Abschlussprüfung Sommer 2015

Fachinformatiker – Systemintegration

Dokumentation zur betrieblichen Projektarbeit

OpenLDAP- und FreeRADIUS-Server

Aufsetzen eines Identity Management-Servers als Ersatz eines veralteten CommuniGate Servers

Abgabetermin: Kaiserslautern, den 18. Mai 2015

Prüfungsbewerber:
Sebastian Deußer
Feuerbachstraße 15
67659 Kaiserslautern

Ausbildungsbetrieb:
taylorix institut für berufliche Bildung e.V.
Lutrinastraße 4
67655 Kaiserslautern

Praktikumsbetrieb:
fgn GmbH
Trippstadter Straße 122
67663 Kaiserslautern

Inhaltsverzeichnis

1. Einleitung

In den meisten Firmennetzwerken wird eine zentrale Stelle benötigt um verschiedene Anwender-Metadaten zu verwalten. Für diese Aufgabe wird üblicherweise ein Verzeichnisdienst verwendet. Basis eines Verzeichnisdienstes ist eine hierarchische Datenbank, die im Netzwerk verteilt angelegt sein kann. In dieser Datenbank können Daten zu verschiedenen Objekten abgelegt werden, wie etwa Konfigurationsdaten für Rechner oder diverse Daten für Anwender wie z.B. Name, Passwort, E-Mail-Konto, Gruppenzugehörigkeiten usw.. Die Anforderungen an einen Verzeichnisdienst wurden in den 80er Jahren von der International Telecommunication Union in der X.500-Spezifikation festgeschrieben, nachdem weltweit Telekommunikationsunternehmen jahrzehntelang Praxiserfahrungen mit dem Thema bei Erstellung und Verwaltung von Telefon-Verzeichnissen sammelten und diese zur Spezifikation beisteuerten.

In der Praxis stellte es sich als unpraktikabel für so gut wie alle Firmen – abgesehen von den großen Telekommunikationsunternehmen – heraus, die gesamte X.500-Spezifikation zu umzusetzen, da dies einen hohen Implementierungsaufwand darstellt und der Betrieb sehr hardwareintensiv ist. Deswegen wurde an der Universität von Michigan 1993 LDAP (Lightweight Directory Access Protocol) entwickelt welches ursprünglich als schlanke Alternative zum DAP (Directory Access Protocol) dienen sollte. DAP wurde traditionell zum Zugriff auf X.500-Verzeichnisse verwendet. Der Ansatz von LDAP war, den Zugriff durch den TCP/IP Protokollstapel zur ermöglichen, womit weit weniger Aufwand verbunden ist als es bei der kompletten Implementierung aller OSI-Schichten, wie es bei DAP der Fall ist. Heutzutage ist LDAP das verbreitetste Protokoll zur Abfrage von Verzeichnisdiensten, u.a. auch da TCP/IP-basierte Netzwerke in Firmennetzwerken der am häufigsten eingesetzte Netzwerktyp ist, und natürlich wegen dem wie beabsichtigt bedeutend geringerem mit LDAP verbundenen Aufwand. LDAP wird in vielen Anwendungen eingesetzt, vor allem im Adressbuchteil der meisten E-Mail-Clients wie z.B. Apple Adressbuch, Microsoft Outlook und Mozilla Thunderbird und in Verzeichnisdiensten wie z.B. Microsoft Active Directory Services, Apple Open Directory und dem aussterbenden Pionier Novell eDirectory. Wie viele Protokolle ist LDAP Client/Server-basiert.

In diesem Projekt wurde OpenLDAP verwendet. Dies ist die am weitesten verbreitete freie Open Source-Implementierung des Netzwerkstandards und steht unter einer eigenen freien Lizenz, der OpenLDAP Public License. OpenLDAP ist außerdem die Referenzimplementierung des Standards, weswegen es in vielen Belangen (z.B. bei Schema-Dateien) mehr auf Protokollkonformität achtet als andere Implementierungen. Im OpenLDAP Projekt ist nicht nur der Serverm der das Abfrageprotokoll zur Verfügung stellt enthalten, sondern auch ein Verzeichnisdienst. Es ist somit für viele Anwendungsfälle eine kostengünstige Lösung zum Aufbau eines Verzeichnisdienstes.

RADIUS (Remote Authentication Dial-In User Service) ist ebenfalls ein Client/Server-basiertes Protokoll zur Authentifizierung, Autorisierung und zum Accounting (AAA-System) von Benutzern bei Einwahlverbindungen zu Netzwerken. RADIUS stellt den de-facto-Standard zur zentralen Authentifizierung von Einwahlverbindungen wie z.B. über ISDN, DSL und WLAN (über IEEE 802.1X) dar. Üblicherweise ist ein RADIUS-Server an einen Verzeichnisdienst angebunden, um von diesem die Benutzerdaten für die Authentifizierung und Autorisierung (und teilweise auch Accounting) abzufragen.

Hier wurde FreeRADIUS verwendet, der – laut Aussage des Projektes – weltweit ver-

breitetste RADIUS-Server. Das freie Open Source-Projekt unter der GPLv2-Lizenz umfasst neben dem RADIUS Server außerdem eine PAM-Bibliothek, ein Apache-Webserver-Modul und eine Client-Bibliothek (im Gegensatz zum Rest des Projektes steht diese unter der BSD-Lizenz).

2. Projektbeschreibung

2.1. Projektumfeld

Die fgn GmbH wurde im August 2000 als SpinOff der Technische Universität (TU) Kaiserslautern gegründet. Die Gründer waren zuvor mehrere Jahre (seit 1996 bzw. 1989) als freischaffende Consultants und Trainer tätig. Die Firma pflegt enge Kontakte zum Regionalen Hochschulrechenzentrum Kaiserslautern (RHRK), da die meisten Mitarbeiter das Netz der TU Kaiserslautern mit ca. 10.000 Ports und Diensten wie Mail, DNS und DHCP in der Vergangenheit betreut haben oder es noch heute betreuen.

Die Kernkompetenz der fgn GmbH ist anspruchsvolles Netzwerk-Knowhow, welches als Dienstleistung in drei eng verknüpften Tätigkeitsfeldern angeboten wird: Schulungen, Workshops und Netzwerk-Consulting (Beratung und vor-Ort-Support von Firmen bei Problemen, Umstrukturierungen, Erweiterungen und Neuaufbau von Produktivnetzwerken).

2.2. Ist-Analyse

Im Praktikumsbetrieb fgn GmbH laufen der E-Mail-Verkehr und die Authentifizierung an den internen Webservices und am OpenVPN-Server über einen alten CommuniGate-Server (v5.0.13 von November 2006). Ursprünglich wurde dieser auf einem eigenen Rechner aufgesetzt, inzwischen aber, wie viele andere Rechner der Firma, virtualisiert.

Die Webservices, die ihn zur Anwender-Authentifizierung verwenden, laufen auf drei anderen VMs, ebenso der OpenVPN-Server. Sie kommunizieren mit dem LDAP-Teil von CommuniGate mittels des Apache-Moduls `mod_ldap` und verwenden zur Autorisierung entsprechend `mod_authnz_ldap` (bzw. auf einem der Rechner wegen eines veralteten Apache Webserver noch `mod_auth_ldap`). Apache prüft dabei momentan nur auf Existenz des angegebenen Benutzeraccounts und ob das richtige Passwort angegeben wurde. Weitere Berechtigungen sind momentan nicht implementiert. Die Ausnahmen dazu sind Nagios und Egroupware, die zwar Berechtigungsgruppen verwenden, diese aber intern verwalten und nicht in LDAP ablegen.

Lediglich die Anwenderkonten auf den Betriebssystemen der diversen Anwender-PCs sind nicht von CommuniGate abhängig. Da die fgn GmbH über das Netz der Technischen Universität Kaiserslautern angebunden ist, müssen alle E-Mails auch über die E-Mail-Server der Universität laufen. Diese verwenden RADIUS, um zu prüfen, ob die E-Mailkonten der Domain `fg-networking.de` tatsächlich vorhanden sind. Der RADIUS-Server dazu wird ebenso von CommuniGate bereitgestellt.

Wegen der recht alten Softwareversion gibt es schon seit längerem regelmäßig Probleme, z.B. mit der SSL-Authentifizierung neuerer E-Mail-Clients (die unterstützten Versionen von SSL/TLS benutzen aktuelle E-Mail-Clients aus Sicherheitsgründen nur noch ungern). Ein weiteres großes Sicherheitsproblem von CommuniGate ist, dass es die Passwörter aller Anwenderkonten im Klartext (ohne sie vorher zu hashen o.ä.) in Textdateien auf dem Server abspeichert.

2.3. Soll-Analyse

Eine Aktualisierung von CommuniGate wäre mit ähnlichem Aufwand verbunden, wie ihn ein komplett neues Aufsetzen von Ersatzservern erfordert (und wäre außerdem mit dem Kauf einer neuen Lizenz verbunden). Deswegen wurde entschieden, die Serverkomponenten E-Mail und Identity Management durch neue Server abzulösen. Da in der Firma momentan sehr viel freie Software verwendet wird, sollen die Ersatzserver auch auf Basis von freier Software aufgesetzt werden. Weil die E-Mail-Infrastruktur sehr kritisch für die Arbeit der Firma ist und bei der Migration der E-Mail-Konten mit vielen vertraulichen firmeninternen Informationen hantiert werden muss, soll die Installation des neuen E-Mail-Servers von einem Mitarbeiter von fgn durchgeführt werden.

Für das Identity Management sollen OpenLDAP und FreeRADIUS zum Einsatz kommen, da dies die verbreitetsten freien Implementierungen von LDAP und RADIUS sind und somit in Büchern und dem Internet das meiste Know-How verfügbar ist. Außerdem erleichert es die spätere Pflege des Systems, da sich für solche verbreiteten Systeme einfacher Personal mit Fachkenntnis finden lässt als für die meisten anderen proprietären Implementierungen.

Für die Verteilung von E-Mails soll ein `postfix`-Server verwendet werden, allerdings war dieser zur Fertigstellung dieses Projektes noch nicht einsatzfähig. Die Integration des neuen E-Mailservers ist damit nicht Teil dieses Projektes und wird zu einem späteren Zeitpunkt durchgeführt. Es werden dazu lediglich die Vorarbeiten auf der Seite des Identity Management getätigt, die unabhängig von der endgültigen Konfiguration des neuen E-Mail-Servers sind.

Somit müssen im Rahmen der Projektarbeit folgende Arbeiten durchgeführt werden:

- Linux-Grundsystem installieren
- OpenLDAP-Server auf dem Linux-System installieren
- OpenLDAP-Server konfigurieren
- Verzeichnisstruktur erstellen
- grundlegende Benutzerdaten (Name, Passwort) aus bestehendem System übernehmen
- FreeRADIUS-Server installieren
- FreeRADIUS-Server konfigurieren und an den OpenLDAP-Server anbinden
- Absicherung des Systems
- Umkonfiguration der entsprechenden Systeme auf den neuen LDAP-Server
- Funktions- und Sicherheitstests

2.4. Wirtschaftlichkeits-Analyse

Wie bereits in der Ist-Analyse erwähnt, gibt es auf Grund des Alters der im bestehenden CommuniGate-Server enthaltenen SSL/TLS-Implementierung regelmäßig Probleme mit neueren E-Mail-Clients. Dies frisst dann jedes Mal Arbeitszeit von zwei Mitarbeitern, dem Mitarbeiter mit dem „zu neuen“ E-Mail-Client und dem fgn-Mitarbeiter der

sich mit den Einstellungen im E-Mail-Client auskennt. Dies passiert inzwischen regelmäßig, praktisch bei jedem Update des verwenden E-Mail-Clients Mozillla Thunderbird (ca. 10 pro Jahr) und verschwendet bei beiden Mitarbeitern mindestens eine halbe Stunde Arbeitszeit. Dies betrifft im Moment drei Mitarbeiter (den E-Mail-Spezialisten nicht mitgerechnet), somit ist dies bei einem angenommen Stundenlohn von 71€ eine Arbeitsausfall von $3 * 2 * 10 * \frac{1}{2}\text{h} * 71€/\text{h} = 2.130€$ pro Jahr. Außerdem wird sehr wahrscheinlich wird der E-Mail-Server irgendwann überhaupt nicht mehr mit neueren E-Mail-Clients benutzbar sein, was etliche der Prozesse der Firma lahmlegen wird. Der Arbeitsausfall davon lässt sich kaum voraussagen, da man in diesem Fall überhastet einen neuen E-Mail-Server aufsetzen müsste, und sich die wirtschaftlichen Folgen einer überhasteten Neuinstallation nur schwer abschätzen lassen. Es würde auch bei den Kunden von fgn ein Image-Schaden entstehen, der kaum in Geld auszudrücken ist.

Die auf der Hand liegende Alternative zu der in diesem Projekt verwendeten Software wäre es eine neue CommuniGate Pro Firmenlizenz zu kaufen. Die Kosten dafür hängen bei von CommuniGate so genannten „Small Licenses“ von der Anzahl der verwalteten E-Mail-Konten ab. Momentan werden bei fgn davon 46 verwaltet, die Softwarelizenz für 50 Konten würde also in absehbarer Zeit zu knapp werden. Der Preis für eine Lizenz für 75 E-Mail-Konten (die nächstgrößere Lizenz) beträgt momentan 1.849€. Dazu kämen dann noch zusätzliche Kosten um alle 10-26 Monate die Lizenz zu verlängern um weiterhin Updates und Support zu erhalten. Momentan sind dies zwischen 277,35€ und 721,11€. Und es ist nicht zu erwarten, dass diese Preise konstant bleiben oder fallen werden. Außerdem kommt bei der Umstellung noch ein nicht unerheblicher Arbeitsaufwand hinzu bei der Migration von der sehr veralteten Server-Version in die neue Version.

Da der Gegenstand dieses Projektes ein Teilersatz des CommuniGate-Servers war, lassen sich die Kosten leider nicht 1:1 miteinander verrechnen. Trotzdem ist als Vorteil anzurechnen, dass keine regelmäßigen Kosten entstehen wie es bei einer ständig erneuerten CommuniGate-Lizenz oder den Problemen nach jedem Thunderbird Update. Die Gesamtkosten des Projekts betrugen 2.485€ (eine genaue Aufstellung findet sich unter Projektkosten), somit amortisiert sich das Projekt gegenüber dem bisherigen Zustand innerhalb des zweiten Jahres. Verglichen mit einem Upgrade von CommuniGate amortisiert es sich erst nach zwei Jahren, aber nur dann, wenn man den Arbeitsaufwand für das CommuniGate Upgrade außer Acht läßt. Da erwartet wird, dass dieser mit dem Gesamtaufwand des Projektes vergleichbar ist, sind die Projektkosten also direkt günstiger als die Kosten für dieselbe Arbeit plus den CommuniGate Lizenzkosten.

2.5. Vorgaben

2.5.1. Wirtschaftliche Vorgaben

Wie die meisten anderen Server der fgn GmbH soll das neue Serversystem in einer eigenen Virtual Machine auf einem der bereits bestehenden VMware ESXi-Servers laufen, weswegen keine zusätzlichen Hardwarekosten anfallen. Da in dem Projekt zudem ausschließlich freie Software zum Einsatz kommen soll, fallen auch keine Softwarelizenzkosten an.

2.5.2. Organisatorische Vorgaben

Das Projekt wird im Praktikumsbetrieb mit Unterstützung des Mitarbeiters Erik Auerswald durchgeführt. Neben der Projektdokumentation wird zusätzlich eine Kundendokumentation für Administratoren im firmeninternen Wiki erstellt. Hinzu kommen Funktions- und Sicherheitstests zur Qualitätssicherung. Eine Anwenderdokumentation ist nicht notwendig, da sich aus Sicht des Anwenders nichts gegenüber dem Ausgangszustand ändern soll.

2.5.3. Zeitliche Vorgaben

Das Projekt wird im Zeitraum vom 04.05.2015 – 18.05.2015 durchgeführt, wobei die Bearbeitungszeit von 35 Stunden nicht überschritten werden darf.

3. Projektplanung

3.1. Planung des Ersatzservers

Als Ersatzserver wurde eine neue Virtual Machine auf einen der firmeneigenen ESXi Servern verwendet. Als Betriebssystem wurde Debian Stable (zur Durchführungszeit des Projektes Version 8.0 Jessie) mit der Standardpaketauswahl ohne zusätzliche Vorauswahlen installiert.

3.2. Planung des Kommunikationskonzepts

Sämtliche firmeninternen Webservices, der OpenVPN-Server, der kommende neue E-Mail-Server und der FreeRADIUS-Daemon greifen über das LDAP – hier ist das Protokoll gemeint – auf den OpenLDAP-Daemon zu, um Benutzer zu authentifizieren und nutzerspezifische Einstellungen abzufragen. Die E-Mail-Server der Universität greifen auf den FreeRADIUS-Daemon zu um Benutzerkonten zu prüfen, welcher daraufhin die entsprechenden Daten beim OpenLDAP-Daemon – per LDAP – erfragt.

3.3. Planung des Sicherheitskonzepts

Das Firmennetzwerk der fgn GmbH ist über das Netzwerk der TU Kaiserslautern ans Internet angebunden. Entsprechend wird jeglicher Netzwerkverkehr von der TU-Firewall vorgefiltert. Das Firmennetz von fgn ist zusätzlich noch durch eine eigene Firewall gesichert. In diese muss – analog zur alten Regel – eine Ausnahme für den neuen RADIUS Server eingetragen werden. Zusätzlich wird auf dem neuen Server eine Software-Firewall installiert, die nur die für LDAP, RADIUS und zur Wartung benötigten Ports zulassen soll.

3.4. Projektablaufplan

Analyse und Planung (insgesamt 6 h)

- Ist-Analyse (3 h)
  - Analyse des bestehenden CommuniGate-Servers und der damit verbundenen Webservices (2 h)

  - Aufnahme der Anforderungen an einen Ersatzserver (1 h)

- Planung (3 h)
  - Ausarbeitung eines Konzepts für den Ersatzserver (1 h)
  - Ausarbeitung des Sicherheitskonzepts (unter Berücksichtigung des Firmenkonzepts) (1 h)
  - Ausarbeitung des Kommunikationskonzepts (Serverdienste untereinander und extern) (1 h)

Umsetzung (insgesamt 20 h)

- Vorbereitungen (6 h)
  - Dokumentation der Konfiguration des zu ersetzenden Servers (2 h)
  - Erstellen einer Liste aller Dienste, die das bestehende Identity Management nutzen (2 h)
  - Prüfung von Möglichkeiten zum Importieren der bestehenden Anwender-Konten in die neue Lösung (2 h)
- Installation und Einrichtung des neuen Servers (8 h)
  - Grundinstallation des Linux-Systems des neuen Servers (1 h)
  - Installation und Konfiguration des LDAP-Servers (3 h)
  - Installation und Konfiguration des RADIUS-Servers (2 h)
  - Absicherung des Rechners (Firewall etc.) (2 h)
- Abschließende Arbeiten (6 h)
  - Umkonfiguration der Webservices (2 h)
  - Import/Anlegen der Anwenderkonten (2 h)
  - Funktions- und Sicherheitstests (2 h)

Dokumentation (insgesamt 9 h)

- Erstellen der Projektdokumentation (8 h)
- Erstellen der Dokumentation für das firmeninterne Wiki (1 h)

4. Umsetzung

4.1. Vorbereitungen

4.1.1. Dokumentation der Konfiguration des zu ersetzenden Servers

Da die Konfigurationsdateien des CommuniGate-Servers sämtliche Anwenderpasswörter im Klartext enthalten, konnte dem firmenexternen Bearbeiter dieses Projektes aus Sicherheitsgründen kein direkter Zugriff auf den Server gewährt werden. Allerdings war dies auch nur bedingt notwendig, da zum Erfassen der wichtigen Konfigurationsdetails (vornehmlich der Struktur des integrierten Verzeichnisdienstes) lediglich Zugriff

auf das Webinterface des Servers (zugänglich unter Port 9010 auf dem bisherigen Server mail.fg-networking.de, Zugriff durch Firewall von außerhalb des Firmennetzes geblockt) notwendig war. Unter Aufsicht von Herrn Auerswald wurde ein Auszug der im Klartext gespeicherten Benutzerdaten begutachtet, vor allem der Eintrag für das Benutzerkonto des Bearbeiters da ihm dieses Passwort bereits bekannt war. Dabei fiel auf, dass alles in einer gut organisierten Ordnerstruktur abgelegt ist, es existiert eine Datei pro Anwender und die Daten in der Datei sind in bezeichneten Feldern abgelegt.

Für das Projekt am Wichtigsten zu beachten war, dass der E-Mail-Server für drei Domains Anwenderkonten verwaltet: fg-networking.de, schabler.de und worden.de. Dies musste natürlich beim Entwurf der neuen Verzeichnisstruktur beachtet werden, um später die Anbindung des neuen E-Mailserver ohne unnötige erneute Umbauten am LDAP zu ermöglichen.

4.1.2. Erstellen einer Liste aller Dienste die das bestehende Identity Management nutzen

Die Webtools, die den bisherigen LDAP-Server verwenden, laufen unter Apache-Webservern auf den Rechnern aio, nms und lab-mm. Sie alle benutzen zum Abfragen von Nutzerdaten die Apache-eigenen LDAP-Module (mod_ldap und mod_authnz_ldap, bzw. mod_auth_ldap auf aio, da hier noch eine ältere Apache-Version verwendet wird).

Somit ist bei der Konfiguration aller Webserver prinzipiell dasselbe zu ändern, damit später der neue Server verwendet wird. So verwenden z.B. alle den alten Server ohne SSL, weswegen zusätzlich zur neuen LDAP- Server-URI auch noch das passende CA Stammzertifkat einzutragen ist. Kopiert werden muss dieses nicht extra, da es auf allen Rechnern bereits zum Bereitstellen von HTTPS-Verbindungen installiert wurde.

Oberflächlich gibt es in der Konfiguration natürlich auch Unterschiede. So haben auf aio mehrere Tools eigene <Location>-Einträge in der Konfiguration in denen jeweils der LDAP Server eingestellt ist, während es auf nms lediglich einen Eintrag für alle Webtools gibt. Aber diese Detailunterschiede machen keinen wirklichen Unterschied bei den später vorzunehmenden Änderungen.

Die Konfiguration von OpenVPN muss auch lediglich auf die neue Server-URL und BaseDN umgestellt werden, sowie das Stammzertifikat eingetragen werden. Dies geschieht in der Datei /etc/openvpn/auth-ldap.config, näheres dazu siehe Änderungen an der OpenVPN Konfiguration in der Kundendokumentation.

Bei Begutachtung der Egroupware-Konfiguration im Administrationsmenü fiel auf, dass hier keine Einstellungen zu LDAP zu finden waren. Nach kurzer Recherche stellte sich heraus, dass in Egroupware – wie bei vielen PHP-Webanwendungen – manche Einstellungen nur im Installer vornehmbar sind, wie z.B. die LDAP-Einstellungen. Das Passwort für diesen Installer leider nicht – wie sonst üblich – im Firmenwiki hinterlegt, und der mit dem Installer vertraute Mitarbeiter befand sich zu Bearbeitungszeit des Projektes im Urlaub. Man hätte zwar relativ einfach das Passwort des Installers durch Editieren der entsprechenden PHP Datei ändern können, aber da keiner der Anwesenden mit dem Egroupware-Installer vertraut war und die Groupware sehr wichtig für die Arbeit der Firma ist, wurde entschieden, sie erst später vom zuständigen Mitarbeiter auf den neuen LDAP-Server umstellen zu lassen.

4.1.3. Prüfung von Möglichkeiten zum Importieren der bestehenden Anwenderkonten in die neue Lösung

Leider bietet CommuniGate selbst keine Funktion zum Export seiner Benutzerdaten an. Über die OpenLDAP-Utils wäre ein Auslesen der Daten möglich, in einer Form, die man in das neue LDAP wieder importieren könnte. Da allerdings CommuniGate für die E-Mail betreffenden Attribute ein proprietäres LDAP-Schema benutzt, wäre der Nachbearbeitungsaufwand für diese Daten sehr hoch.

Aber es sollten erst einmal nur die notwendigsten Attribute (siehe Übernommene LDAP Attribute im Anhang) übernommen werden und CommuniGate speichert die Anwenderdaten in einer mit den Standard Unix/Linux Textverarbeitungswerkzeugen (`sed`, `awk`, `cut`) vergleichsweise einfach verarbeitbaren Form. Somit stellte das Erzeugen von durch LDAP importierbaren Datensätze aus den gespeicherten Dateien von CommuniGate mit Hilfe von Skripten in diesem Fall die sinnvollste Vorgehensweise dar. Da das Entwickeln der Skripte ohne Zugriff auf die Daten umständlich gewesen wäre, hatte Herr Auerswald sich bereit erklärt, diese zu schreiben, da ihm Zugriff auf die Anwenderpasswörter erlaubt ist. Als Unterstützung bei dieser Arbeit wurden Herrn Auerswald ein Template der zu generierenden LDAP Importdaten und der Befehlsaufruf von `slappasswd` zur Verfügung gestellt. Letzteres wird in einem zweiten Skript zum passenden hashen der Passwörter verwendet, damit in den Importdaten nur noch Passwort-Hashes stehen, und diese mit nur noch geringen Datenschutz- und Sicherheitsbedenken verwendet werden können.

4.2. Installation und Einrichtung des neuen Servers

4.2.1. Grundinstallation des Linux Systems des neuen Servers

Nach der Erstellung einer neuen VM durch einen Mitarbeiter von fgn auf dem entsprechendem ESXi-Server wurde der Installer der aktuellen Debian Stable (Version 8.0 `Jessie` zur Bearbeitungszeit des Projektes) ausgeführt und das Grundsystem installiert. Dabei wurden keine der zusätzlichen Paketvorauswahlen (Debian `tasksel`) dazugenommen. Der Debian-Installer hat bei während des Installationsprozesses nach Rückfragen auch die Grundeinrichtung für Basis-Einstellung wie z.B. IP-Adressen und Hostname vorgenommen. Für den neuen Rechner wurde der Hostname `id` in der Domain der Firma (`fg-networking.de`) gewählt.

4.2.2. Installation und Konfiguration des LDAP-Servers

Nach der Grundinstallation wurden im neuen System dann die Pakete `slapd` (benannt nach dem Namen des OpenLDAP-Daemons), `ldap-utils` und `ldapscripts` sowie deren noch nicht im System vorhandenen Paketabhängigkeiten installiert. Da LDAP-over-SSL (LDAPS) verwendet werden soll, damit die über LDAP abgefragten Daten verschlüsselt übertragen werden, mussten mit der Certificate Authority (CA) der Firma ein Zertifikat und ein Private Key für den Server erstellt und zusammen mit dem Stammzertifikat der CA auf den neuen Server kopiert werden.

Beim Entwurf der Verzeichnisstruktur ergaben sich verschiedene Probleme:
Um in einem LDAP-Verzeichnis neue Attribute zu definieren, gibt es sogenannte Schema (eigener Ausdruck, nicht zu verwechseln mit Schema/Schemata). CommuniGate

verwendet zum Verwalten der E-Mail-Anwenderdaten ein eigenes proprietäres LDAP-Schema, um die Daten in selbst definierten Attributen zu speichern. Diese Attribute können somit nicht ins neue LDAP übernommen werden, ohne verschiedene Implementierungsentscheidungen für den neuen E-Mailserver zu kennen. Da dieser zur Bearbeitungszeit dieses Projektes noch nicht weit genug fortgeschritten war, um eine Absprache zu ermöglichen, wurde entschieden, erst einmal nur die wichtigsten Attribute zu übernehmen und die E-Mail Attribute später anzupassen. Dies wird sehr wahrscheinlich auch wieder mittels per Skript generierten Datensätzen möglich sein und stellt somit einen vertretbar geringen Mehraufwand für die E-Mail Server-Einrichtung dar.

Weiterhin musste die neue Verzeichnisstruktur berücksichtigen, dass mehrere voneinander unabhängige Namensräume (die drei in Dokumentation der Konfiguration des zu ersetzenden Servers erwähnten E-Mail Domains) zu verwalten sind. Das bedeutet, dass in den Domains Konten mit derselben `UID` vorhanden sein können, die aber voneinander unabhängig sind. Der erste Ansatz dazu war jeder der drei Domains eine eigene Datenbank (im Sinne von getrennten Dateien, die von einem LDAP-Server verwaltet werden) zu geben. Allerdings ließen sich in verschiedenen Versuchen die Datenbänke zwar anlegen, jedoch war ein Zugriff auf sie nicht möglich (getestet wurde dies mit entsprechenden `ldapsearch`-Aufrufen). Da sich u.a. wegen den eher unpraktischen Log-Leveln (siehe Erklärung der OpenLDAP Log-Level in der Kundendokumentation) von OpenLDAP das genaue Problem mit dieser Vorgehensweise nicht lokalisieren ließ, musste eine andere Struktur ersonnen werden.

Der Ansatz für die alternative Verzeichnisstruktur basierte u.a. darauf, wie LDAP mit Domainnamen umgeht: sie werden an den Trennzeichen (hier: Punkte) in einzelne Domain Components (LDAP-Bezeichnung `dc`) zerlegt. Da alle drei Domainnamen mit `.de` enden, konnte `dc=de` als Wurzel des Baumes der hierarchischen LDAP Verzeichnisstruktur verwendet werden. In der ersten Ebene unter der Wurzel verzweigt dieser Baum dann in die drei Domain Components `fg-networking.de`, `schabler.de` und `worden.de`. Da Objektnamen von ihrem vollen Kontext (quasi ihrem Pfad im Baum) abhängen, sind auch in diesem Modell drei unabhängige Namensräume gewährleistet. In den Domains `schabler.de` und `worden.de` sind nur relativ wenige Benutzerkonten hinterlegt (weniger als 10 Konten pro Domain) und beide Domains haben auch keinen eigenen Administrator (sie werden von fgn mit administriert). Daher gibt es auch keine Bedenken hinsichtlich Datenschutz und Performance wenn sich alle Domains in einer gemeinsamen Datenbank befindet. In der nächsten Ebene wurde dann jeweils eine Organizational Unit (`OU`) namens `people` angelegt in die dann die Benutzerkonten eingeordnet werden. Die `people-OU` wurde eingezogen um zukünftig auch andere Kontentypen wie z.B. Rechnerkonten in LDAP ablegen zu können, ohne dessen Verzeichnisstruktur grundlegend ändern zu müssen, um eine Unterscheidung der Konten zu erhalten.

Die oberste Ebene der Verzeichnisstruktur (die `de`-Wurzel) wurde mit Hilfe des Debian Konfigurationsskripts erstellt. Dabei wurden neben den vier Schema der Debian Standardkonfiguration (`core`, `cosine`, `nis` und `inetorgperson`) zusätzlich das `freeradius`-Schema aus dem `freeradius`-Paket und ein `postfix`-Schema (aus den Galileo Press Praxisbuch zu OpenLDAP 2.4) verwendet (Erläuterungen zu den Schema siehe Erläuterungen zu den verwendeten LDAP Schemas in der Kundendokumentation). Die erste Ebene wurde dann mit `slapadd` angelegt und die Grundstruktur darunter mit `ldapadd` erstellt (genaue Beschreibung der verwendeten LDAP Data Interchange Format (LDIF)-Dateien siehe Erstellung der LDAP-Verzeichnisstruktur in der Kundendokumentation).

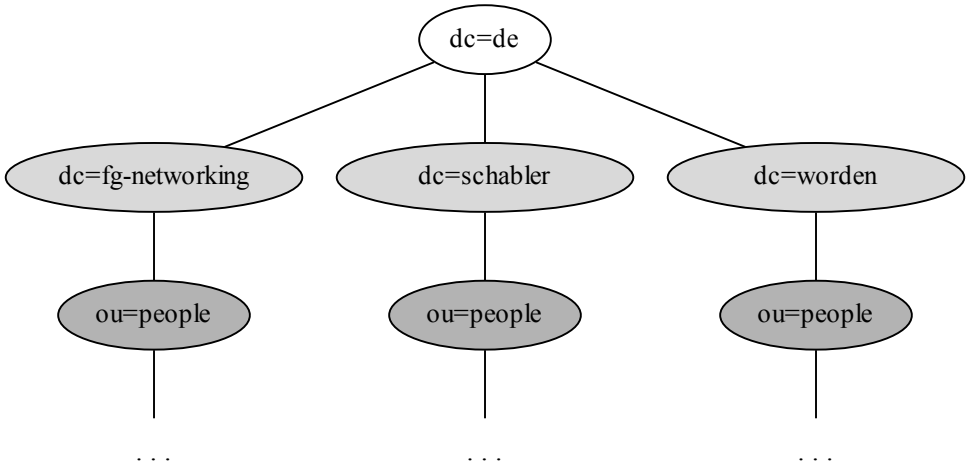

Abbildung 1: Der fertige LDAP-Verzeichnisbaum

4.2.3. Installation und Konfiguration des RADIUS-Servers

Auf dem Server wurden die Pakete `freeradius` und `freeradius-ldap` sowie – zu Testzwecken – das Paket `freeradius-utils` installiert. In den Konfigurationsdateien wurde dann LDAP als mögliche Quelle für Benutzerdaten eingetragen, die LDAP-Module aktiviert und der Zugriff durch die E-Mail-Server der TU Kaiserslautern erlaubt. Zusätzlich musste das zu dem TU E-Mail-Servern gehörende Shared Secret eingetragen werden, welches aus den Konfigurationsdateien von CommuniGate übernommen wurde, da es nicht in der firmeninternen Dokumentation festgehalten war. Näheres zur Konfiguration siehe Konfiguration des FreeRADIUS-Servers in der Kundendokumentation.

4.2.4. Absicherung des Rechners (Firewall etc.)

Wie in Planung des Sicherheitskonzepts erläutert, sind dem Netz, in dem sich der Server befindet, bereits zwei Firewalls vorgeschaltet. Die einzige Änderung, die an diesen vorgenommen werden musste, ist das Eintragen einer Ausnahmeregel mit der der Zugriff auf den RADIUS-Server aus dem Universitätsnetz erlaubt wird. Dafür wird die bereits bestehende Firewall-Regel für den in CommuniGate enthaltenen RADIUS auf die IP des neuen Servers angepasst.

Zusätzlich zu den Firewalls, die bereits das Firmennetz der fgn GmbH schützen, wurde die simpel zu bedienende Uncomplicated Firewall (`ufw`) verwendet, um lediglich die für OpenLDAP, FreeRADIUS und SSH notwendigen Ports zuzulassen, und Netzwerkverbindungen auf den restlichen Ports nicht zuzulassen. Näheres zur Firewall Konfiguration siehe Konfiguration der Firewall in der Kundendokumentation.

Der OpenLDAP-Server wurde so konfiguriert, dass er lediglich SSL verschlüsselte Verbindungen zulässt, somit ist ein Abhören der Kommunikation mit dem LDAP-Server stark erschwert. Modifikation der Daten im Verzeichnisdienst ist nur dem LDAP-

Administrator-Benutzer gestattet, der mit einem – den Passwortrichtlinien von fgn entsprechenden – Passwort gesichert ist. Die Firewall auf dem Server lässt außerdem nur Verbindungen aus dem Firmennetz und nur auf dem entsprechenden Port (636) zu. Als anonymer Benutzer ist lediglich der Zugriff auf Attribute, die nur anderweitig öffentlich verfügbare Informationen wie Name des Anwenders enthalten, und das Testen eines Passworts gegen den gespeicherten Passwort Hash. Letzteres wäre ein ernstzunehmender Angriffspunkt, wenn Verbindungen zum LDAP-Server von außerhalb des Firmennetzes erlaubt wären, was aber durch die Firewalls verhindert wird.

Zum FreeRADIUS-Server können sich generell nur Clients verbinden, die vorher in die Konfiguration eingetragen wurden, da beide Seiten das Shared Secret einstellen müssen. Verbindungen von komplett unbekannten Clients können somit schon rein prinzipbedingt nicht aufgebaut werden. Der einzige Angriffsvektor in dieser Richtung ist also ein Client, der das Shared Secret zwischen dem FreeRADIUS und den TU E-Mail-Servern kennt. Leider ist das Shared Secret die große Schwachstelle des RADIUS-Protokolls (was auch seit ungefähr 15 Jahren hinlänglich bekannt ist), somit ist das Einzige, das dagegen unternommen werden kann eine Verbindungsbeschränkung z.B. durch eine Firewall. Die einzige Möglichkeit eines unberechtigten Zugriffs wäre danach das Herausfinden des Shared Secrets und das Spoofing der IP eines TU Kaiserslautern E-Mailservers. Beides zusammen genommen ist recht unwahrscheinlich und wird noch dadurch erschwert, dass die TU selbst Maßnahmen gegen IP-Spoofing in dem von ihr verwalteten Netz (131.246.0.0/16) betreibt.

Der OpenSSH-Server, der für Fernzugriffe zusätzlich zur eigentliche Serverfunktion auf dem Rechner läuft, wird mit der Debian Standardkonfiguration betrieben, unter der Zugriff auf den root-Account nur mit einem eingetragenen SSH-Key möglich ist. Es existieren auch keine normalen Benutzerkonten auf dem Rechner, weswegen das Angriffsszenario vom Kapern eines Benutzeraccounts und dem darauffolgendem Erlangen von root-Rechten durch eine Schwachstelle (Priviledge Escalation) ausfällt. Wie bei sämtlichen fgn-Servern wurde der SSH-Zugang aus dem gesamten Internet erlaubt. Hier werden aber Brute-Force- Attacken durch die fgn-Firewall erschwert, da diese für SSH-Verbindungsversuche einen Rate Limiter eingestellt hat.

4.3. Abschließende Arbeiten

4.3.1. Umkonfiguration der Webservices

Da die umzustellenden Dienste (Webservices und OpenVPN) bereits den alten LDAP-Server verwenden, musste hier nicht viel eingerichtet werden. Die größte Änderung, die vorzunehmen war, ist daher das zusätzliche Eintragen des CA-Stammzertifikates in die Konfigurationsdatei `/etc/apache2/mods-available/ldap.conf` (bzw. bei OpenVPN in die entsprechende Konfigurationsdatei), da sonst keine LDAP- Verbindung über SSL aufgebaut werden kann. Ansonsten mussten nur noch in der Site-Konfiguration die URL des LDAP Servers und die BaseDN angepasst werden (OpenVPN ist analog anzupassen). Zu Details der anzupassenden Konfigurationen siehe die Abschnitte Änderungen an der Apache Konfiguration und Änderungen an der OpenVPN Konfiguration in der Kundendokumentation.

Wie in Dokumentation der Konfiguration des zu ersetzenden Servers geschildert, konnte Egroupware zur Bearbeitungszeit dieses Projektes noch nicht umgestellt werden, dies muss dann noch vom zuständigen Mitarbeiter vorgenommen werden.

4.3.2. Import/Anlegen der Anwenderkonten

Wie in „Prüfung von Möglichkeiten zum Importieren der bestehenden Anwenderkonten in die neue Lösung“ erwähnt, wurde entschieden, dass die praktikabelste Methode, um die Benutzerkonten im neuen Verzeichnisdienst zu erstellen, die Generierung einer von LDAP importierbaren Datei ist. Mit Hilfe der von Herrn Auerswald erstellten Skripte (Skripte siehe Skript zum Konvertieren der Anwenderkonten und Skript zum Hashen der Anwenderpasswörter im Anhang) wurde dann aus den Daten von CommuniGate eine LDIF-Datei erzeugt, die dann mit `ldapadd` importiert wurde.

Anmerkung: CommuniGate speichert Mailinglisten und Ähnliches ebenfalls in LDAP-Objekten, es wurden hier nur die Konten von echten Anwendern und zur Verwaltung der Webservices etc. nötige Konten importiert.

4.3.3. Funktions- und Sicherheitstests

Schon während der Arbeiten wurden immer wieder prüfbare Teilkomponenten getestet: Vor dem Erstellen der Verzeichnisstruktur wurde bereits eine Teststruktur erstellt, die lediglich die `fg-networking`-Domain und ein Testkonto enthielt. Dieses Testkonto wurde dann mit Hilfe von `ldapsearch` aus den LDAP-Utils abgefragt, noch bevor LDAPS eingerichtet war. Nach der Einrichtung von LDAPS wurde das Stammzertifikat in die Konfigurationsdatei `/etc/ldap/ldap.conf` eingetragen auf den Rechnern, auf denen mit den LDAP-Utils getestet wurde. Dies ist aber für den Normalbetrieb nicht notwendig, da dieser Eintrag nur von den LDAP-Utils ausgewertet wird. Apache und OpenVPN haben dazu eigene Einstellungen.

Die Webservices auf `nms` wurden dann kurzzeitig auf dieses LDAP umgestellt, um die generelle Funktion der Authentifizierung testen zu können. Der Rechner `nms` wurde gewählt, da die Webservices auf ihm wenig benutzt werden, und das auch nur von Mitarbeitern, die zur Bearbeitungszeit vor Ort waren und so einfach und schnell über die Tests informiert werden konnten. Hierbei fiel auf, dass es anfänglich noch einen Fehler in den SSL-Einstellungen gab. Dieser stellte sich aber nach kurzer Fehlersuche als ein einfacher Tippfehler in der Apache-Konfiguration heraus. Nach Korrektur dessen konnte man sich mit dem Testkonto erfolgreich an den Webservices anmelden.

Die Anbindung des FreeRADIUS-Servers an den OpenLDAP-Server wurde mit Hilfe des Programms `radtest` aus den FreeRADIUS-Utils getestet. Hier wurde – unter Verwendung des Shared Secrets – das oben erwähnte Testkonto abgefragt. Mit demselben Befehl, aber einem echten Anwenderkonto, wurde auch der CommuniGate-Server getestet um einen Vergleichswert zu haben, da ein echter Praxistest erst bei Fertigstellung des neuen E-Mail-Servers durchgeführt werden kann.

Abschließend wurde noch versucht, einen Managed Switch an den RADIUS-Server anzubinden, damit darüber Benutzerkonten aus dem LDAP-Verzeichnisdienst zum Anmelden verwendet werden können. Nach Informationen aus den LDAP-Logs funktionierte das Authentifizieren am Server auch, allerdings konnte man sich trotzdem nicht erfolgreich am Switch anmelden. Dafür hätte man zusätzliche Berechtigungen im LDAP hinterlegen müssen. Da nicht sofort ersichtlich wurde, was genau dafür zu konfigurieren wäre, und die Anbindung von Switches erst irgendwann in Zukunft geschehen soll, wurde das Ganze dann nicht weiter verfolgt.

Zum Testen der Sicherungsmaßnahmen wurde nach der Umstellung der Webservices erfolglos versucht, sich an diesen mit falschen Anmeldeinformationen (falscher Be-

nutzername, richtiger Benutzername mit falschem Passwort) anzumelden. Dasselbe wurde mit `radtest` am RADIUS-Server getestet. Abschließend wurde noch per `nmap` von innerhalb der Firmennetze und von einem externen Rechner aus geprüft, ob ausschließlich die richtigen Ports geöffnet sind (näheres dazu in Ergebnis eines fgn internen NMAP Tests und Ergebnis eines externen NMAP Tests im Anhang).

5. Projektkosten

Kosten für die Einrichtung			
Kosten-Kategorie	Projekt	CommuniGate-Upgrade	keine Änderung
Hardware	0,00€	0,00€	0,00€
Softwarelizenzen	0,00€	1.849,00€	0,00€
Arbeitsaufwand	2.485,00€	2.485,00€	0,00€
Gesamt	2.485,00€	4.334,00€	0,00€

Anmerkungen: Es wurde ein Stundenlohn von 71€ angenommen. Hardwarekosten entstehen keine da alles auf Virtual Machines läuft und die Anschaffungskosten für die ESXi-Server nur schwierig auf die VMs aufzuteilen ist.

Jährliche Kosten			
Kategorie	Projekt	CommuniGate-Upgrade	keine Änderung
Hardware	0,00€	0,00€	0,00€
Softwarelizenzen	0,00€	332,82€	0,00€
Arbeitsaufwand	355,00€	213,00€	2.350,00€
Gesamt	355,00€	545,82€	2.350,00€

Anmerkungen: Der Wartungsaufwand für das Projektsystem wurde auf fünf Stunden pro Jahr geschätzt, der für einen neuen CommuniGate Server nur auf drei Stunden, da Unterstützung durch den professionellen Support von CommuniGate in den Lizenzkosten enthalten ist. Die Zusammensetzung der beiden Vergleichskostensätze findet sich in der Wirtschaftlichkeits-Analyse.

6. Projektabschluss

6.1. Fazit

Bis auf das Egroupware und der E-Mail-Server, wurden alle Systeme von fgn, die vorher den LDAP-Server von CommuniGate benutzten, erfolgreich auf den neuen OpenLDAP Server umgestellt. Da der alte E-Mail-Server weiterhin in Betrieb bleibt, bis er vom neuen Server abgelöst wird, findet bis dahin ein Parallelbetrieb der LDAP Server statt. Deswegen werden die Benutzerpasswörter bei Fertigstellung des neuen E-Mail-Servers noch einmal zur Sicherheit synchronisiert werden müssen, dies wird jedoch über die Skripte wieder einfach zu bewerkstelligen sein. Die im Rahmen dieses Projekts erstellten Skripte werden dazu allerdings leicht modifiziert werden müssen da diesmal LDAP Daten verändert werden sollen statt neu hinzugefügt, und die LDIF-Syntax dafür leicht anders ist.

Der FreeRADIUS-Server wurde ebenso erfolgreich eingerichtet und einfacher als erwartet an den OpenLDAP-Server angebunden. Allerdings verrichtet er bisher noch keinen sinnvollen Dienst, da bei fgn RADIUS momentan nur über den E-Mail-Server benutzt wird und dieser weiterhin selbst einen RADIUS-Server betreibt. Dies wird sich voraussichtlich erst mit der Fertigstellung des neuen E-Mail-Servers ändern.

Bei der Zeitplanung des Projektes wäre im Nachhinein Folgendes zu verbessern gewesen: Für den Entwurf und die Implementierung der Verzeichnisstruktur hätte mehr Zeit eingeplant werden müssen. Als der Zeitplan für den Projektantrag ausgearbeitet wurde, waren die Vorrecherchen zu LDAP und vor Allem zur bestehenden Konfiguration noch nicht weit genug fortgeschritten, dass Probleme aus dieser Richtung vorhersehbar gewesen wären. Insgesamt wäre der Entwurf der LDAP-Verzeichnisstruktur am besten als zusätzlicher Punkt zur Planung hinzugefügt worden. In der Umsetzungsphase hätte man dagegen weniger Zeit für die Vorbereitung veranschlagen können, da nur eine übersichtlich kleine Anzahl an Diensten den LDAP-Server verwendet und bei diesen nicht viel an der Konfiguration zu ändern war.

6.2. Ausblick

Die voraussichtliche erste Änderung – nach der Anbindung von Egroupware – für die im Rahmen dieses Projektes erstellten Serverdienste wird nach aktueller Planung die Anbindung des neuen E-Mail-Servers sein. Dafür werden den in OpenLDAP bestehenden Benutzerkonten die Attribute, die der E-Mail-Server benötigt (wie z.B. die E-Mailadresse), mit den korrekten Werten gefüllt werden müssen. Dies wird voraussichtlich wieder über durch Skripte erstellte LDIF-Dateien geschehen.

Ebenso bietet sich für eine Erweiterung des Projektsystems die Einbindung der anderen Linux-Rechner in der Firma an. Dort könnte man dadurch die bisherigen lokalen Benutzerkonten durch zentral in LDAP abgelegte und verwaltete Konten ersetzen. Dazu müsste man auf den Linux-Rechnern LDAP an das PAM-System anbinden (dazu müsste dort vermutlich noch ein passendes PAM-LDAP Modul installiert werden und eventuell auch das LDAP Modul für den Name Switch Service (`NSS`)) und im LDAP-Server die Benutzer um die passenden Attribute (wie z.B. Home-Verzeichnis, UID, Gruppen) erweitern. Letzteres kann wieder geskriptet werden. Als Anwendersystem wird im Moment allerdings nur ein Rechner verwendet, und zwar `fgnfs`, für den der Aufwand im Vergleich zum zu erwartenden Nutzen im Rahmen des Projektes zu groß erschien.

Eine weitere für fgn attraktive Erweiterungsmöglichkeit ist das Anbinden der Managed Switches der Schulungslabore an den FreeRADIUS-Server (und somit an LDAP). Dies würde Problemen, die ab und zu durch Änderungen der Anmeldeinformationen der Switches durch Schulungsteilnehmer auftreten, vorbeugen. Da die Schulungslabore in einem eigenen VPN angebunden sind, müsste RADIUS dazu ebenfalls in dieses VPN eingehängt werden. Des Weiteren müssten Konten für die Switches erstellt werden, die die Attributen enthalten, die zu Autorisierung benötigt werden. In die Switches müsste außerdem der RADIUS-Server eingetragen und im RADIUS-Server die Clients eingetragen werden (jeweils dann mit passenden Shared Secret "Paaren").

fgn hat neben den diversen Linux-Rechnern auch noch 2 Windows-PCs in der Verwaltung, sowie einige an den Schulungslaboren angeschlossene virtuelle Windows-Rechner. Für diese könnte man mit Samba 4 eine kleine Active Directory-Domäne aufbauen, die an den OpenLDAP Server angebunden wird. Allerdings benötigt Samba 4 inzwischen ein eigenes LDAP (dies wird für Replikationsfunktionen benötigt) und

lässt sich somit nur umständlich an das nun bestehende LDAP anbinden. Dieser Erweiterungsmöglichkeit stellt – von den bisher genannten – für fgn die unattraktivste dar, da der Aufwand recht hoch wäre und es nur wenige Windowsrechner gibt die davon tatsächlich profitieren würden.

Quellen

- Deckblattvorlage von http://f.macke.it/LaTeXVorlageFIAE unter Creative Commons
- Informationen zur Entwicklung von LDAP aus http://de.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol#Geschichte
- Homepage des OpenLDAP-Projekts: http://www.openldap.org
- Homepage des FreeRADIUS-Projekts: http://freeradius.org
- Oliver Liebel, John Martin Ungar - OpenLDAP 2.4: das Praxisbuch (2009, Galileo Computing)
- Jonathan Hassel - RADIUS (2003, O'Reilly)
- Bei der Installation von OpenLDAP wurde die folgende Anleitung aus dem Debian Wiki konsultiert: https://wiki.debian.org/LDAP/OpenLDAPSetup
- Zur Anbindung von FreeRADIUS an OpenLDAP wurde folgende Anleitung im Debian Wiki konsultiert (und für stellenweise veraltet befunden) https://wiki.debian.org/FreeRadiusToLdap
- OpenLDAP Log-Level: http://www.openldap.org/doc/admin24/runningslapd.html
- Grafik des LDAP-Verzeichnisbaums erstellt mit Graphviz: http://www.graphviz.org
- Diese Dokumentation wurde erstellt mit LaTeX (http://www.latex-project.org) und verwaltet in Git (http://git-scm.com)

Eidesstattliche Erklärung

Ich, Sebastian Deußer, versichere hiermit, dass ich meine **Dokumentation zur betrieblichen Projektarbeit** mit dem Thema

> *OpenLDAP- und FreeRADIUS-Server – Aufsetzen eines Identity Management-Servers als Ersatz eines veralteten CommuniGate Servers*

selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, wobei ich alle wörtlichen und sinngemäßen Zitate als solche gekennzeichnet habe. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

Kaiserslautern, den 18. Mai 2015

_____

Sebastian Deußer

A. Anhänge

A.1. Übernommene LDAP Attribute

- `uid`: User ID, Name des Anwenderkontos
- `sn`: SurName, Nachname des Anwenders
- `givenName`: Vorname des Anwenders
- `cn`: CommonName, voller Name des Anwenders
- `displayName`: anzuzeigender Name des Anwenders
- `userPassword`: Passwort des Anwenders (wurde mit `slappasswd` gehashed)

A.2. Skript zum Konvertieren der Anwenderkonten

```
#! /bin/bash

# Extract account information from CommuniGate files and
    convert to LDIF
# format useful for importing into OpenLDAP.

set -u
set -e

# Default CommuniGate Domain

DEF_DOMAIN='fg-networking.de'
DEF_ACCOUNT_DIR='/srv/mail/communigate/Accounts'
ACCOUNT_DIRS=$(/bin/ls -1d "${DEF_ACCOUNT_DIR}"/*.macnt)

# Additional Domains

DOMAIN_ACCOUNT_DIRS='/srv/mail/communigate/Domains/schabler.de
    /srv/mail/communigate/Domains/worden.de'
for D in ${DOMAIN_ACCOUNT_DIRS}; do
  ACCOUNT_DIRS="${ACCOUNT_DIRS} $(/bin/ls -1d "${D}"/*.macnt)"
done

for A in ${ACCOUNT_DIRS}; do
  DOMAIN=${DEF_DOMAIN}
  echo "${A}" | /bin/fgrep -q /Domains/ &&
    DOMAIN=$(echo "${A}" | /bin/sed 's|^.*Domains/\([^/]*\)/.*$
    |\1|')
  DC_STRING=$(echo "${DOMAIN}" | /bin/sed 's/^/dc=/;s/\./,dc=/g
    ')
  ACCOUNT_NAME=$(/usr/bin/basename "${A}" .macnt)
  SETTINGS=${A}/account.settings
  REALNAME=$(/bin/sed -n '/RealName/s/^[^"]*"\([^"]*\)".*$/\1/p
    ' "${SETTINGS}")
  test -z "${REALNAME}" && REALNAME="Unknown Name"
  PRENAME=$(echo "${REALNAME}" | /usr/bin/awk '/./{NF--;print
    }')
  SURNAME=$(echo "${REALNAME}" | /usr/bin/awk '/./{print $NF}')
  QUOTED_PW=$(/bin/sed -n 's/^ Password = \(.*\);$/\1/p' "${
    SETTINGS}")
  PASSWORD=$(echo "${QUOTED_PW}" | /bin/sed 's/^"//;s/"$//' | /
    bin/sed 's/\\"/"/g')
  cat <<EOE
dn: uid=${ACCOUNT_NAME},ou=people,${DC_STRING}
objectClass: inetOrgPerson
```

```
objectClass: person
uid: ${ACCOUNT_NAME}
sn: ${SURNAME}
givenName: ${PRENAME}
cn: ${REALNAME}
displayName: ${REALNAME}
userPassword: ${PASSWORD}

EOE
done
```

Dieses Skript liest die Klartext-Dateien von CommuniGate aus und wandelt diese in das passende Format für `ldapmodify` um. Dazu werden die entsprechende Daten in das am Ende der Erstellung der LDAP-Verzeichnisstruktur (Kundendokumentation) Template eingetragen. Das Ganze wird in eine Datei geschrieben, jeder Datensatz getrennt durch eine Leerzeile.

Abdruck des Skript mit freundlicher Genehmigung von fgn und dem Autor Erik Auerswald.

A.3. Skript zum Hashen der Anwenderpasswörter

```
#! /bin/bash

# Replace clear text passwords with slappasswd generated salted
    hashes
# Use as filter.

awk \
'/userPassword/ {
  "slappasswd -s" "\"" $2 "\"" | getline pwhash
  print $1 " " pwhash
}
!/userPassword/
'
```

Dieses Skript wandelt die Klartext-Passwörter in der mit dem vorigen Skript erstellten Datei mit Hilfe von `slappasswd` in von OpenLDAP importierbare Passwort-Hashes um.

Abdruck des Skript mit freundlicher Genehmigung von fgn und dem Autor Erik Auerswald.

A.4. Ergebnis eines fgn internen NMAP Tests

```
# nmap -Pn -sS -sU -p1-65535 -v id.fg-networking.de

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-11 11:09 CEST
Initiating Parallel DNS resolution of 1 host. at 11:09
Completed Parallel DNS resolution of 1 host. at 11:09, 0.00s
   elapsed
Initiating SYN Stealth Scan at 11:09
Scanning gaf-nat-core1.fg-networking.de (131.246.197.6) [65535
   ports]
Completed SYN Stealth Scan at 11:09, 10.40s elapsed (65535
   total ports)
Initiating UDP Scan at 11:09
Scanning gaf-nat-core1.fg-networking.de (131.246.197.6) [65535
   ports]
Completed UDP Scan at 12:46, 5854.26s elapsed (65535 total
   ports)
Nmap scan report for gaf-nat-core1.fg-networking.de
   (131.246.197.6)
Host is up (0.00010s latency).
Not shown: 1310626 closed ports
PORT       STATE          SERVICE
22/tcp     open           ssh
636/tcp    open           ldapssl
1812/udp   open|filtered  radius
1813/udp   open|filtered  radacct

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5865.05 seconds
           Raw packets sent: 149026 (5.224MB) | Rcvd: 298030
   (12.521MB)
```

Wie man sieht sind für das fgn-Netz nur die Ports für SSH (22), LDAPS (636), und RADIUS (1812 und 1813) geöffnet.
`gaf-nat-core1.fg-networking.de` ist der Hostname des ESXi-Servers auf dem die VM läuft.

A.5. Ergebnis eines externen NMAP Tests

```
# nmap -Pn -sS -sU -p1-65535 id.fg-networking.de

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-11 14:09 CEST
Initiating Parallel DNS resolution of 1 host. at 14:09
Completed Parallel DNS resolution of 1 host. at 14:09, 0.00s
   elapsed
Initiating SYN Stealth Scan at 14:09
Scanning gaf-nat-core1.fg-networking.de (131.246.197.6) [65535
   ports]
Completed SYN Stealth Scan at 14:09, 10.40s elapsed (65535
   total ports)
Initiating UDP Scan at 14:09
Scanning gaf-nat-core1.fg-networking.de (131.246.197.6) [65535
   ports]
Completed UDP Scan at 15:46, 5854.26s elapsed (65535 total
   ports)
Nmap scan report for id.fg-networking.de (131.246.197.6)
Host is up (0.00010s latency).
Not shown: 1310629 closed ports
PORT      STATE         SERVICE
22/tcp    open          ssh

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5865.05 seconds
           Raw packets sent: 149026 (5.224MB) | Rcvd: 298030
   (12.521MB)
```

Wie man sieht sind für das restliche Internet nur der Port für SSH (22) geöffnet. `gaf-nat-core1.fg-networking.de` ist der Hostname des ESXi-Servers auf dem die VM läuft.

IHK Pfalz

Sommerprüfung 2015

Ausbildungsberuf
Fachinformatiker/-in Systemintegration

Prüfungsbezirk
Pfalz IT (T2, V1)

Herr Sebastian Deußer
Identnummer: 630307
E-Mail: sebastian.deusser@gmx.de, Telefon: 0631-34288973

Ausbildungsbetrieb: taylorix institut Kaiserslautern
Projektbetreuer: Herr Ramie Al-Masri
E-Mail: r.al-masri@taylorix-institut.com, Telefon: 0631-34288979

Thema der Projektarbeit
Aufsetzen eines Authentifizierungsservers als Ersatz eines veralteten proprietären CommuniGate Servers

1 Thema der Projektarbeit

Aufsetzen eines Authentifizierungsservers als Ersatz eines veralteten proprietären CommuniGate Servers

2 Geplanter Bearbeitungszeitraum

Beginn: 20.04.2015
Ende: 24.04.2015

3 Projektbeschreibung

IST-Zustand:
Im Praktikumsbetrieb fgn GmbH läuft sämtlicher Mailverkehr und Authentifizierung an den internen Webservices u.ä. über einen CommuniGate Server. Ursprünglich wurde der CommuniGate Server auf einem eigenen Rechner aufgesetzt, inzwischen aber wie viele andere Rechner der Firma virtualisiert. Die Webservices, die ihn zur Anwender-Authentifizierung verwenden, laufen auf drei anderen VMs. Lediglich die Anwenderkonten auf den Betriebssystemen der diversen Anwender-PCs sind nicht von CommuniGate abhängig.

SOLL-Zustand:
Da dieser Server veraltet ist, und ein Upgrade mit ähnlichem Aufwand verbunden wäre wie die Migration auf einen neuen Server, soll ein komplett neuer Server aufgesetzt werden. Dabei soll möglichst auf Software mit proprietären Datenstrukturen verzichtet werden, um in Zukunft den Server leichter austauschen zu können. Eine Open Source Software Lösung wird bevorzugt, da in der Firma zur Zeit viel OSS eingesetzt wird.

Lösungsansatz:
Bei einem Austausch müssen die firmeninternen Web- und Netzwerkservices auf den neuen Authentifizierungsserver umkonfiguriert und ggf. angepasst werden. Zu diesen zählen eGroupware und diverse andere Webtools, browserbasierte Frontends der Tools des Network Management Servers, der OpenVPN Server und der neue Mailserver. Des Weiteren werden externe Dienste (z.B. der Mailserver der TU Kaiserslautern) verwendet für die ein RADIUS Server zur Verfügung gestellt werden muss. Es wurde bereits von einem Mitarbeiter damit begonnen einen Ersatz für den Mailserver aufzusetzten, der Ersatz für diesen Teil von CommuniGate ist also nicht Teil dieses Projektes.

Im Rahmen des Projekts muss Folgendes durchgeführt werden:
- Installation und Konfiguration eines LDAP Servers (inklusive Auswahl des LDAP-Schemas etc)
- Installation und Konfiguration eines RADIUS Servers
- Importieren oder Erstellen der Anwender-Konten
- Anpassen der Services auf den neuen Authentifizierungsserver

4 Projektumfeld

Die fgn GmbH wurde im August 2000 als SpinOff der Technische Universität (TU) Kaiserslautern gegründet. Die Gründer waren zuvor mehrere Jahre (seit 1996 bzw. 1989) als freischaffende Consultants und Trainer tätig. Die Firma pflegt enge Kontakte zum Regionalen Hochschulrechenzentrum Kaiserslautern (RHRK), da die meisten Mitarbeiter das Netz der TU Kaiserslautern mit ca. 10.000 Ports, Diensten wie Mail, DNS und DHCP in der Vergangenheit betreut haben oder es heute noch betreuen.

Die Kernkompetenz der fgn GmbH ist anspruchsvolles Netzwerk-Knowhow, welches als Dienstleistung in drei eng verknüpften Tätigkeitsfeldern angeboten wird: Schulungen, Workshops und Netzwerk-Consulting (Beratung und vor Ort Support von Firmen bei Problemen, Umstrukturierungen, Erweiterungen und Neuaufbau von Produktivnetzwerken).

5 Projektphasen mit Zeitplanung

Analyse und Planung (insgesamt 6 h)
Ist-Analyse (4 h)
- Analyse des bestehenden CommuniGate Servers und der damit verbundenen Webservices (3 h)
- Aufnahme der Anforderungen an einen Ersatzserver (1 h)

Planung (2 h)
- Ausarbeitung eines Konzepts für den Ersatzserver (2 h)

Umsetzung (insgesamt 20 h)
Vorbereitungen (7 h)
- Dokumentation der Konfiguration des zu ersetzenden Servers (2 h)
- Erstellen einer Liste aller Dienste, die das bestehende Identity Management nutzen (2 h)
- Prüfung von Möglichkeiten zum Importieren der bestehenden Anwender-Konten in die neue Lösung (3 h)

Installation und Einrichtung des neuen Servers (8 h)
- Grundinstallation des Linux Systems des neuen Servers (2 h)
- Installation und Konfiguration des LDAP Servers (3 h)
- Installation und Konfiguration des RADIUS Servers (3 h)

Abschließende Arbeiten (5 h)
- Umkonfiguration der Webservices (3 h)
- Import/Anlegen der Anwender Konten (2 h)

Dokumentation (insgesamt 9 h)
- Erstellen der Projektdokumentation (7 h)
- Erstellen der Dokumentation für das firmeninterne Wiki (2 h)

6 Dokumentation zur Projektarbeit

Projektdokumentation
Dokumentation Konfiguration und Serversystem für firmeninternes Wiki

7 Anlagen

keine

8 Präsentationsmittel

mit einem Präsentationsprogramm erstellte Vortragsfolien, Laptop, Beamer

9 Hinweis!

Ich bestätige, dass der Projektantrag dem Ausbildungsbetrieb vorgelegt und vom Ausbildenden genehmigt wurde. Der Projektantrag enthält keine Betriebsgeheimnisse. Soweit diese für die Antragstellung notwendig sind, wurden nach Rücksprache mit dem Ausbildenden die entsprechenden Stellen unkenntlich gemacht.

Mit dem Absenden des Projektantrages bestätige ich weiterhin, dass der Antrag eigenständig von mir angefertigt wurde. Ferner sichere ich zu, dass im Projektantrag personenbezogene Daten (d. h. Daten über die eine Person identifizierbar oder bestimmbar ist) nur verwendet werden, wenn die betroffene Person hierin eingewilligt hat.

Bei meiner ersten Anmeldung im Online-Portal wurde ich darauf hingewiesen, dass meine Arbeit bei Täuschungshandlungen bzw. Ordnungsverstößen mit „null“ Punkten bewertet werden kann. Ich bin weiter darüber aufgeklärt worden, dass dies auch dann gilt, wenn festgestellt wird, dass meine Arbeit im Ganzen oder zu Teilen mit der eines anderen Prüfungsteilnehmers übereinstimmt. Es ist mir bewusst, dass Kontrollen durchgeführt werden.

IHK Pfalz

Sommerprüfung 2015

Ausbildungsberuf
Fachinformatiker/-in Systemintegration

Prüfungsbezirk
Pfalz IT (T2, V1)

Herr Sebastian Deußer
Identnummer: 630307
E-Mail: sebastian.deusser@gmx.de, Telefon: 0631-34288973

Ausbildungsbetrieb: taylorix institut Kaiserslautern
Projektbetreuer: Herr Ramie Al-Masri
E-Mail: r.al-masri@taylorix-institut.com, Telefon: 0631-34288979

Thema der Projektarbeit
Aufsetzen eines Authentifizierungsservers als Ersatz eines veralteten proprietären CommuniGate Servers

1 Thema der Projektarbeit

Aufsetzen eines Authentifizierungsservers als Ersatz eines veralteten proprietären CommuniGate Servers

2 Geplanter Bearbeitungszeitraum

Beginn: 04.05.2015
Ende: 18.05.2015

3 Projektbeschreibung

IST-Zustand:
Im Praktikumsbetrieb fgn GmbH läuft sämtlicher Mailverkehr und Authentifizierung an den internen Webservices u.ä. über einen CommuniGate Server. Ursprünglich wurde der CommuniGate Server auf einem eigenen Rechner aufgesetzt, inzwischen aber wie viele andere Rechner der Firma virtualisiert. Die Webservices, die ihn zur Anwender-Authentifizierung verwenden, laufen auf drei anderen VMs. Lediglich die Anwenderkonten auf den Betriebssystemen der diversen Anwender-PCs sind nicht von CommuniGate abhängig.

SOLL-Zustand:
Da dieser Server veraltet ist, und ein Upgrade mit ähnlichem Aufwand verbunden wäre wie die Migration auf einen neuen Server, soll ein komplett neuer Server aufgesetzt werden. Dabei soll möglichst auf Software mit proprietären Datenstrukturen verzichtet werden, um in Zukunft den Server leichter austauschen zu können. Eine Open Source Software Lösung wird bevorzugt, da in der Firma zur Zeit viel OSS eingesetzt wird.

Lösungsansatz:
Bei einem Austausch müssen die firmeninternen Web- und Netzwerkservices auf den neuen Authentifizierungsserver umkonfiguriert und ggf. angepasst werden. Zu diesen zählen eGroupware und diverse andere Webtools, browserbasierte Frontends der Tools des Network Management Servers, der OpenVPN Server und der neue Mailserver. Des Weiteren werden externe Dienste (z.B. der Mailserver der TU Kaiserslautern) verwendet für die ein RADIUS Server zur Verfügung gestellt werden muss. Es wurde bereits von einem Mitarbeiter damit begonnen einen Ersatz für den Mailserver aufzusetzten, der Ersatz für diesen Teil von CommuniGate ist also nicht Teil dieses Projektes.

Im Rahmen des Projekts muss Folgendes durchgeführt werden:
- Installation und Konfiguration eines LDAP Servers (inklusive Auswahl des LDAP-Schemas etc)
- Installation und Konfiguration eines RADIUS Servers
- Importieren oder Erstellen der Anwender-Konten
- Anpassen der Services auf den neuen Authentifizierungsserver

4 Projektumfeld

Die fgn GmbH wurde im August 2000 als SpinOff der Technische Universität (TU) Kaiserslautern gegründet. Die Gründer waren zuvor mehrere Jahre (seit 1996 bzw. 1989) als freischaffende Consultants und Trainer tätig. Die Firma pflegt enge Kontakte zum Regionalen Hochschulrechenzentrum Kaiserslautern (RHRK), da die meisten Mitarbeiter das Netz der TU Kaiserslautern mit ca. 10.000 Ports, Diensten wie Mail, DNS und DHCP in der Vergangenheit betreut haben oder es heute noch betreuen.

Die Kernkompetenz der fgn GmbH ist anspruchsvolles Netzwerk-Knowhow, welches als Dienstleistung in drei eng verknüpften Tätigkeitsfeldern angeboten wird: Schulungen, Workshops und Netzwerk-Consulting (Beratung und vor Ort Support von Firmen bei Problemen, Umstrukturierungen, Erweiterungen und Neuaufbau von Produktivnetzwerken).

5 Projektphasen mit Zeitplanung

Analyse und Planung (insgesamt 6 h)
Ist-Analyse (3 h)
- Analyse des bestehenden CommuniGate Servers und der damit verbundenen Webservices (2 h)
- Aufnahme der Anforderungen an einen Ersatzserver (1 h)

Planung (3 h)
- Ausarbeitung eines Konzepts für den Ersatzserver (1 h)
- Ausarbeitung des Sicherheitskonzepts (unter Berücksichtigung des Firmenkonzepts) (1 h)
- Ausarbeitung des Kommunikationskonzepts (Serverdienste untereinander und extern) (1 h)

Umsetzung (insgesamt 20 h)
Vorbereitungen (6 h)
- Dokumentation der Konfiguration des zu ersetzenden Servers (2 h)
- Erstellen einer Liste aller Dienste, die das bestehende Identity Management nutzen (2 h)
- Prüfung von Möglichkeiten zum Importieren der bestehenden Anwender-Konten in die neue Lösung (2 h)

Installation und Einrichtung des neuen Servers (8 h)
- Grundinstallation des Linux Systems des neuen Servers (1 h)
- Installation und Konfiguration des LDAP Servers (3 h)
- Installation und Konfiguration des RADIUS Servers (2 h)
- Absicherung des Rechners (Firewall etc) (2 h)

Abschließende Arbeiten (6 h)
- Umkonfiguration der Webservices (2 h)
- Import/Anlegen der Anwender Konten (2 h)
- Funkions- und Sicherheitstests (2 h)

Dokumentation (insgesamt 9 h)
- Erstellen der Projektdokumentation (8 h)
- Erstellen der Dokumentation für das firmeninterne Wiki (1 h)

6 Dokumentation zur Projektarbeit

Projektdokumentation
Dokumentation Konfiguration und Serversystem für firmeninternes Wiki

7 Anlagen

keine

8 Präsentationsmittel

mit einem Präsentationsprogramm erstellte Vortragsfolien, Laptop, Beamer

9 Hinweis!

Ich bestätige, dass der Projektantrag dem Ausbildungsbetrieb vorgelegt und vom Ausbildenden genehmigt wurde. Der Projektantrag enthält keine Betriebsgeheimnisse. Soweit diese für die Antragstellung notwendig sind, wurden nach Rücksprache mit dem Ausbildenden die entsprechenden Stellen unkenntlich gemacht.

Mit dem Absenden des Projektantrages bestätige ich weiterhin, dass der Antrag eigenständig von mir angefertigt wurde. Ferner sichere ich zu, dass im Projektantrag personenbezogene Daten (d. h. Daten über die eine Person identifizierbar oder bestimmbar ist) nur verwendet werden, wenn die betroffene Person hierin eingewilligt hat.

Bei meiner ersten Anmeldung im Online-Portal wurde ich darauf hingewiesen, dass meine Arbeit bei Täuschungshandlungen bzw. Ordnungsverstößen mit „null“ Punkten bewertet werden kann. Ich bin weiter darüber aufgeklärt worden, dass dies auch dann gilt, wenn festgestellt wird, dass meine Arbeit im Ganzen oder zu Teilen mit der eines anderen Prüfungsteilnehmers übereinstimmt. Es ist mir bewusst, dass Kontrollen durchgeführt werden.

Abschlussprüfung Sommer 2015

Fachinformatiker – Systemintegration

Dokumentation zur betrieblichen Projektarbeit

OpenLDAP- und FreeRADIUS-Server

Kundendokumentation für Administratoren

Abgabetermin: Kaiserslautern, den 18. Mai 2015

Prüfungsbewerber:
Sebastian Deußer
Feuerbachstraße 15
67659 Kaiserslautern

Ausbildungsbetrieb:
taylorix institut für berufliche Bildung e.V.
Lutrinastraße 4
67655 Kaiserslautern

Praktikumsbetrieb:
fgn GmbH
Trippstadter Straße 122
67663 Kaiserslautern

Kundendokumentation für Administratoren

Wichtige Details

- Server `id.fg-networking.de`
- verwendet LDAP-over-SSL (Port 636), LDAP Standardport nur für Loopback aktiviert (zu ändern in /etc/default/slapd)
- Purge des slapd Pakets löscht nicht die LDAP Datenbank (Konfiguration dieses Verhaltens über das Debian Paketkonfigurationsskript)

Nützliche Links

- https://wiki.debian.org/LDAP/OpenLDAPSetup
- https://wiki.debian.org/FreeRadiusToLdap (zu RADIUS+LDAP, etwas angestaubt sogar für Debian Verhältnisse)
- http://www.postfix.org/LDAP_README.html (Postfix+LDAP Doku)
- http://www.zytrax.com/books/ldap/ch11/multi-dit.html (Beispiel für mehrere Domains in einem LDAP)
- http://httpd.apache.org/docs/2.4/mod/mod_authnz_ldap.html (Apache Doku zum LDAP Auth Modul)

Ändern des Passworts eines LDAP-Users

Um das Passwort eine Users im LDAP Verzeichnis zu ändern bietet sich für die Kommandozeile `ldappasswd` an. Dazu sollten die LDAP-Utils auf dem jeweiligen Rechner richtig konfiguriert sein (siehe in Einrichten von LDAPS (LDAP-over-SSL) den unteren Teil zur `/etc/ldap/ldap.conf`).

```
ldappasswd -S -W -D "cn=admin,dc=de" -x "uid=username,ou=people
    ,dc=fg-networking,dc=de"
```

Dieser Befehl fragt auf der Kommandozeile das neue Passwort für den Account `username` ab (mit Wiederholung) und fragt wenn beide Passwörte übereinstimmen nach dem Passwort des LDAP-Administrators. Mit den Daten meldet es sich dann am LDAP-Server an und speichert das Passwort dann gehashed in der LDAP Datenbank. Username muss natürlich durch den richtigen Namen ersetzt werden und eventuell die erste dc angepasst werden.

Erklärung der OpenLDAP Log-Level

Level	Keyword	Description
-1	any	enable all debugging
0		no debugging
1	(0x1 trace)	trace function calls
2	(0x2 packets)	debug packet handling
4	(0x4 args)	heavy trace debugging
8	(0x8 conns)	connection management
16	(0x10 BER)	print out packets sent and received
32	(0x20 filter)	search filter processing
64	(0x40 config)	configuration processing
128	(0x80 ACL)	access control list processing
256	(0x100 stats)	stats log connections/operations/results
512	(0x200 stats2)	stats log entries sent
1024	(0x400 shell)	print communication with shell backends
2048	(0x800 parse)	print entry parsing debugging
16384	(0x4000 sync)	syncrepl consumer processing
32768	(0x8000 none)	only messages that get logged whatever log level is set

Um Log-Level einzustellen kann man entweder die entsprechende Zahl aus der ersten Spalte, den Hex-Wert oder das Schlüsselwort aus Spalte 2 verwenden. Werden die Zahlen aus Spalte 1 verwendet kann man mehrere Log-Level gleichzeitig auswählen indem man ihre Wert miteinander addiert.

Zum debuggen der Probleme die bei der Durchführung des Projekts auftraten erwiesen sich die meisten der Zusatzausgaben als ungeeignet, lediglich die Traces der Level 1 (0x1 trace) und 4 (0x4 args) konnten weiterhelfen, enthielten aber auch keine weiterführenden Informationen bei Problemen mit dem Zugriff auf die Verzeichnis-Datenbank.

Wenn wie in diesem Projekt ein OpenLDAP-Server mit einem `slapd.d`-Konfigurationsordner statt einer `slapd.conf`-Konfigurationsdatei verwendet wird, muss man, wie sämtliche anderen Einstellungen auch, den Log-Level über eine vorbereitete Datei und `ldapmodify` verändern. Eine entsprechende Datei sieht wie folgt aus:

```
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: 5
```

Diese Datei würde den Log-Level auf 5 setzen. Der entsprechende `ldapmodify`-Aufruf ist dann:

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f olcLogLevel.ldif
```

Ausgeben des Inhalts der LDAP-Datenbank

Mit dem Kommandozeilenprogramm `ldapsearch` kann man nach Einträgen in der LDAP Datenbank suchen. Man kann sich damit auch den gesamten Inhalt der Datenbank anzeigen lassen. Dies geht am einfachsten mit

```
ldapsearch -x -LLL -H ldaps://id.fg-networking.de -b dc=de
```

Erklärung der Parameter: -x stellt auf einfache Authentifizierung um (im Gegensatz zu SASL), -LLL gibt die Daten im LDIF Format aus, ohne Kommentare und ohne Anzeige der Versionsnummer, mit -H wird die URI des LDAP Servers übergeben und -b gibt den Startpunkt im Datenbankbaum für die Suche an.

Hinzufügen eigener Konfiguration und Schema zum OpenLDAP-Server

Neuer Versionen von OpenLDAP benutzen nicht mehr die slapd.conf, sondern ein Konfigurationsverzeichnis slapd.d mit eigener Datenstruktur. Um neue Konfigurationen hinzuzufügen legt man eine LDIF-Datei mit der Konfiguration an und importiert diese mit

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f <file.ldif>
```

Um ein neues Schema einzufügen kopiert man das .schema File nach `/etc/ldap/schema`. Dann erstellt man sich eine temporäre Konfig-Datei (hier als Beispiel `/tmp/schema.conf`) mit folgendem Inhalt

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/mypersonalschema.schema
```

mypersonalschema.schema sei hier das neue Schema. Nun erstellt man sich ein temporäres Verzeichnis (hier `/tmp/ldif_output`) und ruft folgendes auf

```
slaptest -f /tmp/schema.conf -F /tmp/ldif_output
```

Nun editiert man das generierte File z.B. mit

```
vim "/tmp/ldif_output/cn=config/cn=schema/cn={4}
    mypersonalschema.ldif"
```

Hier ändert man dann die ersten drei Zeilen wie folgt

```
dn: cn=mypersonalschema,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: mypersonalschema
```

Am Ende der Datei löscht man dann noch die Zeilen mit folgenden Anfängen

```
structuralObjectClass:
entryUUID:
creatorsName:
createTimestamp:
entryCSN:
modifiersName:
modifyTimestamp:
```

Nun kann man das Ganze in die Systemkonfiguration importieren

```
ldapadd -Y EXTERNAL -H ldapi:/// -f "/tmp/ldif_output/cn=config
    /cn=schema/cn={4}mypersonalschema.ldif"
```

Bei erfolgreichen Import findet sich das Schema nun in `/etc/ldap/slapd.d/cn=config/cn=schema/cn={4}mypersonalschema.ldif`

Einrichten von LDAPS (LDAP-over-SSL)

Zuerst muss man Zertifikat und privaten Schlüssel für das LDAP erzeugen (siehe FGN-CA im Wiki) und diese zusammen mit dem Zertifikat der CA auf den LDAP-Server ablegen (vorzugsweise in `/etc/ssl/certs` bzw. `/etc/ssl/private`). Damit der LDAP-Server die auch verwendet erstellt man eine entsprechende LDIF Datei (hier `olcSSL.ldif`).

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/fg-networking.de_ca.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/id.fg-networking.de-
    key-2015-05-05.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/id.fg-networking.de-crt
    -2015-05-05.pem
```

die man dann in die Konfig importiert mit

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f olcSSL.ldif
```

Nun muss man noch den `SLAPD_SERVICES` Eintrag in `/etc/default/slapd` anpassen damit LDAP auf SSL Verbindungen lauscht.

```
SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
```

(für localhost kann man weiterhin den Standard LDAP (ohne SLL) Port 389 verwenden, LDAPS lauscht standardmäßig auf Port 636). Nach einem Neustart von slapd ist LDAP-over-SSL nun verwendbar.

Auf den Clients muss dann das FGN CA Zertifikat an passende Stelle gelegt werden und folgende Zeile in `/etc/ldap/ldap.conf` eingetragen werden.

```
TLS_CACERT    /etc/ssl/certs/fg-networking.de_ca.pem
```

Fehlt die kann der Client nicht das LDAP Server Zertifikat verifizieren und bricht bei Debian Standardeinstellungen die Verbindung ab. Außerdem muss man in dieselbe Datei noch die neue LDAP Server URI eintragen, z.B.

```
URI ldaps://id.fg-networking.de
BASE dc=fg-networking,dc=de
```

Hier sollte man unter `BASE` auch die LDAP Standard Searchbase angeben, die sinnvollsten Werte dürften hier `dc=fg-networking,dc=de` und `dc=de` sein.

Änderungen an der Apache Konfiguration

Zur Anbindung von LDAP an einen Apache Web-Server wird die `mod_authnz_ldap` verwendet. In der Konfig-Datei `/etc/apache2/mods-available/ldap.conf` muss auch wieder das CA Zertifikat eingetragen werden um LDAPS verwenden zu können. Dazu trägt man (außerhalb jeglichen `<Location>` Kontexts) ein:

```
LDAPTrustedGlobalCert CA_BASE64 /etc/ssl/certs/fg-networking.de
    .pem
```

(In dieser Datei war bereits auch schon der ldap-status handler definiert, an dieser Einstellung muss nichts verändert werden). In der passenden Seitenkonfig (auf NMS: `/etc/apache2/sites-available/default-ssl`) muss man dann noch die URL vom LDAP Server anpassen. Auf NMS sieht die neue Konfig wie folgt aus:

```
<Location />
    AuthType  Basic
    AuthName  "FGN NMS"
    AuthzLDAPAuthoritative  off
    AuthBasicProvider ldap
    AuthLDAPURL ldaps://id.fg-networking.de:636/dc=fg-
   networking,dc=de?uid?sub?
    require valid-user
    Satisfy any
 </Location>
```

Konfiguration des FreeRADIUS-Servers

Zuerst einmal zusätzlich das Paket `freeradius-ldap` installieren (bei Debian sind zwar schon Beispielkonfigs für LDAP mitgeliefert, aber die tatsächlichen Module sind erst in diesem Paket enthalten). In `/etc/freeradius/clients.conf` muss unter `secret` das zu den Uni Mailservern passende Shared Secret eingetragen werden (dies wurde aus der Konfiguration von CommuniGate ausgelesen). Wenn noch Clients an den RADIUS angebunden werden sollen muss unten für die passenden IPs ein Shared Secret vergeben werden das dann auch im Client eingetragen werden muss.

Um LDAP als Authentifizierungsmethode für User zu aktivieren muss in `/etc/freeradius/users` folgende Zeile eingetragen werden:

```
DEFAULT Auth-Type := LDAP
```

Hier ist zu beachten das **EAP nicht mehr funktioniert**. Soll EAP irgendwann benutzt werden sollen muss hier eine andere Möglichkeit gefunden werden (die Dokumentation schlägt eine ähnliche Eintragung für jeden Benutzer einzeln vor).

In `/etc/freeradius/modules/ldap` muss unter `server` der richtige LDAP Server (`id.fg-networking.de`) und unter `basedn` die richtige Searchbase angegeben werden (hier `dc=fg-networking,dc=de`, **muss evtl. noch angepasst werden**)

In `/etc/freeradius/sites-enabled/default` müssen alle Zeilen die `ldap` einkommentiert werden. Einzige Ausnahme bildet die Zeile bei der in den Kommentaren davor erwähnt das sie nur benötigt wird wenn `edir_account_policy_check = yes` eingestellt wurde (Zeile 488 in der aktuellen Datei).

Zum Testen des Ganzen wurde `radtest` aus dem Paket `freeradius-utils` verwendet. Der Aufruf war:

```
radtest <username> <passwort> id.fg-networking.de:1812 10
        <shared-secret>
```

Die Werte in spitzen Klammern müssen natürlich durch die entsprechenden Werte ersetzt werden (ohne die spitzen Klammern).

Erläuterungen zu den verwendeten LDAP Schemas

0. `core` – Enthält LDAP Core Attribute (X.501), wird immer benötigt
1. `cosine` – Enthält die LDAPv3 Attribute (Cosine and Internet X.500 (RFC1274))
2. `nis` – Schema zur Verwendung von NIS, bei uns vermutlich nicht benötigt aber Teil der Linux/Unix Standardinstallationen
3. `inetorgperson` – Schema für die gängigen Personenattribute und andere Attribute für organisationsorientierte Dienste
4. `freeradius` – Schema für RADIUS Atrribute, aus der FreeRADIUS Doku (`/usr/share/doc/freeradius/examples/openldap.schema`)
5. `postfix` – Schema mit zusätzlichen Attributen für postfix address rewrite, von den Autoren des Galileo Press OpenLDAP 2.4 Praxisbuches (in der FGN Bibliothek)

(0-3 sind Teil der Debian Standardkonfig)

Erstellung der LDAP-Verzeichnisstruktur

Die leere Datenbank wurde mit dem interaktiven Debian config script (aufgerufen mit `dpkg-reconfigure slapd`) erzeugt. Als Domain und Organization Name wurde `de` genommen. Die restlichen Fragen wurden mit den Standardantworten beantwortet. Für die drei Domains wurde dann folgende LDIF-Datei (`add_DNs.ldif`) zum Erzeugen verwendet

```
dn: dc=fg-networking,dc=de
o: fg-networking.de
objectClass: top
objectClass: dcObject
objectClass: organization

dn: dc=schabler,dc=de
o: schabler.de
objectClass: top
objectClass: dcObject
objectClass: organization

dn: dc=worden,dc=de
o: worden.de
```

```
objectClass: top
objectClass: dcObject
objectClass: organization
```

Diese wird (nachdem man den LDAP daemon slapd gestoppt hat) in die Datenbank eingefügt mit

```
slapadd -n 1 -l add_DNs.ldif
```

Der Content wird hier mit `slapadd` eingefügt da dies der einfachste Weg ist um dcObjects in der LDAP Datenbank zu erstellen. Für die meisten anderen Datenmanipulationen ist ldapmodify die sicherere und sauberere Variante. Danach kann man (und muss für den nächsten Schritt auch) `slapd` wieder starten.

Als nächstes wurden die `people` organizationalUnits erzeugt, in die alle User Einträge kommen sollen (da wir vor der Fertigstellung des neuen Mailservers nur echte Anwenderaccounts migrieren (keine Mailinglisten Accounts u.ä.) ist dies auch erstmal die einzige benötigte OU). Zum Erzeugen der OUs wurde wieder eine LDIF Datei (`add_content.ldif`) erstellt.

```
dn: ou=people,dc=fg-networking,dc=de
objectClass: organizationalUnit
ou: people

dn: ou=people,dc=schabler,dc=de
objectClass: organizationalUnit
ou: people

dn: ou=people,dc=worden,dc=de
objectClass: organizationalUnit
ou: people
```

Die wurde dann in die Datenbank eingefügt mit

```
ldapmodify -a -H ldapi:/// -D cn=admin,dc=de -W -f add_content.
    ldif
```

Anschließend kann man die User einfügen. Wir haben dazu nach dem folgenden minimalem Template per Skript aus den Klartextdateien von CommuniGate das LDIF dafür generiert.

```
dn: uid=username,ou=people,dc=fg-networking,dc=de
objectClass: inetOrgPerson
objectClass: person
uid: username
sn: Nachname
givenName: Vorname
cn: Vorname Nachname
displayName: Vorname Nachname
userPassword: password
```

Änderungen an der OpenVPN Konfiguration

Konfigurationsdateien `/etc/openvpn/tcp.config` und `/etc/openvpn/udp.config`

```
plugin /usr/lib/openvpn/openvpn-auth-ldap.so /etc/openvpn/auth-
    ldap.config
```

Die Einträge sind notwendig damit das LDAP Plugin überhaupt verwendet wird.

Konfigurationsdatei `/etc/openvpn/auth-ldap.config`

```
<LDAP>
        URL             ldaps://id.fg-networking.de:636
        Timeout         15
        TLSEnable       no
        FollowReferrals yes
        TLSCACertFile   /etc/ssl/certs/fg-networking.de_ca.pem
</LDAP>

<Authorization>
        BaseDN          "dc=fg-networking,dc=de"
        SearchFilter    "(&(uid=%u))"
        RequireGroup    false
</Authorization>
```

OpenVPN muss neu gestartet werden, um die geänderte Konfigurationsdatei anzuwenden.

Konfiguration der Firewall

Der folgende Block zeigt die Ausgabe der Uncomplicated Firewall (`ufw`) über ihre aktuellen Regeln (`ufw` verwendet als Standardregel, die als letzte angewendet wird wenn keine andere Regel zutrifft, ein implizites `* DENY ALL` das nicht angezeigt wird):

```
root@id:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
636                        ALLOW       131.246.197.0/25
636                        ALLOW       10.122.0.0/16
1812                       ALLOW       131.246.197.0/25
1813                       ALLOW       131.246.197.0/25
1812                       ALLOW       10.122.0.0/16
1813                       ALLOW       10.122.0.0/16
1812                       ALLOW       131.246.120.208/28
1812                       ALLOW       131.246.5.14
22                         ALLOW       Anywhere (v6)
```

- SSH (Port 22) ist wie bei Servern bei fgn üblich von sämtlichen Quellrechnern erlaubt (IPv4 und IPv6)

- LDAPS (Port 636) ist aus dem fgn-Subnetz (131.246.197.0/25) und dem privaten fgn-Infrastruktur-Netz (10.122.0.0/16)
- RADIUS (Port 1812 ist der generelle Port des FreeRADIUS-Daemons und Port 1813 ist der Port für Accounting) ist zugelassen für Verbindungen aus dem öffentlichen fgn-Subnetz (131.246.197.0/25), dem privaten fgn-Infrastruktur-Netz (10.122.0.0/16), den TU E-Mail-Servern 131.246.120.208/28 und dem RADIUS-Server der TU 131.246.5.14. Der RADIUS-Proxy Port 1814 wurde hier nicht gebraucht weswegen keine Verbindungen zu ihn freigeschaltet wurden.

Die Firewall-Regeln wurden nach Vorbild der Regeln für den CommuniGate Server erstellt.

Auf den neuen LDAP-Server umgestellte Systeme

- nms Webserver
- aio Webserver
- lab-mm Webserver
- OpenVPN

Noch nicht umgestellte Systeme

- Egroupware (mangels Passwort und Fachwissen vom System)
- Mailserver

Anmerkung: Eine Kundendokumentation für Anwender war nicht notwendig da sich auf Anwenderseite nach der Umstellung keine sichtbaren Änderungen gibt.