Technische Universität München

Institut für Informatik

DCE-gerechte Strukturierung eines großen Workstationverbundes bei der BMW AG

Diplomarbeit

Sven Achter

Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Thomas Paintmayer
	Dr. Arno Kinigadner, BMW AG
Abgabetermin:	15. Mai 1995

Ich versichere, daß ich diese Diplomarbeit selbständig verfaßt und nur die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 13. Mai 1995

Kurzfassung

Die vorliegende Arbeit basiert auf einer konkreten Problemstellung bei der BMW AG. Dort wird zur Zeit damit begonnen, eine zentrale CAD-Installation durch einen weltweit verteilten Workstationverbund abzulösen.
Im Gegensatz zu einem Großrechner mit einer immanent zentralen Sicht auf das gesamte System ist es bei verteilten Verbunden unerläßlich, eine Strukturierung der Umgebung vorzunehmen. Den dabei existierenden Freiheitsgraden steht jedoch keine Methodik gegenüber, die den Strukturierungsprozeß in geeigneter Weise unterstützt.
Die Frage, wie ein solcher verteilter Verbund in möglichst sinnvoller Weise gegliedert werden kann, stellt den Ausgangspunkt dieser Arbeit dar.

Ein wesentliches Ziel dieser Arbeit ist, durch die Bestimmung und Beschreibung von Einflußgrößen die Grundlage für eine zielgerichtete Strukturierung verteilter Verbunde schaffen. In diesem Zusammenhang ist es erforderlich, sowohl Rahmen für die Beschreibung einer verteilten Umgebung unter verschiedenen Sichtweisen zu definieren, als auch geeignete Parameter für die Bewertung der unterschiedlichen Lösungen zu bestimmen.

Um diese Ansätze in einem realen Umfeld überprüfen zu können, muß eine Technologie eingesetzt werden, die aufgrund ihrer Architektur eine möglichst große Flexibilität bei der Strukturierung verteilter Umgebungen zuläßt.
Für diese Arbeit wurde deshalb das *Distributed Computing Environment (DCE)* ausgewählt.

Der entwickelte Beschreibungs- und Bewertungsrahmen wird im Zentrum der Arbeit am Beispiel von DCE auf die konkrete Situation bei der BMW AG angewendet und aus den gewonnenen Ergebnissen wird abschließend die am besten angepaßte Strukturierung abgeleitet.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

1.1 Paradigmenwechsel bei IV-Versorgungsstrukturen

Aufgrund veränderter technologischer und ökonomischer Rahmenbedingungen hat sich in den letzten Jahren ein einschneidender Wandel in den IV-Versorgungsstrukturen vieler Unternehmen zu vollziehen begonnen.

Im Rahmen dieser Entwicklung wird immer mehr Funktionalität, die früher lediglich zentral auf Großrechnern (*Mainframes*) angeboten wurde, in dezentralen Client/Server-Verbunden zur Verfügung gestellt.

Aus technologischer Sicht beeinflussen vor allem folgende Faktoren diese Entwicklung:

- die immer stärkere Verbreitung moderner Netztechnik
  Dies umfaßt vor allem die gewachsene Bandbreite und Zuverlässigkeit. Zudem können mit Hilfe unternehmensweiter, oder gar weltweiter Kommunikationsnetze Daten global verfügbar gemacht werden.
- die stark ansteigende Leistungsfähigkeit von Desktop- und Serverrechnern bei sinkenden Anschaffungskosten.
- Fortschritte in der Software-Entwicklung. Hierbei sind vor allem die Verwendung standardisierter Schnittstellen zu nennen. Dadurch wird auch der Austausch von Informationen zwischen unterschiedlichen Applikationen möglich.

Demgegenüber stehen eine Reihe von ökonomischen Aspekten, von denen die Entwicklung zu dezentralen IV-Infrastrukturen ebenfalls mitgetragen wird:

- der Trend zu flacheren, dezentralisierten Organisationsstrukturen und der damit anwachsende Informationsaustausch und Koordinationsbedarf.
- die Überarbeitung von Geschäftsprozessen zur Anpassung an eine veränderte Wettbewerbssituation.
- die verstärkte Kooperation mit externen Partnern.

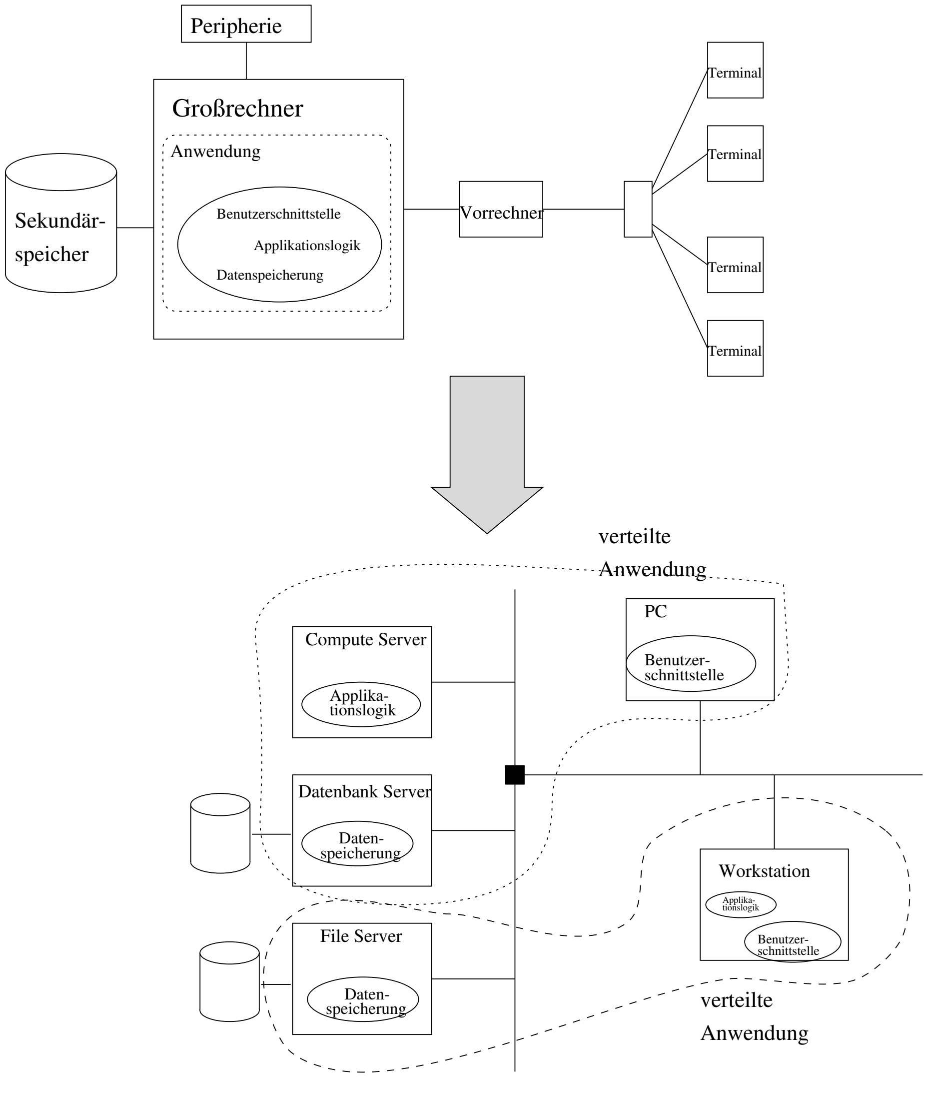


Abbildung 1.1: Paradigmenwechsel bei den IV-Versorgungsstrukturen

1.2 Probleme durch dezentrale IV-Infrastrukturen

Bei der Umsetzung dezentraler IV-Konzepte treten jedoch verstärkt technologische Hindernisse zutage, die sich vor allem im Fehlen von vollständigen Lösungen für das Systemmanagement und der mangelhaften Integrationsfähigkeit heterogener Architekturen manifestieren.

Komplexität verteilter Systemumgebungen

Verteilte Systeme sind meist durch eine große Anzahl an Komponenten charakterisiert, die sich über weite geographische Bereiche ausdehnen können. Die dabei eingesetzten Systeme können die gesamte Bandbreite zwischen PC und Großrechner umfassen.

Im Gegensatz zu zentralen Systemen ist es aufgrund echter Parallelität und asynchroner Kommunikationsbeziehungen nicht möglich, einen globalen Systemzustand zu beschreiben, da kooperierende Teile einer Applikation über mehrere Rechner verteilt sind.

In der Regel werden alle Ressourcen im Kontext des lokalen Betriebssystems verwaltet, was dazu führt, daß die einzelnen Objekte keine netzweite Identität besitzen. Durch die Größe und Komplexität verteilter Systemumgebungen ist es jedoch nicht möglich, jede Komponente bzw. jeden Benutzer in einem lokalen Kontext zu verwalten.
Berücksichtigt man darüberhinaus die Heterogenität solcher Umgebungen, so ist es aufgrund unterschiedlicher Managementschnittstellen nahezu unmöglich, ein integriertes Managementkonzept zu erstellen.

Managementproblematik bei verteilten Systemen

Zentrale Rechensysteme hatten vorrangig die Aufgabe, Benutzern Ressourcen zuzuweisen und diese zu verwalten. Werkzeuge für ein effektives Systemmanagement waren dabei integraler Bestandteil des Betriebssystems.

In verteilten Umgebungen ist man jedoch mit einer Vielzahl unterschiedlicher Systeme konfrontiert. Die Größe und Komplexität dieser Umgebungen machen es unmöglich, die Systeme isoliert zu verwalten.

Darüberhinaus sind „klassische" Managementaufgaben, wie Benutzerverwaltung, die Überwachung der Verfügbarkeit und Leistung, Sicherheitsmanagement, etc. nicht mehr auf den Kontext eines einzelnen Systems beschränkt, sondern beziehen sich nun auf die gesamte verteilte Umgebung.
Die Heterogenität der beteiligten Systeme bedingt zudem, daß die Managementaufgaben zwischen den unterschiedlichen Systemen differieren.

Integration heterogener Systemumgebungen

Es ist also zwingend erforderlich, über die reine Interoperabilität der Systeme eine Integration der einzelnen Rechner im Rahmen einer verteilten Infrastruktur vornehmen zu können.
Der Blick darf dabei jedoch nicht nur auf „offene" Systeme beschränkt bleiben, da der Aufwand und das unternehmerische Risiko einer vollständigen Migration hin zu

offenen Informationsverbunden zu groß ist. Es müssen also auch die proprietären, zentralen Rechensysteme in die unternehmensweite Infrastruktur eingebettet werden können.

Ein Ansatz dieser Problematik zu begegnen ist, die heterogenen Systeme über eine gemeinsame Softwareschicht, die auf den unterschiedlichen Betriebssystem- und Kommunikationsarchitekturen aufsetzt zu koppeln. Diese auch als *Middleware* bezeichnete Komponente erlaubt eine Kooperation zwischen heterogenen Systemen eines Verbundes über gemeinsame Schnittstellen und Dienste. Ein Repräsentant dieser Klasse ist das *Distributed Computing Environment* der *Open Software Foundation.*

1.3 Die Architektur von OSF/DCE

Das *Distributed Computing Environment (DCE)* der *Open Software Foundation (OSF)*, einer Organisation, in der sich eine Reihe namhafte Hersteller zusammengeschlossen hat, um die Verbreitung von „offenen" Technologien zu fördern, ist eine integrierte, herstellerunabhängige Umgebung, die vor allem Interoperabilität in heterogenen, verteilten Systemen gewährleisten soll.
DCE setzt sich aus einer Reihe von Basisdiensten zusammen, die die Unabhängigkeit von konkreten Betriebssystemen und Transportprotokollen sicherstellen und zudem einen netzweiten Kontext für Applikationen definieren.

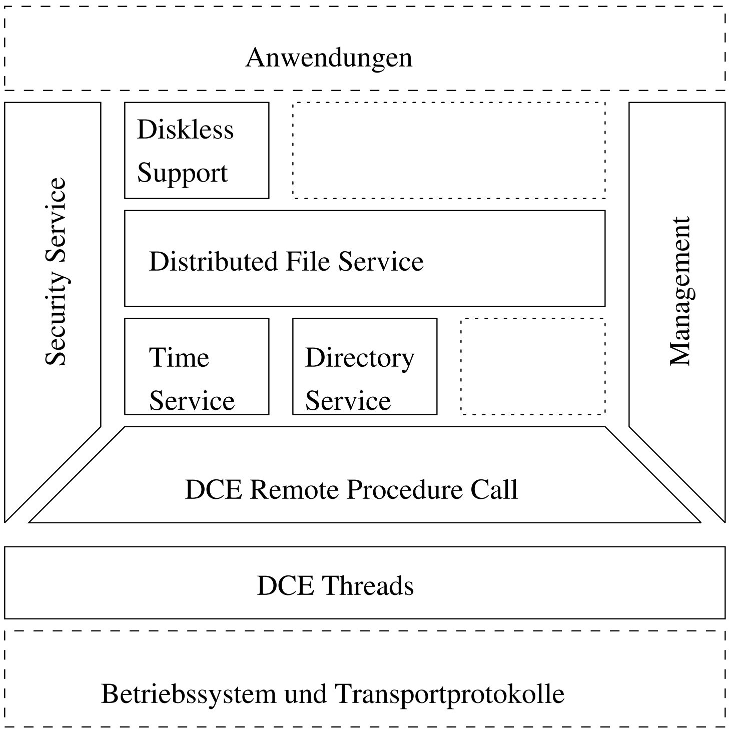


Abbildung 1.2: Die Architektur von OSF/DCE

Eine kurze Beschreibung der Komponenten und Dienste von DCE ist dieser Arbeit im Anhang beigefügt.

Bedeutung von Zellen im Rahmen von DCE

Verteilte Systeme setzen sich aus einer Menge von Einzelsystemen *(Knoten)* zusammen. Wie im vorangegangenen Abschnitt dargelegt, ist es jedoch erforderlich einen verbundweiten Kontext für solche Umgebungen zu definieren, um eine effiziente Nutzung und Administration zu ermöglichen. Eine solche Strukturierung eines DCE-Verbundes erfolgt über die Definition von Zellen.

Mit Hilfe von Zellen werden Verbunde zu Einheiten mit gemeinsamen Sicherheitsdienst und gemeinsamen Namensraum zusammengefaßt. Im Rahmen dieser Dienste lassen sich Ressourcen und Benutzer innerhalb verschiedener Zellen anordnen. Die Zuordnung von Benutzern und Ressourcen zu Zellen erfolgt dabei meist über Kriterien wie gemeinsamer Kooperation, oder geographischer Nähe. Dabei gilt es jedoch zu berücksichtigen, daß die durch Zellen zusammengefaßten Rechnerverbunde paarweise disjunkt sein müssen.
Im Zusammenhang mit der engen Integration der Datenbank des Sicherheitsdienstes, sowie des Dateiraumes in der Namensraum einer Zelle stellt dies eine Restriktion bei der Konzipierung einer Zellstruktur dar.

DCE stellt jedoch auch Mechanismen zur Verfügung, die eine Kooperation zwischen den Diensten und Benutzern unterschiedlicher Zellen erlauben. Somit ist es möglich, mit Zellen unterschiedliche administrative Bereiche zu beschreiben, ohne dabei eine weitreichende Zusammenarbeit zwischen unterschiedlichen Bereichen zu beschränken.

1.4 Strukturierungsaspekte bei verteilten Umgebungen

Verteilte Umgebungen sind nur dann sinnvoll einsetzbar, wenn sie die Kooperation zwischen unterschiedlichen Benutzern ermöglichen. Optimalerweise sollten verteilte Systeme sogar die konkreten Kooperationsabläufe (*workflows*) unterstützen, viel entscheidender ist jedoch, daß die Struktur der Kooperation geeignet auf die Funktionalität verteilter Basisplattformen abgebildet werden kann. Dabei muß berücksichtigt werden, daß sowohl die Teilnehmer an Kooperationsbeziehungen (Subjekte), als die Objekte, d.h. der Gegenstand der Zusammenarbeit, über mehrere Rechensysteme verteilt sind.

Es müssen in einer verteilten Umgebung demnach Dienste existieren, die auf der einen Seite eine Identifizierung von Benutzern vornehmen können und auf der anderen Seite Mechanismen zur Verfügung stellen, die die entsprechenden Objekte vor unberechtigtem Zugriff zu schützen.
Dabei muß durch die Konfiguration sichergestellt werden, daß sich Kooperationsbeziehungen zwischen den Subjekten geeignet ausdrücken lassen und daß auf die Kooperationsressourcen von jedem Partner in definierter Weise zugegriffen werden kann.
Zu diesem Zweck müssen sich Benutzer, sowie Ressourcen gruppieren lassen und es besteht die Notwendigkeit, Zugriffsrelationen zwischen Gruppen von Subjekten und Objekten zu spezifizieren (vgl. Abbildung 1.3).
Außerdem sollten für ein möglichst transparentes Arbeiten persönliche bzw. gruppenorientierte Sichtweisen auf die gesamte Infrastruktur möglich sein.

Ein weitere Strukturierungsaspekt ergibt sich aus der Zuordnung von Teilen eines

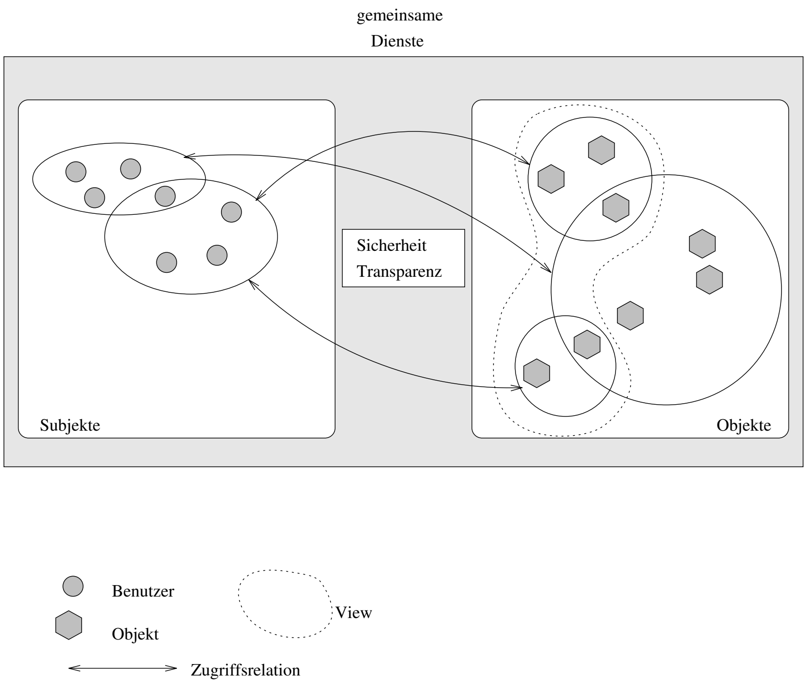


Abbildung 1.3: Strukturierung eines verteilten Verbundes anhand von Kooperationsbeziehungen

Verbundes zu unterschiedlichen Organisationen. Hierbei muß die Strukturierung vor allem die Zuständigkeitsbereiche voreinander abgrenzen.
Über die Grenzen dieser Bereiche muß jedoch sowohl was die Nutzung, als auch die Administration betrifft, eine gewisse Form von Kooperation möglich sein.
Wie in Abbildung 1.4 skizziert, kann unter diesen Bereich sowohl die Zusammenarbeit mit externen Partnern, als auch das Nutzen externer Dienstleistungen (*Outsourcing*) fallen.

Innerhalb einer Organisation ist man wiederum aufgrund der Aufbauorganisation mit unterschiedlichen, vornehmlich hierarchischen Strukturen konfrontiert.

Gerade große Firmen sind typischerweise über eine Reihe von Standorten verteilt, an denen eigene Organisationsstrukturen auf Bereichs- bzw. Abteilungsebene bestehen. Jedoch besthehen nicht nur zwischen organisatorischer und geographischer Struktur Abhängigkeiten, sondern ebenso zwischen Dienst- und topologischer Struktur.

Verteilte Verbunde können auch als Zusammenschluß unterschiedlicher Dienste interpretiert werden. Diese Dienste werden meist verbundweit zur Verfügung, aus organisatorischen Gründen jedoch meist zentral verwaltet.
Ein Beispiel hierfür sind unternehmensweite Produktdatenbanken, die an zentraler Stelle gepflegt werden.
Je komplexer die topologische Struktur eines verteilten Verbundes ist, desto mehr Probleme stellen sich bei der Nutzung der Dienste ein:

- Bei großen Verbunden ist eine einzige Dienstinstanz aus Leistungsgründen in der Regel nicht ausreichend. Es müssen also mehrere Instanzen eines Dienstes angeboten werden. Dabei dürfen jedoch keine Konsistenzprobleme auftreten.
- Sobald innerhalb eines Verbundes mehrere Instanzen eines Dienstes vorhan-

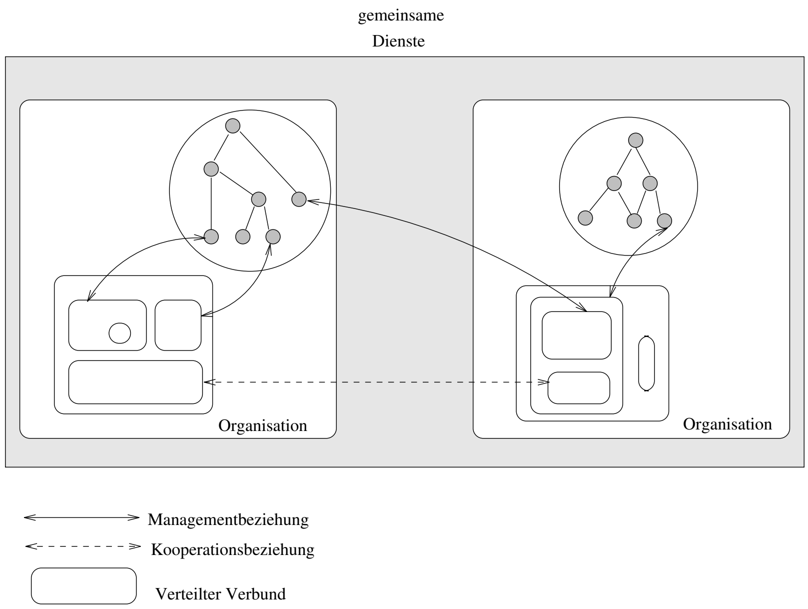


Abbildung 1.4: Strukturierung eines verteilten Verbundes anhand der Organisationsstruktur

den sind, muß berücksichtigt werden, daß aufgrund der topologischen Struktur stark unterschiedliche Antwortzeiten auftreten können. Es muß also sichergestellt werden, daß Clients nach Möglichkeit Serverinstanzen innerhalb des lokalen Teilnetzes nutzen (vgl. Abbildung 1.5).

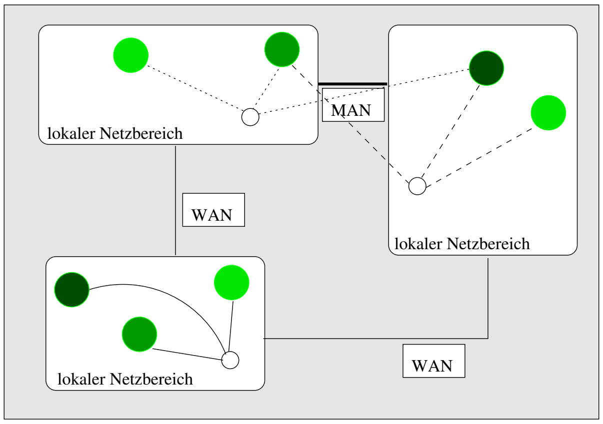


Abbildung 1.5: Strukturierung eines Verbundes anhand der topologischen Struktur

Selbst dieser kurze Überblick über unterschiedliche Strukturierungsaspekte zeigt, daß es für eine umfassende Strukturierung eines verteilten Verbundes nicht ausreichend ist, lediglich Teilaspekte zu berücksichtigen. Ein vollständiges Konzept muß demnach alle Einflüsse auf die Strukturierung einbeziehen und nach Möglichkeit Konflikte, die durch unterschiedliche Sichtweisen bedingt sind, eliminieren.

1.5 Problemstellung

Bei der BMW AG ist geplant, eine zentrale CAD-Installation durch einen Workstationverbund abzulösen, der weltweit über mehrere Standorte verteilt ist. In einer mehrstufigen Migration werden circa 600 CATIA-Arbeitsplätze in dezentrale Umgebungen überführt.

Dieser Verbund ist in hohem Maße von der effizienten Erbringung eines Dateidienstes abhängig. Deshalb ist geplant, zu einem späteren Zeitpunkt DFS – und damit DCE – als verteilte Basisplattform einzusetzen.
Der Einsatz von DCE bedingt jedoch stets, den Aufbau einer entsprechenden Zellstruktur.

Aufgrund der momentan noch geringen Verbreitung von DCE als Plattform für den Betrieb verteilter Systemumgebungen stehen kaum aussagekräftige Untersuchungen zu Zellstrukturen zur Verfügung. Darüberhinaus existieren keine Referenzinstallation, anhand deren die Qualität einer Zellstruktur für Verbunde dieser Komplexität belegt und gemessen werden könnte.
Dieser Mangel an Erfahrung macht es erforderlich, einen möglichen Übergang auf DCE im Vorfeld genau zu planen, da nachträgliche Änderungen an der Zellstruktur nur mit einem großen Aufwand durchgeführt werden können.
Der möglichst guten Anpassung der DCE-Infrastruktur an das vorliegende Szenario kommt dabei besonders große Bedeutung zu, da Störungen, die durch Unzulänglichkeiten der Zellstruktur hervorgerufen werden, in einem unternehmenskritischen Bereich wie der Fahrzeugentwicklung nicht hinnehmbar sind.

Von entscheidender Bedeutung für das gesamte Vorgehen ist, die unabhängig von DCE existierenden Anforderungen an den Betrieb und die Nutzung einer verteilten Systemumgebung zur Grundlage aller Überlegungen zu machen.
In erster Linie gilt es also eine betreiber- und nutzungsgerechte Strukturierung des Verbundes über Zellstrukturen zu realisieren.

Ziel dieser Arbeit ist es, anhand eines konkreten Falles die Möglichkeiten der Zellstrukturierung für große Workstationverbunde zu demonstrieren und zu bewerten. Wichtig ist in diesem Zusammenhang auch das Identifizieren möglicher technologischer Einschränkungen, die die Zellstrukturierung beeinflussen können. Diese können sich sowohl aus dem Szenario, als auch aus der Architektur von DCE ergeben.

1.6 Ausblick auf die folgenden Kapitel

In einem ersten Schritt werden Untersuchungen, die sich mit dem Betrieb und der Strukturierung verteilter Umgebungen auseinandersetzen auf ihre Anwendbarkeit auf die Problematik der Zellstrukturierung hin untersucht. Dabei stehen vor allem Domänenkonzepte im Vordergrund, da sie konzeptionell in einem engen Zusammenhang zur Zellbildung zu sehen sind.

Nach der Klärung allgemeiner Strukturierungsmöglichkeiten müssen Kriterien definiert werden, die es erlauben die Zellstrukturierung systematisch zu betreiben.
Diese Einflußgrößen sollen einen möglichst vollständigen Rahmen für den Entwurf und eine daran anschließende Bewertung der zu definierenden Zellstrukturen bilden.
Die Zielsetzung dieses Kapitels ist, die Voraussetzungen für einen Top-Down-Ansatz beim Entwurf konkreter Zellstrukturierungen zu schaffen.

Bevor der eigentliche Kern der Arbeit – die Darstellung und Bewertung unterschiedlicher Zellstrukturen – folgt, wird das Szenario bei BMW, das als Grundlage der Untersuchungen dient, vorgestellt.
Aus diesem Szenario ergeben sich die Anforderungen, die im Rahmen der Diskussion unterschiedlicher Ansätze bei der Zellstrukturierung umgesetzt werden müssen.

Im Zentrum der Arbeit werden dann unterschiedliche Ansätze für die Zellstrukturierung auf die Problemstellung bei der BMW AG angewendet. Für jede vorgestellte Zellstruktur wird eine Bewertung anhand der aufgestellten Kriterien vorgenommen.

Anschließend werden die Ergebnisse der Untersuchung zusammengefaßt. Dabei sind die unterschiedlichen Ansätze zur Zellstrukturierung vergleichend einander gegenüber zu stellen und die Vorzüge bzw. Nachteile herauszuarbeiten.
Zudem soll an dieser Stelle darauf eingegangen werden, welche funktionalen Einschränkungen im Zusammenhang mit der Architektur von DCE die unterschiedlichen Zellkonzepte aufweisen.

Den Abschluß der Arbeit bildet eine Empfehlung für eine Zellstruktur, die die BMW-spezifischen Anforderungen am vollständigsten löst.

Kapitel 2

Existierende Lösungen im Bereich der Strukturierung verteilter Umgebungen

2.1 Domänenkonzepte

Im Bereich verteilter Systeme existieren eine Reihe von Ansätzen, die versuchen, über die logische Gruppierung von Komponenten die Komplexität verteilter Systemumgebungen besser beherrschbar zu machen. Diese Ansätze unterscheiden sich jedoch in der Beschreibung was innerhalb Domänen zusammengefaßt werden soll, und wie Relationen zwischen unterschiedlichen Domänen charakterisiert werden können.

Eine ausführliche Diskussion der unterschiedlichen Ansätze würde den Rahmen dieser Arbeit sprengen, deshalb wird im folgenden lediglich ein Domänenkonzept vorgestellt, das in vielen Bereichen die Möglichkeit bietet, Ansätze für die Zellstrukturierung wiederzuverwenden.

Das entsprechende Domänenkonzept ist im Rahmen des DOMINO-Projektes am Imperial College [DOMAINS] [Manage 90] entstanden.

Für die Beschreibung verteilter Systeme wird dabei ein objektorientierter Ansatz gewählt. Dabei werden zwei Klassen unterschieden:

- Managed Objects:
  Managed Objects werden durch eine eigene Managementschnittstelle charakterisiert, über die der Objektzustand erfragt bzw. modifiziert werden kann.

- Manager:
  Managerobjekte können sowohl menschliche Verwalter, als auch Prozesse sein. Manager können selbst auch wieder Managed Objects sein, etwa um hierarchische Verwaltungsstrukturen zu beschreiben.
  Die Art wie die Interaktion zwischen Managern und Managed Objects verläuft wird über Zugriffsregeln beschrieben.

Im Rahmen von DCE entsprechen die Managed Objects den einzelnen Diensten bzw. Teilbereichen dieser Dienste und die Manager werden durch die DCE-Identitäten

(Principals) von Verwaltern repräsentiert.
Da nahezu alle Teile von DCE über Zugriffskontrollisten verwaltet werden; es lassen sich Relationen zwischen Managern und Objekten durch Zugriffrechte beschreiben.

Zur Strukturierung des Managements werden Domänen eingesetzt, um spezifische Sichtweisen auf die zu verwaltenden Objekte zu definieren. Die Grenzen der einzelnen Domänen beschreiben dabei auch die Grenzen der Zuständigkeit innerhalb eines Verbundes.
Die Zielsetzung der Einteilung eines verteilten Verbundes in Domänen ist, die zu verwaltenden Objekte nicht mehr isoliert, sondern als Einheit betrachten und verwalten zu können.

Für eine effektive Strukturierung ist es jedoch nicht ausreichend, lediglich die Objekte innerhalb von Domänen zusammenzufassen, es muß darüberhinaus auch eine Anordnung von Managern innerhalb spezieller Managerdomänen möglich sein.

2.2 Ergebnisse zur Zellstrukturierung im Rahmen von OSF/DCE

Die vorliegende Version 1.0 von OSF/DCE wird vorrangig zur Evaluierung der Konzepte und Schnittstellen von DCE genutzt. Gerade im industriellen Umfeld existieren noch keine größeren DCE-Installationen die bereits produktiv genutzt werden. Eine Reihe von Universitäten und Rechenzentren haben über die letzten Jahre Pilotinstallationen in Betrieb genommen. Auf den daraus gewonnenen Ergebnissen [DCE Perf 93] [Login Perf 94] basiert zum Teil diese Arbeit.
Als Grundproblem hat sich dabei herausgestellt, daß diese Pilotinstallationen meist nur einen geographisch und zahlenmäßig eng eingegrenzten Raum umfassen.

Aus diesem Grund existieren aus diesen Projekten nur in eingeschränkten Maße Ergebnisse [Mack 94], die für diese Arbeit verwendbar sind, da viele DCE-Installationen nicht explizit unter dem Aspekt des Systemmanagements betrieben werden, vor allem jedoch unter den genannten Einschränkungen meist nur aus einer Zelle bestehen.

Einige Anhaltspunkte, die für die Wahl einer Zellstruktur herangezogen werden können, zählt die OSF in ihrer Dokumentation auf [OSF Admin].

Die genannten Hinweise für die Einteilung eines Verbundes in Zellen haben jedoch nur am Rande eine Bedeutung für diese Arbeit, da sie keinen strukturierten Entwurf von Zellen unterstützen, sondern lediglich für spezielle Teilprobleme bei der Implementierung einer Zelle heranzogen werden können.

Kapitel 3

Einflußfaktoren für die Wahl einer Zellstruktur

Aufgrund der Komplexität und Vielfalt von verteilten Umgebungen kann es kein generisches Zellkonzept geben. Es ist vielmehr nötig in der Planungsphase eine genaue und vollständige Analyse der sich darstellenden Verhältnisse durchzuführen, da die Zellstruktur auf die Konzepte für den Betrieb und die Nutzung der IV-Infrastruktur abzustimmen ist. Daraus resultiert, daß vorrangig die Einflüsse aus der gegebenen Infrastruktur berücksichtigt werden müssen. Es gilt darüberhinaus zu untersuchen, inwieweit DCE architekturbedingt mögliche Freiheitsgrade einschränkt.
Der Entwurf konkreter Zellstrukturen ist deshalb in erster Linie ausgehend von den Zielsetzungen der zu schaffenden Infrastruktur, hin zu einer konkreten Realisierung zu betreiben und nicht als Anpassung der vorliegenden Verhältnisse an eine ad hoc aufgestellte Zellimplementierung.

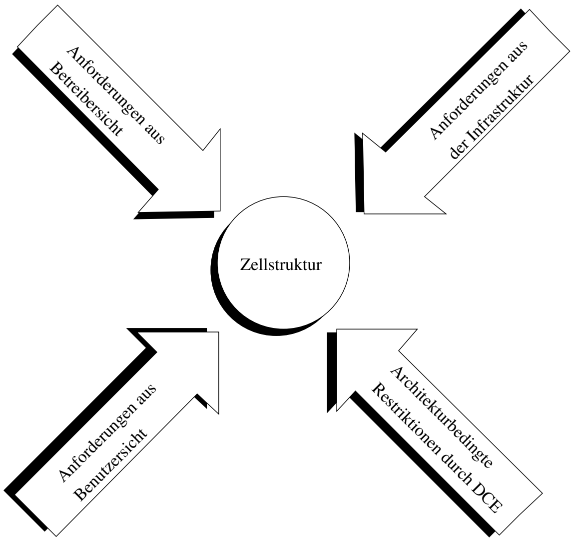


Abbildung 3.1: Einflußgrößen für die Wahl einer Zellstruktur

3.1 Infrastruktur

3.1.1 Ausdehnung eines Verbundes

Im Rahmen der Infrastruktur muß zunächst die Größe der gesamten Installation berücksichtigt werden. Die Ausdehnung kann eine Workgroup, ein Gebäude, eine Stadt oder gar Standorte auf mehreren Kontinenten umspannen. Eine ähnliche Bandbreite kann eine Installation hinsichtlich der Anzahl der eingesetzten Rechner und registrierten Benutzer aufweisen.
Die daraus resultierende Komplexität des Gesamtsystems findet ihren Niederschlag u.a. in der zugeordneten Netzstruktur und in den Aspekten der Verteiltheit. Von besonderer Bedeutung im Zusammenhang mit der Größe eines Verbundes sind die Ausprägungen der Skalierbarkeit, vor allem im Administrations- und Leistungsbereich.

3.1.2 Topologie

Die räumliche Trennung von Dienstnachfrage und Diensterbringung ist ein wesentliches Merkmal des Client/Server-Modells. Sie bedingt, daß sowohl Aufträge, als auch Ergebnisse über ein Netzwerk transportiert werden müssen. Die Dienstgüteparameter des unterliegenden Netzes, wie etwa Durchsatz, Verzögerung und Verfügbarkeit, haben also erheblichen Einfluß auf die Qualität der Bearbeitung der entfernten Prozeduraufrufe.
Innerhalb eines lokalen Netzes ergeben sich aufgrund geringer Transportzeiten diesbezüglich keine speziellen Auswirkungen auf die Zellstruktur. Handelt es sich jedoch bei der Netzstruktur um einen Verbund von Teilnetzen, so sind Parameter wie Bandbreite, Zuverlässigkeit und Verkehrsaufkommen der einzelnen Teilnetze bestimmende Faktoren für die Zellstrukturierung.

Um einen möglichst effizienten Betrieb zu ermöglichen, müssen folgende Ziele im Rahmen der Zellstruktur umgesetzt werden:

- Minimierung des DCE-Verkehrs, speziell über Verbindungen geringer Bandbreite, um das Antwortzeitverhalten der genutzten Dienste nicht zu beeinträchtigen.
- Minimierung des DCE-Verkehrs über organisationsweit genutzte Backbones, da diese allgemein genutzte Betriebsmittel mit unter Umständen stark schwankender Verkehrsmenge sind.
- Die Verfügbarkeit soll auch bei eventuell auftretenden Netzstörungen möglichst umfassend gewährleistet sein.

Der Umfang, in dem diese Ziele realisiert werden können, hängt jedoch stark davon ab, ob die am intensivsten genutzten Ressourcen innerhalb desselben Teilnetzes vorhanden sind. Der Grad, der dadurch charakterisierten funktionalen Eigenständigkeit von Netzbereichen beeinflußt in zentraler Weise die Planung einer Zellstruktur.

Ein weiterer Gesichtspunkt ist, ob Kommunikation auch über öffentliche Netze stattfindet, da in diesem Fall zusätzliche Sicherheitsmaßnahmen getroffen werden müssen. Zudem hat hierbei die Minimierung des Verkehrs aufgrund volumenbezogener Abrechnung eine hohe Priorität.

Generell läßt sich feststellen, daß die Netzstruktur kein originäres Kriterium für die Wahl einer Zellstruktur darstellt, jedoch im Zusammenhang mit der Systemstruktur von DCE im Kontext anderer Gesichtspunkte, wie etwa der Leistung oder der Verfügbarkeit erheblichen Einfluß ausübt.
Das Gewicht, das dabei der Netzstruktur beizumessen ist, hängt zudem entscheidend von der eingesetzten Technologie ab. Gerade in Hinblick auf die moderne Weitverkehrstechnik gehen die Grenzen zwischen LAN und WAN zunehmend fließend ineinander über. Somit wird auch die Bedeutung der Netztopologie bei der Wahl einer Zellstruktur geringer.

3.1.3 Kooperationsaspekte

Die Art, in der die Diensterbringung verteilt ist, spiegelt sich in den einzelnen Client/Server-Beziehungen einer verteilten Umgebung wider. Anhand dieser Beziehungen läßt sich Kooperation im Rahmen eines Verbundes beschreiben.
Berücksichtigt man darüberhinaus die Häufigkeit dieser Beziehungen, sowie die ausgetauschten Datenmengen, so erhält man Aufschluß über funktionale und organisatorische Abhängigkeiten bzw. über die Eigenständigkeit der einzelnen Bereiche.

Im Kontext von DCE drückt sich die Art der Nutzung eines Verbundes zusätzlich durch die unterschiedlichen Kooperationsmodelle aus:

- Client/Server Modell:
  Beim Client/Server-Modell findet Kooperation über die Nutzung gemeinsamer Ressourcen statt. Es bestehen also keine dauerhaften Kooperationbeziehungen zwischen einzelnen Benutzern, sondern lediglich Kooperation, die streng nach Dienstnachfrage und Diensterbringung gegliedert ist.
  Ein Beispiel für dieses Kooperationsmodell ist die Zuordnung von Betriebsmitteln zu einer Menge unabhängiger Benutzer (z.B. gemeinsame Nutzung eines Druckdienstes)

- Modell der gemeinsamen Datenhaltung:
  Die Kooperation vollzieht sich asynchron über den Austausch von Dateien im Rahmen eines globalen, verteilten Dateisystems. Die kooperationsrelevanten Informationen können zur Unterstützung von Gruppenaktivitäten in einem, jeweils einer Gruppe zugeordneten *Repository* verwaltet werden.

Motivation für die Strukturierung ist also nicht nur die Menge der ausgetauschten Information, sondern vor allem das eingesetzte Kooperationsmodell.
Kooperation, die sich an der Nutzung gemeinsamer Ressourcen orientiert, ist also eher im Rahmen einer monolithischen Zelle zu realisieren, da die Zuordnung von Ressourcen zu Benutzergruppen über die Strukturierung des Namensraumes umgesetzt werden kann. Zudem besteht innerhalb einer Zelle die Möglichkeit, persönliche Sichtweisen auf den gesamten Namensraum zu definieren
Demgegenüber wird durch Kooperation über den Austausch von Dateien die Wahl einer konkreten Zellstruktur weniger stark beeinflußt, da Zugriffe über Zellgrenzen hinweg bei *DFS* möglich sind. Die entsprechenden Daten und Benutzer können also über mehrere Zellne verteilt sein.

3.1.4 Funktionale Differenzierung der Rechensysteme

Aus administrativer Sicht ist die Unterscheidung von Client- und Serverkomponenten auf der Bearbeitungsebene nicht ausreichend. Von großer Bedeutung ist, wie die Kooperationsbeziehungen innerhalb einer Infrastruktur technologisch realisiert sind. Das Konfigurationsmanagement muß diese Gegebenheiten in angemessener Weise umsetzen. Unter diesen Punkt fallen in erster Linie die Verteilung der Dienste und Ressourcen.
Aus dieser Sichtweise zerfällt die Menge aller Rechner in zwei Klassen:

1. Serverrechner:
   Serverrechner zeichnen sich durch ein spezielles Profil aus, das durch die Art und Menge der von ihnen erbrachten Dienste geprägt ist.

2. Clientrechner:
   Im Gegensatz dazu sind die Clientrechner meist mit allen Clientkomponenten der verschiedenen Dienste ausgestattet und weisen zur Vereinfachung des Managements eine weitgehend identische Konfiguration auf.

Von zentraler Bedeutung ist in diesem Zusammenhang auch die Zuordnung von Clients zu spezifischen Serverinstanzen innerhalb eines Dienstes. Ohne Eingriffe in die Konfiguration einer Zelle werden die Serveraufrufe zufällig über alle Serverinstanzen verteilt. Gerade unter dem Aspekt der Minimierung des globalen Netzverkehrs ist es jedoch wünschenswert, diesen Lastausgleich auf der Basis lokaler Server zu definieren. Clients sollten also nach Möglichkeit Serverinstanzen innerhalb desselben Teilnetzes nutzen.

3.2 Organisation

Eine zentrale Herausforderung, die sich beim Entwurf einer Zellstruktur ergibt, ist, die organisatorischen Konzeptionen aus Sicht

- der Betreiber,
- des Unternehmens
- und der Benutzer

innerhalb eines Zellkonzeptes möglichst vollständig und exakt umsetzen zu können.

3.2.1 Betreiberorganisation

Die Betreiberorganisation beschreibt, wie die Zuständigkeiten für die Verwaltung der verteilten Umgebung innerhalb einer Organisation geregelt sind.
Durch die Verteilung von Zuständigkeiten für gewisse Teilbereiche wird ein Managementkonzept definiert, das im Rahmen einer Zellstruktur zu unterstützen ist.
Bei diesem Punkt ist vorrangig darauf zu achten, daß sich die Aufbau- und Ablaufstrukturen der Betreiberorganisation geeignet durch die Wahl der Zellstruktur reflektiert werden, um einen effizienten Betrieb zu gewährleisten.
Für die Organisation des Management existieren eine Reihe von grundlegenden Konzeptionen:

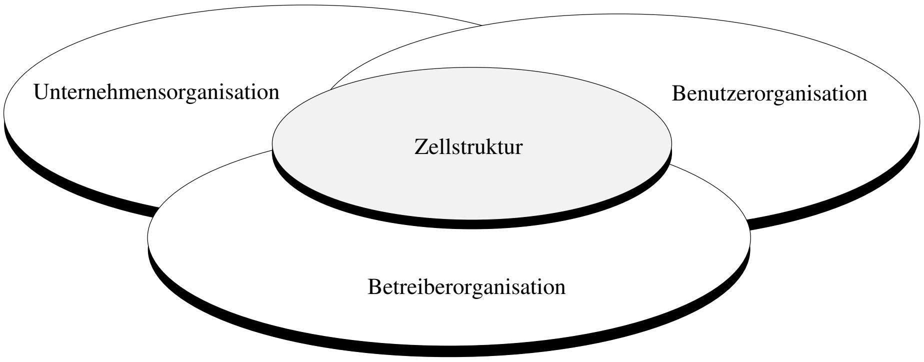


Abbildung 3.2: unterschiedliche organisatorische Einflüsse auf die Zellstruktur

- zentralisiert:
  Einer der gebräuchlichsten Ansätze für das Management verteilter Systeme ist das Prinzip der zentralen Kontrolle. Dabei hat eine einzige Verwaltungseinheit vollständige Kontrolle über alle Elemente des verteilten Systems.
- hierarchisch:
  Der hierarchische Ansatz entspricht dem zentralisierten bis auf die Tatsache, daß gewisse Tätigkeiten bzw. die Verantwortung für gewisse Bereiche der verteilten Umgebung delegiert werden.
  Die Kernaufgaben bleiben jedoch der Organisationseinheit an der Wurzel vorbehalten.
- dezentral bzw. autonom:
  Hierbei werden die Zuständigkeiten für dir Verwaltung eines Verbundes über mehrere Verwaltungsinstanzen verteilt. Die dadurch definierten Bereiche werden eigenständig verwaltet.
- föderativ:
  In diesem Ansatz kann keine Organisationseinheit das Recht, ohne Absprache mit einer anderen, Kontrolle über einen Teil des verteilten Systems auszuüben. Für administrative Handlungen müssen die gegenseitigen Rechte und Rollen ausgehandelt werden.

3.2.2 Unternehmensorganisation

Wesentlichen Einfluß auf die Zellstruktur hat die Art in der sich Kooperation aus unternehmerischer Sicht darstellt.
Dabei gilt es vor allem die Grenzen der einzelnen Organisationseinheiten und die innerhalb und zwischen ihnen stattfindenden Interaktionen im Rahmen eines Zellkonzepts geeignet zu beschreiben. Als Anhaltspunkte dafür dienen die Datenströme, die zwischen Organisationseinheiten fließen.
Darüberhinaus ist es von Bedeutung, wie sich diese Kooperationsbeziehungen in Hinsicht auf unterschiedliche Projekte verhalten. Je dynamischer sich diese Abläufe darstellen, desto flexibler muß der Mechanismus sein, der diese Beziehungen ausdrückt.

Die Aufbauorganisation eines Unternehmens spielt bei der Strukturierung dann eine wesentliche Rolle, wenn die organisatorischen Einheiten die Kosten, sowohl für die Komponenten, als auch für die in Anspruch genommenen Dienste übernehmen müssen. In diesem Fall ist es erforderlich, den einzelnen Abteilungen eine gewisse Autonomie bei der Nutzung und bei Erweiterungen ihres Teilbereiches einzuräumen.

3.2.3 Benutzerorganisation

Die in einem vorangegangenen Abschnitt angesprochene Verteilung der Ressourcen inklusive deren Funktionalität, und die Art ihrer Nutzung läßt sich auch als Aufbau- und Ablauforganisation aus Benutzersicht interpretieren.
Sie beschreibt aus technischer Sicht, wie sich innerhalb eines verteilten Verbundes Kooperation vollzieht.

Darüberhinaus ist zu untersuchen, in welche Gruppen die gesamte Benutzerpopulation eingeteilt ist. Anhaltspunkte für eine solche Einteilung liefern:

- die Zuordnung von Benutzern zu Organisationseinheiten,
- die Zuordnung von Benutzern zu den von ihnen ausgeübten Funktionen,
- die Zuordnung von Benutzern zu den von ihnen genutzten Ressourcen.

3.3 Administration

Eine wichtige Aufgabe innerhalb des Managements verteilter Systeme ist es, in möglichst flexibler Weise die Kontrolle über die Verwaltung der Ressourcen vergeben zu können. Aufgrund der Größe und Komplexität verteilter Umgebungen stellt die individuelle Zuordnung von Ressourcen zu Managern keine akzeptable Lösung dar. Statt dieser 1:1-Beziehungen ist es unbedingt erforderlich, n:m-Beziehungen zwischen den beiden Gruppen herzustellen.
Hierbei dienen Domänenkonzepte als geeignetes Hilfsmittel. Aus Betreibersicht verfolgt eine Domänenbildung vor allem folgende Ziele:

- Für jede Domäne soll eine gewisse Menge von Regeln (*policies*) umgesetzt werden.
  So ist es etwa aus Konsistenzgründen wünschenswert, daß disjunkte Benutzerdomänen auch disjunkte *Unix ID*-Bereiche zugeordnet sind.
- Unterschiedliche Domänen sollen autonom administriert werden können.
  Aktionen, die nur die Domäne selbst betreffen, wie z.B.: das Hinzufügen eines Rechners, sollten ohne Koordination mit anderen Domänen durchgeführt werden können.
- Die Domänen sollen eine angemessene Strukturierung des gesamten Verbundes ermöglichen.
  Ein verteilter Verbund, gerade im Kontext von DCE, läßt sich auch als Zusammenschluß verschiedener Dienste interpretieren. Die Strukturierung des Verbundes sollte jedoch nicht ausschließlich über die Dienststruktur, sondern vor allem über die Aufgabenstruktur des Betreibers realisiert werden.
  Ein Beispiel ist das Einrichten eines neuen Benutzers. Dazu ist es notwendig, daß ein Verwalter sowohl Administratorrechte für gewisse Bereiche der Benutzerdatenbank besitzt, sowie die Rechte, ein Benutzerverzeichnis im Dateisystem anzulegen. Ein authorisierter Verwalter sollte deshalb nicht die gesamte Kontrolle über beide Dienste haben, sondern lediglich über jene Ausschnitte, die zur Erbringung der Aufgabe nötig sind.

Innerhalb einer Betreiberorganisation ist also selbst wieder, je nach Aufgabe, eine Strukturierung vorzunehmen, mit dem Ziel, Kontrolle nicht direkt an Individuen, sondern an gewisse Rollen vergeben zu können. Diesen Rollen können dann Personen assoziiert werden, um die Kontrolle über definierte Teilbereiche der verteilten Umgebung an diese zu delegieren.
Überdies schafft dieses Verfahren die nötige Transparenz, um Vorgänge im System nachvollziehen zu können. Von einer allmächtigen Verwaltungsinstanz, wie dem `root`-Account in UNIX ist also auf jeden Fall abzusehen.

3.4 Sicherheit

Eine der zentralen Herausforderungen in verteilten Umgebungen ist die Gewährleistung des Schutzes von Informationen. Im Gegensatz zu zentralen Systemen ist es in einer vernetzen Infrastruktur nicht möglich, die Sicherheitsgrenze eines Systems mit seiner physikalischen Ausdehnung gleichzusetzen. In verteilten Umgebungen müssen über die Implementierung von Authentifizierungs- und Authorisierungsmechanismen hinaus Maßnahmen getroffen werden, um mögliche Bedrohungen für die Sicherheit des gesamten Systems auszuschließen.

3.4.1 Sicherheit der gesamten Infrastruktur

Zum ersten gilt es zu untersuchen, wie gut sich die Sicherheitsmechanismen von DCE innerhalb verschiedener Zellstrukturen umsetzen lassen. Dabei ist auch von Interesse, in welchem Ausmaß der gesamte Verbund von einem Einbruch betroffen wird.

Darüberhinaus muß untersucht werden, wie sich unterschiedliche Sicherheitsanforderungen für unterschiedliche Bereiche eines Verbundes im Rahmen der jeweiligen Zellstruktur umsetzen lassen.

3.4.2 Sicherheit auf Rechnerebene

Beim Einsatz der Sicherheitsmechanismen von DCE muß berücksichtigt werden, daß Ressourcen, die nicht unter der Verwaltung von DCE stehen, nur durch die Mechanismen des lokalen Betriebssystems geschützt werden können.
Da DCE seinerseits Informationen in lokalen Dateien speichert, können sicherheitskritische Daten auch dann in die Hände eines Eindringlings fallen, wenn er nur die Mechanismen des lokalen Betriebssystems überwindet.
Rechner, die besonders kritische Daten (z.B. Benutzerdatenbanken) halten, sind deshalb zusätzlich physikalisch zu sichern und nach Möglichkeit unter Rechenzentrumsbedingungen zu betreiben.

An dieser Stelle sollte nicht unerwähnt bleiben, daß die Problematik des unberechtigten Zugriffs auf Dateien des lokalen Dateisystems auch Konsequenzen im Bereich der Gesamtsicherheit einer Zelle hat, da zwei wesentliche Informationen auf jedem Rechner in lokalen Dateien gespeichert werden.

1. Die Tickets aller Benutzer und Dienste auf einem Rechner
   Die entsprechenden Dateien sind zwar nur für den Eigentümer lesbar, ein

Benutzer mit Superuserrechten kann jedoch diese Tickets mißbrauchen, um selbst die netzweite Identität eines anderen Benutzers anzunehmen.

2. Die Datenbank des *Portmappers*
   Diese Datei ist sogar global beschreibbar, um es allen Diensten zu ermöglichen, sich korrekt zu registrieren. Im Falle des Mißbrauchs kann jedoch jeder lokale Benutzer diese Datei zerstören und somit alle Dienste eines Rechners außer Funktion setzen.

3.4.3 Sicherheit auf Kommunikationsebene

Auf Kommunikationsebene werden Nachrichten, die zwischen Clients und Servern ausgetauscht werden durch die speziellen Sicherheitsmechanismen geschützt.
Das unberechtigte Eindringen in ein System ist jedoch – wie beschrieben – auch weiterhin eine erstzunehmende Bedrohung für die Sicherheit der gesamten Zelle. Gerade wenn Zugänge zu einem öffentlichen Netz vorhanden sind, ist es unbedingt erforderlich, sich gegen potentielle Angriffe so weit wie möglich zu schützen.
Eine verbreitete Technik unerlaubten Zugriffe auf das eigene Netzwerk zu unterbinden, stellt der Einsatz von sogenannten *Firewalls* dar.
In diesem Zusammenhang muß untersucht werden, wie unabhängig die durch die *Firewalls* beschriebenen Sicherheitsbereiche von den durch die Zellengrenzen beschriebenen Sicherheitsdomänen sind und wie sich beide Sicherheitsmechanismen in einem gegebenen Zellkonzept kombinieren lassen.

3.5 Ausfallsicherheit, Verfügbarkeit, Fehlertoleranz

In einer verteilten Umgebung ist die Diensterbringung meist von mehreren Dienstinstanzen abhängig, die ihrerseits wiederum über mehrere Rechner verteilt sein können. Es ist offensichtlich, daß bei dieser verketteten Bearbeitung von Aufträgen alle benötigten Instanzen aktiv sein müssen, um einen störungsfreien Betrieb zu gewährleisten.
Das ordnungsgemässe Funktionieren der Netzinfrastruktur ist ein weiterer Parameter, der die Verfügbarkeit von verteilten Systemen bestimmt.
Eine verteilte Umgebung besitzt also aufgrund dieser Vielzahl möglicher Fehlerquellen eine geringere Gesamtverfügbarkeit als ein zentrales System.

Eine möglichst weitreichende Verfügbarkeit verteilter Verbunde ist nur zu gewährleisten, falls folgende Bedingungen erfüllt sind:

- Die unbedingt benötigten Applikationen müssen lokal auf den Arbeitsplatzrechnern installiert sein.
- Der Zugriff auf die vom Benutzer benötigten Daten sollte auch im Falle einer auftretenden Störung zumindest in beschränktem Umfang möglich sein.
- Die verschiedenen Dienste sollten möglichst über mehrere Maschinen im Netz verteilt sein.
- Die für die Erbringung von Diensten kritischen Serverinstanzen müssen mehrfach vorhanden sein.
- Ein Auftrag soll - falls möglich - von einem Server innerhalb desselben Netzes bearbeitet werden, um die Anzahl möglicher Fehlerquellen zu minimieren

Als größtes Problem stellt sich dabei die Verfügbarkeit der Daten heraus. Da DCE nur die Read-Only-Replikation von Daten gestattet, ist es nur eingeschränkt möglich, hierfür mit den Mitteln von DCE eine effektive Lösung zu schaffen. Für Informationen, die einer häufigen Veränderung unterliegen, scheidet dieses Verfahren folglich aus, besonders wenn die Aktualität der Daten, wie etwa bei Quellcode oder Konstruktionszeichnungen ein kritischer Parameter ist.
Für Server, die verfügbarkeitskritische Daten halten, ist es demnach notwendig über andere Mechanismen, wie etwa redundante Hardware (Unterbrechungsfreie Stromversorgung, Standby-Rechner, gespiegelte Platten) die Verfügbarkeit zu gewährleisten.

Unabhängig von der Planung der Zellstruktur liegt es in der Verantwortung des Betreibers durch eine geeignete Verteilung der Ressourcen und den Einsatz von Hochverfügbarkeitslösungen eine möglichst hohe Hardwareverfügbarkeit sicherzustellen.
Im Zusammenhang mit der Verfügbarkeit von DCE muß jedoch beachtet werden, daß alle zur Ausführung benötigten Dienste aktiv sind. Diese Dienstverfügbarkeit kann über den Einsatz von Replikation erhöht werden. Zudem können durch die Verteilung der Dienste über mehrere Maschinen isolierte Fehlerquellen minimiert werden. Ist mindestens eine Instanz eines benötigten Dienstes aktiv, so laufen Störungen für einen Benutzer transparent ab. Um auch gegen eventuelle Netzstörungen geschützt zu sein, empfiehlt es sich, in jedem Teilnetz Replikate der Basisdienste anzubieten. Darüberhinaus sollte eine Zelle stets so dimensioniert werden, daß sie den Einsatz von mehreren Replikaten pro Dienst erlauben.

3.6 Migration

Im allgemeinen wird die Freiheit bei der Wahl einer Zellstruktur schon dadurch beschränkt, daß ein möglichst reibungsloser Umstieg von der existierenden Verwaltungsstruktur in die neue DCE-Umgebung garantiert sein muß.

Desweiteren muß gerade bei großen Verbunden gewährleistet sein, daß der Übergang schrittweise vollziehbar ist, da ein ad hoc durchgeführter Umstieg administrativ nicht zu bewältigen ist.
Optimalerweise sollte sogar sichergestellt werden können, daß beide Verwaltungsstrukturen in der Lage sind, bis zum Abschluß der Migration zu koexistieren.

3.7 Transparenz

Aus Benutzersicht ist Transparenz ein zentrales Kriterium. Über die, durch die Architektur der Dienste von DCE umgesetzten Transparenzformen gilt es sicherzustellen, daß Zellgrenzen innerhalb eines logischen Verbunds möglichst nicht zutage treten.
Wichtige Transparenzeigenschaften sind auch, daß der Benutzer zur Erfüllung seiner Aufgaben innerhalb einer Sicherheitsdomäne nur ein Login braucht, das für alle Rechner gültig ist, auf die er Zugriff haben muß.
Zum anderen ist es sinnvoll, daß er die von ihm benötigten Daten stets unter demselben Zugriffspfad vorfindet.
Es ist also zu untersuchen, inwieweit diese Anforderungen an die Transparenz der verteilten Umgebung durch Zellgrenzen eingeschränkt werden.

3.8 Änderungsflexibilität

Verteilte Umgebungen zeichnen sich durch die Fähigkeit aus, sich an veränderte Rahmenbedingungen anpassen zu können. Es ist deshalb zwingend erforderlich, daß die Flexibilität einer verteilten Umgebung auch nach der Definition einer Zellstruktur erhalten bleibt.
In diesem Zusammenhang wirkt eine Reihe von Einflüssen auf die Zellstruktur ein:

- Organisatorische Veränderungen
  Änderungen der Organisationsstruktur sind vor allem im industriellen Umfeld häufiger zu erwarten. Diese Tatsache legt es nahe, die Zellstruktur nicht starr an Organisationsgrenzen zu definieren, da sonst mit den Zellgrenzen auch eine Reihe von Ressourcen und Benutzern verlagert werden müßte. Allzu feinkörnige Zellstrukturen sind also im allgemeinen nicht empfehlenswert.
  Vor besonderer Bedeutung bei diesem Punkt sind auch Änderungen in der Betreiberorganisation. Diesbezüglich sollte eine möglichst flexible Zuordnung zwischen Verwaltern und Verantwortungsbereichen möglich sein.
  Delegation von Verwaltungstätigkeiten sollte deshalb über eine rollenbezogene Zugriffskontrolle und nicht bereichsbezogen über Zellgrenzen definiert werden.

- Änderungen der Konfiguration
  Eine Ausprägung der Flexibilität einer verteilten Umgebung liegt darin, daß Komponenten bezüglich ihrer Funktion, oder ihrer Lage nicht statisch sind. Man muß also in der Lage sein, diesen Veränderungen Rechnung zu tragen.

- Performanceverhalten
  Beim Erreichen der Grenze, an der eine Zelle nicht mehr mit einer zufriedenstellenden Leistungsfähigkeit betrieben werden kann, müssen Maßnahmen getroffen werden, die es erlauben, die in einer Zellstruktur enthaltenen Konzeption in eine alternative Zellstruktur zu retten.
  Die Zellstruktur muß also nach Möglichkeit aufgebrochen werden können, ohne den Betrieb zu beeinträchtigen und ohne eine Neuorganisation der Verwaltung zu erzwingen.

- Reaktion auf Erfahrungen einer Pilotphase
  Die Komplexität verteilter Verbunde hat zur Folge, daß sie in der Entwurfsphase nicht in allen Aspekten exakt geplant werden können. Die Flexibilität einer Zellstruktur wird also auch dadurch bestimmt, wie stark Erfahrungen aus einem Testbetrieb in eine endgültige Struktur einfließen können.

Wesentlich bei allen diesen Punkten ist, nicht nur Änderungen im allgemeinen durchführen zu können, sondern diese stets in Einklang mit der, der Zellstruktur zugrundeliegenden Konzeption umzusetzen.

3.9 Skalierbarkeit

Verteilte Umgebungen bewegen sich in einer großen Bandbreite zwischen kleinen, auf ein lokales Netz begrenzten Installationen und unternehmensweiten Verbunden. Skalierbarkeit drückt sich durch das Vorhandensein von Mechanismen aus, die trotz den Verschiedenheit der möglichen Umgebungen einen einheitlichen Betrieb verteilter Verbunde erlauben.

Ein weiterer Aspekt von Skalierbarkeit ist der Bezug zur Leistungsfähigkeit einer Zellstruktur. Die Planung einer Zellstruktur muß sicherstellen, daß durch das Hinzufügen weiterer Benutzer, Maschinen und Dienste die Dienstgüte möglichst wenig beeinträchtigt wird.

3.10 Leistungsgesichtspunkte

Ein weiteres Kriterium, das bei der Analyse von Zellstrukturen berücksichtigt werden muß ist das Performanceverhalten.
Dies erfordert in erster Linie eine Untersuchung, wie sich Kooperation über Zellgrenzen hinweg im Vergleich zu monolithischen Zellstrukturen verhält.

Aufgrund fehlender, oder nur sehr unvollständiger Untersuchungen im Bereich Performance [Russel 94], [Scalability 93], ist jedoch die Einschränkung zu treffen, daß nur ausgewählte Fragestellungen betrachtet werden können.
Unabhängig davon steht jedoch fest, daß die Leistungsfähigkeit und die Skalierbarkeit jeder Zelle und jedes Zellverbundes auf jeden Fall durch die Bandbreite des Netzes nach oben beschränkt sind.
Da alle Dienste durch das Client/Server-Modell realisiert sind, ist also die effiziente Erbringung einer Funktion in erster Linie davon abhängig, wie schnell die Daten zwischen Clients und Servern ausgetauscht werden können.

3.10.1 Anwendungscharakteristik

Wesentlich für die Bewertung der Leistungsfähigkeit einer Zellstruktur ist auch, welche Anforderungen von Seiten der Anwendung vorliegen. So machen Systeme zur Transaktionsverarbeitung häufig Gebrauch vom Verzeichnisdienst machen, bei einer hohen Frequenz der Kommunikationsbeziehungen, jedoch bei relativ geringen Datenmengen pro Transaktion.
Dem stehen Applikationen gegenüber, die vor allem auf dem Austausch von Dateien beruhen. Hier ist die Zugriffshäufigkeit geringer, die transportierten Datenmengen pro Aufruf allerdings wesentlich höher.

Diese Unterschiede sind bei der Bewertung der Leistungscharakteristik einer Zellstruktur zu berücksichtigen.

3.11 Verkehrscharakteristik der DCE-Basisdienste

Um konkretere Aussage über die Skalierbarkeit im Leistungsbereich treffen zu können, ist es erforderlich das durch DCE hervorgerufene Verkehrsaufkommen zu untersuchen.
Im wesentlichen sind dabei für jeden Dienst die unterschiedlichen Verkehrsarten

Hintergrundverkehr: Verkehr, der auch ohne Benutzerbetrieb vorhanden ist.

Queryverkehr: Serveraufrufe, die keine Modifikationen auf den Datenbanken durchführen und somit von Replikaten bearbeitet werden können.

Updateverkehr: Änderungen, die auf den Datenbanken der Masterinstanzen der Dienste durchgeführt werden müssen.

Replikat-Updateverkehr: Kommunikation, um die Konsistenz zwischen unterschiedlichen Serverinstanzen sicherzustellen.

gesondert zu betrachten.

3.11.1 Einfluß der Netzbandbreite

Im Rahmen einer Analyse der Firma IBM [Russel 94] wurde das Antwortzeitverhalten verschiedener Teilaspekte der Interaktion mit den Diensten von DCE, wie Login und Suche nach Bindeinformationen in Netzen unterschiedlicher Bandbreite untersucht.

	16 Mbit/s Link	4Mbit/s Link	38,4 kbit/s
Verhältnis der Bandbreite zu einem 16 Mbit/s Token-Ring	$\frac{1}{1}$	$\frac{1}{4}$	$\frac{1}{417}$
Ping	1	2	75
Authentifizierter RPC 4KB call-level auth. packet-level auth.	 1 1	 1,4 1,1	 36 8
Importieren von Bindeinformationen	1	1,5	2,3
DCE Login	1	1,4	1,8
DCE Start	1	1,3	1,4

Tabelle 3.1: Einfluß der Bandbreite auf das Antwortzeitverhalten von DCE

Das Ergebnis der Studie besagt, daß trotz der zu erwartenden Verzögerungen keine Einschränkungen der Funktionalität nachzuweisen waren. Es ist ersichtlich, daß sich Leitungen geringer Bandbreite weniger stark als zu vermuten auf das Antwortzeitverhalten der entfernten Prozeduraufrufe niederschlagen. Neben dem Durchsatz des Netzes hat also auch der Durchsatz der entsprechenden Server erheblichen Einfluß auf die gesamte Bearbeitungszeit eines entfernten Prozeduraufrufes.
Gerade zu Spitzenlastzeiten ist jedoch davon auszugehen, daß die Transportzeiten einen dominanten Einfluß auf die Bearbeitungszeit ausüben werden, der selbst bei Zugriffen innerhalb desselben LAN nicht mehr zu vernachlässigen ist.

Dieses Problem ist kaum durch die Wahl der Zellstruktur zu beherrschen, es kann lediglich versucht werden, durch Replikation der Dienste in den LAN-Segmenten möglichst viel DCE-spezifischen Verkehr auf das lokale Netz zu beschränken.

3.11.2 Hintergrundverkehr

Die hier genannten Aussagen und Zahlen sind Untersuchungen der *University of Massachusetts* [DCE Perf 93] entnommen.
Die Zahlen dieser Studie basieren auf einer, innerhalb eines LANs existierenden Zelle mit etwa 20 Rechnern. Zum Einsatz kamen dabei ein *Security Server*, zwei *CDS-Server* und drei *Time-Server*.
Auch hier muß wiederum eingeschränkt werden, daß eine lineare Übertragung der Ergebnisse auf andere Szenarien nur in sehr eingeschränktem Maße zulässig ist. Die

Bedeutung der Zahlen ist in erster Linie vor dem Hintergrund zu sehen, daß eine Abschätzung des entstehenden Verkehrs Aufschlüsse darüber geben soll, wie weit sich eine Zelle dimensionieren läßt und wo am sinnvollsten Instanzen der entsprechenden Dienste zu plazieren sind.

Nachfolgend ist in einer Graphik die Verkehrsverteilung innerhalb der beschriebenen Beispielzelle mit etwa 20 Maschinen akkumuliert über einen Zeitraum von 12 Stunden dargestellt.

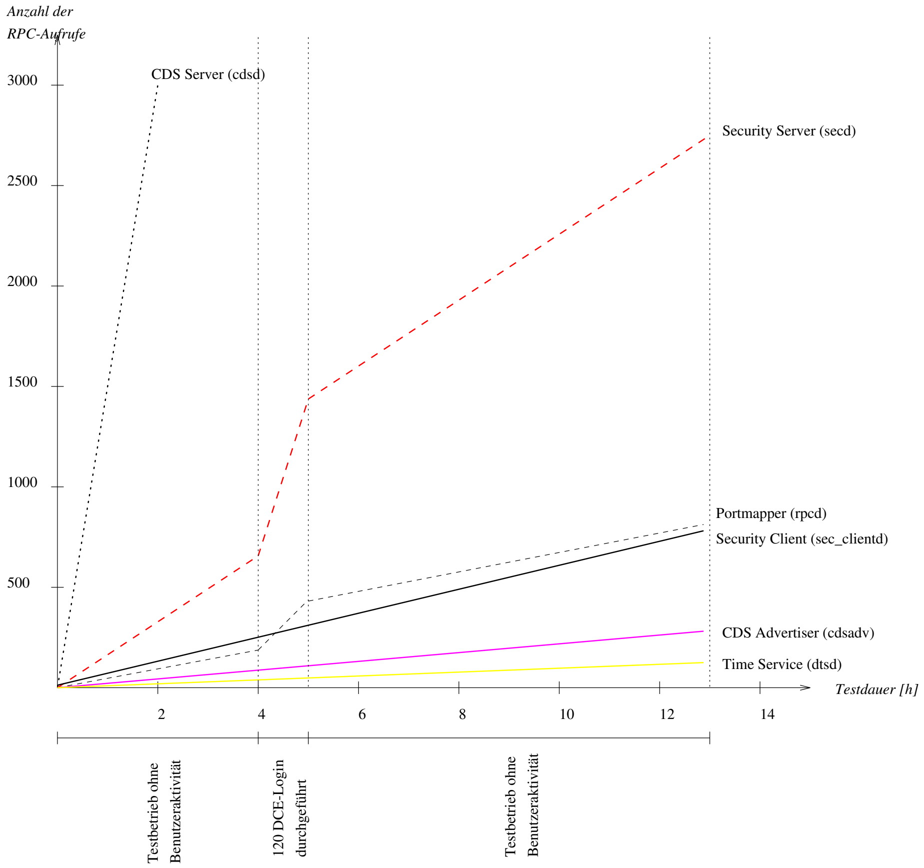


Abbildung 3.3: Hintergrundverkehr in einer DCE-Zelle

Es ist auffällig, daß selbst in Phasen ohne Benutzerbetrieb eine signifikante Hintergrundlast alleine durch die Dienste hervorgerufen wird.
Die Tatsache, daß es sich die Ergebnisse auf eine Zelle bezieht, die lediglich aus etwa 20 Maschinen besteht, läßt den Schluß zu, daß eine Eindämmung des Hintergrundverkehrs bzw. der Verteilung der Hintergrundlast über mehrere Dienstinstanzen beim Entwurf von Zellstrukturen große Bedeutung beizumessen ist. Besonderes Augenmerk muß dabei auf den Verzeichnisdienst gerichtet werden, da dieser selbst in Phasen ohne Benutzeraktivität ein große Anzahl von Requests zu bearbeiten hat.

Im folgenden wird deshalb das Verkehrsverhalten der einzelnen Dienste untersucht, um Anhaltspunkte für die Leistungsfähigkeit unterschiedlicher Zellstrukturen zu gewinnen.

3.11.2.1 Clientkomponenten der DCE-Dienste

Die Gesamtmenge des von den Clientsystemen erzeugten Hintergrundverkehrs steigt linear mit der Zellgröße. Der Verkehr, der dabei von einem einzigen Client erzeugt wird, ist jedoch unabhängig von der Größe der Zelle. Die obengenannte Untersuchung [DCE Perf 93] quantifiziert den Hintergrundverkehr eines Clientsystems mit 0.05 $\frac{RPC-Aufrufe}{sec}$ bzw. 0.6 $\frac{Pakete}{sec}$.

3.11.3 Security Service

Hintergrundverkehr

Hier stellt die Untersuchung einen sublinearen Zusammenhang zwischen der Größe der Zelle und dem Verkehraufkommen fest, wie folgende Tabelle aus [DCE Perf 93] verdeutlicht.

Zellgröße	3 Rechner	21 Rechner	Verhältnis $\frac{1}{7}$
Anzahl der Secucity Server	1	1	$\frac{1}{1}$
einkommende RPC-Aufrufe / sec	0.10	0.26	$\frac{1}{2.6}$
ausgehende RPC-Aufrufe / sec	0.01	0.02	$\frac{1}{2}$

Tabelle 3.2: Hintergrundverkehr des Sicherheitsdienstes

Der Hintergrundverkehr des Sicherheitsdienstes besteht zum einen aus den Paßwortwechseln der einzelnen Server- bzw. Maschinenprincipals, welche nur vom Master-Replikat der Zelle bearbeitet werden können. Diese Paßwortwechsel werden von jedem Rechner periodisch im Abstand von 10 Minuten durchgeführt.
Dazu kommen noch die Authentifizierung, d.h. die Ticketvergabe an Dienste, die sich ihrerseits auf andere Services abstützen. Ein Beispiel hierfür sind die *Clerks* des Time Service, die ihre Server über CDS suchen und somit sowohl ein Ticket für eine Instanz des Verzeichnisdienstes, als auch für den entsprechenden *Time Server* benötigen.
Im Hintergrundverkehr sind also zwei Komponenten vertreten, wobei die erste linear mit der Anzahl der Maschinen in einer Zelle wächst, wohingegen die zweite in erster Linie von der Anzahl der Serverinstanzen in einer Zelle abhängt.

Lookup Verkehr

Die Nutzung des Sicherheitsdienstes durch die Benutzer besteht im wesentlichen aus dem Login und dem Anfordern von Tickets für die verschiedenen DCE-Dienste. Da Tickets eine relativ lange Lebensdauer haben, müssen sie während eines Arbeitstages meist nur einmal angefordert werden.
Eine detaillierte Untersuchung des Login-Verkehr findet sich in [Login Perf 94].

Ein wichtiges Ergebnis einer Untersuchung der University of Michigan [CITI 94-1] ist die Unabhängigkeit des Antwortzeitverhalten des Sicherheitsdienstes von der

Größe der Benutzerdatenbank. Dies wird durch Messungen anhand einer Datenbankgröße von über 50000 Einträgen belegt.

Update Verkehr

Unter den Update-Verkehr ist beim Sicherheitsdienst in erster Linie das Modifizieren der Benutzerdatenbank zu zählen. Diese Änderungen werden zuerst im Adreßraum des Serverprozesses durchgeführt. In Intervallen wird die gesamte Datenbank auf Platte zurückgeschrieben und an die Replikate verteilt. Bei sehr großen Benutzerdatenbanken wird dabei das Antwortzeitverhalten der Master-Instanz allein durch das Rückschreiben auf den Plattenspeicher signifikant beeinträchtigt, wie [CITI 94-1] belegt.

Replikat-Update Verkehr

Das Propagieren von Updates wird angestoßen, sobald die Masterinstanz den Inhalt der Benutzerdatenbank vom virtuellen Speicher auf Plattenspeicher zurückschreibt. Die Frequenz dieser Sicherungsvorgänge (*Checkpoints*) hängt von der Änderungshäufigkeit der Datenbank ab. Die Replikate bleiben trotz möglicher Inkonsistenzen verfügbar.

Selbst bei einer stabilen Benutzerpopulation sind die Änderungen der Maschinenpaßwörter an die Replikate zu verteilen. Somit ist die zu verteilende Datenmenge vor allem von der Anzahl der Maschinen in einer Zelle bestimmt.

3.11.4 Cell Directory Service

Hintergrundverkehr

Zellgröße	3 Rechner	21 Rechner	Verhältnis $\frac{1}{7}$
Anzahl der CDS Server	1	2	$\frac{1}{2}$
einkommende RPC-Aufrufe / sec	0.82	1.67	$\frac{1}{2.04}$
ausgehende RPC-Aufrufe / sec	0.008	0.008	$\frac{1}{1}$

Tabelle 3.3: Verkehrscharakteristik des *Cell Directory Service*

Der Hintergrundverkehr von CDS wird vor allem durch den Hintergrundverkehr der anderen Dienste induziert, die sich auf den Verzeichnisdienst abstützen. Mögliche Engpässe in der Skalierbarkeit werden sich also zuerst beim Verzeichnisdienst abzeichnen.
Darüberhinaus wurde in [DCE Perf 93] festgestellt, daß durch die Masterinstanz wesentlich mehr Verkehr hervorgerufen wurde, als durch die Replikate.
Da die Replikation von CDS jedoch auf Basis von Verzeichnissen beruht, läßt dies den Schluß zu, daß für einen möglichst effizienten Lastausgleich, die von bestimmten Bereichen am stärksten genutzten Verzeichnisse am besten auf einer Serverinstanz in den jeweiligen Teilnetzen plaziert werden sollten. Diese Partitionierung nach topologischen Gesichtspunkten kann einen wesentlichen Beitrag zu einem effizienten

Lastausgleich darstellen.

Lookup Verkehr

Der überwiegende Teil der Interaktion mit CDS besteht aus der Suche nach Bindeinformationen der von einem Client benötigten Server. Diese Aufgabe kann von jedem CDS-Server, der die benötigten Daten als Replikat vorliegen hat, erfüllt werden. Es bietet sich also an, den gesamten Namensraum auf jedem Server zu replizieren, um somit einen möglichst effizienten Lastausgleich zu erreichen. Zudem wird durch das Zwischenspeicherung der Ergebnisse auf der Clientseite erreicht, daß im Laufe einer Sitzung immer seltener auf den Verzeichnisdienst zugegriffen werden muß.
Die Geschwindigkeit mit der ein Eintrag gefunden wird, hängt im wesentlichen davon ab, wie lange der Pfad bis zum Suchergebnis ist. Meßgrößen hierfür sind die Anzahl der kontaktierten *Clearinghouses* und die Tiefe des Eintrags innerhalb des Suchpfades.

Update Verkehr

Updates treten bei CDS dann auf, wenn Server ihre (partiellen) Bindeinformationen beim Verzeichnisdienst registrieren oder löschen. Dies geschieht jedoch nur beim Hinzufügen, Löschen, Starten oder Stoppen von Diensten. Im regulären Betrieb einer Zelle sind also keine Update-Operationen zu erwarten.

Replikat-Update Verkehr

Die Änderungen an Verzeichniseinträgen können entweder unmittelbar, oder in definierten Intervallen an die replizierten Verzeichnisse propagiert werden.
In der Regel ist es ausreichend, diese Updates einmal im Laufe eines Tages durchzuführen. Verlegt man also den Update-Prozeß in eine Phase, in der kein Benutzerbetrieb herrscht, so stellt die Anzahl der Replikate keinen begrenzenden Faktor für die Leistungsfähigkeit einer Zelle dar.

Die Architektur des CDS erlaubt also den weitreichenden Einsatz von Replikation. Zudem ist es möglich, den überwiegenden Teil des Verkehrs gleichmäßig über alle Serverinstanzen zu verteilen. Möglichen Engpässen kann also durch Hinzufügen neuer Replikate begegnet werden.

3.11.5 Time Service

Beim *DTS* keine direkte Interaktion mit den Benutzern statt. Aus diesem Grund wird sämtlicher Verkehr unter dem Bereich Hintergrundverkehr zusammengefaßt.

Hintergrundverkehr

Aufgrund der Architektur des *Distributed Time Service* holen die Clientsysteme im Normalfall – d.h. wenn alle lokalen Server verfügbar sind – die Zeitstempel von Servern innerhalb desselben LANs ein. Das globale Verkehrsaufkommen von *DTS* hängt also nicht direkt von der Zellgröße ab, sondern von der Anzahl der LANs und

Zellgröße	3 Rechner	21 Rechner	Verhältnis $\frac{1}{7}$
Anzahl der Time Server	1	3	$\frac{1}{3}$
einkommende RPC-Aufrufe / sec	0.04	0.13	$\frac{1}{3.3}$
ausgehende RPC-Aufrufe / sec	0.09	0.10	$\frac{1}{1.1}$

Tabelle 3.4: Verkehrscharakteristik des *Distributed Time Service*

somit der Anzahl der globalen Timeserver zwischen welchen die Zeit synchronisiert werden muß.

Generell gilt jedoch festzustellen, daß der durch DTS hervorgerufene Verkehr als unkritisch einzustufen ist.

3.11.6 Distributed File Service

Hintergrundverkehr

Ohne Benutzerbetrieb findet lediglich in äußerst geringem Maße Kommunikation zwischen den einzelnen Instanzen des *Fileset Location*-Dienstes statt.

Lookup Verkehr

Auch im Rahmen von DFS läßt sich Replikation einsetzen, um die beim lesenden und ausführenden Zugriff auf Dateien entstehende Last über verschiedene Server zu verteilen. Dabei ist der Replikationsmechanismus auf Schnappschüsse eines *Filesets*, d.h. einer Gruppe von Dateien beschränkt. Die Verwendung replizierter Filesets ist also nur bei Daten sinnvoll, die auch bei möglichen Inkonsistenzen verfügbar bleiben müssen, und Daten, die nur selten geändert werden.

Das Antwortzeitverhalten bei einem Dateizugriff hängt auch davon ab, wie schnell der entsprechende Fileserver, auf dem einen *Fileset* gespeichert ist, gefunden werden kann. Es ist also besonders wichtig, daß auf eine lokale Instanz des *Fileset Location*-Dienstes zugegriffen werden kann.

Die angeforderten Dateien werden lokal – d.h vom Client – zwischengespeichert. Folgende Zugriffe auf dieselbe Datei erzeugen unter der Voraussetzung, daß in der Zwischenzeit kein anderer Benutzer schreibend auf die Datei zugegriffen hat, keinen weiteren Verkehr.

Update Verkehr

Von zentraler Bedeutung für den konsistenten Betrieb eines verteilten Dateisystems ist, daß Änderungen der Lage von Filesets oder das Hinzufügen bzw. Löschen von Filesets unmittelbar für alle Clients sichtbar werden. Aus diesem Grund müssen Änderungen an der *Fileset Location*-Datenbank (*FLDB*) sofort an alle Replikate weitergeleitet werden.

Unmittelbare Updates begrenzen stets die Anzahl der sinnvoll betreibbaren Replikate.

Modifikationen werden allerdings nur sehr unregelmäßig durchgeführt, außerdem ist die dabei entstehende Datenmenge gering.
Demgegenüber ist die rein lesende Interaktion mit der *FLDB* sehr häufig und damit kritisch für Antwortzeiten bei jedem Dateizugriff. Aus diesem Grund sollte von der Replikation der *Fileset Location*-Datenbank in maßvoller Weise Gebrauch gemacht werden.

3.12 Sonderfälle

Im Gegensatz zu Applikationen, die direkt oberhalb der Betriebssystemschicht angesiedelt sind und für die die Existenz von DCE auf einer Maschine oder innerhalb eines Verbundes vollständig transparent ist, können bei Anwendungen, die auf DCE aufsetzen, starke Abhängigkeiten zu der entsprechenden Zellumgebung bestehen.
Ein Beispiel ist ENCINA, ein System zur Transaktionsverarbeitung, das in nur im Rahmen einer Zelle die volle Funktionalität besitzt.
Solche Ausnahmen können Teile der hier aufgeführten Überlegungen hinfällig machen und einen dominanten Einfluß auf die Zellstruktur ausüben.

Kapitel 4

Das Szenario

Im Rahmen der Fahrzeugentwicklung bei der BMW AG ist geplant, schrittweise eine zentrale CAD-Installation (CATIA) von einem IBM VM-Host in eine Client/Server-Struktur zu überführen.
Dabei sollen im ersten Schritt ressourcenintensive Bereiche vom Host ausgelagert und in eine Struktur von Graphikworkstations und zentralen File-Servern migriert werden.
Ziel ist, im Laufe der nächsten Jahre alle Teile der Fahrzeugentwicklung in Client/Server-Verbunde zu integrieren.

4.1 Infrastruktur

4.1.1 Ausdehnung des Verbundes

Die Abteilungen, die CATIA einsetzen sind weltweit verteilt und arbeiten zum Teil schon in verteilten Umgebungen.
Nach dem Abschluß der Migration werden ca. 600 CAD-Arbeitsplätze in verteilte Verbunde integriert sein.

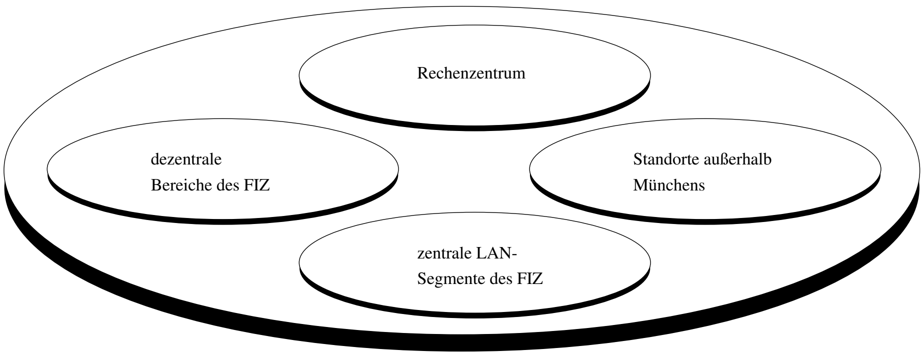


Abbildung 4.1: Standorte des CATIA-Verbundes

4.1.2 Topologie

Die Netzanbindungen der einzelnen Bereiche weisen sehr unterschiedliche Bandbreitenprofile auf. Grundlegend sind aber vier unterschiedliche Standortarten zu unterscheiden.

1. Das Rechenzentrum (*IVZ-2*) :
   Innerhalb eines Host-to-Host FDDI-Ringes sind die zentralen Ressourcen, wie Dateiserver und Ausgabegeräte für das Plotten, sowie ein Backup-Server angeordnet.
2. Die zentralen LAN-Segmente des Forschungs- und Ingenieurzentrums (*FIZ*):
   In den einzelnen Abteilungen sind die Rechner an ein, zum Teil aus mehreren Ethernet-Segmenten bestehendes lokales Netzwerk angeschlossen.
   Diese lokalen Netzwerke umfassen neben den CATIA-Arbeitsplätzen noch weitere Anwenderbereiche, wie etwa einen CAE-Verbund.
   Die lokalen Netze sind über Router an das Münchner Unternehmensbackbone (FDDI) angeschlossen.
3. Die *FIZ*-Außenstellen:
   Die dezentralen Bereiche innerhalb Münchens sind über 2 $\frac{Mbit}{sec}$ Standleitungen mit dem Backbonenetz verbunden. Bis zum vollständigen Abschluß der CATIA-Migration bleibt die zur Verfügung stehende Bandbreite fest zwischen TCP/IP und dem Terminalprotokoll für den Hostzugriff aufgeteilt.
4. Die dezentralen Bereiche (Werke):
   Alle Bereiche außerhalb Münchens arbeiten in einer eigenen Netzinfrastruktur. Sie sind über WAN-Verbindungen (2 $\frac{Mbit}{sec}$) an das Münchner Backbonenetz angeschlossen. Jedoch ist die verfügbare Bandbreite zwischen Sprach- und Datenverkehr aufgeteilt.

4.1.3 Kooperationsmodell

Die gesamte Infrastruktur setzt sich aus einer Reihe von Workgroups auf Abteilungsebene zusammen, denen jeweils zusätzliche, zentrale Ressourcen für die Datenhaltung, die Plotausgabe und das Backup zugeordnet sind.
Die Kooperation zwischen den einzelnen Workgroups findet über den Austausch von Dateien über eben diese zentralen Ressourcen statt. Einigen Workgroups ist darüberhinaus ein Abteilungsserver zugeordnet.

4.1.4 Funktionale Differenzierung der Rechensysteme

Im Rahmen des CATIA-Verbundes existieren drei Arten von Rechnern.

1. Graphikworkstations:
   Sie stellen die Arbeitsplatzrechner der Anwender dar. Sie werden *dataless* betrieben, d.h. auf ihnen werden lediglich das Betriebssystem und Anwenderprogramme installiert, jedoch keine Anwenderdaten gespeichert. Es ist dabei nicht vorgesehen Serverfunktionalität auf diese Rechnern zu verlagern, um eine möglichst identische Konfiguration zwischen allen Arbeitsplätzen zu gewährleisten.

2. Utility Server:
   Diese Rechner übernehmen Serverfunktionalität für einen Anwenderbereich. In erster Linie dienen sie als Applikationsserver und werden von den Anwendern für das Beschreiben externer Datenträger genutzt.
   Die Software-Verteilung für eine Workgroup erfolgt ebenfalls von dieser Stelle aus.
   Es sind jedoch nicht alle Workgroups mit Utility Servern ausgestattet.

3. File Server:
   Die Aufgabe der Dateiserver besteht in der Speicherung der erzeugten CAD-Daten. Diese werden zum Teil in projektspezifischen Verzeichnissen und zum Teil in den privaten Verzeichnissen der Anwender gespeichert.
   Im Fall der zentralen Bereiche des *FIZ* teilen sich mehrere Workgroups einen File Server, in den dezentralen Bereichen steht den Workgroups ein eigener Dateiserver zur Verfügung.

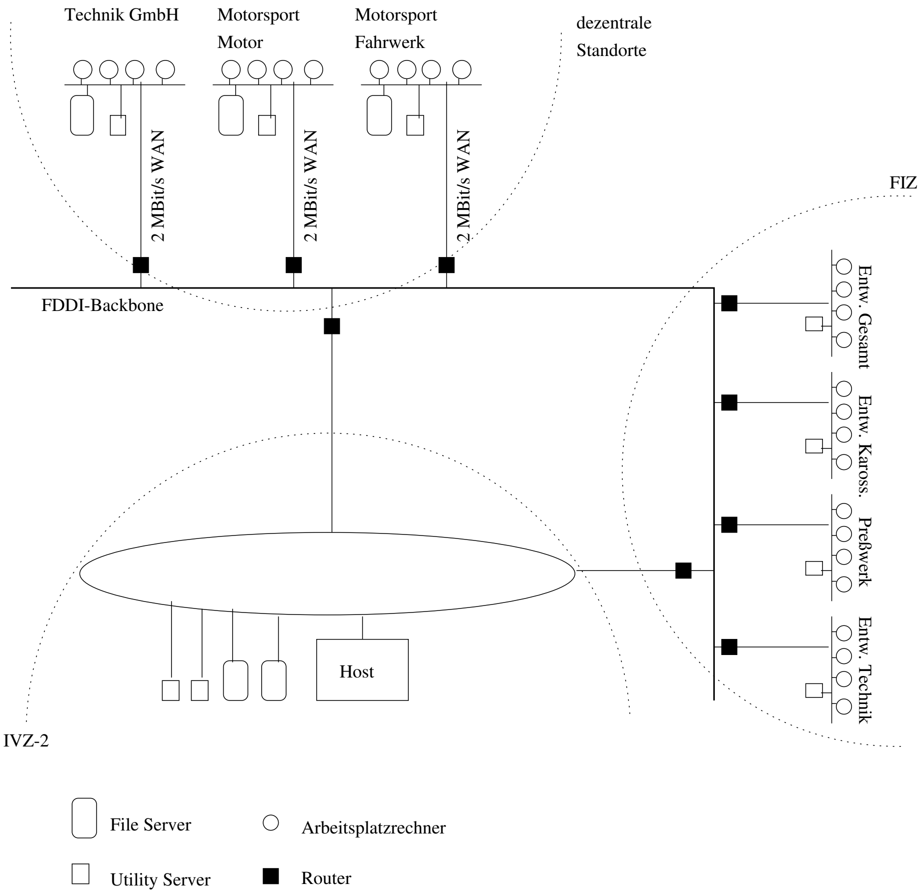


Abbildung 4.2: Aufbau des CATIA-Verbundes

4.2 Organisation

4.2.1 Betreiberorganisation

Für alle Bereiche innerhalb Münchens existiert eine zentrale Betriebsbetreuung. Ihre Aufgabenstruktur ist unterteilt zwischen Rechenzentrumsbetrieb und dem Betrieb der Anwenderbereiche. Darüberhinaus existiert eine Vor-Ort-Betreuung.
Die Standorte außerhalb Münchens arbeiten in einer eigenen Netzinfrastruktur und werden durch eigene Betreiberorganisationen verwaltet.

Im folgenden ist ein exemplarischer Querschnitt über die Aufgabenbereiche aufgeführt.

- zentrale Aufgaben (Rechenzentrum):
  - Serverbetrieb
  - Benutzer- und Gruppenverwaltung
  - Verwaltung der Datenbestände
  - Backup
- dezentrale Aufgaben: (Anwenderbereiche)
  - Installation neuer Hardware
  - Software-Updates
  - Betriebsüberwachung (Systeme, Netzwerk, Leistung, Sicherheit, Verfügbarkeit, Integrität)
  - Störungsmanagement, Help-Desk
- Vor-Ort-Betreuung:
  - Betriebsüberwachung
  - Operating

4.2.2 Unternehmensorganisation

Der diskutierte Bereich umfaßt drei unterschiedliche Organisationseinheiten:

1. Technik GmbH
2. Motorsport GmbH
3. Forschungs- und Ingenieurzentrum (FIZ)

Innerhalb des *FIZ* herrscht einer hoher Grad an Kooperation zwischen den einzelnen Abteilungen. Darüberhinaus findet ein Datenaustausch – allerdings in weit geringerem Umfang – zwischen den einzelnen Standorten statt.

4.2.3 Benutzerorganisation

Der CATIA-Verbund wird ausschließlich von Entwicklungsingenieuren genutzt. Bei allen Überlegungen gilt es zu berücksichtigen, daß eine mobile Benutzerpopulation vorliegt. Die Benutzer müssen also in die Lage versetzt werden, den gesamten Verbund von jedem Arbeitsplatz aus nutzen zu können.

Desweiteren liegt im Bereich des *FIZ* eine überlappende Benutzerpopulation zwischen dem CATIA-Verbund und einem parallel dazu existierenden CAE-Verbund vor.
Die zwischen den beiden Verbunden bestehenden Kooperationsbeziehungen sind in einer längerfristigen Zellstrategie zu berücksichtigen.

4.3 Lösungsansatz NIS und NFS

Im ersten Migrationsschritt werden zunächst *Network Information System (NIS)* und das *Network File System (NFS)* eingesetzt. Dabei wird entweder der gesamte Bereich innerhalb Münchens in einer *NIS*-Domäne zusammengefaßt, oder drei *NIS*-Domänen in Anlehnung an die Organisationseinheiten errichtet.
Der Zugriff auf die privaten bzw. Projektdaten erfolgt via *NFS* auf die File-Server. Der Datentransfer zwischen den einzelnen Standorten wird über das *File Transfer Protocol (FTP)* abgewickelt.

Kapitel 5

Anwendung von Zellstrukturen auf das Szenario

5.1 Monolithische Zelle

Monolithischen Zellen fassen komplette Anwenderbereiche innerhalb einer Zelle zusammen, mit dem Ziel eine möglichst ganzheitliche Sicht auf die Infrastruktur zu ermöglichen.
Diese ganzheitliche Sicht ergibt sich aus dem einheitlichen Namensraum, dem einheitlichen Dateisystem und einer zentralen Benutzerdatenbank.

Besonderes Augenmerk ist bei der Errichtung einer monolithischen Zelle auf die Verteilung der Dienstinstanzen zu richten, da die Größe und Komplexität der Umgebung eine effiziente Lastverteilung erfordert.

Bei einer monolithischen Zellstruktur ist es zudem unumgänglich, über die Festlegung der Zellgrenze hinaus eine Strukturierung vorzunehmen, die eine Anpassung an die infrastrukturellen und organisatorischen Anforderungen erlaubt.

Besonders für den Bereich der Administration müssen Mechanismen entwickelt werden, die eine flexible Delegation von Verwaltungstätigkeiten erlauben, da gerade bei großen Zellen die Managementaufgaben nicht mehr zentral durchführbar sind. Diese Mechanismen müssen sowohl eine bereichs-, als auch eine aufgabenbezogene Dezentralisierung des Systemmanagements gestatten.

Möglichkeiten der Strukturierung ergeben sich vor allem aus dem hierarchischen Aufbau des Namensraums. Eine Domänenbildung innerhalb einer Zelle wird dabei durch Teilbäume der Verzeichnishierarchie beschrieben.
Das zellweite Dateisystem kann darüberhinaus in einzelne administrative Bereiche gegliedert werden.

Eine weitere Voraussetzung für die Umsetzung von Delegation ist die Zuordnung von Rollen zu Objekten innerhalb einer Domäne. Diese Zuordnung geschieht dabei über die Mechanismen der Zugriffskontrolle. Ressourcen, Dienste, Daten und die Elemente der Benutzerdatenbank können über Zugriffskontrollisten einem gewissen Managementbereich zugewiesen werden.

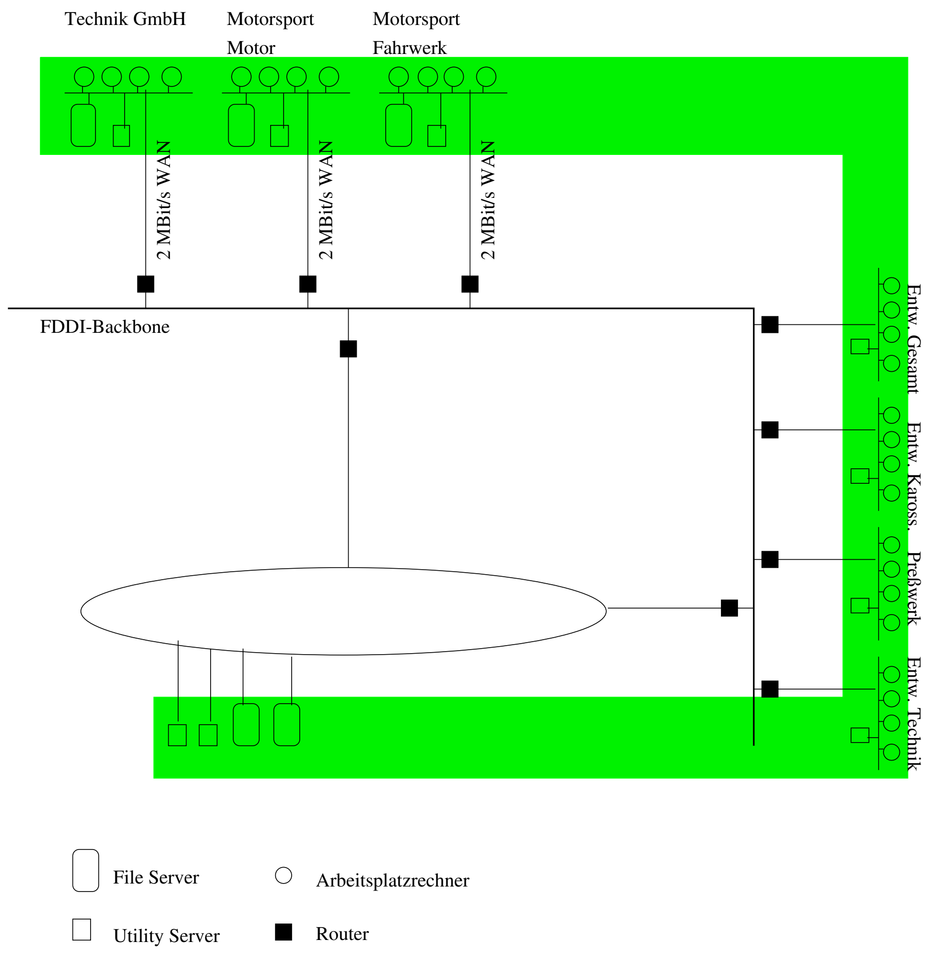


Abbildung 5.1: Monolithische Zelle

Die Rechte zur Verwaltung von Objekten können im Rahmen von Zugriffskontrollisten entweder an einzelne Verwalter, oder an Gruppen von Administratoren vergeben werden.

Mit diesen Mechanismen lassen sich innerhalb einer monolithischen Zelle Domänen und Rollen definieren. Dies schafft die Voraussetzung, über die Methoden der Zugriffskontrolle eine flexible Form der Delegation vorzunehmen.

Der konzeptionelle Hintergrund bei der Wahl einer monolithischen Zellstruktur ist, DCE als ein Dienstpaket zu betrachten, das den einzelnen Anwenderbereichen angeboten werden soll.
Dieser Dienstaspekt von DCE läßt sich nach seinen Ausprägungen aus Betreibersicht noch weiter differenzieren:

1. Es sollen Ressourcen mittels DCE verwaltet werden. Diese Ressourcen können dann von den Anwendern über die Mechanismen von DCE genutzt werden. Die entsprechenden Dienste werden lediglich zentral angeboten.

2. Mit den DCE-Diensten wird eine verteilte Infrastruktur aufgebaut. Diese Dienste können dann auch ganz oder teilweise dezentral zur Verfügung gestellt werden.

3. Über den Einsatz von DCE hinaus kann auch der Betrieb, oder Teilaufgaben des Systemmanagements (z.B. Benutzerverwaltung) von einem zentralen Anbieter übernommen werden.

5.1.1 Infrastruktur

5.1.1.1 Die zentralen LAN-Segmente des *FIZ* und das Rechenzentrum

Ein wesentliches Merkmal der gesamten Infrastruktur im zentralen Bereich des *FIZ* ist, daß keine autonomen Workgroups vorliegen, sondern daß diese Workgroups auf Dienste, wie etwa Datei- oder Plotdienste des Rechenzentrums angewiesen sind. Für die einzelnen Abteilungen besteht also die Notwendigkeit, regelmäßig auf Ressourcen des Rechenzentrums zuzugreifen. Es existieren also eindeutige funktionale Abhängigkeiten zwischen dem Rechenzentrum und den einzelnen Workgroups.
Logisch gesehen stellt das Rechenzentrum eine zentrale Ressource dar, über die die gesamte Kooperation zwischen den unterschiedlichen Bereichen abgewickelt wird; es liegt also im Schnittbereich aller Kooperationsbeziehungen des gesamten Verbundes. Diesen Gegebenheiten wird durch eine monolithische Zellstruktur Rechnung getragen, indem sie durch die Vereinigung der unterschiedlichen Workgroups und des Rechenzentrums eine konsistente Sicht auf die gesamte Infrastruktur ermöglicht.

5.1.1.2 Die dezentralen Bereiche des FIZ

Im Gegensatz zu den zentralen LAN-Segmenten des FIZ, wo wesentliche Teile der benötigten Ressourcen nur über das Rechenzentrum bezogen werden können, haben die dezentralen Standorte eigene File-Server und können somit funktional weitgehend autonom von den zentralen Bereichen operieren.
In administrativer Hinsicht sind sie jedoch an die zentralen Bereiche des *FIZ* gebunden. Um den gesamten Verbund möglichst effizient betreiben zu können, liegt es nahe, auch diese Standorte in der monolithischen Zelle zu vereinigen.
Da die am meisten genutzten Ressourcen dezentral vorhanden sind, bestehen auch in Hinblick auf die geringere Bandbreite keine Einwände gegen dieses Vorgehen, weil lediglich der Hintergrundverkehr über die WAN-Verbindung abgewickelt werden muß.
Ein weiteres Argument für die Integration in eine monolithische Zelle stellt die einheitliche Nutzung des Backup-Mechanismus von DCE für den gesamten Bereich dar, da der Einsatz des Backup-Systems von DFS auf eine Zelle beschränkt ist.

5.1.1.3 Die Standorte außerhalb Münchens

Bei den Standorten außerhalb Münchens ist eine vollständige Autonomie, sowohl in funktionaler, als auch in administrativer Hinsicht gegeben. Dies würde isoliert betrachtet schon für die Errichtung eigener Zellen sprechen; berücksichtigt man darüberhinaus die geringere Bandbreite der Verbindungen, so erscheint es zwingend erforderlich, diese Bereiche in separaten Zellen anzuordnen.

Kooperation zwischen den unterschiedlichen Standorten kann dennoch über Interzell-Kommunikation stattfinden.

Die eigentliche Diskussion einer Zellstruktur wird sich deshalb ausschließlich mit den Bereichen *FIZ* und *FIZ dezentral* beschäftigen.

5.1.2 Verteilung der Dienste

Um das Konfigurationsmanagement möglichst übersichtlich zu gestalten, ist es sinnvoll, die Dienste nach Möglichkeit stets auf einem einzigen Serverrechner anzubieten. Im vorliegenden Fall steht dafür in einigen Workgroups ein *Utility Server* zur Verfügung.

Das zentrale Anbieten aller Dienste auf einem Rechner hat den Vorteil, daß die Dienste, die untereinander kooperieren, wie etwa der *Cell Directory Service* und der *Fileset Location Service* ihre Anfragen nicht über das Netzwerk stellen müssen, sondern die Bearbeitung einer Anfrage innerhalb eines Rechners geschehen kann.

Demgegenüber ist beim Ausfall des entsprechenden Servers keine Dienstinstanz mehr innerhalb desselben Teilnetzes verfügbar. Darüberhinaus wird die Last auf einen Rechner konzentriert, was unter Umständen zu Leistungsengpässen führen kann.

In Workgroups, in denen kein *Utility Server* zur Verfügung steht ist es ratsam, die Replikate der jeweiligen Dienste über mehrere Rechner zu verteilen.

Die Verzeichnisdienste

Wie aus der in Abschnitt 3.11 skizzierten Verkehrscharakteristik hervorgeht, ist an erster Stelle die Verteilung der Last beim Verzeichnisdienst sicherzustellen. Dazu ist es notwendig, Replikate möglichst innerhalb jeder Workgroup zu plazieren.

Die Einrichtung mindestens eines *CDS-Servers* pro Subnetz ist zudem empfehlenswert, damit die *CDS-Clerks* beim Start über Broadcasts automatisch einen Server finden. Falls innerhalb eines Teilnetzes kein CDS-Server vorhanden sein sollte, muß dem Client über ein Kommando eine Serverinstanz zugewiesen werden.

Eine Instanz des Verzeichnisdienstes sollte also auf jedem *Utility Server* installiert werden.

Auch an den dezentralen Standorten sollte mindestens ein Replikat des Verzeichnisdienstes installiert werden.

Zur Kooperation mit anderen Zellen ist es zudem nötig, mindestens einen *Global Directory Agent (GDA)* zur Anbindung an den globalen Namensraum zu installieren. Dieser ist sinnvollerweise auf einem *CDS-Server* des Rechenzentrums zu installieren.

Der Dateidienst

Für die Verteilung des Dateisystems bleibt durch die dedizierte Zuordnung weniger Maschinen zu dieser Funktion nur geringer Gestaltungsfreiraum. Die Funktionalität des Dateidienstes gliedert sich jedoch in zwei unabhängige Teile; eine Komponente für das Lokalisieren von Dateien und und eine Komponente für das Exportieren von Dateien.
Der folgende Abschnitt beschränkt sich hauptsächlich auf die Verteilung der Lokationskomponente. Alle Maschinen, die Daten in das verteilte Dateisystem exportieren sollen, müssen natürlich dementsprechend als *File Exporter* konfiguriert werden.

Bei der Verteilung der Lokationskomponente kann man sich von ähnlichen Überlegungen wie beim Verzeichnisdienst leiten lassen. Auch hier sollte jeweils eine Instanz auf jedem *Utility Server* installiert werden, da bei jedem Zugriff auf eine Datei eine Interaktion zwischen dem *Cache-Manager* und der *Fileset Location Database*

(FLDB) stattfindet.

In Anbetracht der Tatsache, daß im vorliegenden Szenario ausschließlich auf sehr große Dateien zugegriffen wird und somit das Lokalisieren einer Datei gegenüber dem eigentlichen Dateizugriff kaum ins Gewicht fällt, kann in einer Workgroup, in der kein *Utility Server* zur Verfügung steht, von einer Replikation der *Fileset Location Database* abgesehen werden. Stattdessen kann eine Instanz auf einem Server im Rechenzentrum genutzt werden.

Eine Besonderheit bei der Replikatverwaltung der *FLDB* ist das Fehlen eines permanenten Master-Replikats. Welches Replikat Änderungen durchführen kann, wird durch ein Votierungsverfahren unter den Servern bestimmt. Aufgrund dieser Besonderheit gilt es als Nebenbedingung zu beachten, daß nach Möglichkeit stets eine ungerade Anzahl von Fileset Location-Servern konfiguriert wird.

Für Daten, die nur einer seltenen Modifikation unterliegen, wie z.B. Normteilbibliotheken, kann zudem der Replikationsmechanismus von DFS genutzt werden, um häufig benötigte Daten den Benutzern dezentral zur Verfügung zu stellen. Diese Entscheidung hängt jedoch wesentlich vom verfügbaren Plattenplatz in den einzelnen Workgroups ab.

Der Sicherheitsdienst

Beim *Security Service* gilt es zu berücksichtigen, daß die Minimierung des erzeugten Verkehrs und die Maximierung der Sicherheit in unmittelbarer Konkurrenz stehen. Jedem Replikat des Sicherheitsdienstes ist auch eine Kopie der gesamten Benutzerdatenbank des Sicherheitsdienstes einer Zelle zugeordnet, die nur im Rahmen der Mechanismen des UNIX-Dateischutzes gesichert ist.

Ein Einbrecher, dem es gelingt, Superuserrechte auf einem *Security Server* zu erlangen, hat somit Zugriff auf alle geheimen Schlüssel der Zelle. Aufgrund dieser Tatsache ist es erforderlich, sämtliche Rechner, die eine Kopie der Benutzerdatenbank halten, gegen allgemeinen Benutzerzugriff zu sichern. Diese Möglichkeit besteht jedoch nur bei Systemen, die unter Rechenzentrumsbedingungen betrieben werden.

Folglich ist es aus Sicherheitsgründen nicht ratsam, innerhalb der Workgroups *Security Server* zu installieren.
Im Rechenzentrum sollte auf einem Serverrechner das Masterreplikat des Sicherheitsdienstes installiert werden und zusätzlich zur Steigerung des Gesamtdurchsatzes und der Verfügbarkeit noch mindestens ein *Slave Server* eingerichtet werden.

An den dezentralen Standorten sollte ebenfalls ein Replikat des Sicherheitsdienstes plaziert werden, um den Netzverkehr zu minimieren und eine möglichst hohe Verfügbarkeit auch bei Netzstörungen sicherzustellen. Da in diesen Bereichen die File-Server ohnehin unter Rechenzentrumsbedingungen betrieben werden, kann auf ihnen ohne Beeinträchtigung der Sicherheit jeweils ein Replikat des Sicherheitsdienstes installiert werden.

Der Zeitdienst

Beim *Distributed Time Service (DTS)* ist die Konfiguration weitgehend durch die Netzstruktur determiniert.
Um eine möglichst genaue Synchronisation zu erreichen, sollte darauf geachtet werden, daß sich zwischen den *Clerks* und ihren lokalen Servern keine Netzkomponenten befinden, die die Übertragung von Zeitstempeln verzögern könnten.

In [OSF Admin] wird vorgeschlagen, in jedem LAN-Segment 3 Server zu konfigurieren und zwar einen globalen Server (*global server*), einen lokalen Server (*local server*) und einen Vermittlungsserver (*courier server*).
In Anbetracht der Tatsache, daß bei einer großen Anzahl von LAN-Segmenten und der damit verbundenen Menge von globalen Servern, durch deren gegenseitige Koordination relativ viel Verkehr hervorgerufen wird, erscheint es aus meiner Sicht ratsamer, pro Subnetz nur einen globalen Server einzurichten und in jedem LAN-Segment einen *Courier Server* und 2 lokale Server zu betreiben. Die globalen Server sollten dabei nach Möglichkeit mit externen Zeitgebern ausgestattet werden. Dadurch wird eine maximale Genauigkeit ihrer Systemuhren garantiert, und es entfällt darüberhinaus die Notwendigkeit der Synchronisation unter den globalen Servern.

An der Synchronisation der Server innerhalb eines LANs, sind ein globaler Server, der LAN-spezifische Courier Server und alle lokalen Server desselben LANs beteiligt (vgl. Abbildung 5.2). Durch die Verwendung externer Zeitgeber an den globalen Servern wird also sichergestellt, daß von außen keine Ungenauigkeiten in die Errechnung der neuen Systemzeit einfließen können. Server des lokalen Netzes, deren Uhr weit von der tatsächlichen Zeit abweichen, finden aufgrund ihres geringen Toleranzintervalles keinen Einfluß in der neu berechneten Systemzeit.

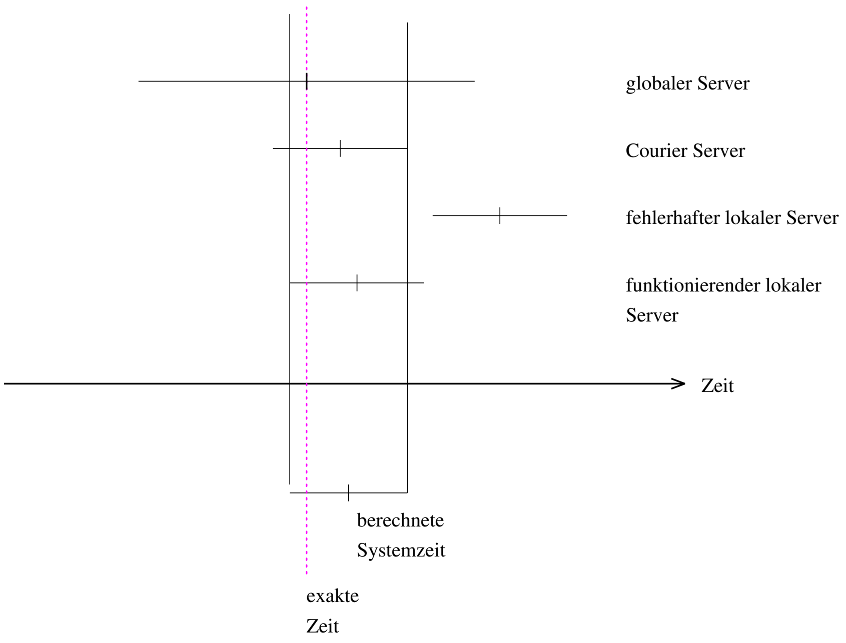


Abbildung 5.2: Berechnung der neuen Systemzeit eines Courier Servers

Die Bedeutung des Zeitdienstes sollte jedoch auf keinen Fall unterschätzt werden, da es die Sicherheitsmechanismen von DCE erfordern, daß die Systemuhren, der in einen Authentifizierungsvorgang involvierten Systeme weniger als 5 Minuten voneinander abweichen. Dies gilt auch, wenn die Systeme unterschiedlichen Zellen zugeordnet sind. Um also eine störungsfreie Kommunikation auch mit anderen Zellen durchführen zu können, sollte jede Zelle mindestens einen externen Zeitgeber besitzen.

5.1.3 Kooperationsaspekte

Charakteristischerweise ist ein Benutzer logisch dem Workgroupsegment zugeordnet, in dem er gerade arbeitet. Die Konfiguration der gesamten Umgebung muß also sicherstellen, daß er stets auf die Serverinstanzen zugreift, die innerhalb desselben Teilnetzes wie sein Arbeitsplatz liegen.
Im Fall der *CDS-Server* ist dies stets gewährleistet, da sich diese über *Broadcasts* bekanntmachen. Anders verhält es sich mit den *Security-* und *Fileset Location*-Servern. Sie müssen durch eine Suche im Namensraum der Zelle gefunden werden. Die entsprechenden Einträge dieser Serverinstanzen sind im Namensraum in *RPC-Gruppen* organisiert. Die Semantik beim Zugriff auf eine Gruppe ist jedoch eine zufällige Auswahl. Es ist also in dieser Konfiguration nicht möglich, eine definierte Zuordnung zwischen Clients und den entsprechenden Serverinstanzen in den einzelnen Workgroups herzustellen.

Im vorliegenden Fall könnte dies dazu führen, daß ein Client aus den zentralen LAN-Segmenten des *FIZ* einen Security-Server der Motorsport GmbH kontaktiert. Die Bearbeitungszeit eines Auftrages würde durch die hohen Transportzeiten über das WAN stark ansteigen.

Die Zellkonfiguration muß also sicherstellen, daß – falls vorhanden – stets ein Server innerhalb desselben Teilnetzes genutzt wird. Dies kann dadurch erreicht werden, daß man den entsprechenden Servereintrag des lokalen Servers im Suchpfad des Verzeichnisdienstes vor dem Gruppeneintrag mit allen Serverinstanzen der Zelle plaziert. Somit wird jeder Client und Benutzer zuerst den lokalen Server nutzen, und nur falls dieser nicht erreichbar ist, eine andere Serverinstanz kontaktieren. Der Suchpfad besteht aus einer Verkettung von sog. *RPC-Profiles* (vgl. Abschnitt A.5). Für gewöhnlich existieren in einer Zelle LAN-spezifische und zellspezifische *Profiles*. Zwischen diesen läßt sich für jede Abteilung bzw. jeden LAN-Verbund ein weiteres *Profile* einfügen, in dem die lokalen Serverinstanzen registriert werden (siehe Abbildung 5.3).

5.1.4 Administration

5.1.4.1 Delegation von Verwaltungstätigkeiten

Die Delegation von Zuständigkeiten ist im Rahmen einer monolithischen Zelle über eine Substrukturierung des Namensraumes zu erreichen. Dabei sind vor allem zwei Teilbäume der Verzeichnishierarchie von Interesse:

1. Das Verzeichnis `/.:/hosts`, in dem pro Maschine ein Verzeichnis mit Einträgen für die Bindeinformationen des *Portmappers*, des *CDS-Clerks* und eventuell eines *CDS-Servers* existieren. Darüberhinaus ist in diesem Verzeichnis auch der Einstiegspunkt für Suchoperationen dieser Prozesse auf dem Namensraum der Zelle angelegt.

2. Das Verzeichnis `/.:/sec/principal/hosts`, in dem die Maschinenprincipals registriert sind.

Über die Substrukturierung dieser Verzeichnisse durch das Einfügen einer weiteren Verzeichnisebene kann das Management der Rechner, sowie die Installation neuer Rechner nach den geltenden Namensraumkonventionen (ein Rechner heißt dann als *Principal* nicht mehr `hosts/`*hostname*, sondern z.B. `hosts/`*Bereich_i/hostname*) an bereichsbezogene Administratoren abgegeben werden.

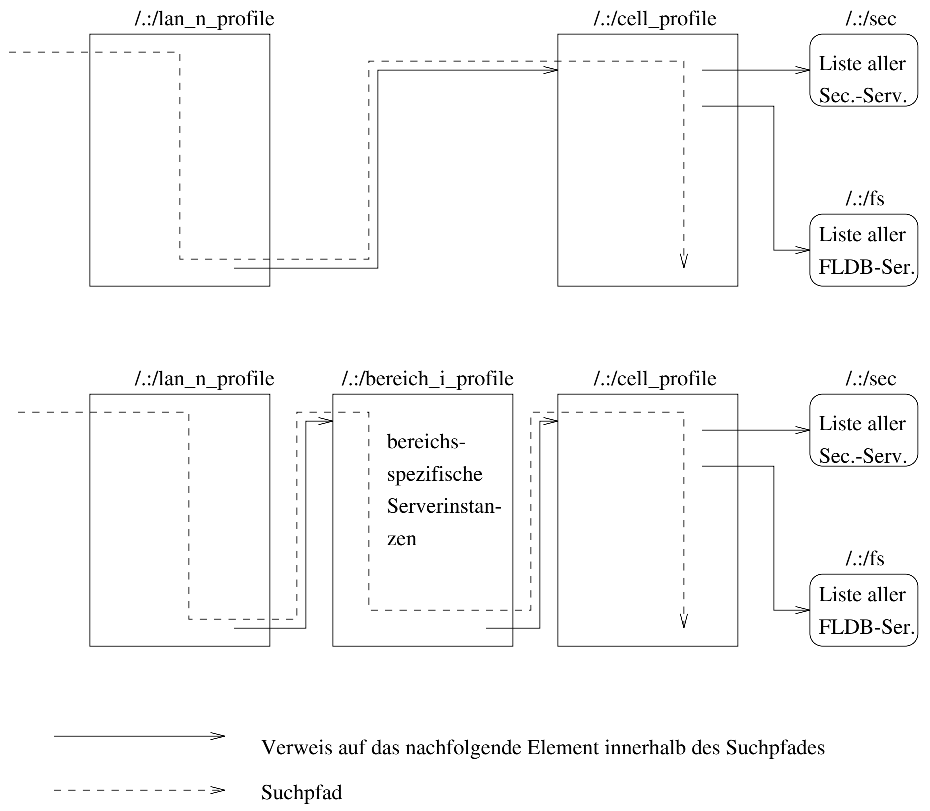


Abbildung 5.3: Erweiterung des Suchpfades

In diesen beiden Verzeichnissen läßt sich nun entweder nach organisatorischer Struktur, oder nach Lokationstyp eine weitere Hierarchieebene einfügen.

Es empfiehlt sich, bei dieser Strukturierung die Verteilung der CDS-Server zu berücksichtigen. In diesem Fall lassen sich die Master-Replikate der bereichsspezifischen Verzeichnisse auf den Servern innerhalb der einzelnen Netzbereiche ablegen. Durch diese Maßnahme kann der Update-Verkehr des *Cell Directory Service* weitgehend lokal gehalten werden.

Um Delegation sinnvoll realisieren zu können, müssen auch entsprechende Verwalterobjekte erzeugt werden, denen dann bestimmte Rollen zugeordnet werden können.
Rollen lassen sich im Rahmen von DCE am effektivsten über Gruppen realisieren. Hierbei existieren wiederum zwei denkbare Alternativen:

1. Man erzeugt eine Gruppe (z.B.: `bereich_i_adm`), in die man dann die bereichsspezifischen Verwalter einträgt.
2. Man setzt die Substrukturierung auch im Namensraum der Gruppenverwaltung fort (z.B.: `/.:/sec/group/`*Bereich_i*) und definiert dort Administratorgruppen für bestimmte Tätigkeiten.
   Diese Lösung bietet darüberhinaus die Möglichkeit der Definition von lokalen Benutzergruppen auf Workgroupebene, etwa um den Zugriff auf private Ressourcen einer Workgroup feinkörniger und ohne Einschaltung einer zentralen Betreuungsinstanz zu regeln.

In die entsprechende Gruppen werden dann die Verwalter eingetragen, und der Gruppe unterhalb ihrer Bereichsverzeichnisse im Namensraum über Zugriffskontrollisten volle Administrationsrechte garantiert.

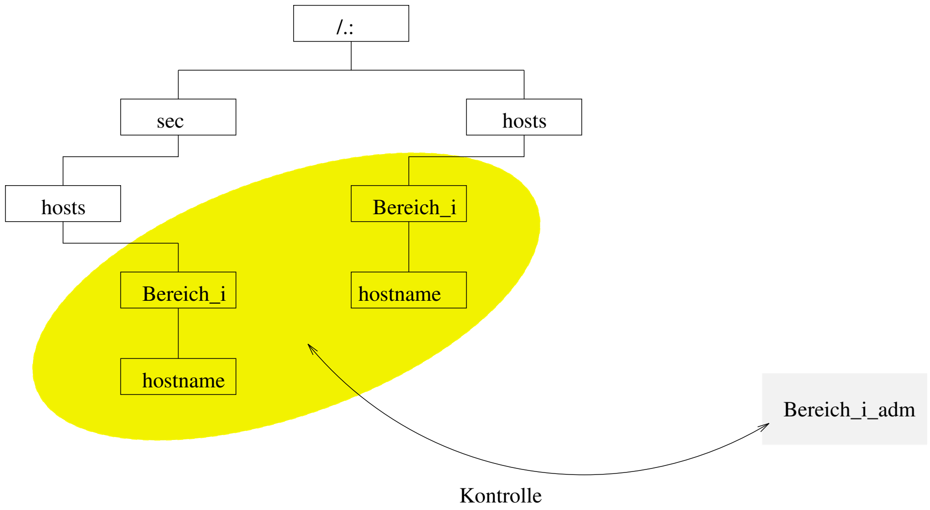


Abbildung 5.4: Delegation über die Strukturierung des Namensraumes

Eine äquivalente Struktur wie bei Rechnern und Gruppen ließe sich auch auf den Bereich der interaktiven Benutzer übertragen (`/.:/sec/principal/`*Bereich_i*). Der Vorteil der strukturierten Darstellung würde jedoch verloren gehen, sobald ein Benutzer zwischen zwei Abteilungen wechselt, da er in diesem Fall gelöscht und wieder neu aufgesetzt werden müßte, um die neuen Verhältnisse entsprechend zu reflektieren. Ein bloßes Verschieben eines Benutzers zwischen zwei Verzeichnissen ist dabei nicht möglich.

Desweiteren müssen Informationen aus der Benutzerdatenbank in die Paßwortdateien der einzelnen Rechner exportiert werden. Viele UNIX-Applikationen benötigen diese Informationen, um eine Zuordnung von numerischen Benutzeridentifikatoren zu Benutzernamen durchführen zu können. Eine Abbildung hierarchischer Principalnamen in flache UNIX-Benutzernamen ist innerhalb des entsprechenden Werkzeugs von DCE nicht vorgesehen.

Will man trotzdem auch im Bereich der Benutzerverwaltung eine Form von Delegation implementieren, so muß man dies über die Zugriffsrechte der einzelnen Principal-, Gruppen- und Organisationsobjekte realisieren.

Dabei ist es möglich, In diesem Fall werden alle Benutzer in einem Verzeichnis registriert, die Kontrolle über die entsprechenden Objekte jedoch streng zwischen verschiedenen Verwaltungsbereichen getrennt.

Eine detaillierte Darstellung der benötigten Rechte für Modifikationen an der Benutzerdatenbank findet man in [OSF Admin].

Eine weitere Strukturierungsmöglichkeit existiert im Bereich des Dateisystems. Hierbei können beliebige Teilmengen von File-Servern einer Zelle zu administrativen Einheiten (sog. *administrative domains*) zusammengefaßt werden.
Jeder der so definierten Domänen ist eine Liste der *Principals* zugeordnet, die Verwaltungsoperationen auf dem Dateisystem im Kontext des beschriebenen Bereiches durchführen dürfen.

Mit dieser Funktionalität ist es möglich, sehr abgestufte Verwalterrechte für das Dateisystem zu vergeben, da innerhalb jeder *Administrative Domain* für jeden Aufgabenbereich eine eigene administrative Liste existiert:

- Eine Liste für die Manipulation der *Fileset Location Database*
- Eine Liste für die Verwaltung der Datenbestände einer Domäne.

  Durch einen Eintrag in beiden Listen hat ein Administrator das Recht, auf den File-Servern der entsprechenden Domäne *Filesets* zu manipulieren und in das zellweite Dateisystem zu exportieren.
- Eine Liste für die Servermaschinen einer Domäne, die Updates von einer *System Control-* bzw. *Binary Distribution*-Maschine erhalten.
- Eine Liste für die Kontrolle der Serverprozesse auf einem Fileserver.

  Ein für die Betriebsüberwachung zuständiger Administrator kann kann z.B. abgestürzte Serverprozesse neu starten, ohne das Recht zu besitzen, die Datenbestände der Maschine zu manipulieren.
- Eine Liste für die Kontrolle der Backup-Datenbank

Auf diese Weise ist es möglich, den einzelnen Bereichen eine kontrollierte Autonomie über ihre lokalen Dateiserver zuzubilligen.
Dazu muß eine entsprechende Gruppe für das Rollenobjekt erzeugt werden, für die zu verwaltenden Server eine eigene *administrative domain* definiert werden und durch geeignete Konfiguration der *administrative lists* die Zugriffskontrolle implementiert werden.

Im Gegensatz zu Zellen können administrative Domänen in DFS auch überlappend definiert werden. So ist es möglich, alle Dateiserver einer Zelle in einer globalen Domäne zusammenzufassen und zusätzlich bereichsbezogene Domänen zu definieren. Damit kann die Administration der Datenbestände sowohl zentral, als auch dezentral durchzuführt werden.und die Verwalterrechte sehr abgestuft zu vergeben. Durch eine abgestufte Vergabe von Verwalterrechten kann z.B. einer zentralen Betriebsüberwachung das Recht zur Kontrolle der Dienstprozesse auf allen Rechnern übertragen und gleichzeitg die Datenverwaltung auf den dezentralen Servern an eine dezentrale Verwaltungsinstanz delegiert werden.

Die Definition einer zentralen administrativen Domäne ist jedoch stets zu empfehlen, damit die notwendige Verteilung von Konfigurationsdateien und *Systembinaries* von zentraler Stelle aus durchgeführt werden kann.

5.1.4.2 Benutzerverwaltung

Aus administrativen Gründen ist es unbedingt ratsam, Zugriffsschutz über Gruppen zu organisieren, da Modifikationen nur an einer Stelle – nämlich der Zugehörigkeit zur Gruppe – und nicht an vielen Stellen – d.h. den jeweiligen *ACLs* – durchgeführt werden müssen.
Bei der Zuordnung von *Principals* zu Gruppen fordert DCE, daß alle Mitglieder einer Gruppe auch innerhalb derselben Zelle registriert sind wie die Gruppe selbst. Diese Forderung ist innerhalb einer monolithischen Zelle stets erfüllt. Somit kann die Benutzerverwaltung und die Verwaltung der Zugriffsrechte sehr effizient durchgeführt werden.

Im vorliegenden Fall besteht also die Möglichkeit, alle Benutzer in eine globale CATIA-Projektgruppe aufzunehmen, um damit den Zugriffsschutz auf systemweite Projektdaten sicherzustellen. Darüberhinaus ist es auch möglich, sehr feinkörnig Gruppen zu definieren, um etwa gewisse Bereiche zu sichern, die ausschließlich von den einzelnen Workgroups genutzt werden sollen.
Der gesamte Benutzerbestand läßt sich mit diesen Methoden sehr flexibel strukturieren.

Auch die Dynamik von Projektgruppen ist im Rahmen einer zentralen Benutzerverwaltung sehr gut beherrschbar.

5.1.4.3 Verwaltung der Datenbestände

Eine der wichtigsten Managementaufgaben im Rahmen eines Dateisystem ist das Replizieren und Verlagern von Datenbeständen zwischen verschiedenen Filesystemen, einerseits aus Performancegründen und andererseits, um Überläufe eines Dateisystems zu verhindern.
Die Architektur von DFS gibt jedoch hierbei einige Einschränkungen vor:

- Die Replikatbildung ist nur innerhalb einer Zelle möglich
- Filesets lassen sich nur innerhalb einer Zelle verschieben
- Das DCE-eigene Backupsystem arbeitet nur im Kontext der lokalen Zelle

Um also die volle Funktionalität des *Distributed File System* nutzen zu können ist es erforderlich, alle Fileserver in einer Zelle zusammenzufassen.
In Anbetracht der Tatsache, daß ein Backup-Dienst zentral angeboten werden soll, ist es absolut zu empfehlen, auch die dezentralen Bereiche mit in die zentrale Zelle aufzunehmen.
Ein weiterer Punkt in diesem Zusammenhang ist die Verwaltung der privaten Daten der Benutzer und der zentralen Projektdaten.
Für die privaten Daten eines Benutzers sollte ihm ein privater *Fileset* zugeteilt werden. Dies erlaubt es, den Plattenplatz, den ein Benutzer maximal belegen darf, über eine *Quota* zu kontingentieren.

Um Überläufe von Dateisysteme zu verhindern, kann der projektspezifische Unterbaum des Dateisystems in mehrere *Filesets* gegliedert werden. Ja nach Entwicklung der Plattenplatzsituation ist ohne Unterbrechung des Benutzerbetriebes das Verschieben von *Filesets* auf Platten mit ausreichender Kapazität möglich.

5.1.5 Sicherheit

5.1.5.1 Sicherheit auf Verbundebene

Mit dem Betrieb des DCE-Sicherheitsdienstes ausschließlich unter Rechenzentrumsbedingungen ist ein Maximum an Sicherheit gewährleistet. Dennoch gilt es zu bedenken, daß alle Benutzeraccounts an die lokalen Paßwortdateien exportiert werden. Somit ist ein Zugriff auf alle verschlüsselten Benutzerpaßwörter möglich. Es ist also unter allen Umständen administrativ sicherzustellen, daß die Paßwörter so gewählt werden, daß ein Angriff mit den gängigen Werkzeugen scheitert. Zu diesem Zweck gibt es im Rahmen des Sicherheitsdienstes eine *Policy*, mit der man die

Verwendung mindestens eines nicht-alphanumerischen Zeichens in einem Paßwort erzwingen kann.

Diese *Policies* lassen sich darüberhinaus für die Definition unterschiedlicher Sicherheitsanforderungen für unterschiedliche Gruppen von Benutzern verwenden.

Es ist offensichtlich, daß der Aufwand zur Behebung von Schäden, die durch einen Einbruch in das Sicherheitssystem einer Zelle entstehen umso größer ist, je größer die Ausdehnung einer Zelle ist.

5.1.5.2 Sicherheit auf Kommunikationsebene

Ein Netzzugang, der auch für den Informationsaustausch zwischen zwei Teilen einer Zelle genutzt wird, kann durch einen Firewall nicht im vollen Umfang gesichert werden.
Als zentrales Problem stellt sich dabei heraus, daß die Kommunikation zwischen Klienten und Servern im Rahmen von DCE nicht über a priori bekannte Kanäle *(well known ports)* stattfindet. Ein Firewall wird jedoch in der Regel so konfiguriert, daß er nur Pakete von bestimmten Quelladressen auf bestimmten Ports passieren läßt. Bei diesem Verfahren ist es nicht möglich DCE-Dienste jenseits des Firewalls zu nutzen.

Ist es unumgänglich mehrere Teile einer Zelle durch *Firewalls* zu trennen, so muß ein umgekehrtes Konfigurationsverfahren gewählt werden. In diesem Fall können lediglich Verbindungen zu Teilnetzen, oder Netzdiensten, die als kritisch identifiziert wurden unterbunden werden. Für Verbindungen zu den entfernten Teile der Zelle dürfen jedoch lediglich besonders kritische Dienste (z.B. telnet) unterbunden werden, um die Kommunikation im Rahmen von DCE nicht zu beeinträchtigen. Dieses Verfahren bietet jedoch nicht dasselbe Maß an Sicherheit, wie das oben skizzierte.

Gerade das in letzter Zeit häufig thematisierte *address spoofing*, d.h. die Vorspiegelung eines falschen Ursprungs eines Paketes durch die Modifikation des Quelladreßfeldes, stellt beim zweiten Ansatz eine große Bedrohung dar, da sich bei einer zentralen Zelle mit einer Ausdehnung über einen *Firewall* hinaus, jenseits des *Firewalls* sowohl freundliche als auch feindliche Teilnetze existieren.
Die Errichtung einer Zelle über *Firewalls* hinaus ist also nach Möglichkeit zu vermeiden.

5.1.6 Verfügbarkeit

In einer verteilten Umgebung zählt Verfügbarkeit – und damit verbunden Fehlertoleranz – zu den Dienstgüteparametern mit der höchsten Priorität.
Die monolithische Zellstruktur trägt dem Rechnung, indem durch die Replikation aller Basisdienste in Bezug auf DCE alle isolierten Fehlerquellen (*single point of failure*) ausgeschaltet werden.
Im Kontext der Verfügbarkeit ist von entscheidender Bedeutung, welche Bereiche beim Ausfall eines Dienstes in Mitleidenschaft gezogen werden. Diesbezüglich läßt sich nach dem Gewicht der Störung noch eine feinere Unterteilung vornehmen:

- Arbeitsplatzrechner:
  hier hat ein Ausfall nur lokale Auswirkungen, andere Benutzer werden von dem Ausfall nicht beeinflußt.

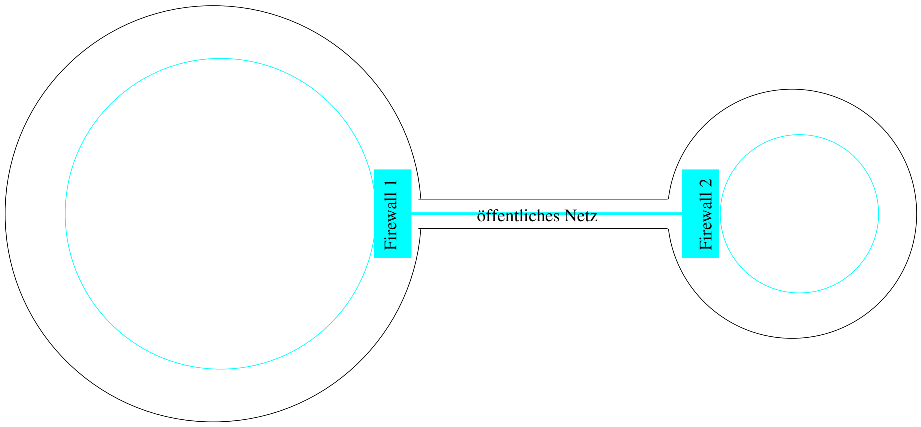


Abbildung 5.5: Problematik bei unterschiedlichen Sicherheitsdomänen aus Sicht von DCE und des Firewalls

- Workgroup-Server:
  ein Ausfall dieses Rechners hat Einfluß auf die Dienstgüte der Bearbeitung innerhalb der Workgroup.
  Falls die Clients aufgrund eines Fehlers eine Serverinstanz nicht erreichen, so wählen sie innerhalb des Bindevorgangs einen anderen Server. Der Ausfall des bevorzugten Servers führt jedoch zu einem schlechteren Antwortzeitverhalten.

- File-Server:
  Sie sind die kritischen Komponenten des Verbundes, ihre Verfügbarkeit ist also unter allen Umständen zu gewährleisten. Die Verfügbarkeit im Rahmen von DFS sorgt dabei ein spezieller Überwachungsmechanismus, der im Fehlerfall die Dienstprozesse von DFS neu startet. Zusammen mit der Replikation der Basisdienste wird also von Applikationsseite – unter Voraussetzung der Hardwareverfügbarkeit – eine maximale Verfügbarkeit garantiert.
  Besondere Maßnahmen sind allerdings für die beiden File Server im Rechenzentrum des *FIZ* zu treffen, da sie nicht nur als Last-, sondern auch als Verfügbarkeitsverbund betrieben werden sollen. Physikalisch läßt sich dies durch die Zuordnung eines einzigen Plattenpools zu beiden Rechnern bewerkstelligen.
  Im Rahmen von DFS sind aber spezielle Konfigurationsmaßnahmen erforderlich, um einen möglichst fehlertransparenten Betrieb zu gewährleisten. Dabei ist ein Mechanismus umzusetzen, der den Betrieb des gesamten Plattenspeichers möglichst unterbrechungsfrei durch den noch verfügbaren Fileserver zu ermöglicht.
  Zu diesem Zweck werden in der hier vorgeschlagenen Lösung alle Platten in die Konfigurationen beider Rechner eingetragen. Jeder Rechner exportiert im Normalzustand nur die ihm zugewiesenen Partitionen.
  Fällt ein Server aus, so exportiert der andere zusätzlich die Partitionen des ausgefallenen Rechners und synchronisiert seinen neuen Zustand mit der *Fileset Location Database*.

  Aus Sicht der Clients entspricht dies einem Verschieben von *Filesets* im laufenden Betrieb. Sie müssen lediglich ihren Token-Status rekonstruieren. Eventuell auf Dateien bestehende Sperren *(locks)* gehen bei diesem Verfahren jedoch verloren.
  Vor dem Wiederanlauf des ausgefallenen Systems muß die ursprüngliche Kon-

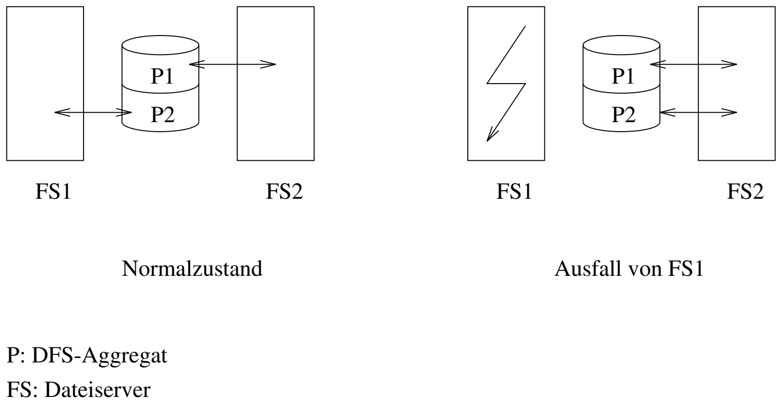


Abbildung 5.6: Verfügbarkeitsverbund von zwei File-Servern

figuration wiederhergestellt werden.

- Netzstörung:
  Durch Replikation der Basisdienste in den einzelnen LAN-Segmenten bzw. den dezentralen Bereichen wirken sich kurzfristige Netzstörungen in den Transitnetzen nicht auf die Verfügbarkeit aus. Ein Zugriff auf zentrale Ressourcen ist zwar nicht möglich, da jedoch Dateien lokal zwischengespeichert werden, kann auf diesen lokalen Kopien weitergearbeitet werden.
  Problematisch wirken sich Netzstörungen zwischen einem Arbeitsplatzrechner und einem Dateiserver aus, wenn sie während des Speichervorgangs auftreten. In diesem Fall bricht der *Cache Manager* den Speichervorgang nach 3 Minuten ab und verwirft auch sämtliche Änderungen an der entsprechenden Datei in seinem Cache. Sollen die geänderten Daten nicht verloren gehen, so müssen sie innerhalb dieser Zeit lokal, d.h. auf der Systemplatte, zwischengespeichert werden.
  Desweiteren gilt es zu berücksichtigen, daß während der Störung in den einzelnen LAN-Segmenten keine Instanz des Sicherheitsdienstes verfügbar ist. Bei einer Störung im Bereich von einigen Stunden ist es möglich, daß durch den Ablauf von Berechtigungen (*Tickets*) die Betriebsstabilität in den betroffenen Segmenten gefährdet wird. In diesem Fall ist es erforderlich nach Behebung der Störung die Dienstprozesse neu zu starten.

5.1.7 Migration

Die zentrale Zellstruktur eröffnet die Möglichkeit, eine DCE-Infrastruktur schrittweise aufzubauen. Der wesentliche Vorteil dieses Vorgehens liegt darin, daß zuerst lediglich der Zeit-, Sicherheits- und Verzeichnisdienst errichtet werden muß.

In der Folge lassen sich Anwenderbereiche und Benutzer in die Zelle integrieren. Nach vollständiger Überführung des gesamten Verbundes kann dann damit begonnen werden, die Datenbestände nach DFS zu migrieren.

Es besteht also die Möglichkeit bis zum Abschluß der Migration parallel die alten Verwaltungsstrukturen weiter zu betreiben. Damit ist eine größtmögliche Stabilität beim Aufbau der DCE-Infrastruktur gewährleistet.

5.1.8 Transparenz

Im Rahmen einer monolithischen Zelle werden sämtliche Anforderungen an die Transparenz am vollständigsten umgesetzt. Für einen Benutzer ist es nicht einmal notwendig den Zellnamen zu kennen, da er stets in einem lokalen Kontext arbeitet. Lediglich durch die Präferenzen beim Zugriff auf gewisse Serverinstanzen wird das Transparenzprinzip durchbrochen. Dies bedeutet, daß sobald ein Benutzer von einem Arbeitsplatz außerhalb seiner Workgroup auf die Dienste der Zelle zugreift, nicht die nächstgelegene Serverinstanz erreicht wird, sondern jene innerhalb seiner eigentlichen Workgroup.
Um auch in dieser Hinsicht völlige Transparenz zu schaffen, kann das passende Bereichsprofil in der Login-Umgebung entsprechend dem aktuellen Arbeitsplatz gesetzt werden.

5.1.9 Änderungsflexibilität

5.1.9.1 Reaktion auf organisatorische Veränderungen

Die Struktur der Zelle ist vorrangig an die topologischen Verhältnisse angepaßt. Abhängigkeiten zu den Organisationseinheiten bestehen so gut wie nicht. Aus diesem Grund sind Änderungen in diesem Bereich aus Sicht der Zelle vollständig transparent.

5.1.9.2 Reaktion auf Konfigurationsänderungen

Im Laufe der Lebensdauer einer verteilten Umgebung werden alle Komponenten einer gewissen Veränderung unterworfen. Es werden neue Maschinen hinzugefügt, Dienste zwischen Rechnern verlagert, Maschinen an anderen Orten aufgestellt und Systemparameter, wie etwa IP-Adressen geändert.

Eine prinzipielle Unterscheidung muß dabei zwischen Clientrechnern und Serverrechnern getroffen werden, da die Konfiguration eines Clients mit sehr geringem Aufwand wiederhergestellt werden kann. Deshalb empfiehlt es sich bei Konfigurationsänderungen an Clients die Systeme einfach neu zu konfigurieren.
Außerdem ist bei Clientrechnern eine Betriebsunterbrechung hinzunehmen, wohingegen dies bei Servern Auswirkungen auf die Verfügbarkeit, oder zumindest auf die Dienstgüte in Teilen des gesamten Verbundes hätte.
Bei Veränderungen an Serverrechnern ist darüberhinaus ein wesentlich größerer Aufwand nötig, da teilweise Informationen über die Lage des Servers in Caches und lokalen Dateien gespeichert werden. Um einen Dienst zwischen zwei Rechnern zu verlagern, oder die IP-Adresse eines Servers zu ändern, muß also nicht nur der Server zeitweilig außer Betrieb genommen werden, es müssen auch die Kontextinformationen auf seinen Clients gegebenenfalls gelöscht oder modifiziert werden.
Eine detaillierte Darstellung dieser Thematik für CDS und den Sicherheitsdienst kann in [OSF Admin] bzw. [Transarc 94] studiert werden.

Sollen Datenbestände zwischen zwei Rechnern verlagert werden, so kann dies innerhalb einer Zelle über das Verschieben von Filesets geschehen. Auch Plattensysteme lassen sich zwischen zwei Rechnern verschieben. Dazu ist es allerdings erforderlich auch die entsprechenden Informationen der *Fileset Location Database* angepaßt werden.

Im Gegensatz dazu gibt es für die Änderung der IP-Adresse eines File Servers ein spezielles Kommando. Es ist zudem möglich, der Identität eines File Servers bis zu vier unterschiedliche IP-Adressen zuzuordnen. Damit ist es möglich mit einem einzigen *File Server Principal* auch sogenannte *Multi Homed Server* zu betreiben.

5.1.9.3 Einbeziehung anderer Verbunde zu einer integrierten Infrastruktur

Parallel zu dem diskutierten CATIA-Verbund existieren innerhalb derselben geographischen und organisatorischen Bereiche noch weitere Workstationverbunde. Um eine Zusammenarbeit mit anderen Verbunden betreiben zu können, und um die Dienstleistungen des Rechenzentrums auch einem erweiterten Kreis von Benutzern zu erschließen, ist es von großer Bedeutung, diese Bereiche möglichst gut in die existierende Infrastruktur einzubetten.

Als Kernproblem stellt sich dabei die durch die Maschinen und Dienste hervorgerufene Hintergrundlast innerhalb der Zelle heraus.
Bei einer Erweiterung einer monolithischen Zelle können sich unter Umständen Leistungsengpässe abzeichnen.

Deshalb erscheint es unvermeidlich für weitere Verbunde, obwohl sie sich innerhalb derselben Netzstruktur befinden, eine eigene Zellstruktur aufzubauen.
Doch nicht nur die unerwünschte zellbezogene Trennung von Rechnern innerhalb derselben Netze tritt dabei als Problem zutage, auch das Rechenzentrum zerfällt bei diesem Vorgehen in mehrere Zellen. Es ist also nicht möglich, alle Dienste für die Anwenderbereiche zentral anzubieten und zu verwalten. Dies hat zur Folge, daß eine einheitliche Sicht auf die gesamte Infrastruktur mit der monolithischen Zellstruktur technisch nicht realisierbar ist.

Durch die limitierte Erweiterungsfähigkeit einer zentralen Zellstruktur kann es beim Umstieg zu einem unternehmensweiten Einsatz von DCE zu den angesprochenen konzeptionellen Konflikten kommen. Gerade in Hinblick auf eine immer stärker werdende Kooperation zwischen unterschiedlichen Bereichen kommt der DCE-Infrastruktur eine ähnliche Bedeutung wie der Netzinfrastruktur zu. Sie muß sowohl benutzer-, als auch betreibergerecht sein und Raum für flexible Erweiterungen lassen.

5.1.10 Skalierbarkeit

Über die Grenzen der Skalierbarkeit einer Zelle ist es nahezu unmöglich Aussagen zu treffen. Wie viele Maschinen, gleichzeitige Benutzer, etc. eine Zelle unterstützen kann und wann der durch Replikation und Hintergrundverkehr entstehende *Overhead* einen Leistungsabfall bewirkt, kann nicht beantwortet werden. Im allgemeinen wird jedoch davon ausgegangen, daß Zellgrößen von über 1000 Benutzern durchaus realistisch sind. Ob sich dies jedoch linear auf die Maschinenskalierbarkeit ausweiten läßt, muß bezweifelt werden. Eine Installation, die dies belegen könnte, ist nicht bekannt.
Da jedoch stets darauf verwiesen wird [Russel 94], daß die Netzkapazität ein wesentlicher, limitierenden Faktor ist, muß im vorliegenden Fall angenommen werden, daß durch die hohe Netzbelastung die Grenze, vor allem in Bezug auf die Anzahl von Maschinen, auf jeden Fall niedriger anzusetzen ist.

Im administrativen Bereich ist dagegen volle Skalierbarkeit gewährleistet, da die beschriebenen Mechanismen bei jeder Zellgröße umsetzbar sind.

Ein großer Vorteil monolithischer Zellen ist, daß die Komplexität der Systemverwaltung zum überwiegenden Teil im Rahmen der Konfiguration zu lösen ist. Erweiterungen, wie das Hinzufügen neuer Benutzer, inklusive der für sie geltenden Zugriffsregeln können mit sehr geringem Aufwand durchgeführt werden.

5.1.11 Leistungsaspekte

Ein großes Problem bei monolithischen Zelle ist die Minimierung des Hintergrundverkehrs. Im vorliegenden Fall kommt dem Hintergrundverkehr, der über das lokale Netz hinausgeht, aufgrund der immensen Datenströme zwischen dem Rechenzentrum und den Workgroupsegmenten eine große Bedeutung zu.
Diese Problematik wird dadurch noch verschärft, da es aus Sicherheitsgründen nicht ratsam erscheint, den Sicherheitsdienst auch in den einzelnen Workgroups zu replizieren.

Beim *Cell Directory Service* ist hingegen durch die Partitionierung des Namensraumes und der damit verbundenen Begrenzung des Updateverkehrs eine entscheidende Maßnahme zur Verkehrsminimierung getroffen worden.
Die Replikation der Workgroup-spezifischen Verzeichnisse auf mindestens einen weiteren *CDS-Server* sollte jedoch unbedingt durchgeführt werden.

Durch die sparsame Verteilung von globalen Time-Servern entsteht auch beim *Time Service* lediglich geringer Hintergrundverkehr.
Der zur Synchronisation der Clients nötige Verkehr wird architekturbedingt auf das lokale Netzwerk beschränkt.

Beim *Fileset-Location*-Dienst ist die lesende Zugriffshäufigkeit wesentlich häufiger als die schreibende. Die Replikation dieses Diensten in den einzelnen Workgroupsegmenten hat also einen positiven Effekt auf die gesamten Netzbelastung, da Replikat-Updates nur in unregelmäßigen Abständen auftreten.

5.2 Isolierte Rechenzentrumszelle und Zellen auf Workgroupebene

Als begrenzender Faktor eines zentralen Ansatzes hat sich vor allem die Maschinenskalierbarkeit herausgestellt. Dieser Problematik ist nur dadurch zu begegnen, daß man die monolithische Zellstruktur aufbricht und versucht, möglichst viel Verkehr auf die lokalen Netzbereiche zu beschränken.
Dies kann nur durch die Etablierung von Zellen auf Workgroupebene realisiert werden.
In diesem Kontext werden auch die dezentralen Bereiche und das Rechenzentrum in separaten Zellen angeordnet. Zudem wird auch für jede Workgroup eine eigene Zelle errichtet.
Der Workgroup-Ansatz versucht zudem, den funktionalen Abhängigkeiten Rechnung zu tragen. Die Kooperation im FIZ erfolgt sternförmig über den Austausch von Dateien innerhalb der Rechenzentrumszelle.
Das Rechenzentrum als Schnitt aller Kooperationsbeziehungen wird also aus dem Zellverbund ausgegliedert und stellt eine Art zentraler Ressource dar.

Die Kooperation mit den anderen Zellen wird über die *Peer-to-Peer*-Beziehungen zwischen den dezentralen Zellen und der Rechenzentrumszelle abgewickelt.

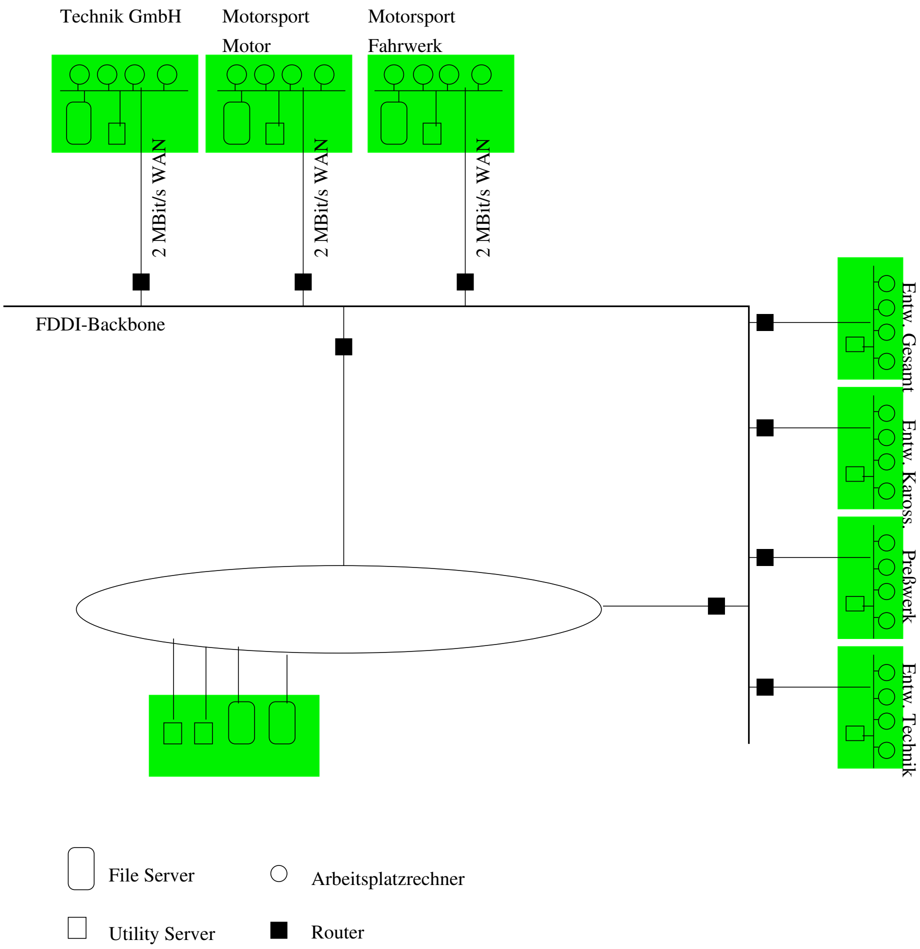


Abbildung 5.7: Workgroupzellen

Desweiteren orientiert sich diese Zellstruktur an den, durch die Netztopologie bestimmten Gegebenheiten. Aus diesem Grund werden auf Workgroupebene aus Sicht von DCE vollständig autonome Zellen mit eigener Benutzerpopulation definiert.

Unter Ausnutzung der Interzell-Funktionalität fungiert das Rechenzentrum als zentrale Ressource, auf die aus den Workgroupzellen zugegriffen werden kann.
Im Sinne die Dienstaspektes von DCE werden also in erster Linie Ressourcen über die Mechanismen von DCE den einzelnen Anwenderbereichen zur Verfügung gestellt.

Anhand dieser Mehrzellstruktur soll darüberhinaus untersucht werden, ob sich zentrale und hierarchische Administrationkonzepte unabhängig von den existierenden Zellgrenzen realisieren lassen. Zu diesem Zweck wird die Funktion der Rechenzentrumszelle über die reine Diensterbringung hinaus erweitert, sodaß sie auch als Verwaltungsdomäne für den gesamten Verbund genutzt werden kann.

Ein Ziel des Workgroupansatzes ist, über Zugriffsrechte für Principals einer Administratorzelle die Verwaltungsaufgaben in den einzelnen Workgroupzellen zu zentralisieren.

5.2.1 Verteilung der Dienste

5.2.1.1 Die zentralen LAN-Segmente des *FIZ*

In einem Zellverbund muß jede unabhängige Zelle mit einem kompletten Satz von Basisdiensten ausgestattet sein. Um auch in diesem Fall der funktionalen Differenzierung von Server- und Clientsystemen Rechnung zu tragen, werden diese Dienste zentral auf jedem Workgroup-Server angeboten.
Jeder *Utility Server* muß demnach sowohl mit einem *Security Server*, einem *CDS Server*, einen globalem *Time-Server* und einem *Global Directory Agent* zur Interzellkommunikation ausgestattet sein. In den Workgroups, in denen kein Workgroup-Server zur Verfügung steht, müssen die entsprechenden Serverinstanzen über mehrere Arbeitsplatzrechner verteilt werden.
Aufgrund der großen Anzahl von Workgroupzellen sollten diese aus Gründen einer einfacheren Verwaltung nicht über *X.500*, sondern über den *Domain Name Service* registriert werden.

Die Konfiguration der zusätzlichen *Time Server* kann analog zu der bei monolithischen Zellen beschriebenen Methode (vgl. Abschnitt 5.1.2) erfolgen.
Wie schon in anderem Zusammenhang angesprochen, muß die Synchronisation der Systemuhren zwischen der Rechenzentrumszelle und den einzelnen Workgroupzellen auch weiterhin gewährleistet sein, um den Dateizugriff im Rahmen von DFS durchführen zu können. Dies ist jedoch problematisch, da der Synchronisationsmechanismus von DTS auf eine Zelle beschränkt ist.

Eine Möglichkeit der Zeitsynchronisation zwischen unterschiedlichen Zellen ist die Verwendung des *Network Time Protocol (NTP).*
NTP setzt dabei ein hierarchisches Konzept der Synchronisation um. An der Wurzel dieser Struktur steht gewöhnlich ein primärer Server, der sich über einen externen Zeitgeber synchronisiert. Dieser Server wird sich üblicherweise im Rechenzentrum befinden.
In der vorliegenden Konstellation sind also alle *Utility Server* als sekundäre *NTP-Server* zu konfigurieren. Dadurch ist eine netzeinheitliche Systemzeit auch über Zellgrenzen hinweg zu realisieren.

Alternativ dazu kann auch ein Rechner pro Workgroup mit einem externen Zeitgeber ausgestattet werden.

5.2.1.2 Das Rechenzentrum

Auch im Rechenzentrum wird eine unabhängige Zellstruktur aufgebaut. Hier sollten die Dienste ähnlich wie beim monolithischen Ansatz mit mehreren Replikaten konfiguriert werden, da diese Dienste nicht nur den zellinternen Verkehr zu bewältigen haben, sondern darüberhinaus auch die Anfragen aus den Workgroupzellen bearbeiten müssen.
Die *Utility Server* im Rechenzentrum werden wie beim monolithischen Ansatz mit allen Basisdiensten ausgestattet.

5.2.1.3 Die dezentralen Bereiche

Da sich das Modell der Mehrzellstrukturen stark an den funktionalen Abhängigkeiten orientiert, werden auch für die dezentralen Bereiche eigene Zellen implementiert. Auch hierbei kann bei der Diensteverteilung der zuvor diskutierte Ansatz übernommen werden, mit dem Unterschied, daß nunmehr auch ein Master-Securityserver angeboten werden muß.

Eine strikte Auslegung des Workgroupkonzeptes legt es nahe, topologische Gegebenheiten auch in der Zellstruktur widerzuspiegeln. Hierbei spielt der Teilaspekt, daß Update- bzw. Replikat-Update-Verkehr zumindest teilweise über zwei WAN-Strecken hinweg abgewickelt werden müßte, eine Rolle. Im Vordergrund der Überlegungen steht jedoch die Tatsache, daß durch die Trennung kein zusätzlicher Aufwand entsteht, da ohnehin der gesamte Verbund anhand topologischer Merkmale strukturiert ist.

5.2.2 Kooperationmodelle

Da alle Zellen innerhalb klar abgegrenzter Netzbereiche existieren, ist es bei diesem Ansatz nicht erforderlich, spezielle Maßnahmen für die Zuordnung von Clients zu spezifischen Serverinstanzen zu treffen.

Auch beim Zugriff auf Ressourcen der Rechenzentrumszelle bzw. der dezentralen Zellen sind replizierte Serverinstanzen deshalb stets als gleichwertig zu betrachten.

5.2.3 Administration

Für die Kooperation der Zellen untereinander ist es erforderlich, zwischen den Zellen paarweise Interzell-Accounts anzulegen.
Das Kooperationsmodell zwischen dem zentralen Bereich des *FIZ* und den anderen Zellen des Unternehmens basiert dabei auf dem Austausch von Dateien über das Rechenzentrum. Zur Unterstützung dieses Kooperationsmodells wäre es also lediglich erforderlich, Interzell-Kommunikation zwischen der Rechenzentrumszelle und den dezentralen Zellen aufzusetzen.
Soll jedoch im Rahmen des Zellkonzepts auch der Mobilität der Benutzer Rechnung getragen werden, so ist es notwendig auch zwischen den Workgroupzellen und zwischen den Workgroupzellen und den dezentralen Zellen Surrogatschlüssel auszutauschen. Bei insgesamt n Zellen beläuft sich Anzahl der auszutauschenden Schlüssel

auf $\frac{n(n-1)}{2}$.
Im konkreten Fall mit 8 Zellen innerhalb Münchens wären dies folglich 28 Schlüssel.

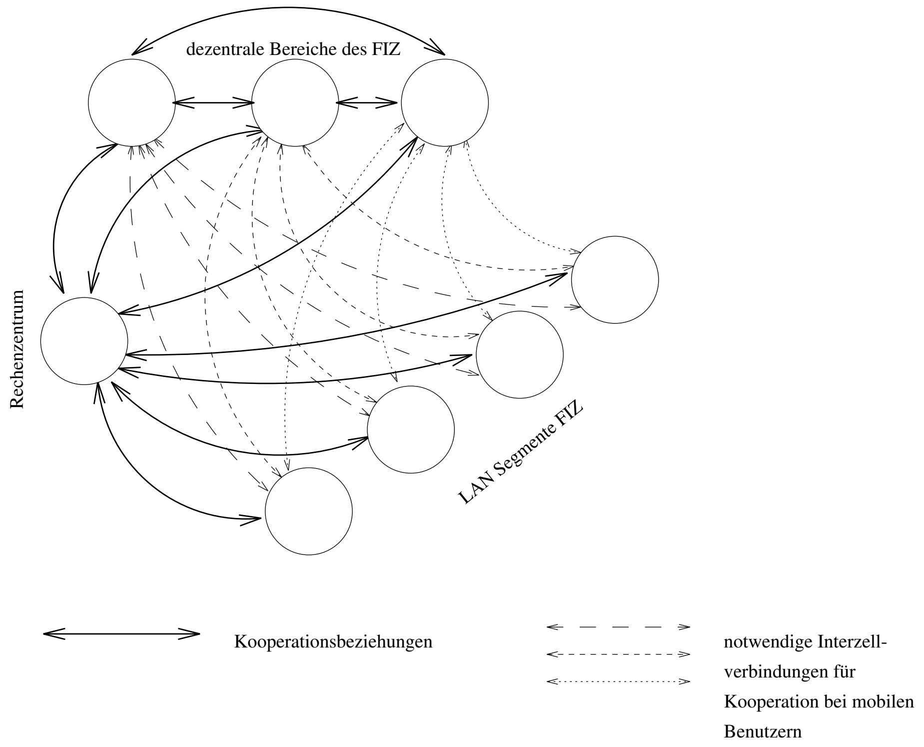


Abbildung 5.8: Gegenüberstellung der Kooperations- und Interzellbeziehungen

Die hohe Anzahl von Schlüsseln stellt einen signifikanten administrativen Aufwand dar. Alleine aus diesem Grund ist es nicht sinnvoll, die Verwaltung der Umgebung auf Zellebene zu organisieren. Die aus der Vielzahl von Zellen erwachsende Komplexität der gesamten Umgebung muß also vor allem in Hinsicht auf die Verwaltung handhabbar gemacht werden. Zu diesem Zweck wird die Rechenzentrumszelle als Administrationszelle für alle Bereiche innerhalb Münchens definiert.

5.2.3.1 Delegation von Verwaltungstätigkeiten

Durch die Vielzahl von Zellen, die es in diesem Ansatz zu verwalten gilt, muß eine Möglichkeit zur zellübergreifenden Administration geschaffen werden. Dies durch die Definition von Verwalterrollen auf Zellebene und die Zuordnung von Systemmanagern zur einer Menge gleichartiger, da lediglich zellbezogener Rollen zu realisieren, ist aus Gründen der Transparenz nicht zu vertreten.
Es muß also ein Mechanismus gefunden werden, der es erlaubt, Objekte, die funktional einer bestimmten Zelle zugeordnet sind, unter die Kontrolle eines Verwalters aus einer anderen Zelle zu stellen.

Da die Manipulation eines Objektes untrennbar mit den, für es geltenden Zugriffsregeln zusammenhängt, können durch die Nutzung spezieller *ACL*-Einträge für *Principals* bzw. Gruppen aus fremden Zellen Verwaltungsdomänen auch über Zellgrenzen hinweg implementiert werden.
Dies läßt sich am Beispiel der Schlüsselverwaltung demonstrieren:

Für die Verwaltung der Interzell-Schlüssel des gesamten Zellverbundes wird in der Rechenzentrumszelle eine Gruppe `interc_admin` erzeugt, die die mit dieser Aufgabe verbundene Rolle verkörpert.
Danach muß in jeder Zelle die Zugriffskontrolliste für das Verzeichnis des Sicherheitsdienstes, in dem die *Zell-Principals* registriert werden derart geändert werden, daß lediglich die besagte Gruppe Schreib-, Lösch- bzw. Einfügerechte besitzt.
Nachdem die Konfiguration abgeschlossen ist, obliegt die Kontrolle der Interzell-Beziehungen ausschließlich der Rolle des zentralen Interzell-Verwalters.

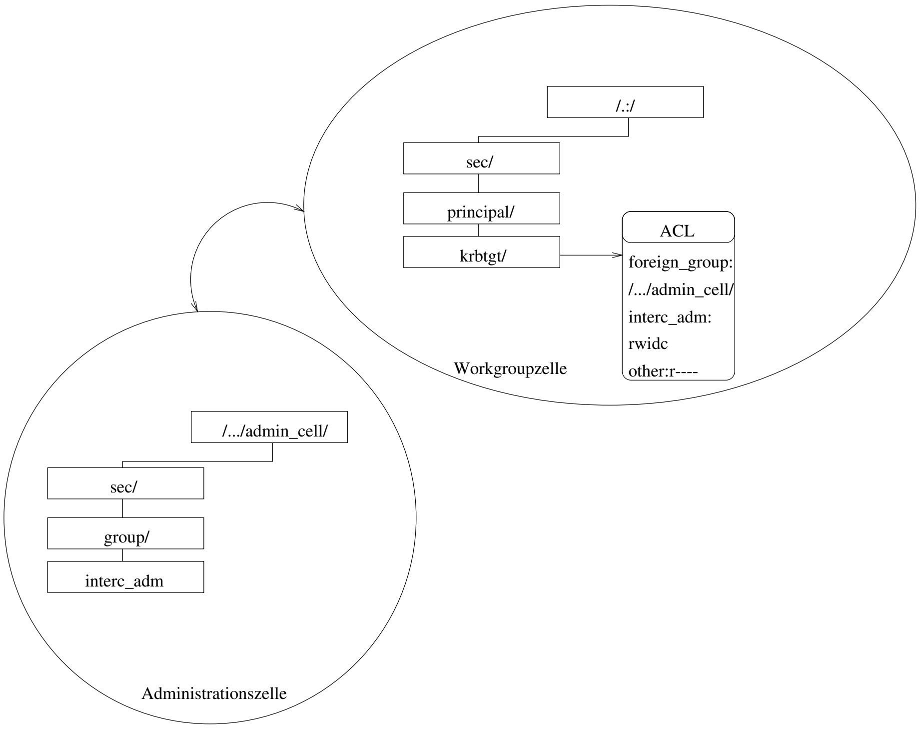


Abbildung 5.9: Beispiel für eine zellübergreifende Kontrolle der Interzell-Kommunikation

Durch die Umsetzung dieses Konzeptes für alle anfallenden Verwaltungsaufgaben ist es möglich, die Rechenzentrumszelle nicht nur für die Erbringung von Diensten zu nutzen, sondern ihre Funktion auf eine Administrationszelle für den gesamten Zellverbund zu erweitern.

5.2.3.2 Benutzerverwaltung

Dieser Konzeption der Delegation folgend, werden die Benutzer in einer ihnen zugeordneten Workgroupzelle registriert. Die Benutzerverwaltung wird jedoch auch weiterhin zentral durchgeführt. Dazu wird in der Administrationszelle eine spezielle Gruppe (z.B.: `CATIA-admin`) eingerichtet, die volle Administrationsrechte auf dem Namensraum des Sicherheitsdienstes aller Workgroupzellen hat. Die Registrierung von Benutzern kann nun zwar nicht mehr an zentraler Stelle, aber dennoch von zentraler Stelle aus durchgeführt werden.

Für jede Zelle ist darüberhinaus eine Gruppe der CATIA-Benutzer anzulegen, um die Verwaltung der Zugriffskontrolle auf die Datenbestände der Serverzelle nicht individuell für jeden Benutzer organisieren zu müssen. Stattdessen werden die Rechte auf den Projektverzeichnissen über die CATIA-Gruppen der einzelnen Workgroups vergeben. Im Vergleich zur monolithischen Zellstruktur wird die Prozedur beim Anlegen von Projektverzeichnissen jedoch aufwendiger, da es nicht mehr ausreichend ist, lediglich eine Projektgruppe zu definieren.

Besonders ist bei der Benutzerverwaltung darauf zu achten, daß die von der zentralen Betreuungsinstanz erzeugten Objekte – d.h. die *Principals* der CATIA Benutzer und die Gruppe der CATIA Benutzer in den einzelnen Workgroupzellen –) von niemanden sonst manipuliert werden können. Eine strikte Kontrolle der *ACLs* dieser Objekte ist also unbedingt erforderlich.
Über die anderen Bereiche der Zellnamensraumes kann den dezentralen Verwaltungsinstanzen weitreichende Freiheit gewährt werden.

Um die Verwaltung der Benutzer möglichst effizient durchführen zu können, empfiehlt es sich, den einzelnen Zellen disjunkte UID-Bereiche zuzuweisen.

5.2.3.3 Verwaltung der Datenbestände

Aufgrund der speziellen Anordnung der Ressourcen im zentralen Bereich des *FIZ*, verbleiben auch alle wesentlichen Teile des Datenbestandes im Rechenzentrum.
Durch die Verteilung der Benutzerpopulation erfordert das Management der Zugriffskontrolle nun einen höheren Konfigurationsaufwand, da keine homogene Benutzergruppe aller CATIA-Benutzer mehr existiert.
Beim Anlegen eines Projektverzeichnisses ist es nunmehr notwendig, alle benötigten Projektgruppen aus den Workgroupzellen in die entsprechende Zugriffskontrolliste einzutragen.
Durch den Vererbungsmechanismus der *ACLs* beschränkt sich dieser Aufwand auf die initiale Konfiguration beim Einrichten eines Projektverzeichnisses.

Ein weiteres Problem stellt die Tatsache dar, daß die administrativen Domänen von DFS auch auf eine Zelle begrenzt sind. Für die dezentralen Bereiche muß also jeweils eine administrative Domäne errichtet werden, in der dann eine zentrale Betreuungsinstanz aus der Rechenzentrumszelle Verwaltungsaufgaben übernehmen kann. Die läßt sich über die Einträge der entsprechenden Verwalterrollen in den in Abschnitt 5.1.4.1 beschriebenen administrativen Listen regeln.

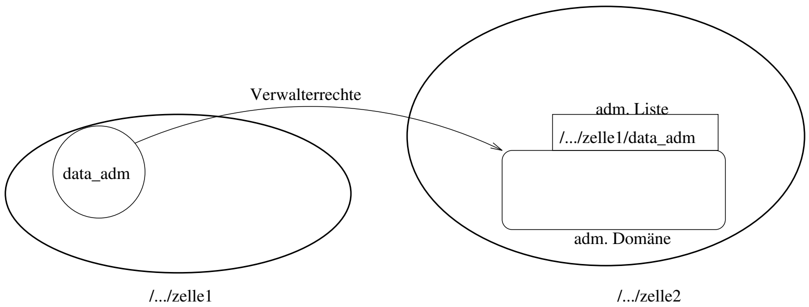


Abbildung 5.10: Verwaltung der Datenbestände über Zellgrenzen

Eine wesentliche Funktionseinschränkung bei einer Mehrzellstruktur stellt die Begrenzung des DFS-eigenen Backup-System auf den Dateiraum einer Zelle dar.
Aufgrund dieser Tatsache ist man nicht mehr in der Lage das Backup Fileset-bezogen durchzuführen. Um dennoch einen zentralen Backup-Dienst anbieten zu

können, müssen auf allen Dateiserver, die einen Backupdienst außerhalb des lokalen Zellbereichs nutzen wollen, ihre *Filesets* zusätzlich in ihr lokales Dateisystem mounten.

Das Backup kann dann maschinenbezogen mit DCE-unabhängigen Werkzeugen durchgeführt werden. Es sollte jedoch berücksichtigt werden, daß die spezielle Funktionalität des Fileset-Managements (Verschieben und Replikation von Filesets) in diesem Fall nicht mehr möglich sind.

5.2.4 Sicherheit

5.2.4.1 Sicherheit des gesamten Verbundes

Auch in diesem Ansatz verbleiben die sicherheitskritischen Daten unter der Kontrolle des Rechenzentrums. Der Zugriff auf diese Daten erfolgt jedoch aus fremden Zellen. Zwar weisen die Sicherheitsmechanismen von DCE auch bei Kommunikationsbeziehungen über Zellgrenzen hinweg dieselbe Mächtigkeit auf, ein nicht zu vernachlässigendes Problem stellen im vorliegenden Fall jene Security-Server dar, die nicht gegen allgemeinen Benutzerzugriff geschützt sind. Da jede Zelle Interzell-Beziehungen zu allen anderen Zellen des Verbundes unterhält, hat auch der Einbruch in eine Workgroupzelle globale Auswirkungen, da ein Eindringling die Identität jedes Benutzers der betroffenen Zelle annehmen kann und somit auch Zugriff auf dessen Datenbestände bzw. auf alle Projektdatenbestände hat.

Mehrzellstrukturen können jedoch auch dazu genutzt werden, eine zellbezogene Zugriffskontrolle zu implementieren. Diese Möglichkeit der Sicherung einer Zelle besteht in der Unterbindung von Interzell-Beziehungen.
Dadurch ist es möglich, die Zugriffe auf lokale Ressourcen so zu beschränken, daß lediglich Zellen mit denen explizite Kooperation – und somit Interzell-Kommunikation – besteht, in der Lage sind die Ressourcen der eigenen Zelle zu nutzen.

Mit dieser Methode lassen sich unterschiedliche Sicherheitsanforderungen für unterschiedliche Bereiche realisieren.

Im vorliegenden Fall ist es sogar möglich, Zugriffe nur in eine Richtung zu erlauben. So ist es etwa denkbar, Interzell-Beziehungen zwischen den Zellen der Motorsport GmbH und den Workgroupzellen des FIZ zu unterbinden, zwischen der Rechenzentrumszelle und den Zellen der Motorsport GmbH jedoch Kooperation zuzulassen. Da die Motorsport GmbH lediglich Datensenke ist, kann sie Dateien auf den Fileservern des FIZ nutzen und gleichzeitig besondere Sicherheitsmaßnahmen implementieren, indem sie lediglich Interzell-Beziehungen zwischen ihren Standortzellen und dem Rechenzentrum zuläßt.

5.2.4.2 Sicherheit auf Kommunikationsebene

Im Rahmen der Workgroupzellen ist die Ausdehnung einer Zelle stets auf ein lokales Netz begrenzt. Der Einsatz von *Firewalls* an den Zugängen zu öffentlichen Netzen beeinträchtigt das Arbeiten innerhalb der Zelle nicht.

Worauf *Firewalls* Einfluß nehmen, ist die Kooperation zwischen unterschiedlichen Zellen, da sie die Kommunikation mit den DCE-Diensten in einer fremden Zelle unterbinden. Aus diesem Grund empfiehlt es sich, für den Austausch von Dateien ein Dateitransferprotokoll zu benutzen, für das ein Applikationsgateway (*proxy server*) existiert, das auf dem *Firewall* installiert werden kann.

Somit ist der erforderliche Grad an Kommunikationssicherheit zu erzielen. Diese Lösung erlaubt es zudem, unter Gewährleistung der Sicherheit auch Daten mit Partnern auszutauschen, die selbst nicht DCE nutzen.

Eine weitere Möglichkeit ist, den Firewall zu einer *Gateway-Zelle* mit eigenem Dateisystem zu erweitern. In diesem Dateisystems können dann Bereiche eingerichtet werden, die als gemeinsamer Briefkasten von Benutzern innerhalb bzw. außerhalb einer Sicherheitsdomäne genutzt werden können. Auf diese Weise kann der Transfer von Informationen zwischen dem eigenen Bereich und externen Partnern mit voller Unterstützung durch die Sicherheitsmechanismen von DCE abgewickelt werden.

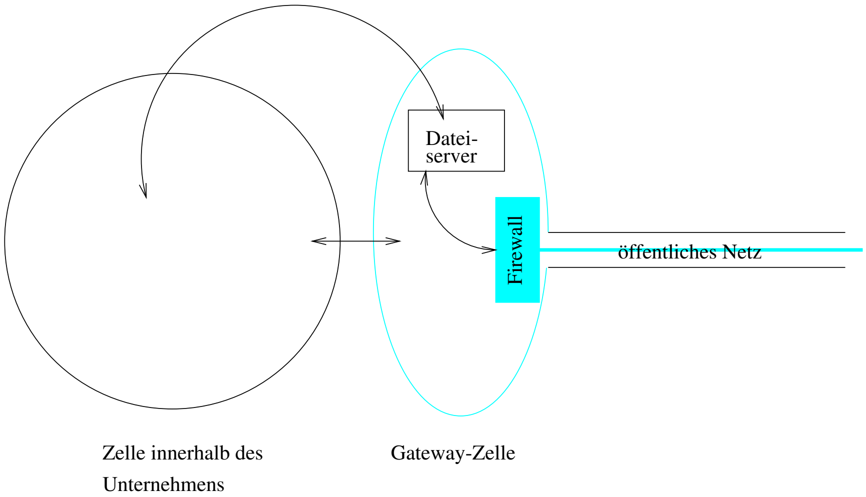


Abbildung 5.11: Der Firewall als Gateway-Zelle

5.2.5 Verfügbarkeit

Bei einer Mehrzellstruktur, die wie im Falle des FIZ funktionale Abhängigkeiten zwischen Zellen aufweist, wird die Verfügbarkeit des gesamten Systems durch die Verfügbarkeit der einzelnen Zellen bestimmt.
Für die Kooperation zwischen zwei Zellen ist es also erforderlich, daß beide Zellen verfügbar sind.

Im Rechenzentrum ist eine hohe Verfügbarkeit der Zelle über Replikation der Basisdienste sichergestellt. Hier haben also individuelle Fehlfunktionen der Komponenten von DCE keine weitreichenderen Auswirkungen.

Anders verhält es sich mit den einzelnen Workgroupzellen. Durch deren feinkörnige Struktur kann der Ausfall eines Dienstes die gesamte Zelle außer Funktion setzen. Aufgrund der engen Integration aller DCE-Dienste untereinander existieren mehrere isolierte Fehlerquellen pro Workgroupzelle, da bereits der Ausfall eines Serverprozesses eine Zelle außer Funktion setzen kann.

In den dezentralen Bereichen stellt sich die Situation ähnlich dar. Da bei diesen Zellen vor allem das Arbeiten innerhalb der eigenen Zelle im Vordergrund steht, sollte auf jeden Fall ein zusätzliches Replikat des CDS-Servers installiert werden. Von einer Replikation des Security-Servers sollte jedoch aus Sicherheitsgründen Abstand genommen werden.

Einfluß von Netzstörungen

Die Auswirkungen von Netzstörungen zwischen zwei Zellen wirken sich nicht auf die Betriebsstabilität der beiden Zellen aus. Es ist jedoch keine Kooperation mehr zwischen den betroffenen Zellen möglich.
Kritisch wirkt sich jedoch eine Netzstörung zwischen der Rechenzentrumszelle und den zentralen LAN-Segmenten aus, da aufgrund der funktionalen Abhängigkeiten keine zentralen Dienste mehr genutzt werden können.

5.2.6 Migration

Im Rahmen der gewählten Zellstruktur kann die Migration bezüglich der Errichtung von Zellen abteilungsbezogen durchgeführt werden. Voraussetzung ist jedoch, daß zuerst das Rechenzentrum in eine DCE-Infrastruktur überführt wird.

Ein Punkt, der die Migration in diese Zellstruktur erschwert, ist die Tatsache, daß der gesamte, vorher zentral verwaltete Benutzerbestand partitioniert werden muß. Aus diesem Grund ist es nicht möglich, mittels der Werkzeuge von DCE das Eintragen der Benutzer in die Datenbank des Sicherheitsdienstes zu automatisieren.

Darüberhinaus erweist sich bei dieser Mehrzellstruktur als Nachteil, daß die Datenbestände des FIZ zu Beginn der Migration nicht nur über DFS exportiert werden müssen, sondern auch auf LFS-Partitionen kopiert werden müssen, um Zugriffe auch über Zellgrenzen zu erlauben. Die gesamten Datenbestände müssen also auf LFS-Partitionen verlagert werden, bevor der Betrieb der Workgroupzellen aufgenommen werden kann.
Ein schrittweiser Umstieg, wie im monolithischen Fall ist also nicht möglich.

Es besteht jedoch Möglichkeit die Datenbestände parallel via NFS und DFS zu exportieren. Dadurch bleibt es möglich, eine stufenweise Migration durchzuführen und nicht den gesamten Verbund auf einmal in eine DCE-Infrastruktur zu überführen, da die Bereiche, die DCE noch nicht einsetzen auch weiterhin über NFS auf die Daten zugreifen können.

5.2.7 Transparenz

Aus Benutzersicht wird bei einer Mehrzellstruktur die Transparenz zumindest teilweise eingeschränkt. Dies liegt darin begründet, daß im Gegensatz zu einer monolithischen Zelle die Zellnamen nicht mehr ignoriert werden können.
Im vorliegenden Ansatz arbeitet jede Workgroup auf einem eigenen Zellkontext.

Durch die Art der Nutzung des CATIA-Verbundes ist dieses Problem vorrangig auf die Dateisysteme der einzelnen Zellen konzentriert. Um allen Workgroupzellen eine möglichst konsistente Sicht auf den gesamten Namensraum aller produktiven Zellen – das sind die Zellen, die Projekt- und Benutzerdaten halten – können zwei Maßnahmen getroffen werden.

1. Man integriert die wesentlichen Teile des verteilten Dateisystems über Links in das lokale Dateisystem jedes Clientrechners.

2. Man mountet die entsprechenden Filesets der Rechenzentrumszelle in den Namensraum des Dateisystems jeder Workgroupzelle

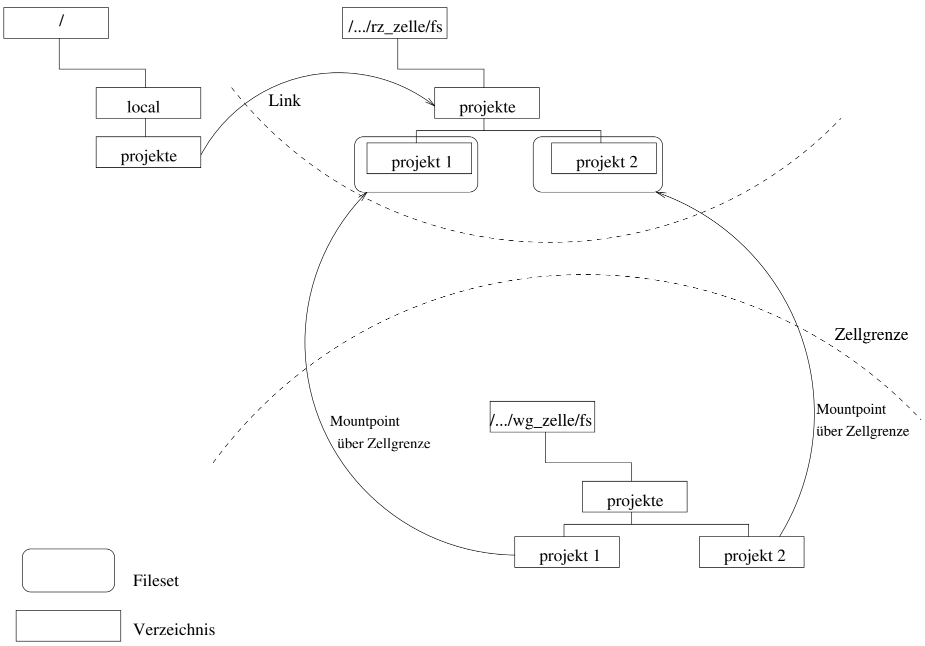


Abbildung 5.12: Sicherstellen einer konsistenten Sicht auf das verbundweite Dateisystem

Dadurch kann erreicht werden, daß die Sicht auf das verteilte Dateisystem von allen Arbeitsplätzen aus identisch ist. Darüberhinaus hat man die Möglichkeit, diejenigen Teile des Datenbestandes, die für gewisse Anwenderbereiche nicht wesentlich sind, aus den Dateisystem einer Workgroupzelle „auszublenden“.

5.2.8 Änderungsflexibilität

5.2.8.1 Reaktion auf organisatorische Veränderungen

Zwar ist diese Zellstruktur an die Netztopologie angelehnt, aufgrund der engen Zusammenhänge zwischen Topologie und Abteilungsstruktur existieren jedoch starke Abhängigkeiten zwischen Zell- und Organisationsstruktur.

Das Wechseln von Rechnern und Benutzern zwischen Abteilungen kann also nicht mehr transparent geschehen, da eine Integration in eine andere Zelle unumgänglich ist.

5.2.8.2 Reaktionen auf Konfigurationsänderungen

Ist es nicht nur erforderlich Server innerhalb einer Zelle zu verlagern, sondern in eine andere Zelle zu integrieren so ist dies stets mit einer vollständigen Neukonfiguration verbunden.
Auch das unter dem Abschnitt 5.1.9.2 bei einer monolithischen Zelle angesprochene Verlagern von Plattenspeicher scheitert, da die Identifikatoren der Filesets nur zellweit eindeutig sind. Aus diesem Grund ist es notwendig die entsprechende Fileset-Struktur in der neuen Zelle anzulegen, die Daten zu kopieren, die Maschine neu zu installieren und danach die Daten zurück auf die Maschine zu verlagern.

Auch in Hinsicht auf das Wechseln von Benutzern zwischen zwei Abteilungen ist die Umgebung nicht flexibel. In diesem Fall muß der Benutzer als Principal in der neuen Zelle registriert werden, eventuell müssen Daten aus der alten Zelle in die neue kopiert werden, und er muß als Principal in seiner alten Zelle gelöscht werden.

5.2.8.3 Reaktionen auf Performanceengpässe

Die Größe der Workgroupzellen bewegt sich in einem Rahmen (d.h. etwa 50 Rechner und Benutzer pro Zelle), deren Betrieb unter Gewährleistung der Leistung auf jeden Fall sichergestellt ist.
Diesbezüglich ist die Notwendigkeit von Änderungen also nicht gegeben.

Das Problem eines Performance-Engpasses kann sich dagegen in der Rechenzentrumszelle einstellen. Aufgrund der relativ geringen Replikationsmöglichkeiten durch die begrenzte Anzahl von Servern, kann Leistungsengpässen nur durch das Hinzufügen weiterer Maschinen begegnet werden.

5.2.8.4 Integration mit anderen Verbunden

Im wesentlichen lassen sich andere Verbunde relativ nahtlos in die existierenden Workgroupzellen integrieren. Dabei existieren zwei Alternativen:

1. Die anderen Verbunde werden anhand ihrer Verteilung im Netz in die existierenden Workgroupzellen integriert.
2. Die anderen Verbunde werden analog zum CATIA-Verbund in separate Workgroupzellen unterteilt

In beiden Fällen sollten jedoch die entsprechenden Server des zu integrierenden Verbundes in die existierende Rechenzentrumszelle integriert werden, um eine möglichst transparente Sicht auf die Umgebung zu gewährleisten.

Das zentrale Problem einer Erweiterung der Zellstruktur ist jedoch, daß zur Erbringung einer Funktion alle Requests innerhalb der Rechenzentrumszelle bearbeitet werden müssen. Wie schon im vorangegangenen Abschnitt ausgeführt, wird der Erweiterung durch die zentral zur Verfügung stehenden Dienst- und die Netzkapazität begrenzt.

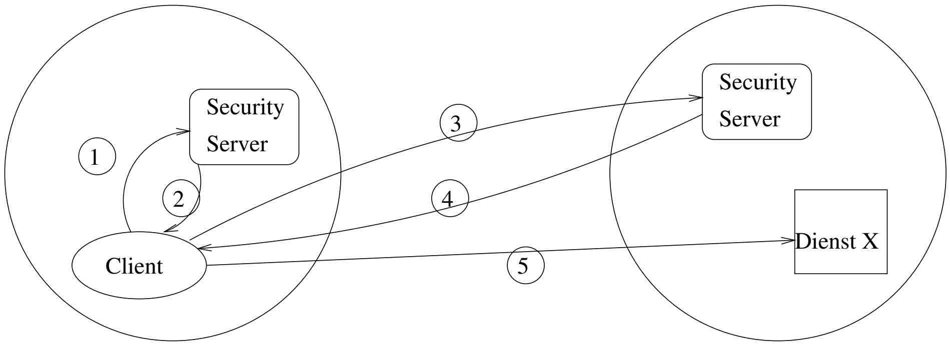
5.2.9 Skalierbarkeit

Ein Problem dieser differenzierteren Zellstruktur ist die Beschränkung, der für die Erbringung der Dienste wesentlichen Server auf den Bereich des Rechenzentrums. Dadurch ist die Anzahl der maximal zu bedienenden Clients durch die Kapazität der Rechenzentrumsserver limitiert.
Aufgrund der speziellen Anwendungscharakteristik sind jedoch gewisse Verzögerungen, die durch die erhöhte Last der zentralen Server hervorgerufen werden zu tolerieren, da der größte Teil der Zeit für den Dateitransport aufgewendet werden muß.

Bei der administrativen Skalierbarkeit stellt sich das Problem, daß der Aufwand für die Betriebsbetreuung linear mit der Anzahl der Workgroupzellen steigt.
Das Konzept der Workgroupzellen ist also für Umgebungen, die über eine Vielzahl von LANs verteilt sind nicht geeignet.

5.2.10 Leistungsaspekte

Ein häufig im Zusammenhang mit Mehrzellstrukturen angesprochenes Thema sind die höheren Antwortzeiten, die aus dem Mehraufwand der Interzell-Kommunikation entstehen.
Prinzipiell läßt sich dabei feststellen, daß bei initialen Aufrufen von Diensten in einer fremden Zelle eine erhöhte Interaktion mit den Basisdiensten festzustellen ist. Dies ist in erster Linie die Suche nach einer Instanz des Verzeichnisdienstes der fremden Zelle, sowie der Erwerb von Tickets für Dienste der fremden Zelle.
Sowohl die Anfragen an den Verzeichnisdienst einer fremden Zelle, als auch das *Foreign Privilege Ticket Granting Tickets (FPTGT)*, mit dem man bei dem entsprechenden Sicherheitsdienst der fremden Zelle Tickets für weitere Dienste anfordern kann, werden von den Clients in einem Cache abgelegt und können damit bei nachfolgenden Aufrufen wiederverwendet werden.
Sobald also diese Initialisierungsphase abgeschlossen ist - sprich der Benutzer das *FPTGT* besitzt - verläuft die weitere Kooperation mit annähernd demselben Aufwand, wie er innerhalb einer Zelle notwendig wäre.



1. Client stellt Anfrage zum Aufruf eines fremden Servers
2. Security Server verschlüsselt das PAC mit dem gemeinsamen Surrogatschlüssel der beiden Zellen
3. Client authentifiziert sich damit beim Security Service der fremden Zelle und fordert ein Ticket für den Dienst X an.
4. Security Server liefert die Authentifizierungsinformationen für den Dienst X
5. Client authentifiziert sich gegenüber dem Dienst X

Abbildung 5.13: Dienstaufrufe über Zellgrenzen

Die Leistungsfähigkeit innerhalb einer Workgroupzelle ist auf jeden Fall gewährleistet. Nur bei Dateizugriffen in der Rechenzentrumszelle kommen die Verzögerungen aufgrund der zellübergreifenden Kommunikation zustande. Aufgrund der Anwendungscharakteristik (jedes Modell, das geladen wird umfaßt 10 MB) ist jedoch anzumerken, daß diese vorbereitende Kommunikation gegenüber dem eigentlichen Dateitransport kaum ins Gewicht fällt.

Verkehrsanalyse

Mit den vorliegenden Vorschlag ist es gelungen, den Hintergrundverkehr zu minimieren und auf die einzelnen lokalen Netzwerke zu begrenzen. Auch sämtliche Formen des Update-Verkehrs werden auf die jeweilige Lokation begrenzt.
Der Preis ist, daß nun sämtlicher in den Workgroupzellen erzeugter Lookup-Verkehr zwischen dem Rechenzentrum und den LAN-Segmenten abgewickelt werden muß. Da jedoch viele dieser Lookup-Ergebnisse lokal zwischengespeichert werden, wird lediglich vor Dateizugriffen der entsprechende Fileseteintrag gesucht. Die dabei anfallende Kommunikationsmenge ist jedoch verglichen mit dem eigentlichen Dateitransport der CAD-Daten vernachlässigbar.
Es wird also im Vergleich zu den transportierten Dateien nur ein sehr geringer zusätzlicher Verkehr erzeugt.

5.3 Client- und Serverzellen

Die nun vorzustellende Zellstruktur ist ein Versuch, durch die Ausweitung des Client/Server-Modells auf die Zellstruktur die Mechanismen monolithischer Zellen und verteilter Zellen in einem Modell zu verschmelzen.

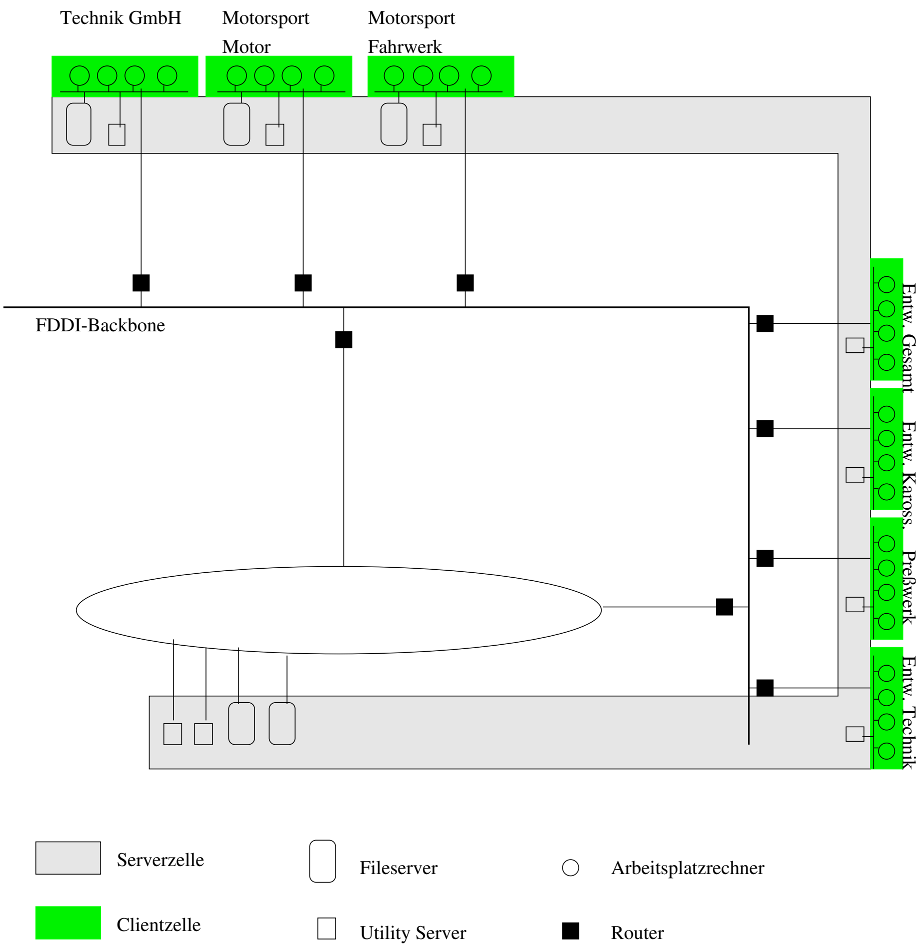


Abbildung 5.14: Client/Server-Zelle

Charakteristischerweise wird im Rahmen des Downsizing Serverfunktionalität über eine Reihe von Rechnern verteilt. Darüberhinaus betrifft dieser Prozeß nicht nur einen Anwenderbereich, sondern meist die gesamte IV-Infrastruktur einer Organisation. Im Gegensatz zu monolithischen Zellstrukturen, die versuchen, einzelne Anwenderbereiche zusammenzufassen, ist das Ziel der Client/Server-Zellen eine DCE-gerechte Strukturierung der gesamten Infrastruktur.

Sie folgt dabei der funktionalen Differenzierung der Rechensysteme, indem sie für Server- und Clientsysteme unterschiedliche Sichtweisen durch die Zellstruktur definiert. Dies geschieht zum einen deshalb, weil die Anzahl der Clientsysteme die Anzahl der Serversysteme meist um ein Vielfaches übersteigt, und da zum anderen für Client- bzw. Serverkomponenten unterschiedliche Verwaltungsanforderungen bestehen.

Dieses Vorgehen bringt aus Sicht der Nutzung und der Administration eine Reihe von Vorteilen:

- Durch das Zusammenfassen der produktiven Teile einer Umgebung, d.h. der Serverkomponenten, wird eine zentrale Sicht auf das gesamte System, sowohl unter dem Aspekt der Verwaltung, als auch der Nutzung ermöglicht.

- Durch die zellmäßige Trennung von Arbeitsplatzrechnern und Serverrechnern kann Engpässen bei der Maschinenskalierbarkeit entgegengetreten werden. Durch das Herauslösen der Clientsysteme besteht also die Möglichkeit – im Vergleich zu monolithischen Zellen – größere Verbunde unterstützen zu können, da der Hintergrundverkehr vollständig innerhalb der Clientzellen gehalten werden kann.

- Durch die Entkoppelung von Client- bzw. Serverfunktionalität auf der Ebene eines Anwenderbereiches ist es möglich, die Serversysteme mehrerer, oder gegebenenfalls aller Anwenderbereiche in einer Serverzelle zusammenzufassen. Diese Zelle kann dann von einer zentralen Betreiberorganisation verwaltet werden .
  Die Serverzellen einzelner Bereiche lassen sich also in einer *Datacenter*-Zelle bündeln.
  Die interne Struktur der *Datacenter*-Zelle kann dann mit den Mechanismen einer monolithischen Zelle an die Aufbau- und Ablauforganisation des Betreibers angepaßt werden.

- Die Strukturierung der einzelnen Anwenderbereiche in den Clientzellen ist völlig unabhängig von der Struktur der Serverzelle. Dieser Freiheitsgrad kann dazu genutzt werden, den speziellen Anforderungen im Zusammenhang mit der Infrastruktur Rechnung zu tragen. Darüberhinaus beeinträchtigt die Struktur der Clientzellen in keiner Weise die Sicht der Benutzer auf das gesamte System, da alle produktiven Bereiche innerhalb der Serverzelle eine Einheit (*Unified Distributed Resource*) darstellen.

- Die Erweiterbarkeit einer solchen Zellstruktur besteht in der Fähigkeit weitere Maschinen in die Client- und Serverzellen einbinden zu können und in der Integration zusätzlicher Anwenderbereiche.
  Dabei ist jedoch zu berücksichtigen, daß Server- und Clientsysteme dieser Anwenderbereiche ebenso klar getrennt sein müssen wie im Fall des CATIA-Verbundes, um sich nahtlos in eine Client/Server-Zellstruktur eingliedern zu lassen.

5.3.1 Infrastruktur

5.3.1.1 Die zentralen LAN-Segmente des *FIZ* und das Rechenzentrum

Die Serverzelle

Im vorliegenden Fall wird durch das Rechenzentrum nur ein DCE-basierter Dienst, nämlich der Dateidienst angeboten. Prinzipiell muß jedoch die Frage gestellt werden, wie alle durch das Rechenzentrum angebotenen Dienste, sofern sie auf Komponenten von DCE basieren, innerhalb der zentralen Zellstruktur verwaltet werden.
Denkbare Alternativen wären eine multifunktionale Serverzelle, die nach innen anhand der Dienststruktur gegliedert wird, oder separate Zellen für jeden Dienst.

Wie die Serverzelle exakt zu gestalten ist hängt davon ab, wie die einzelnen DCE-Dienste für die Anwender zur Verfügung gestellt werden sollen. Diese Tatsache findet sich in der Struktur der Clientzellen wieder.

- Die Dienste werden nur zentral angeboten:
  Für sehr kleine Zellen ist es nicht sinnvoll, dezentral Replikate aller Dienste zur Verfügung zu stellen, da unter Umständen der Replikat-Verkehr größer oder nur unwesentlich geringer ist, als der eigentliche Lookup-Verkehr. Alle Rechner dieser Zelle werden folglich in einer Clientzelle zusammengefaßt, oder in eine bereits bestehende Clientzelle integriert.

- Die Dienste werden auch dezentral angeboten:
  Zur Minimierung des Netzverkehrs zwischen einer Client- und einer Serverzelle werden Replikate der wichtigsten Dienste dezentral auf einem „Satelliten" der Serverzelle zur Verfügung gestellt. Im vorliegenden Fall bedeutet dies, daß auf dem *Utility Server* einer Workgroup ein Replikat des *CDS* und der *FLDB* der Serverzelle liegt.

- Es werden nicht nur die Dienste angeboten, sondern auch der Betrieb dezentraler Bereiche übernommen:
  Um dies möglichst effizient betreiben zu können, sollten die Clientzellen möglichst zu funktionalen Einheiten zusammengefaßt werden; im Fall des CATIA-Verbundes also alle Workstations nach Möglichkeit in einer Clientzelle vereinigt werden.

In all diesen Fällen ist jedoch stets das gesamte Rechenzentrum in der Serverzelle enthalten.

Lösungen für die Clientdomäne

Feinkörnige Zellstruktur auf Workgroupebene

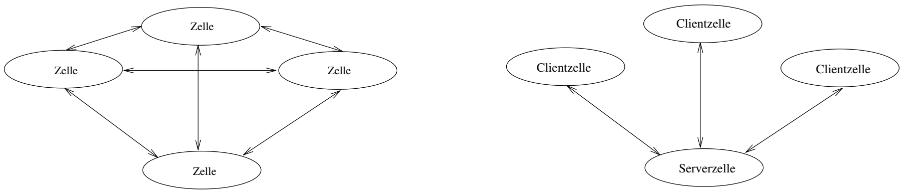
Die Arbeitsplatzrechner werden bei dieser Zellstruktur (vgl. Abb. 5.14 in eigenen Zellen angeordnet. Diese Clientzellen dienen jedoch nur dazu, den Zugang zur Serverzelle, in der alle produktiven Rechnerressourcen gebunden sind, zu ermöglichen. In den Clientzellen werden keine Benutzer des CATIA-Verbundes registriert. Die einzigen Kennungen, die in den Clientzellen eingerichtet werden, sind jene, die standardmäßig für die Zellverwaltung vorgesehen sind, sowie die nötigen Kennungen für die nicht interaktiven *Principals*, d.h. für die Rechner und Dienste der Clientzelle. Um mit der Serverzelle im Rahmen der Sicherheitsmechanismen von DCE kommunizieren zu können, muß zusätzlich eine Interzellkennung erzeugt werden.

Der administrative Mehraufwand, der bei der Wahl einer Mehrzellstruktur zwangsläufig entsteht, wird bei dieser Konzeption minimiert, da für die Clientzellen nur die, für den Betrieb einer Zelle notwendigen Basisdienste aufgesetzt werden müssen.

Einen weiteren Vorteil der Client/Server-Zellen stellt die Verringerung der Interzell-Beziehungen dar. Kooperation findet im Rahmen der Client/Server-Zellen überhaupt nicht mehr zwischen einzelnen Workgroupzellen statt. Stattdessen dient die Serverzelle als gemeinsames Betriebsmittel für alle Clientzellen in den unterschiedlichen LAN-Segmenten.

Bei n Zellen müssen beim Konzept der Workgroupzellen $n(n-1)$ Interzell-Accounts verwaltet werden, wohingegen die Lösung in der hier beschriebenen Konstellation nur $2 * (n-1)$ Interzell-Accounts benötigt (siehe Abb. 5.15).

Da diese Interzell-Authentifizierung eine gegenseitige Absprache der Systemverwalter beider involvierter Zellen bedingt, ist die Minimierung ihrer Anzahl ein wichtiger Beitrag, den administrativen Aufwand möglich gering zu halten.



vollständige Vermaschung bei unabhängigen Zellen

Peer-to-Peer Verbindungen zwischen Clientzellen und der Serverzelle

Abbildung 5.15: Struktur der Interzell-Beziehungen

Für die Verwaltung der Interzell-Schlüssel bietet sich auch hier das im Rahmen der Workgroupzellen in Abschnitt 5.2.3.1 diskutierte Verfahren an.

Kombination mit dem Workgroupansatz

Als weitere Alternative läßt sich die Zellstruktur aus dem Workgroupansatz übernehmen. In diesem Fall werden zusätzlich zu den Arbeitsplatzrechnern auch die *Utility Server* in die Clientzellen integriert (siehe Abb. 5.16). Damit wird erreicht, daß auch aus Sicht des Konfigurationsmanagements eine klare Trennung von Client- und Server-Systemen wiederhergestellt wird.

Im Gegensatz zur in Abschnitt 5.2 vorgestellten Workgroupstruktur, können nun durch die Zentralisierung der Benutzer und Datenbestände in der Serverzelle im Bereich des Systemverwaltung die flexiblen Ansätze einer monolithischen Zelle zum Einsatz kommen.

Diese Zellstruktur stellt also eine Verschmelzung der bisher diskutierten Strukturierungsoptionen dar. Im Gegensatz zu monolithischen Zelle werden Maschinen- und Benutzerskalierbarkeit voneinander entkoppelt.

Im Bereich des Managements beschränken sich die Aufgaben innerhalb einer Clientzelle auf die Betriebsüberwachung, da alle anderen Managementaufgaben in der Serverzelle in der Serverzelle zentralisiert sind.

Die einzige Aufgabe, die von zentraler Stelle für die Clientzellen durchgeführt werden muß, ist die Verwaltung der Interzell-Accounts. Hier kommt das im Rahmen der Workgroupzellen in Abschnitt 5.2.3.1 erwähnte Verfahren zum Einsatz. Ansonsten können administrative Zugriffsrechte auf die gesamten Clientzellen relativ frei an die Vor-Ort-Administratoren vergeben werden.

Nachteilig an dieser Lösung wirkt sich jedoch das Fehlen von Replikaten der Dienste der Serverzelle aus. Wie beim Workgroup-Ansatz können Replikate lediglich innerhalb des Rechenzentrums angeboten werden. Somit sind dieser Strukturierungsalternative in Bezug auf die Skalierbarkeit Grenzen gesetzt.

Funktionaler Ansatz

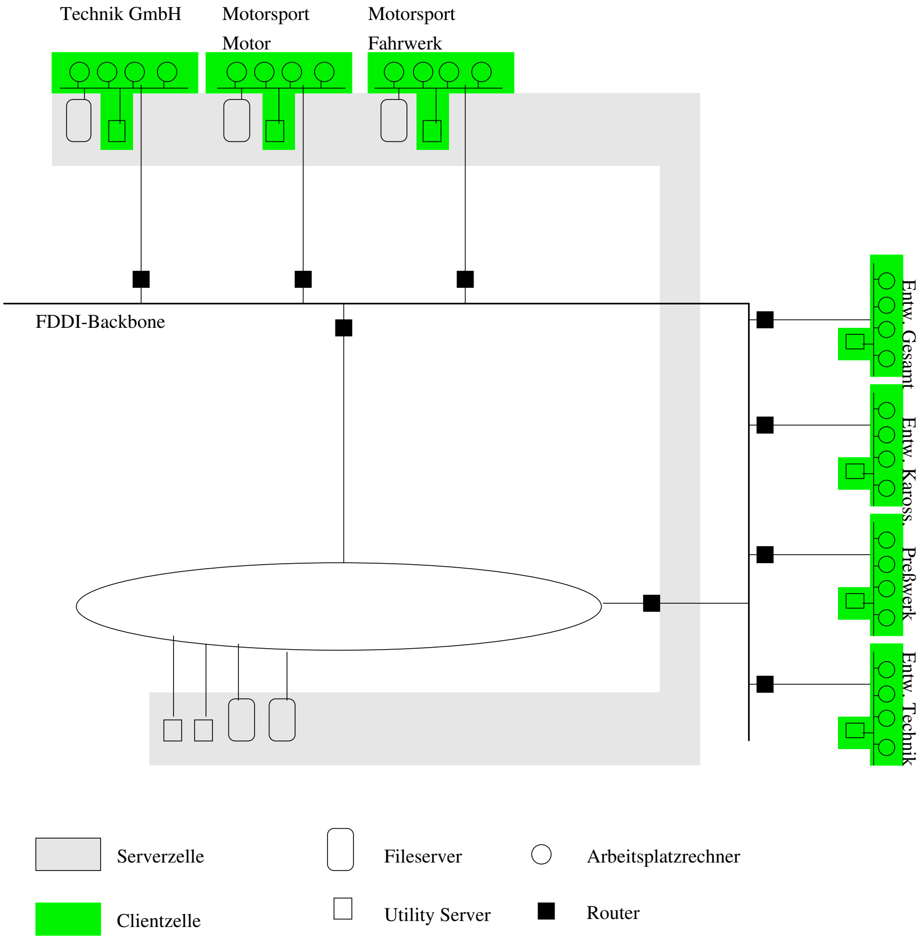


Abbildung 5.16: Clientzellen auf Workgroupebene

Statt einzelner Workgroups werden nun funktionale Bereiche (vgl. Abbildung 5.17) zusammengefaßt, um die Anzahl der benötigten Zellen zu minimieren. So können im FIZ einzelne Workstationverbunde etwa in eine CATIA-Zelle, eine CAE-Zelle usw. integriert werden.
Die Charakterisierung der Clientzellen erfolgt dann lediglich über die innerhalb ihres Bereichs verfügbaren Applikationen.
Sobald diese Applikationen nicht auf lokalen DCE-Ressourcen basieren, sondern lediglich auf Diensten des Rechenzentrums, haben die Zellgrenzen in Bezug auf die Nutzung überhaupt keinen Einfluß mehr.
Das Zusammenfassen mehrerer LAN-Segmente bringt darüberhinaus den Vorteil, daß nunmehr auch wieder in den Clientzellen mehrere Replikate eines Dienstes vorhanden sind, die Verfügbarkeit also wieder umfassend gewährleistet werden kann.

Hybrider Ansatz

Hierbei werden die Konzepte des funktionalen Ansatzes und das der feinkörnigen Zellstruktur geeignet kombiniert. Das Ziel hierbei ist, die funktionale Trennung von Client- und Serverrechnern zu berücksichtigen, aber gleichzeitig eine maximale Skalierbarkeit für die Dienste der Serverzelle zu erreichen.
Dies wird dadurch umgesetzt, daß ein Teil der *Utility Server* in den zentralen LAN-

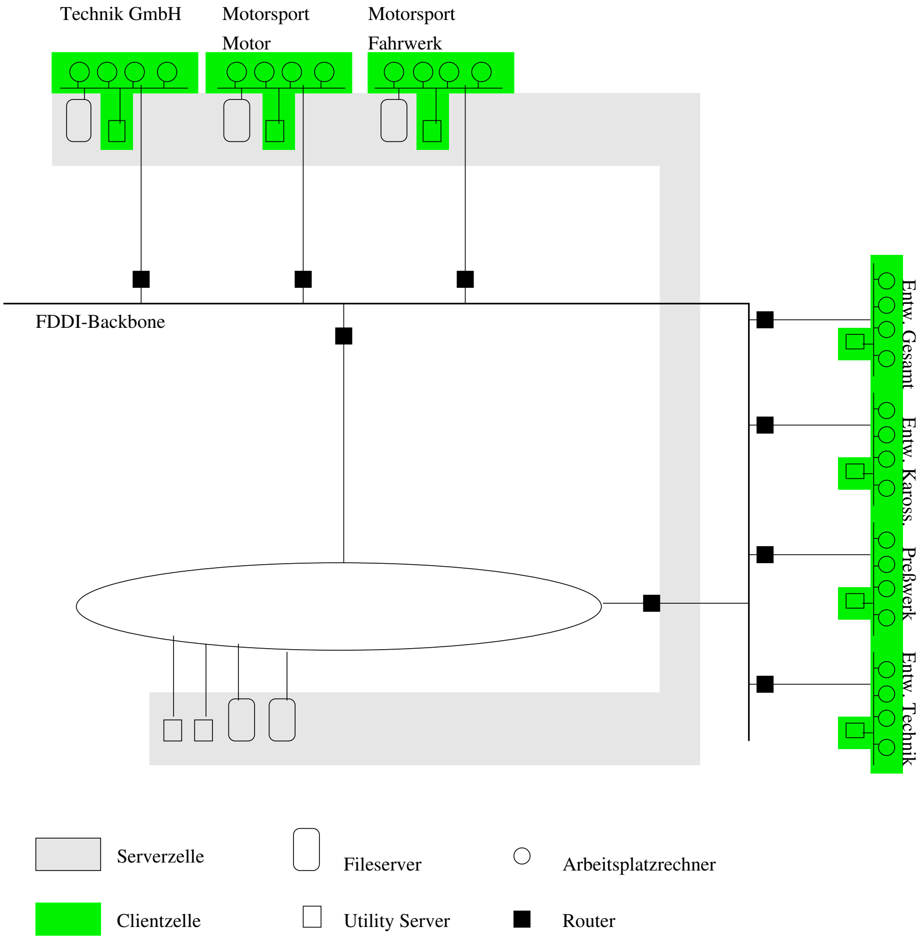


Abbildung 5.17: Funktionaler Ansatz

Segmenten des *FIZ* Dienste für die Clientzelle zur Verfügung stellt und der andere Teil Replikate der Dienste der Serverzelle trägt (vgl. Abbildung 5.18).
Damit erzielt man durch die Möglichkeiten der Replikation sowohl für die Clientzelle, als auch für die Serverzelle eine hohe Verfügbarkeit und Leistungsfähigkeit.

5.3.1.2 Die dezentralen Bereiche

Anwendung des Client/Server-Konzeptes

Im Fall der dezentralen Bereiche des *FIZ* stehen mehrere Servermaschinen zur Verfügung. Man hat also die Möglichkeit auf dem *Utility Server* die für eine Clientzelle benötigten Dienste einzurichten und auf dem *File Server* Replikate der Dienste der Serverzelle zu plazieren.
Somit wird erreicht, daß lediglich der Hintergrundverkehr eines einzigen Rechners über die WAN-Verbindung transportiert werden muß. Durch die Integration aller File Server in einer Zelle wird darüberhinaus innerhalb Münchens ein zentrales Dateisystem realisiert.
Dies schafft die Möglichkeit, die Vorteile, die die Administration einer zentralen Zelle bietet, für den gesamten administrativen Bereich zu nutzen und gleichzeitig den über die WAN-Verbindung laufenden Verkehr weitestgehend zu minimieren.

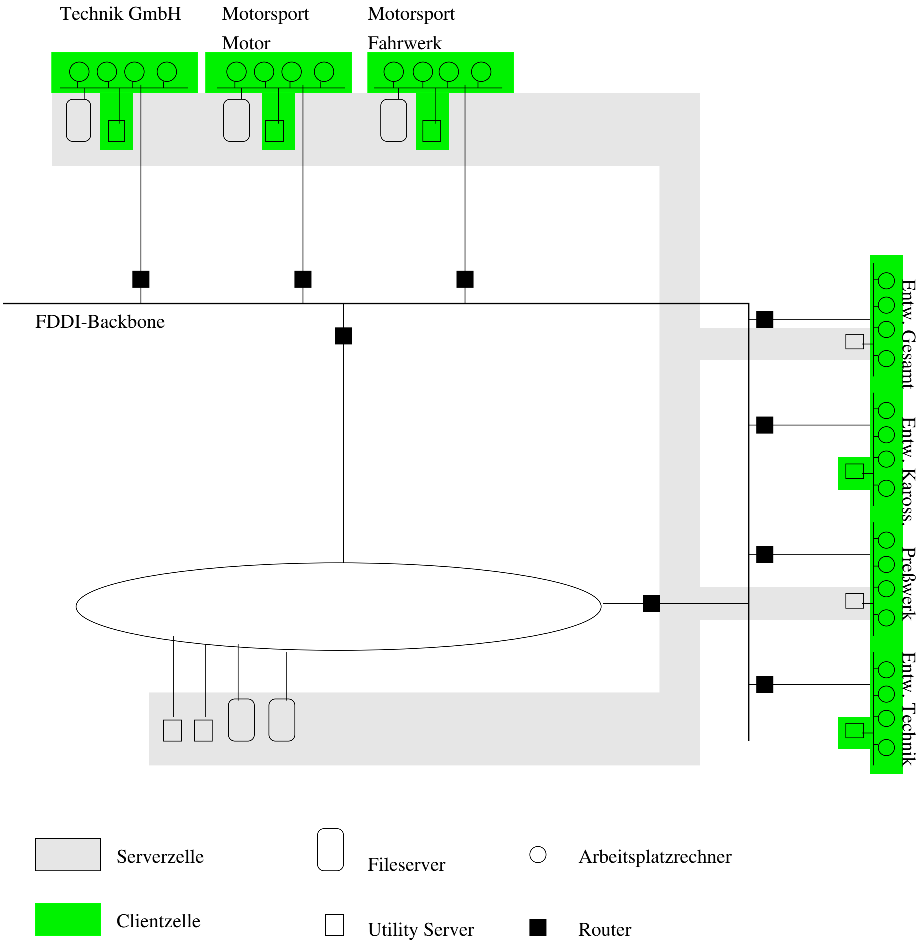


Abbildung 5.18: Hybride Struktur für eine Clientzelle

Wie auch schon im Kontext der monolithischen Zelle erwähnt, ist es bei der Wahl einer Zellstruktur zu empfehlen, das für einen Großteil eines Verbundes entwickelte Zellkonzept nach Möglichkeit auf alle Bereiche auszudehnen, um einen möglichst hohen Grad an Konsistenz für den gesamten Verbund sicherzustellen.

Errichten separater Zellen

Für die Errichtung separater Zellen in den dezentralen Bereichen spricht, daß sie organisatorisch und auch funktional weitestgehend unabhängig sind.

Das zentrale Kriterium, das hinter dem Konzept der Client/Server-Zellen steht, ist die Erweiterungsfähigkeit. Aufgrund der Autonomie der dezentralen Bereiche und der vollständigen Entflechtung von anderen Verbunden sind sie in der Lage, in einer eigenen Infrastruktur zu arbeiten.

Bei einem zentralen Managementansatz können die Zellen der dezentralen Bereiche wie Workgroupzellen behandelt werden. Die Definition der Anforderungen für die benötigten Managementkonzepte und deren Bewertung wurde bereits im Rahmen der Workgroupzellen in Abschnitt 5.2 vorgenommen.

Falls die dezentralen Bereiche in eigenen Zellen angeordnet werden sollen, so können

in diesem Fall die beiden Standorte der Motorsport GmbH innerhalb einer Zelle zusammengefaßt werden.
Bei ihrer Konfiguration sollte man wie bei einer monolithischen Zelle verfahren. Die in diesem Zusammenhang diskutierte Unterscheidung von Rechenzentrums- und Workgroup-Ressourcen läßt sich nahezu identisch auf Problematik zweier durch WANs getrennter Standorte übertragen.
Diese Wahl berücksichtigt zwar nicht den Aspekt der Verkehrsminimierung, jedoch erscheint dieses Problem bei einer Anzahl von 12 bzw. 13 Maschinen pro Standort als vernachlässigbar, wenn man bedenkt, daß lediglich Update- und Replikat-Update-Verkehr über die Verbindungen gesendet werden.

5.3.1.3 Zusammenfassung

Unter allen Anordnungsmöglichkeiten im Bereich der Client/Server-Zellen erscheint der hybride Ansatz als der geeignetste. Er soll im folgenden eingehender diskutiert werden. Für die dezentralen Bereiche wird ebenfalls der Client/Server-Ansatz verwendet, da die entsprechende Diskussion für standortbezogene Zellen bereits im Zusammenhang mit den Workgroupzellen durchgeführt wurde.

5.3.2 Kooperationsaspekte

Eine Konsequenz des hybriden Zellkonzeptes stellt die komplexe topologische Struktur der Serverzelle dar. Sie umfaßt das gesamte Rechenzentrum, einen Teil der *Utility Server* in den LAN-Segmenten des FIZ, sowie die dezentralen File Server. Somit zerfällt aus Sicht der einzelnen Teilbereiche die Menge der Replikate innerhalb der Serverzelle in günstige – d.h. innerhalb desselben Teilnetzes vorhandene – und ungünstige Replikate – d.h. Replikate, die unter Umständen an einem anderen Standort plaziert sind.
Wie im diesem Zusammengang im Rahmen der monolithischen Zelle angesprochen, muß also durch die Konfiguration der Zellstruktur sichergestellt werden, daß nach Möglichkeit Replikate innerhalb desselben Teilnetzes genutzt werden.

Bei einer monolithischen Zelle war dies über die Definition eines Suchpfades für den Namensraum der Zelle möglich (vgl. Abschnitt 5.1.3).
Im vorliegenden Fall operieren die Benutzer und die entsprechende Serverinstanz auf unterschiedlichen Zellkontexten. Die Suche nach der Serverinstanz muß also über Zellgrenzen hinweg erfolgen. Aus diesem Grund ist das Problem nicht über die Strukturierung des Suchpfades möglich, da sich dieser auf den lokalen Zellkontext beschränkt.

Die Suche im Namensraum muß also derart strukturiert werden, daß die unterschiedlichen Sichtweisen der einzelnen Clientzellen zum Ausdruck kommen. Von dieser Strukturierung sind die Instanzen des Sicherheitsdienstes und des *Fileset-Location*-Dienstes betroffen, da Instanzen beider Dienste über mehrere Standorte verteilt sind. Wie in Abschnitt A.5 erwähnt, können innerhalb spezieller Einträge des Namensraums (*RPC-Profiles*) Dienstinstanzen mit Prioritäten versehen werden. Für jeden Lokationsbereich müssen solche Einträge im Namensraum der Serverzelle erzeugt werden.

Als nächster Schritt muß sichergestellt werden, daß Anfragen stets den Eintrag des richtigen Standortes nutzen. Dies kann über die Mechanismen der Zugriffskontrolle des Verzeichnisdienstes geschehen.
Zu diesem Zweck werden die Einträge so geschützt, daß Benutzer und Dienste aus

/.../server_zelle/standort_i_profile

Dienstkennung	Dienstinstanz	Priorität
Sicherheitsdienst	lokaler Server	hoch
Fileset-Location-Dienst	lokaler Server	hoch
...	...	...
Sicherheitsdienst	entfernter Server	gering
Fileset-Location-Dienst	entfernter Server	gering

Abbildung 5.19: Beispiel eines standortbezogenen Namensraumeintrags für den Sicherheitsdienst der Serverzelle

den Clientzellen lediglich den für sie vorgesehenen Eintrag lesen können, die Einträge anderer Standorte jedoch nicht.
In einem zentralen Element, in dem alle standortbezogenen Einträge zusammengefaßt sind, erfolgt dann über die Zugriffkontrolle die Auswahl des richtigen Eintrages.

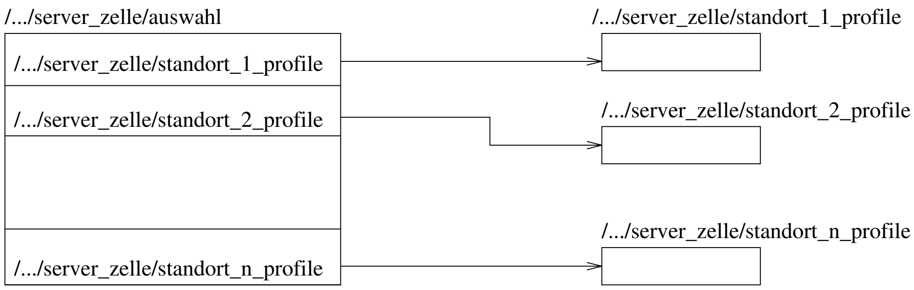


Abbildung 5.20: Auswahl des standortbezogenen Eintrags über Zugriffskontrolle

Schließlich müssen die Verweise für die Suche nach Instanzen des Sicherheitsdienstes und des *Fileset Location*-Dienstes auf den Verzeichniseintrag umgelenkt werden, in dem die Auswahl der standortbezogenen Einträge vorgenommen wird. Dieser Eintrag wird am Einstiegspunkt der Suche im Namensraum der Serverzelle vorgenommen.

5.3.3 Administration

Gerade unter dem Gesichtspunkt einer späteren Erweiterbarkeit, sollte im Zusammenhang mit der Zellstruktur eine Strategie gewählt werden, die es verhindert, daß aufgrund steigender Rechner- und Benutzerzahlen der Verwaltungsaufwand für die zentralen Betreuungsinstanzen linear wächst. Durch die weitgehende Übernahme der Konzepte des monolithischen Ansatzes werden Benutzer- und Datenverwaltung so effizient wie möglich gestaltet. Andererseits erreicht man durch die Integration der Arbeitsplatzrechner in eigene Zellen eine flexible Delegation von Verwaltungsaufgaben, ohne daß Administrationsrechte für die zentralen Bereiche abgetreten

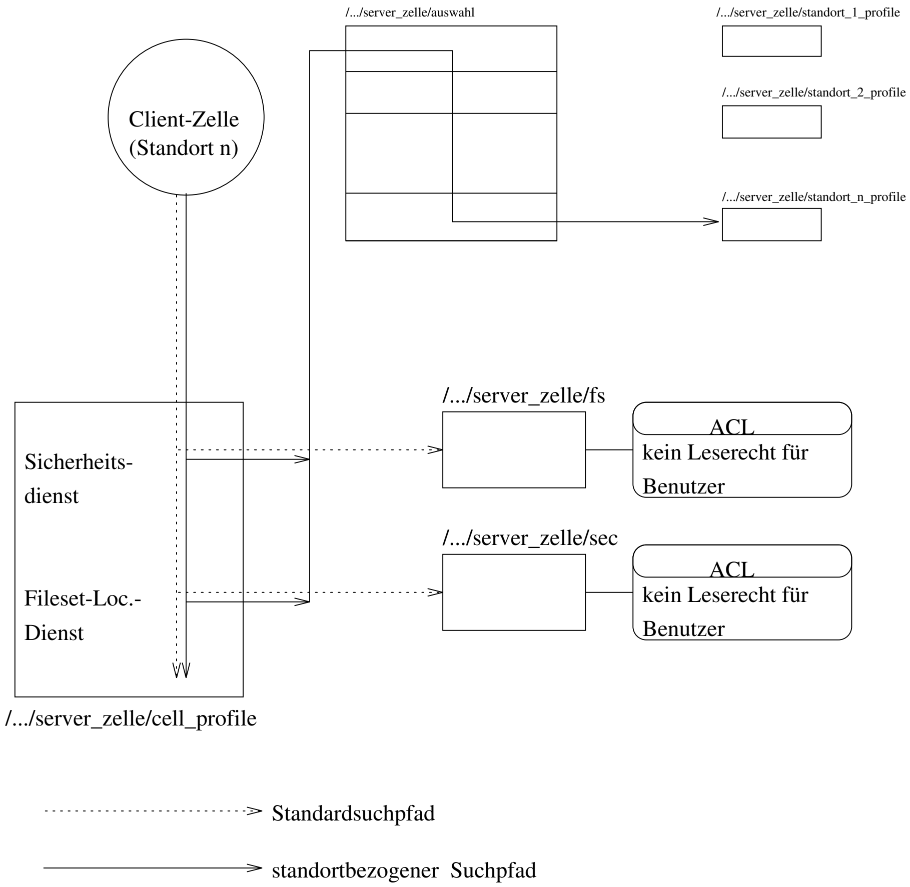


Abbildung 5.21: Umlenkung des Suchpfades

werden müssen.

5.3.3.1 Delegation von Verwaltungstätigkeiten

Durch die Struktur der Client/Server-Zellen wird eine zweistufige Form der Delegation ermöglicht:

1. Die Routineadministration der Workgroups kann über die Clientzellen delegiert werden.
2. Die Aufgabenverteilung im Bereich der zentralen Betriebsbetreuung kann entsprechend dem monolithischen Ansatz für die Serverzelle implementiert werden.

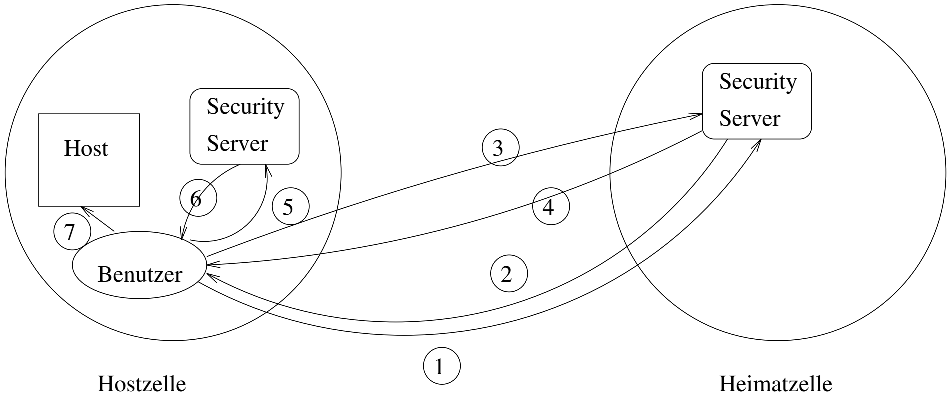
Die Serverzelle beherbergt sowohl den gesamten Datenbestand, als auch die ganze Benutzerpopulation. Die Kernaufgaben der Systemverwaltung – nämlich die Pflege des Daten-, sowie des Benutzerbestandes – bleiben also auch weiterhin unter zentraler Kontrolle.
Durch die Eingrenzung der kritischen Systeme auf die Serverzelle sind zudem eventuell auftretende Probleme leichter zu diagnostizieren und zu lokalisieren.

Die Funktionalität der Clientzellen beschränkt sich vollständig auf die Bereitstellung einer DCE-Infrastruktur für den Zugriff auf die zentralen Ressourcen. Somit besteht das Management der Clientzellen ausschließlich aus der Betriebsüberwachung. Diese kann aufgeteilt nach Verantwortungsbereich entweder von der dezentralen Betriebsbetreuung, oder aber von der Vor-Ort-Betreuung durchgeführt werden.

5.3.3.2 Benutzerverwaltung

Die flexiblen Administrationkonzepte der monolithischen Zellen haben gezeigt, daß eine zentrale Registrierung von Benutzern gerade im Bereich der Verwaltung der Zugriffskontrolle erhebliche Vereinfachungen mit sich bringt.
Diese Möglichkeiten nutzt auch die Client/Server-Struktur, da sie Benutzer lediglich in der zentralen Zelle registriert.

Hierbei wird die Tatsache genutzt, daß im Rahmen des Sicherheitsdienstes Logins auch über Zellgrenzen hinweg durchgeführt werden können.
Das bedeutet, daß sich ein Benutzer an einem Rechner einloggen kann, der nicht in der Zelle liegt, in der der Benutzer als *Principal* registriert ist.
Einzige Voraussetzung hierfür ist, daß die Sicherheitsdienste der beiden involvierten Zellen miteinander kooperieren können. Dies wird durch eine entsprechende Interzell-Kennung realisiert. Der Ablauf eines solchen zellübergreifenden Logins ist in Abbildung 5.22 dargestellt.



1. Der Benutzer authentifiziert sich gegenüber dem Sicherheitsdienst seiner Heimatzelle
2. Der Benutzer erhält sein Privilege Ticket Granting Ticket
3. Der Benutzer fordert ein Foreign Privilege Ticket Granting Ticket für die Hostzelle an
4. Der Benutzer erhält die Authentifizierungsinformation für die Hostzelle
5. Der Benutzer fordert ein Ticket für den Maschinen-Principal an
6. Der Sicherheitsdienst der Hostzelle authentifiziert den Benutzer
7. Der Benutzer authentifiziert sich gegenüber dem Maschinen-Principal und kann somit die Legitimität beider involvierter Sicherheitsdienste überprüfen

Abbildung 5.22: Ablauf eines Logins über Zellgrenzen hinweg

Bei der Benutzerverwaltung können die Ansätze, die im Zusammenhang mit der monolithischen Zelle vorgestellt wurden unmodifiziert übernommen werden.

5.3.3.3 Verwaltung der Datenbestände

Aufgrund der Tatsache, daß alle Dateiserver in der Serverzelle vereinigt sind, können auch hier die Konzepte, die im Rahmen der monolithischen Zelle diskutiert wurden, implementiert werden.

5.3.4 Sicherheit

5.3.4.1 Sicherheit auf Verbundebene

Da alle geheimen Schlüssel der Benutzer lediglich in der Serverzelle zugänglich sind, ist die Sicherheit des Verbundes ebenso, wie bei einer monolithischen Zelle zu bewerten.

Unter der Annahme, daß es einem Eindringling gelänge, die Sicherheitsmechanismen der Clientzelle außer Kraft zusetzen, hätte er Zugriff auf den Interzell-Schlüssel. Da jedoch der Intercell-Principal keine Berechtigung für ein Login besitzt, ist es nicht möglich damit Zugriff auf Ressourcen der Serverzelle zu erlangen.

5.3.4.2 Sicherheit auf Kommunikationsebene

Beim Einsatz von *Firewalls* treten bei dieser Zellstruktur dieselben Probleme wie bei einer monolithischen Zelle auf.

Vor allem in Anbetracht der Tatsache, daß Client/Server-Zellen konzeptionell auf der Kommunikation im Rahmen eines gesamten Verbundes basieren, sind die Sicherheitskonzepte aus Sicht von DCE bzw. aus Sicht des *Firewalls* nicht in Einklang zu bringen.

Ist es jedoch erforderlich *Firewalls* an Netzzugängen zu installieren, so müssen die Bereiche jenseits des Firewalls in eigenen Zellen angeordnet werden.

5.3.5 Verfügbarkeit

Die Verfügbarkeit aus der Sicht eines Benutzers wird dadurch bestimmt, ob die Zelle, in der er gerade arbeitet und die Serverzelle in Betrieb sind.
Die Verfügbarkeit der Serverzelle ist wie bei den vorherigen Ansätzen durch Replikation zu garantieren.

Da die hybride Zellstruktur auch bei der Clientzelle Replikation vorsieht, ist im Bereich des FIZ eine ähnliche Verfügbarkeit, wie bei einer monolithischen Zelle zu gewährleisten.

Für die dezentralen Bereiche sind also ebenfalls mindestens zwei Instanzen des CDS-Servers und des Security-Servers vorzusehen. Wie im Abschnitt Sicherheit erwähnt, kann die Replikation des Security-Servers der Clientzelle ohne Beeinträchtigung der Sicherheit durchgeführt werden.

5.3.6 Migration

Aufgrund der zentralen Registrierung aller Benutzer des Verbundes kann die Migration ähnlich wie beim monolithischen Ansatz durchgeführt werden. In einem ersten

Schritt wird die Zellstruktur innerhalb des Rechenzentrums aufgebaut und in der Folge die einzelnen Anwenderbereiche in die Clientzellen integriert.

5.3.7 Transparenz

Auch bei dieser Wahl der Zellstruktur ist man mit dem Problem zellokaler Kontexte konfrontiert. Diese treten jedoch nicht nur beim Zugriff auf Daten, sondern auch beim Login zutage.
Es ist nicht mehr ausreichend, sich mit seinem einfachen Principalnamen einzuloggen, sondern man muß diesem den entsprechenden Namen der Zielzelle voranstellen. Eine weitere nachteilige Eigenschaft des Logins über Zellgrenzen hinweg ist, daß den Prozessen eines Benutzers keine eindeutige *UID (UNIX-ID)* mehr zugeteilt wird. Diese Information ist jedoch für die Authentifizierung und Authorisierung eines Benutzers durch das UNIX-Betriebssystem zwingend erforderlich.

Um diesen Konflikt aufzulösen muß ein modifiziertes Loginprogramm verwendet werden. Im Rahmen von DCE existiert keine verbindliche Vorschrift, wie ein Login durchzuführen ist. Zum Standardumfang von DCE gehört aus diesem Grund lediglich ein Programm, mit dem sich ein Benutzer aus einer Shell heraus gegenüber dem Sicherheitsdienst authentifizieren kann. Um jedoch auch die Benutzerverzeichnisse in DFS halten zu können, ist es erforderlich ein integriertes Loginprogramm zu benutzen, das sowohl den Login in das lokale Betriebssystem, als auch in DCE durchführt.
Manche Hersteller haben solch ein Programm als *Value Added Tool* in ihre DCE-Produkte aufgenommen, eine einheitliche Lösung hierfür existiert jedoch nicht.
Darüberhinaus gehört der Zugriff auf einen Rechner zu den wenigen Teilbereichen von DCE, die nicht über Zugriffskontrollisten verwaltet werden können. Der Ausschluß des Zugriffs auf einen Rechner kann lediglich über eine lokale Datei benutzerbezogen konfiguriert werden.
Im Rahmen einer Kooperation zwischen IBM und dem Rechenzentrum der Universität Stuttgart [Gottschalk 94] wurde eine Loginlösung entwickelt, die als Grundlage für das Problem der Client/Server-Zellen herangezogen werden kann.

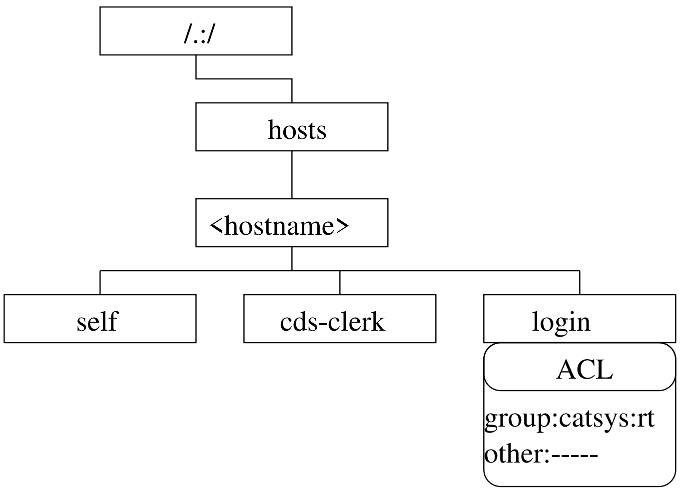


Abbildung 5.23: Zugriffskontrolle auf einen Rechner über einen speziellen CDS-Eintrag

Diese Lösung erlaubt es, nach Angabe von Principalname und Paßwort und ei-

ner Authentifizierung durch DCE zu überprüfen, ob der Zugriff auf den Rechner gewährt werden soll. Falls der Benutzer in einer fremden Zelle registriert ist, wird daraufhin sein Eintrag für das Paßwortfile aus der Benutzerdatenbank angefordert. Entspricht seine UNIX-ID keiner UNIX-ID der lokalen Benutzerdatenbank, so wird ein temporärer Eintrag mit den Daten des Benutzers in der lokalen Paßwortdatei erzeugt und der Benutzer auch in das lokalen Betriebssystems eingeloggt. Beim Ausloggen kann der entsprechende Eintrag wieder gelöscht werden.
Im Rahmen eines solchen Loginprogrammes wäre es auch möglich, eine Abbildung hierarchisch strukturierter Principalnamen in flache UNIX-Benutzernamen vorzunehmen. Die Vorteile hierarchischer Principalnamen wurden in Abschnitt 5.1.4.2 skizziert.

Alternativ kann den Benutzern zusätzlich ein Account in der Clientzelle eingerichtet werden.
Bei diesem Ansatz loggt sich der Benutzer zunächst in seinen lokalen Account ein und authentifiziert sich anschließend gegenüber der Serverzelle mit seinem zentralen Account. Bei diesem Schritt werden dann lediglich die DCE-Informationen modifiziert, der lokale Betriebssystemkontext des Benutzers bleibt davon unberührt.

5.3.8 Änderungsflexibilität

5.3.8.1 Reaktion auf organisatorische Veränderungen

Ähnlich wie die monolithische Zellstruktur bestehen bei der hybriden Client/Server-Zelle keine Abhängigkeiten zu den einzelnen Abteilungsgrenzen. Das zentrale Registrieren der Benutzer macht eine Verlagerung von Benutzern zwischen Zellen ohnehin überflüssig.

5.3.8.2 Reaktion auf Konfigurationänderungen

Im wesentlichen gilt hier dasselbe, wie bei monolithischen Zellen, da wahrscheinlich lediglich Arbeitsplatzrechner innerhalb einer Clientzelle verlagert werden.
Werden Server innerhalb einer Zelle verlagert, so gelten ebenfalls die Richtlinien der monolithischen Zelle.

Sollten jedoch Server zwischen Zellen verlagert werden, so ist, wie in Abschnitt 5.2.8.2 erwähnt, eine Neukonfiguration unumgänglich.

5.3.8.3 Reaktion auf Performanceengpässe

Die Client/Server-Zellen sind konzeptionell auf eine möglichst gute Lastverteilung ausgelegt. Im Gegensatz zur monolithischen Zelle hat die Serverzelle lediglich die Aufträge von Benutzern zu bearbeiten. Die durch die Maschinen hervorgerufene Last wird in den Clientzellen gehalten.
Darüberhinaus bietet das hybride Modell auch die Möglichkeit Replikate der Dienste aus der Serverzelle dezentral zur Verfügung zu stellen.

Die Struktur der Clientzelle hat zudem keinen Einfluß auf die Funktionalität der gesamten Zellstruktur. Es ist deshalb möglich, sie zu teilen, falls es zu Engpässen kommen sollte.

5.3.8.4 Integration anderer Verbunde

Auch die Integration mit anderen Verbunden kann relativ nahtlos geschehen. Die dahinterstehende Konzeption ist, eine zentrale Zelle als umfassenden Server für die unterschiedlichsten Clients (das sind in diesem Fall Clientzellen) zur Verfügung zu stellen.
Voraussetzung ist jedoch, daß die entsprechenden Verbunde ähnlich strukturiert sind, d.h. sich aus Rechenzentrums- und Workgroup-Ressourcen zusammensetzen.

5.3.9 Skalierbarkeit

Das vorrangige Entwurfsziel dieser Zellstruktur war es, einen möglichst hohen Grad an Skalierbarkeit, vor allem für große Verbunde, zu gewährleisten.
Durch die Entflechtung von Maschinen- und Benutzerskalierbarkeit ist es gelungen, den Hintergrundverkehr innerhalb der Serverzelle vollständig zu minimieren und die Hintergrundlast der Dienste in der Serverzelle klein zu halten.
Der feinkörnige und der hybride Ansatz erlauben zudem durch den Einsatz von Replikation eine hohe Skalierbarkeit im Bereich der Dienste.

Die Benutzerskalierbarkeit im Rahmen des Sicherheitsdienstes erscheint wesentlich unproblematischer, da von Benutzerseite kaum Änderungen an der Datenbank durchgeführt werden und die Häufigkeit, mit der Logins durchgeführt, oder *Tickets* angefordert werden relativ gering ist; die beiden Letzteren können zudem von Replikaten bearbeitet werden.
Unter Berücksichtigung dieser Tatsachen scheint es möglich, auch sehr große Benutzerpopulationen (am *Center for Information Technology Integration (CITI)* wurde sogar gezeigt [CITI 94-1], daß die Datenbank des Sicherheitsdienstes auch bei einer Größe von 50000 Einträgen nutzbar bleibt) innerhalb einer Zelle zu registrieren.

Ein weiterer wichtiger Aspekt im Rahmen der Skalierbarkeit ist, wie einfach das Performanceverhalten bei der Erhöhung von Systemparametern (Maschinen, Benutzer, etc.) vorausgesagt werden kann. Da sich jedoch im Fall der Client/Server-Zellen der einzige leistungsbezogene Parameter die Anzahl der gleichzeitigen Benutzer ist, kann man mit relativ einfachen Mitteln die Bedarfgrößen für neue Replikate, oder den Ausbau von Servern ermitteln.

In administrativer Hinsicht ist aufgrund des äquivalenten Administrationskonzeptes eine ebenso hohe Skalierbarkeit wie bei einer monolithischen Zelle gegeben.

5.3.10 Leistungsaspekte

Die Client/Server-Zellen trennen durch ihren Aufbau die Lastanteile, die durch Benutzer erzeugt werden, von denen, die durch den Hintergrundverkehr der DCE-Dienste hervorgerufen werden. Dies wird durch die Begrenzung des Hintergrundverkehr auf die Clientzellen erreicht.
Durch diese Maßnahme werden die Serverinstanzen im Rechenzentrum entlastet, können also eine größere Anzahl von Benutzeranfragen bearbeiten. Dadurch wird die im Vergleich zur monolithischen Zelle geringere Anzahl von Replikaten kompensiert.
Wie bei jeder Mehrzellstruktur erhöht sich jedoch bei initialen Aufrufen von Diensten in der Serverzelle der Interaktionsaufwand mit den Basisdiensten. Davon ist in er-

ster Linie die Suche nach Dienstinstanzen der Serverzelle betroffen. Da jedoch die Ergebnisse dieser Suchoperationen lokal zwischengespeichert werden, ist im Laufe einer Sitzung mit keinen Verzögerungen zu rechnen.

5.4 Zusammenfassung der Ergebnisse

Die Diskussion unterschiedlicher Ansätze für die Zellstrukturierung hat gezeigt, daß trotz eines präzise definierten Szenarios eine Vielfalt von möglichen Lösungen existiert.
Dabei unterscheiden sich die verschiedenen Ansätze im wesentlichen nur durch die Effizienz, mit der die Anforderungen an eine DCE-Infrastruktur umgesetzt werden konnten.
Auf der anderen Seite decken die vorgestellten Modelle nahezu vollständig die Strukturierungsmöglichkeiten im Rahmen der Zellstrukturen ab. Gerade die Client/Server-Zellen zeigen, wie durch geeignete Kombination zentraler Zellkonzepte und Mehrzell-Konzepte Alternativen für die Anordnung verteilter Verbunde in Zellen abgeleitet werden können.

Mit den vorgestellten Zellkonzepten wird einer großer Bereich von Alternativen bei der Einteilung eines Verbundes in Zellen berücksichtigt. Um die Analyse der unterschiedlichen Ansätze so übersichtlich wie möglich zu gestalten, wurde darauf verzichtet, näher auf die Kombination unterschiedlicher Zellkonzepte innerhalb eines Szenarios einzugehen.
In der Regel wird jedoch eine sinnvolle Kombination aller Konzepte zu einer geeigneten Lösung für eine konkrete Problemstellung führen.
Zentrale Bedeutung haben dabei die in Kapitel 3 vorgestellte Entwurfs- und Zielkriterien. Die Analyse unterschiedlicher Zellstrukturen hat bestätigt, daß diese Kriterien stets als Grundlage für die Strukturierung eines Verbundes herangezogen werden müssen.
Die Planung konkreter Zellstrukturen erfordert also in erster Linie eine Auseinandersetzung mit diesen Kriterien.

Für eine abschließende Beurteilung der erhaltenen Ergebnisse ist es erforderlich, anhand der Strukturierungskriterien eine Bewertung zwischen den unterschiedlichen Zellstrukturen vorzunehmen. Gerade in Hinblick auf eine erweiterte Fragestellung, z.B. der Anwendung der Resultate auf andere Szenarien, müssen Vor- und Nachteile der einzelnen Ansätze einander vergleichend gegenüber gestellt werden.

Zu diesem Zweck ist jedoch zuerst eine Strukturierung bzw. Kategorisierung und fallspezische Gewichtung der einzelnen Kriterien vorzunehmen.
Die Kriterien können entsprechend der Abbildung 3.2 in unterschiedliche Teilbereiche gegliedert werden, die den Sichtweisen auf einen verteilten Verbund folgen:

- Anforderungen, die durch die Infrastruktur implizit gegeben sind
- Anforderungen, die von Betreiberseite bestehen
- Anforderungen aus Benutzersicht
- Beschränkungen der Funktionalität von DCE

Infrastrukturelle Anforderungen

Anzahl und topologische Verteilung der Ressourcen haben einen großen Einfluß auf konkrete Zellstrukturen. Teilaspekte dieser Problematik werden von den einzelnen Zellansätzen sehr unterschiedlich behandelt. Diese Unterschiede manifestieren sich vor allem in der Art und Weise, wie sich der DCE-spezifische Hintergrundverkehr verteilt , in der Größe sinnvoll unterstützbarer Umgebungen und wie effizient bei einer komplexen Netzstruktur die Dienstevermittlung realisiert werden kann.

Monolithische Zellen berücksichtigen kaum die speziellen infrastrukturellen Gegebenheiten einer verteilten Umgebung, da sie aufgrund ihrer Konzeption versuchen, die gesamte Infrastruktur in einer Zelle zusammenzufassen. Zwar ist es möglich, durch geeignete Plazierung und Replikation der Dienstinstanzen einen Teil des Verkehrs auf die lokalen Netzbereiche zu begrenzen. Gewisse Anteile des Hintergrundverkehrs, sowie der gesamte Update- und Replikat-Update-Verkehr müssen jedoch zwischen den einzelnen Teilnetzen abgewickelt werden.
Zudem ist unklar, wie weit sich monolithische Zellen bezüglich der Anzahl von Maschinen und gleichzeitigen Benutzer skalieren lassen.

Im Gegensatz zu monolithischen Zellen sind die Workgroup-Zellen vollständig nach der Netzstruktur ausgerichtet. Innerhalb einer Workgroup-Zelle werden lediglich lokale Netzbereiche zusammengefaßt. Nichtlokaler Netzverkehr wird deshalb nur erzeugt, wenn auf eine Ressourcen in einer fremden Zelle zugegriffen wird. Aufgrund der starken Partitionierung der gesamten Infrastruktur lassen sich technisch auch sehr große Verbunde unterstützen.

Anders als beim monolithischen und Workgroup-Ansatz setzen Client/Server-Zellen eine spezielle Infrastruktur voraus. Sie basieren auf einer strikten Trennung zwischen lokalen und zentralen Ressourcen. Dieses Zellkonzept ist besonders auf die Nutzung zentraler Ressourcen abgestimmt.
So ist es etwa nicht möglich, eine Umgebung, die aus einer Vielzahl privater File Server (d.h. Arbeitsplatzrechner, die eigene Dateibestände verwalten) bestehen, nach dem Prinzip der Client/Server-Zellen zu strukturieren, da in diesem Fall die Zellstruktur zu einer monolithischen Zelle entarten würde.
Zudem ist eine Client/Server-Struktur auf Verbunde ausgerichtet, die aus Leistungsgründen nicht mehr durch monolithische Zellstrukturen unterstützt werden können, da ihre Skalierbarkeit lediglich durch einen Parameter – der Anzahl gleichzeitiger Benutzer – bestimmt ist.

Aus Sicht der Verkehrsminimierung sind die Client/Server-Zellen zwischen den beiden anderen Ansätzen anzusiedeln. Zum einen begrenzen sie den Hintergrundverkehr durch den Einsatz der Client-Zellen, zum anderen ermöglichen sie eine Replikation der Dienste der Serverzelle in den Netzsegmenten der Client-Zellen, was dazu dient, auch wesentliche Teile des Lookup-Verkehrs auf die lokalen Netzbereiche zu beschränken. Die Anzahl der Replikate der Serverzelle kann dabei so variiert werden, daß eine möglichst geringe Netzbelastung und ein möglichst gutes Antwortzeitverhalten garantiert werden kann.

Die Diskussion der Client/Server-Zellen hat jedoch gezeigt, daß die Dienstevermittlung in komplex strukturierten Netzverbunden extrem kompliziert ist. Für einen möglichst effizienten Einsatz der Client/Server-Zellen sollte die Menge der Dienstinstanzen aus möglichst gleichwertigen Elementen bestehen, d.h. die Bearbeitungsdauer sollte relativ unabhängig von der jeweils gewählten Dienstinstanz und der Lage des entsprechenden Clients sein. Ist dies der Fall, so kann auf die aufwendige Strukturierung des Suchpfades (siehe Abschnitt 5.3.2) verzichtet werden.

Anforderungen aus Betreibersicht

Im Zentrum jeder Diskussion einer Zellstruktur stand stets, wie effizient sich die administrativen Anforderungen im Rahmen der jeweiligen Zellstruktur realisieren lassen.
Gerade bei großen Verbunden, die von einer einzigen Organisation betrieben werden sollen, ist den administrativen Anforderungen der größte Stellenwert beim Entwurf von Zellstrukturen einzuräumen, da eine effiziente Verwaltung Grundvoraussetzung für einen erfolgreichen Betrieb verteilter Umgebungen darstellt.

Ein zentrales Ergebnis bei der Umsetzung administrativer Konzepte war bei allen Untersuchungen, daß eine Zelle stets genau einer Betreiberorganisation zugeordnet sein sollte. Desweiteren hat die Analyse der Alternativen gezeigt, daß einheitliche administrative Bereiche auch geeignet durch Mehrzellstrukturen darstellbar sind.
Alle drei Ansätze verwendeten dabei äquivalente Mechanismen zur Realisierung der Anforderungen:

- Domänenbildung:
  Eine Strukturierung der Umgebung wurde über die Definition von Zellgrenzen und die Substrukturierung der Namensräume vorgenommen.

- Definition von Rollen:
  Unterschiedliche Rollen wurden über spezielle Administratorgruppen realisiert. Die Zuordnung zwischen Rollen und administrativen Bereichen wurde dabei über die Mechanismen der Zugriffkontrolle (ACLs) umgesetzt.

Die Strukturierung des Managements kann dabei entsprechend der in Abschnitt 3.2.1 beschriebenen Organisationsformen erfolgen.
Im Vergleich der unterschiedlichen Ansätze hat sich jedoch herausgestellt, daß der Verwaltungsaufwand umso größer ist, je größer die Anzahl der Zellen ist.
Zwar besteht die Möglichkeit, selbst Workgroup-Zellen mit zentralen, bzw hierarchischen Managementkonzepten zu betreiben, der Aufwand hierfür ist jedoch wesentlich größer als im Fall der monolithischen bzw. der Client/Server-Zellen.

Neben diesen organisatorischen Aspekten unterscheiden sich die unterschiedlichen Ansätze auch hinsichtlich der Dienstgüteparameter.

Sicherheit

Wie in Abschnitt 3.4 beschrieben, sind drei Aspekte der Sicherheit, nämlich Sicherheit auf Verbund-, Rechner- und Kommunikationsebene zu differenzieren.
Auf Verbund-, bzw. Rechnerebene kann beim Workgroup-Ansatz nur eine geringeres Maß an Sicherheit garantiert werden, da die Rechner, die die Benutzerdatenbank verwalten nicht gegen allgemeinen Benutzerzugriff geschützt werden können.
Auf Kommunikationsebene können nur Firewalls als geeignetes Werkzeug eingesetzt werden. Dabei ist es unter dem Aspekt der Sicherheit nicht sinnvoll, Zellen so zu dimensionieren, daß ihre Grenzen über die durch Firewalls bestimmten Sicherheitsdomänen hinausreichen.

Verfügbarkeit

Die Unterschiede in der Verfügbarkeit der einzelnen Zellstrukturen werden durch die Fähigkeit Replikation auch in den einzelnen Anwenderbereichen einzusetzen

bestimmt. Die Konsequenzen, die Netzstörungen oder der Ausfall eines File-Servers nach sich ziehen, sind in allen Fällen nahezu identisch.
Bei der Verfügbarkeit schneiden monolithische, bzw. Client/Server-Zellen aufgrund der größeren Replikationsmöglichkeiten besser ab als die Workgroup-Zellen.

Änderungsflexibilität

Problematisch stellen sich bei allen Ansätzen Konfigurationsänderungen dar, besonders wenn von diesen Änderungen Serverrechner betroffen sind.
Grundsätzlich sollte vermieden werden, die wichtigsten Teile einer Zelle – dies sind in erster Linie die Masterreplikate der Dienste – zwischen Rechnern zu verlagern.

Skalierbarkeit

Aus administrativer Sicht wird die Skalierbarkeit durch zwei Parameter bestimmt. Zum einen ist dies die Menge von Maschinen, Benutzern und Daten, zum anderen die Anzahl der Zellen. Aus diesem Grund sollte die Anzahl der Zellen innerhalb eines Bereiches minimiert werden.
Demgegenüber steht jedoch die Skalierbarkeit im Leistungsbereich. Hierbei kann es bei großen Verbunden erforderlich sein, mehrere Zellen zu konfigurieren.

Die Analyse der unterschiedlichen Zellstrukturen hat dabei gezeigt, daß administrative und leistungsbezogene Skalierbarkeit in unmittelbarer Konkurrenz stehen.
Monolithische Zellen besitzen eine obere Schranke im Leistungsbereich, wohingegen der Verwaltungsaufwand bei Workgroup-Zellen bei einer steigenden Zellanzahl immer größer wird.
Auch hier versuchen die Client/Server-Zellen Abhilfe zu schaffen, indem sie die produktiven und damit verwaltungsintensiven Teile eines Verbundes in einer Serverzelle zusammenfassen und auf der anderen Seite die Arbeitsplatzrechner in eigenen Zellen anordnen. Somit wird die Hintergrundlast in der Serverzelle reduziert und eine weitreichende Skalierbarkeit im Leistungs- und Administrationsbereich ermöglicht.

Leistungsfähigkeit

Die Leistungsfähigkeit einer Zellstruktur hängt vor allem von der Fähigkeit ab, durch die Replikation der Basisdienste einen Lastausgleich zwischen unterschiedlichen Rechnern bzw. Teilnetzen vorzunehmen. Replikate der Dienste sollten deshalb möglichst in den lokalen Netzen plaziert werden. Bei monolithischen und Client/Server-Zellen wurden deshalb auf den Workgroup-Servern Instanzen der wichtigsten Dienste eingerichtet.
Im Rahmen der Workgroup-Zellen wurde auf diese Replikation verzichtet, da lediglich Dateizugriffe Last in der Rechenzentrumszelle erzeugen.
Aufgrund der speziellen Anwendungscharakteristik wirken sich jedoch mögliche Verzögerungen bei der Interaktion mit den Basisdiensten der Rechenzentrumszelle beim Laden einer CAD-Zeichnung nicht wesentlich aus.

Anforderungen aus Benutzersicht

Für einen Benutzer ist es entscheidend, daß er während seiner Arbeit nicht durch Betriebsstörungen unterbrochen wird. Desweiteren muß sichergestellt sein, daß er

seine Aufgaben möglichst effizient erfüllen kann.
Eine Zellstruktur muß sich also aus Benutzersicht vorrangig durch Verfügbarkeit, Leistungsfähigkeit und Transparenz auszeichnen.

Am einfachsten ist Transparenz stets bei monolithischen Zellen sicherzustellen, da die Sicht auf den Verbund zellweit einheitlich ist.
Doch auch bei Mehrzellstrukturen läßt sich durch geeignete Maßnahmen (vgl. Abschnitt 5.2.7) eine einheitliche Sicht, zumindest auf das verbundweite Dateisystem herstellen.
Eine weitere wichtige Transparenzeigenschaft stellt ein einheitliches, in einem Schritt ausgeführtes Login (*single sign on*) dar. Ein integriertes Loginprogramm, welches einen Benutzer zugleich gegenüber DCE und dem lokalen Betriebssystem authentifiziert, ist zudem erforderlich, wenn die Benutzerverzeichnisse (*Home Directories*) in DFS liegen sollen.

Funktionale Restriktionen

Die Gestaltungsfreiheit bei der Wahl von Zellstrukturen kann dadurch eingeschränkt werden, daß zur Erfüllung gewisser Aufgaben eine Funktionalität benötigt wird, die aufgrund der Architektur von DCE nur in bestimmten Zellstrukturen genutzt werden kann.

Bestimmte Mechanismen von DCE lassen sich dabei in Mehrzellstrukturen entweder gar nicht, oder nur unter erhöhtem Aufwand nutzen.
An erster Stelle sind hierbei gewisse Teilbereiche des *Distributed File Systems* zu nennen. So sind die Möglichkeiten des Datenmanagements vollständig auf den Kontext einer Zelle begrenzt.
Filesets können weder zwischen Zellen verschoben werden, noch ist es möglich, den Replikationsmechanismus über Zellgrenzen hinweg zu nutzen.
Die gravierendste Restriktion ist jedoch, daß das Backup-System lediglich innerhalb einer Zelle eingesetzt werden kann.

Eine weitere Problematik stellt das Management der Zugriffskontrolle über Zellgrenzen hinweg dar. Aus Effizienzgründen ist es gerade bei großen Verbunden erforderlich, Zugriffsrechte auf Ressourcen gruppenbezogen vergeben zu können. Die Kontrolle des Zugriffs kann bei dieser Lösung zentral durchgeführt werden, da lediglich über die Zugehörigkeit zu einer Gruppe einem Benutzer die nötigen Rechte zur Nutzung einer gewissen Menge von Ressourcen gewährt werden kann. Die Menge der Ressourcen kann somit in gewisse Klassen eingeteilt und der Zugriff auf einzelne Klassen über Gruppen organisiert werden.
Es ist jedoch erst ab DCE Version 1.2 geplant, Benutzer aus fremden Zellen in Gruppen der lokalen Zelle registrieren zu können.
Benutzerpopulationen, die eine logische Einheit bilden, jedoch über mehrere Zellen verteilt sind, erschweren also erheblich das Management der Zugriffskontrolle. Eine Zellstruktur sollte deshalb stets daraufhin ausgelegt sein, Benutzer, die innerhalb desselben Projektes arbeiten auch innerhalb einer Zelle zusammenzufassen.

Kapitel 6

Empfehlung für die Zellstrukturierung des CATIA-Verbundes

Die zentrale Herausforderung bei der Einteilung des CATIA-Verbundes in Zellen stellt die große Anzahl von Maschinen und Benutzern dar. Nach Abschluß der Migration müssen etwa 600 Rechner durch die DCE-Infrastruktur unterstützt werden. Hierbei muß durch die Zellstruktur sichergestellt werden, daß sich der Verbund effizient nutzen und betreiben läßt.

Aufgrund der Tatsache, daß für die Skalierbarkeitsgrenze im Bereich der Leistung von Zellen keine Referenzen existieren, erscheint es sinnvoll, sich im Bereich von München für den Ansatz der Client/Server-Zellen zu entscheiden, da er sich durch eine größte Skalierbarkeit sowohl im Leistungs- als auch im Administrationsbereich auszeichnet.

Eine Alternative, die Last einer DCE-Infrastruktur zu verteilen bietet der Workgroup-Ansatz, jedoch hat der zusammenfassende Vergleich aller Zellstrukturen gezeigt, daß die Struktur der Workgroup-Zellen aufgrund ihrer Komplexität im Bereich des Managements für große Verbunde ungeeignet ist. Alleine der erste Migrationsschritt würde eine Struktur aus 8 Zellen umfassen. Berücksichtigt man darüberhinaus die Tatsache, daß sich im Bereich des FIZ der CATIA-Verbund nach Abschluß der Migration über etwa 30 LAN-Segmente erstreckt, so ist die Komplexität der entstehenden Workgroup-Zellstruktur nicht mehr beherrschbar.

Gerade in Zusammenhang mit der Integration des CATIA- und des CAE-Verbundes und der weiteren Migration von CATIA-Anwenderbereichen ist es von herausragender Bedeutung, daß sich diese Teilbereiche nahtlos in eine existierende DCE-Infrastruktur einbetten lassen.
Darüberhinaus gilt es zu berücksichtigen, daß all diese Anwenderbereiche des FIZ von einer zentralen Betreiberorganisation verwaltet werden. Da sich die Aufgabenstruktur für alle Anwenderbereiche ähnelt, kann also durch die Zusammenfassung aller Serverressourcen innerhalb einer Zelle des Rechenzentrums ein wesentlicher Beitrag für ein effizientes Management aller zentralen Ressourcen geleistet werden.

Somit können mit einer *Datacenter*-Zelle – also einer Zelle, die die Serverressourcen für alle Anwenderbereiche bündelt – und mehreren Client-Zellen viele Teilaspekte des Szenarios abgedeckt werden:

- Alle zentralen Ressourcen können zentral verwaltet und einem großen Kreis von Benutzern erschlossen werden.
  Diese Benutzer können zudem alle innerhalb einer Zelle registriert werden. Benutzer, die sowohl den CATIA- als auch dem CAE-Verbund zugeordnet sind, benötigen demzufolge nur noch eine Benutzerkennung.
  Auf welche Teile des zentralen Bereichs ein Benutzer zugreifen kann, ist über die Zugriffskontrolle innerhalb der Serverzelle zu regeln.

- Durch multifunktionale Arbeitsplätze soll ein möglichst transparentes Arbeiten in den Anwenderbereichen unterstützt werden. Durch das Zusammenfassen aller Serverbereiche innerhalb einer Zelle steht den multifunktionalen Arbeitsplätzen eine ebenfalls multifunktionale *Datacenter*-Zelle zur Verfügung. Die Benutzer können also von jedem Arbeitsplatz transparent auf die von ihnen benötigten Daten zugreifen.
  Für eine effiziente Nutzung der zentralen DCE-Dienste in den Anwenderbereichen werden darüberhinaus Replikate der Basisdienste der Serverzelle auf Abteilungsservern der zentralen LAN-Segmente angeboten.

- Im Zusammenhang mit DCE beschränkt sich die Administration der in den Clientzellen zusammengefaßten Anwenderbereiche auf die Betriebsüberwachung. Die Trennung der Umgebung in Client-Zellen und eine Server-Zelle reflektiert also auch die Aufgabenverteilung im Rahmen der Betriebsbetreuung, da die Zellstruktur das Rechenzentrum und die Anwenderbereiche in unterschiedlichen Zellkontexten verwaltet.

- Client-Zellen können frei strukturiert werden. Für die Sicht auf die gesamte Infrastruktur spielt es keine Rolle, wie viele Client-Zellen errichtet werden. Grundsätzlich sollte jedoch die Anzahl der Client-Zellen so gering wie möglich gehalten werden, um den Aufwand für die Verwaltung der Client-Zellen zu minimieren. Von der unabhängigen Strukturierbarkeit sollte lediglich dann Gebrauch gemacht werden, wenn sich Leistungsengpässe in den errichteten Client-Zellen abzeichnen.

Für die Bereiche außerhalb Münchens sind aufgrund der geringeren Bandbreite separate Zellen zu errichten. Da diese Bereiche auch von eigenen Betreiberorganisationen verwaltet werden, findet hiermit auch eine klare Abgrenzung der administrativen Zuständigkeiten statt.
Eine Kooperation mit den Bereichen innerhalb Münchens kann mit den Möglichkeiten der Interzell-Kommunikation realisiert werden. Die dafür notwendigen Interzell-Schlüssel müssen nur zwischen den dezentralen Zellen und der Serverzelle ausgetauscht werden, da die Kooperation zwischen den unterschiedlichen Standorten lediglich auf dem Austausch von Dateien beruht, der alleine über die Serverzelle abgewickelt werden kann.

Weniger eindeutig stellt sich die Lage bei den dezentralen Standorten innerhalb Münchens dar.
In diesem Zusammenhang muß also diskutiert werden, wie mit den Bereichen der Technik und Motorsport GmbH zu verfahren ist, die zwar organisatorisch und funktional unabhängige Bereiche darstellen, jedoch innerhalb des Administrationsbereiches der zentralen Betriebsbetreuung liegen.

In diesem Zusammenhang gilt es zu berücksichtigen, daß nur in begrenztem Umfang Kooperation zwischen der Technik und Motorsport GmbH und dem FIZ stattfindet.

Es bieten sich also zwei nahezu gleichwertige Strukturierungsalternativen an:

1. Die Ausgliederung der dezentralen Standorte aus dem Zellverbund des FIZ. Hierbei wäre für die Technik und die Motorsport GmbH jeweils eine Zelle zu errichten. Die Konsequenzen dieser Alternative sind:
   - Durch die Ausgliederung würden innerhalb der Server-Zelle, die nun auf das FIZ beschränkt ist, bezüglich des Antwortzeitverhaltens nahezu gleichwertige Dienstinstanzen vorliegen. Von einer komplexen Konfiguration der Dienstevermittlung könnte also abgesehen werden.
   - Der Workgroup-Ansatz hat demonstriert, daß ein zentrales Management auch über Zellgrenzen hinweg möglich ist. Da es sich im vorliegenden Fall nur um zwei Zellen handelt, die auf diese Art verwaltet werden müßten, ist der entstehende Mehraufwand jedoch gering.
   - Das Backup der dezentralen Fileserver kann nicht mehr mit den Mechanismen von DFS durchgeführt werden, da sich File- und Backup-Server in unterschiedlichen Zellen befinden.
     Eine Organisation der dezentralen Bereiche in separaten Zellen würde also dazu führen, daß für die dezentralen Bereiche eine rechnerbezogene Backup-Lösung verwendet werden müßte. In diesem Fall könnte man für die dezentralen Bereiche Teile der Funktionalität von DFS nicht mehr nutzen. So wäre es in diesem Fall nicht möglich, *Filesets* im laufenden Betrieb zu verlagern, oder Replikate von *Filesets* zu erzeugen.
2. Die Integration in den Zellverbund. Hierbei würden die dezentralen File Server in die Server-Zelle integriert werden und standortbezogen Client-Zellen errichtet werden. Diese Lösung hat zur Folge, daß
   - das Backup für alle Bereiche mit den Werkzeugen von DFS durchgeführt werden kann
   - die komplexe Konfiguration der standortbezogenen Suchpfade realisiert werden müßte.

Aus administrativer Sicht gilt es also abzuwägen, ob für die einfachere Form der Dienstevermittlung eine Backup-Strategie mit DFS für die dezentralen Bereiche aufgegeben werden soll oder umgekehrt.

Berücksichtigt man die organisatorischen und funktionalen Eigenständigkeit der dezentralen Standorte, so liegt es nahe, die Technik und Motorsport GmbH in jeweils einer Zelle zusammenzufassen. Durch diese Maßnahme wird einerseits die Netzbelastung der WAN-Verbindungen reduziert und andererseits eine komplexe Konfiguration der Dienstevermittlung überflüssig.
Ein wichtiges Argument für die Integration beider Standorte der Motorsport GmbH in eine Zelle stellt die relativ geringe Anzahl an Maschinen dar. Aufgrund dieser Tatsache wäre eine zellbezogene Trennung mit einem unverhältnismäßigen Mehraufwand im administrativen Bereich verbunden.
Für die in diesem Zusammenhang nötige Form der Dienstvermittlung kann auf die wesentlich einfacheren Mechanismen einer monolithischen Zelle zurückgegriffen werden.

Es sie an dieser Stelle noch einmal ausdrücklich erwähnt, daß auch bei dieser Lösung weiterhin ein zentrales Backup möglich ist. Dies kann durch gängige Backup-Werkzeuge realisiert werden. Der Unterschied zur Backup-Lösung von DFS besteht lediglich darin, daß das Backup nicht mehr den gesamten Dateiraum einer Zelle, sondern lediglich den Dateiraum eines Fileservers umfaßt.

Die vorgeschlagene Zellstruktur hat demnach folgendes Aussehen:

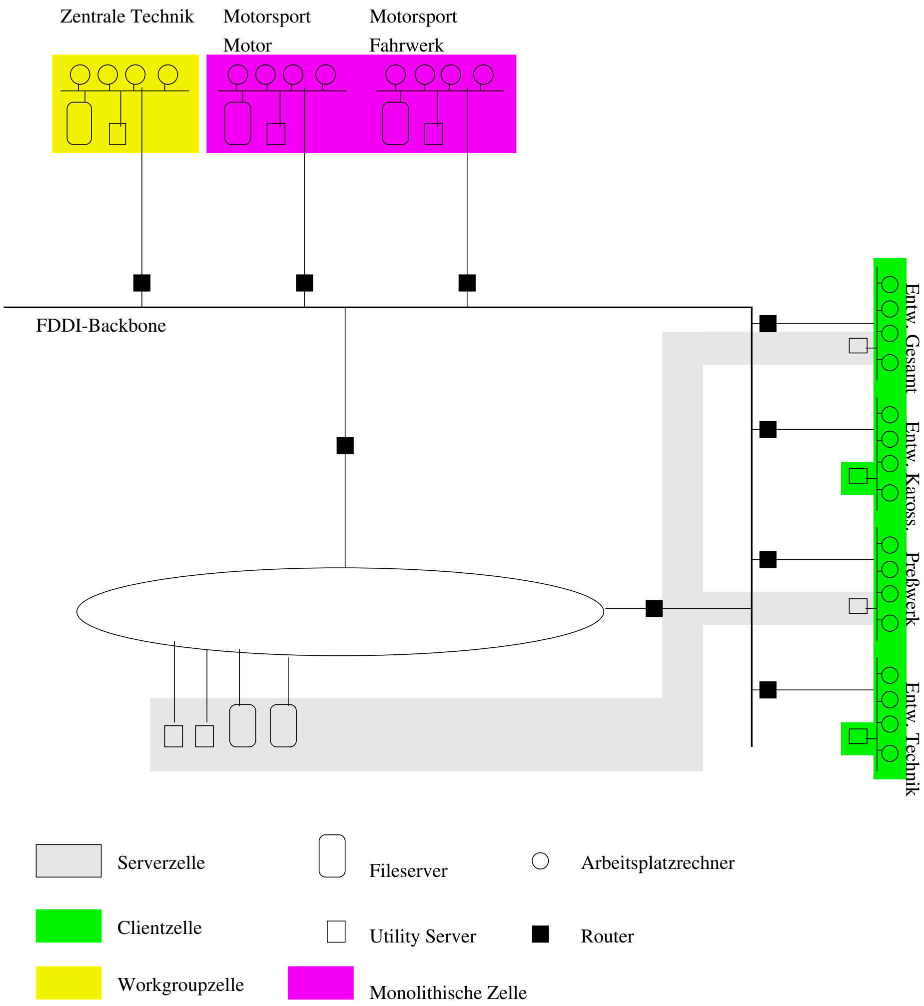


Abbildung 6.1: Empfehlung für die Einteilung des CATIA-Verbundes

Somit sind in dieser DCE-Infrastruktur Elemente aus allen Zellmodellen enthalten. Die Vorzüge dieser Struktur können anhand der vollständigen Diskussion der einzelnen Ansätze in Kapitel 5 verifiziert werden.

Anhang A

Die Architektur von OSF/DCE

A.1 Das Client/Server-Modell

Das Client/Server-Modell beschreibt die räumliche und logische Trennung zwischen Diensterbringung und Dienstnachfrage. Es hat sich als grundlegendes Modell für die verteilte Informationsverarbeitung durchgesetzt.
Im Rahmen von DCE tritt häufig der Begriff des *Clerks* auf. Clerks sind ein Beispiel für relative Rollen im Zusammenhang mit Client/Server-Beziehungen. Logisch sind sie zwischen dem Client und dem entsprechenden Server angesiedelt. Clients richten dabei ihre Anfragen an den Clerk, der seinerseits diese Anfrage an den Server weiterleiten kann, wenn die angeforderte Information noch nicht in seinem lokalen Speicher vorliegt.

A.2 Leichtgewichtige Prozesse

Mit der immer stärker voranschreitenden Verbreitung von Multiprozessorarchitekturen wird ein Mechanismus benötigt, der es erlaubt, echte Nebenläufigkeit auch innerhalb eines Prozesses zu realisieren. Dies ist vor allem für Serverprozesse von Bedeutung, da sie für jede Verbindung mit einem Client einen eigenen prozeßinternen Kontrollfluß *(Thread)* starten können. Diese Technik ermöglicht es, für eine einzelne Client/Server-Beziehung das semantisch besser beherrschbare Modell der synchronen Kommunikation einzusetzen, insgesamt jedoch durch mehrere Kontrollflüsse asynchron Aufträge innerhalb eines Serverprozesses bearbeiten zu können.

A.3 Entfernter Prozeduraufruf

Der *Remote Procedure Call (RPC)* stellt eine semantische Erweiterung des aus vielen gängigen Programmiersprachen bekannten Konstrukts des Prozeduraufrufs dar. Diese Erweiterung besteht im wesentlichen darin, daß Prozeduraufruf und die Abarbeitung des Prozedurrumpfes nicht mehr auf einen gemeinsamen Adreßraum beschränkt bleiben. Aus Sicht des Aufrufers besteht kein Unterschied zwischen einer lokalen und einer entfernten Prozedur, womit die Tatsache, ob eine Prozedur auf

einem entfernten Rechner – und wenn ja, auf welchem – ausgeführt wird, vollkommen transparent bleibt.
Auf Parameterebene existieren darüberhinaus Möglichkeiten – z.B. das Festlegen der operationellen Semantik (*at-most-once, at-least-once, exactly-once*), die Auswahl von Serverinstanzen (Binden) und die Fehlerbehandlung (Kommunikationsfehler, Serverfehler) – die die speziellen Anforderungen in einem verteilten Umfeld realisieren.
Jede Form der Kommunikation findet bei DCE über den entfernten Prozeduraufruf statt. Somit ist eine weitreichende Unabhängigkeit von der unterliegenden Kommunikationsarchitektur gegeben.
Es ist also nicht erforderlich, DCE-Verbunde anhand der eingesetzten Protokolle zu strukturieren.

A.4 Zeitsynchronisation

Die Aufgabe des *Distributed Time Service (DTS)* ist es, die Systemuhren der einzelnen Rechner mit einer netzwerkweiten Zeit *(Universal Coordinated Time (UTC))* zu synchronisieren.
Auch dieser Dienst ist nach dem Client/Server-Prinzip aufgebaut. Die Clients beziehen Zeitstempel von einer definierten Anzahl von Servern und errechnen daraus ihre neue Systemzeit, wohingegen sich die Server untereinander synchronisieren.
Die Zeitstempel beschreiben dabei keinen exakten Zeitpunkt, sondern ein Zeitintervall innerhalb dessen die Systemzeit des Servers liegt und dessen Grenzen durch geschätzte, auftretende Verzögerungen beim Transport zum Client bestimmt werden.
Der *DTS* ist vor allem von Bedeutung, wenn zur Bestimmung des globalen Systemzustandes eine Serialisierung von Ereignissen benötigt wird. Zudem hängen die Sicherheitsmechanismen von DCE von einer Synchronisation der Systemuhren ab.

A.5 Verzeichnisdienste

Die Komplexität verteilter Systeme beruht in erster Linie auf ihrer geographischen Verteiltheit, ihrer großen Anzahl von Objekten und ihrer Dynamik.
Zur Beherrschung dieser Problematik werden Verzeichnisdienste eingesetzt, um die Verwaltung der Ressourcen innerhalb eines administrativen Bereiches zentral durchführen zu können.

Das Anforderungsprofil an einen solchen Verzeichnisdienst ist sehr umfangreich und eine Reihe von Fragestellungen müssen durch ihn adressiert werden.

Dienstevermittlung

- welche Dienste stehen in der Umgebung zur Verfügung?
  Diese auch als *Yellow Pages* bezeichnete Funktionalität ermöglicht eine attributbasierte Suche nach Diensten im Namensraum.

- Wie findet ein Client einen Server für einen Dienst?
  Für die Flexibilität einer verteilten Umgebung muß sichergestellt sein, daß diese Entscheidung zur Laufzeit durchgeführt werden kann. Darüberhinaus muß die Möglichkeit bestehen, unter einer Menge von kompatiblen Servern

eine Auswahl zu treffen. Dieser Vorgang des Bereitstellens bzw. Auslesens von kompatiblen Bindeinformation wird auch als *Trading* bezeichnet.

- Wie kann unter identischen Serverinstanzen die Last verteilt werden und wie lassen sich Präferenzen bei der Auswahl ausdrücken?
  Der Verzeichnisdienst muß also über die Möglichkeit einzelne Objekte zu registrieren, auch Mechanismen für die Anordnung von gleichartigen Objekten zur Verfügung stellen.

Namensdienst

- Auflösung von benutzerorientierten, symbolischen Namen in ressourcenorientierte, physikalische Namen.
  Die Notwendigkeit für einen Namensdienst *(white pages)* stellt sich zum einen, um eine effektive Nutzung erst zu ermöglichen und um sicherzustellen, daß Objekte auch nachdem sie physikalisch verlagert wurden, weiter unter demselben Namen zu erreichen sind.

  Als Grundlage müssen jedoch die zu verwalteten Ressourcen als verbundweite Objekte realisiert werden; sie müssen also eine globale Identität besitzen.
  DCE ordnet allen Objekten einen global eindeutigen Identifikator (*Universal Unique Identifier (UUID)* zu.

- Zuordnung mehrerer symbolischer Namen zu einem Objekt (*Aliasing*)
  Dadurch lassen sich persönliche Sichtweisen auf den Namensraum definieren und in einfacher Weise Umstrukturierungen vornehmen.
  Neben Verzeichnissen und Objekteinträgen stellt CDS auch Verweise (*softlinks*) zur Verfügung

Managementanforderungen

- Der gesamte Namensraum muß partitionierbar sein.
  Die Größe von verteilten Systemen kann dazu führen, daß sich der gesamte Namensraum nicht mehr sinnvoll, d.h. z.B. performant, auf einem einzigen Server zur Verfügung gestellt werden kann. Es muß also die Möglichkeit bestehen, gewisse Teilbäume auf andere Systeme auszulagern. Dies soll jedoch transparent in Bezug auf den Zugriff bleiben. Um eine Sicht auf den ganzen Namensraum von jedem Server aus zu ermöglichen, muß zudem ein Mechanismus existieren, der die einzelnen Partitionen trotz ihrer unterschiedlichen Lage zu einem logischen Ganzen zusammenfügt. Der Namensraum muß also durch eine Verweisstruktur verknüpft werden können.
  Die Architektur von CDS sieht vor, daß jede Instanz des Verzeichnisdienstes auf einer eigenen Datenbank arbeitet. Über Verweise lassen sich auch Teile aus den Datenbanken anderer Server referenzieren.

- Verfügbarkeit
  Um die Verfügbarkeit des Namensraumes unabhängig von der Verfügbarkeit eines einzelnen Servers zu machen, ist eine Replikation von Einträgen vorzusehen. Mit der Replikation müssen jedoch auch Mechanismen eingeführt werden, die die Konsistenz des Namensraumes nach Änderungsoperationen wiederherstellen.
  Im Rahmen von CDS kann dabei zwischen unmittelbaren und periodischen Updates gewählt werden.

- Integration von heterogenen Namensräumen zum einem einheitlichen Namensraum
  Dieses Problem tritt in zwei Ausprägungen auf:

  1. Integration der Namensräume verschiedener Dienste zu einem logischen Ganzen.
     Hierfür stellt der *Cell Directory Service (CDS)* ein spezielles *Junction*-Protokoll zur Verfügung, mit dessen Hilfe beliebige Namensräume in den Namensraum des Verzeichnisdienstes einer administrativen Domäne eingebunden werden können.
     Im Falle von DCE sind der Namensraum des Sicherheitdienstes, sowie der Namensraum des Dateisystems in den CDS-Namensraum einer Zelle integriert.
  2. Integration der Namensräume verschiedener Organisationen zu einem weltweiten, globalen Namensraum.
     Um die Kooperation zwischen unterschiedlichen administrativen Domänen zu ermöglichen, bedarf es eines Mechanismus zur Zusammensetzung der lokalen Namensräume zu einem globalen Namensraum.
     Im Rahmen von DCE wird dies über die Registrierung des lokalen Namensraumes im *OSI Directory* (CCITT X.500/ISO 9594) oder im *Domain Name Service (DNS)* implementiert.
     Die Kooperation zwischen zwei Zellen hängt jedoch nicht davon ab, in welchem globalen Namensraum sie registriert sind.

  Die Integration der Namensräume unterschiedlicher Dienste und die Gliederung des globalen Namensraumes in unabhängige lokale Namensräume definieren also implizit betrennte Bereiche einer verteilten Umgebung. Diese Domänen werden in DCE als *Zellen* bezeichnet.
  Jedes DCE-Objekt ist in genau einer solchen Zelle registriert. Es sind also keine Überlappungen zwischen unterschiedlichen Zellen möglich.

- Die Informationen des Verzeichnisdienstes müssen geeignet geschützt werden können. CDS realisiert diese Anforderung über die Verwendung der Zugriffskontrollisten auf Einträgen und Verzeichnissen.

Dienstevermittlung

Da im Laufe der Arbeit die Zuordnung von Clients zu spezifischen Serverinstanzen eine Rolle spielt, sollen an dieser Stelle einige Aspekte der Trading-Problematik im Rahmen von DCE erörtert werden.

Grundlegend muß es möglich sein, gleichwertige Dienstinstanzen anhand eines Attributs identifizieren zu können. Zu diesem Zweck führt DCE ein Schnittstellenkonzept ein. Jeder Dienst erhält dabei eine eindeutige Schnittstellenkennung (*Interface-UUID*). Die Differenzierung der Instanzen erfolgt dann über eine eindeutige Objektkennung (*Object UUID*).
Ein Server exportiert diese Informationen in den Namensraum der Zelle. Über eine Suche nach der entsprechenden Schnittstellenkennung im Namensraum können Clients kompatible Serverinstanzen suchen.

Für die Navigation durch den Namensraum stehen dabei drei Sorten von Einträgen zur Verfügung:

1. Server-Einträge:
   Sie enthalten die physikalische Lage (Rechner, Protokollstapel, Port) einer Dienstinstanz.

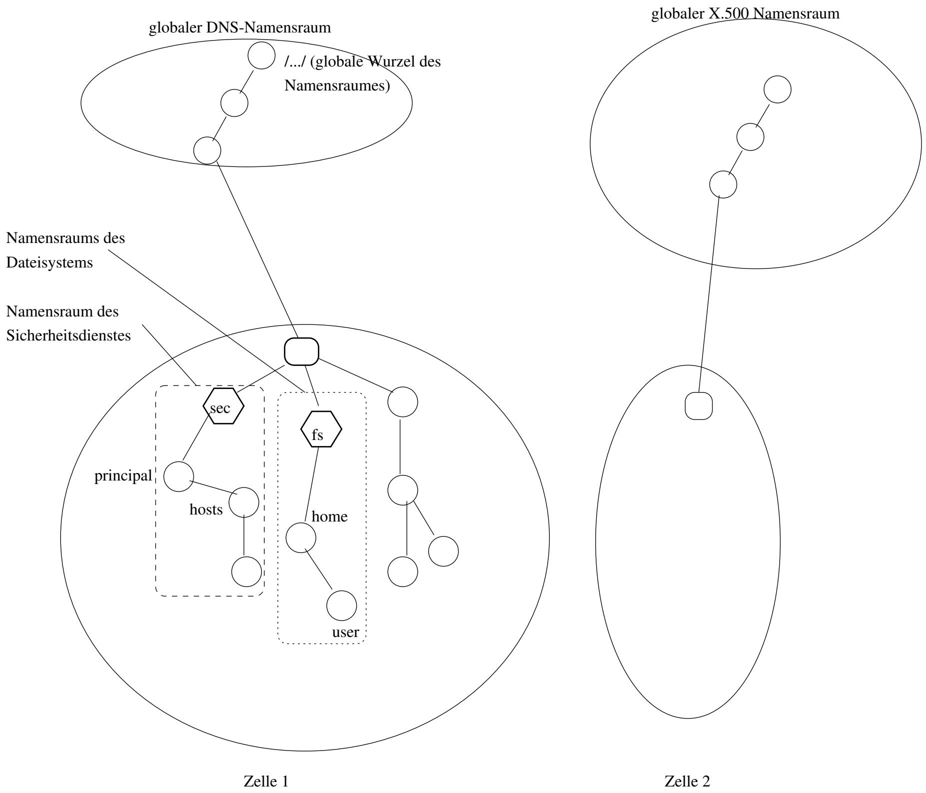


Abbildung A.1: Namensräume des Verzeichnisdienstes

2. Gruppen-Einträge:
   Sie enthalten eine ungeordnete Menge von Serverinstanzen. Die Auswahl einer spezifischen Serverinstanz ist nicht möglich. Die Semantik des Zugriffs ist eine zufällige Auswahl.
   Gruppen können auch kaskadiert werden.

3. „Profile“-Einträge:
   Wie bei Gruppeneinträgen können hier eine Menge von Serverinstanzen aufgeführt werden. Profiles können sowohl Server-Einträge, Gruppen-Einträge, als auch Verweise auf andere Profiles enthalten.
   Diese Kette von Profiles, die im Laufe einer Suche durchlaufen werden kann, beschreibt den Suchpfad innerhalb des Namensraumes.
   Profiles bieten darüberhinaus die Möglichkeit spezifische Einträge mit Prioritäten zu versehen. Dadurch existieren zwei Möglichkeiten die Auswahl einer Serverinstanz zu erzielen:

   (a) Durch Plazierung des Servereintrags im Suchpfad vor allen anderen Servereinträgen desselben Dienstes. Für unterschiedliche Benutzer können dann unterschiedliche Suchpfade definiert werden.
   (b) Durch das Versehen eines Servereintrags mit einer höheren Priorität.

A.6 Netzwerkweite Sicherheit

A.6.1 Ein Modell für Sicherheitsaspekte

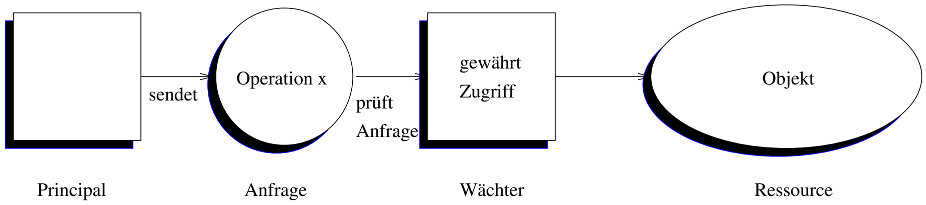


Abbildung A.2: Modell der Zugriffskontrolle

Das gängigste Konzept zur Implementierung von Sicherheit ist das Modell der Zugriffskontrolle [Authen 92]. Dieses Modell basiert auf vier Elementen:

Principals repräsentieren den Ursprung von Zugriffsoperationen. Da auch Dienste unter gewissen Umständen auf andere Dienste zugreifen, müssen sie in der Lage sein, auch als Client operieren zu können.
Aus diesem Grund können *Principals* sowohl interaktive Benutzer, als auch Dienstprozesse sein.

Requests sind Aufträge an einen Server, Operationen auf bestimmten Objekten durchzuführen.

Wächter sind verantwortlich, jeden *Request* daraufhin zu untersuchen, welcher Benutzer ihn initiiert hat und ob die auf dem Objekt durchzuführende Operation für den Initiator zulässig ist.
Die Überprüfung des Ursprungs wird als *Authentifizierung* bezeichnet, die Interpretation der Zugriffsregeln als *Authorisierung*. Diese Regeln werden meist in Form von Zugriffskontrollisten (*Access Control List, ACL*) für jedes Objekt realisiert.

Objekte stellen die Betriebsmittel dar. Dies können Geräte, Dateien oder Dienste sein.

A.6.2 Anforderungen an einen netzweiten Sicherheitsdienst

Nach dem OSI Referenz Modell [ISO 7498-2] muß ein netzweiter Sicherheitsmechanismus folgende Dienste anbieten,

Authentifizierung Bei der Authentifizierung muß ein Benutzer den Nachweis seiner Identität erbringen. Ziel ist es, daß beide Kommunikationsteilnehmer die Sicherheit haben, mit dem gewünschten Partner zu kommunizieren.
Im OSI Authentication Framework [ISO 10181-2] sind die möglichen Verfahren in 5 Klassen, abgestuft nach Sicherheit, unterteilt. [1]

Klasse 0 Verfahren der Klasse 0 fordern beim Benutzer dessen Paßwort an, das im Klartext über des Netz zu einer Verifikationsinstanz gesendet wird. Die Risiken dabei sind, daß ein Paßwort abgefangen wird, bzw. daß sich ein Eindringling als Verifikationsinstanz ausgibt.

[1] Für den folgenden Abschnitt gilt die Vereinbarung:
Sei V ein kryptographisches Verfahren, K_U der geheime Schlüssel eines *Principals* U und I eine beliebige Information, so bezeichnet $K_U^V(I)$ die Anwendung des Verfahrens V mit dem Schlüssel K_U auf die Information I.

Klasse 1 Hier wird das Paßwort verschlüsselt übertragen. Ein Eindringling kann sich deshalb nicht mehr unter der Identität des Benutzers an einem Terminal einloggen, er kann jedoch den abgehörten Zeichenstrom seinerseits an die Verifikationsinstanz schicken und somit eine fremde Identität annehmen.

Klasse 2 Die Funktionsweise ist identisch zur Klasse 1, bis auf die Tatsache, daß für unterschiedliche Verifikationsinstanzen, unterschiedliche Verschlüsselungen verwendet werden.

Klasse 3 Bei diesen Verfahren wird das Paßwort nicht mehr unmittelbar genutzt, sondern es wird aus dem Paßwort ein geheimer Schlüssel K_U abgeleitet. Damit verschlüsselt der Benutzer U eine, von der Verifikationsinstanz erhaltene Information I und sendet diese zurück. Um es einem Eindringling unmöglich zu machen, durch das Abfangen der Authentifizierungsnachricht $(K_U(I))$ die Identität des legitimen Benutzers anzunehmen, muß für jeden Authentifizierungsvorgang eine eindeutige Information I versendet werden. Diese Information wird dann als *Challenge* oder *Nonce* bezeichnet.

Klasse 4 Diese Verfahren sind eine Erweiterung von der Klasse 3. Der Unterschied besteht darin, daß in I auch Informationen enthalten sind, mit deren Hilfe die Legitimität der Verifikationsinstanz überprüft werden kann. Dadurch ist es einem Eindringlich unmöglich, sich als Verifikationsinstanz auszugeben.
Ein Repräsentant dieser Klasse ist *Kerberos*, welches auch im Rahmen von DCE zum Einsatz kommt.

Zugriffskontrolle: Hierbei ist der wichtigste Aspekt der Schutz von Objekten im Rahmen der Mechanismen der lokalen Betriebssysteme. Dafür existieren zwei Ansätze:

1. *Access Control Lists (ACL)*
   Sie ordnen jedem Objekt die Menge aller berechtigten Benutzer inklusive deren Rechte zu.
2. *Capabilities*
   Sie ordnen jedem Subjekt die Menge der Ressourcen zu, auf die es in angegebener Weise zugreifen darf.

Zur netzweiten Zugriffskontrolle werden beide Mechanismen in geeigneter Weise kombiniert. Voraussetzung ist jedoch, muß man in der Lage ist, sowohl Subjekte als auch Objekte netzwerkweit eindeutig identifizieren. Dazu verwendet DCE globale Identifikatoren (*UUIDs (Universal Unique Identifiers)*).
Zur Realisierung einer netzweiten Zugriffskontrolle erhält jeder *Principal* nach erfolgreicher Authentifizierung ein *Privilege Attribute Certificate (PAC)*, in welchem seine Identität, sowie seine Zugehörigkeit zu Benutzergruppen enthalten ist. Demgegenüber besitzen die Objekte Kontrollattribute, die autorisierte Subjekte inklusive deren Rechte in Form von netzweiten *Access Control Lists* verwalten.

Vertraulichkeit: Die versendeten Daten müssen bei ihrer Übertragung durch das Netz vor unberechtigtem Lesen durch Dritte geschützt werden. Diese Aufgabe kann von kryptographischen Verfahren (z.B. *Data Encryption Standard (DES)*, RSA-Verfahren) wahrgenommen werden. Bei DCE kommt das symmetrische DES-Verfahren zum Einsatz.

Integrität: Es muß ein Mechanismus existieren, mit dem verhindert werden kann, daß Dritte die versendeten Information verfälschen. Zu diesem Zweck können kryptographische Verfahren in Verbindung mit Prüffeldern eingesetzt werden.

Anerkennung: Es muß sichergestellt sein, daß nicht nur der eigentliche Empfänger die Identität des Senders bestimmen kann, sondern auch eine weitere, unabhängige Instanz, damit der Sender nicht leugnen kann eine Nachricht verschickt zu haben. Für diese Problematik lassen sich digitale Unterschriften im Rahmen von *Public Key* Verfahren einsetzen.
Dieselbe Problematik tritt natürlich auch in der entgegengesetzten Richtung auf. Diesbezüglich muß gewährleistet sein, daß einem Empfänger nachgewiesen werden kann, daß er die Nachricht tatsächlich empfangen hat.
Zur Sicherstellung dieser Verbindlichkeit von Kommunikation existiert in DCE kein Mechanismus.

A.6.3 Die Komponenten des Sicherheitsdienstes von DCE

Die Sicherheitsumgebung von DCE setzt sich aus mehreren Diensten zusammen.

Authentication Service Dieser Dienst stellt sicher, daß die Identitäten der kommunizierenden Partner auf ihre Korrektheit hin überprüft werden.

Privilege Service Nachdem die Identität verifiziert wurde, muß entschieden werden, ob der Benutzer das Recht bekommen soll, auf die von einem Server verwalteten Ressourcen zugreifen zu dürfen. Diese Aufgabe erfüllt der Privilege Service, indem er die zur Gewährung des Zugriffs notwendige Information an den Client liefert.

Registry Service Dieser Dienst verwaltet alle sicherheitsrelevanten Informationen in einer zentralen Datenbank. In der Datenbank befinden sich Einträge für alle Benutzer der Zelle, für Gruppen von Benutzern und für Organisationen.
Organisationen stellen dabei eine spezielle Form von Gruppen dar. Mit Organisationen können jedoch keine Zugriffsrechte assoziiert werden. Organisationen dienen dazu, über *Policies* bestimmte Sicherheitsvorschriften (z.B. minimale Paßwortlänge) für eine Menge von Benutzern zu definieren.

Access Control Lists Durch den Eintrag in eine ACL werden Benutzer berechtigt, auf die, der ACL assoziierte Ressource zuzugreifen. Diese Einheiten können Dateien, sowie Einträge des Verzeichnis- und Sicherheitsdienstes sein. ACL erweitern das Konzept der UNIX Permissions hin zu einer personenbezogenen Authorisierung. Neben der Lese-, Schreib- und Ausführungsauthorisierung bieten sie zudem die Möglichkeit die Erzeugung und das Löschen von Verzeichniseinträgen zu kontrollieren. Der verwaltende Zugriff auf ACLs wird über ein zusätzliches Kontrollattribut des Objektes gewährt.

Login Facility Die sogenannte Login Facility ersetzt die gewöhnliche Login-Umgebung des Systems, um den Benutzer von der Komplexität der Authentifizierung- und Authorisierungsverfahren abzuschirmen. Dabei sind jedoch lediglich die Schnittstellen zwischen Client und Sicherheitsdienst definiert, eine verbindliche Vorschrift, wie eine Loginprozedur gestaltet sein muß, existiert nicht.

DCE bietet auch die Möglichkeit der authentifizierten Kommunikation mit anderen Zellen. Diese Beziehung kann jedoch nur wechselseitig zwischen zwei Zellen errichtet werden. Dazu ist es nötig, das innerhalb einer Zelle verwendete Authentifizierungsverfahren zu erweitern.

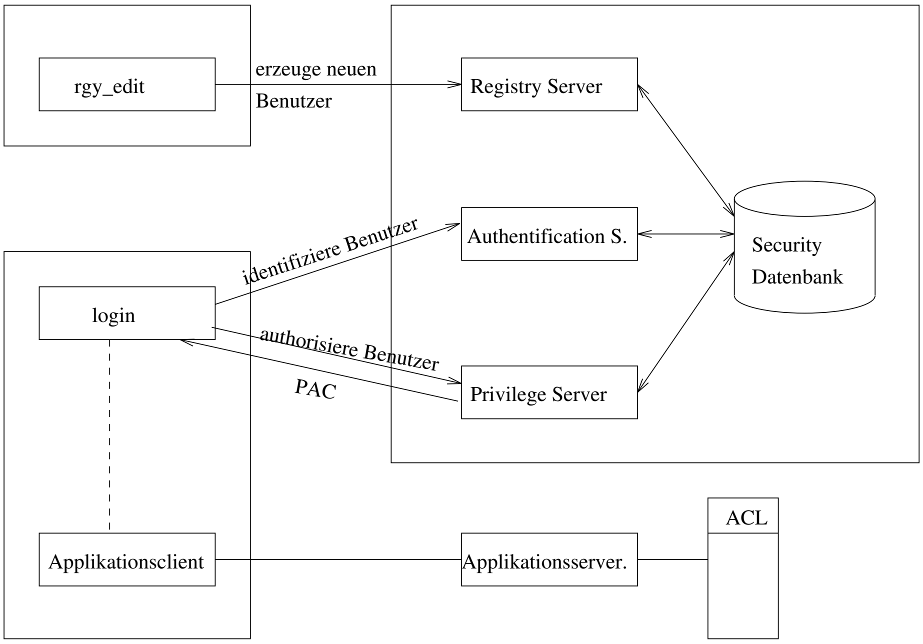


Abbildung A.3: Komponenten des Sicherheitsdienstes

Zu diesem Zweck wird zwischen den Sicherheitsdiensten zweier Zellen ein gemeinsamer Schlüssel ausgetauscht. Dieser sogenannte *Surrogatschlüssel* wird in einem speziellen Interzell-Account der beiden verwaltet.

A.7 Das verteilte Dateisystem *DFS*

Die Architektur von DFS setzt sich im wesentlichen aus drei Komponenten zusammen:

1. physikalischen Dateisystem:
   Das physikalische Dateisystem ist für die Organisation der Daten auf einem Plattenspeicher verantwortlich. Im Rahmen von DFS existieren dabei drei Ebenen von Daten:

   (a) Aggregate:
   Aggregate sind vergleichbar mit Plattenpartitionen.

   (b) Filesets:
   Fileset stellen die administrativen Einheiten des physikalischen Dateisystems dar. Jeder Fileset enthält einen eigenen Verzeichnisbaum, der an eine Stelle des zellweiten Dateisystems gemountet werden kann.

   (c) Dateien und Verzeichnisse

2. Dateiserver:
   Der Dateiserver macht die gespeicherten Daten verfügbar.

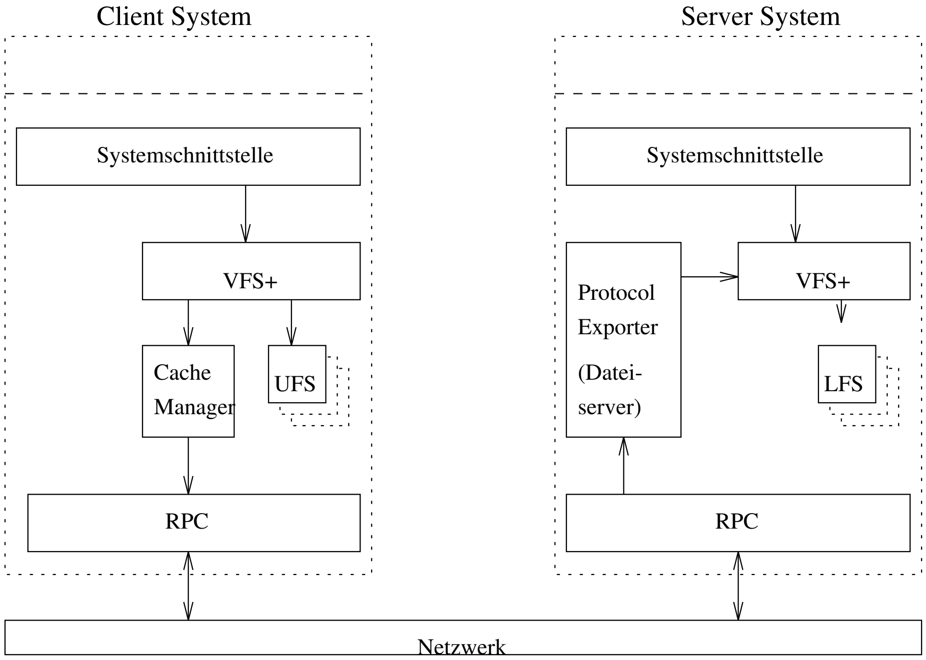
3. Fileset-Datenbank:
   In ihr wird die Lage der Filesets und ihre Wurzelverzeichnisse (*Mountpoints*) verwaltet.

Die zentrale Aufgabe eines verteilten Dateisystem ist es, die Nutzung und die Verwaltung von verteilten Datenbeständen möglichst transparent zu gewährleisten. Die Ausprägungen dieser Transparenz sind:

- Zugriffstransparenz:
  Für die Nutzung von DFS stehen dieselben Schnittstellen wie für den lokalen Dateizugriff zur Verfügung
- Nebenläufigkeitstransparenz:
  DFS stellt für die Synchronisation paralleler Dateizugriffe einen Mechanismus zur Verfügung, der eine konsistente Bearbeitung von Dateien erlaubt. Bevor einem Client der Zugriff auf eine Datei gewährt wird, muß er ein sogenanntes *Token* anfordern, das ihm die korrekte Bearbeitung seiner Aufträge garantiert. Bevor etwa ein Schreib-*Token* für eine Datei vergeben wird, entzieht der Server allen Clients ihre Lese-*Tokens*. Nachdem die Schreiboperation abgeschlossen ist, können die Clients ein neues Lese-*Token* anfordern und erhalten dabei automatisch die aktuellste Version der Datei.
- Lokationstransparenz:
  DFS organisiert seinen Namensraum auf der Basis einer Zelle. Aus diesem Grund kann auf eine Datei stets über denselben Pfad zugegriffen werden. Ist die Zelle darüberhinaus im globalen Namensraum registriert, so ist die Datei weltweit unter demselben Pfad zu erreichen.
- Fehlertransparenz:
  Die Fileserver verwalten für jede Verbindung mit einem Client einen Kontext. Somit sind Server in der Lage, nach Systemfehlern einen konsistenten Zustand herzustellen.
  Darüberhinaus ist es möglich Kopien von Filesets zu erzeugen, sogenannte *Backup-Filesets*. Mit ihrer Hilfe kann ein Benutzer ohne Eingriff eines Administrators gelöschte oder beschädigte Dateien wiederherstellen.

Über diese Transparenzeigenschaften bietet DFS zusätzliche Mechanismen um die speziellen Anforderungen in einer verteilten Umgebung zu entsprechen:

- Verfügbarkeit:
  DFS setzt ein transaktionsbasiertes physikalisches Dateisystem, das *Local File System (LFS)* ein. Damit wird die zeitaufwendige Prozedur des *File System Checks* beim Wiederanlaufen nach einem Fehlerfall überflüssig.
  Zudem unterstützt DFS eine Read-Only-Replikation von Filesets.
- Sicherheit:
  DFS nutzt in vollem Umfang die Sicherheitsmechanismen von DCE. Dateien und Verzeichnisse können durch Zugriffskontrollisten (ACL) geschützt werden.
- Heterogenität:
  Neben dem *Local File System* können auch gewöhnliche UNIX-Dateisysteme in den globalen Dateiraum exportiert werden.
- Leistungsfähigkeit:
  Zur Steigerung der Leistung, zur Verringerung der Netz- und Serverlast erlaubt DFS das Zwischenspeichern von Dateien durch die Clients *(Caching)* Zusammen mit dem Einsatz von verbindungsorientierten Protokollen ist damit auch der Einsatz über Weitverkehrsnetze möglich.



VFS+: UNIX Virtual File Switch mit DCE Erweiterungen
UFS: UNIX File System
LFS: Local File System

Abbildung A.4: Architektur von DFS

DFS trifft auch spezielle Maßnahmen, die die Administration des Dateisystems erleichtern:

- Filesets können im laufenden Betrieb zwischen Platten und Rechnern verlagert werden.
- Es ist ein Backup im laufenden Betrieb möglich.
- Die Verfügbarkeit von Serverprozessen wird automatisch überwacht.
- Durch die Verwendung spezieller Variablen ist es möglich, auch in heterogenen Umgebungen eine möglichst konsistente Konfiguration aller Systeme herzustellen.
  Diese Variablen sind:
  - `@sys`:
    Mit Hilfe dieser Variable kann zur Laufzeit – d.h. beim Zugriff auf eine Datei – eine Betriebssystem-spezifische Auswahl getroffen werden. Anwendungsbereiche sind die Auswahl von unterschiedlichen Konfigurationsdateien (z.B. zum Einstellen der Benutzerumgebung) für unterschiedliche Betriebssysteme.
  - `@host`:
    Hier wird die Auswahl maschinenbezogen durchgeführt. Dieser Mechanismus ist vor allem dann von Bedeutung, wenn die Clientsysteme *diskless*, also ohne eigenes Betriebssystem betrieben werden sollen.

.

Im Rahmen dieser Arbeit ist es aufgrund des Umfangs und der Komplexität nicht möglich, einen vollständigen Überblick über die Funktionalität der Komponenten von DCE zu geben. Aus diesem Grund wurde lediglich die Architektur der einzelnen Dienste vorgestellt.
Der Leser sei an dieser Stelle an die zu DCE existierende Literatur verwiesen. Eine Überblick über die Funktionsweise von DCE erhält man etwa in [Ros 92], oder [Schill 93].
In aller Ausführlichkeit kann die Thematik anhand der, von der OSF herausgegebenen Dokumentation [OSF Admin] studiert werden.

Literaturverzeichnis

[OSF Intr] Open Software Foundation: *Introduction to OSF DCE Revision 1.0 Update 1.0.1* Open Software Foundation, Cambridge (1992)

[OSF Admin] Open Software Foundation: *OSF DCE 1.0 Administration Guide* Open Software Foundation, Cambridge (1992)

[OSF User] Open Software Foundation: *OSF DCE 1.0 Users Guide and Reference* Open Software Foundation, Cambridge (1992)

[OSF AppDev] Open Software Foundation: *OSF DCE 1.0 Application Development Guide* Open Software Foundation, Cambridge (1992)

[OSF Ov] Open Software Foundation: *Distributed Computing Environment, An Overview* `http://www.osf.org:8001/`

[OSF OpS] Open Software Foundation: *Interoperability: A Key Criterion for Open Systems* `http://www.osf.org:8001/`

[OSF RPC] Open Software Foundation: *Remote Procedure Call in a Distributed Computing Environment* `http://www.transarc.com`

[OSF Dir] Open Software Foundation: *Directory Services in a Distributed Computing Environment* `http://www.transarc.com`

[OSF File] Open Software Foundation: *File Systems in a Distributed Computing Environment* `http://www.osf.org:8001/`

[OSF Sec] Open Software Foundation: *Security in a Distributed Computing Environment* `http://www.osf.org:8001/`

[OSF Tech] Open Software Foundation: *OSF DCE 1.0 Technical Supplement* Open Software Foundation, Cambridge (1992)

[DCE Impact] Rich Salz *DCE – and its Impact on System Administrators* `http://www.osf.org:8001/people/salz/lisa8.ps` (1994)

[Leser 1] Norbert Leser: *The Distributed Computing Environment Naming Architecture* `http://www.osf.org:8001/`

[Leser 2] Norbert Leser: *Federated Naming and Object Location with OSF DCE* `http://www.osf.org:8001/`

[Leser 3] Norbert Leser: *Towards a Worldwide Distributed File System*
The OSF DCE File System as an Example `http://www.osf.org:8001/`

[Johnson 91] Brad Curtis Johnson: *A Distributed Computing Environment Framework:*
An OSF Perspective `http://www.osf.org:8001/`

[Schill 93] Alexander Schill: *DCE Das OSF Distributed Computing Environment Einführung und Grundlagen* Springer Verlag (1993)

[Ros 92] Ward Rosenberry, David Kenney & Gerry Fisher: *Understanding DCE* O´Reilly & Associates, Inc. (1992)

[Middle 93] Philip A. Bernstein *Middleware An Architecture for Distributed System Services* Technical Report CRL 93/6 Digital Equipment Corporation, Cambridge Research Lab (1993)

[Trade 94] K. Müller, M. Merz, W. Lamersdorf *Der TRADE-Trader, Ein Basisdienst offener verteilter Systeme* `http://www.dbis1.informatik.uni-hamburg.de` (1994)

[Trader 94] Ashley Beitz, Mirion Bearman *An ODP Trading Service for DCE* `http://www.dstc.edu.au/` (1994)

[NIST 95] Distributed Systems Management Working Group OSE-TC OSE *Requirements for Distributed Systems Management Draft 1.1* (31 January 1995) `ftp://nemo.ncsl.nist.gov/pub/dsm/require.txt`

[DOMAINS] Morris S. Sloman & Jonathan D. Moffett *Domain Management for Distributed Systems* in Integrated Network Management Proc. of the IFIP TC 6/WG 6.6 Symposium on Integrated Network Management
Boston, MA, USA 16.-17.05.1989

[Manage 90] Morris S. Sloman & Jonathan D. Moffett *Managing Distributed Systems* `http://www-dse.doc.ic.ac.uk/dse-papers/management/` (1990)

[Mechanism 93] Morris S. Sloman & Jonathan D. Moffett *User and Mechanism Views of Distributed Systems Management* IEE/IOP/BCS Distributed Systems Engineering Vol. 1, No. 1 August 93

[Sloman 94] Morris Sloman: *Network and Distributed Systems Management* Addison Wesley Publishing Company (1994)

[Mack 94] Dr. Dieter Mack: *Administration und Delegation in einer campusweiten DCE-Zelle* `/afs/rus.uni-stuttgart.de/dcewg/Proceedings/`

[Gottschalk 94] Klaus Gottschalk: *DCE-Projekt am Regionalen Rechenzentrum der Universität Stuttgart* `/afs/rus.uni-stuttgart.de/dcewg/Proceedings/`

[Pehkonen 94] Jean A. Pehkonen: *DCE DFS: A Look Beyond AFS* `/afs/rus.uni-stuttgart.de/dcewg/Proceedings/`

[Chinitz 94] Jonathan Chinitz *Implementing Security in a DCE Environment* `ftp://ftp.isoft.com/SHARE94.ps`

[Transarc 1] M. Spasojevic, M. Satayanarayanan: *A Usage Profile and Evaluation of a Wide-Area Distributed File System* `ftp://grand.central.org/afs/transarc.com/public/ps/`

[Transarc 2] Micheal L. Kazar et al.: *DEcorum File System Architectural Overview* `ftp://grand.central.org/afs/transarc.com/public/ps/`

[BMW 9/94] BMW AG: *Projektplan CATIA Migration in C/S Architektur*

[BMW IV] BMW AG: *Konzept einer dezentralen IV-Betriebsunterstützung*

[BMW 11/94] BMW AG: *Umsetzung des Dateikonzeptes zur Pilot-Installation von VENUS/AIX bei BMW*

[Russel 94] Bob Russel: *DCE Performance Study* AIXpert Ausgabe November 1994

[Transarc 94] Dan Hamel: *DCE Troubleshooting* `ftp://grand.central.org/afs/transarc.com/public/ps/dce/doc/trouble1.ps` `ftp://grand.central.org/afs/transarc.com/public/ps/dce/doc/trouble2.ps`

[Deployment 94] Jack Danahy: *Deployment of DCE in a Production Environment* Hewlett-Packard DCE White Paper Series Number 5

[Scalability 93] Bob Bissen, Sean Mullen: *Distributed Computing Environment Scalability Testing* Hewlett-Packard DCE White Paper Series Number 1, v.2.0

[CITI 90-2] C.J. Antonelli, W.A. Doster, P. Honeyman: *Access Control in a Workstation-Based Distributed Computing Environment* `http://www.citi.umich.edu/`

[CITI 94-1]
Mark R. Carter: *Adding 50,200 Users to a DCE Registry: A Comparison of OSF DCE V1.0.2 and IBM DCE/6000 V1.2* `http://www.citi.umich.edu/`

[CITI 94-2] Chuck Lever: *Using DFS Without DCE/LFS* `http://www.citi.umich.edu/`

[CITI 94-3] Sarr Blumson: *Workload Characterization in a Large Distributed File System* `http://www.citi.umich.edu/`

[DCE Perf 93] Art Gaylord: *DCE Performance* `http://www.pilgrim.umass.edu/`

[Login Perf 94] Art Gaylord: *DCE Login Performance Study* `ftp://ftp.pilgrim.umass.edu/pub/osf/sig/sig.ps`

[ODP RM 94-1] ISO/IEC
JTC1/SC21/WG7: *ITU-T X.901 — ISO/IEC ODP Reference Model Part1 Overview* `ftp://ftp.gmd.de/pub/docs/RM-ODP/part1.ps`

[ODP RM 94-2] ISO/IEC
JTC1/SC21/WG7: *ITU-T X.901 — ISO/IEC ODP Reference Model Part2 Prescriptive Model* `ftp://ftp.gmd.de/pub/docs/RM-ODP/part2.ps`

[ODP RM 94-3] ISO/IEC
JTC1/SC21/WG7: *ITU-T X.901 — ISO/IEC ODP Reference Model Part3 Descriptive Model* `ftp://ftp.gmd.de/pub/docs/RM-ODP/part3.ps`

[ISO 7498-2] Information Processing Systems, Open Systems Interconnection, *Reference Model, Part 2: Security Architecture* (1988)

[ISO 10181-2] Information Technology, *OSI Security Model Part 2: Authentication Framework* (1990)

[Wallchart 94] International Business Maschines Corporation: *A Guide to Open Client/Server* Publication No. G511-3184-00

[Authen 92] B. Lampson, M. Abadi, M. Burrows, E.Wobber: *Authentication in Distributed Systems: Theory and Practice* Technical Report No. 83 Digital Equipment Corporation, System Research Center