Windows 2000 Advanced Server: Clustertechnologie zur Unterstützung der Microsoft ITG-Infrastrukturdienste

Whitepaper

(engl. Originaltitel: Windows 2000 Advanced Server: Clustering Microsoft ITG Infrastructure Service)

Kurzzusammenfassung

Microsoft® Cluster Server (MSCS), erstmals mit dem Betriebssystem Windows NT® Server 4.0 Enterprise Edition eingeführt, wird unter Windows® 2000 als Clusterdienst bezeichnet. Der Clusterdienst in Windows 2000 Advanced Server und Windows 2000 Data Center Server stellt eine hohe Verfügbarkeit bereit, da ein Server in einem Cluster die Ausführung eines Dienstes oder einer Anwendung übernehmen kann, wenn der Server, auf dem dieser Dienst bzw. die Anwendung ausgeführt wurde, ausfällt – ein Verfahren, das als *Failover* bezeichnet wird. Diese Dienste und Anwendungen werden über so genannte "virtuelle Server" bereitgestellt. Ein virtueller Server verhält sich für den Benutzer wie ein einzelnes System. Der Cluster kann eine beliebige Anzahl virtueller Server bereitstellen, deren Leistung nur durch die Kapazität der einzelnen Server im Cluster und den verfügbaren Speicherplatz beschränkt ist. Die Clusterserver werden vom Administrator als eine einzige Einheit gesteuert, wobei die Verwaltung des Clusters remote durchgeführt werden kann.

Die Information Technology Group (ITG) von Microsoft hat als einer der ersten Produktanwender mehrere kritische Infrastrukturdienste unter dem Betriebssystem Microsoft 2000 Advanced Server im Cluster gruppiert, bevor dieses in die Produktion ging. Vor jeder größeren Produktfreigabe wird die neue Microsoft-Software von der ITG bereitgestellt, um das jeweilige Produkt in der Praxis zu testen.

Zu den Vorteilen des Clusterdienstes zählen für die ITG:

- **Die Unterstützung eines parallelen Updates:** Bei einem parallelen Update wird ein Server (ein so genannter *Knoten*) in einem Cluster offline geschaltet und aktualisiert, anschließend werden sämtliche Clusterressourcen auf diesen Knoten verschoben und dasselbe Verfahren für die anderen Knoten durchgeführt. Dieses Verfahren ermöglicht es, die Ausfallzeiten auf ein Minimum zu reduzieren, was vor allem in der Softwareumgebung der ITG sehr wichtig ist, in der häufige Aktualisierungen für den Ablauf der Softwareentwicklung erforderlich sind.

- **Verbesserte Verwendung der Hardwareressourcen**: Ein Cluster mit freigegebenen Servern unterstützt beispielsweise den Zugriff Tausender Benutzer auf mehrere Terabyte Daten, die sich in Tausenden von Dateiordnern befinden, und kann dennoch schnelle Antwortzeiten aufrechterhalten.

- **Höhere Verfügbarkeit**: Das Zusammenfassen der Daten auf einem Servercluster sorgt dafür, dass der Failoverschutz des Serverclusters für alle Daten bereitgestellt wird. Sowohl die geplanten als auch die ungeplanten Ausfallzeiten werden minimiert, wobei viele Failover bei der ITG weniger als eine oder zwei Minuten dauern.

- **Einfacher Benutzerzugriff**: Aufgrund der Integration der Freigaben auf vielen einzelnen Dateiservern in eine freigegebene Verzeichnisstruktur im Cluster ist ein einfacherer und schnellerer Benutzerzugriff auf die Freigaben möglich. Die Benutzer greifen auf einen virtuellen Server zu und wissen dabei nicht, auf welchem der physischen Server im Cluster die Daten jeweils gespeichert sind.

Dieses Whitepaper beschreibt die Hardware- und Softwarespezifikationen, auf deren Grundlage die ITG mehrere kritische Infrastrukturdienste unter Windows 2000 Advanced Server in seiner Windows 2000-Produktionsdomäne im einheitlichen Modus im Cluster bereitgestellt hat. Diese grundlegenden Infrastrukturdienste stellen die Basis der neuen weltweiten Windows 2000-basierten Netzwerkarchitektur von Microsoft dar.

Im ersten Teil dieses Whitepapers werden die allgemeinen Komponenten des Clusterdienstes für alle Infrastrukturdienste erläutert, die die ITG wie hier beschrieben implementiert hat. Der zweite Teil liefert genauere Informationen über die geclusterten ITG-Infrastrukturdienste, wie den DHCP-Dienst (Dynamic Host Configuration Protocol), den WINS-Dienst (Windows Internet Naming System) und das verteilte Dateisystem DFS (Distributed File System). Es werden repräsentative Hardwarespezifikationen für die verschiedenen Server sowie Tipps zur Überwachung und Verwaltung gegeben. Beachten Sie, dass die Namen und IP-Adressen nur als Erläuterungsbeispiele dienen und es sich aus Sicherheitsgründen nicht um tatsächlich verwendete Namen handelt.

Das Unternehmensnetzwerk von Microsoft enthält sowohl ein internes Netzwerk (Corpnet) als auch ein Netzwerk, an das die Kunden angeschlossen sind (Interneteigenschaften). Dieses Whitepaper befasst sich im Wesentlichen mit den Corpnet-Servern, die sich im Hauptsitz des Unternehmens, in Redmond, Washington, befinden. In anderen Teilen des globalen Unternehmens Microsoft sind die Serverspezifikationen möglicherweise etwas anders. Das vorliegende Dokument stützt sich auf die ursprüngliche Entwicklungsarbeit, mit der die ITG vor der Veröffentlichung von Windows 2000 Advanced Server begonnen hat. Es ist unbedingt zu berücksichtigen, dass die Serverkonfigurationen und –spezifikationen häufig geändert wurden und auch künftig erweitert werden.

Dieses Whitepaper richtet sich an IT-Architekten, Entwickler und Berater auf der Unternehmensebene. Es handelt sich nicht um eine Bedienungsanleitung. Für jede Unternehmensumgebung gelten eigene Bedingungen, und daher sollte jede Organisation die in diesem Dokument beschriebenen Pläne, Spezifikationen und "Erkenntnisse" an die jeweils eigenen Anforderungen anpassen.

Übersicht über den Clusterdienst

Durch die Bereitstellung einer hohen Verfügbarkeit, indem die Dienste für die Clients von mehreren Servern zur Verfügung gestellt werden, sorgt der Clusterdienst für minimale Ausfallzeiten und Supportkosten. Wenn ein Server ausfällt, stellt ein anderer Server im Cluster die Dienste des ausgefallenen Servers zur Verfügung. Die Ressourcen, die die Dienste für die Clients bereitstellen, werden für diese als *virtuelle Server* angezeigt. Diese virtuellen Server sind nicht an irgendeinen bestimmten physischen Server gebunden, und es ist für die Clients nicht ersichtlich, von welchem physischen Server die Dienste tatsächlich bereitgestellt werden. Den Clientbenutzern ist nicht bewusst, dass sie nicht mit einem eigenständigen Server, sondern mit einem Cluster kommunizieren. Das Clustering erlaubt der ITG darüber hinaus, parallele Hardware- und Softwareupdates auf in Clustern gruppierte Knoten durchzuführen, wobei die geplanten Ausfallzeiten minimal sind (normalerweise unter einer oder zwei Minuten).

Das vorliegende Dokument definiert einen Cluster als eine Gruppe von zwei unabhängigen Computersystemen, so genannten Knoten, auf denen der Windows 2000 Advanced Server-Clusterdienst ausgeführt wird und die beide mit einem gemeinsamen externen Speicher verbunden sind und zusammen als ein einzelnes System arbeiten, um sicherzustellen, dass für das Unternehmen wichtige Dienste und Ressourcen stets für die Clients verfügbar sind.

Der Clusterdienst basiert auf einem *freigabelosen* Modell, bei dem jeder Server Besitzer der lokalen Geräte ist und diese verwaltet. Geräte, die im Cluster gemeinsam verwendet werden, wie ein gemeinsam verwendeter Datenträger oder Verbindungsmedien, sind im selektiven Besitz eines Servers und werden stets nur von einem einzigen Server verwaltet.

Das freigabelose Modell vereinfacht die Verwaltung von Speichermedien, Standardanwendungen und Diensten. Das Verwenden dieses Modells ermöglicht die Unterstützung von Windows 2000- und Windows NT-basierten Anwendungen und Datenträgerressourcen sowie "clusterfähigen" Anwendungen und Diensten, wie SQL Server™ 2000 und Microsoft Exchange 2000, durch den Clusterdienst.

Cluster für den Clusterdienst sind nicht mit anderen Clustertechnologien unter Windows 2000, wie z. B. Netzwerklastenausgleich (Network Load Balancing, NLB), zu verwechseln. Beispielsweise verwendet die ITG den Netzwerklastenausgleich für die Verteilung eingehender Webanforderungen innerhalb eines Clusters von Internetserveranwendungen (die z. B. auf Microsoft Internetinformationsdienste basieren, dem in Windows 2000 Server integrierten Webserver) sowie für Proxy- und Streamingmedien-Dienste. Die ITG verwendet Clusterdienst-Server zur Bereitstellung von Infrastrukturdiensten, wie DHCP, WINS und DFS sowie Back-End-Messaging- und Datenbankanwendungen.

Der Clusterdienst unterstützt Windows 2000- und Windows NT Server-basierte Standardtreiber für lokale Serverspeichermedien und deren Verbindungen. Für die externen Speichermedien, die im Cluster gemeinsam verwendet werden, sind jedoch SCSI-Geräte erforderlich. Der Clusterdienst unterstützt PCI-basierte Standard-SCSI-Verbindungen, einschließlich SCSI-Bus mit mehrfachen Initiatoren sowie SCSI über Fibre Channel (FC). Bei Fibre Channel-Verbindungen handelt es sich um SCSI-Geräte, die statt an einem SCSI-Bus an einem Fibre Channel-Bus angeschlossen sind.

Virtuelle Server

Anwendungen und Dienste, die auf den Knoten im Cluster ausgeführt werden, werden für die Benutzer und Arbeitsstationen als *virtuelle Server* angezeigt. Bei einem virtuellen Server handelt es sich um eine Gruppe, die aus einer oder mehreren Ressourcen besteht, die eine Anwendung oder einen Dienst bereitstellen. Jede dieser Gruppen hat einen eigenen Netzwerknamen sowie eine eigene IP-Adresse und stellt eine Failovereinheit dar. Da jeder virtuelle Server über einen eigenen Netzwerknamen und eine eigene IP-Adresse verfügt, unterscheidet sich das Verfahren zur Herstellung einer Verbindung mit einem virtuellen Server für den Benutzer oder Client nicht von einer Verbindung mit einem einzelnen physischen Server. Tatsächlich wird die Verbindung mit einem virtuellen Server hergestellt, der auf einem beliebigen Knoten im Cluster ausgeführt werden kann.

Auf einem Clusterknoten können mehrere virtuelle Server ausgeführt werden, die mehrere Anwendungen oder Dienste darstellen, wie aus Abbildung 1 ersichtlich ist.

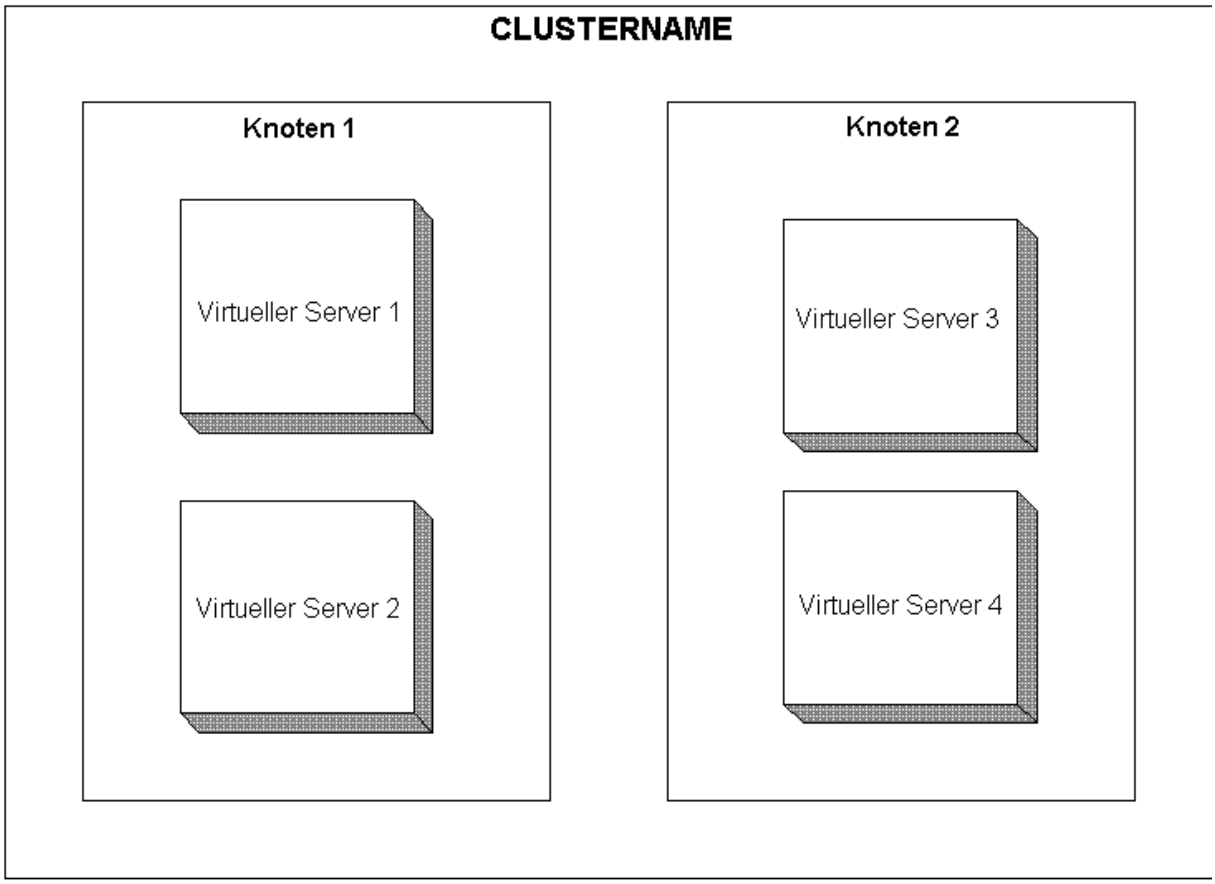

Abbildung 1: Virtuelle Server unter Clusterdienst

Die Clients stellen eine Verbindung mit der IP-Adresse her, die vom Clusterdienst für den virtuellen Server veröffentlicht wird. Im Fall eines Anwendungs- oder Serverfehlers wird die gesamte Ressourcengruppe, die den Dienst oder die Anwendung zur Verfügung stellt, vom Clusterdienst auf einen anderen Knoten innerhalb des Clusters verschoben. Wenn der Client während der aktuellen Sitzung einen Ausfall erkennt, versucht er, die ursprüngliche Verbindung genauso wiederherzustellen. Da der Clusterdienst die IP-Adresse des virtuellen Servers ganz einfach einem intakten Knoten im Cluster zuweist, kann der Client die Verbindung zu der betroffenen Anwendung oder dem Dienst wiederherstellen, ohne dass ersichtlich wird, dass diese(r) jetzt auf einem anderen Knoten im Cluster ausgeführt wird. Die Clientansicht der vier virtuellen Server auf dem Client ist in Abbildung 2 dargestellt.

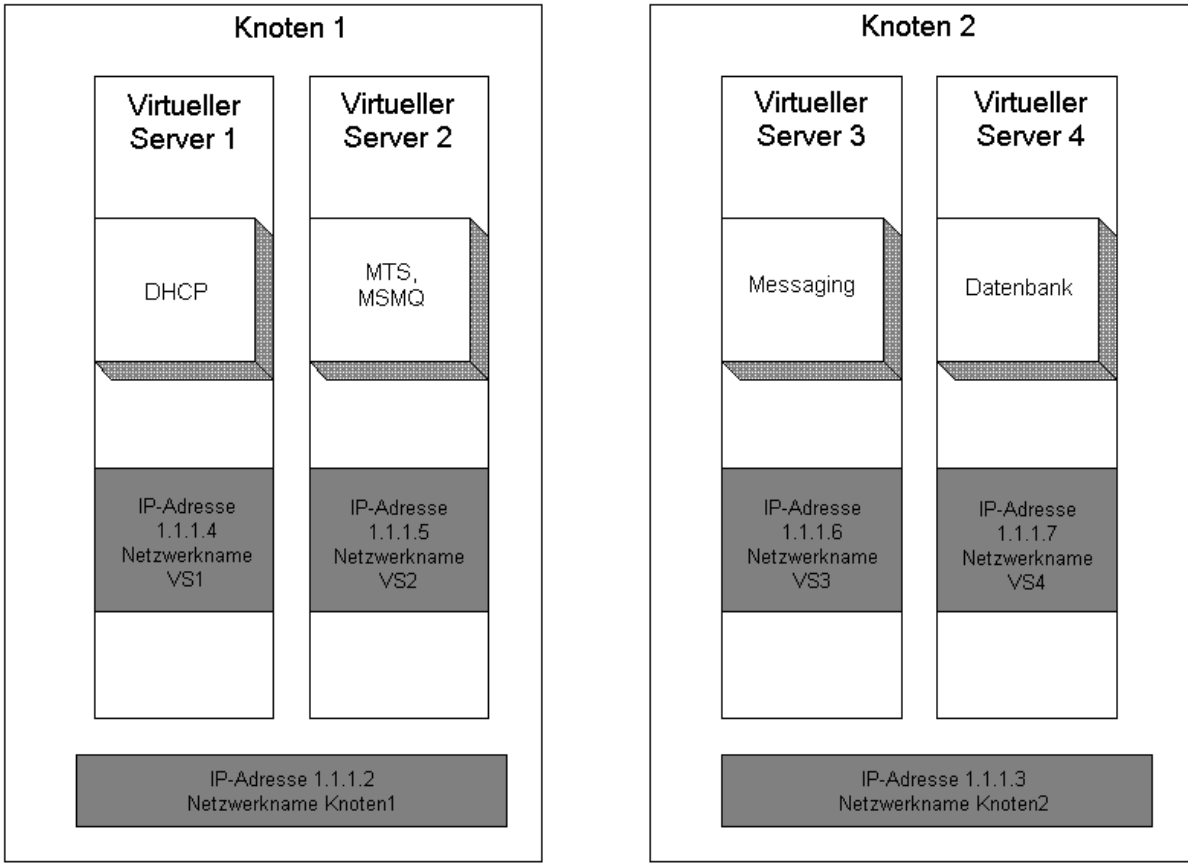

Abbildung 2: Clientseitige Ansicht der virtuellen Clusterdienst-Server

Anmerkung Microsoft Transaction Service (MTS) und Microsoft Message Queue (MSMQ) sind in Windows 2000 Server enthalten.

Hardwarekomponenten

Ein Cluster besteht aus einer Reihe von Hardwarekomponenten, zu denen *Knoten*, ein *Clusterdatenträger* und *Netzwerkschnittstellen* gehören.

Knoten: Ein Windows 2000 Advanced Server-Cluster besteht aus zwei identischen Servern, die als *Knoten* bezeichnet werden. Ein Knoten ist ein Server, der Windows 2000 Advanced Server als Betriebssystem verwendet. Die Knoten müssen entweder Domänencontroller oder von einem Domänencontroller authentifizierte Mitgliedsserver sein. Sie verfügen über eigene Ressourcen, wie eine Festplatte und eine dedizierte Netzwerkschnittstellenkarte (Network Interface Card, NIC) für die private Clusternetzwerkkommunikation. Darüber hinaus haben die Knoten in einem Cluster gemeinsamen Zugriff auf Clusterressourcen, wie ein externes Festplattenspeichersystem, das als *Clusterdatenträger* bezeichnet wird.

Clusterdatenträger: Ein Clusterdatenträger ist ein externes Speichersystem, das mit allen Knoten in einem Cluster verbunden ist. Jeder Knoten im Cluster enthält außerdem seinen eigenen separaten Systemdatenträger. Die ITG verwendet externe Festplattenarrays, so genannte Storage Area Networks (SANs) als Clusterdatenträger.

Netzwerkschnittstellenkarten (NICs): ITG verwendet doppelte Netzwerkadapter, die in einem Cluster zwei Dienste bereitstellen: Die Clientkommunikation und die private Clusterkommunikation. Für die Konfiguration der einzelnen NICs sind drei Einstellungen möglich:

- Clientkommunikation mit dem Cluster
- Clusterknotenkommunikation innerhalb des Clusters
- Beide Funktionen

Ein Beispiel für eine Clusterkonfiguration mit zwei Netzwerkschnittstellen ist in Abbildung 3 dargestellt. Beide NICs sind mit dem Firmennetzwerk verbunden – eine sorgt für die Clientverbindung, während die andere nur für die interne Clusterkommunikation zuständig ist.

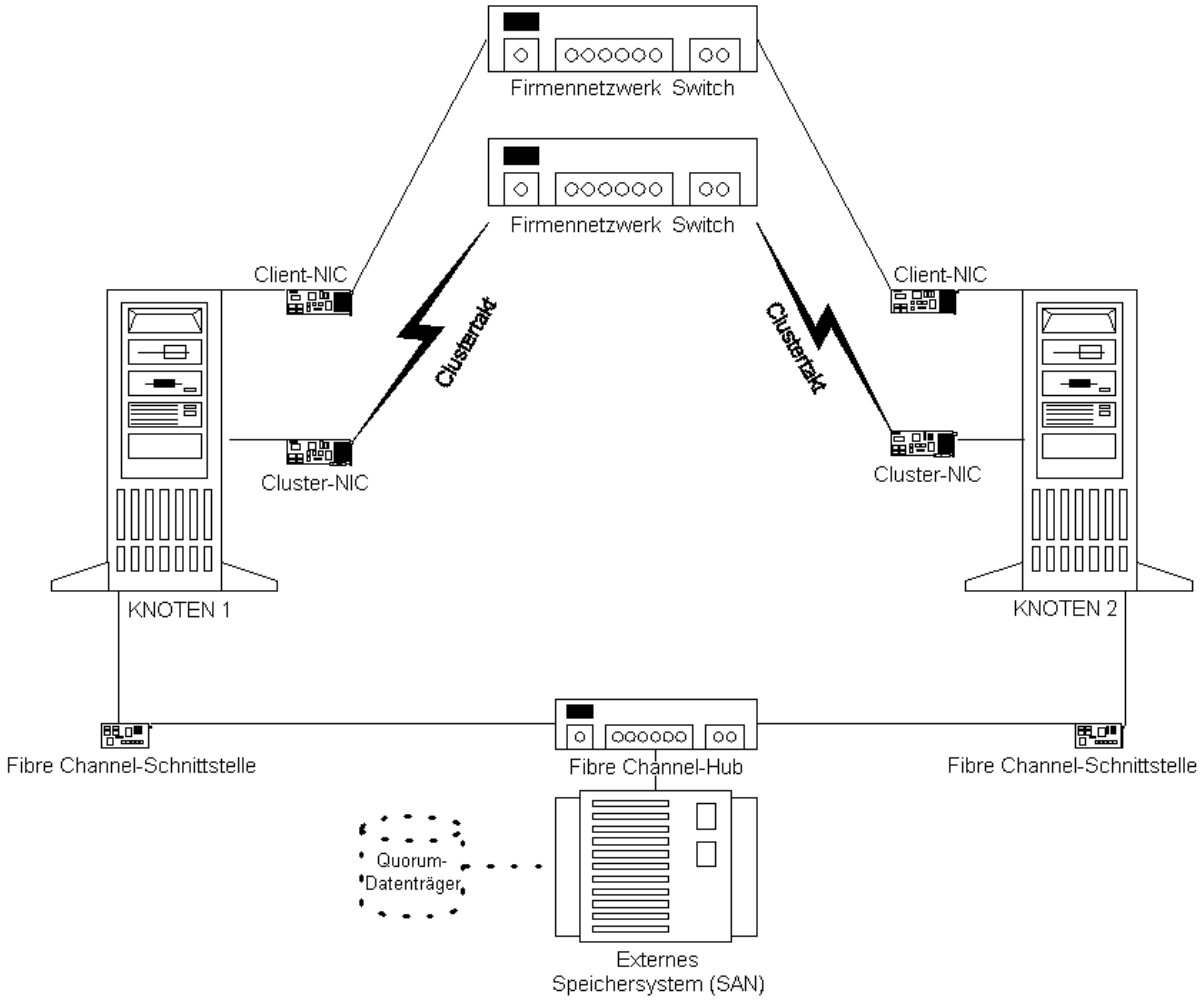

Abbildung 3: Beispiel einer Clusterkonfiguration mit zwei NICs

SANs

Ein Storage Area Network (SAN) ist ein Hochgeschwindigkeitsnetzwerk, das eine direkte Verbindung zwischen den Speicherelementen und Hostservern bereitstellt. Ein SAN kann für lokale oder entfernte, gemeinsam verwendete oder dedizierte Speichermedien verwendet werden. Mithilfe von SANs hat die ITG die Möglichkeit, über größere Entfernungen auf externe Speichermedien zuzugreifen, wobei serielle Fibre Channel-Verbindungen (FC-Signal mit 1GBit/s) verwendet werden.

Die ITG-Analyse hat gezeigt, dass mithilfe von SANs die Leistung für viele Anwendungen verbessert werden könnte, die große Datenmengen zwischen mehreren Servern über das Netzwerk übertragen: Netzwerkressourcen werden für andere Transaktionen freigegeben, und die Übertragung von Massendaten über das SAN ist wesentlich schneller, da ein gemeinsamer Speicher verwendet wird. Vor der Implementierung von SANs wurde von der ITG beispielsweise eine umfangreiche Verkaufsdatenbank verwaltet, für die am Wochenende fünf Mal 70 GB Daten über das Netzwerk übertragen werden mussten und 24 Stunden geplanter Ausfallzeit erforderlich waren. Die SAN-Architektur sorgt dafür, dass dasselbe Verfahren nur 2 bis 3 Stunden dauert, wobei das Netzwerk nicht beansprucht wird.

Als weiteres Beispiel hat die ITG ebenfalls mehrere große Server entwickelt und implementiert, auf denen SQL Server ausgeführt wird, die einen über FC angeschlossenen externen RAID-Festplattenspeicher verwenden. Der größte Teil dieses Speichers ist für die einzelnen Server reserviert, verfügt aber über FC-Controller und einen gemeinsamen FC-Hub oder –Switch. Mehrere SQL Server-basierte Server verwenden einen gemeinsamen Clusterdatenträger und umgehen beim SQL-Verwaltungsverfahren "Sichern – Kopieren – Laden" die Phase des Kopierens. Die Analyse der ITG zeigte, dass Verzögerungen beim Sichern, Kopieren und Laden üblicherweise aufgrund mangelnder Netzwerkgeschwindigkeiten zwischen benachbarten Servern auftraten. Durch das Verwenden eines gemeinsamen Sicherungsdatenträgers war der zeitintensivste Teil des Verfahrens – das Kopieren – nicht mehr erforderlich.

Zu den wichtigsten Elementen der verschiedenen hardwarespezifischem SANs gehören Folgende:

- *Externer Speicher*: Speicher, der nicht für den privaten Zugriff einzelner Server installiert ist.
- *Zentraler Speicher*: Speicher, auf den zentral zugegriffen und der zentral verwaltet und kontrolliert werden kann.
- *Remoteclustering*: Speicher, auf den sowohl einzelne als auch mehrere Server zugreifen können.

Die Hardwarekomponenten, aus denen ein SAN besteht, ähneln denen eines Netzwerks, das über Speicherelemente verfügt. Hostserver benötigen FC-Schnittstellen und Speicherkomponenten, wie Bandgeräte, Festplattenlaufwerke, RAID-Controller sowie Hubs und Switches.

Punkt-zu-Punkt-Topologien sowie hubbasierte FC-AL (FC Arbitrated Loop)- und switchbasierte FC Fabric-Verbindungen stehen zur Verfügung. Der aktuelle FC-Standard basiert auf einer Datenübertragungsrate von 1 GBit/s, die sowohl mit Kupferkabel als auch optischen Medien über große Entfernungen erreicht wird. Die maximale Anzahl der Knotenadressen beträgt für eine einzelne FC-AL-Verbindung 127 Knoten, und die maximale Anzahl FC-Switches beträgt 16 Millionen. In einem SAN können Hubs und Switches kombiniert werden.

Die einzige Software, die erforderlich ist, um einen Server an einem SAN zu beteiligen, ist ein PCI-HBA-Schnittstellentreiber (Hostbusadapter).

Quorum-Datenträger

Der wichtigste Datenträger im SAN ist der Quorum-Datenträger, bei dem es sich um einen einzelnen Datenträger im System handelt, der als *Quorumressource* bezeichnet wird – ein Datenträger, der für den Fall eines Systemausfalls einen permanenten physischen Speicher bereitstellt. Auf diesem Datenträger ist die Clusterkonfiguration gespeichert, und alle Knoten im Cluster müssen in der Lage sein, mit dem Knoten zu kommunizieren, der Besitzer dieses Datenträgers ist. Es ist möglich (wird jedoch nicht empfohlen), einen Datenträger sowohl zum Speichern der Daten der Clusteranwendungen und –dienste als auch als Quorum-Datenträger zu verwenden.

Wenn ein Cluster erstellt wird oder wenn die Netzwerkkommunikation zwischen den Knoten eines Clusters vorübergehend ausfällt, wird die Quorumressource verwendet, um zu verhindern, dass die Knoten mehrere Cluster bilden. Um einen Cluster zu bilden, muss ein Knoten den Besitz der Quorumressource anfordern und diesen übernehmen. Wenn ein Knoten beispielsweise während des Erkennungsprozesses einen Cluster nicht findet, versucht er, seinen eigenen Cluster zu bilden, indem er die Steuerung der Quorumressource übernimmt. Wenn der Knoten damit jedoch keinen Erfolg hat, kann er keinen Cluster bilden.

Auf der Quorumressource wird die aktuellste Version der Clusterkonfigurationsdatenbank in Form von Wiederherstellungsprotokollen und Registrierungsprüfpunktdateien gespeichert, die knotenunabhängige Informationen zur Clusterkonfiguration sowie Statusdaten enthalten. Wenn ein Knoten einem Cluster beitritt oder diesen bildet, wird die private Kopie der Konfigurationsdatenbank des betreffenden Knotens vom Clusterdienst aktualisiert. Wenn ein Knoten einem bestehenden Cluster beitritt, kann der Clusterdienst die Daten von den anderen aktiven Knoten abrufen. Der Clusterdienst verwendet die Wiederherstellungsprotokolle der Quorumressource, um folgende Aufgaben durchzuführen:

- Er stellt sicher, dass nur jeweils ein Satz aktiver kommunizierender Knoten als Cluster arbeiten darf.
- Er sorgt dafür, dass ein Knoten nur dann einen Cluster bilden kann, wenn er in der Lage ist, die Steuerung der Quorumressource zu übernehmen.
- Er sorgt dafür, dass ein Knoten nur dann einem bestehenden Cluster beitreten kann oder in einem bestehenden Cluster verbleibt, wenn er mit dem Knoten kommunizieren kann, der die Quorumressource steuert.

Eine einfache Clusteranordnung, die den Besitz des Quorum-Datenträgers zeigt, ist in Abbildung 4 dargestellt.

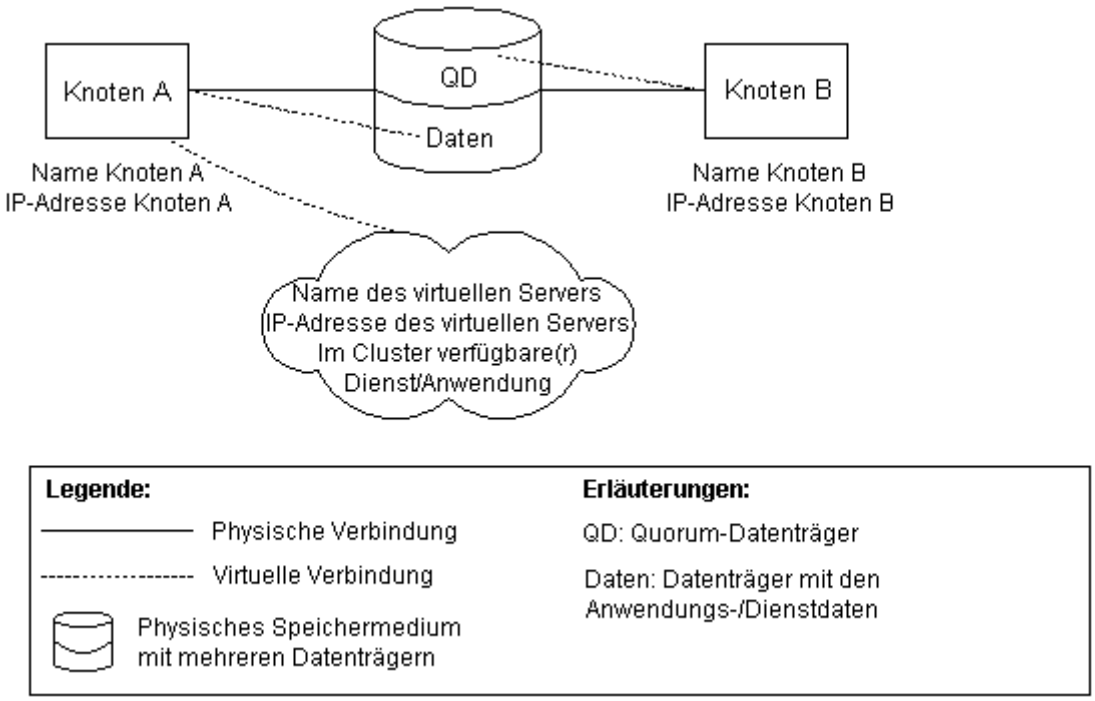

Abbildung 4: Eine einfache Clusterkonfiguration

In dieser Abbildung sind zwei Knoten mit einem SAN verbunden, aber das SAN enthält mehrere Datenträger (in diesem Fall zwei).

Knoten A stellt einen virtuellen Server bereit. Das heißt, er stellt den Netzwerknamen, die IP-Adresse, den Dienst oder die Anwendung zur Verfügung und hat exklusiven Zugriff auf die Anwendungs- bzw. Dienstdaten, die mit diesem virtuellen Server verbunden sind. Knoten B ist an der Bereitstellung des virtuellen Servers für die Clients nicht aktiv beteiligt.

Knoten B ist Besitzer des Quorum-Datenträgers, womit deutlich wird, dass der Knoten, der den virtuellen Server zur Verfügung stellt, nicht unbedingt der Knoten sein muss, der ebenfalls die Quorumressource steuert. Knoten A könnte in diesem Cluster Besitzer des Quorum-Datenträgers sein. Die ITG empfiehlt als optimale Vorgehensweise, die Daten für einen virtuellen Server nicht auf dem Datenträger im SAN zu speichern, der als Quorum-Datenträger fungiert.

Failover

Der Clusterdienst verwendet das private Netzwerk, um Knotenausfälle und Statusänderungen festzustellen und den Cluster als eine Einheit zu verwalten. In einem vordefinierten Intervall (standardmäßig alle 5 Sekunden) werden "Clustertakt"-Meldungen gesendet. Wenn ein Knoten mit einer bestimmten Häufigkeit (standardmäßig 3 Mal) nicht auf diese Meldungen reagiert, leitet der intakte Server das vorkonfigurierte Failoververfahren ein.

Hardwareanforderungen

Jede Clusterdienstlösung (einschließlich Knoten, Controller und Speichersystem) muss die Hardwareanforderungen von Windows 2000 Advanced Server erfüllen. Die Hardware muss sich in der Hardwarekompatibilitätsliste (HCL) für den Clusterdienst befinden. Beispielsweise müssen beide der HCL-entsprechenden Knoten über folgende Komponenten verfügen:

- Zwei PCI-Netzwerkadapter – einen für die Verbindung zum öffentlichen Netzwerk und den anderen für das private Clusternetzwerk zwischen den Knoten.
- Einen separaten PCI-Speicherhostadapter (SCSI oder Fibre Channel) für die gemeinsamen Datenträger, und zwar zusätzlich zum Adapter für den Startdatenträger für jeden einzelnen Knoten.
- Ein HCL-entsprechendes SAN, das an alle Knoten angeschlossen ist und als Clusterdatenträger verwendet wird. Alle gemeinsamen Datenträger, einschließlich des Quorum-Datenträgers, müssen physisch an einen gemeinsamen Bus angeschlossen und auf allen Knoten erreichbar sein. SCSI-Geräten müssen eindeutige SCSI-ID-Nummern zugewiesen werden, und sie müssen ordnungsgemäß abgeschlossen werden. Die gemeinsamen Datenträger müssen als Windows 2000-Basisdatenträger konfiguriert sein (nicht dynamisch), und alle Partitionen auf den Datenträgern müssen NTFS-formatiert sein. Obwohl nicht erforderlich, wird die Verwendung einer fehlertoleranten RAID-Konfiguration für alle Datenträger dringend empfohlen.
- Speicherkabel für den Anschluss der gemeinsamen Speichergeräte an alle Computer.
- Identische Hardware für alle Knoten, und zwar für jeden einzelnen Steckplatz und jede Karte. Dies erleichtert die Konfiguration und vermeidet mögliche Kompatibilitätsprobleme.

Softwarekomponenten

Ein Cluster enthält verschiedene Softwarekomponenten, einschließlich dem Betriebssystem, dem Clusterdienst, den Clusterressourcen sowie den im Cluster verfügbaren Diensten und Anwendungen selbst. Beachten Sie, dass einige Softwarekomponenten direkt zu den Hardwarekomponenten in Beziehung stehen.

Betriebssystem: Auf jedem Knoten im Cluster muss Windows 2000 Advanced Server ausgeführt werden. Windows 2000 Server bietet keine Clusteringunterstützung. Windows 2000 Advanced Server unterstützt Cluster mit zwei Knoten.

Clusterdienst: Auf jedem Knoten im Cluster muss der Clusterdienst installiert sein. Dieser Dienst muss mit einem Domänenbenutzerkonto ausgeführt werden, damit von beiden Knoten die Authentifizierung durchgeführt werden kann. Dasselbe Konto muss auf allen Knoten verwendet werden und dort ein Administratorkonto sein.

Ressourcen: Ressourcen sind einzelne Elemente, die innerhalb des Clusters verschiedene Aufgaben erfüllen. Hierzu gehören Datenträgerressourcen, die Quorumressource, IP-Adressen, Netzwerknamen sowie im Cluster verfügbare Dienste.

Datenträger: Die im Clusterdatenträger, der mit allen Knoten verbunden ist, konfigurierten Datenträger. Damit ist in diesem Zusammenhang nicht die physische Hardware gemeint, die mit allen Knoten verbunden ist. Ein Datenträger ist eine Ressource innerhalb eines Clusters, die für das Speichern von Dienst- bzw. Anwendungsdaten und/oder als Quorumressource zur Verfügung steht. Beachten Sie, dass auf einem einzelnen physischen Datenträgersystem mehrere Datenträger konfiguriert werden können. In einem SAN enthält der Datenträger die Daten, die entweder von den Diensten, von Serveranwendungen, die im Cluster ausgeführt werden, oder von Anwendungen verwendet werden, die den Cluster verwalten. Zu jedem Zeitpunkt kann immer nur ein Knoten des Clusters einen der Datenträger des Cluster-SANs besitzen oder darauf zugreifen. Der Besitz eines Datenträgers wechselt von einem Knoten zum nächsten, wenn für die Datenträgergruppe ein Failover erfolgt oder wenn sie auf einen anderen Knoten verlagert wird.

- **Quorum-Datenträger**: Auf dem Quorum-Datenträger (der auch als "Quorumressource" bezeichnet wird) ist die Clusterkonfigurationsdatenbank gespeichert, die Informationen zur Wiederherstellung des Clusters in seiner aktuellen Konfiguration enthält. Die Datenbank befindet sich auf einem physischen Speicher, so dass der Cluster in Betrieb gehen kann, falls ein Knoten ausfällt. Um einen Cluster zu bilden, muss ein Knoten Zugriff auf den Quorum-Datenträger haben. Um einem Cluster beitreten zu können, muss ein Knoten in der Lage sein, mit dem Knoten zu kommunizieren, der Zugriff auf den Quorum-Datenträger hat. Um sicherzustellen, dass die Clusterkonfigurationsdaten den anderen Knoten zur Verfügung stehen, wenn der Knoten, der Besitzer des Quorum-Datenträgers ist, ausfallen sollte, muss die Quorumressource auf einem physischen Speichergerät gespeichert sein, mit dem alle Knoten verbunden sind. Die ITG empfiehlt als optimale Vorgehensweise, einen einzelnen Datenträger im Speicherarray ausschließlich als Quorumressource zu verwenden.

- **IP-Ressource:** Die IP-Adresse des Clusters bzw. die IP-Adresse, die die Clients zur Kommunikation mit einem virtuellen Server verwenden. Hierbei muss es sich um eine statische IP-Adresse handeln, die sich in demselben Subnetz wie die IP-Adressen der Knoten befindet, sich jedoch von der IP-Adresse unterscheidet, die in den Knoten des Clusters konfiguriert ist. Für jeden virtuellen Server, den der Cluster bereitstellt, muss eine IP-Ressource konfiguriert sein.
- **Namenressource:** Der Netzwerkname des Clusters bzw. der Netzwerkname, den die Clients zur Kommunikation mit einem virtuellen Server verwenden. Dieser Name muss sich von dem Namen unterscheiden, der in den Knoten des Clusters konfiguriert ist. Für jeden virtuellen Server, den der Cluster zur Verfügung stellt, muss eine eindeutige Namenressource konfiguriert sein.
- **Im Cluster verfügbare Dienste:** Die Dienste, die vom Cluster für die Clients bereitgestellt werden. Hierzu gehören beispielsweise Dateifreigaben, Druckerwarteschlangen, DFS-Server, DHCP-Server und WINS-Server. Ein im Cluster verfügbarer Dienst muss zunächst als Dienst auf den einzelnen Servern vorhanden sein. Um beispielsweise einen DHCP-Cluster zu erstellen, muss der DHCP-Dienst zunächst auf jedem einzelnen Knoten installiert werden. Anschließend wird die im Cluster verfügbare DHCP-Serverressource im Cluster erstellt und der geclusterte Dienst mithilfe des Clusterverwaltungsprogramms verwaltet. Um den betreffenden Dienst oder die Anwendung zu beenden, muss die gesamte Clusterressource offline geschaltet werden.

Nicht alle Dienste oder Anwendungen werden vom Clusterdienst unterstützt. Dienste und Anwendungen, die im Cluster zur Verfügung gestellt werden können, besitzen folgende Eigenschaften:

- Die Kommunikation der Clients mit den Diensten erfolgt über IP-Adressen.
- Die Daten für einen Dienst können an den jeweils vom Clusteradministrator angegebenen Speicherort verschoben werden.
- Die Clients können verloren gegangene Verbindungen zum Server wiederherstellen.

Darüber hinaus unterstützt der Clusterdienst Ressourcen mit den Bezeichnungen "Allgemeine Anwendung" und "Allgemeiner Dienst", wenn die Anwendung bzw. der Dienst die aufgeführten drei Kriterien erfüllt.

Der Clusterdienst von Windows 2000 Advanced Server unterstützt die folgenden grundlegenden Infrastrukturdienste:

- DHCP
- Distributed Transaction Coordinator (DTC)
- Dateifreigabe
- Message Queue Service (MQS), Bestandteil von Windows 2000 Server
- NNTP (Network News Transfer Protocol)-Server
- Druckerwarteschlange
- SMTP (Simple Mail Transfer Protocol)-Server

- Zeitserver
- WINS

Andere Dienste, wie Datenbank- und Messagingdienste, werden ebenfalls unterstützt, aber die Ressourcen hierfür werden mit den Produkten SQL Server 2000- und Exchange Server 2000 bereitgestellt.

Jede Zusammenstellung von Ressourcen, die eine Failovereinheit darstellt, wird als *Ressourcengruppe* bezeichnet. Sämtliche Ressourcen in der Gruppe werden zusammen von einem Knoten auf einen anderen verschoben und auf dem neuen Knoten wieder in der richtigen Reihenfolge gestartet. Gruppen werden im Allgemeinen für die Erstellung virtueller Server verwendet. Wenn ein virtueller Server mithilfe einer Gruppe erstellt wird, enthält diese eine IP-Adresse, einen Namen, die Ressource oder Ressourcen für den Dienst oder die Anwendung, der bzw. die zur Verfügung gestellt wird, sowie mindestens eine Datenträgerressource.

Netzwerkanforderungen

Um einen Infrastrukturnetzwerkdienst im Cluster zur Verfügung zu stellen, sind mindestens drei Komponenten für das Netzwerk erforderlich:

- Eindeutige NetBIOS-Namen für den Cluster und den/die virtuellen Server.
- Sechs (oder mehr) eindeutige IP-Adressen: Zwei für die Netzwerkadapter im privaten Netzwerk, zwei für die Netzwerkadapter im öffentlichen Netzwerk, eine für den Cluster selbst und eine für jeden virtuellen Server.
- Ein Domänenkonto für den Clusterdienst (alle Knoten müssen Mitglieder derselben Domäne sein).

Installationsverfahren

Nachdem die einzelnen Knoten eingerichtet sind und das gemeinsame externe Speichermedium korrekt angeschlossen wurde, ist das Verfahren zur Clusterkonfiguration jeweils davon abhängig, ob der Cluster für netzwerk- oder serverspezifische Daten verwendet werden soll. Unabhängig von der Verwendung des Clusters enthält die Clusterkonfiguration jedoch stets die folgenden Schritte:

- Partitionieren der Clusterdatenträger entsprechend den jeweiligen Anforderungen.
- Erstellen der erforderlichen Verzeichnisstruktur.
- Installieren des Clusterdienstes auf dem ersten Knoten.
- Starten der Clusterverwaltung.
- Installieren des Clusterdienstes auf weiteren Knoten und Hinzufügen dieser Knoten zum Cluster.
- Festlegen der gewünschten Größe für die Quorumprotokolldateien des Clusters.
- Erstellen der Ressourcen "physischer Datenträger", "IP-Adresse", "Netzwerkname" und "Dateifreigabe".
- Zuweisen der Dateisystemberechtigungen.

- Starten des Dienstes (z. B. DHCP oder WINS) auf dem virtuellen Server.

Im Cluster verfügbare Infrastrukturdienste bei der ITG

Entsprechend den Angaben in diesem Dokument verfügt die ITG über eine Reihe von Windows 2000 Advanced Server-basierten Clustern, die verschiedene Dienste und Anwendungen zur Verfügung stellen. Dieser Teil des Whitepapers erläutert im Einzelnen die Hardware- und Softwarekomponenten, die von der ITG für die Bereitstellung von Infrastrukturdiensten, wie DHCP, WINS und DFS, im Cluster konfiguriert werden. Alle im Cluster verfügbaren Infrastrukturdienste, die hier erläutert werden, verwenden die im ersten Abschnitt dieses Whitepapers behandelten Komponenten gemeinsam, sofern es nicht anders erwähnt wird. Clusteranwendungen (wie SQL Server 2000 und Exchange Server 2000) werden in diesem Rahmen nicht untersucht, da die Implementierung der Clusterunterstützung in diesen Produkten jeweils ganz unterschiedlich sein kann.

Die IP-Adressen für die Clients in Redmond werden von drei DHCP-Clustern bereitgestellt. Somit sorgt die ITG für proaktive Redundanz in einer Umgebung, in der zuvor nur reaktive Wiederherstellungsverfahren zur Verfügung standen. Die andere Möglichkeit für DHCP wäre ein Entwurf mit "aufgeteiltem Bereich" gewesen, der eine wesentlich größere Komplexität und einen viel höheren Verwaltungsoverhead verursacht hätte.

Ein WINS-Cluster dient als Replikationshub für die WINS-Matrix des Unternehmens, womit sich die Anzahl der Replikationshubs für jeden Replikationspartner von zwei auf einen reduziert und die Replikationsmatrix vereinfacht wird.

Ein Dateiservercluster dient als Produktinstallationspunkt für Verschlüsselungssoftware, die nicht aus den Vereinigten Staaten exportiert werden darf. Ein DFS-Stammcluster (root cluster) dient als Einstiegspunkt für "Produkt"-Installationen auf dem Campusgelände des Unternehmens. Die Clustertechnologie stellt für diese Umgebungen Redundanz zur Verfügung, die dort vorher nicht vorhanden war.

DHCP

Unter Windows 2000 werden DHCP-Servercluster vom System unterstützt. Wenn ein Knoten, der einen virtuellen DHCP-Server bereitstellt, ausfällt, übernimmt der andere Knoten Besitz der Ressourcen, einschließlich IP-Adressen, Netzwerkname, externes Speichersystem und DHCP-Serverdienst, so dass für die Clients nur eine minimale Dienstunterbrechung spürbar wird. Für dieses Failoververfahren wird oftmals weniger als eine Minute benötigt.

Die DHCP-Implementierung der ITG umspannt mit über 150 Servern innerhalb des gesamten Corpnet den ganzen Globus. Praktisch alle IP-Adressreservierungen bei Microsoft werden mithilfe von DHCP durchgeführt. Beispielsweise wurden in der Windows NT 4.0-Umgebung von fünf DHCP-Servern ca. 80.000 Adressleases für unternehmensinterne Büros, Entwicklungsabteilungen, RAS-Clients und Server im Rechenzentrum des Unternehmens verwaltet, wie in Abbildung 5 dargestellt ist. Dies ist zwei Mal so viel wie für das gesamte übrige Microsoft-Netzwerk insgesamt. Leider war der Lastenausgleich für diese Aufgabe jedoch nicht effizient, und ein Test zeigte deutliche Leistungsdiskrepanzen zwischen den Servern. Bei Ausfall eines DHCP-Servers wären ca. 35.000 Clients nicht mehr in der Lage gewesen, Leases zu erneuern oder neue zu erhalten. Obwohl ein solcher Ausfall nicht sofort sämtliche Clients beträfe, würde er dennoch eine schwerwiegende Beeinträchtigung der Benutzer darstellen, die versuchen, Leases zu erhalten oder zu erneuern, und könnte sich auf die laufenden Geschäfte von Microsoft sehr nachteilig auswirken.

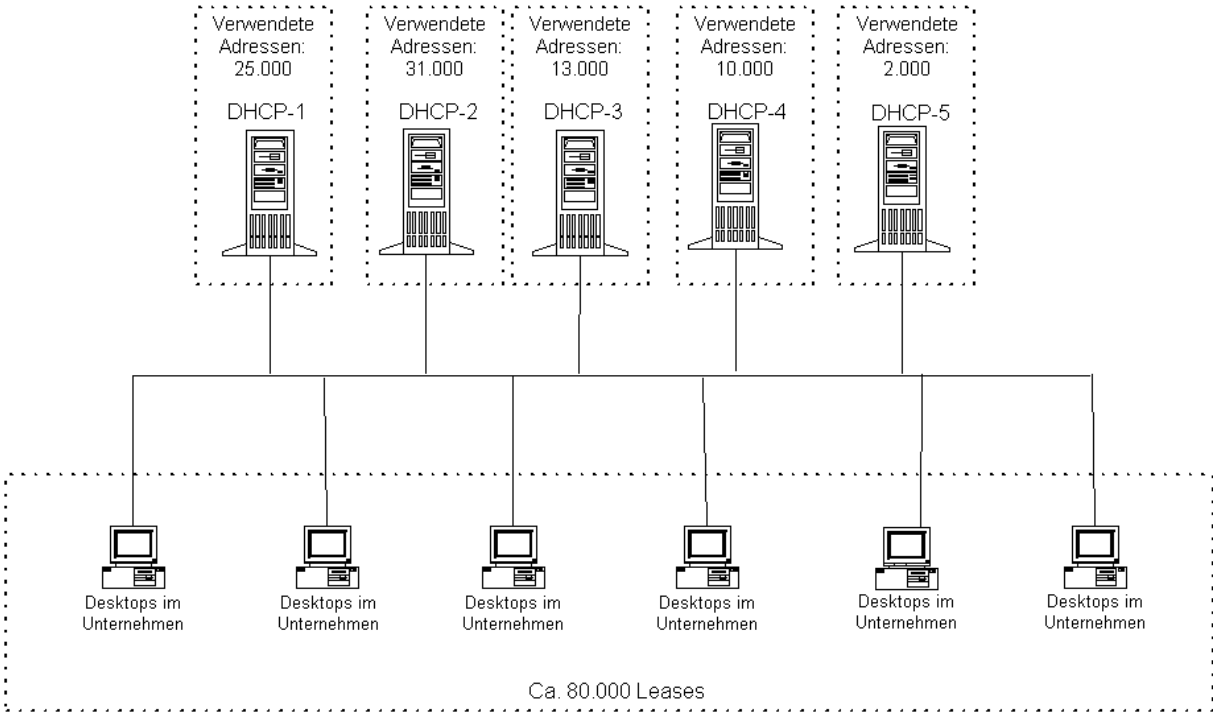

Abbildung 5: Die DHCP-Topologie vor der Clusterinstallation

Um diese Probleme zu vermeiden und eine proaktive Redundanz bereitzustellen, wurden von der ITG drei DHCP-Servercluster erstellt, an denen sechs Server und drei externe FC-Speichersysteme beteiligt sind. Die Größe der einzelnen DHCP-Cluster, die jeweils zwei Server und ein externes Speichersystem umfassen, wurde unter Berücksichtigung zukünftiger Bedürfnisse für eine gleichmäßige Verteilung der aktiven Leases auf die einzelnen Cluster ausgelegt, so dass jeder Cluster, wie in Abbildung 6 dargestellt, etwa 25.000 aktive Leases verwalten würde. Aufgrund der großen Anzahl der verwendeten Bereiche und Adressen wäre keine alternative Lösung, die die Erstellung von Bereichen nach einem Ausfall enthielte, in der Lage, die von ITG angestrebten Antwortzeiten zu erreichen.

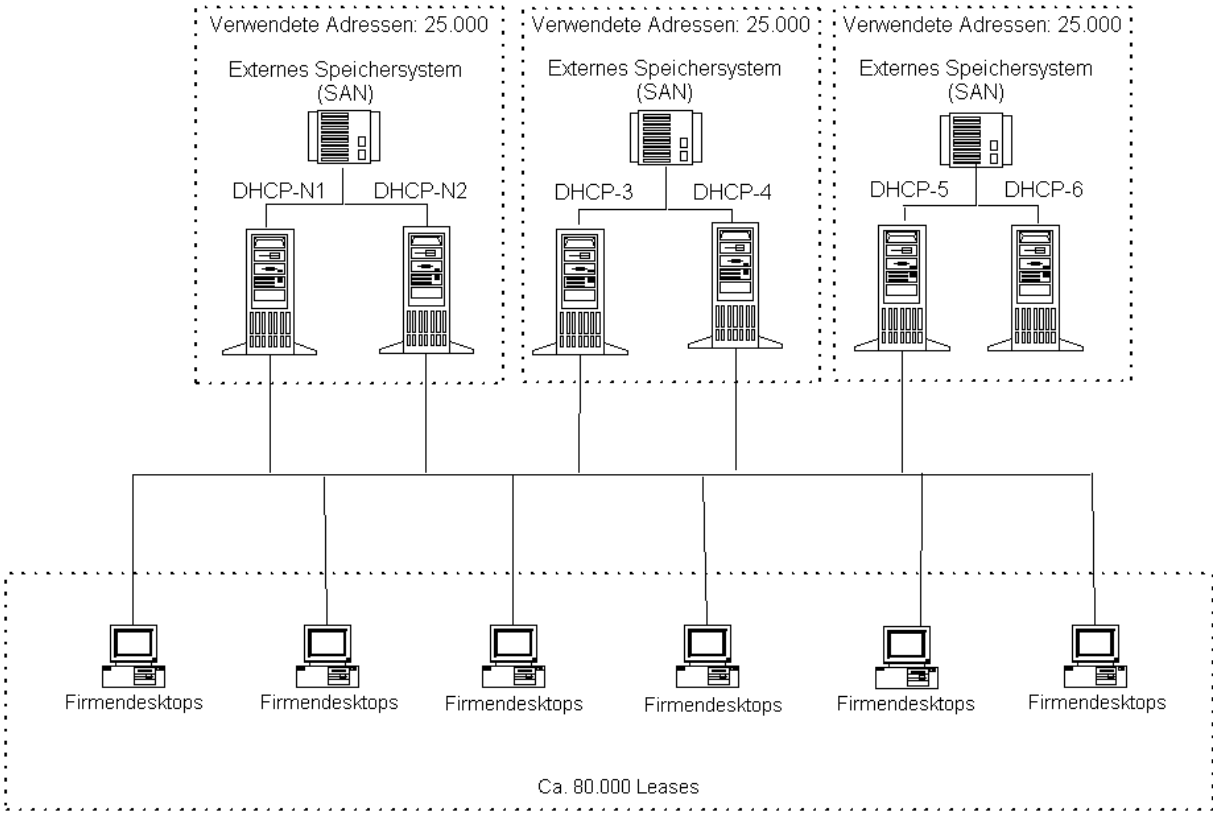

Abbildung 6: Die DHCP-Topologie nach der Clusterinstallation

Neben dem Bedarf für künftige Anforderungen wurde für die Größe der Server zusätzlich berücksichtigt, dass DHCP-Server unter Windows 2000 eine größere Anzahl an Aufgaben als unter Windows NT 4.0 ausführen müssen, wie zum Beispiel:

- DDNS-Registrierung, Aktualisierungen und Löschen von Forward- und Reverse-Lookupeinträgen.
- Zuweisen von IP-Multicastadressen über MADCAP (Multicast Address Dynamic Client Allocation Protocol).
- Clientkonfigurationen auf der Basis von Klassen-IDs, die eine bestimmte Konfiguration auf der Grundlage des Clienttyps ermöglichen. Beispielsweise können Windows 2000-DHCP-Clients so konfiguriert werden, dass sie ihre DHCP-Leases beim Herunterfahren freigeben.

Darüber hinaus unterstützt DHCP unter Windows 2000 Hersteller- und Benutzerklassen, wodurch sich der Aufwand für die Leaseverwaltung deutlich reduziert. Beispielsweise kann die Leasedauer für RRAS-Clients begrenzt werden.

Tabelle 1 zeigt die High-Level-Hardwarespezifikationen für die einzelnen Knoten der DHCP-Cluster bei der ITG.

Tabelle 1: High-Level-Spezifikationen für geclusterte DHCP-Server

Minimale CPU	Minimaler RAM	EDS/Cluster	RAID-Konfiguration
Dual P3 500 MHz	256 MB	4 x 4 GB	2 X RAID 1 4 GB

Die SAN-Datenträger der einzelnen Knoten wurden jeweils als ein RAID 1-Datenträger konfiguriert, wobei einer dieser Datenträger die DHCP-Datenbank und der andere den Quorum-Datenträger bereitstellte. Da die RAID-Konfiguration Fehlertoleranz zur Verfügung stellt, besitzt jeder Datenträger zwei Unterverzeichnisse, eines für die Sicherung und das andere für die Überwachungsprotokolle.

Im Anschluss an die Erstellung der DHCP-Cluster bei der ITG wurde die Konflikterkennung aktiviert, und dann wurden immer jeweils acht Bereiche gleichzeitig von den bestehenden DHCP-Servern auf die neuen DHCP-Server migriert. Im Einzelnen wurden hierzu folgende Schritte durchgeführt:

1. Erstellen von 8 neuen Bereichen auf einem DHCP-Cluster.
2. Aktivieren der Bereiche auf dem DHCP-Cluster.
3. Aktualisieren der UDP-Anschluss 67-Broadcast-Weiterleitung des Routers, der für dieses Subnetz zuständig ist.
4. Deaktivieren der Bereiche auf dem bestehenden DHCP-Server.
5. Warten, bis alle Clients dieser Bereiche ihre Leases auf dem "alten" DHCP-Server beendet haben.
6. Wiederholen des gesamten Verfahrens für die nächsten 8 Bereiche.
7. Deaktivieren der Konflikterkennung, nachdem die Migration aller Bereiche abgeschlossen ist.

WINS

WINS löst die Probleme, die die Auflösung von NetBIOS-Namen über IP-Broadcasts mit sich bringt, und sorgt dafür, dass sich die ITG-Administratoren nicht mehr mit der Aktualisierung statischer Zuordnungsdateien, wie z. B. LMHOST-Dateien, befassen müssen. Die Namenauflösung im Microsoft-Firmennetzwerk erfolgt standardmäßig mittels dynamischem DNS unter Windows 2000, und die Mehrzahl der verwalteten ITG-Desktops arbeitet mit Windows 2000 Professional. Dennoch werden auch noch ältere Clients (Windows 3.X, Windows 9.X, Windows NT 4.0) und von NetBIOS abhängige Anwendungen für die Entwicklung und zu Testzwecken verwendet. Daher muss die ITG die WINS-Infrastruktur so verwalten, dass sich NetBIOS-fähige Clients bei einem designierten WINS-Server registrieren können.

Die Windows NT 4.0-basierte WINS-Replikationstopologie der ITG, eine der umfangreichsten WINS-Infrastrukturen weltweit, umfasste über 40 WINS-Server, bei denen weit mehr als 800.000 Einträge registriert waren. Um die Konsistenz zu gewährleisten und für die Clients stets korrekte Informationen bereitzustellen, werden die Einträge von WINS-Clients auf alle WINS-Server repliziert.

Die WINS-Serverarchitektur verfügt über zwei Servertypen:

- **Namenserver**: Ein Server, der die Mehrzahl der Namenauflösungsabfragen von den Clients registriert und auflöst. Für jeden WINS-Client sind zwei Namenserver als *primärer* und *sekundärer* Server konfiguriert, wobei die Konfiguration entweder statisch oder über DHCP erfolgt. Der primäre Server ist der Server, der den Client registriert und "Besitzer" seiner Datensätze ist. Wenn eine Namensabfrage auf dem

primären Server fehlschlägt oder der primäre Server selbst ausfällt, wird der sekundäre Server verwendet.

- **Replikationshub/Sicherung:** Es wurden zwei Replikationshubs zur Durchführung der regionalen und globalen Replikation zwischen den Namenservern konfiguriert. Jeder WINS-Server besitzt eine Datenbank, in der für alle Clients der in der Replikationsmatrix enthaltenen Server Datensätze gespeichert sind. Nach der ersten Replikation der Datenbank werden nachfolgende Clientaktualisierungen weiter innerhalb der WINS-Infrastruktur repliziert. Die Replikationszeiten reichten von 15 Minuten zwischen Servern innerhalb desselben Subnetzes bis zu 8 Stunden bei der Replikation über das WAN.

Zur Vereinfachung der Replikationsmatrix, Bereitstellung von Redundanz und für eine effizientere Verwaltung des WINS-Datenverkehrs wurden zwei neue Server und ein SAN als Cluster installiert, um als WINS-Replikationshub zu dienen.

Abbildungen 7 und 8 zeigen die Replikationsmatrix vor und nach der Implementierung des WINS-Clusters. Beachten Sie, dass die Replikationsmatrix deutlich vereinfacht wurde, obwohl der "Nachher"-Matrix neue regionale WINS-Server hinzugefügt wurden.

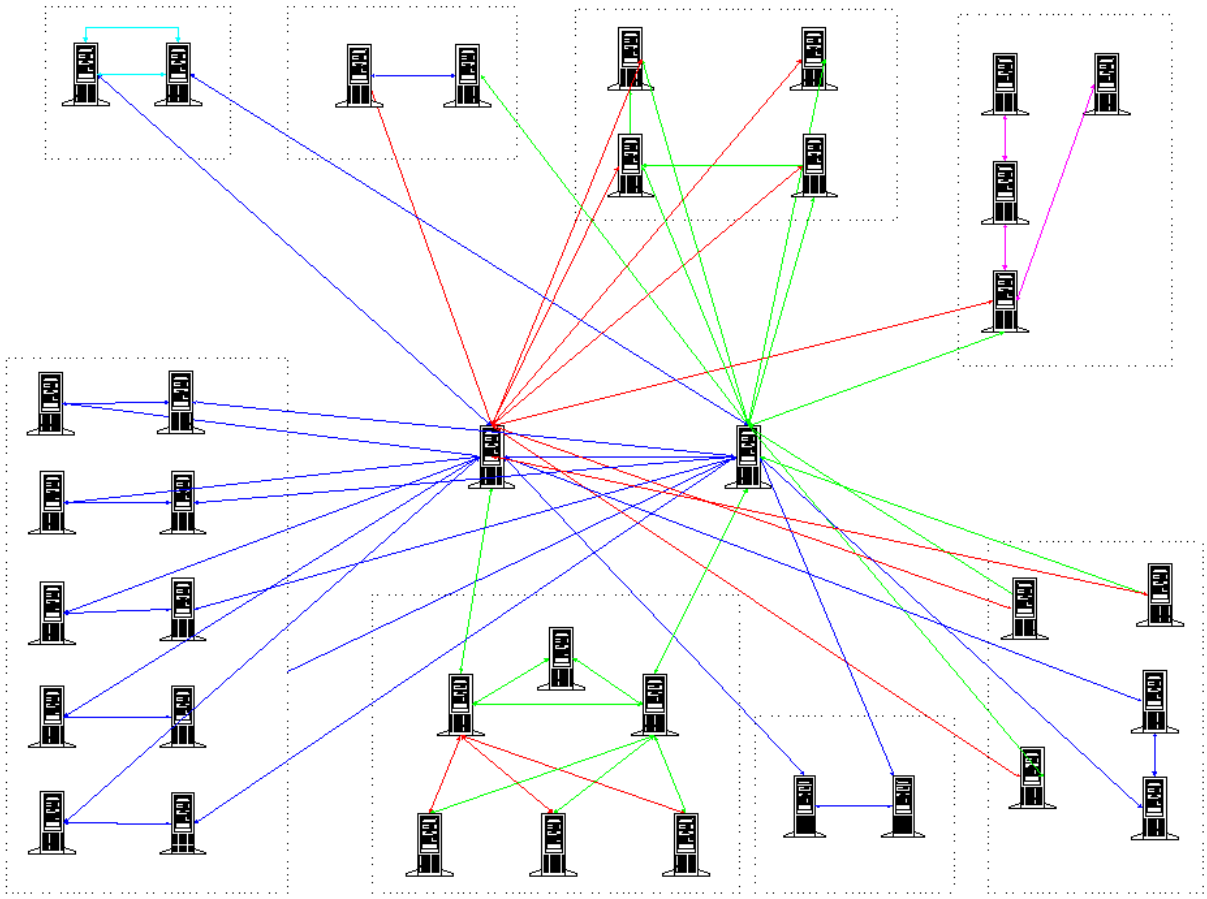

Abbildung 7: Die WINS-Topologie vor der Clusterinstallation

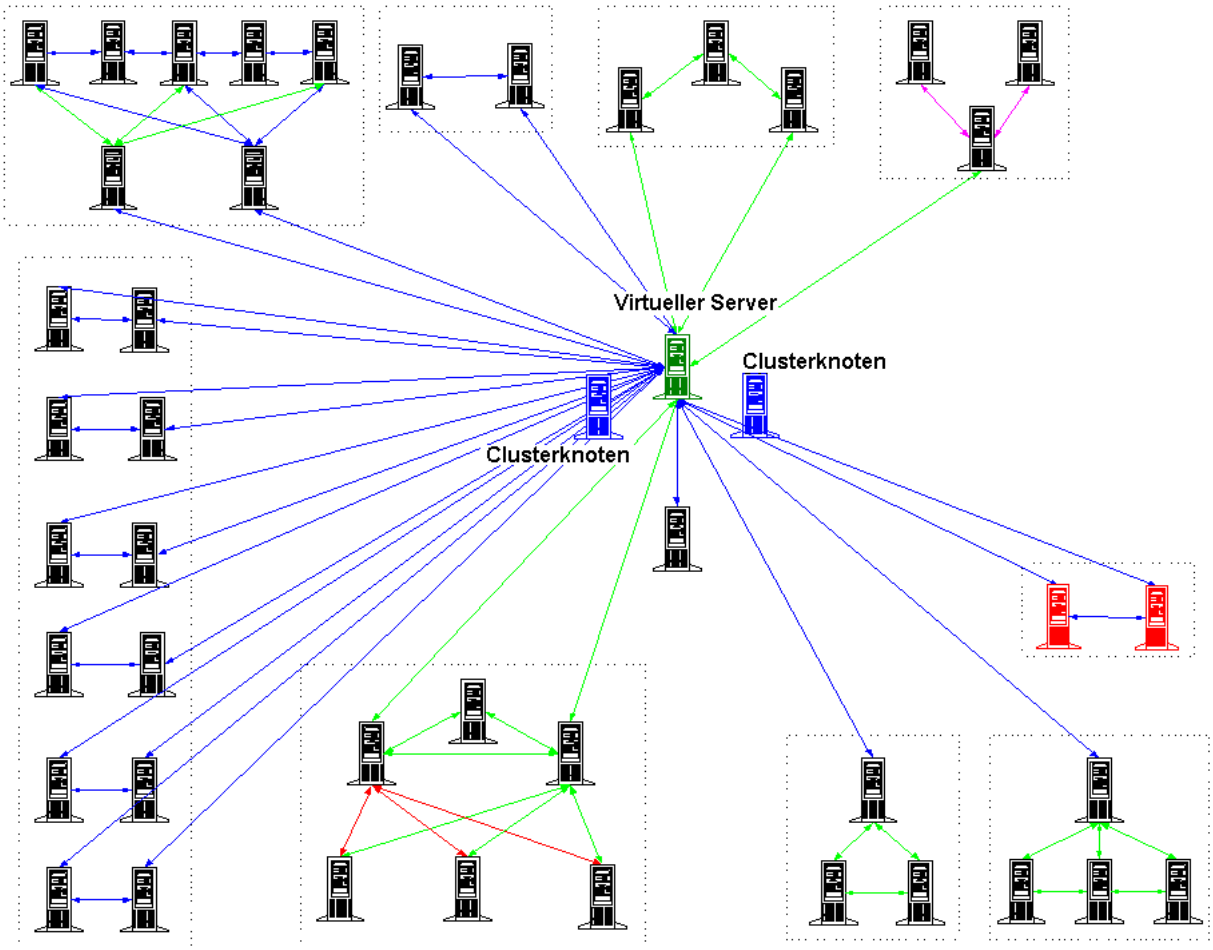

Abbildung 8: Die WINS-Topologie nach der Clusterinstallation

Tabelle 2 zeigt die High-Level-Hardwarespezifikationen für die einzelnen Knoten des WINS-Replikationshubs.

Tabelle 2: High-Level-Spezifikationen für geclusterte DHCP-Server

Minimale CPU	Minimaler RAM	EDS/Cluster	RAID-Konfiguration
Dual PIII 450 MHz	256 MB	7 X 9,1 GB 2 x 4 GB	RAID 5 (Datenbank) RAID 1 (Quorum)

Nach der Erstellung des Clusters wurden von der ITG verschiedene WINS-Parameter (siehe Tabelle 3) für die einzelnen Knoten definiert, und anschließend wurde der Replikationsdienst des WINS-Hubs auf dem Knoten gestartet.

Tabelle 3: Einstellungen der WINS-Parameter

Parameter	Einstellung
Standardpfad für die Sicherungskopie	D:\wins-db\backup
Sichern der Datenbank beim Herunterfahren des Servers	Ja
Erneuerungsintervall	4 Tage
Alterungsintervall	4 Tage
Alterungszeitüberschreitung	6 Tage
Überprüfungsintervall	24 Tage
Datenbankkonsistenz überprüfen	Nein
Änderungen in der Datenbank protokollieren	Ja
Detaillierte Ereignisse im Windows-Ereignisprotokoll eintragen	Nein
Burstverarbeitung aktivieren	Mittel
Datenbankpfad	D:\wins-db\wins.mdb
Erste Versionserkennung	0
Replikation nur mit Partnern	Ja
Migrieren	Nein
Pull-Replikation beim ersten Start auslösen	Ja
Ständige Verbindungen für Push/Pull	Aktiviert

Verteiltes Dateisystem – der DFS-Stamm "Produkte"

Das verteilte Dateisystem DFS stellt Redundanz und Lastenausgleich für Dateifreigaben bereit. Die ITG verfügte über einen sehr aktiven DFS-Stamm unter Windows NT 4.0, mit dem über 100 verschiedene Verknüpfungen auf mehrere unterschiedliche Dateiserver und Freigaben bereitgestellt wurden. Die Benutzer dieses DFS-Stammes waren Angestellte, die im Hauptsitz des Unternehmens Microsoft-Produkte von den Freigaben installierten.

Als ersten Schritt des Planes zur Erstellung einer globalen domänenbasierten DFS-Architektur bei Microsoft, wurde von der für die Produktverteilung zuständigen Gruppe eine Webseite implementiert, die als Front-End für die Installation von Produkten dienen sollte.

DFS-Stämme können sich auf einem Mitgliedsserver oder Domänencontroller befinden und sowohl als eigenständiges oder domänenbasiertes DFS implementiert werden. Leider kann der DFS-Stamm bei einem eigenständigen DFS ein Einzelpunktversagen verursachen. Ein domänenbasiertes DFS bietet für die ITG mehrere Vorteile:

- Windows 2000 sorgt dafür, dass die DFS-Topologie automatisch im Active Directory™-Dienst veröffentlicht wird, so dass es für alle Benutzer auf allen Servern in der Domäne angezeigt wird.
- Die ITG-Administratoren haben die Möglichkeit, die DFS-Stämme und gemeinsamen Ordner auf mehrere Server in der Domäne zu replizieren, so dass die Benutzer auch dann auf ihre Dateien zugreifen können, wenn einer der physischen Server, auf denen sich die Dateien befinden, nicht mehr zur Verfügung steht.

Wenn für einen Datenträger mehrere alternative Pfade vorhanden sind, stellen DFS-Clients eine bestimmte Art des Lastenausgleichs zur Verfügung, indem sie für die Liste der vom DFS-Stammserver zurückgegebenen Referenzen eine zufällige Reihenfolge verwenden.

Die Informationen über die DFS-Topologie werden auf den DFS-Servern in einer so genannten PKT-Struktur (Partition Knowledge Table) gespeichert. Die PKT-Datenstruktur setzt sich aus dem DFS-Verzeichnisnamen und der Liste der Referenzserver zusammen, mit denen sich die DFS-Clients verbinden. Wenn ein Verzeichnis im DFS-Namespace verwendet wird, wird der im lokalen Cache gespeicherte Teilbereich der PKT-Struktur von den DFS-Clients von oben nach unten "durchwandert". Wenn ein Zeitgeber für die Gültigkeitsdauer (TTL) abläuft, kehren die Clients zum DFS-Stamm oder zu den untergeordneten Replikaten zurück, der jeweilige Client wird neu gestartet, oder keiner der Server in der PKT-Struktur des Clients steht zur Verfügung.

Beachten Sie, dass zum Zeitpunkt der Erstellung dieses Dokuments vom DFS nur das Verwenden von computerbasiertem DFS durch den Clusterdienst unterstützt wird. Auf Systemen, auf denen der Clusterdienst ausgeführt wird, können Sie keine fehlertoleranten DFS-Topologien erstellen.

Tabelle 4 enthält repräsentative High-Level-Hardwarespezifikationen für diesen häufig verwendeten DFS-Cluster.

Tabelle 4: Hardwarespezifikationen für DFS-Cluster

Minimale CPU	Minimaler RAM	EDS/Cluster	RAID-Konfiguration
Dual P600 733 MHz	256 MB	4 X 9 GB 2 x 4 GB	Raid 5 (Daten) RAID 1 (Quorum)

Darüber hinaus wurde von der ITG ein vorhandener Windows NT Enterprise Edition 4.0-basierter Druckcluster aktualisiert, der für 155 Drucker auf dem Campusgelände der Unternehmenszentrale zuständig war. Dieser Cluster wurde ausgewählt, um parallele Updates von Windows NT 4.0 Enterprise Edition-Clustern auf Windows 2000 Advanced Server-Cluster zu steuern, ohne dabei stark beanspruchte Dienste, wie das Drucken, zu beeinträchtigen. Zusätzliche Redundanz wurde nicht bereitgestellt. Die Vorteile von Windows 2000, wie das Veröffentlichen der Drucker im Active Directory, konnten jedoch ohne Beeinträchtigung der Dienste verwendet werden.

Tabelle 5 enthält repräsentative High-Level-Hardwarespezifikationen für die im Cluster verfügbaren Druckserver.

Tabelle 5: Spezifikationen für geclusterte Druckserver

Minimale CPU	Minimaler RAM	EDS/Cluster	RAID-Konfiguration
Dual-P600 733 MHz	256 MB	3 x 9 GB (Spooldaten) 2 x 4 GB (Quorum)	RAID 5 (Spool) RAID 1 (Quorum)

Die ITG-Clusterverwaltung

Verwaltung der im Cluster verfügbaren Dienste

Mit wenigen Ausnahmen werden bei der ITG die Dienste, die sich auf einem Cluster befinden, mithilfe derselben Tools wie die auf einem eigenständigen Server installierten Dienste verwaltet. Die Snap-In-Tools der Microsoft Management Console (MMC) bzw. die Befehlszeilentools greifen auf den Namen oder die IP-Adresse des virtuellen Servers zu, der den betreffenden Dienst bereitstellt, anstatt eine Verbindung mit einem bestimmten Knoten im Cluster herzustellen. Beispielsweise werden bei der Konfiguration der WINS-Replikation die Partner so konfiguriert, dass die Replikation mit der IP-Adresse des virtuellen Servers und nicht mit den einzelnen IPs der Knoten durchgeführt wird, und die Verwaltung eines im Cluster verfügbaren DFS-Stammes erfolgt über die Verbindung mit dem Namen des virtuellen Servers.

Überwachung

Die ITG verwaltet die im Cluster verfügbaren Infrastrukturdienste größtenteils genauso wie reguläre Server und verwendet dazu meistens dieselben Tools. Eine Ausnahme sind beispielsweise Dateifreigabeberechtigungen (keine Verzeichnisberechtigungen), für deren Änderung das Clusterverwaltungsprogramm benötigt wird.

Für die Überwachung des Clusterstatus ist die Überwachung des Clusterdienstes auf den einzelnen Knoten, die Überwachung der Clusterressourcen selbst und (bei Bedarf) die Überwachung des Dienstes erforderlich, der vom Cluster bereitgestellt wird. Die ITG verwendet verschiedene Skripttools von Drittanbietern, um folgende Aufgaben durchzuführen:

- Überwachung einzelner Knoten, um sicherzustellen, dass die Knoten zur Verfügung stehen, dass sie Bestandteil des Clusters sind, und dass der Clusterdienst auf jedem Knoten ausgeführt wird.
- Überwachung der Clusterressourcen für den Fall, dass eine Clusterressource offline geschaltet wird oder ausfällt.
- Überwachung der zur Verfügung gestellten Dienste. Es werden entsprechend dem jeweiligen Dienst unterschiedliche Skripts verwendet.

Tools für die Problembehandlung

Die Ereignisanzeige

Eines der effektivsten Tools für die Behandlung Windows 2000-basierter Probleme ist die Ereignisanzeige. Da die Ereignisreplikation in einem Cluster standardmäßig aktiviert ist, gibt das Ereignisprotokoll auf jedem Cluster Auskunft über die Ereignisse sämtlicher im Cluster enthaltenen Knoten. Darüber hinaus werden die Ereignisse sämtlicher Knoten in den Ereignisprotokollen jedes Knotens aufgezeichnet, so dass die Administratoren alle Knotenereignisse in chronologischer Reihenfolge an einer zentralen Stelle einsehen können. Diese Funktion kann bei Bedarf deaktiviert werden.

Tabelle 6 enthält eine Aufstellung der wichtigsten Ereignisse, die von der ITG routinemäßig auf den Clustern überwacht werden.

Tabelle 6: Wichtige EventIDs im Ereignisprotokoll

Ereignisquelle	Ereignis-ID - Schweregrad	Ereignis	Bedeutung und Maßnahmen
Datenträger	51, Warnung	Bei einem Auslagerungsvorgang wurde ein Fehler festgestellt. Betroffen ist Gerät <Gerätename>.	Eine häufige Warnung auf einem Servercluster, die normalerweise ausgegeben wird, wenn der Besitz eines Datenträgers von einem Knoten auf einen anderen übertragen wird. Sofern keine anderen Ereignisse eintreten, die zu Problemen führen können, kann diese Warnung ignoriert werden.
ClusSvc	1009, Fehler	Der Clusterdienst konnte keinem vorhandenen Cluster beitreten und keinen neuen Cluster erstellen. Der Clusterdienst wurde beendet.	Dieser Fehler enthält ein Datenwort, das zur Problembehandlung verwendet werden kann. Konvertieren Sie den Hexadezimalwert des Datenworts in einen Dezimalwert, und geben Sie dann an der Eingabeaufforderung den Befehl "net helpmsg <Dezimalwert des Datenworts>" ein, um weitere Informationen über den Fehler anzeigen zu lassen. Beispielsweise ergibt der Datenwort-Wert 000013de den Dezimalwert 5086, und "net helpmsg 5086" gibt die Meldung aus: "Der Quorum-Datenträger wurde vom Clusterdienst nicht gefunden."

ClusSvc	1062, Information	Der Microsoft Clusterdienst konnte dem Cluster beitreten.	Der Knoten, von dem diese Meldung ausgegeben wurde, ist einem bestehenden Cluster beigetreten. Diese Meldung wird nicht von dem Knoten protokolliert, der im Cluster zuerst gestartet wird.
ClusSvc	1122, Information	Der Knoten hat die Kommunikation mit dem Clusterknoten '<Knotenname>' im Netzwerk '<Schnittstellenname>' (wieder)hergestellt.	Der Knoten, von dem diese Meldung ausgegeben wurde, hat die Netzwerkverbindung zu dem angegebenen Knoten über die angegebene Schnittstelle wiederhergestellt. Wie bei der ClusSvc-Warnung 1123 gibt dieses Ereignis keinen Aufschluss darüber, welcher der Knoten von dem Problem betroffen war. Es empfiehlt sich unter Umständen, die Ursache des Fehlers zu ermitteln.
ClusSvc	1123, Warnung	Die Kommunikation zwischen dem Knoten und dem Clusterknoten '<Knotenname>' im Netzwerk '<Schnittstellenname>' ist abgebrochen.	Der Knoten, von dem diese Meldung ausgegeben wurde, hat die Netzwerkverbindung zu dem angegebenen Knoten über die angegebene Schnittstelle abgebrochen. Diese Fehlermeldung gibt nicht darüber Aufschluss, bei welchem der Knoten das Netzwerkproblem aufgetreten ist. Überprüfen Sie die Clusterknoten, um die Ursache zu ermitteln und das Problem zu beheben.
ClusSvc	1135, Warnung	Der Clusterknoten <Knotenname> wurde aus der aktiven Clusterzugehörigkeit entfernt. Der Clusterdienst könnte auf dem Knoten angehalten worden sein, es könnte ein Knotenfehler vorliegen, oder die Kommunikation zwischen dem Knoten und den anderen aktiven Clusterknoten ist abgebrochen.	Ein unbekannter Fehler des Knotens hat dafür gesorgt, dass dieser aus dem Cluster entfernt werden musste. Überprüfen Sie den Knoten, um die Ursache des Problems zu ermitteln.

Die Clusterprotokolldatei

Der Clusterdienst gestattet es, dass auf jedem Knoten detaillierte Informationen über die Clusteraktivität protokolliert werden. Im Gegensatz zu den Ereignisprotokollen werden diese Protokolle nicht von allen Knoten synchronisiert. Jedes Knotenprotokoll gibt die Perspektive des jeweiligen Knotens innerhalb des Clusters wieder. Standardmäßig ist das Clusterprotokoll auf den Knoten aktiviert, und es wird jeweils ein Protokoll (mit dem Namen **Cluster.log**) im Verzeichnis **%SystemRoot%\Cluster** der einzelnen Knoten des Clusters erstellt. Nach seiner Aktivierung erreicht das Clusterprotokoll eine statische Größe von 8 MB (konfigurierbar in 1-MB-Schritten), wobei die Ereignisse nach der FIFO-Methode (First In First Out) gelöscht werden. Die Problemdiagnose mithilfe der Clusterprotokolldateien ist sehr komplex und würde im Rahmen dieses Whitepapers zu weit gehen. Weiterführende Informationen zur Clusterdiagnose finden Sie am Ende dieses Dokuments im Abschnitt "Weitere Informationen".

Windows 2000 DHCP-Leistungsindikatoren

Das Betriebssystem Windows 2000 enthält neue Leistungsindikatoren für die Überwachung der aktuellen DHCP-Serverleistung und die Kapazitätsplanung. Bei der ITG werden standardmäßig folgende Indikatoren überwacht:

- **Nacks/Sek.**: Die Rate der vom DHCP-Server gesendeten DHCP-Nacks.
- **Angebote/Sek.**: Die Rate der vom DHCP-Server gesendeten DHCP-Angebote.
- **Acks/Sek.**: Die Rate der vom DHCP-Server gesendeten DHCP-Acks.
- **Länge der aktiven Warteschlange**: Die Anzahl der Pakete in der Verarbeitungswarteschlange des DHCP-Servers.
- **Länge der Warteschlangen-Konflikterkennung**: Die Anzahl der Pakete in der DHCP-Serverwarteschlange, für die Konflikterkennung (ping) durchgeführt werden muss.
- **Abweisungen/Sek.**: Die Rate der vom DHCP-Server empfangenen DHCP-Abweisungen.
- **Entdeckungen/Sek.**: Die Rate der vom DHCP-Server empfangenen DHCP-Entdeckungen.
- **Duplikate verworfen/Sek.**: Die Rate der vom DHCP-Server empfangenen doppelten Pakete.
- **Benachrichtigungen/Sek.**: Die Rate der vom DHCP-Server empfangenen DHCP-Benachrichtigungen.
- **Millisekunden/Paket (Durchschnitt)**: Durchschnittliche Zeit pro Paket, die der DHCP-Server benötigt, um eine Antwort zu senden.
- **Pakete abgelaufen/Sek.**: Die Rate der abgelaufenen Pakete in der DHCP-Servernachrichtenwarteschlange.
- **Pakete empfangen/Sek.**: Die Rate der vom DHCP-Server empfangenen Pakete.
- **Freigaben/Sek.**: Rate der vom DHCP-Server empfangenen DHCP-Freigaben.
- **Anforderungen/Sek.**: Die Rate der vom DHCP-Server empfangenen DHCP-Anforderungen.

Ereignisse des DHCP-Systemprotokolls

Zu den wichtigsten DHCP-Systemereignissen, die bei der ITG überwacht werden, zählen Folgende:

- **Ereignis-ID 1011:** Der DHCP-Server hat an den Client (MAC-Adresse) für die Adressanforderung (IP-Adresse) ein NACK-Signal (Negative Acknowledgement Message) ausgegeben. Dies weist darauf hin, dass der DHCP-Server die Ausgabe der angegebenen IP-Adresse an den Client mit der betreffenden MAC-Adresse abgelehnt hat. Die häufigste Ursache hierfür ist, dass der DHCP-Server nicht über ein Lease für den Client verfügt, was normalerweise darauf zurückzuführen ist, dass ein Router für die Weiterleitung von DHCP-Entdeckungen an einen DHCP-Server konfiguriert wurde, der kein Lease für dieses Subnetz besitzt.
- **Ereignis-ID 1014:** Die Jet-Datenbank hat folgenden Fehler zurückgegeben: [Nummer]. DHCP verwendet das Jet-Datenbankmodul zum Speichern der Leaseinformationen. Die Nummer, auf die in dieser Fehlermeldung verwiesen wird, ist in einer Liste der Jet-Datenbankfehler aufgeführt.
- **Ereignis-ID 20057: Der DHCP/BINL-Server hat festgestellt, dass er nicht autorisiert ist, den Dienst für Clients in diesem Netzwerk für die Windows-Domäne [Domänenname] auszuführen.** Der DHCP-Server ist für diese Domäne nicht autorisiert. Verwenden Sie das DHCP-Snap-In, um den Server zu autorisieren.

WINS-Leistungsindikatoren

In Tabelle 7 sind die WINS-spezifischen Objekte und Leistungsindikatoren aufgeführt, die bei der ITG zur Beurteilung der Clientaktivität verwendet werden.

Tabelle 7: WINS-Leistungsindikatoren

Objekte und Leistungsindikatoren	Beschreibung
Gruppenkonflikte/s	Die Rate, mit der vom WINS-Server empfangene Gruppenregistrierungen zu Konflikten mit Datenbankeinträgen geführt haben.
Einzelkonflikte/s	Die Rate, mit der vom WINS-Server empfangene Einzelregistrierungen und -erneuerungen zu Konflikten mit Datenbankeinträgen geführt haben.
Konflikte insgesamt/s	Die Summe der Einzel- und Gruppenkonflikte pro Sekunde. Die Gesamtrate, mit der Konflikte am WINS-Server auftreten.
Gruppenregistrierungen/s	Die Rate, mit der Gruppenregistrierungen vom WINS-Server empfangen werden.
Registrierungen insgesamt/s	Die Summe der Einzel- und Gruppenregistrierungen pro Sekunde. Dies ist die Gesamtrate, mit der Registrierungen vom WINS-Server empfangen werden.
Einzelregistrierungen/s	Die Rate, mit der Einzelregistrierungen vom WINS-Server empfangen werden.
Gruppenerneuerungen/s	Die Rate, mit der Gruppenerneuerungen vom WINS-Server empfangen werden.
Einzelerneuerungen/s	Die Rate, mit der Einzelerneuerungen vom WINS-Server

	empfangen werden.
Erneuerungen insgesamt/s	Die Summe der Einzel- und Gruppenerneuerungen pro Sekunde.
Abfragen/s	Die Rate, mit der Abfragen vom WINS-Server empfangen werden.
Erfolgreiche Abfragen/s	Gesamtzahl der erfolgreichen Abfragen/s.
Fehlgeschlagene Abfragen/s	Gesamtzahl der fehlgeschlagenen Abfragen/s.
Freigaben/s	Die Rate, mit der Freigaben vom WINS-Server empfangen werden.
Erfolgreiche Freigaben/s	Gesamtzahl der erfolgreichen Freigaben/s.
Fehlgeschlagene Freigaben/s	Gesamtzahl der fehlgeschlagenen Freigaben/s.

Datensicherung

Nur der Knoten, der Besitzer des Datenträgers ist, kann zur Durchführung von Datensicherungen auf diesen Datenträger zugreifen. Die ITG sichert regelmäßig die C$-Datenträger der einzelnen Knoten, die jeweils die Systempartition und die Dateien des Betriebssystems enthalten. Bei der Sicherung bestimmter Datenträger auf dem SAN wird entweder der Name des virtuellen Servers oder des Clusters angegeben, je nachdem, welcher Datenträger gesichert werden soll.

Ändern des Kennworts für den Clusterdienst

Der Clusterdienst benötigt ein Benutzerkonto, unter dem der Dienst gestartet werden kann. Auf allen Knoten muss dasselbe Konto verwendet werden, bei dem es sich um ein Administratorkonto handeln muss. Das Sicherheitsmodell der ITG gestattet nicht die Verwendung von Konten, bei denen das Kennwort nie abläuft. Daher werden für die routinemäßige Änderung des Kennworts für dieses Konto kurze Ausfallzeiten geplant. Das Kennwort wird nur beim Starten des Clusterdienstes überprüft. Es muss jedoch nicht nur mit dem aktuellen Kennwort der Domäne übereinstimmen, sondern auch mit dem Kennwort, das von den anderen Knoten verwendet wird. Die ITG wendet das folgende Verfahren an, um dafür zu sorgen, dass die Beeinträchtigungen durch die erforderlichen Kennwortänderungen für einen aus zwei Knoten bestehenden Cluster mit einer Ressourcengruppe möglichst gering sind:

- Bestimmen, auf welchem Knoten die Gruppe zum aktuellen Zeitpunkt ausgeführt wird.
- Ändern des Kennworts für die Domäne.
- Beenden des Clusterdienstes auf dem Knoten, der nicht Besitzer der Gruppe ist.
- Ändern des Kennworts für den Clusterdienst auf diesem Knoten.
- Ändern des Kennworts für den Clusterdienst auf dem Knoten, der Besitzer der Gruppe ist.
- Aktivieren des Clusterdienstes auf diesem Knoten.
- Starten des Clusterdienstes auf dem Knoten, der nicht Besitzer der Gruppe ist.

Für Cluster mit zwei Knoten und zwei oder mehr Gruppen wendet die ITG das folgende Verfahren an:

- Verschieben sämtlicher Gruppen auf einen Knoten.
- Ändern des Kennworts für die Domäne.
- Beenden des Clusterdienstes auf dem Knoten, der nicht Besitzer der Gruppen ist.
- Ändern des Kennworts für den Clusterdienst auf diesem Knoten.
- Ändern des Kennworts für den Clusterdienst auf dem Knoten, der Besitzer der Gruppen ist.
- Aktivieren des Clusterdienstes auf diesem Knoten.
- Starten des Clusterdienstes auf dem Knoten, der nicht Besitzer der Gruppen ist.
- Zurückverschieben der Gruppen an ihren jeweiligen ursprünglichen Speicherort.

Erkenntnisse

Der Clusterdienst hat sich für die ITG für verschiedene Aufgaben, unter anderem die Zusammenführung von Servern und Bereitstellung einer hohen Verfügbarkeit, als nützlich erwiesen. Wie in jeder Umgebung mit hoher Verfügbarkeit stellen die korrekte Hardwarekonfiguration sowie die Überwachung und Verwaltung des Systems jedoch nur

einige der erforderlichen Aufgaben dar. Eine entsprechende Schulung sowie die korrekte Anwendung der Verfahren zur Systemkontrolle, wie die Überwachung der Ereignisprotokolle, sind ebenfalls wichtig. Die Systemüberwachung spielte eine äußerst wichtige Rolle, was bei jeder Implementierung weiterer SAN-Hardware deutlich wurde.

Bei der Implementierung der Infrastrukturdienste im Cluster konnte die ITG folgende Erkenntnisse sammeln:

- Die Unterstützung paralleler Updates ist für die Verwaltung der Dienste bei häufigen Software- und Hardwareaktualisierungen äußerst wichtig. Beispielsweise wurden die Betriebssysteme Windows 2000-basierter Server bei der ITG während der Entwicklung und der Abschlusstests häufig aktualisiert. Bei mindestens 30 Minuten pro Aktualisierung bedeutete dies ein hohes Maß an Ausfallzeiten, da eine große Anzahl Server vorhanden war. Durch das Zusammenfassen dieser Server in Clustern reduzierte sich die Ausfallzeit auf weniger als eine Minute pro Aktualisierung. Da sowohl für die Hardware als auch die Software eine andere Verwaltung erforderlich ist, rechnet die ITG damit, dass dies weiterhin der wesentliche Vorteil sein wird, den der Clusterdienst bietet.

- Um die hohe Verfügbarkeit standardmäßig zu gewährleisten, stellt die ITG sicher, dass ein ausreichender Vorrat an Ersatzteilen zur Verfügung steht, einschließlich der für die Storage Area Networks (SANs) erforderlichen Ersatzteile.

- Der Quorum-Datenträger im SAN ist die Komponente, der die größte Bedeutung zukommt. Der Datenträger, der als Quorum-Datenträger verwendet wird, sollte nicht ebenfalls zum Speichern der Daten für einen virtuellen Server verwendet werden.

- Die korrekte Netzwerkkonfiguration sowohl der privaten als auch der öffentlichen Netzwerkverbindungen ist von entscheidender Bedeutung. Bei Clusternetzwerknamen kann es ebenso wie bei anderen NetBIOS-Namen Probleme mit doppelt vorhandenen Netzwerknamen geben. Das Ändern der Einstellungen für IP-Adresse, Subnetz oder Netzwerkadapter auf einem Knoten kann die Offlineschaltung eines Clusters wegen eines Namenfehlers verursachen.

- Die Funktionen der Energieverwaltung sollten auf Clusterservern deaktiviert werden. Ein Clusterknoten, der Festplatten abschaltet oder in den Standbymodus wechselt, kann einen Clusterausfall verursachen, da der betreffende Knoten für die anderen Mitglieder des Clusters als offline angezeigt wird.

- Die Schulung des Supportpersonals ist von entscheidender Bedeutung. Die Konfiguration von Diensten auf eigenständigen Servern ist bei der ITG wesentlich häufiger zu finden als die Konfiguration im Cluster. Viele ITG-Supportmitarbeiter, die sich mit Windows NT 4.0 und den von diesem Betriebssystem unterstützten Diensten gut auskennen, waren mit der Unterstützung von Diensten in einer Clusterumgebung weniger vertraut.

- Wie bei zahlreichen ITG-Implementierungen gehörten diese Cluster zu den ersten auf Windows 2000 Advanced Server basierenden Clustern überhaupt, die in einer Produktionsumgebung implementiert werden sollten. Es gab keine Erfahrungswerte, anhand derer vorausgesagt werden konnte, wie die Hardwareplattformen und SANs unter Produktionsbedingungen arbeiten würden. Die Evaluierung der Umgebung vermittelte wesentliche Erkenntnisse darüber, wie zukünftige Umgebungen skaliert werden sollten und welche Verbesserungen noch vor der Produktfreigabe in Windows 2000 integriert werden könnten.

- Die Überwachung der Verfügbarkeit erfolgt normalerweise durch die Beobachtung der Verfügbarkeit der einzelnen Server. Die Verfügbarkeit eines einzelnen Servers in einem Cluster ist jedoch nicht unbedingt für die Verfügbarkeit des virtuellen Servers ausschlaggebend, der vom Cluster zu Verfügung gestellt wird. Auch die standardmäßige Überwachung der Verfügbarkeit stellt eine besondere Herausforderung dar. Es genügt nicht, wenn sichergestellt wird, dass der virtuelle Server vorhanden ist. Wenn es Probleme mit einem Knoten gibt, kann der virtuelle Server unter Umständen noch Dienste bereitstellen, die Redundanz ist jedoch eventuell nicht mehr vorhanden. Die ITG entwickelt zurzeit neue Methoden zur Bestimmung der Betriebszeit.

Künftige Weiterentwicklungen

Die künftige Entwicklung des Clusterdienstes wird sich auf mehrere Bereiche konzentrieren, die für die ITG von Bedeutung sind:

- Zertifizierung und Unterstützung noch größerer Clusterkonfigurationen mit noch mehr Knoten.

- Einfachere Installation und Überprüfung von Clusterkonfigurationen, einschließlich der Unterstützung neuer Hardwaretypen.

- Einfachere und leistungsfähigere Verwaltung clusterbasierter Anwendungen und Dienste, wobei der Schwerpunkt weiterhin auf einer skriptbasierten, entfernten und unbeaufsichtigten Verwaltung liegt.

- Ausdehnung der auf Clustern basierenden Verfügbarkeits- und Skalierbarkeitsvorteile auf eine noch größere Anzahl von Systemdiensten.

- Verstärkte Integration der Infrastruktur und Schnittstellen aller Windows-basierten Clustertechnologien zur Verbesserung der Leistung, Flexibilität und Verwaltbarkeit.

- Fortgesetzte Unterstützung unabhängiger Softwareanbieter (Independent Software Vendors, ISVs) und Entwickler zur Vereinfachung der Entwicklung, Installation und Unterstützung clusterfähiger Anwendungen, um die Verfügbarkeit und Skalierbarkeit zu verbessern.

Schlussfolgerung

Bei den ITG-Projekten zur Bereitstellung der Infrastrukturdienste im Cluster haben sich mehrere Vorteile des Clusterdienstes herausgestellt, unter anderem:

- Reduzierte Anschaffungs- und Folgekosten aufgrund der Zusammenführung von Servern.
- Höhere Verfügbarkeit der Anwendungen und Dienste. Die Clusterdienste sorgen aufgrund der Unterstützung paralleler Updates und der Fähigkeit, während geplanter und ungeplanter Ausfallzeiten ein Failover der Ressourcen zu ermöglichen, für minimale Ausfallzeiten.
- Verbesserte Leistung und Verfügbarkeit der stark beanspruchten High-End-Datei- und Infrastrukturserver.

Die Erfahrungen der ITG haben dabei geholfen, Standards für Clustertopologien zu entwickeln, die bei zukünftigen Clusterimplementierungen berücksichtigt werden sollen. Die ITG ist bereits dabei, für eine weiterführende Standardisierung der Clusterhardware und Clustertopologien zu sorgen.

Die ITG gibt ihre hier beschriebenen "Erkenntnisse" gerne weiter, in der Hoffnung, dass die Kunden bei Bedarf von diesen Erfahrungen profitieren können. Mit der weiteren Bereitstellung von Windows 2000 Advanced Server und Windows 2000 Data Center Server durch Microsoft wird die ITG ihre Erfahrungen auch weiterhin an die Kunden weitergeben.

Weitere Informationen

Weitere IT Showcase-Informationen finden Sie unter
http://www.microsoft.com/germany/technet/forum/showcase_archiv.htm bzw.
http://www.microsoft.com/technet/showcase (englischsprachig).

Oder unter:

"How Microsoft Works" unter
http://www.microsoft.com/solutions/HowMicrosoftWorks/default.htm (englischsprachig)

"Windows 2000 Clustering Technologies: Cluster Service Architecture" unter
http://www.microsoft.com/TechNet/win2000/win2ksrv/technote/clustsrv.asp
(englischsprachig)

Microsoft Windows Hardewarekompatibilitätsliste (Microsoft Windows Hardware Compatibility List, HCL) unter http://www.microsoft.com/hcl/default.asp (englischsprachig)

Exploring Windows Clustering Technologies unter
http://www.microsoft.com/ntserver/ntserverenterprise/exec/overview/clustering/default.asp
(englischsprachig)

"Step-by-Step Guide to Installing Cluster Service" unter
http://www.microsoft.com/windows2000/library/planning/server/clustersteps.asp
(englischsprachig)

Microsoft Windows 2000 Server Resource Kit - Distributed Systems Guide: "Interpreting the Cluster Log." (englischsprachig)

Windows 2000 Deployment Guide – Chapter 18 - Ensuring the Availability of Applications and Services unter http://www.microsoft.com/TechNet/win2000/dguide/chapt-18.asp#b (englischsprachig)

Cluster-Aware Software Products List unter http://www.microsoft.com/ntserver/ntserverenterprise/exec/overview/Clustering/partnerlist.asp (englischsprachig)

Wenn Sie Fragen, Kommentare oder Vorschläge zu diesem Dokument haben oder weitere Informationen über Microsoft IT Showcase anfordern möchten, senden Sie bitte eine englischsprachige E-Mail an showcase@microsoft.com.