View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Dokumenten-Publikationsserver der Humboldt-Universität zu Berlin

Überblick zum Distributed Computing Environment (DCE)

Warum DCE?

Bei DCE handelt es sich um eine Rechner-umgebung, die es erlaubt, sehr großen Gebilden, wie zum Beispiel der Humboldt-Universität, einen einheitlichen, logischen Namensraum zuzuordnen und trotzdem eine verteilte Verwaltung der Ressourcen ermöglicht. Worin liegt der Grund, sich mit der Weiterentwicklung des UNIX-Environments zu beschäftigen? Es gibt zwei Tendenzen im Workstation-Bereich, die eine Neugestaltung der klassischen UNIX-Umgebung erfordern.
Zum einen erkennen die Nutzer in wachsendem Maße die Beschränktheit ihres eigenen Umfeldes - es ist prinzipiell zuwenig Plattenplatz vor Ort, der zudem auch nur sporadisch gesichert wird, die Compute-Power reicht vorn und hinten nicht, die Mail geht verloren, wenn die eigene Workstation abgeschaltet ist (oft wird die Mail noch an den Rechner geschickt) usw. Aufgrund schwindender Mittel, mit denen der Nutzer sonst seine Löcher gestopft hätte, und wachsender Bedürfnisse in Richtung Komfort beginnt er sich nach neuen Ufern umzusehen. Und es gibt viel zu entdecken, denn ...
Zum anderen werden durch das Rechenzentrum universitätsübergreifende Dienste angeboten, wie zum Beispiel als jüngste Erwerbung die Erweiterung des zentralen UniTree auf der Convex des RZ durch ein System dezentraler File-Server. Das eröffnet den Nutzern in den Instituten einen ca. 1 TByte großen, virtuellen Plattenraum.
Dies erzeugt aber gleichzeitig das Problem, daß die Nutzerverwaltung des RZ in die Institute eindringt. Wie bringt man die in den Instituten und im Rechenzentrum gewachsenen Strukturen in Einklang?
Ein umfassendes Environment, das entfernte Nutzer und Ressourcen miteinander verbinden kann, sollte folgende Anforderungen erfüllen:

- umfassende, skalierbare und integrierte Dienste
- verteilte Verwaltung von Diensten und Nutzern
- einheitlicher Namensraum
- optimale Sicherheitsfunktionen
- ein universitätsweiter File-Service
- normierte Schnittstellen und Verfügbarkeit auf heterogenen Plattformen
- hohe Performance
- geringer Ressourcenbedarf

Zwei Lösungsansätze sind für eine universitätsweite UNIX-Umgebung derzeit erkennbar.

NIS+

Im Herbst 1992 wurde mit dem Erscheinen von SUNs Solaris 2.0 auch eine neue Version des Network Information Service (früher Yellow Page) unter dem Kürzel NIS+ vorgestellt. Diese hebt die flache Namensverwaltung von YP auf und bietet eine hierarchische Struktur, die dezentral verwaltet werden kann. Nachteilig ist allerdings, daß Server für NIS+ derzeit nur auf Solaris 2.x-Systemen lauffähig sind.

DCE

Die zweite Möglichkeit für einen übergreifenden, hierarchischen Namens-Service mit verteilter Verwaltung bietet das von der OSF (Open Software Foundation) propagierte DCE. Zumindest auf den gängigen Rechnerplattformen (wie DEC, HP, IBM...) sind DCE-Server möglich, und SUN-Solaris 2.x besitzt mit den Federated Services einen Einstieg in die DCE-Welt, die sie auch als Server geeignet machen. Die Leistungsfähigkeit dieses Paketes soll hier näher beleuchtet werden.

Historischer Hintergrund

Wie erwähnt, ist DCE ein Kind der OSF. Die OSF ist eine Stiftung mit der Zielsetzung der Erarbeitung neuer Technologien im UNIX-Software-Umfeld. Sie ist im Juni 1988 als Antwort auf AT&Ts UNIX-Lizenzpolitik gegründet worden. Derzeit besitzt die OSF über 400 Mitglieder, deren Hauptsponsoren Bull, DEC, Hitachi, HP, IBM und SNI sind [3]. Neue Software-Technologien werden durch einen Ausschreibungsmechanismus (RFT - Request for Technology) ermittelt. An ihm können alle Firmen teilnehmen, die für die geforderte Zielsetzung entsprechend ausgereifte und dokumentierte Programme anbieten können. Ein OSF-Evaluation-Team bewertet und selektiert die eingereichten Vorschläge und integriert sie in eine Gesamtkonzeption. Das bekannteste Ergebnis eines OSF-RFTs ist das grafische Nutzer-Interface 'Motif'.
Der RFT für DCE erfolgte 1989, die Selektion erfolgte bis Juni 1990. Danach folgte die Integrationsphase mit IBM als Hauptintegrator, die im Januar 1992 mit Release 1.0 seinen ersten Abschluß fand. Die aktuelle, fehlerbereinigte Version ist Release 1.0.2 vom Februar 1993.

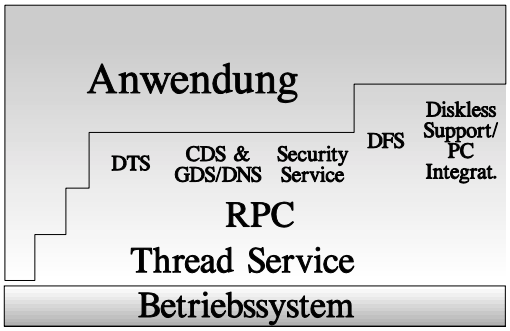
Grundlegende Prinzipien

Überblick

Aus DCE-Sicht zerfällt die Welt in DCE-Zellen, die typischerweise die Ausdehnung einer Yellow-Page-Domain besitzen. Intern wird eine Zelle durch einen Satz obligatorischer und optionaler Dienste verwaltet. Zu den obligatorischen Diensten gehört der Cell Directory Service (CDS), der für die allgemeine Namensauflösung innerhalb der Zelle zuständig ist, der Security Service, in dem die Nutzerverwaltung,

[3] Laut SunFlash-Mail vom 25.03.94 sind AT&T und SUN Mitglieder der OSF geworden.

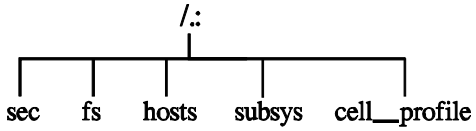
-Authentifikation und -Autorisierung abläuft und der Distributed Time Service (DTS), der die Zeit innerhalb der Zelle synchronisiert (wichtig für den Security Service). Optional können für die Kommunikation zwischen den Zellen der Global Directory Service (GDS) oder das Domain Name System (DNS) herangezogen werden. Weitere optionale Komponenten sind ein netzwerkweites Distributed File System (DFS) sowie die Unterstützung von diskless Workstations und PCs. Alle diese Dienste werden über dedizierte Server realisiert. Auf allen Rechnern einer Zelle müssen zudem die erforderlichen Client-Komponenten vorhanden sein (Funktionsbibliotheken, keine gesonderten Service-Prozesse). Die Architektur wird in dem folgenden Bild veranschaulicht:



Alle Dienste werden über eine DCE-RPC-Implementierung verwirklicht, die ihrerseits auf einen multi-threaded Service aufsetzt.

Directory Service

Der Cell Directory Service in seiner ursprünglichen Form wird durch den Distributed Naming Service von DEC repräsentiert. Seine Aufgabe ist die Abbildung logischer Namen auf physikalische Werte (Internetadresse, UID ...). CDS-Einträge können über mehrere Server verteilt und/oder repliziert werden. Beim Client werden CDS-Antworten über einen längeren Zeitraum in einem Cache gehalten, so daß doppelte Anfragen vermieden werden können. Der Namensraum wird durch den CDS innerhalb einer Zelle folgendermaßen vordefiniert:



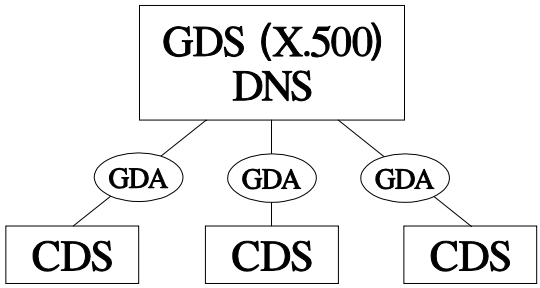
/.: - Zellwurzel
/.:/sec - Einträge des Security Service (Nutzer- und Servereinträge)
/.:/fs - Einhängepunkt für das DFS (Abk. '/:', z.B. statt /.:/fs/home geht /:/home)
/.:/hosts - Einträge für alle Rechner der Zelle (Internetadresse)
/.:/subsys und /.:/cell_profile - Systemeinträge

Beispiele:
/.:/sec/principal/h0123abc - Nutzereintrag
/.:/sec/group/p0123 - zugehöriger Gruppeneintrag
/:/home/p0123/h0123abc - Home-Directory
/.:/hosts/joker - Rechner-Eintrag

Je nach Objekt werden unterschiedliche Attribute durch CDS (bei 'sec' durch Security Service, bei 'fs' durch DFS) verwaltet, die das Objekt näher beschreiben (z.B. beim Nutzereintrag: UID, GID, Paßwort, Shell...). Durch Soft-Links können Aliases für bestehende Namen generiert werden, z.B.

/.:/hugo/my_ws → /.:/hosts/arion

über /.:/hugo/my_ws ist jetzt auch arion erreichbar.
Zellübergreifende Namen können über DNS oder GDS (entspricht DIR-X X.500 von Siemens) aufgelöst werden. Die globale Wurzel wird mit '/...' identifiziert - wird sie erkannt, dann beauftragt CDS einen Global Directory Agent (GDA) mit der Namensauflösung, der das je nach Form der Adresse entweder X.500- oder DNS-konform erledigt.



Beispiele für globale Adressierung:
/.../rz.hu-berlin.de/hosts/joker
/.../C=DE/O=HU-Berlin/OU=RZ/sec/group/p0123

Die X.500- bzw. DNS-Adresse dient gleichzeitig als Zellname. Der Zellwurzelanteil '/.:' wird bei globalen Adressen substituiert.

Security Service

Der Security Service hat drei Hauptaufgaben:
- Authentisierung (wer darf), realisiert durch Kerberos von MIT/Athena
- Autorisierung (was darf er), auf der Grundlage von Security Component von HP
- Verschlüsselung von Nachrichten über DES Secret Key mit 64 Bit Schlüssellänge

Um Nutzer-Authentifikation zu ermöglichen, wird auf einem dedizierten Security Server die Nutzer-Datenbasis über einen Registry Server erstellt. Dies kann bei vorhandener 'passwd' mit dem schönen Kommando 'import_passwd' geschehen. Der Nutzer kann nun zwischen verschiedenen Authentisierungs-Sicherheitsstufen wählen:

- *Auth. zu Beginn:* Vor der Interaktionsphase mit einem Server werden Client und Server gegeneinander authentisiert, danach gilt die Verbindung als sicher.

- *Auth. pro Aufruf:* Jeder einzelne Client-Aufruf an den Server führt zur Authentisierung.
- *Auth. pro Paket:* Jede einzelne übertragene Nachricht wird authentisiert.
- *Schutz vor Modifikation:* Es wird garantiert, daß übertragene Nachrichten nicht modifiziert wurden.
- *Vollständige Verschlüsselung:* Jedes unberechtigte Lesen/Kopieren wird durch Verschlüsselung verhindert.

Es sollte bei der Wahl der Stufe ein Kompromiß zwischen Sicherheitsbedürfnis und erforderlichem Zeitaufwand gefunden werden.
Autorisierung wird durch Access Control Lists (ACL) dezentral auf den Servern durchgeführt. Dabei werden zwei Typen von ACLs unterschieden:

Object-ACL: sind direkt an einem Objekt (CDS-Server, Datei...) befestigt

Creation-ACL: wird an einem CDS-Directory angebracht - Objekte, die in diesem Directory kreiert werden, erben diese ACL

Die Client-Anfrage an ein Server-Objekt (Datei, Drucker...) wird durch einen ACL-Manager über die Einträge in der ACL überprüft.

Beispiel einer CDS-Server-ACL:

CDS-Name:	/.:/CDS_Server_abt4	
user_obj	/.:/sec/principal/hugo: rwidt	
foreign_user	/.../osf.de/sec/principal/egon	: r---t
group_obj	/.:/group/abt_1	: r-i-t
group	/.:/group/abt_2	: r-i-t
unauthenticated		: ----t

„hugo“ aus der aktuellen DCE-Zelle besitzt alle Rechte auf dem Server (r-read, w-write, i-insert, d-delete, t-test), während „egon“ aus der Zelle 'osf.de' nur lesen darf. Die Gruppen abt_1 und abt_2 besitzen das Einfüge-Recht, dürfen aber bestehende Daten weder modifizieren noch löschen. Unbekannte dürfen lediglich die Übereinstimmung von Objekt-Attributwerten mit vorgegebenen Werten testen.

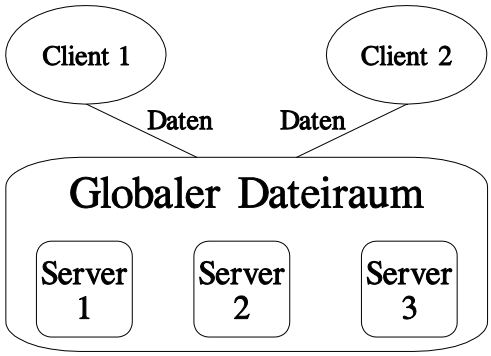
Time Service

Er beruht auf der Distributed Time Synchronisation von DEC. Dem DTS obliegt die Aufgabe, alle Rechner einer Zelle zeitlich zu synchronisieren. Durch Einbeziehung externer Zeitgeber (z.B. durch Funkuhren) ist es möglich, die Zelle mit einer korrekten Zeit zu versehen. Die Arbeit des Time Service ist Voraussetzung für die Funktionsfähigkeit des Security Service.

File Service

Das DCE Distributed File System beruht auf dem Andrew File System (AFS) der Firma Transarc. Es stellt die Implementierung einer verteilten, netzwerkweiten Dateiverwaltung dar, die sich systemtechnisch durch folgende Eigenschaften auszeichnet:

- *Lokationstransparenz:* Es wird ein logischer, globaler Dateiraum aufgebaut, der die physikalische Verteilung der Dateien auf mehrere Server verbirgt. Eine Umverteilung von Dateien von einem Server auf den anderen bleibt ohne Folgen für den logischen Pfadnamen. Die Dateinamen entsprechen der UNIX-Konvention und sind unabhängig von jeder Ortsangabe. Sie entsprechen der CDS-Directory-Konvention und können auch zellübergreifend genutzt werden.



- *Replikation:* Um die Verfügbarkeit von Software auf den DFS-Servern zu erhöhen, können Read-Only-Kopien auf mehrere Server 'repliziert' werden. Nur das Original bleibt für Änderungen offen. Die Änderungen können explizit oder periodisch an die anderen Server weitergegeben werden.
- *Caching:* Der DFS-Client cacht ganze Dateien oder große Teile davon. Das hat den Vorteil, daß es den Server entlastet und zur besseren Skalierbarkeit von DFS beiträgt. Nachteilig dagegen ist, daß Änderungen in der Datei auf dem Server erst nach dem Schließen auf dem Client bemerkt werden.
- *Recovery:* Durch einen Log-Mechanismus im lokalen File System des DFS-Servers wird eine schnellere Verfügbarkeit nach einem Systemabsturz erreicht.
- *Backup:* Es können im laufenden Betrieb volle und inkrementelle Backups gefahren werden. Die Sicht auf den globalen Dateiraum ermöglicht dabei auch Backups von mehreren Servern.
- *Interoperabilität:* NFS-Clients können mit Hilfe eines NFS/DFS-Umsetzers auf den jeweiligen DFS-Server zugreifen.
- *Management:* Ein umfangreicher Satz administrativer Werkzeuge ermöglicht die Kontrolle und Verwaltung von DFS-Servern.
- *Zugriffskontrolle:* Der Zugriff auf DFS-Bestandteile wird durch ACLs geregelt. Sie bieten gegenüber den UNIX-Möglichkeiten eine verfeinerte Kontrolle.

Beispiel einer DFS-Directory-ACL in der Zelle rz.hu-berlin.de:

CDS-Name:	/.:/fs/home/h0123abc	
user_obj	/.:/sec/principal/h0123abc	: rwxid
user	/.:/sec/principal/h0444xyz	: r-xi-
foreign_user	/.../bio.hu-berlin.de/sec/principal/egon	: rwxid
group_obj	/.:/group/p0123	: r-xi-

group /.:/group/p0444 : r----
unauthenticated : -----

Hat der Nutzer Egon einen Account im Rechenzentrum (h0123abc) und einen in seiner Zelle bio.hu-berlin.de (egon), so kann mit der obigen ACL der vollständige gegenseitige Zugriff auf seine Dateien gewährleistet werden. Dies bietet die Möglichkeit, Berührungspunkte von unterschiedlichen Zellen konfliktfrei zu gestalten (siehe Einleitung).

Weitere Dienste

Diskless Support Service
Die Integration plattenloser Workstations in eine DCE-Umgebung erfolgt auf drei Ebenen. Über einen Boot-Server werden das Betriebssystem und die Startkonfiguration bereitgestellt, ein Swap-Server unterstützt die Workstation beim Aus- und Einlagern von Prozeßkontexten und zugehörigen Speicherbereichen, und über das DFS wird eine Einbindung in den DCE-Dateiraum erreicht.

PC-Integration
Mit der PC-Integrations-Komponente ist es DOS/Windows- und OS/2-Rechnern möglich, sich als Clients in die DCE-Umgebung (CDS, Time, Security) einzuhängen. Mit PC/NFS (SUN) können die PCs auf Dateien im DFS zugreifen, ohne die volle Funktionsvielfalt zu erhalten. Die entfernte Druckernutzung wird über LAN Manager/X (HP/Microsoft) unterstützt.

Bewertung und Ausblick

DCE ist ein Netzwerkbetriebssystem, das in heterogenen und globalen Netzen arbeitsfähig ist. Es ersetzt in seiner Funktionalität NIS und NFS. Aufgrund des Zellkonzeptes und verschiedener anderer Bestandteile (z.B. CDS- und DFS-Caching) ist es in sehr großen Netzen einsetzbar und skaliert sehr gut. DCE zeichnet sich durch eine konsequente Verschleierung der Lokalität von Objekten im Zugriffspfad aus, wodurch eine leichte Portabilität der Objekte erreicht wird. Die Management-Aufgaben eines solchen funktionsreichen Systems sind naturgemäß sehr komplex, werden aber durch einen Satz unterstützender Werkzeuge gut abge-deckt.
DCE-Komponenten sind auf vielen Plattformen verfügbar. Nachteilig sind die Kosten, da sowohl ein Mehraufwand an Ressourcen als auch die Lizenzen bezahlt werden müssen. Die Basis-Elemente von DCE stehen von einigen Firmen (DEC, HP, IBM) über eine Campus-Lizenz zur Verfügung. Einige Bestandteile des DCE können auch unabhängig vom DCE-Kernel (CDS, Security, DTS) betrieben werden, so z.B. das AFS (DCE-DFS). Ziel des Rechenzentrums ist es, das System dezentraler File-Server künftig auch AFS-fähig zu machen und sich so eine Option für den Einstieg in das DCE offenzuhalten. Zu den gesammelten Erfahrungen beim Aufbau einer DCE-Testzelle im Rechenzentrum kann in einer der nächsten RZ-Mitteilungen nachgelesen werden.

TLAs

ACL - Access Control List
AFS - Andrew File System
CDS - Cell Directory Service
DCE - Distributed Computing Environment
DES - Data Encryption Standard
DFS - Distributed File System
DNS - Domain Name Service
DTS - Distributed Time Service
GDA - Global Directory Agent
GDS - Global Directory Service
LFS - Local File System
MIT - Massachusetts Institute of Technology
NFS - Network File System
NIS - Network Information Service, Synonym für YP - Yellow Page
OSF - Open Software Foundation
RFT - Request For Technology
RPC - Remote Procedure Call
TLA - Three Letter Acronym
UFS - UNIX File System

Literatur

Alexander Schill:
DCE - Das OSF Distributed Computing Environment.
Springer-Verlag, 1993.

Frank Sittel