Einführung von DCE am Rechenzentrum

Einleitung

Vier Jahre ist es her, daß ein erster Artikel zu DCE (Distributed Computing Environment) in den RZ-Mitteilungen Nr.7 erschien. Damals wurden die Historie und die grundlegenden Prinzipien beleuchtet und ein Test im RZ in Aussicht gestellt. Für all diejenigen, die den Artikel nicht mehr zur Hand haben, und für die neu Hinzugekommenen sei ein zusammenfassender Überblick vorangestellt.
Also, worum geht's?

Seit der Wende ruhen Nutzerverwaltung und File-System auf den Schultern des doch inzwischen betagten NIS/NFS. Eine immer weiter wachsende Nutzergemeinde erzeugt dabei immer größere Probleme.

Wie aus der Übersetzung hervorgeht, handelt es sich bei DCE um eine verteilte Rechnerumgebung. Sie zeichnet sich dadurch aus, daß in ihr Tausende von Rechnern, Zigtausende von Nutzern und Terabyte an Daten in einen einheitlichen Namensraum integriert, aber dennoch dezentral verwaltet werden können. Sich mit einem so mächtigen System am RZ auseinanderzusetzen, wird im wesentlichen durch folgende Gründe vorangetrieben:

- NIS wird schwerfällig
  Derzeit sind am RZ ca. 16 000 Nutzer im NIS eingetragen. Durch Paßwortwechsel der Nutzer kommt es zu Problemen bei der Generierung und Verteilung der NIS-Dateien.
- NIS als Sicherheitsproblem
  Man kann NIS nach außen etwas absichern, aber es gibt keine wirkungsvollen Mittel, um ein Abgreifen der Paßwort-Datei durch Nutzer zu verhindern – ein potentielles Sicherheitsloch.
- NFS inflexibel
  Eine so große Nutzergemeinde zieht ein sehr großes Home- und Software Directory nach sich. Eine Reorganisation der File Server aufgrund von Havarien, Lastausgleich oder ähnlichen Gründen wird durch die NFS-Punkt-zu-Punkt-Verbindung zwischen Client und Server fast unmöglich.
- NFS-Lock Problem
  Abgestürzte Mail Clients hinterlassen einen File-Lock auf dem NFS-ge'mount'eten Mail-Verzeichnis, der von alleine nicht mehr verschwindet. Ein erneuter Aufruf des Clients scheitert oder wird mit Fehlermeldungen garniert.

Mit anderen Worten: Quantität sprengt Qualität. NIS/NFS sollte durch Besseres abgelöst werden. Die Wahl fiel auf DCE, da es auf praktisch allen Plattformen vom Win3.1-PC bis zur Cray lauffähig ist und die oben genannten Schwächen nicht nur nicht besitzt, sondern noch viel mehr bietet.

Kurzer Überblick zu DCE

DCE ist ein Kind der OSF, das Anfang 1992 mit der Version 1.0 das Licht der Welt erblickte. Ziel der Entwicklung war ein sicheres, skalierbares und umfassendes Umfeld für die Integration von Unix-Systemen. Die Grundlage für die Realisation ist eine RPC-Implementierung, die auf einen multithreaded Service aufsetzt. Drei tragende Säulen ruhen für den Nutzer sichtbar auf diesem Fundament:

- CDS – ein Directory Service
- Security Service – auf Kerberos basierend
- DFS – ein umfassender File Service

Auf diese Bestandteile soll im folgenden kurz eingegangen werden.

Directory Service

Aus der Sicht von DCE ist die kleinste Verwaltungseinheit eine Zelle. In ihr sorgt ein Cell Directory Service (CDS) für Ordnung. Zu seinen Aufgaben zählt:

- Registrierung aller Workstations der Zelle mit ihren Diensten
- Vermittlung von Clients an die Server
- Aufbau von Zell-Hierarchien
- Verbinden mit anderen Zellen

Als Vermittlungsdienst sorgt CDS dafür, daß ein Client seinen Server findet (der Client kennt den Standort vorher nicht!), so ist eine leichte Verschiebbarkeit von Diensten gewährleistet. Der CDS ist jedoch nicht allwissend, über sogenannte „junctions" (Verbindungselemente) delegiert er Informationssuchende an entsprechende Server-Prozesse für den Security- bzw. DFS-Raum. Administratoren haben über „hostdata" die Möglichkeit, DCE-spezifische Daten auf jeder

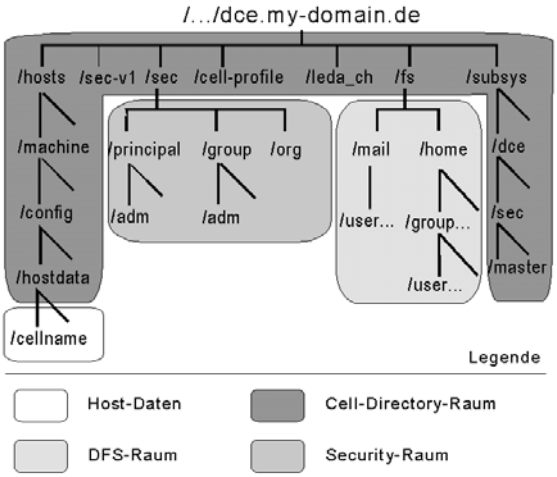

Abb. 1: Aufgabenteilung in einer DCE-Zelle

Workstation zu manipulieren. Das Bild 1 verdeutlicht ein wenig die Zusammenhänge.

Die globale Zellwurzel wird durch „/...“ repräsentiert, in ihr werden die Zellen eingehängt. Zwei Wege für globale Vernetzung stehen zur Verfügung:

- DNS
- X.500

Der Pfadname auf einen Rechner im DCE lautet:

/.../dce.hu-berlin.de/hosts/leda oder
/.../C=DE/O=HU-Berlin/OU=DCE/hosts/leda

Abkürzend kann „/.:“ für die eigene Zelle verwendet werden.

Security Service & ACLs

Wie der CDS-Raum ist auch der Security-Bereich in Directories strukturiert. Zusätzlich zu Nutzern und Gruppen gibt es die Institution der Organisation, an der Voreinstellungen wie Paßwortlänge für ihre Mitglieder vorgenommen werden können. Um eine weltweite Eindeutigkeit der Nutzer zu gewährleisten, wird bei der Account-Vergabe nicht nur für lokale Zwecke ein UID vergeben, sondern für zellüberschreitende Aktionen auch ein UUID (unique universal identifier). Für Nutzer können Aliasnamen angelegt werden, die sich den UID und UUID teilen (für Unix nicht unterscheidbar), aber verschiedene Namen, Paßworte, Home Directories usw. bekommen können.

Im Gegensatz zu NIS werden Änderungen in der Security-Datenbasis pro Datensatz an alle Replica Server verteilt.

Im gesamten DCE-Raum wird der Zugriff auf die Objekte (Nutzer, Dateien, Dienste ...) und Container (Directories) durch ACLs gesteuert. Das heißt, man kann im DCE den Zugriff zu Directories und Dateien, außer durch Unix-Modi, auch – wie im VINES üblich – durch Zugriffslisten steuern. In den Containern (Directories) ruhen drei ACLs, die, wie in Bild 2 dargestellt, vererbt werden.

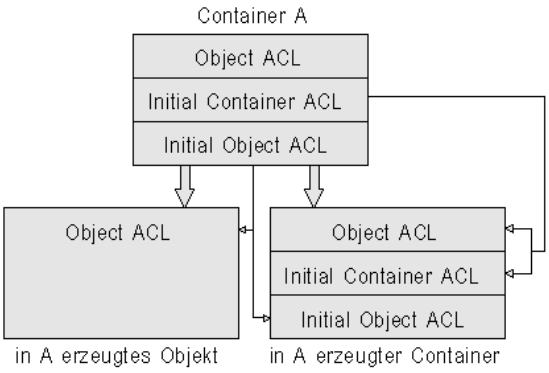

Abb. 2: ACL-Vererbung im DCE
Die dünnen Pfeile geben den Vererbungspfad an.

Folgende Access Rights kommen zur Anwendung:

- allgemeine ACLs:
  c- control (Recht ACL am Obj./Dir zu ändern)
  r- read (Leserecht am Objekt/im Directory)
  i- insert (Einfügerecht im Directory)
  d- delete (Löschrecht im Directory)
- zusätzliche ACLs im DFS
  w- write (Schreibrecht am Objekt/im Dir)
  x- execute (Ausführung am Objekt/im Dir)
- zusätzliche ACLs im Security-Bereich
  D- delete (Löschrecht am Objekt)
  n- name (Umbennungsrecht)
  ... und noch viele mehr

Bemerkung: zum Löschen im Security-Raum wird „d“-Recht im Directory und „D“-Recht am Objekt benötigt (siehe unten).

DFS

Mit DFS besitzt DCE ein globales File System, das auf Transarc’s AFS beruht. Für die ACLs pro Datei wurde als lokales File System das Episode File System integriert.

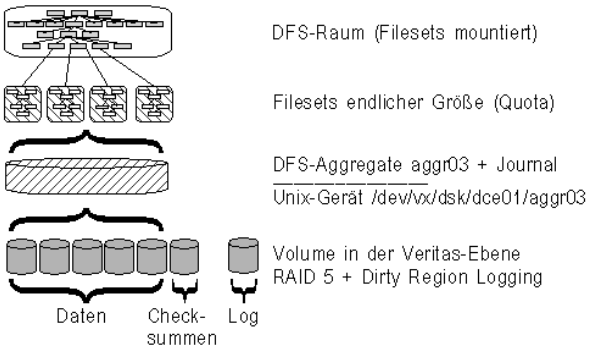

Abb. 3: Abbildung eines RAID-5 Volumes auf ein Aggregate, in dem Filesets des DSF liegen

Dieses Episode File System besteht aus zwei Komponenten:

- Aggregates
  sind physische Behälter, in denen Filesets erzeugt werden können. Für diese wird ein Journal über Schreibaktivitäten geführt, das nach einem Crash ein „fsck“ unnötig macht.
- Filesets
  sind „File Systeme“, die durch einen Quota-Mechanismus in ihrer Größe beschränkt werden.

Im Bild 3 wird ein RAID-5 Disk System in ein Unix-Gerät (/dev/...) abgebildet, das mit seinem Datenvolumen dann ein Aggregate bildet. In ihm können dann Filesets angelegt werden, die dann in den DFS-Raum über Mount-Punkte eingehängt werden. Wichtig ist an dieser Stelle, daß dieser DFS-Baum auf der Server-Seite zusammengefügt wird – unter Beteiligung aller

File Server der Zelle. Der Client importiert den fertigen DFS-Baum, wie in Bild 4 dargestellt (keine Arbeit am Client!).

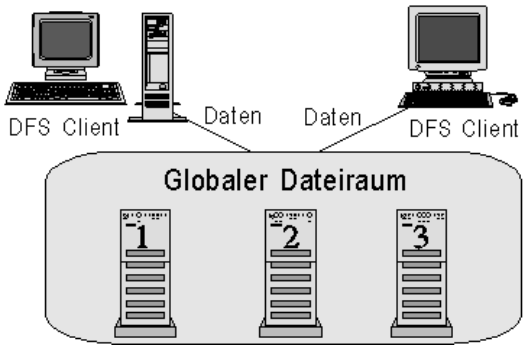

Abb. 4: Clients importieren den fertigen DFS-Raum

Zudem enthalten die Filesets keine Informationen vom Ort, an dem sie sich befinden. Ein Verschieben von Filesets von einem Server zum anderen bleibt für den DFS-Raum ohne Folgen.
Folgenden Eigenschaften besitzt DFS:

- Caching
  Clients cachen große Dateimengen und entlasten damit den Server.
- Replikation
  Filesets können ReadOnly auf andere Server repliziert werden.
- Backup
  DFS besitzt einen Netzwerk-Backup-Mechanismus.
- ACL
  Im DFS gibt es ACLs pro Datei.
- DFS/NFS Secure Gateway
  Systeme ohne DCE-Zugang können via NFS bedient werden.
- Fileset Komfort
  Filesets können im laufenden Betrieb vergrößert, verkleinert, gesichert und von einem Server zum anderen ge'move't werden.

Plattformübersicht

Im Workstation-Bereich wird die DCE-Software von den jeweiligen Anbietern zur Verfügung gestellt. Sun stellt dabei die Ausnahme dar – dort erfolgt eine Versorgung durch Transarc. Bei DEC, HP und IBM sind die Client-Komponenten und ein Teil der Server-Software Bestandteil von Campus- bzw. Korb-Verträgen. Bei allen anderen Systemen muß man zahlen. Für Windows 95/NT hat man bei der DCE-Software die Auswahl zwischen den Firmen Gradient, DEC und IBM. Die DFS-Bestandteile kommen dabei von Transarc. Die Abb. 5 gibt Auskunft über die DCE-Funktionalität jeder Plattform.

Im Rahmen unserer Testzelle sind die Server-Funktionalitäten von Sun und Win NT überprüft worden sowie die Client-Fähigkeit von DEC, HP, Sun, SGI und Win NT. Allen gemeinsam ist der Fakt, daß DCE auf ungepatchten Systemen so gut wie gar nicht läuft (sowohl Kernel als auch DCE Patche werden benötigt). Die Server laufen (im richtigen Patchlevel) sehr stabil. Die Clients konnten in den Grundfunktionalitäten CDS, Security, DFS auf allen Plattformen überzeugen. Ein integriertes Login (das sowohl lokale als auch DCE-Accounts umfaßt) wird bei DEC, HP und SGI mitgeliefert. Problematisch scheint lediglich Sun, da Transarc lediglich ein /bin/login in integrierter Form liefert (damit kein xdm, dtlogin, ftpd, rshd). Aber alle diese Löcher konnten aus dem Public Domain Umfeld geschlossen werden. Zudem ist ein umfassend integriertes Login für Solaris 2.6 angekündigt. Der DCE-Client von Gradient für Win NT beherrscht zwar ebenfalls einen solchen integrierten Login – setzt aber voraus, daß alle Accounts außer in der DCE-Registry noch in der NT-Registry mit gleichem Paßwort enthalten sein müssen, was indiskutabel erscheint. An der Lösung dieses Problems wird noch gearbeitet.

Plattform	Basic Client	DFS Client	Security Server	Cell Dir Server	Global Dir Server	Time Server	DFS Server	Episode File System
DEC-Unix	X	X	X	X	X	X	X	-
HP-UX	X	X	X	X	X	X	X	X
IBM-AIX	X	X	X	X	X	X	X	X
SGI-IRIX	X	X	X	X	X	X	X	-
Sun-Solaris	X	X	X	X	X	X	X	X
OS/2 1)	X	X	X	X	-	X	-	-
Win/NT	X	X	X	X	X	X	X	X
Win/95	X	X 2)	-	-	-	-	-	-
Win31	X	X 2)	-	-	-	-	-	-
MacOS	X	X 2)	-	-	-	-	-	-

1) Die Kenntnisse des Autors zu OS/2 sind älteren Datums und möglicherweise nicht mehr aktuell.
2) DFS-Light von Transarc

Abb. 5: Übersicht zu Plattformen und deren Funktionalität

Ansprüche ans DCE am RZ

Sieht man sich die Möglichkeiten von DCE an, so sollte man in die Startkonfiguration einer RZ-DCE-Zelle einige Überlegungen investieren. Drei Gegebenheiten spielen dabei eine Rolle:

- Fast die halbe Universität hat am RZ einen Account.
- Das RZ betreibt ein Dutzend File Server, verteilt auf verschiedene Standorte der Universität.
- Die Nutzerverwaltung von Teilen der Chemie und Physik geschieht per NIS am RZ.

Naheliegend ist es also, den Struktureinheiten, die es wünschen, die Verwaltung ihrer Nutzer und Nutzerdateien an ihrem Standort im Rahmen dieser DCE-Zelle durch sie selbst zu ermöglichen. Flankierend dazu kann der vor Ort befindliche File Server zum DFS-Server ausgebaut werden. Das heißt, eine zentrale Forderung an die Gestaltung der RZ-DCE-Zelle ist die Möglichkeit einer **dezentralen Verwaltung.**
Während Sicherheit, Skalierbarkeit und globales File System DCE/DFS-Features sind, ist für die Forderung der dezentralen Verwaltbarkeit einige Handarbeit notwendig. Zwei mögliche Herangehensweisen können in Betracht kommen:

- Für diese Struktureinheiten hierarchische Zellen ausgründen
- Innerhalb einer Zelle eine Struktur erzeugen, die gegeneinander abgeschirmte, administrative Bereiche im CDS-, DFS- und Security-Bereich enthält

Gegen die erste Variante spricht der Materialaufwand für neue Zellen. Zwei bis drei dedizierte Server pro Zelle müßten bereit stehen, die Security-Server sogar gut verschlossen. Der administrative Aufwand ist hoch, obwohl nur Nutzer- und Dateiverwaltung interessieren.

Die zweite Variante dagegen kommt mit geringerem Hardware-Aufwand aus. Die Stabilität der Zelle wird vom RZ gewährleistet, und die lokalen Administratoren kümmern sich nur noch um die Verwaltung von Nutzern, Dateien und Rechnern. Diese Vorgehensweise wird vom RZ favorisiert.

Das Konzept der dezentralen Verwaltung innerhalb einer Zelle ist von Dieter Mack (Rechenzentrum der Universität Stuttgart) schon vor Jahren formuliert worden. Im folgenden wird dieses Verwaltungskonzept vorgestellt, das auch Einfluß auf die Namensstruktur der Accounts hat.

Der strukturierte Namensraum

Wie erwähnt, ist der gesamte DCE-Raum in einer Directory-Struktur organisiert. Ob man im /.:/sec/principal-Directory Einträge vornehmen darf, hängt lediglich von den Zugriffsrechten (ACLs) ab. Um einen Tummelplatz für eine Vielzahl von gegeneinander abgeschirmter Admins im Security-Raum zu schaffen, nutzt man die Eigenschaft, auch im Security-Bereich Directories anlegen zu können. Man richtet eine Directory-Ebene für die zu administrierende Organisation ein, an der dann die Rechte befestigt werden, die es einem lokalen Admin erlauben, Nutzerverwaltung auszuüben. Ähnlich geht man im CDS-Raum für die Rechner-Einträge und im DFS-Raum für Dateiverzeichnisse vor. Das Bild 6 veranschaulicht eine solche administrative Domäne.

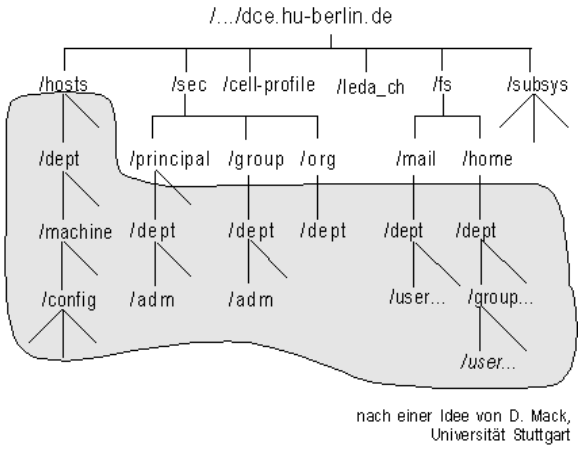

Abb. 6: Zusätzliche Directory-Ebene „dept“ im DCE

Der Nachteil dieses Verfahrens besteht darin, daß Accounts generiert werden, in denen das Directory (das zusätzlich im Security-Raum angelegt wurde) sichtbar ist, wie z. B. „bio/egon“. Die Unix-Systeme verhalten sich weitestgehend neutral. Das prinzipielle Zusammenspiel dieser Accounts mit dem Terminal-, Mail- und Web-Service ist schon gesichert. Ein Test mit Anwendungspaketen läuft.

Verteilte Rechte im Security-Raum

Ein Beispiel für die administrative Delegierung von Rechten soll das eben dargestellte Konzept verdeutlichen. Ein Admin der Geologie „geo/adm“ schaut sich die Zugriffsrechte in seiner Security-Umgebung an und sieht folgendes:

```
dcecp> acl show /.:/sec/principal/geo
{user geo/adm rid}
dcecp> acl show /.:/sec/principal/geo -io      1)
{user geo/adm rcDnfmaug}
dcecp> acl show /.:/sec/principal/geo/adm
{user_obj rfmaug}                              2)
```

1) Mit dem Flag „-io“ wird die Initial Object ACL angezeigt, d. h. die Liste, die ein neu geschaffener Nutzereintrag erbt.

2) Mit user_obj wird der Besitzer, in diesem Fall der Account „selbst“ = geo/adm bezeichnet.

Er hat Einfüge- und Löschrecht in seinem Directory, er hat volle Rechte bei allen Nutzern, die er anlegt. Aber er kann weder sich selbst noch sein Directory umbenennen (fehlendes „n“) oder löschen (fehlendes „D“), und er kann diesen Zustand durch ACL-Manipulation auch nicht ändern (fehlendes „c“). Es erscheint dem Autor wichtig, daß die Integrität des Security-Raumes nicht durch unbeabsichtigtes Löschen zerstört wird. Ein manipulierender Zugriff zum Directory /.:/sec/principal/bio wird ihm wegen fehlender Rechte in diesem Directory verwehrt. Dort hat der „bio/adm“ das Sagen.

DFS-Struktur

Der Pfad zu den Home-Directories ändert sich beim Übergang in das DFS. Folgender Pfad gilt dann:

/.../dce.hu-berlin.de/fs/home/org/group/ident

Die Studentin „med/susi“ wird dann im Directory

/.../dce.hu-berlin.de/fs/home/med/stud/susi

abgesetzt. Der derzeitige Quota-Mechanismus wird dahin gehend geändert, daß jeder Nutzer jetzt sein eigenes Fileset erhält. Das Fileset wird 10% größer sein als der vor der Umstellung vorhandene Quota-Wert, mindestens jedoch 10 MByte betragen.

Am importierten Software-Pfad ändert sich nichts. Das automount-Verzeichnis /volume wird durch einen Link ins DFS ersetzt, so daß ein Wechsel nach /volume/bin dann folgenden Pfad erzeugt:

/.../dce.hu-berlin.de/fs/volume/sparc_sunos55/bin,

sofern der Nutzer auf einer Sun arbeitet.

Die Dienste: Mail, Web, FTP...

Die entsprechenden Experten werden geeignete Formen der Mitteilung finden, um Änderungen, die sich beim Übergang zum DCE/DFS ergeben, kundzutun.

Die Ausnahmen

Es gibt Systeme am RZ, denen man beim besten Willen kein DCE mehr beibringen kann oder für die noch niemand einen DCE-Client geschrieben hat. Das sind zum einen die Convex C3820 und zum anderen alle unsere Linux-Systeme. Für diese Rechner wird ein DFS/NFS-Secure Gateway eingerichtet, das diesen einen Zugriff zum DFS ermöglicht (Bild 7). Um eine Zugriffsberechtigung zu erlangen, muß man allerdings ein Login am Gateway absolvieren. Für die Convex wird eine Paßwort-Datei aus der DCE-Registry erzeugt (dies ist schon für die weitere Unitree-Nutzung wichtig).

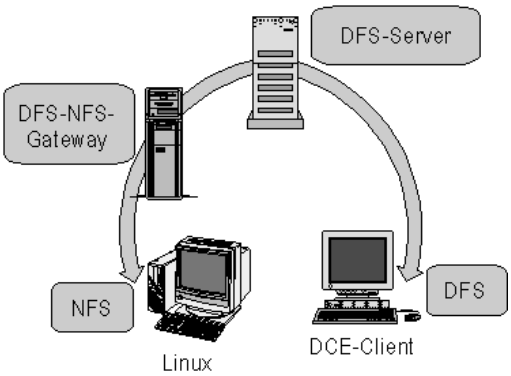

Abb. 7: Wirkung des DFS-NFS-Gateway

Der Prozeß der Einführung von DCE

Überblick

Die DCE-Registry kann nicht aus den verschlüsselten Paßwörtern der NIS-passwd-Datei aufgebaut werden, so steht das Problem, die Paßwörter der Nutzer ins DCE zu bringen. Da unsere Nutzer gehalten sind, einmal in sechs Monaten ihr Paßwort zu wechseln, nutzen wir diese Gelegenheit, ihr geändertes Paßwort in die vorbereitete DCE-Registry umzuleiten. Nach Ablauf von sechs Monaten wird NIS abgeschaltet und aus der Login-Policy der Client-Rechner entfernt. Zugleich werden die Home-Directories ins DFS kopiert und DCE wird damit die einzige Möglichkeit des Login.

Tag X-182: DCE-Registry wird erstellt

Sechs Monate vor Einführung von DCE wird die DCE-Registry aus der NIS-passwd und Datenbankinformationen erzeugt (Bild 8).

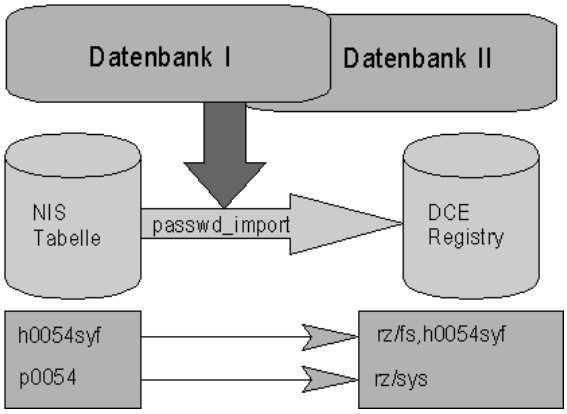

Abb. 8: Erzeugung der DCE-Registry

Der NIS-Account h0054syf wird in der Registry zu den zwei Accounts mit neuem und altem Home-Directory.

Typ	Account	Home Directory
Primär Alias	rz/fs h0054syf	/.:/fs/home/rz/sys/fs /home/p0054/h0054syf

Den alten Account als Alias einzurichten verfolgt zwei Ziele:

- In der Umstellphase können die Client-Rechner auf DCE umgestellt werden. Sollte einem Nutzer ein Login über DCE glücken, so wird er doch auf sein NFS Home Directory abgesetzt.

- Nach der Umstellung kann sich der vorletzte Nutzer, dem noch nicht aufgefallen ist, daß eine neue Zeit angebrochen ist, noch auf seinen alten Account anmelden (den letzten erreicht man ohnehin nicht).

Nach geglücktem Registry-Aufbau wird ab sofort jeder Nutzer-Paßwort-Wechsel sowohl im NIS als auch auf beiden DCE-Accounts vollzogen. Die NIS-Authentisierung auf den Unix-Systemen läuft bis zum Tag X weiter.

Tag X: UFS-DFS-Transfer

In den frühen Morgenstunden des Tages X stellen alle NFS-Server ihren Betrieb ein. Die Nutzerverzeichnisse und Mailboxen werden ins DFS kopiert (die Software ist schon am Vortag dort hineingelangt). Zeitgleich werden bei allen Alias-Accounts die Home-Directories auf das DFS-Home-Directory umgestellt. Alle NIS-Server stellen ihren Betrieb ein. Auf den Client-Rechnern wird die Login-Policy NIS entfernt. Mit dem Hochfahren der DFS-Server beginnt die DCE-Ära am RZ.

Tag X+91: Aliasnamen verlieren Gültigkeit

Drei Monate nach dem DCE-Start werden die Aliasnamen und damit die letzten Überreste der NIS-Zeit gelöscht.

Ausblicke

Cross-Cell-Authentication

Einen stabilen Betrieb unserer Produktionszelle vorausgesetzt, können Cross-Cell-Verbindungen zu weiteren universitären DCE-Zellen in Deutschland in Angriff genommen werden. Dann könnte man folgendes sehen:

```
% ls  /.../*
/.../dce.hu-berlin.de/fs
/.../dce.uni-karlsruhe.de/fs
/.../dce.uni-muenster.de/fs
/.../dce.uni-stuttgart.de/fs
...
```

Verbreitung in der HU

Aus Nutzersicht ist die DCE-Verbreitung aus vielen Gründen interessant. Zwei davon sind:

- Warum viele Accounts, wenn einer reicht?
- Er erreicht seine Daten an der HU, von der Uni Stuttgart oder von der Stanford University mit „cp“.

Welches Datum steckt hinter Tag X?

Voraussichtlich der 1. April 1999.

TLAs

ACL	- Access Control List
CDS	- Cell Directory Service
DCE	- Distributed Computing Environment
DFS [1]	- Distributed File System
DNS	- Domain Name Service
DTS	- Distributed Time Service
GDA	- Global Directory Agent
GDS	- Global Directory Service
LFS	- Local File System, auch EFS
EFS	- Episode File System oder Enhanced File System bei HP
NFS	- Network File System
NIS	- Network Information Service, Synonym für YP - Yellow Page
OSF	- Open Software Foundation
RPC	- Remote Procedure Call
TLA	- Three Letter Acronym
UFS	- Unix File System
UID	- Unix Identifier

[1] Microsoft führt mit Win NT 5.0 ebenfalls ein verteiltes File System mit Namen „DFS“ ein. Dieses hat mit dem hier besprochenen DCE-DFS nur das Kürzel gemeinsam, sonst gar nichts.

Frank Sittel
sittel@rz.hu-berlin.de

Statt einer Literaturangabe

Was	Wo
Copyright für das strukturierte Namenskonzept	http://www.uni-stuttgart.de/People/mack/
„Die“ DCE-Home Page	http://www.opengroup.org/tech/dce/
Sun-DCE und die komplette Dokumentation DCE 1.1	http://www.transarc.com/
IBM	http://www.networking.ibm.com/dce/dcehome.html
HP	http://www.hp.com/gsy/dce/products.html
DEC	http://www.digital.com/dce/
DCE für Win 3.1/95/NT, MacOS	http://www.gradient.com/
„Ein“ Versuch DCE für Linux	http://www.bu.edu/~jrd/FreeDCE/
Newsgruppe	news:comp.soft-sys.dce