DECOIT

CeBIT 2015

CeBIT cebit.com HANNOVER 16–20. MÄRZ 2015

Active Directory unter Linux

Prof- Dr.-Ing. Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
http://www.decoit.de
detken@decoit.de

Kurzvorstellung der DECOIT GmbH

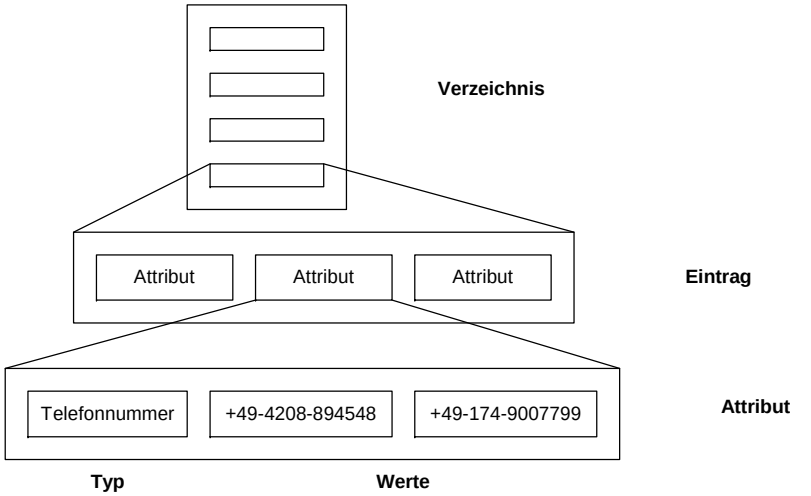
- Gründung am 01.01.2001
- Seit 2003: Sitz im Technologiepark an der Universität Bremen
- Fokus: Herstellerneutrale, ganzheitliche Beratung von IT-Lösungen
- Zielsetzung: akademische Lösungsansätze in kommerzielle Marktprodukte/Lösungen umsetzen
  - Consulting: ganzheitliche sowie herstellerneutrale Beratung
  - Systemmanagement: Umsetzung und Support von Hersteller- oder Open-Source-Lösungen
  - Software-Entwicklung: Entwickeln von Individuallösungen mit hohem Innovationscharakter
  - Forschungsprojekte: innovative IT-Lösungen
- Heute: Full-Service-Anbieter im IT-Umfeld
- Enge Kooperationen zu Herstellern, Anbietern und Hochschulen

Verzeichnisdienste

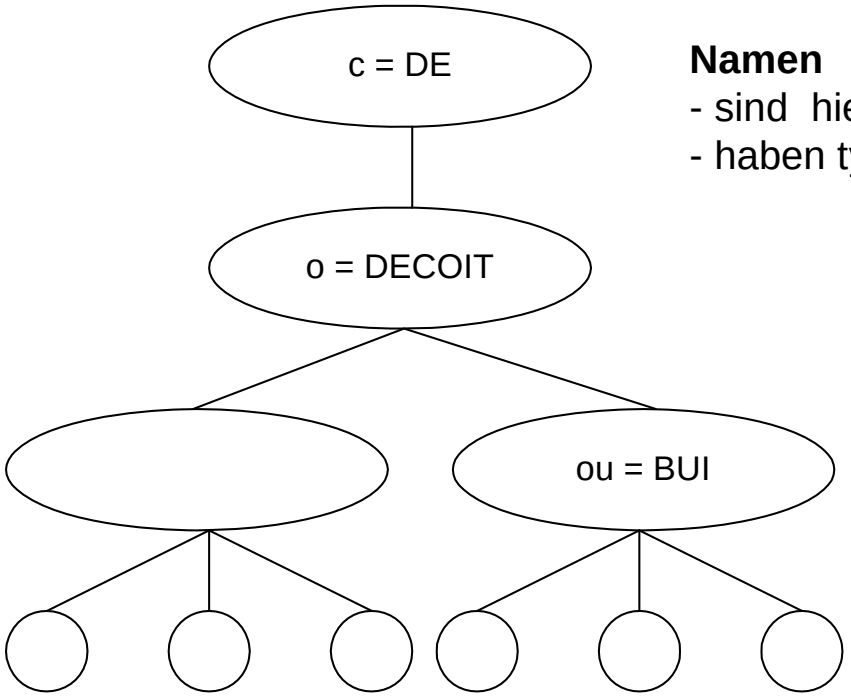
- Heute haben sich grundsätzlich zwei Verzeichnisdienste in Unternehmensnetzen durchgesetzt: Active Directory (AD) und Lightweight Directory Access Protocol (LDAP)
- Während das AD von Microsoft propagiert wird, setzt LDAP auf offene Internet-Standards nach RFC-4510 und RFC-4511
- Beide Verzeichnisdienste sind allerdings nur eingeschränkt kompatibel zueinander
- Ein Unternehmen muss sich daher im Normalfall entscheiden, auf welcher Basis es arbeiten will

Abbildung von Objekten

- Verzeichnisdienste werden verwendet, um an zentraler Stelle Anwender-, Rechner- und IP-Telefonie-Daten verwalten und Zugriffsrechte definieren zu können
- Dem Verzeichnisdienst liegt eine hierarchische Datenbank zugrunde, die ähnlich wie ein Telefonbuch aufgebaut ist
- Das Verzeichnis
  - Organisationseintrag
  - Gruppeneintrag
  - Geräteeintrag
  - Personeneintrag



Eindeutige Namen für Objekte



Namen
- sind hierarchisch
- haben typisierte Komponenten

Distingueshed Name
cn = Kai-Oliver Detken, ou = BUI, o = DECOIT, c = DE

DECOIT

Warum hierarchisch?

- Dezentrale Verwaltung der Daten: verteilte Verwaltung eines Verzeichnisses
- Durch Verzeichnispfade können doppelte Namen durchaus vorhanden sein (z.B. unterschiedliche Abteilungen)
- Flache Einträge (kein Verzeichnispfad) benötigen weniger Änderungen bei z.B. Wechsel einer Person in andere Abteilungen
- Alias-Einträge sind Pointer bzw. Soft-Links, die auf „echte“ Einträge zeigen
- Directory Information Tree (DIT)
  - Global eindeutige Namen
  - Skalierbar
  - Verteilt administrierbar
  - Verteilte Datenhaltung

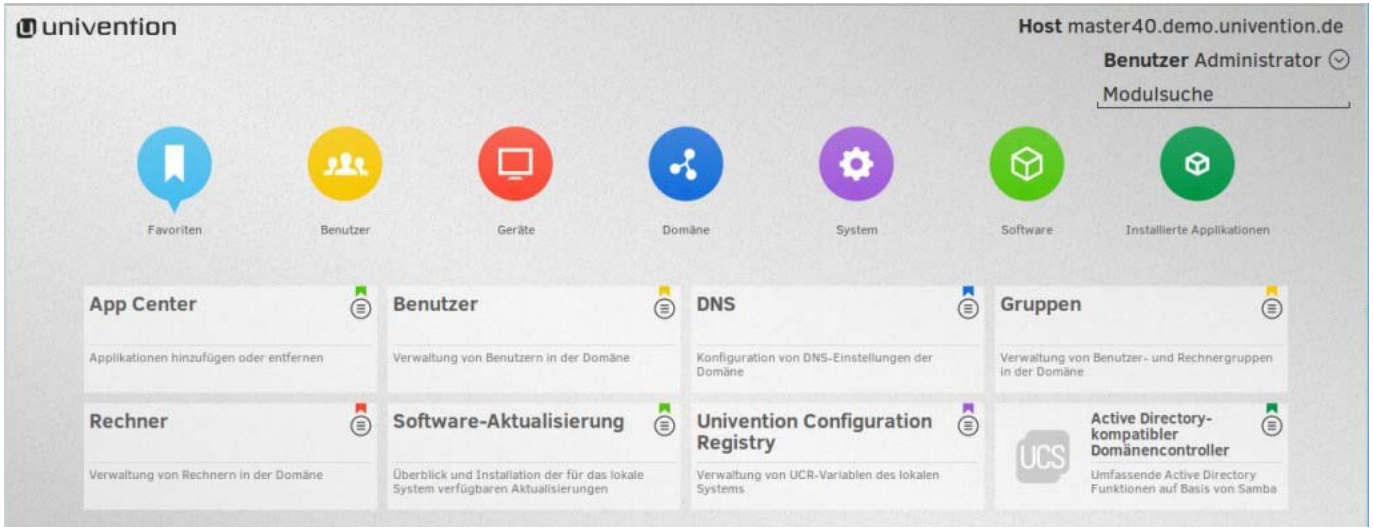
Heterogene Netze

- Heute kommen allerdings heterogene Netze zum Einsatz
- Oftmals werden Linux-, Mac-OS-X- und Windows-Systeme parallel eingesetzt
- Eine reine Microsoft-Umgebung mit AD-Verzeichnisdienst stößt dann aber an ihre Grenzen
- Nutzt man LDAP- und AD-Domänen parallel, sind auch die Eingaben mehrfach einzugeben für neue Objekte
- Daher wäre es optimal, wenn man eine zentrale Pflegemöglichkeiten hätte, ohne auf die Vorteile einer heterogenen Umgebung verzichten zu müssen
- Der Univention Corporate Server (UCS) bietet eine solche Möglichkeit an!

UCS-Serversystem

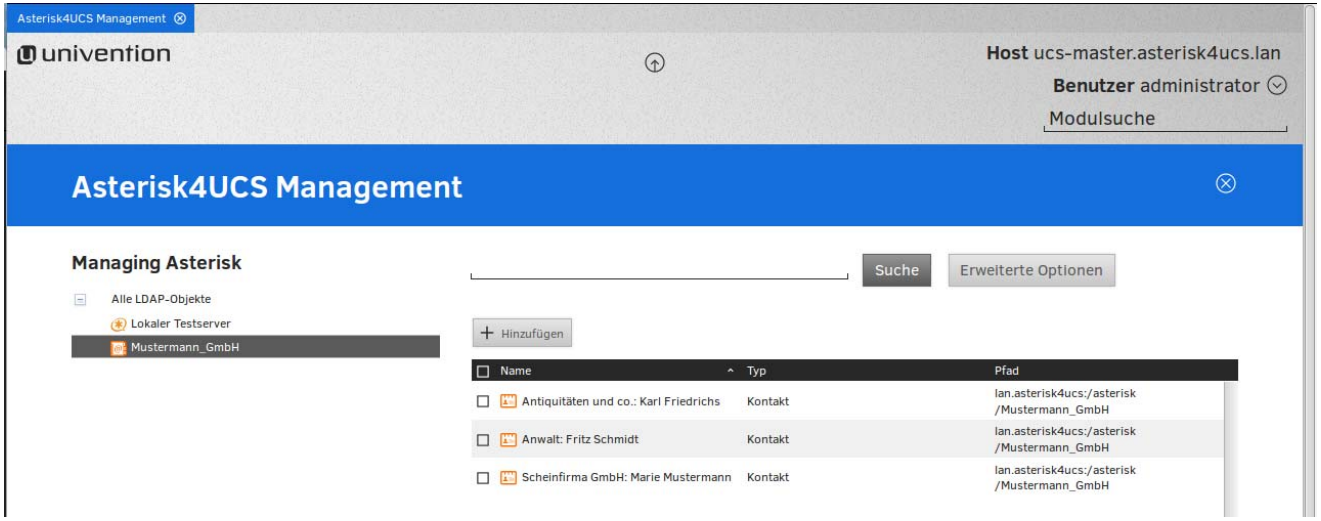
- Das UCS-Managementsystem enthält ein zentral administrierbares Identity-Managementsystem
- Dadurch kann ein einheitlicher Login – unabhängig davon, welche Dienste oder Systeme genutzt werden – eingerichtet werden
- Berechtigungen werden dabei über Rollenkonzepte oder Gruppenzugehörigkeiten definiert
- Auch anspruchsvolle Anforderungen lassen sich realisieren:
  - Selektive Replikation bestimmter Benutzerkonten (z.B. an Außenstandorten)
  - Integration Cloud-basierter Anwendungen
  - Erstellung hochwertiger Reports
  - Anbindung kundenspezifischer Datenbanken

Univention Management Console (UMC)



- In der Version UCS 4.0 wurde die grafische Oberfläche komplett überarbeitet (u.a. auch für mobile Geräte)
- Als Linux-Basis kommt Debian 7 „Wheezy“ mit dem Kernel 3.16 zum Einsatz
- Samba in der Version 4 ist enthalten (AD-Kompatibel!)

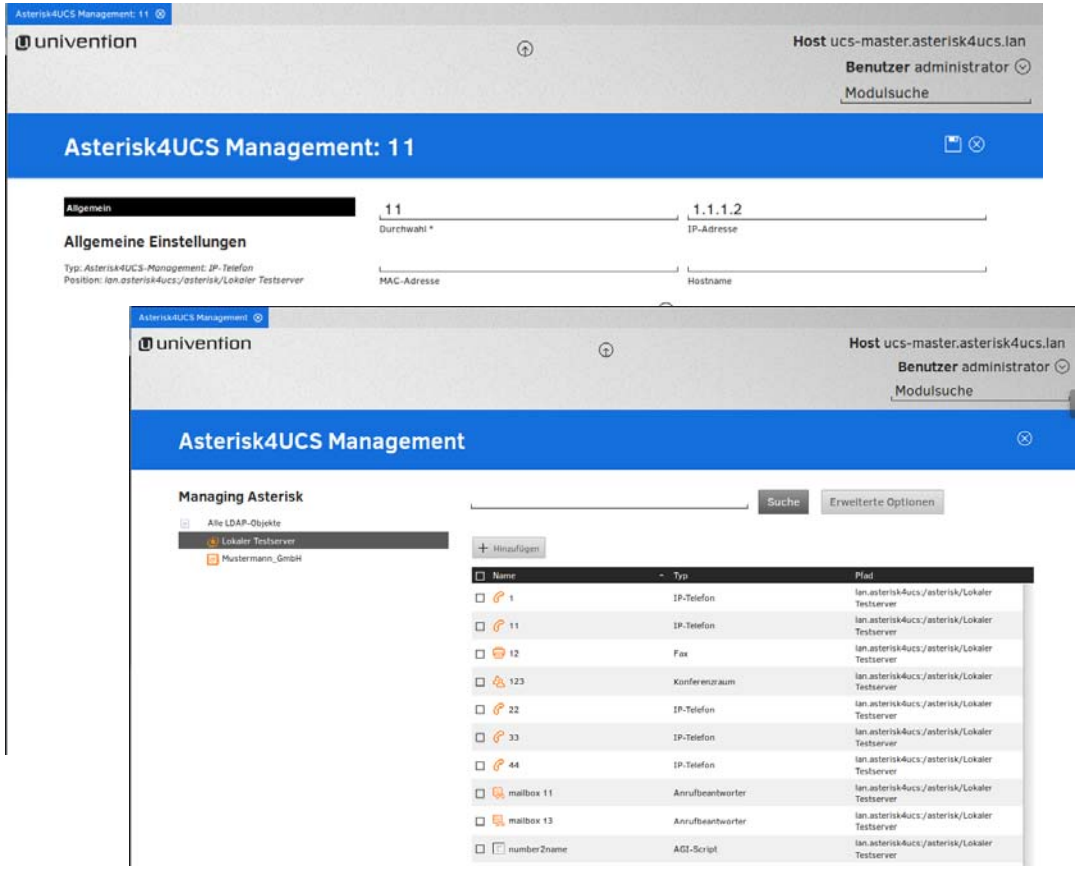
LDAP-Einbindung für Asterisk



- *Asterisk4UCS* ist eine zentrale Administrationsmöglichkeit für eine VoIP-basierte Asterisk-Umgebung auf UCS-Basis
- Der UCS-Server von Univention stellt ein zentrales Identity- und Infrastruktur-Management mittels LDAP bereit, welches durch Asterisk4UCS um IP-Telefonie-Daten erweitert wurde

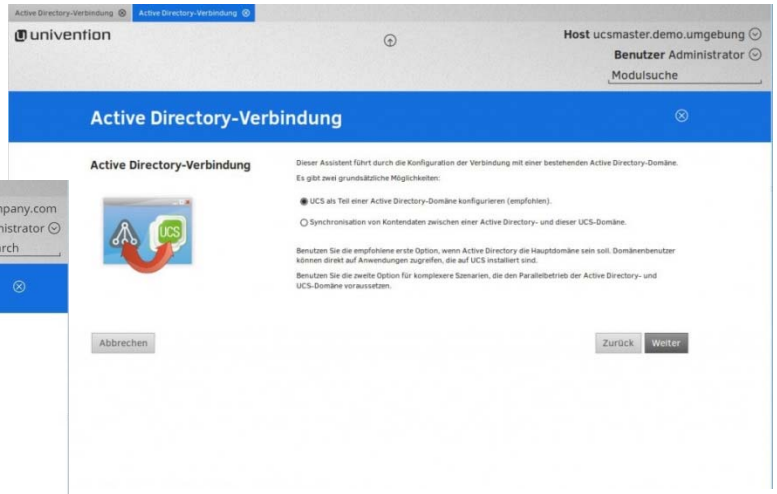
Asterisk4UCS-Kernfunktionalität

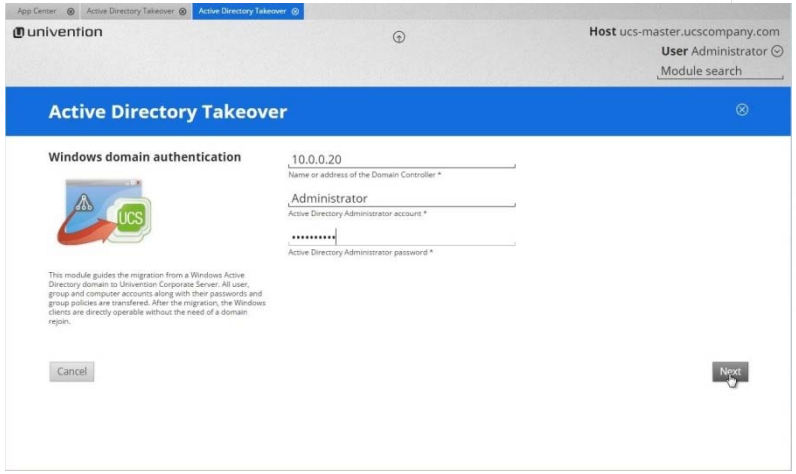
- Telefon- und Benutzerzuweisung
- Telefontypen
- Telefongruppen
- Konferenzräume
- Mailbox
- Warteschleifen
- Fax
- Faxgruppen
- Out-of-the-Box-Installation eines Asterisk-Systems



Zusammenspiel AD-LDAP

- Es lassen sich mit einem UCS-Server zwei verschiedene Varianten nutzen, um eine AD mit einzubeziehen:
  - Active-Directory-Verbindung
  - Active Directory Takeover





Active-Directory-Verbindung

- UCS baut analog zur Microsoft AD-Domäne einen Vertrauenskontext in Form einer UCS-Domäne auf, deren Identitäten wie Benutzer, Gruppen und Rechner im OpenLDAP-Verzeichnisdienst gespeichert werden
- Es können nun beide Systeme (Microsoft und UCS) transparent miteinander verbunden und ein Migrationspfad etabliert werden
- Mehrere AD-Domänen können parallel synchronisiert werden
- Zwei Anwendungen sind möglich:
  - UCS-Master kann einer gleichnamigen, bereits bestehenden AD-Domäne beitreten, wodurch diese auf alle UCS-Funktionen zugreifen kann (ohne Änderung an der AD-Domäne)
  - Automatische Synchronisation von verschlüsselten Passwörtern, Gruppendefinitionen und anderen Verzeichnisobjekten

Active Directory Takeover

- Mit AD Takeover lassen sich komplette Microsoft AD-Domänen zu UCS automatisch migrieren (AD 2003, 2008 und 2012)
- Der AD Takeover erkennt nach Eingabe der Adresse des bestehenden AD-Domänen-Controllers alle in der Domäne vorhandenen Benutzer, Computer und Gruppen
- Diese werden automatisch vollständig mit allen dazugehörenden Richtlinien in die neue Domäne kopiert
- An den Clients müssen keine weiteren Änderungen mehr vorgenommen werden und die Benutzer merken von der Umstellung nichts

DECOIT

Unternehmensvorteile

- Ein Unternehmen muss sich nicht mehr entscheiden, welchen Verzeichnisdienst es ausschließlich nutzen muss
- Es lassen sich die Vorzüge beider Welten miteinander vereinen
- Die heterogene Nutzung von Windows-Desktop-, Linux-Server- und Smartphone-Systemen macht dies auch unabdingbar
- Ein Unternehmen hat daher die Wahl und kann anhand der Funktionalität sowie den Lizenzkosten entscheiden, wo welches System zum Einsatz kommen soll

Zusammenfassung

- Verzeichnisdienste sollte heute in jeder Unternehmensgröße zum Einsatz kommen
- Zentrale Administration (z.B. der VoIP-Infrastruktur) wird ermöglicht
- Parallelbetrieb verschiedener Verzeichnisdienste ist möglich
- Die direkte Verbindung im Member Mode ermöglicht es, dass der UCS ein gleichwertiges Mitglied einer AD-Domäne wird
- Die Authentifizierung kann direkt gegen die AD-Domäne vorgenommen werden
- Dienste und Apps vom UCS lassen sich über die AD-Domäne nutzen
- Mehrserver-Umgebungen werden ebenfalls unterstützt
- Eine Komplettmigration auf LDAP (UCS) kann ebenfalls später vorgenommen werden

DECOIT

Vielen Dank für ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Tel.: 0421-596064-0
Fax: 0421-596064-09