Warp9 IT-Sicherheit und Netzwerkmanagement

Fedora Directory Server - LDAP als Bindeglied zwischen UNIX und Active Directory

Michael Buth
IT Security Consulting
Warp9 GmbH

web: http://warp9.de
web: http://www.vpngate.de
mail: kontakt@warp9.de

Ausgangssituation

- Enterprise Kunde mit heterogener Netzwerkstruktur hat Linux, UNIX, Solaris und Active Directory Systeme (AD) in seinem RZ im Einsatz
- Über 10.000 Standorte greifen auf die RZ Systeme zu
- Sowohl UNIX als auch AD Benutzer haben Zugriff auf eine Vielzahl an Rechnersystemen
- Auf jedem UNIX Rechner eigenen Benutzer und Passwort
  - Reale Personen haben mehrere verschiedene Benutzerkonten und Kennwörter
  - Benutzer muss sich mehrere Benutzerkonten und Kennwörter merken
- Unterschiedliche Kennwortrichtlinien und Konventionen
- Unübersichtliche und komplexe Benutzer- und Gruppen-Administration

Motivation

- Zentrale einheitliche Benutzerverwaltung der UNIX und der Active Directory Benutzer
- Administrative Übersicht auf alle Daten
- Möglichkeit zur webbasierten Verwaltung
- Offener Standard soll Unabhängigkeit von Herstellern ermöglichen
- Performance, Flexibilität und Skalierbarkeit
- Hohe Ausfallsicherheit
- Hohe Sicherheit durch Authentifizierung und Autorisierung

LDAP

- Das **Lightweight Directory Access Protocol (LDAP)** wird seit 1993 an der Universität von Michigan entwickelt
- LDAP ist ein Anwendungsprotokoll, dass im OSI-Modell oberhalb der Transportschicht (TCP) angesiedelt ist.
- LDAP ermöglicht mittels TCP/IP den Zugriff auf **hierarchische** Datenbanken, sprich **Verzeichnisdienste.**
- LDAP beschreibt die auf Abfragen basierende Kommunikation auf objektbezogene Daten zwischen LDAP-Clients und Verzeichnissen. Diese Daten können unter anderem aus Benutzer- und Gruppendaten, IP Daten, Systemkonfigurationen etc. bestehen.
- **LDAP Verzeichnisse** sind in Form eines Baumes (**Tree**) hierarchisch strukturiert.
- Das oberste Objekt innerhalb dieser hierarchischen Verzeichnisstruktur wird als **Root (Suffix)** bezeichnet.
- Darunter verzweigen sich **Container-Objekte (Organizational Unit (OU))** und **Objekte (O)**.
- Jedes Objekt ist dabei mindestens einer Objektklasse mit Attributen zugeordnet.
- Diese Objektklassen sind durch genormte, erweiterbare **Schemata**, die die Struktur bestimmen, definiert.
- Jedes Objekt wird durch seinen **eindeutigen Namen (Distinguished Name (DN))** innerhalb des Verzeichnisses identifiziert.
- LDAP ist auf Autorisierung und Authentifizierung, sowie Personendaten Abfragen optimiert
- LDAP bietet einen sehr schnellen Lesezugriff und eine breite Unterstützung von Softwareprodukten
- LDAP ist bereits „Quasi-Standard“ zur Authentifizierung, Autorisierung und für Adressdatenbanken.
- LDAP übernimmt vom X.500 Standard das flexible objektorientierte Datenmodell.
- LDAP bietet eine verteilte redundante Datenhaltung, die Replikation von Daten zwischen verschiedenen Standorten und eine sehr hohe Verfügbarkeit.

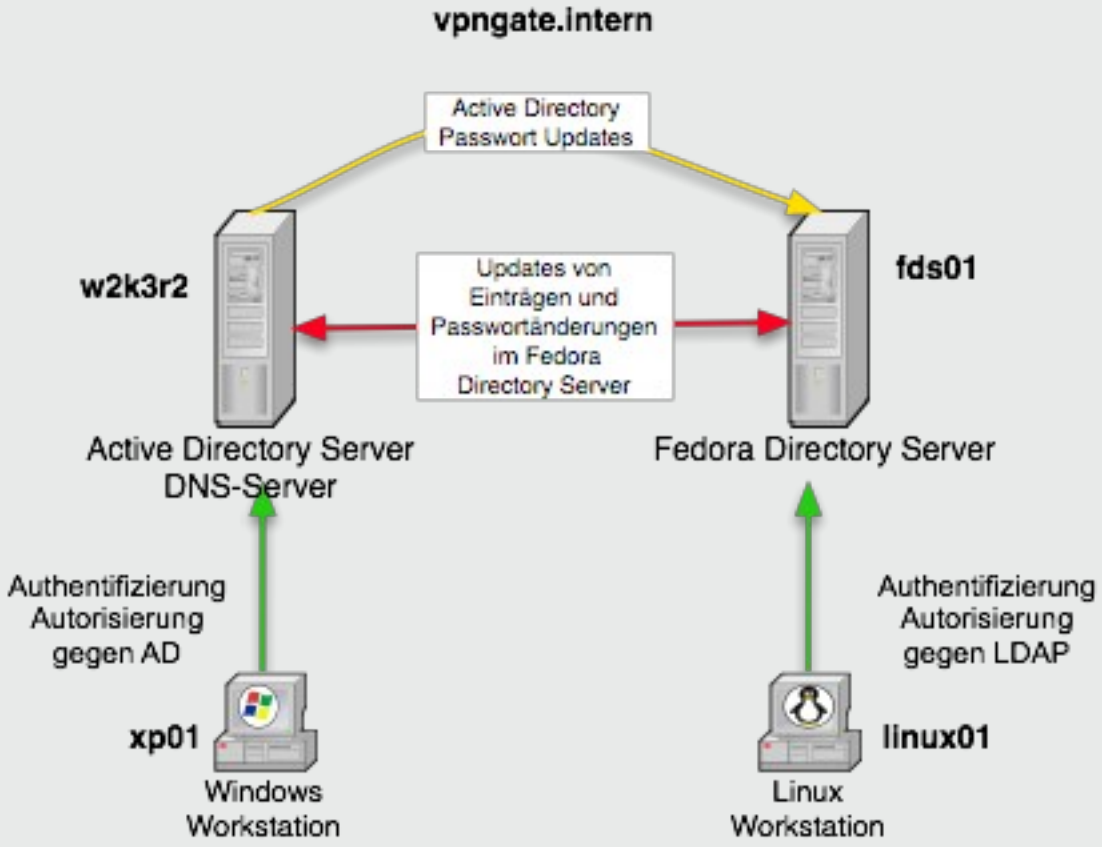
Mehrwert für den Kunden

- Investition in eine zukunftsorientierte Technik
- Gewährleistung der Investitionssicherheit
- Transparenz in der Kosten-Nutzen-Betrachtung
- Kosteneinsparung durch vereinfachte Verwaltung und reduzierte Ausfallzeiten bei gleichzeitig hoher Sicherheit
- Zentrale Administration und Datenhaltung

Fedora Directory Server als „Lösung“

- LDAP V3 (*UNIX Kompatibilität*)
- Synchronisation von Benutzer-, Gruppen und Kennwort-Informationen mit dem Active Directory (*Windows Kompatibilität*)
- ACI (Access Controll Information) und Rollen
- Sichere Authentifizierung (SSLv3, TLSv1 und SASL)
- Vierfache Master Replikation
- Steht unter GPL Lizenz
- Auf Java basierende Verwaltungskonsole
- Webbasierte Verwaltungskonsole
- Überzeugende Stabilität und Performance

Infrastruktur für das Testszenario



Installation der Testumgebung

- Voraussetzungen zur Installation des Fedora Directory Server
  - Fedora Distribution: FC2, FC3, FC4, FC5, FC6, F7, F8
  - Red Hat Enterprise Linux: RHEL3, RHEL4, RHEL5
  - Apache 2, worker model (im Paket *„httpd“* enthalten)
  - Java Runtime (JRE 1.4.2 oder neuer) für die Console
  - SELinux muss im Permissive Modus laufen
  - PKI Struktur (TLSv1 / SSLv3, CA) für LDAP mit SSL (LDAPS)

Installation des FDS

- Die Installation des Fedora Directory Servers erfolgt mittels RPM
  - `[fds01 ~]$ cd download`
  - `[fds01 download]$ rpm -Uvh fedora-ds-1.0.4-1.FC6.i386.rpm`
  - `[fds01 download]$ cd /opt/fedora-ds/setup`
  - `[fds01 fedora-ds]$ ./setup`
- Darauf hin öffnet sich der Installationsdialog für den FDS
  - Hostname, Port, Benutzer ID, Port des Admin Servers (1500) etc. werden hierdurch festgelegt.
  - Das Setup konfiguriert nun eine Datenbank-Instanz und startet den LDAP Server *(ns-ldap)* und den Verwaltungsserver *(httpd, port 1500)*
- Die Verbindung zur Admin Console des FDS kann aufgebaut werden
  - `[fds01 fedora-ds]$ ./startconsole`

    ```
    Username: admin
    Password: **********
    URL: http://fds01.vpngate.intern:1500
    ```

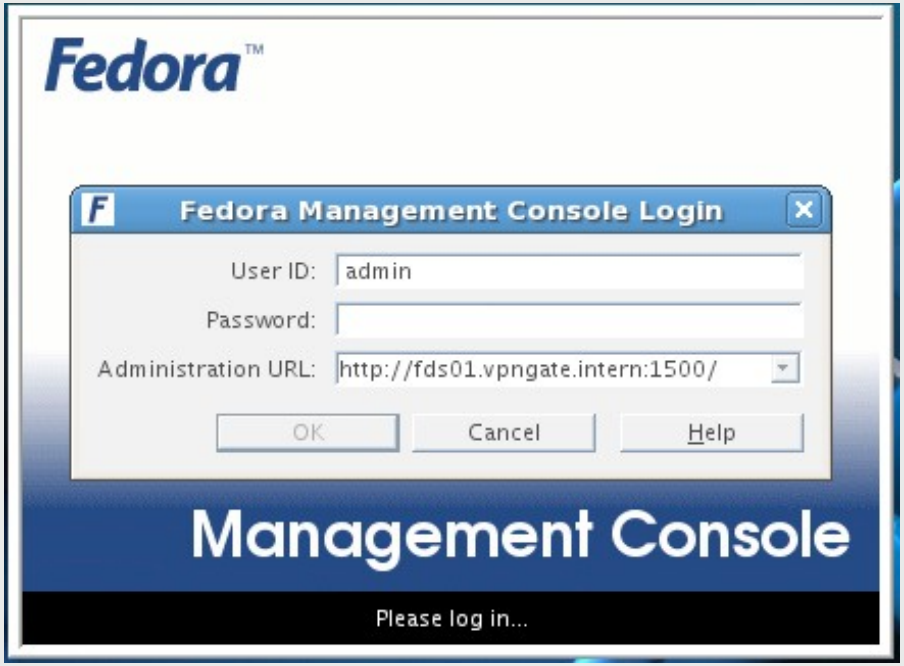
Console starten

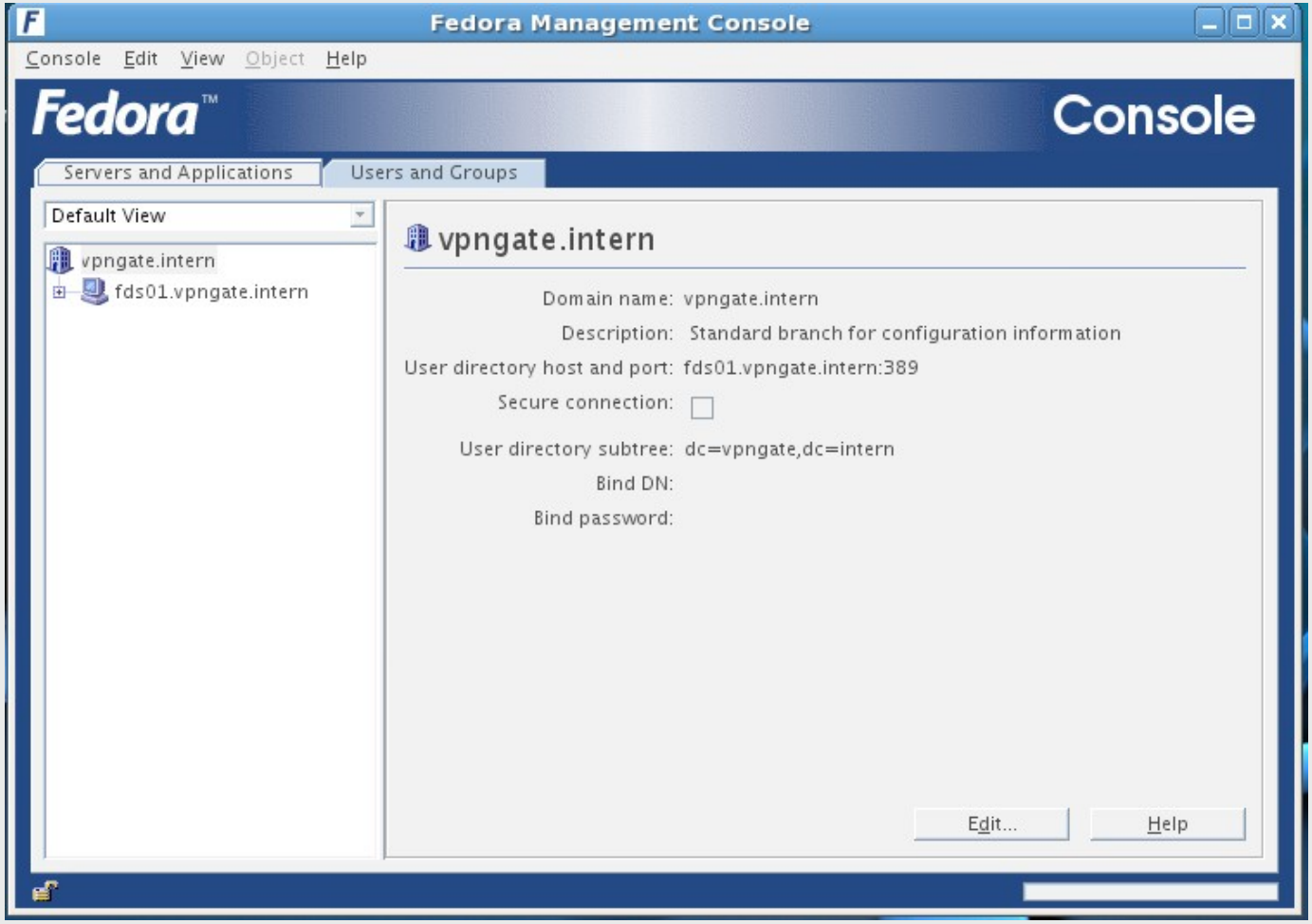
root@fds01:/opt/fedora-ds

Datei Bearbeiten Ansicht Terminal Reiter Hilfe

```
[root@fds01 ~]# cd /opt/fedora-ds/
[root@fds01 fedora-ds]# slapd-fds01/start-slapd
[root@fds01 fedora-ds]# ./start-admin
[root@fds01 fedora-ds]# ./startconsole -u admin -a http://fds01.vpngate.intern:1500/ &
```

Login und Admin Console




Fedora Management Console
Console Edit View Object Help
Fedora™
Console
Servers and Applications
Users and Groups
Default View
vpngate.intern
fds01.vpngate.intern
vpngate.intern
Domain name: vpngate.intern
Description: Standard branch for configuration information
User directory host and port: fds01.vpngate.intern:389
Secure connection:
User directory subtree: dc=vpngate,dc=intern
Bind DN:
Bind password:
Edit...
Help

SSL Konfiguration Fedora Directory Server

- **Automatisierte scriptgesteuerte Konfiguration**
  - ein von Fedora bereitgestelltes Script
    - Download URL: http://directory.fedora.redhat.com/download/setupssl.sh
    - erstellt Zertifikate für die CA, den Directory Server und den Admin Server
    - erstellt die Passwortdateien ***pin.txt*** und ***password.conf***.
    - aktiviert SSL für den FDS
    - exportiert die erstellte CA für z.B. Replicas, OpenSSL etc.

- **Das Script setzt folgendes voraus:**
  - `hostname` **muss zwingend** den **FQDN** des Rechners ausgeben
  - Der FQDN **muss** zur Überprüfung der Zertifikate von allen Clients per DNS aufgelöst werden können
  - Fedora DS ist als RPM Paket als **root** in das Verzeichnis /**opt/fedora-ds** installiert worden.
  - Das Script muss als **root** ausgeführt werden.
  - Eine saubere „frische“ Fedora Installation
  - Nutzung der Standard-Ports **389** (LDAP) und **636** (LDAPS)

fds01.vpngate.intern - Fedora Directory Server - fds01

Console Edit View Object Help

Fedora™ Directory Server

Tasks | Configuration | Directory | Status

- fds01.vpngate.intern:389
  - Data
  - Replication
  - Schema
  - Logs
  - Plug-ins

Encryption | SNMP | Manager | SASL Mapping

Settings | Performance

☑ Enable SSL for this server

☑ Use this cipher family: RSA

Security Device: internal (software)

Certificate: CA certificate

Cipher: Settings...

Client Authentication

- ○ Do not allow client authentication
- ◉ Allow client authentication
- ○ Require client authentication
- ☐ Use SSL in Fedora Console

☑ Check hostname against name in certificate for outbound SSL connections

Save | Reset | Help

Windows Sync

Die Windows Sync Features sind in 2 „Module“ unterteilt in:

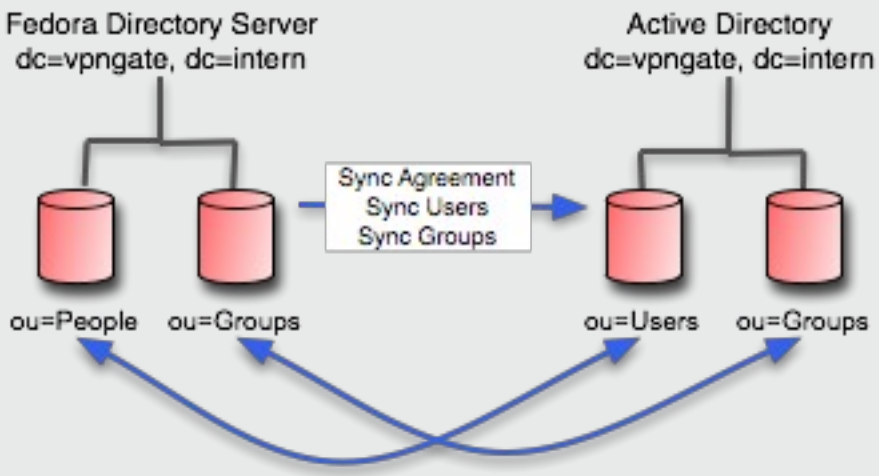
§ **Directory Server Windows Code**

- Code, der einen großen Anteil der Sync-Funktionalität durchführt.
- Code ist in der **Multi-Master-Replication** des Servers integriert.
- Code verwendet denselben Changelog wie die Multi-Master-Replikation.

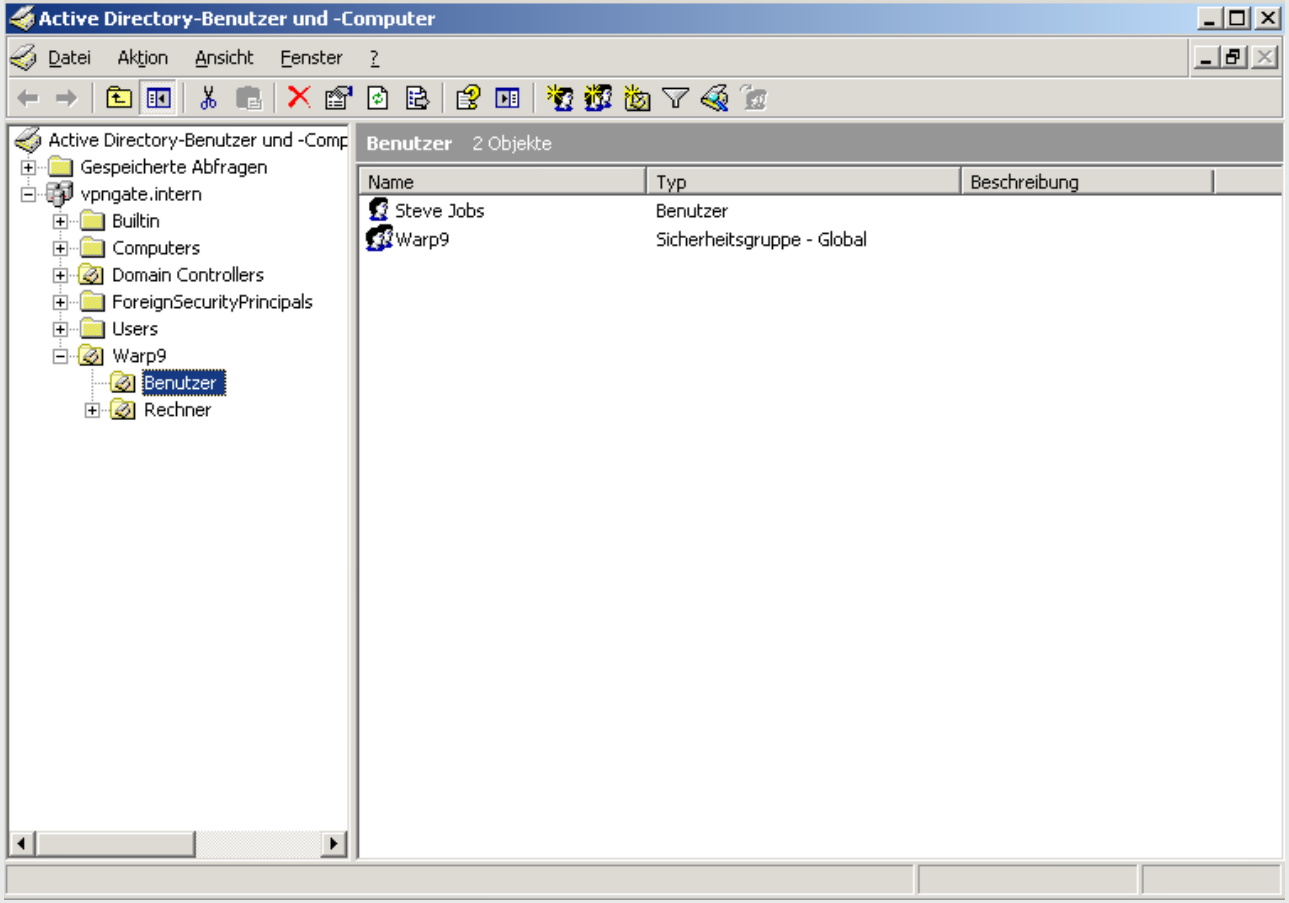
2. Password Sync Service

- MSI- Paket, wird auf dem Aktive Directory Controller installiert.
- Dienst erkennt Kennwortänderungen für Windows-Benutzer.
- Änderungen werden zum Fedora DS über LDAPS weitergegeben.

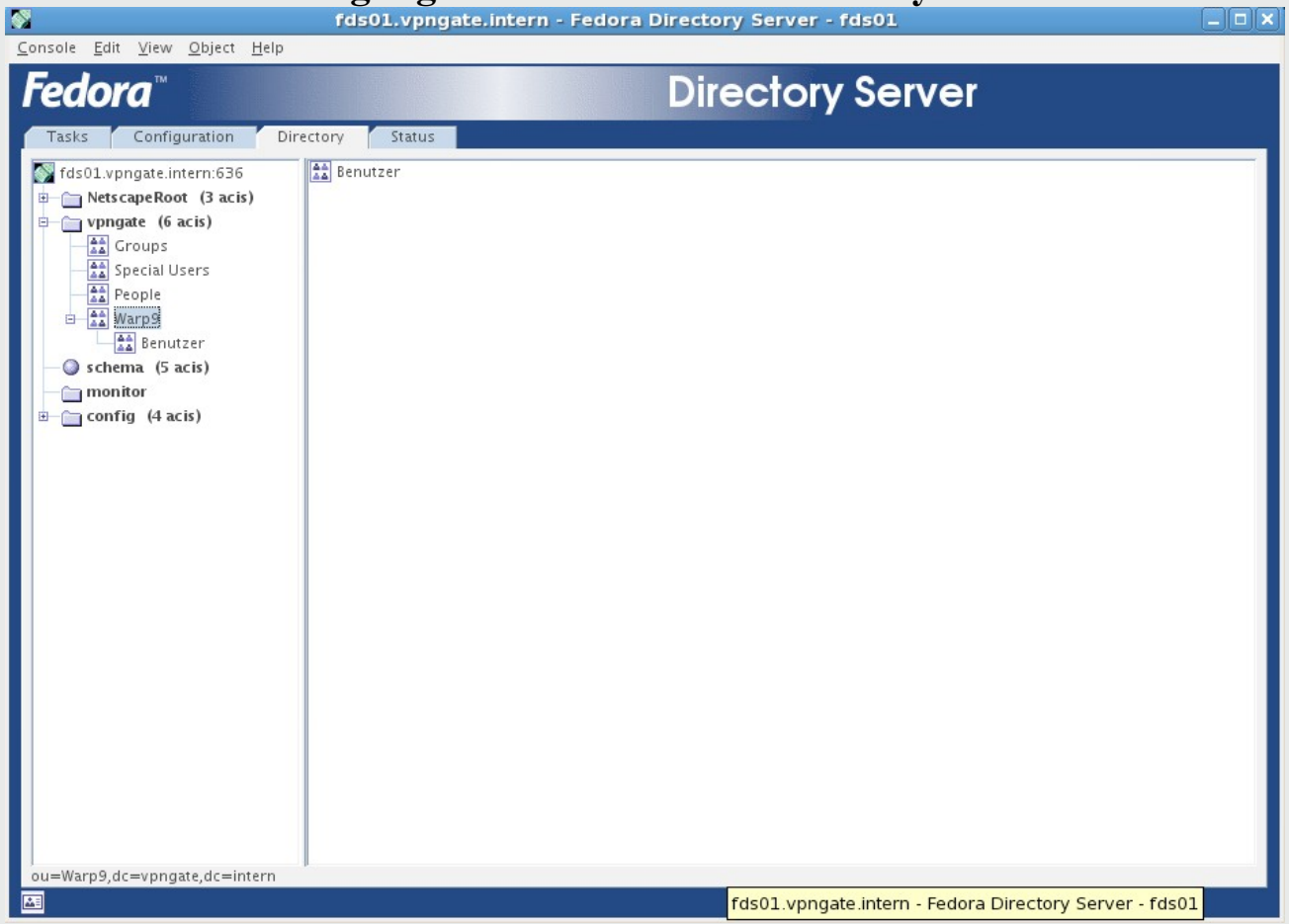
Funktionsweise von Windows Sync



Ausgangssituation Active Directory



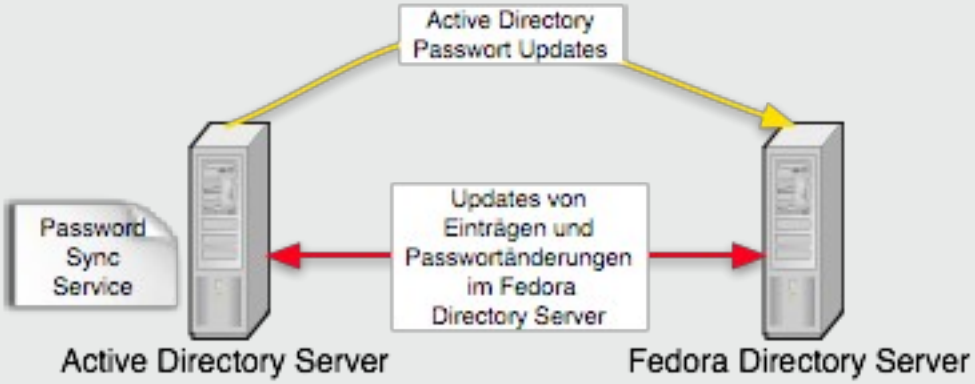
Ausgangssituation Fedora Directory



Funktionsweise von Windows Sync

- Über LDAPS werden Aktualisierungen in beide Richtungen ausgetauscht
- ***Synchronization Agreements*** kontrollieren die Synchronisation
- Sync Agreements enthalten ***Sets of Information*** (u.a. Hostname und Port des AD Servers)
- Subtree **DNs** (***Distinguished Name***) werden in den Sync Agreements vereinbart.
- Zwischen AD und FDS werden **nur** Benutzer- und Gruppenobjekte synchronisiert
- Synchronisation einzelner Subtrees erfolgt in beide Richtungen
- Untergeordnete ***Container-Objekte (OUs)*** des Subtrees müssen manuell erstellt werden
- Windows Sync kann Container Objekte nicht eigenständig erstellen!
- Windows Sync kontrolliert, welche Einträge synchronisiert werden.
- Auch ***Subsets*** aller Einträge können synchronisiert werden
- Der ***Replication-Changelog*** des FDS registriert Modifizierungen
- Manueller ***Re-Synchronization Process*** kann am FDS initiiert werden.
- Im AD regelt ***Dirsync*** in 5 min. Intervallen die Synchronisation von Modifikationen
- Im FDS können „Updates“ auch manuell synchronisiert werden.
- Der ***Password Sync Service*** synchronisiert Kennwort Änderungen.

Funktionsweise Password Sync



Installation des Sync Services

- Der Directory Server Windows Code ist in der Multi-Master-Replication des FDS integriert.
- Password Sync Dienst wird auf dem AD-Server installiert.
- Kennwortänderungen werden zwischen FDS und AD über LDAPS synchronisiert.
  - Bereits existierende verschlüsselte AD-Benutzer Kennwörter werden nicht synchronisiert
  - Synchronisierung erfolgt erst bei Änderung des Kennwortes

Voraussetzungen zur Installation des Sync Services

Fedora-DS:

- CA-Zertifikat (Pass Sync)
- FDS Server Zertifikat (Pass Sync)
- Der Verzeichnisserver muss Secure LDAP unterstützen.
- Windows Sync Benutzer muss im AD Domänen-Admin Rechte besitzen.

Active Directory:

- CA-Zertifikat (Pass Sync)
- „Trusted“ Server-Zertifikat des FDS (Pass Sync)
- Server Zertifikat des AD Servers (LDAPS)
- Im Server Zertifikat muss für ***Subject alternative name*** muss die **IP-Adresse** des Servers eingetragen werden.
- AD-Server **muss** LDAPS unterstützen.
- Kennwortkomplexitätsrichtlinien müssen in der AD Domäne aktiviert sein.
- Directory Server Sync Benutzer benötigt Schreibrechte auf Kennwort Attribute des Subtrees.

Installation des Sync Services

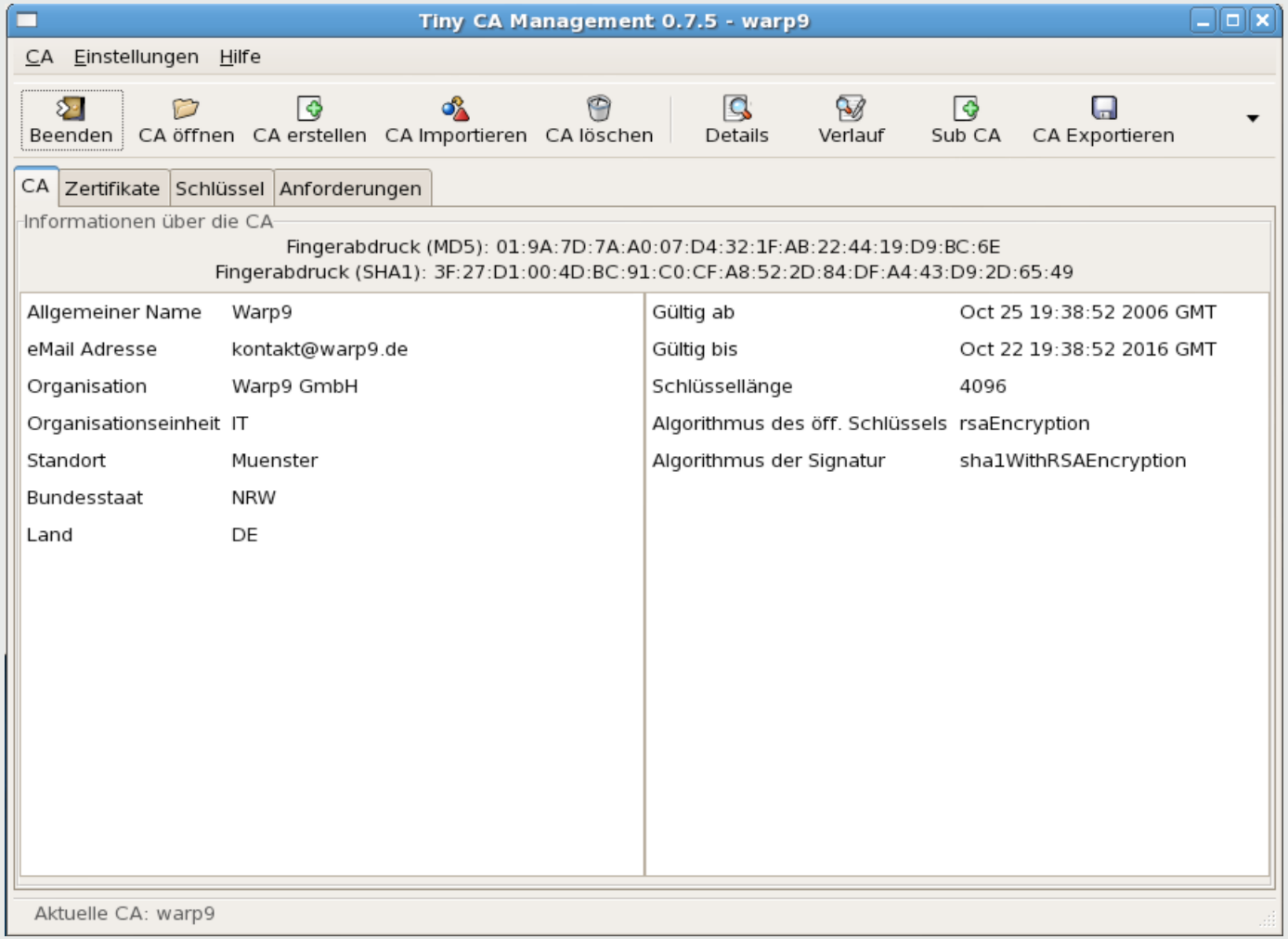
Installation Fedora-DS:

- Windows Code ist Bestandteil des FDS
- PKI Struktur ist ebenfalls bereits durch das „Fedora-Script“ implementiert worden.

Installation AD-Server:

- Server Zertifikat für die LDAPS Unterstützung wird z.B. mittels TinyCA2 erstellt.

Warp9 IT-Sicherheit und Netzwerkmanagement



Installation des Sync Services

Installation AD-Server:

- In TinyCA2 wird *ein neuer Schlüssel und Zertifikat (Server)* erstellt.
  - Der Common Name muss dem FQDN des AD-Servers entsprechen.
  - Beim Sign Request/Create Certificate **muss** die **IP-Adresse** des AD Server im Feld eMail Adresse (***Subject alternative name)*** eingetragen werden.

- Erstelltes Zertifikat muss für den AD-Server exportiert werden
  - PKCS#12 Zertifikat und Schlüssel
  - Anzeigename entspricht FQDN des AD Servers
  - Mit Passwort exportieren
  - CA Zertifikat zu PKCS#12 Struktur hinzufügen
  - Exportierte .p12-Datei auf den AD-Server kopieren

Installation des Sync Services

Installation AD-Server:

- Zertifikat und Key mittels **MMC Zertifikate** auf dem AD-Server installieren.
  - AD Server Zertifikat liegt dann unterhalb „*Eigene Zertifikate*“
  - Zertifikat der CA liegt unterhalb „*Vertrauenswürdige Stammzertifizierungsstellen*“

- AD-Server neu starten und LDAPS (Port 636) Unterstützung testen:
  - netstat -p tcp -n
  - telnet localhost 636
  - GUI: LDP (Support Tools Server CD)

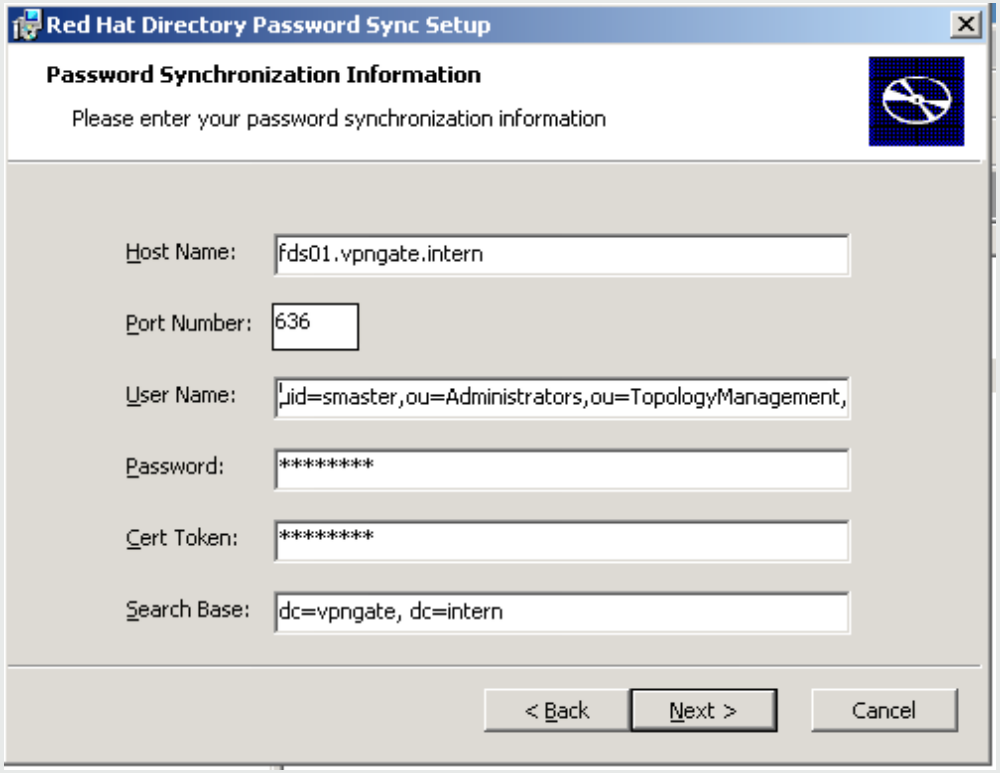
Installation des Sync Services

Installation AD-Server:

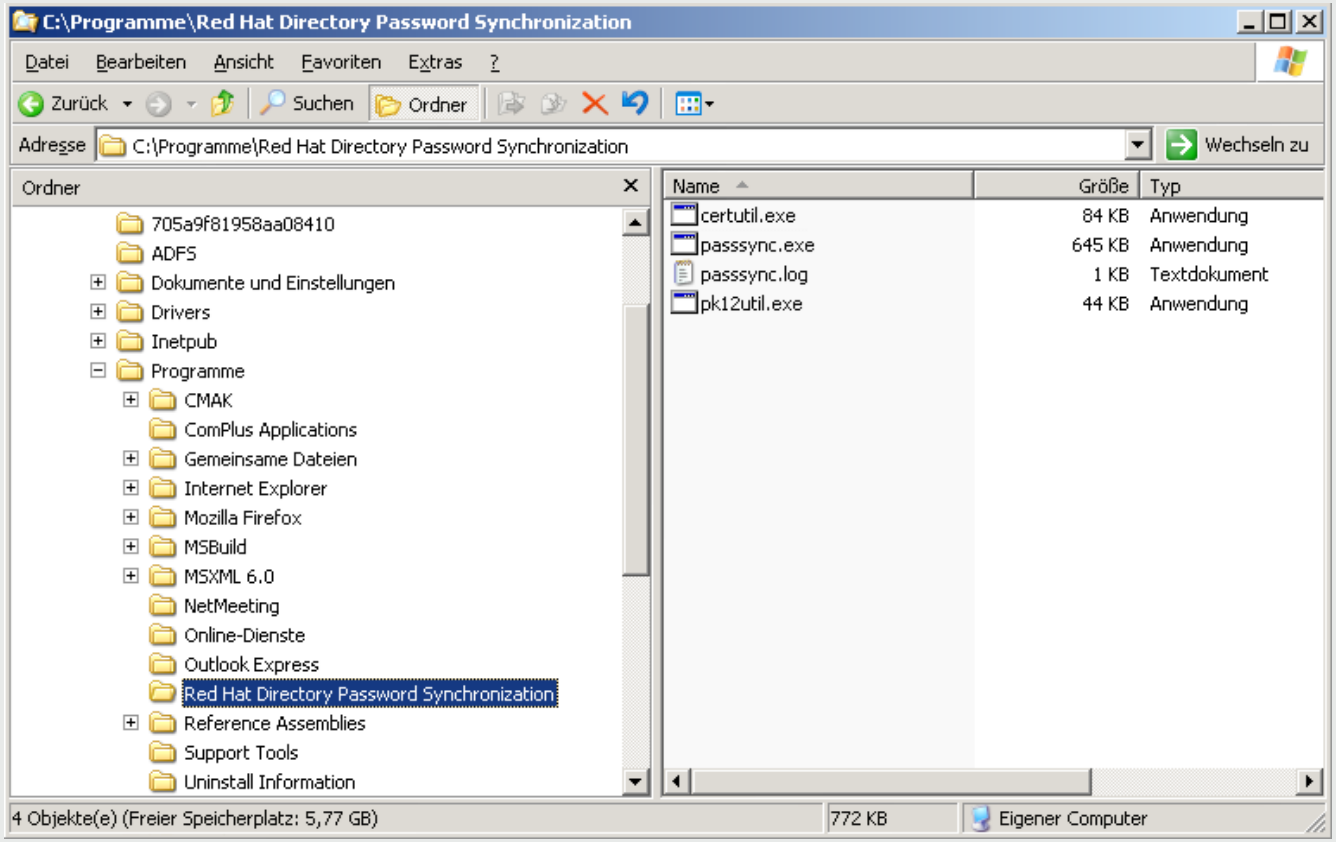
- Die Datei ***PassSync.msi*** auf dem AD-Server installieren
- Download URL: http://directory.fedoraproject.org/download/PassSync-20060330.msi
- Folgende Parameter müssen als Password Synchronisation Information angegeben werden:

  - (FDS) Hostname: **ds01.vpngate.intern**
  - (LDAP SSL) Port Number: **636**
  - (Bind DN) User Name: **uid=smaster,ou=Administrators,ou=TobgyManagement,o=NetscapeRoot**
  - (Bind DN -) Passwort: ********
  - Cert Token: ********
  - Search Base: **dc=vpngate,dc=intern**

Installation des Sync Services



Installation des Sync Services



Installation des Sync Services

Zertifikate für den Password Sync Service

Auf dem Fedora-DS:

- Mittels ***pk12util*** das Server Zertifikat exportieren:
  - `[fds01 fedora-ds alias]$ pk12util -d . -P slapd-`*serverID*`- -o servercert.p12 -n Server-Cert`
- Mit Hilfe von ***certutil*** das Zertifikat der CA des Directory Server exportieren:
  - `[fds01 fedora-ds alias]$ certutil -L -d . -P slapd-fds01- -n "CA certificate“ -a > cacert.asc`
- Zertifikate auf den AD-Server kopieren

Installation des Sync Services

Auf dem AD-Server:

- Mit Hilfe von ***certutil*** eine neue Zertifikatsdatenbanken erstellen
  - `C:\Programme\Red Hat Directory Password Synchronization\certutil -d . -N`
- Das FDS Server Zertifikat mittels ***pk12util*** in die neue Zertifikatsdatenbank importieren.
  - `C:\Programme\Red Hat Directory Password Synchronization\pk12util.exe -d "C:\Programme\Red Hat Directory Password Synchronization" -i servercert.p12`
- Trusted Peer Status herstellen
  - `C:\Programme\Red Hat Directory Password Synchronization\certutil -d "C:\Programme\Red Hat Directory Password Synchronization" -M -n Server-Cert -t "P,P,P“`
- CA Zertifikat des FDS importieren
  - `C:\Programme\Red Hat Directory Password Synchronization\certutil -A -d . -n "CA certificate" -t "CT,," -a -i cacert.asc`

Changelog aktivieren

fds01.vpngate.intern - Fedora Directory Server - fds01

Console Edit View Object Help

Fedora™ Directory Server

Tasks | Configuration | Directory | Status

- fds01.vpngate.intern:636
  - Data
  - Replication
    - NetscapeRoot
    - userRoot
  - Schema
  - Logs
    - Access Log
    - Error Log
    - Audit Log
  - Plug-ins

Supplier Settings | Legacy Consumer Settings

Settings which configure this server to track changes made to your directory data for replication.

☑ Enable Changelog

Replication Changelog

Changelog database directory: /opt/fedora-ds/slapd-fds01/changelogdb

Browse... Use default

Max changelog records: ☑ unlimited

Max changelog age: days ☑ unlimited

Save Reset Help

Replica erstellen

- Bei der Erstellung der Replica muss der **Current Supplier DN** angegeben werden. Der Supplier Bind DN entspricht einem entsprechend berechtigtem Benutzer im Active Directory:
  - `cn=SyncMaster,cn=users,dc=vpngate,dc=intern`

Synchronization Agreement erstellen

fds01.vpngate.intern - Fedora Directory Server - fds01

Console Edit View Object Help

Fedora™ Directory Server

Tasks | Configuration | Directory | Status

fds01.vpngate.intern:636
- Data
- Replication
  - NetscapeRoot
  - u
- Sche
- Logs
  - A
  - Error Log
  - Audit Log
- Plug-ins

New Replication Agreement...
New Windows Sync Agreement
Refresh Ctrl-R

Replica Settings
Enable Replica

Replica Role
ster
Multiple Master
Dedicated Consumer

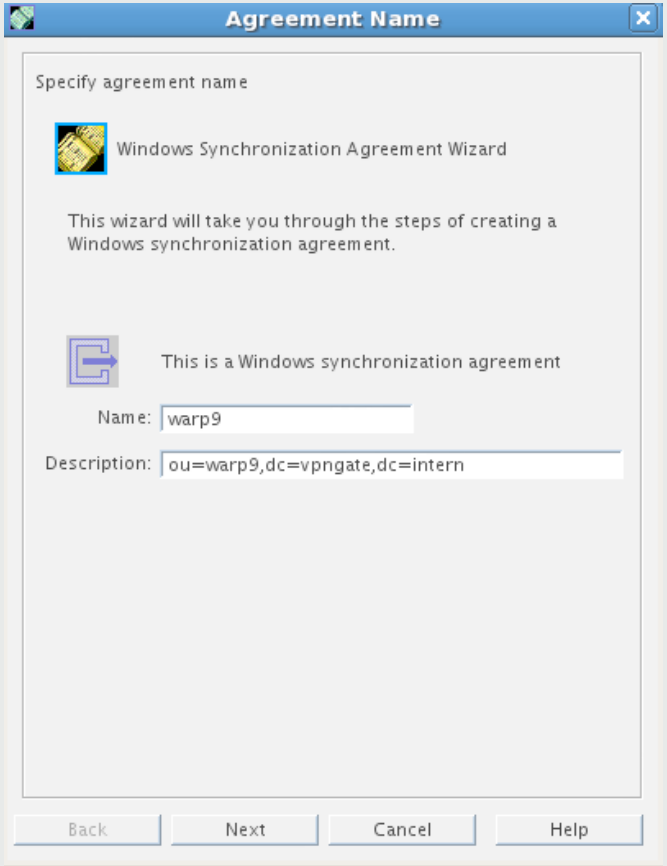
Common Settings
Replica ID: 42 (Must be unique among the IDs of the master replicas)
Purge delay: 7 Day(s) Never
Updatable by a 4.X Replica

Update Settings
Current Supplier DNs:
cn=syncmaster,cn=users,dc=vpngate,dc=intern
Delete
Enter a new Supplier DN:
Add
Current URLs for referrals (Optional)

Save Reset Help

Synchronization Agreement erstellen

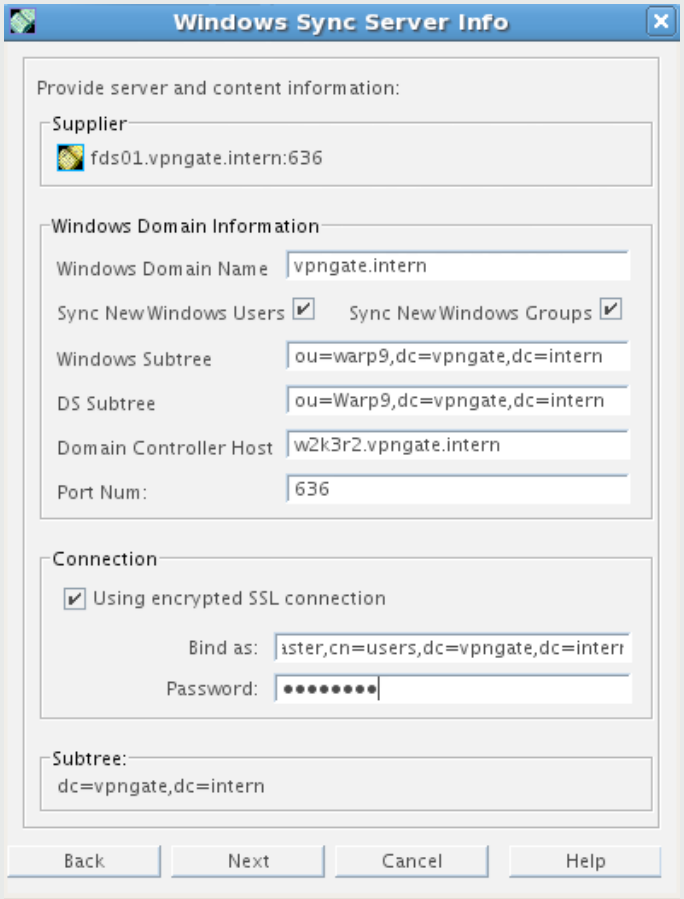
Der Wizzard startet:



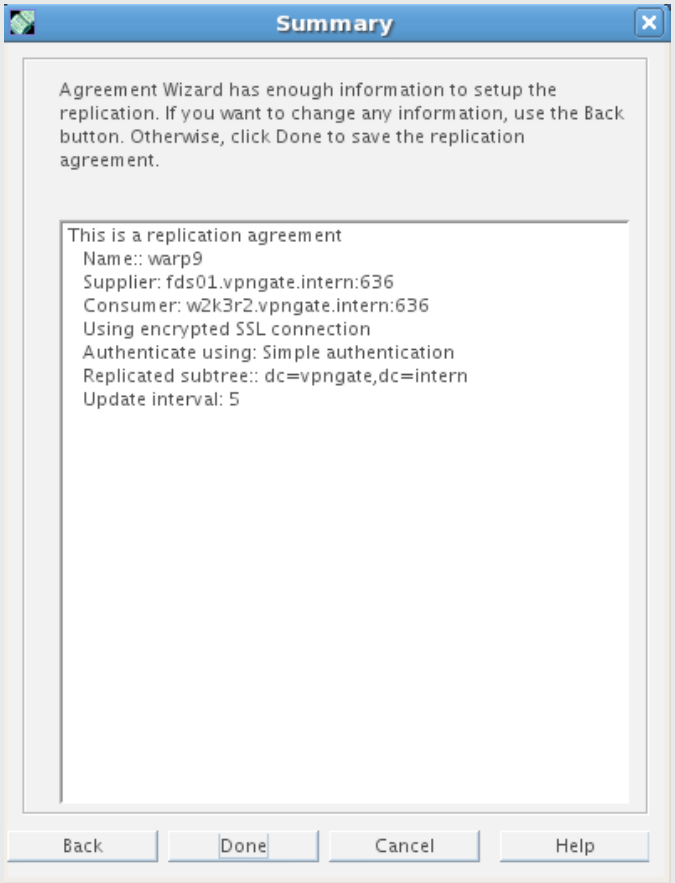
Synchronization Agreement erstellen

- Im Fenster ***Windows Sync Server Info*** werden folgende Parameter abgefragt:
  - **Windows Domain Name:** *vpngate.intern*
  - **Sync New Windows Users:** Ist dieser Wert aktiviert, werden alle von dem Agreement betroffenen Benutzer automatisch auf dem Directory Server erstellt bzw. synchronisiert
  - **Sync New Windows Groups:** Ist dieser Wert aktiviert, werden alle von dem Agreement betroffenen Gruppen automatisch auf dem Directory Server erstellt bzw. synchronisiert
  - **Windows Subtree:** Hier wird der Subtree von dem im AD aus synchronisiert werden soll angegeben: *ou=warp9,dc=vpngate,dc=intern*
  - **DS Subtree:** Hier wird der Subtree zu dem im FDS synchronisiert werden soll angegeben: *ou=warp9,dc=vpngate,dc=intern*
  - **Domain Controller Host:** *w2k3r2.vpngate.intern*
  - **Port Num:** Hier wird der LADAPS Port *636* angegeben.
  - **Using encrypted SSL connection:** Für die Synchronisation von modifizierten Passwörtern **muss** diese Checkbox angehakt sein. Ansonsten weigert sich die Active Directory Passwörter unverschlüsselt zu übertragen.
  - **Bind As:** Hier müssen die Windows Sync Manager Benutzer Informationen eingetragen werden: *cn=SyncMaster, cn=Users,dc=vpngate, dc=intern*
  - **Password:** Kennwort des Sync Manager Benutzers eintragen.

Synchronization Agreement erstellen



Synchronization Agreement erstellen / Zusammenfassung



Synchronisation starten

- Nachdem das Sync Agreement erstellt worden ist, kann nun der Synchronization Process gestartet werden. Das Windows Sync Agreement mit der rechten Maustaste anklicken und ***Initiate Full Re-Synchronization*** auswählen.

- Zur Überprüfung des Synchronisationsstatus können unter dem Reiter ***Status*** die entsprechenden Logs und der Replikationsstatus kontrolliert werden.

- Im Reiter ***Directory*** kann natürlich auch das Ergebnis der Replikation in den entsprechenden Subtrees überprüft werden.

Synchronisation starten

fds01.vpngate.intern - Fedora Directory Server - fds01

Console Edit View Object Help

Fedora™ Directory Server

Tasks | Configuration | Directory | Status

- fds01.vpngate.intern:636
  - Data
  - Replication
    - NetscapeRoot
    - userRoot
      - war
  - Schema
  - Logs
  - Plug-ins

Delete Synchronization Agreement
Send and Receive Updates Now
Initiate Full Re-syncronization
Refresh Ctrl-R

Summary | Connection

This is an Active Directory agreement

Description: ou=warp9, dc=vpngate, dc=intern

ds01.vpngate.intern:636
/2k3r2.vpngate.intern:636

DS Subtree: ou=Benutzer,ou=Warp9, dc=vpngate,dc=intern
Windows Subtree: ou=Benutzer,ou=warp9,dc=vpngate,dc=intern
Replicated subtree: dc=vpngate,dc=intern

Status

Update in progress: FALSE
Last update message: Incremental update succeeded
Number of changes sent since startup: 42:1/0
Begin time of last update: Mon Nov 19 01:53:26 CET 2007
End time of last update: Mon Nov 19 01:53:26 CET 2007

Full (Re)synchronization Status

Full (Re)synchronization: not in progress
Last update message: Total update succeeded
Begin time of last update: Mon Nov 19 01:53:26 CET 2007
End time of last update: Mon Nov 19 01:53:26 CET 2007

Save | Reset | Help

Synchronisation überprüfen

fds01.vpngate.intern - Fedora Directory Server - fds01

Console Edit View Object Help

Fedora™ Directory Server

Tasks | Configuration | Directory | Status

- fds01.vpngate.intern:636
  - Performance Counters
  - Logs
  - Replication Status

Refresh ☑ Continuous refresh

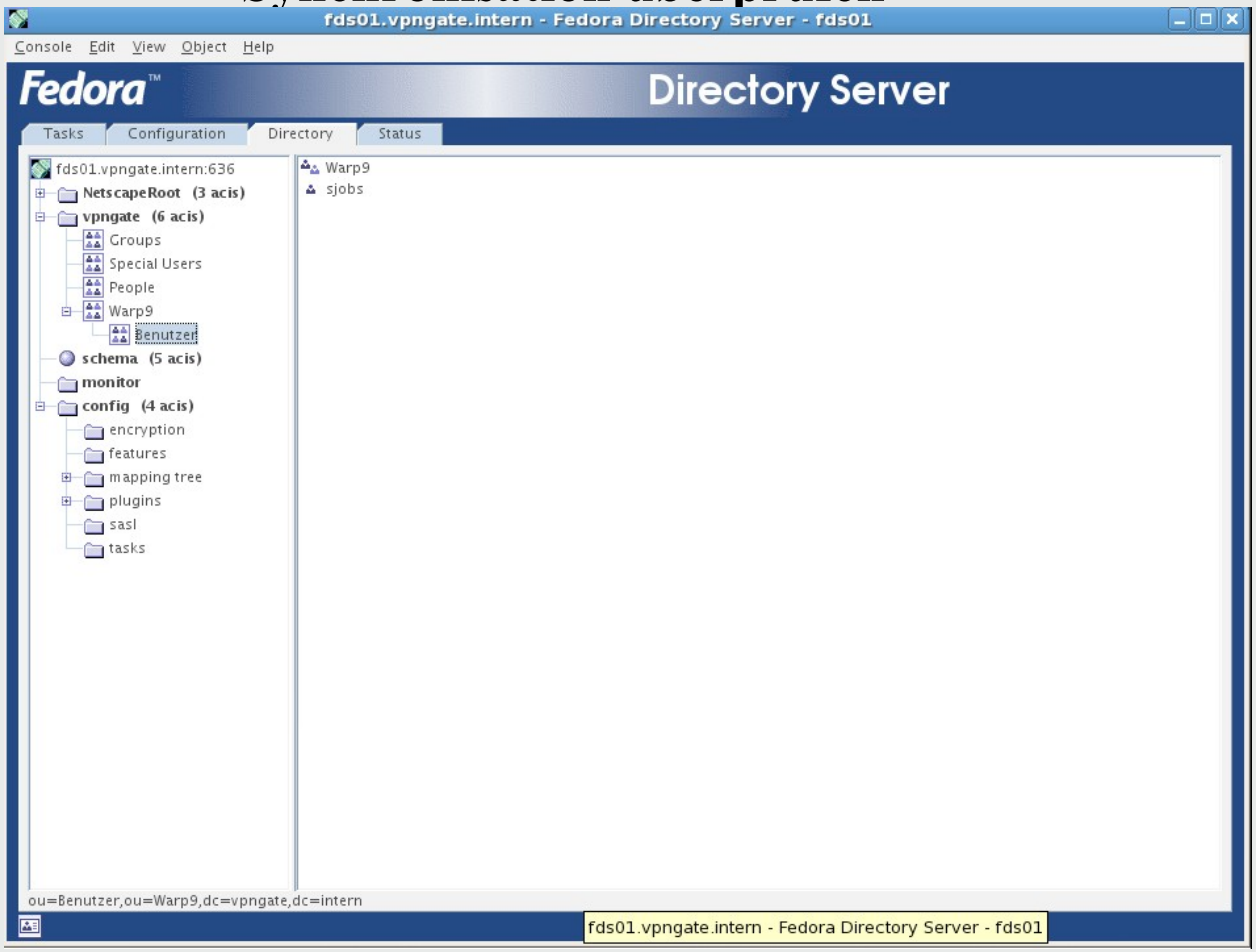
Agreement	Replica suffix	Consumer
warp9	dc=vpngate,dc=intern	w2k3r2.vpngate.intern:636

Agreement	warp9
Replica suffix	dc=vpngate,dc=intern
Consumer	w2k3r2.vpngate.intern:636
Supplier	fds01.vpngate.intern:636
Number of changes	42:1/0
Last replica update began	Mon Nov 19 01:53:26 CET 2007
Last replica update ended	Mon Nov 19 01:53:26 CET 2007
Last update message	Incremental update succeeded
Consumer initialization	not in progress
Last consumer init. update message	Total update succeeded
Last consumer initialization began	Mon Nov 19 01:53:26 CET 2007
Last consumer initialization ended	Mon Nov 19 01:53:26 CET 2007

Help

fds01.vpngate.intern - Fedora Directory Server - fds01

Synchronisation überprüfen



Web Interface zur Verwaltung des FDS

Fedora Management Console - Windows Internet Explorer

http://fds01.vpngate.intern:1500/dist/download

Fedora Management Console

Fedora
Server
Products

Services for Users

Directory Server Express
Search for users by name, user ID or extension.

Directory Server Org Charts
Browse org charts of your organization.

Services for Administrators

Directory Server Gateway
Search for and edit directory entries.

Fedora Home Page
Check for upgrades and information about Fedora server products.

Fedora Administration Express
View server status and configuration/log data.

Copyright (C) 2001 Sun Microsystems, Inc. Used by permission.
Copyright (C) 2005 Red Hat, Inc.
All rights reserved.

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2

Warp9 IT-Sicherheit und Netzwerkmanagement

Fedora Directory Server - LDAP als Bindeglied zwischen UNIX und Active Directory

Vielen Dank für Ihre Aufmerksamkeit !

Michael Buth

web: http://warp9.de
web: http://www.vpngate.de
mail: kontakt@warp9.de

Warp9 IT-Sicherheit und Netzwerkmanagement

Dieses Dokument ist nur für den internen Gebrauch bestimmt.

Jede Art von Kopie, Verteilung oder Veröffentlichung der Informationen in diesem Dokument in gedruckter oder elektronischer Form ist nicht gestattet, außer es liegt eine schriftliche Genehmigung der Warp9 GmbH vor.

Dieses Dokument unterliegt dem ausschließlichen und unbeschränkten Nutzungs- und Urheberrecht.

© 2007 Warp9 GmbH, Münster

Warp9 IT-Sicherheit und Netzwerkmanagement

Impressum

Firma:	Warp9 GmbH
Vertretungsberechtigte Geschäftsführer:	Dr. Klaus Schmoltzi, Michael Buth
Sitz der Gesellschaft:	Scheibenstr. 109, 48153 Münster
Registergericht:	Amtsgericht Münster
Registernummer:	HRB 5465

Umsatzsteuer-Identifikationsnummer gemäß § 27a Umsatzsteuergesetz:	DE201558029
Finanzamt Münster-Innenstadt:	337 5911 0768

Inhaltlich Verantwortliche gemäß § 6 MDStV:	Dr. Klaus Schmoltzi, Michael Buth

Haftungshinweis: Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung für die Inhalte externer Links. Für den Inhalt der hier verlinkten URLs sind ausschließlich deren Betreiber verantwortlich.

Alle Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt und sind möglicherweise eingetragene Warenzeichen. Die Firma Warp9 GmbH richtet sich im Wesentlichen nach der Schreibweise der Hersteller. Andere hier genannte Produkte können Warenzeichen des jeweiligen Herstellers sein.

Warp9® und **Transwarp®** sind eingetragene Warenzeichen der Warp9 GmbH.

Warp9 GmbH
Scheibenstraße 109
48153 Münster

Phone:	+49 251 973 190
Fax:	+49 251 973 192 9
E-Mail:	kontakt@warp9.de
Internet:	http://warp9.de