben, einschließlich der Details der zur erfolgreichen Implementierung dieser Sicherungs- und Wiederherstellungslösung erforderlichen Planungs- und Konfigurationsschritte.

Einführung

Die IDC-Architektur wurde entwickelt, um Stabilität ohne Einzelpunktversagen bereitzustellen. Es ist jedoch äußerst wichtig, angemessene Sicherungen vorzunehmen, damit Daten und Systemkonfigurationen im Fall eines schwerwiegenden Ausfalls wiederhergestellt werden können. Auch wenn Sie alle denkbaren Vorsichtsmaßnahmen ergreifen, können Sie dennoch nicht auf alle Notfälle oder Ausfälle vorbereitet sein, die sich auf ein Rechenzentrum auswirken können. Deshalb ist die Planung einer Wiederherstellungsstrategie so wichtig.

Die Wichtigkeit einer Sicherung der IDC-Umgebung

Die Menge der in IDC-Umgebungen gespeicherten Daten variiert, kann jedoch auf mehrere Terabytes anwachsen, so wie auch die Anzahl der unterstützten Benutzer steigt. Bei dieser Art einer sich ständig ändernden Umgebung müssen unternehmenswichtige Anwendungen verfügbar sein, Ausfallzeiten auf ein Minimum reduziert werden und muss die zunehmende Abhängigkeit von mehreren Schichten effizient verwaltet werden.

Die Sicherung von IDC-Umgebungen ist wesentlich, um wichtige Daten zu schützen und ihre schnelle Wiederherstellung im Fall eines (kleinen oder großen) Datenverlusts zu ermöglichen.

Ein Datenverlust kann folgende Ursachen haben:

- Ausfall eines Festplattensubsystems
- Stromausfall (mit beschädigten Daten als Folge)
- Systemsoftwareausfall
- Versehentliches oder absichtliches Löschen oder Ändern von Daten
- Viren
- Naturkatastrophen (d. h. Brände, Überschwemmungen, Erdbeben u. ä.)
- Diebstahl oder Sabotage

Ein Unternehmen muss sich von einem Ausfall oder Notfall schnell erholen können, unabhängig davon, ob es sich dabei um den Ausfall einer einzelnen Komponente oder die vollständige Zerstörung eines Standorts handelt. Sie sollten deshalb beim Entwerfen einer Sicherungs- und Wiederherstellungsarchitektur alle Ausfallarten berücksichtigen. Sie sollten die Architektur auf der Grundlage genau definierter Systemverfügbarkeitsanforderungen auswählen und dabei Inhalt und Konfiguration der einzelnen Server berücksichtigen.

Beurteilen der Situation

Berücksichtigen Sie für alle in eine IDC-Umgebung eingeführten Betriebssysteme und Anwendungen die folgenden Fragen:

- Wie sehen mögliche Ausfallszenarien aus?
- Welche Daten sind wichtig, und wo befinden sie sich?
- Wie häufig müssen Sicherungen durchgeführt werden?
- Wann sollten vollständige anstatt inkrementeller oder differenzieller Sicherungen durchgeführt werden?
- Welche Sicherungsmedien werden verwendet (Magnetplatte, magnetooptischer Datenträger oder Band)?
- Werden Sicherungen online oder offline durchgeführt?
- Werden Sicherungen manuell oder automatisch nach einem Zeitplan gestartet?
- Womit wird die Gültigkeit von Sicherungen geprüft?
- Wo werden die Sicherungen gespeichert (intern, extern oder beides)?

Eine gute Sicherungs- und Wiederherstellungsarchitektur muss einen Notfallvermeidungsplan, Verfahren und Tools zur Unterstützung der Wiederherstellung nach einem Notfall oder Ausfall sowie detaillierte Verfahren und Standards zur Durchführung der Wiederherstellung beinhalten. Die Architektur sollte für alle Themenbereiche klar die Personen, Prozesse und Technologien definieren, die für den Erfolg erforderlich sind.

Sicherungsdesign

Bei der Entwicklung einer Sicherungslösung für die IDC-Architektur sollten Sie eine Reihe von Faktoren berücksichtigen. So müssen Sie beispielsweise bestimmen, wie Sie Notfälle vorhersehen und vermeiden, entscheiden, welche Teile der Umgebung gesichert werden sollen und wie oft, und sich informieren, wie Sie eine Sicherungs- und Wiederherstellungsstrategie für die Umgebung planen. Die fertig gestellte Lösung sollte ausführlich dokumentierte Notfallvermeidungs- und Wiederherstellungspläne beinhalten.

Notfallvermeidungsplan

Ein Notfallvermeidungsplan muss Ereignisse vorhersehen, die sich auf den Systembetrieb auswirken können, und entsprechende Maßnahmen bereitstellen. Bei den Ereignissen, die zu einer Störung von Internetdiensten führen können, kann es sich um ein Internetverbindungsproblem, um geringfügige Fehler in Komponenten, die nicht einfach ersetzt werden können, oder auch um komplexere Softwareprobleme handeln.

Zu den Elementen eines erfolgreichen Notfallvermeidungsplanes gehören geografische Redundanz sowie die Remotespeicherung von Sicherungsbändern. Die Verwendung redundanter, geografisch entfernter Rechenzentren stellt eine gute Methode dar, um sicherzustellen, dass bei einem regionalen Zwischenfall weiterhin Dienste bereitgestellt werden können. Durch das Entfernen der Sicherungsbänder aus den einzelnen Rechenzentren wird verhindert, dass sowohl das Rechenzentrum als auch der Sicherungsmechanismus des Rechenzentrums verloren gehen. Je nach Wichtigkeit der Daten können mehrere externe Speichereinrichtungen verwendet werden. Die externe Speicherung führt nicht unbedingt zu wesentlich höheren Kosten in der Sicherungs- und Wiederherstellungsarchitektur; viele Unternehmen stellen externe Speicherdienste bereit und stellen Sicherungsbänder zu bzw. holen diese ab, sobald eine Rotation der Bänder erforderlich ist.

Ein Notfallvermeidungsplan muss auf der Grundlage der Leistungs- und Verfügbarkeitsanforderungen erstellt werden, die für die jeweilige Hostanwendung definiert wurden. Wenn die Anwendung für eine bestimmte Region bestimmt ist, ist es z. B. nicht sinnvoll, ein zweites, geografisch entferntes Rechenzentrum in die Planung einzubeziehen.

Wiederherstellungsplan

Ein Wiederherstellungsplan bereitet ein Unternehmen auf die Wiederherstellung nach unvermeidbaren Zwischenfällen und Ausfällen vor. Beim Entwickeln des Planes sollte Folgendes berücksichtigt werden:

- **Können die Geschäftsabläufe während eines Zwischenfalls oder Ausfalls fortgesetzt werden?** Ein Wiederherstellungsplan sollte Verfahren zur Aufrechterhaltung von Geschäftsabläufen während eines Zwischenfalls oder Ausfalls (einschließlich Netzwerkausfälle) beinhalten. Beispiel: Die Telefone in der Vertriebsabteilung klingeln weiter, auch wenn der Server nicht betriebsbereit ist, so dass die Mitarbeiter Aufträge u. U. manuell annehmen müssen, bis der Server wieder betriebsbereit ist. Alle Abteilungen sollten Strategien für Situationen dieser Art ausarbeiten.
- **Wie soll der Wiederherstellungsplan erstellt und verwaltet werden?** Um seinen Erfolg zu gewährleisten, muss der Wiederherstellungsplan ordnungsgemäß verwaltet werden. Es wird empfohlen, einem oder mehreren Mitarbeitern des Unternehmens die Verantwortung für die Überwachung der Vorbereitungsmaßnahmen für den Notfall zu übertragen. Jemand muss die Hardwareschutzgeräte installieren und warten, sicherstellen, dass alle Abteilungen für den Fall eines vorübergehenden Serverausfalls einen Plan haben und dass regelmäßig Sicherungen durchgeführt und rotiert werden, sowie eine ausführliche Dokumentation zur Unterstützung des Wiederherstellungsplanes erstellen.

Optimale Vorgehensweisen für die Entwicklung einer Sicherungslösung

Beachten Sie bei der Entwicklung einer Sicherungslösung folgende Empfehlungen:

- Beziehen Sie beim Entwickeln und Testen von Sicherungs- und Wiederherstellungsstrategien die richtigen Mitarbeiter ein, und verwenden Sie geeignete Ressourcen.
- Erstellen Sie ein Unternehmensdiagramm für den Datenschutz, das die Verantwortungsbereiche und Kontaktinformationen aller Personen enthält.
- Führen Sie zunächst eine vollständige Sicherung aller Datenträger durch, die geschützt werden müssen.
- Sichern Sie den Systemstatus aller Server, und stellen Sie sicher, dass der Microsoft Active Directory®-Verzeichnisdienst für alle Domänencontroller enthalten ist.
- Drucken und lesen Sie Sicherungsberichte für CommVault Galaxy-Systeme, um sicherzustellen, dass alle Dateien ordnungsgemäß gesichert werden.
- Führen Sie periodische Datenwiederherstellungstests durch, um sicherzustellen, dass die Dateien richtig gesichert werden.
- Stellen Sie sicher, dass Sicherungsmedien, Systeme und Server so gesichert werden, dass ein Administrator gestohlene Daten auf Ihrem Server nicht unerlaubt wiederherstellen kann.
- Entwickeln und implementieren Sie einen Wiederherstellungstestplan, um die Integrität der Sicherungsdaten zu gewährleisten.

Sicherungsstrategien

Sie sollten bei der Planung einer Sicherungslösung eine Reihe von Faktoren berücksichtigen, wie z. B. die ausschließliche Sicherung notwendiger Daten, die sorgfältige Planung der Sicherungen und die Auswahl des geeigneten Sicherungstyps für die Durchführung.

Vermeiden unnötiger Sicherungen

Beim Entwerfen einer Sicherungsstrategie ist die Versuchung groß, eine vollständige Sicherung aller Server in der Umgebung durchzuführen. Denken Sie jedoch daran, dass Ihr Ziel eine erfolgreiche Wiederherstellung der Umgebung nach einem Ausfall oder Zwischenfall ist. Die Sicherungsstrategie sollte deshalb auf die folgenden Ziele ausgerichtet sein:

- Die wiederherzustellenden Daten sollten einfach zu finden sein.
- Die Wiederherstellung sollte so schnell wie möglich erfolgen.

Wenn Sie unterschiedslos alle Server sichern, müssen Sie eine größere Datenmenge wiederherstellen. Die derzeit erhältlichen Bandspeicher- und -sicherungsprodukte ermöglichen zwar eine schnelle Datenwiederherstellung, allerdings können Ausfallzeiten erhöht werden, wenn alles vom Band wiederhergestellt werden muss. Die meisten Sicherungsprodukte erfordern z. B. die folgenden Schritte:

1. Neuinstallieren des Betriebssystems.
2. Neuinstallieren der Sicherungssoftware.
3. Wiederherstellen der Sicherung vom Band.

Je mehr Dateien gesichert werden, desto länger dauert die Sicherung, und, was noch wichtiger ist, desto länger dauert es, die Dateien wiederherzustellen. Wenn es zu einem Zwischenfall kommt, ist die Zeit ein wichtiger Faktor; je kürzer also der Wiederherstellungsprozess, desto besser. Darüber hinaus wirken sich umfangreiche Sicherungen, die regelmäßig durchgeführt werden, negativ auf die Netzwerkleistung aus, sofern kein dediziertes Sicherungsnetzwerk eingerichtet wird.

Wenn Sie die optimale Sicherungsstrategie für Ihre Umgebung festgelegt haben, sollten Sie unbedingt eine Testwiederherstellung im gesamten Testnetzwerk durchführen. Durch den Test können Problembereiche identifiziert und nützliche Erfahrungen bei der Wiederherstellung von Systemen in der IDC-Umgebung gewonnen werden, ohne den Druck, ein Produktionssystem wieder online bringen zu müssen.

(Die CommVault Galaxy-Schnittstelle, die weiter unten in diesem Kapitel beschrieben wird, vereinfacht die Datenidentifizierung, so dass Sie die für eine Sicherung geeigneten Daten auswählen und dann wichtige Daten zuerst wiederherstellen können).

Auswählen eines geeigneten Zeitpunktes für die Sicherung

Das Sichern einer E-Commerce-Umgebung ist nicht dasselbe wie das Sichern der Infrastruktur eines lokalen Unternehmensnetzwerks (Local Area Network oder LAN). Bei lokalen Unternehmensnetzwerken nimmt die Netzwerknutzung außerhalb der Hauptgeschäftszeiten im Allgemeinen ab. In einer E-Commerce-Umgebung steigt die Nutzung im Allgemeinen am frühen Abend an und kann bis zu den frühen Morgenstunden auf diesem Niveau bleiben, vor allem dann, wenn die Kundenbasis auf mehrere Zeitzonen verteilt ist. Deshalb ist es u. U. nicht möglich, einen idealen Zeitpunkt für die Sicherung Ihrer Umgebung zu finden. Beachten Sie die folgenden Richtlinien, um die Auswirkungen für die Webkunden zu reduzieren:

- Planen Sie Sicherungen so, dass diese nicht in Webnutzungs-Spitzenzeiten fallen.
- Sichern Sie keine unnötigen Daten.
- Führen Sie regelmäßige Testwiederherstellungsoperationen in einem Testnetzwerk durch, um sicherzustellen, dass die richtigen Sicherungen durchgeführt werden.

Auswählen des geeigneten Sicherungstyps

Es gibt drei Hauptsicherungstypen:

- Normal
- Inkrementell
- Differenziell

Außerdem stellt die CommVault Galaxy-Software zwei Sicherungstypen bereit, die den Sicherungsprozess unterstützen und innerhalb des kritischen Sicherungsfensters Zeit sparen:

- Auxiliary Copy
- Synthetic Full

Normale Sicherung

Bei einer normalen (oder vollständigen) Sicherung werden alle ausgewählten Dateien kopiert und jede Datei als gesichert gekennzeichnet (d. h. das Archivattribut wird deaktiviert). Bei normalen Sicherungen wird nur die aktuellste Kopie der Sicherungsdatei bzw. des Sicherungsbandes benötigt, um alle Dateien wiederherzustellen. Eine normale Sicherung wird im Allgemeinen beim erstmaligen Erstellen eines Sicherungssatzes durchgeführt.

Inkrementelle Sicherung

Bei einer inkrementellen Sicherung werden nur die Dateien gesichert, die seit der letzten normalen oder inkrementellen Sicherung erstellt oder geändert wurden. Die Dateien werden als gesichert gekennzeichnet (d. h. das Archivattribut wird deaktiviert). Bei einer Kombination aus normaler und inkrementeller Sicherung sind der letzte normale Sicherungssatz und alle inkrementellen Sicherungssätze erforderlich, um alle Daten wiederherzustellen.

Differenzielle Sicherung

Bei einer differenziellen Sicherung werden nur die Dateien kopiert, die seit der letzten normalen oder inkrementellen Sicherung erstellt oder geändert wurden. Die Dateien werden als gesichert gekennzeichnet (d. h. das Archivattribut wird deaktiviert). Bei einer Kombination aus normaler und differenzieller Sicherung werden die Dateien oder Bänder aus der letzten normalen Sicherung und der letzten inkrementellen Sicherung benötigt, um alle Daten wiederherzustellen.

Auxiliary Copy

Eine zusätzliche (oder sekundäre) Kopie (Auxiliary Copy) ist eine Kopie der Sicherungsdaten. Die kopierten Daten sind ein echtes Abbild der primären Sicherungskopie und können für den Fall, dass primäre Sicherungsserver, Geräte und Medien verloren gehen oder zerstört werden, als Hot-Standby-Sicherungskopie verwendet werden. Primäre und sekundäre Kopien verwenden unterschiedliche Medien und häufig auch unterschiedliche Sicherungsbibliotheken.

Synthetic Full Backup

Bei einer synthetischen vollständigen Sicherung (Synthetic Full Backup) wird die aktuellste vollständige Sicherung der ausgewählten Daten mit allen folgenden inkrementellen und/oder differenziellen Sicherungen kombiniert und das Ergebnis in einer Archivdatei gespeichert. Synthetische vollständige Sicherungen werden in erster Linie verwendet, um die Leistung von Wiederherstellungsoperationen zu verbessern, denn für eine erfolgreiche Wiederherstellung ist dann nur noch eine einzelne Sicherung erforderlich.

Vor- und Nachteile der verschiedenen Sicherungstypen

Bei der Entscheidung für einen Sicherungstyp müssen die Auswirkungen der Sicherung auf die Netzwerkbandbreite sowie die zur Datenwiederherstellung erforderliche Zeit berücksichtigt werden. In Tabelle 1.1 werden die Vor- und Nachteile der verschiedenen Sicherungstypen beschrieben.

Tabelle 1.1: Vergleich der Sicherungstypen

Sicherungstyp	Vorteile	Nachteile
Normal (vollständig)	Dateien lassen sich einfacher finden, weil sie sich auf dem aktuellen Sicherungsmedium befinden. Erfordert nur ein Medium oder einen Satz Medien zur Dateiwiederherstellung.	Hoher Zeitaufwand. Werden Dateien selten geändert, sind die Sicherungen nahezu identisch.
Inkrementell	Erfordert die geringste Datenspeichermenge. Stellt die schnellsten Sicherungen bereit.	Eine vollständige Systemwiederherstellung kann länger dauern als bei einer normalen oder differenziellen Sicherung.
Differenziell	Für die Wiederherstellung werden nur die Medien aus den letzten normalen und differenziellen Sicherungen benötigt. Stellt eine schnellere Sicherung bereit als die normale Sicherung.	Eine vollständige Systemwiederherstellung kann länger dauern als bei einer normalen Sicherung. Bei einer hohen Zahl von Datenänderungen können die Sicherungen länger dauern als beim inkrementellen Typ.
Auxiliary Copy	Erstellt exakte Kopien der Sicherungsbänder für die Redundanz. Kopien können schneller generiert werden als tatsächliche Sicherungen. Kopien können für die Wiederherstellung intern aufbewahrt werden.	
Synthetic Full	Konsolidiert normale und inkrementelle Sicherungen in einer neuen normalen Sicherung innerhalb einer Bibliothek, die außerhalb des Netzwerkes und/oder von wichtigen Servern gespeichert wird. Reduziert Sicherungs- und Wiederherstellungszeiten.	

Auswählen des geeigneten Speichermediums

Neben der Auswahl des geeigneten Sicherungstyps und Zeitpunktes für die Sicherung sollten Sie sich mit den verfügbaren Speichermedientypen auseinandersetzen und eine geeignete Auswahl treffen.

Berücksichtigen Sie bei der Auswahl eines Speichermediums die folgenden Faktoren:

- die zu sichernde Datenmenge
- den zu sichernden Datentyp
- das Sicherungszeitfenster
- die Umgebung
- die Entfernung zwischen den gesicherten Systemen und dem Speichergerät
- das Budget Ihres Unternehmens
- die Vereinbarungen auf Dienstebene für die Wiederherstellung von Daten

In Tabelle 1.2 werden die Vor- und Nachteile der gängigen Sicherungsmedientypen zusammengefasst.

Tabelle 1.2: Vergleich der Sicherungsmedientypen

Sicherungsmedientyp	Vorteile	Nachteile
Band	Stellt eine schnelle Sicherung und lange Aufbewahrung bereit. Besitzt eine hohe Speicherkapazität. Kostengünstiger als magnetische oder magnetooptische Datenträger.	Schnellerer Verschleiß und höhere Fehleranfälligkeit als bei magnetischen und magnetooptischen Datenträgern. Schwierig zu konfigurieren und zu warten, vor allem in SAN-Konfigurationen. Regelmäßige Reinigung der Laufwerke erforderlich.
Magnetplatte	Einfach zu konfigurieren und zu warten. Kann für Datenstaging verwendet werden.	Das teuerste Medium für die Erstspeicherung.
Magnetooptischer Datenträger	Bietet die längste Lebensdauer ohne Verschlechterung des Mediums.	Bietet die langsamste Sicherung und Wiederherstellung. Schränkt die Hardwareauswahl ein.

Galaxy-Softwaremodule und Hauptfunktionen

Die IDC-Architektur von Microsoft verwendet CommVault Galaxy für Windows 2000 als Sicherungslösung. Zu den Softwaremodulen des CommVault Galaxy-Frameworks gehören folgende Komponenten:

- ein oder mehrere Intelligent DataAgents (iDataAgents), die bestimmte Daten sichern und wiederherstellen
- ein oder mehrere MediaAgents, die die Übertragung von Daten zwischen iDataAgents und Sicherungsmedien überwachen
- ein CommServe StorageManager, der die iDataAgents und MediaAgents steuert

All diese Softwaremodule können sich auf demselben Computersystem, jeweils einzeln auf einem separaten System oder kombiniert auf verschiedenen Systemen befinden.

Zusammen bilden iDataAgents, MediaAgents und CommServe StorageManager eine einzelne *CommCell*, den Hauptbaustein des Galaxy-Frameworks.

CommCell

Die Galaxy-Software unterstützt das Erstellen mehrerer einzelner CommCells. Jede CommCell enthält die für die Anforderungen des zu sichernden Systems benötigte Anzahl von iDataAgents und MediaAgents (zu diesen Anforderungen gehören das Sicherungszeitfenster, der Leistungsdurchsatz und die Datenmenge innerhalb der CommCell). Über einen einzigen Anmeldebildschirm können Benutzer von einer beliebigen webbasierten Konsole im Unternehmen aus die einzelnen CommCells auswählen und verwalten.

Weitere Informationen zur CommCell und den entsprechenden Bereitstellungsoptionen finden Sie unter "Architektur und Bereitstellungsstrategie von Galaxy" weiter unten in diesem Kapitel.

CommServe StorageManager

Ein einzelnes CommServe StorageManager-Softwaremodul (*CommServe*) weist Kombinationen aus MediaAgents und iDataAgents an. CommServe ist das Befehls- und Steuerungszentrum der CommCell. Die CommServe-Software verarbeitet alle Aktivitätsanforderungen zwischen MediaAgents und iDataAgents und überwacht und verwaltet alle Sicherungen und Wiederherstellungen. Es werden ausschließlich Steuerungsinformationen durch das CommServe-Softwaremodul geleitet, nicht die Sicherungs- und Wiederherstellungsdaten selbst.

Das CommServe-Modul beinhaltet die zentralen Ereignis- und Aufgaben-Manager sowie die logische und physische Verwaltungsstruktur und beherbergt außerdem den Metadatenbankkatalog. In dieser Datenbank befinden sich Metadaten zur Art und zum Speicherort der gesicherten Daten. Der zentrale Ereignis-Manager protokolliert alle Ereignisse und stellt bei wichtigen Ereignissen eine einheitliche Benachrichtigung bereit. Der Aufgaben-Manager steuert die wichtigsten Aktivitäten der Software und stellt Neustartfunktionen für Galaxy bereit. Da die CommCell-Konsole bei der Verwendung einer Webbrowserschnittstelle oder eines Microsoft Management Console (MMC)-Snap-Ins angezeigt wird, können Sie das gesamte Galaxy-System remote verwalten, entweder intern aus einem virtuellen lokalen Netzwerk in der IDC-Umgebung oder extern durch den webbasierten Zugriff über ein virtuelles privates Netzwerk (Virtual Private Network oder VPN).

Der CommServe StorageManager kann sich auf einem eigenen dedizierten System befinden oder auf einem System, das auch einen MediaAgent und/oder iDataAgent enthält.

MediaAgent

Das MediaAgent-Softwaremodul verwaltet die Datenverschiebung zwischen den physischen Sicherungsspeichergeräten und den entsprechenden iDataAgents. MediaAgents verwalten die Sicherungsspeichergeräte, die im Allgemeinen über einen lokalen Busadapter angeschlossen sind, wie z. B. über einen SCSI-Adapter. Die MediaAgent-Software wurde so konzipiert, dass sie speichermedienunabhängig ist, und kann somit eine Vielzahl von Speichermodellen unterstützen. Dank dieses Ansatzes können sich Unternehmen schnell an Änderungen in der Speichertechnologie anpassen. MediaAgents kommunizieren z. B. mit den folgenden Speichergerättypen:

- **Bandbibliotheken**. Der MediaAgent verwaltet die verschiedenen Bandmedien und Bandlaufwerke in der Bibliothek sowie die Bewegung des darin befindlichen Roboterarmes. Die Verwendung von Bandbibliotheken spart Zeit, begrenzt die Möglichkeit menschlicher Irrtümer, stellt "Lights-out data protection" (unbedienten, automatisierten Datenschutz) bereit und ermöglicht die Konsolidierung von Daten durch synthetische vollständige Sicherungen.
- **Allein stehende Bandlaufwerke**. Der MediaAgent verwaltet das Bandlaufwerk. Sie müssen Medien manuell laden und entfernen, so dass Sie auf die Verwendung von allein stehenden Bandlaufwerken möglichst verzichten sollten.
- **Magnetplatte.** Die magnetische Speicherung kann aus mehreren Datenträgern oder einem redundanten Array aus unabhängigen Datenträgern (Redundant Array of Independent Disks oder RAID) bestehen. Dank steigender Datenträgergrößen, gesunkener Preise und schnellerer Übertragungsraten hat diese Option an Beliebtheit gewonnen. Die Speicherkosten für Magnetplatten sind immer noch höher als die für Bänder oder magnetooptische Datenträger, in vielen IDC-Umgebungen ist jedoch wegen der Notwendigkeit schneller Sicherungen die Verwendung von Magnetplatten für die Zwischenspeicherung vor der Sicherung auf Band erforderlich.
- **Magnetooptischer Datenträger**. Magnetooptische Datenträger bieten einen Datendurchsatz von 6 Megabyte (MB) pro Sekunde und eine jahrzehntelange Lagerfähigkeit. Strichcodierte magnetooptische Bibliotheken werden immer beliebter als Medium für ein hierarchisches Storage Management, bei dem Richtlinien zur Verschiebung weniger häufig verwendeter Dateien von den teureren Magnetplatten erstellt werden.

iDataAgent

Der iDataAgent (Intelligent DataAgent) ist das Softwaremodul, das die Datenübertragung an die Sicherungsmedien über den MediaAgent verwaltet. Es gibt für jeden verwalteten Datentyp einen spezifischen iDataAgent. In der IDC-Umgebung gibt es bestimmte iDataAgents für die Dateisysteme des Betriebssystems Microsoft Windows® 2000 Server (z. B. Web- und Anwendungsserver), die Computer mit Microsoft Exchange Server 2000 und Microsoft SQL Server™ 2000-Datenbanken. Für jeden verwalteten Datentyp wird pro Clientsystem ein iDataAgent benötigt, unabhängig davon, ob es sich um ein physisches oder virtuelles System handelt, wie z. B. in gruppierten Systemen oder in SAN-Konfigurationen, in denen es viele virtuelle Dateisysteme oder Clients gibt. Jeder iDataAgent kann pro Client mehrere Instanzen des entsprechenden Datentyps verwalten. So kann z. B. ein Galaxy iDataAgent für Windows 2000, der für die Verwaltung des Windows-NTFS-Dateisystems konfiguriert ist, mehrere Dateisysteminstanzen auf demselben Clientcomputer verwalten.

Indizierung

Die Galaxy-Software verwendet ein zweiteiliges synchronisiertes Indizierungsschema. Das Schema besteht aus einem zentralen Metadatenbankkatalog in der CommServe StorageManager-Software und einem Index, der sich auf demselben Computer wie die MediaAgent-Software befindet.

Um die Such- und Wiederherstellungsleistung zu verbessern, verwaltet jeder MediaAgent einen Index der auf die Sicherungsmedien geschriebenen Sicherungsdaten. Eine permanente Kopie des Indexes wird auf den Sicherungsmedien gespeichert, und eine aktive Kopie des Indexes wird auf dem Datenträger des Speichermediums verwaltet, auf dem der MediaAgent installiert ist. Dieser lokale Indexcache ist begrenzt. Beim Schreiben neuer Daten auf die Sicherungsmedien werden neue Indizes erstellt. Mithilfe konfigurierbarer Parameter können Administratoren die Größe des Caches sowie die Lebensdauer des lokalen Indexes festlegen. Wenn der Index die vorkonfigurierte Kapazität überschreitet, werden ältere Indizes mithilfe des am längsten nicht verwendeten (Least Recently Used oder LRU) Algorithmus überschrieben

DataPipe

Die Galaxy DataPipe-Technologie wurde entwickelt, um Daten so schnell zu verschieben, wie der Quellclient diese bereitstellen und das Sicherungsmediengerät diese schreiben kann. Die Galaxy-Software verwendet denselben Prozess zum Schreiben von Sicherungen auf direkt verknüpfte SCSI-Geräte, mit SAN verknüpfte Geräte und Remotenetzwerk-TCP/IP-Verbindungen (Transmission Control Protocol/Internet Protocol).

Die Galaxy DataPipe stellt eine hochleistungsfähige Datenverschiebung mit niedrigem Overhead bereit. Über TCP/IP-Netzwerke können Sie Datenübertragungsraten erreichen, die nah an das theoretische Limit des Netzwerkes heranreichen (abzüglich des Protokolloverheads). Die Datenübertragungsmethode funktioniert mit unterschiedlichen Medientypen ebenso gut wie mit identischen Medientypen.

Dynamische Laufwerkfreigabe

Galaxy kann Bandgeräte (Bibliotheken und Laufwerke) in einer Switched-SAN-Fabric-Konfiguration freigeben, wobei bei mehr als einem MediaAgent alle oder einige Laufwerke der Bandbibliothek gemeinsam genutzt werden.

Die Implementierung der dynamischen Laufwerkfreigabe (Dynamic Drive Sharing oder DDS) in der Galaxy-Software ermöglicht die richtlinienbasierte Freigabe von Bandbibliotheks-Laufwerkressourcen zwischen mehreren Sicherungssystemen. Die Galaxy-Software verwendet eine Softwareebene zur Verwaltung der Gerätefreigabe. Dieser Ansatz stellt eine bedeutend höhere Zuverlässigkeit bereit als eine einfache SCSI-Reserve and Release-Strategie (Reservierung und Freigabe) und sorgt für eine einfachere Datenverwaltung.

Zu den Vorteilen von DDS und Bibliotheksfreigabe gehören die folgenden:

- eine bessere Sicherungsleistung
- eine höhere Investitionsrendite für Hardware
- geringere Hardwareausgaben
- verbesserter Datenschutz
- schnellerer Datenzugriff

Sicherheit

CommVault Galaxy verwendet Authentifizierungsmechanismen, um sicherzustellen, dass die Kommunikation zwischen den Galaxy-Clients (iDataAgents) und den Galaxy-Komponenten (CommServe und MediaAgents) nur zwischen erkannten Modulen durchgeführt wird. Die grafische Benutzeroberfläche (Graphical User Interface oder GUI), eine CommServe-Anwendung, verarbeitet Anforderungen von benutzerinitiierten GUI-Sitzungen; sie ist außerdem verantwortlich für die Anfrage/Antwort-Authentifizierung von Benutzern und für die Verarbeitung der Anforderungen dieser Benutzer. Da CommServe authentifizierte Verbindungen verwendet, können Computer außerhalb des Galaxy-Bereichs keine Verbindung zu Galaxy-Prozessen herstellen.

Die CommCell-Software verwendet ein Netzwerkkennwort als interne Sicherheitsmaßnahme, um sicherzustellen, dass eine Galaxy-Kommunikation nur zwischen CommCell-Computern erfolgt. Standardmäßig weist Galaxy allen Computern in der CommCell ein anderes Kennwort zu (bei dem es sich nicht um ein Kennwort auf Benutzerebene handelt). Sie können jederzeit ein neues CommCell-Netzwerkkennwort für einen Computer in der CommCell festlegen.

Der Zugriff auf die Ressourcen und Funktionen einer CommCell wird auf der Grundlage einer Kombination der CommCell-Ressourcen, Funktionen, Benutzergruppen und Konten erteilt oder verweigert. Der Galaxy-Administrator weist Benutzernamen und Kennwörter zu. Die Galaxy-Benutzerkonten existieren lediglich im Galaxy-Kontext; es handelt sich nicht um Windows-Konten.

Während der Installation erstellt Galaxy einen permanenten Benutzer mit dem Namen *cvadmin*, bei dem es sich um den CommCell-Standardadministrator handelt. Dieser Benutzername kann nach der Installation nicht mehr geändert werden und besitzt alle innerhalb einer CommCell verfügbaren Rechte, einschließlich der Rechte zum Erstellen von Benutzerkonten.

Architektur und Bereitstellungsstrategie von Galaxy

Die IDC-Umgebung ist auf einer mehrstufigen Architektur aus physischen VLANs und verteilten Microsoft .NET-basierten Anwendungsservern aufgebaut. Die empfohlene Data-Storage-Verwaltungsstrategie von Galaxy beinhaltet Verfahren für Sicherungs- und Wiederherstellungsoperationen von der Systemebene bis zu Anwendungen und Anwendungskonfigurationen. Die Strategie schützt die Daten in den einzelnen Systemen, in den virtuellen lokalen Netzwerken (VLANs) und in der gesamten IDC-Umgebung.

Galaxy verwendet alle verfügbaren Technologien, die in IDC verwendet werden, wie z. B. Clustering, Storage Area Network (SAN) für die Geschwindigkeit und Sicherheitstechniken wie IP Security (IPSec), um eine hohe Verfügbarkeit in der IDC-Umgebung zu ermöglichen. Außerdem verwendet Galaxy Clustering zum Schutz gegen ein Failover der Komponenten (wie CommServe und MediaAgents). Die Galaxy-Lösung wurde als Schutz gegen Komponenten-, Server- oder Anwendungsausfälle entwickelt, außerdem als Schutz gegen den Verlust des gesamten Rechenzentrums, wie z. B. im Brandfall.

Da alle Schichten der IDC-Architektur durch die Firewalls und die Switched-VLAN-Umgebung kommunizieren, wird eine verteilte Sicherungs- und Wiederherstellungsarchitektur empfohlen. Diese Empfehlung beruht nicht auf einer Anforderung oder Beschränkung der Galaxy-Software, sondern soll vielmehr die Verfügbarkeit der IDC-Umgebung erhöhen.

Verteilen des MediaAgents als Strategie

Durch das Platzieren eines MediaAgents in allen VLANs wird Folgendes erreicht:

- Eine effektive Kontrolle der Sicherungsdatenübertragung wird möglich.
- Die Menge der zwischen VLANs übertragenen Daten wird reduziert.
- Die Sicherheit für Server wird verbessert und die Firewallkonfiguration vereinfacht.

So beinhaltet das Infrastruktur-VLAN in der IDC-Architektur mindestens fünf Server mit .NET-basierten Anwendungen, die alle mehrere verteilte Komponenten enthalten. Für die Sicherung der einzelnen Anwendungsserver ist es daher erforderlich, Ports an den einzelnen Servern und dem Firewall zu öffnen, um die Verbindung zum Daten/Management-VLAN für den Sicherungsverkehr zu ermöglichen. Wenn ein MediaAgent im Infrastruktur-VLAN platziert wurde, kann der MediaAgent die Anwendungsserver lokal sichern und die Daten später, wenn weniger Netzwerkverkehr herrscht, mit der Funktion Auxiliary Copy der Galaxy-Software auf das Bandmedium im Daten/Management-VLAN kopieren. Um diese Methode verwenden zu können, muss der MediaAgent über den entsprechenden Festplattenspeicher zum Speichern der Sicherungsdaten vor der Übertragung auf das Bandmedium verfügen.

Abbildung 1.1 veranschaulicht die verteilte Galaxy-Architektur für die IDC-Umgebung.

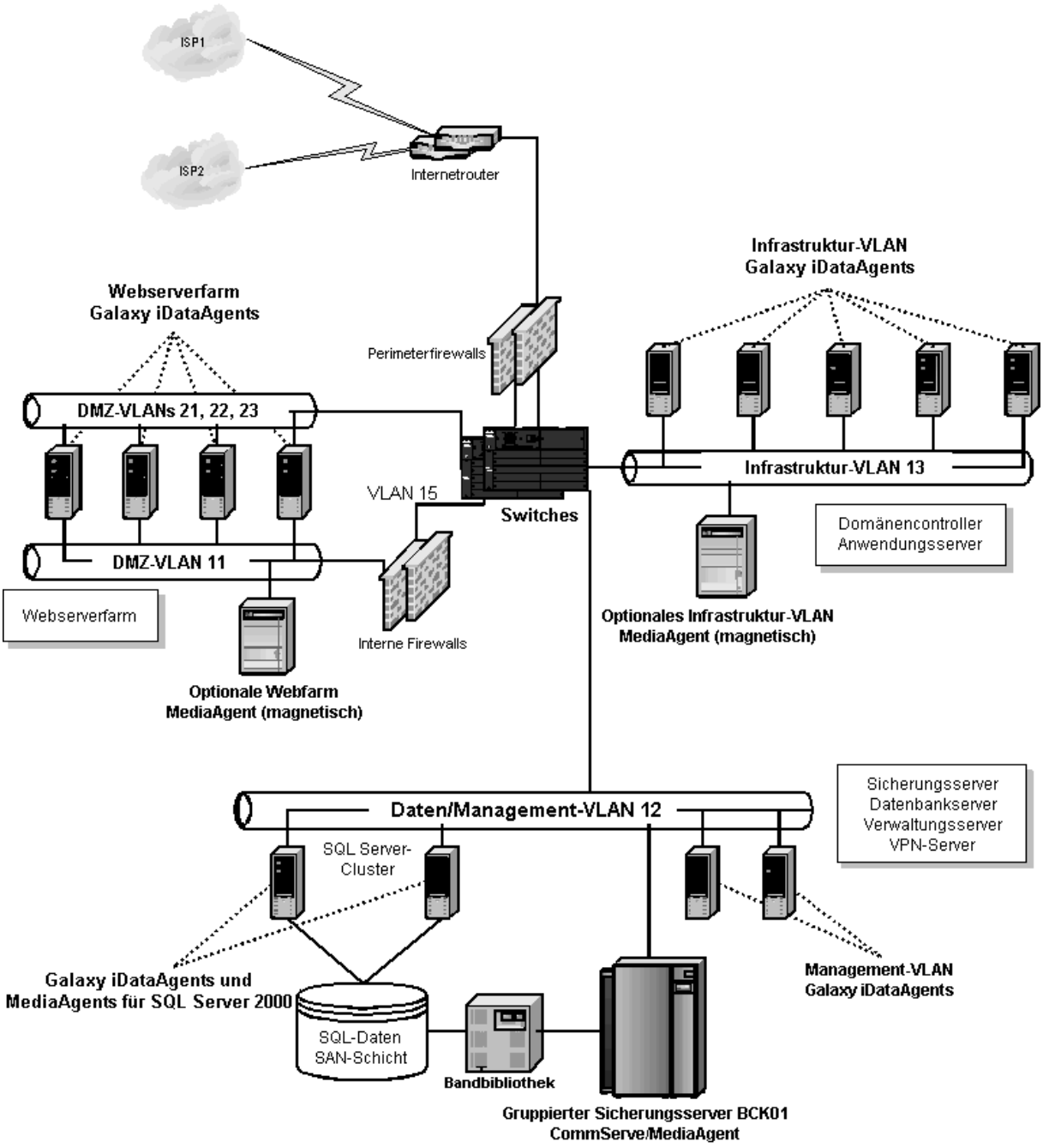

Abbildung 1.1: Verteilte Galaxy-Architektur

CommCell-Bereitstellungsstrategie

Wie bereits erwähnt, bilden iDataAgents, MediaAgents und der CommServe StorageManager zusammen eine CommCell, den Hauptbaustein des Galaxy-Frameworks. Die in Abbildung 1.2 dargestellten Steuerungs- und Datenpfade gehen von einer herkömmlichen LAN-basierten Computerumgebung aus. Wenn die Galaxy-Software in einer Speichernetzwerkumgebung bereitgestellt wird (z. B. beim Sichern von Microsoft SQL Server 2000 im Daten-VLAN), können die Steuerungs- und Datenflüsse unterschiedlich sein.

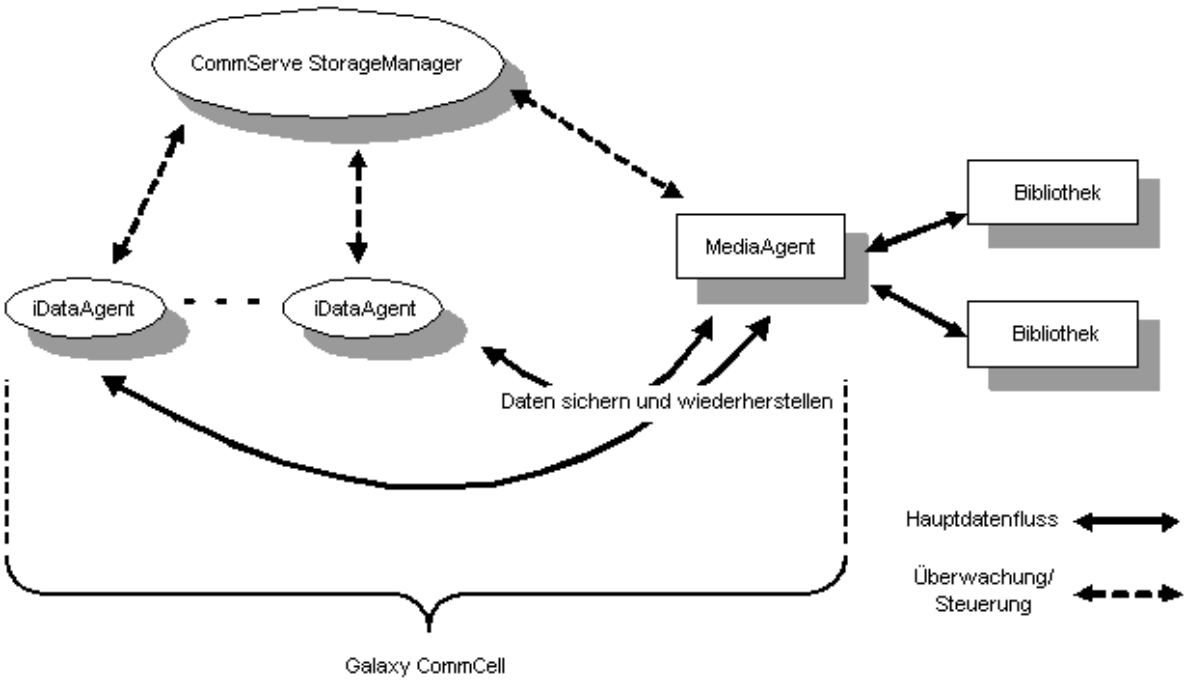

Abbildung 1.2: Galaxy CommCell

Bei extrem großen Systemen gibt Ihnen die Galaxy-Architektur die Möglichkeit, die iDataAgent- und MediaAgent-Module auf demselben Computer zu platzieren, um einen hochleistungsfähigen, direkt verknüpften Durchsatz bereitzustellen (Abbildung 1.3).

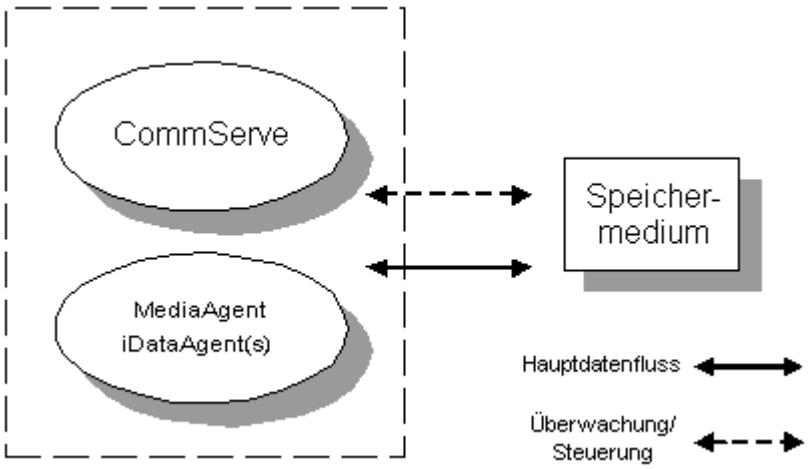

Abbildung 1.3: iDataAgent und MediaAgent in einem großen System

In Umgebungen, in denen eine zentrale Verwaltung und Speicherung wichtig sind (z. B. in Umgebungen, die zentrale Speicherung für eine einzelne Abteilung verwenden, oder in Rechenzentrumsumgebungen mit Doppelboden, in denen alle Operationen zentralisiert werden), passt sich die Galaxy-Lösung mühelos an die Datenschutzstrategie an. Mehrere über das Netzwerk verteilte iDataAgents können Überwachungs- und Steuerungsinformationen und Daten an einen zentral verwalteten MediaAgent und verknüpften Speicher übergeben (Abbildung 1.4).

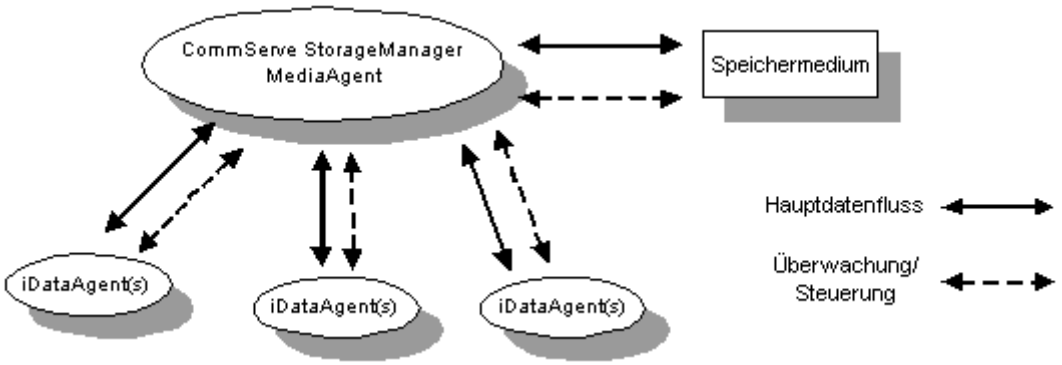

Abbildung 1.4: Zentrale Steuerung in der Galaxy-Lösung

Sie können die Galaxy-Software auch mit einer zentralen Steuerung verteilter Speicher bereitstellen. Dadurch ist es nicht mehr erforderlich, Sicherungsdaten über das lokale Netzwerk zu verschieben, was zu einer bedeutenden Reduzierung der Sicherungs- und Wiederherstellungszeit führt. Abbildung 1.5 veranschaulicht die zentrale Verwaltungssteuerung einer lokalen und Remotespeicherung in einem System, auf dem Galaxy-Software ausgeführt wird. Da zwischen der MediaAgent- und der CommServe StorageManager-Software ausschließlich Steuerungsinformationen übergeben werden, können langsame Kommunikationsverbindungen verwendet werden.

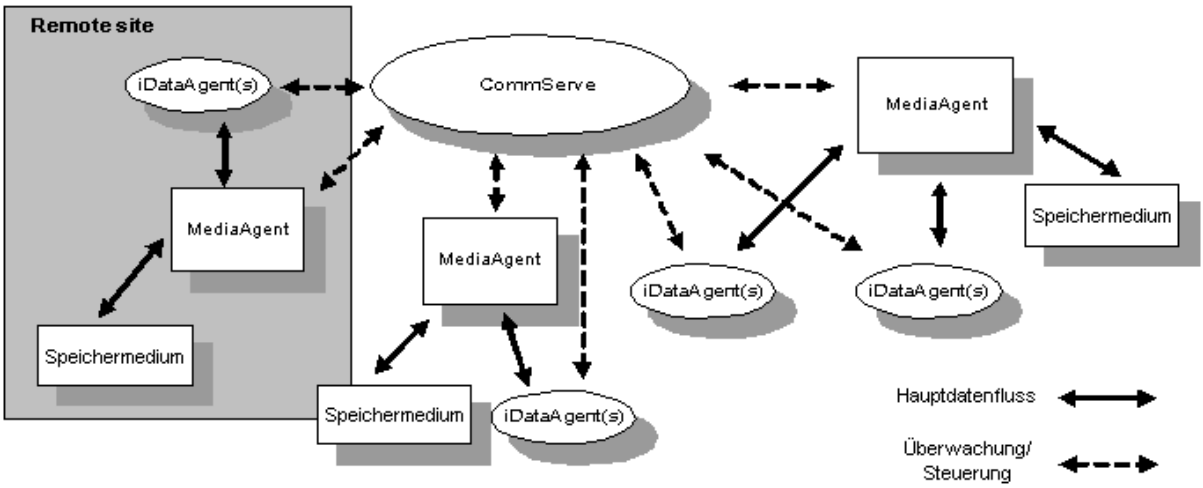

Abbildung 1.5: Verwaltungssteuerung einer lokalen und Remotespeicherung

Die Galaxy-Software unterstützt Storage-Area-Network-Architekturen (SAN) (Abbildung 1.6). In der IDC-Umgebung verwendet der SQL Server 2000-Cluster im Daten-VLAN ein SAN für die Datenspeicherung. Die Galaxy-Bandbibliothek ist auch mit dem SAN verknüpft. Das bedeutet, dass die MediaAgents die SAN-Geschwindigkeit zur Übertragung von Daten an die Bandbibliothek nutzen können. In SAN-Umgebungen unterstützt die Galaxy-Software die LAN-freie sowie die serverfreie und serverlose Sicherung und Wiederherstellung von Anwendungsdaten.

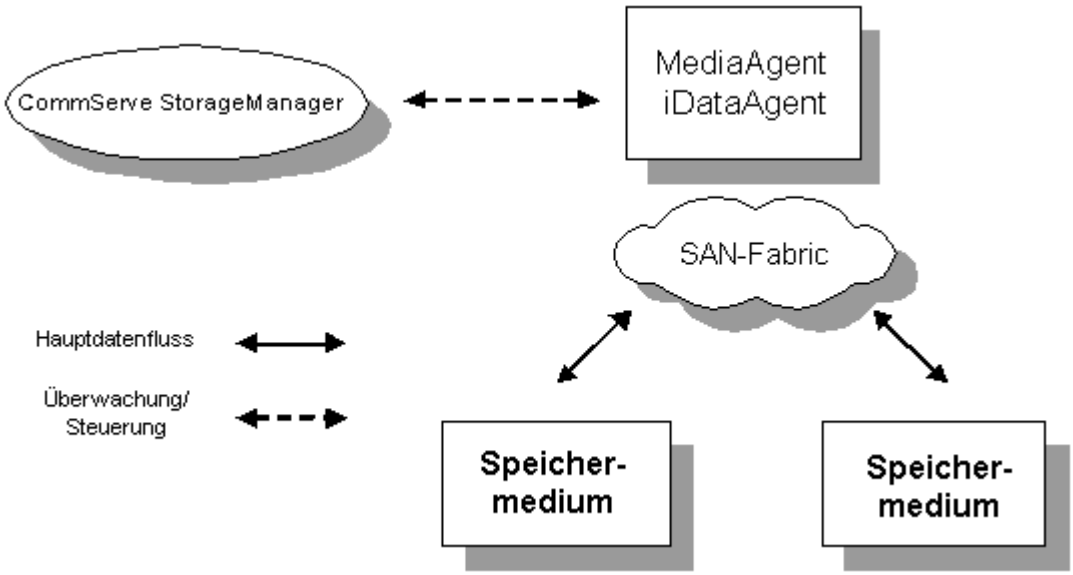

Abbildung 1.6: Galaxy-Software in SAN-Umgebungen

Empfehlung Um DDS zur Freigabe aller Laufwerke in der Bibliothek zu verwenden, konfigurieren Sie alle Laufwerke sowohl in den MediaAgents auf dem SQL Server-Cluster als auch im MediaAgent auf dem CommServe-Modul. Der MediaManager des CommServe-Moduls verwaltet die Ressourcenzuweisung. Detaillierte Informationen zum Konfigurieren von MediaAgents finden Sie in *CommVault Galaxy CommCell Media Management Administration Guide* (englischsprachig).

Entscheiden, was gesichert und wiederhergestellt werden soll

Nahezu jede Systemkomponente kann gesichert werden, und Sicherungsmedien sind relativ erschwinglich. Die Versuchung, alle Komponenten der IDC-Architektur zu sichern, ist daher groß. Eine Lösung dieser Art erfordert jedoch eine beträchtliche Menge Zeit und Bandbreite, um die Sicherung und Wiederherstellung des Systems durchzuführen.

Daher ist es wichtig, einen Blick auf alle Teile der Implementierung der IDC-Architektur zu werfen und zu bestimmen, welche Daten bei Aufruf des Wiederherstellungsplanes wiederhergestellt werden müssen. Diese Vorgehensweise hilft Ihnen, sich für eine effektive Sicherungs- und Wiederherstellungsstrategie zu entscheiden und potenzielle Schwächen im Anwendungsdesign zu identifizieren. Bei bedeutenden Änderungen in der Anwendungsarchitektur sollten Sie Ihre Sicherungsstrategie neu bewerten.

Abbildung 1.7 kann bei der Entscheidung behilflich sein, welche Server in der IDC-Architektur gesichert werden müssen. Die folgende Diskussion stellt Sicherungsempfehlungen für typische IDC-Umgebungen bereit.

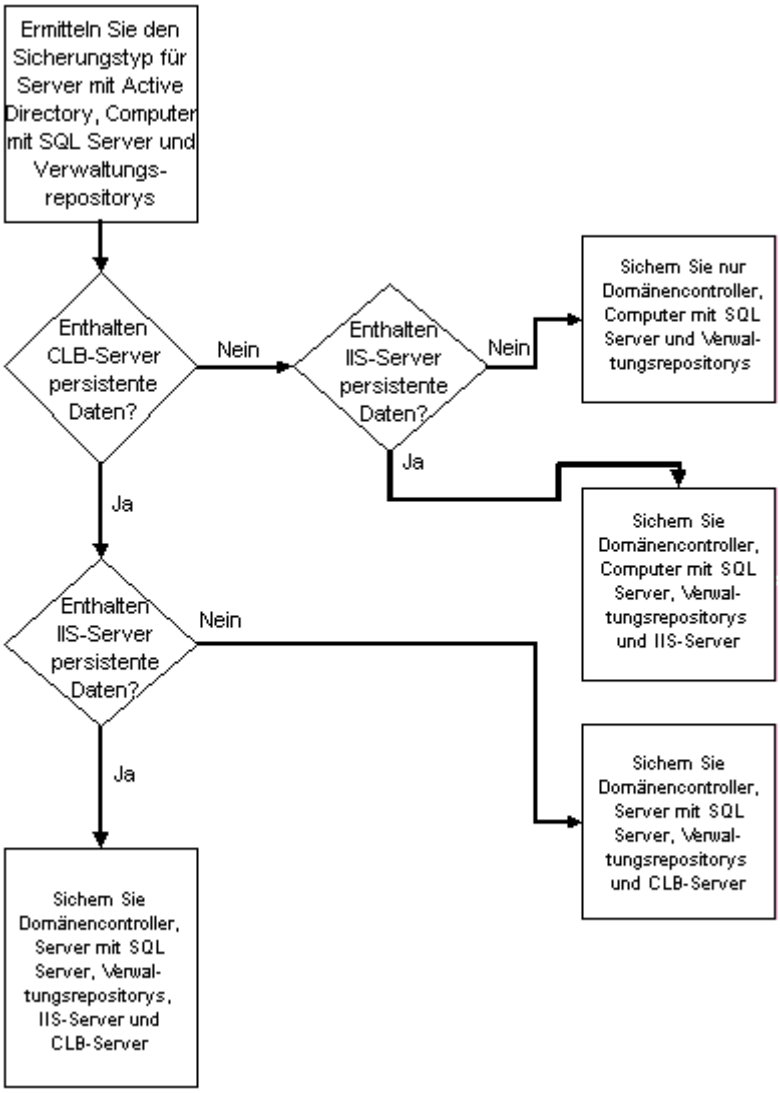

Abbildung 1.7: Flussdiagramm des Sicherungsentwurfs

Front-End-Webwiederherstellung

Es wird empfohlen, dass ein Wiederherstellungsprozess für die Front-End-Webfarm in der IDC-Architektur das Neuerstellen der Server mithilfe automatischer Builds beinhaltet. Eines der Hauptziele des Entwurfs für das Front-End-Web in der IDC-Architektur besteht darin, dass auf keinem der Webserver persistente Daten gespeichert werden sollen. Bei allen Servern der Webschicht handelt es sich um Klone, die Inhalt und Einstellungen von Microsoft Application Center 2000 erhalten, das sich im Infrastruktur-VLAN befindet. Aus diesem Grund müssen die Webserver der meisten Webanwendungen nicht gesichert werden. So wird die zu sichernde Datenmenge enorm reduziert und die Firewallkonfiguration vereinfacht.

In einigen Fällen kann es erforderlich sein, einzelne Webserver zu sichern (z. B. wenn Sie kein Microsoft Application Center 2000 verwenden oder beispielsweise eine Business-to-Business-Anwendung (B2B) ausführen, bei der persistente Daten auf den Webservern gespeichert werden müssen). Sie sollten dies jedoch möglichst vermeiden. Falls erforderlich, können Sie die CommVault Galaxy-Sicherungs- und Wiederherstellungslösung jedoch über einen Firewall verwenden, um die Webserver in dieser Schicht zu sichern und wiederherzustellen.

Empfehlung Für die Sicherung von IDC-Webservern müssen Sie Galaxy iDataAgent für Windows 2000 auf den Servern installieren. Außerdem sollten Sie einen dedizierten Server in diesem VLAN als Host für einen MediaAgent verwenden, der auf Magnetplatte und nicht auf Band schreibt. Dieser Ansatz bietet folgende Vorteile:

- Der Sicherungs- und Wiederherstellungsverkehr wird im VLAN lokalisiert.
- Die Medien sind mühelos verfügbar (Bänder müssen beispielsweise nicht geladen werden), und die Sicherung und Wiederherstellung von Daten auf oder von Magnetplatte ist schnell.
- Sekundäre Kopien können in Zeiten niedriger Netzwerkauslastung (selektiv) auf die Back-End-Bänder kopiert werden.

Infrastruktur-VLAN

Das Infrastruktur-VLAN enthält die Domänencontroller für Windows 2000 und, falls die Anwendungsarchitektur dies erfordert, die Lastenausgleichsserver, auf denen die Komponentendienste ausgeführt werden, die Business-to-Consumer-Komponenten (B2C), auf denen Microsoft Commerce Server ausgeführt wird, und die B2B-Komponenten, auf denen Microsoft BizTalk™ Server ausgeführt wird (einschließlich Produktkatalogsystem, Profilerstellungssystem und Geschäftsprozesspipelines). Außerdem enthält es die Controller und Stagingserver für Application Center 2000. Wenn die Anwendungsarchitektur Active Directory nutzt, um Kundenkontodaten, einschließlich Benutzerauthentifizierung und Computerkonten, in der Active Directory-Datenbank zu speichern, sollte die erfolgreiche Sicherung und Wiederherstellung von Active Directory eine ebenso hohe Priorität besitzen wie die Wiederherstellung der Daten von SQL Server 2000-Computern im Daten-VLAN.

Auch wenn die Webanwendung Active Directory nicht für die Datenspeicherung oder Benutzerauthentifizierung nutzt, ist es trotzdem wichtig, dass die Active Directory-Domänencontroller regelmäßig gesichert werden. Active Directory kann Sicherheitsinformationen speichern, wie z. B. Zertifikate, Replikationskomponenten und Systemressourcen. Darüber hinaus verfügen auch andere Server in der Umgebung über Berechtigungen und Dienstkonten, die auf Instanzen von Konten basieren, die in Active Directory gespeichert sind. Falls eine aktuelle Instanz von Active Directory nicht wiederhergestellt werden kann, ist ein beträchtlicher Aufwand erforderlich, um Computerkonten neu zu synchronisieren und Berechtigungen neu zuzuweisen.

Wenn die Webanwendung ein Array aus Lastenausgleichsservern verwendet, auf denen von Application Center verwaltete Komponentendienste ausgeführt werden, sollten Sie nur den Stagingserver sichern. Da die IDC-Architektur automatische Installationen aller Server bereitstellt, können die Server, auf denen Komponentendienste ausgeführt werden, so schnell neu erstellt werden, wie sie aus einer Sicherung wiederhergestellt werden können; zudem ist das Neuerstellen u. U. weniger problematisch als das Wiederherstellen aus Sicherungen. Da der Stagingserver jedoch die aktuelle Masterkopie der komponentendienstbasierten Anwendung und der Konfiguration für Application Center enthält, sollte er gesichert werden, um die für die Wiederherstellung des gesamten Arrays erforderliche Zeit zu reduzieren.

Empfehlung Auf den Servern muss ein iDataAgent installiert werden. Wie beim Front-End-Web können Sie einen optionalen dedizierten Server als Host für einen MediaAgent verwenden, der auf Magnetplatte und nicht auf Band schreibt. Dieser Ansatz hat folgende Vorteile:

- Der Sicherungs- und Wiederherstellungsverkehr wird im VLAN lokalisiert.
- Die Medien sind mühelos verfügbar (Bänder müssen beispielsweise nicht geladen werden), und die Sicherung und Wiederherstellung von Daten auf oder von Magnetplatte erfolgt schnell.
- Sekundäre Kopien können in Zeiten niedriger Netzwerkauslastung (selektiv) auf die Back-End-Bänder kopiert werden.

Daten-VLAN

Die Datenbankserver mit SQL Server 2000 im Daten-VLAN benötigen höchstwahrscheinlich eine leistungsstarke Sicherungslösung. Sie enthalten wahrscheinlich Kunden- und Finanzinformationen sowie wichtige Daten für die Funktionen der IDC-Webanwendung. Wird keine leistungsstarke Sicherungs- und Wiederherstellungslösung verwendet, könnte dies zu einer beträchtlichen Störung im Unternehmen führen.

Deshalb müssen alle Datenbankserver mit Livedaten so häufig wie möglich gesichert werden. Ein gruppierter iDataAgent für SQL Server 2000 muss auf Computern mit SQL Server 2000 konfiguriert werden.

Empfehlung Durch das Platzieren von MediaAgent und iDataAgents auf derselben physischen Hardware im Daten-VLAN wird die Sicherungszeit reduziert und die Sicherungs- und Wiederherstellungsleistung verbessert. Da die SQL Server 2000-Datenschicht in einer SAN-Umgebung konfiguriert ist, wird durch das Installieren eines MediaAgents auf demselben Server wie der iDataAgent die Geschwindigkeit und Zuverlässigkeit der verfügbaren SAN-Umgebung genutzt, ohne dass zusätzliche Hardwarekosten anfallen.

Standby-Wiederherstellungsoption für das Daten-VLAN

Da das Daten-VLAN aus Datensicht die wichtigste Schicht der IDC-Architektur darstellt, sollten Sie die Datenbanken häufig sichern und sie auf exakt replizierten Computern mit SQL Server 2000 an einem anderen Standort wiederherstellen. Dazu können Sie das Protokollversand-Dienstprogramm von SQL Server 2000 in Verbindung mit der Galaxy-Lösung verwenden. Diese Strategie stellt eine höhere Verfügbarkeit der Datenschicht bereit. Außerdem werden Probleme wie Datenbeschädigung und Virenangriffe verhindert, falls die Daten nicht durch Clustering und Replikation geschützt sind. Diese Option ist kostengünstig und stellt eine Strategie für die Verfügbarkeit in Umgebungen mit einer gewissen Ausfalltoleranz bereit.

Management-VLAN

Überwachungs- und Verwaltungsrepositorys sollten ebenfalls gesichert werden, da sie Verlaufsdaten zum System enthalten. So können beispielsweise Sicherheitsereignisse in diesen Repositorys archiviert werden; einige Unternehmen, wie z. B. Finanzdienstleister, sind u. U. rechtlich dazu verpflichtet, diese Daten für einen bestimmten Zeitraum aufzubewahren.

Zusammenfassung von Empfehlungen

In Tabelle 1.3 werden der Status aller VLANs in einer IDC-Umgebung sowie die relevanten Sicherungs- und Wiederherstellungsempfehlungen zusammengefasst.

Tabelle 1.3: Sicherungs- und Wiederherstellungsempfehlungen

VLAN	Status	Empfehlung
Front-End-Web-VLAN in Standardumgebungen. Front-End-Schnittstellenschicht (oberste Schicht).	Von Application Server 2000 verwaltete Webserverklone. Keine gespeicherten persistenten Daten.	*IIS-Webserverfarm*: Neuerstellen von Servern mithilfe automatischer Builds (keine Sicherungen erforderlich). *Priorität: Niedrig* – Sicherungs-/Wiederherstellungsoption optional.
Front-End-Web-VLAN in bestimmten B2B-Umgebungen. Front-End-Schnittstellenschicht (oberste Schicht).	Von Application Server 2000 verwaltete Webserverklone. B2B-Anwendungen, bei denen persistente Daten auf Webservern gespeichert werden müssen.	Sie müssen persistente Daten sichern. *Priorität: Hoch* – Verwenden Sie eine leistungsstarke Sicherungs- und Wiederherstellungsstrategie.
Infrastruktur-VLAN. Geschäftslogikschicht (mittlere Schicht).	Enthält Geschäftslogik. Kann außerdem Benutzerauthentifizierung und Computerkonten enthalten, die in Active Directory gespeichert sind. Zu den Komponenten gehören der Controller für Application 2000, Stagingserver, Active Directory/Domain Name System-Server (DNS), Commerce Server 2000 (für B2C-Webanwendungen), BizTalk Server 2000 (für B2B-Webanwendungen), Exchange Server 2000 (für die E-Mail-Komponente von BizTalk Server).	*Application Center 2000:* Sie müssen die Controllerkonfiguration für Application Center 2000, Inhalt auf Stagingservern und COM+-Daten sichern. *Active Directory, DNS und Exchange Server 2000*: Sie müssen die B2C-Anwendung und den Systemstatus sichern. *BizTalk Server 2000-Komponenten*: Sie müssen den Systemstatus, alle Komponenten und die B2B-Anwendung sichern. *Priorität: Hoch* – Verwenden Sie eine leistungsstarke Sicherungs- und Wiederherstellungsstrategie.
Daten-VLAN-Datenbankschicht (unterste Schicht).	Enthält wichtige Daten, die von Commerce Server 2000, BizTalk Server 2000 und Webanwendungen verwendet werden. Die Daten werden von gruppierten SQL Server 2000 in einer SAN-Umgebung verwaltet und gespeichert.	*SQL Server 2000*: Sie müssen den Systemstatus und alle Datenbanken sichern. *Priorität: Hoch/Sehr hoch* – Verwenden Sie eine leistungsstarke Sicherungs- und Wiederherstellungsstrategie.
Management-VLAN. Verwaltungs- und Systemmanagement.	Überwachungs- und Verwaltungsserver und VPN-Server.	*Überwachungs- und Verwaltungsrepositorys*: Sie müssen Systemverlaufsdaten sichern. *Priorität: Mittel* – Verwenden Sie eine mittlere Sicherungs- und Wiederherstellungsstrategie.

Entwerfen und Konfigurieren der Galaxy-Lösung

In diesem Abschnitt werden Verfahren zum Entwerfen und Konfigurieren eines Galaxy-Systems für optimale Leistung bereitgestellt.

Um ein Galaxy-System zu entwerfen und zu implementieren, müssen Sie Folgendes ermitteln:

- erforderlicher Speicher
- erforderliche Speichergeräte
- erforderliche MediaAgents

Ihr Erstentwurf eines Galaxy-Systems sollte Ihnen vorläufige Hardware- und Speicheranforderungen bereitstellen. Sie können denselben Prozess dann erneut durchführen, um den Entwurf für bestimmte Speicheranforderungen zu verfeinern. Im Abschnitt "Optimale Vorgehensweisen für das Konfigurieren von Galaxy-Komponenten" weiter unten in diesem Kapitel finden Sie Empfehlungen für die Verbesserung des Entwurfs. Zur Veranschaulichung ist ein Beispiel des Entwurfsprozesses für ein Galaxy-System angegeben.

Überlegungen zur Hardware

Details zur Hardwarelösung, die für die IDC-Architektur verwendet wird, finden Sie auf der folgenden Website:

http://www.microsoft.com/solutions/IDC/default.asp (englischsprachig)

Es ist wichtig, dass Sie ermitteln, welche zusätzliche Systemhardware Sie für die interne Sicherung, die Geräteredundanz und die externe Speicherung benötigen. Bei vielen Umgebungen hat sich die Verwaltung einer Testeinrichtung bewährt, die über dieselben Geräte wie die Produktionsumgebung verfügt, sich jedoch an einem anderen Standort befindet.

Anmerkung Informationen zu den Hardwareanforderungen für Galaxy-Systeme finden Sie in der Dokumentation zu Galaxy oder auf folgender Website: http://www.commvault.com (englischsprachig)

Speicheranforderungen

Bei den Speicheranforderungen handelt es sich um die Gesamtmenge an Speicherplatz und Speichermedien, die zur Aufrechterhaltung von Sicherungen in einem bestimmten Zeitraum erforderlich sind.

Um die Speicheranforderungen Ihres Systems zu berechnen, müssen Sie Folgendes ermitteln:

- Anzahl der Clients
- Datenaufbewahrungsfrist
- erforderlicher Speicher
- erforderliche Speichermedien

Sie müssen zunächst diese Anforderungen ermitteln, um die Größe des von Ihrer Lösung benötigten physischen Speicherplatzes einzuschätzen.

Ermitteln der Anzahl von Clients

Ermitteln Sie die Anzahl der Clientcomputer im Galaxy-System.

Ermitteln des Datenaufbewahrungsschemas

Die Datenaufbewahrungsfrist ist der Zeitraum, für den ein bestimmter Satz von Sicherungsdaten für die Wiederherstellung verfügbar bleiben muss. Wenn die Datenaufbewahrungsfrist abgelaufen ist und Sie das Löschdienstprogramm ausgeführt haben, sind die Medien zur Wiederverwendung verfügbar.

Verwenden Sie folgende Kriterien, um das Datenaufbewahrungsschema zu ermitteln:

- Anzahl der vollständigen Sicherungszyklen, die im Speicher aufbewahrt werden (*Zyklen*). Ein vollständiger Sicherungszyklus beinhaltet die vollständigen Sicherungen sowie alle anderen Sicherungen bis zur nächsten vollständigen Sicherung.
- Anzahl der inkrementellen/differenziellen Sicherungen in einem vollständigen Zyklus (*Inkremente*).

Ermitteln des erforderlichen Speichers

Der erforderliche Speicher ist die Gesamtmenge von Daten, die während der Datenaufbewahrungsfrist auf den Speichermedien verwaltet werden. Index ist der auf dem MediaAgent erforderliche Platz zum Speichern der Indexdaten, die die in einer bestimmten Sicherung gespeicherten Benutzerobjekte definieren. Der Index wird am Ende der Sicherung auf den Speichermedien archiviert.

Verwenden Sie die folgenden Kriterien, um Ihre Gesamtspeicheranforderungen zu ermitteln:

Erforderlicher Speicher = Vollständige Sicherungen + Inkrementelle Sicherungen + Index

Wobei gilt:

Vollständige Sicherungen = (Zyklen * Verwendeter Speicherplatz)

Inkrementelle Sicherungen = (Zyklen * Tägliche Änderung * Inkremente)

Index = 4 % (Vollständige Sicherungen + Inkrementelle Sicherungen)

Verwendeter Speicherplatz ist der gesamte Speicherplatz, der für alle Clients verwendet wird.

Zyklen ist die Anzahl der vollständigen Sicherungszyklen.

Tägliche Änderung ist die geschätzte tägliche Datenänderungsrate.

Inkremente ist die Anzahl der inkrementellen und/oder differenziellen Sicherungen in jedem vollständigen Sicherungszyklus.

Nehmen Sie beispielsweise an, dass der Sicherungszyklus für Ihr System vier Wochen beträgt und Sie sechs inkrementelle Sicherungen pro Woche ausführen. Gehen Sie dann davon aus, dass der auf allen Clients verwendete Gesamtspeicherplatz (Verwendeter Speicherplatz) 1 Terabyte (TB) beträgt und sich die geschätzte tägliche Änderung (Tägliche Änderung) auf 10 % bzw. 100 Gigabyte (GB) beläuft.

Die Größe aller vollständigen Sicherungen ist wie folgt:

(4 Zyklen * 1 TB) = 4 TB

Die Größe aller inkrementellen Sicherungen ist wie folgt:

(4 Zyklen * 6 Inkremente * 100 GB Tägliche Änderung) = 2,4 TB

Die Größe des Indexes ist wie folgt:

4 % von 6,4 TB = 256 GB

Der erforderliche Speicher ist wie folgt:

4 TB + 2,4 TB + 256 GB = 6,656 TB

Ermitteln der Speichermedienanforderung

Die Speichermedienanforderung ist die Menge an physischen Medien (Band, Magnetplatte oder magnetooptischer Datenträger), die benötigt wird, um die gesamten Speicheranforderungen für die Datenaufbewahrungsfrist zu erfüllen.

Verwenden Sie die folgenden Kriterien, um Ihren Speichermedienbedarf zu ermitteln:

*Speichermedien = Erforderlicher Speicher / (Medien * Komprimierungsrate)*

Wobei gilt:

Speichermedien ist die Menge erforderlicher Speichermedien.

Erforderlicher Speicher ist das im vorherigen Beispiel berechnete Gesamtergebnis.

Medien ist die unkomprimierte Kapazität des verwendeten Medientyps.

Komprimierungsrate ist das Komprimierungsverhältnis der Hardware.

Wenn Sie auf der Grundlage des vorherigen Beispiels davon ausgehen, dass das von Ihnen verwendete Band unkomprimiert eine Kapazität von 60 GB hat und die Hardwarekomprimierung ein Komprimierungsverhältnis von 2:1 zulässt, benötigen Sie die folgende Anzahl von Bändern:

6,656 TB / (60 GB * 2) = 56 Bänder

Ermitteln der Speichergeräteanforderung

Die Speichergeräteanforderung ist die Anzahl von Bandlaufwerken, die benötigt wird, um eine vollständige Sicherung simultan auf allen Clients durchzuführen, damit die Sicherungen innerhalb eines bestimmten Zeitraumes oder Sicherungszeitfensters beendet werden.

Verwenden Sie die folgenden Kriterien, um Ihren Speichergerätebedarf zu ermitteln:

Laufwerke (Minimum) = (Vollständig / Sicherungsrate) / Sicherungszeitfenster

*Laufwerke (Maximum) = (Clients * Datenströme * Sicherungsdauer) / Sicherungszeitfenster*

Wobei gilt:

Laufwerke ist die Anzahl erforderlicher Bandlaufwerke.

Vollständig ist die Größe einer einzelnen vollständigen Sicherung für alle Clients.

Sicherungsrate ist die geschätzte Sicherungsrate in GB pro Stunde.

Sicherungszeitfenster ist das Sicherungszeitfenster (die für die Durchführung von Sicherungen zur Verfügung stehende Zeit) in Stunden.

Nehmen Sie auf der Grundlage des vorherigen Beispiels an, dass die vollständige Sicherungsgröße für alle Clients 1 TB beträgt, dass Ihr Laufwerk eine Sicherungsrate von 35 GB pro Stunde ermöglicht, dass das Sicherungszeitfenster acht Stunden beträgt, jeder Client 2 Sicherungsdatenströme hat und dass die Sicherung pro Client zwei Stunden dauert.

Die Mindestzahl erforderlicher Laufwerke ist dann wie folgt:

(1 TB / 35 GB pro Stunde) / 8 Stunden = 4 Laufwerke

Die maximale Anzahl erforderlicher Laufwerke ist dann wie folgt:

(30 Clients * 2 Datenströme * 2 Stunden) / 8 Stunden = 15 Laufwerke

Ermitteln der Anzahl von MediaAgents

Ein Galaxy MediaAgent verwaltet die Bibliothek und die Übertragung von Daten zwischen Clients und Sicherungsmedien.

Verwenden Sie die folgenden Kriterien, um Ihren Bedarf an MediaAgents zu ermitteln:

MediaAgents = Laufwerke / Laufwerke pro Bibliothek

Wobei gilt:

MediaAgents ist die Anzahl der erforderlichen MediaAgents.

Laufwerke ist die Anzahl erforderlicher Bandlaufwerke.

Laufwerke pro Bibliothek ist die Anzahl der Laufwerke in der Bibliothek.

Wenn Sie auf der Grundlage des vorherigen Beispiels davon ausgehen, dass eine Bibliothek 10 Sicherungslaufwerke enthält, ist die erforderliche Anzahl von MediaAgents wie folgt:

15 Laufwerke / 10 = 2 MediaAgents

Optimale Vorgehensweisen für das Konfigurieren von Galaxy-Komponenten

Durch das Konfigurieren von Galaxy-Komponenten und das Befolgen optimaler Vorgehensweisen für eine bestmögliche Leistung können Sie das von Ihnen entworfene Galaxy-System verbessern. Sie können bestimmte Komponenten oder Anwendungen konfigurieren oder die Speicheranforderungen an die Anforderungen Ihrer speziellen IDC-Umgebung anpassen.

Die folgende Konfiguration wird bereitgestellt, um die Verfügbarkeit und Leistung der IDC-Umgebung zu verbessern und zu unterstützen.

Konfigurieren von CommServe

In diesem Abschnitt werden optimale Vorgehensweisen und Empfehlungen für das Implementieren von Galaxy CommServe in der IDC-Umgebung bereitgestellt.

CommServe-Redundanz

Das CommServe-Modul sollte in einer gruppierten Windows 2000-Umgebung implementiert werden.

CommServe-Dimensionierung

Ein CommServe-Modul kann bis zu 35 Clients verwalten. Die Anzahl der Clients in der Umgebung kann variieren, je nachdem, welches Design und welche Hardware Sie verwenden. Bei Umgebungen mit mehr als 35 Clients sollten Sie ein weiteres CommServe-Modul bereitstellen.

Hardware und Software für CommServe

Verwenden Sie zur Optimierung der Leistung eines gruppierten CommServe-Moduls einen Computer mit vier Prozessoren, der unter Windows 2000 Advanced Server ausgeführt wird. Der Computer sollte die folgenden Mindestanforderungen erfüllen:

- Pentium-kompatibler Prozessor mit 700 Megahertz (MHz) oder schnellerer Xeon-Prozessor
- 2 GB RAM
- Mindestens 8 GB Festplattenspeicher zuzüglich Indexcache

Konfigurieren von MediaAgents

In diesem Abschnitt werden optimale Vorgehensweisen und Empfehlungen für das Implementieren von Galaxy MediaAgents in der IDC-Umgebung bereitgestellt.

MediaAgent-Dimensionierung

Um die Leistung zu erhöhen und den Netzwerkverkehr zu reduzieren, platzieren Sie einen MediaAgent auf demselben Computer wie ein iDataAgent mit hohen Speicheranforderungen.

MediaAgent-Redundanz

Ein MediaAgent kann in einer gruppierten Windows 2000-Umgebung implementiert werden, in der Failoverfunktionen erforderlich sind.

Datenaufbewahrung

Verwenden Sie einen Zyklus von vier Sicherungen pro Monat für das Datenaufbewahrungsschema. Führen Sie einmal pro Woche eine vollständige Sicherung und täglich inkrementelle Sicherungen durch.

Verwenden Sie bei der Planung von vollständigen Sicherungen die Option **Start new media** in den Advanced Backup Options.

Speicherrichtlinien

Verwenden Sie für jeden iDataAgent eine separate Speicherrichtlinie.

Nehmen Sie den Clientnamen und iDataAgent-Typ in alle Speicherrichtliniennamen auf (z. B. Server1_SQL).

Erhöhen Sie die Anzahl von Datenströmen, so dass diese der maximalen Anzahl konfigurierter Laufwerke entspricht.

Komprimierungsmodi

Verwenden Sie für alle Speicherrichtlinien die Hardwarekomprimierung, indem Sie das Attribut **Hardware Compression** festlegen.

Hardware und Software für MediaAgent

Verwenden Sie zur Optimierung der Leistung des Servers, der den MediaAgent verwaltet, einen Computer mit vier Prozessoren, der unter Windows 2000 Server ausgeführt wird. Der Computer sollte die folgenden Mindestanforderungen erfüllen:

- Pentium-kompatibler Prozessor mit 700 MHz oder schnellerer Xeon-Prozessor
- 2 GB RAM
- Mindestens 8 GB Festplattenspeicher zuzüglich Indexcache

Konfigurieren von Speichermedien

Wenn Sie in der IDC-Umgebung Speichermedien verwenden, beachten Sie die folgenden Empfehlungen:

- Verwenden Sie magnetische Medien nur dann, wenn die Gesamtspeicheranforderung auf einem Client unter 20 GB liegt.
- Wenn sich die primäre Kopie einer Sicherung auf einem magnetischen Medium befindet, müssen Sie eine zusätzliche Kopie erstellen, von der Sie sekundäre Kopien auf Band machen können.
- Setzen Sie für magnetische Medien kurze Datenaufbewahrungsfristen fest (z. B. zwei Tage für eine vollständige Sicherung).

Konfigurieren der externen Speicherung

Wenn Sie eine externe Speicherung konfigurieren, beachten Sie die folgenden Empfehlungen:

1. Weisen Sie jeden iDataAgent einer Speicherrichtlinie zu. Wenn ein iDataAgent mehrere Subclients besitzt, weisen Sie alle derselben Speicherrichtlinie zu.
2. Benennen Sie die Speicherrichtlinie mithilfe eines einfachen Namensschemas, wie z. B. *Hostname_Anwendungstyp*. Wenn beispielsweise ein Server namens Avocado, der unter Exchange Server ausgeführt wird, als Host für zwei Galaxy iDataAgents namens Dateisystem und Exchange-Datenbank dient, werden die Speicherrichtlinien, auf die der Server zeigt, Avocado_fs und Avocado_exdb genannt.
3. Verwenden Sie bei der Planung von vollständigen Sicherungen die Option **Start new media** in den Advanced Backup Options. Auf diese Weise wird das vorherige aktive Band für die Speicherrichtlinie als Full gekennzeichnet.

Wenn Sie diese Schritte durchführen, können Sie Bänder wöchentlich offsite nehmen. Um festzustellen, welche Bänder Sie offsite nehmen können, führen Sie den Bericht Backups on Media für die entsprechenden Speicherrichtlinien in der CommCell aus, und geben Sie an, dass der Bericht nur die Bänder anzeigen soll, die für die Bibliothek als Full und In gekennzeichnet sind.

Falls die Datenaufbewahrungsfrist für die auf den externen Bändern gespeicherten Daten noch nicht abgelaufen ist, können Sie die Bänder wieder vor Ort bringen und die Daten wiederherstellen. Ist die Datenaufbewahrungsfrist abgelaufen und die Bänder wurden nicht wieder verwendet, können Sie das Galaxy Disaster Recovery Tool (Wiederherstellungstool) verwenden, um die Daten wiederherzustellen.

Anmerkung Das Wiederherstellungstool unterstützt aktuell die Wiederherstellung von Daten aus Dateisystemsicherungen. Im Verlauf des Jahres wird CommVault Unterstützung für Exchange 2000 und andere Anwendungstypen hinzufügen.

Wenn Sie ausgewählte Sicherungsmedien (z. B. vollständige Sicherungen für das Ende des Monats, Quartals und Jahres) behalten möchten, verwenden Sie die Option **View media** in der Galaxy Backup History, um die entsprechenden Bänder zu identifizieren und sicherzustellen, dass sie nicht wieder verwendet werden. Verwenden Sie das Wiederherstellungstool, um die Sicherungen von den Bändern wiederherzustellen.

Verwenden Sie die Funktion für eine zusätzliche Kopie (Auxiliary Copy) der Galaxy-Software, um zu verhindern, dass die externen Daten veralten. Dazu ist ein separater Satz Bänder erforderlich, die speziell für die externe Sicherung verwendet werden. Die Funktion für eine zusätzliche Kopie kopiert Galaxy-Archivdateien von der primären Kopie einer bestimmten Speicherrichtlinie auf eine zusätzliche (sekundäre, tertiäre usw.) Kopie. Der Kopiervorgang kann zwischen gleichen Medien (z. B. von Band zu Band) oder unterschiedlichen Medien (z. B. von Magnetdatenträger zu Band) durchgeführt werden. Nach Ausführen der zusätzlichen Kopie können Sie das zur zusätzlichen Kopie gehörende Band offsite nehmen. Die Ablaufzeiten (Aufbewahrungszeiten) für die Daten der zusätzlichen Kopie können länger sein als die Aufbewahrungszeiten auf der primären Kopie.

Konfigurieren von iDataAgents für SQL Server 2000

Wird Stripping unterstützt, verwenden Sie Speicherrichtlinien für mehrere Datenströme.

Die Auswirkung von Sicherungen auf einen Client

Zum Ausführen von Sicherungen werden Hardwareressourcen (vor allem CPU und RAM) auf dem Clientcomputer benötigt. Wie sehr sich ein Sicherungsvorgang auf einen Client auswirkt, hängt davon ab, welche Hardwareressource verfügbar ist und ob gleichzeitig andere Vorgänge auf dem Clientcomputer ausgeführt werden.

- Stellen Sie sicher, dass der Clientcomputer zumindest die in Kapitel 2, "Backup and Restore Deployment" (bisher nur englischsprachig verfügbar), beschriebenen Mindestanforderungen erfüllt.
- Führen Sie alle unwichtigen Aufgaben oder anderen Vorgänge (z. B. Virenprüfungen) außerhalb des Sicherungszeitfensters durch.
- Führen Sie Sicherungen auf einem Client abends oder an Zeitenpunkten durch, an denen minimale Aktivität auf dem Client herrscht.
- Führen Sie Sicherungen von Subclients nacheinander aus.
- Stellen Sie das Betriebszeitfenster so ein, dass Sicherungen nicht tagsüber oder während anderer aktiver Zeiten durchgeführt werden.