Domino und LDAP

In der letzten Ausgabe haben wir uns mit den Verzeichnissen von Domino beschäftigt. Diese stellen in Verbindung mit dem speziellen LDAP-Protokoll eine Möglichkeit des schnellen und zielgerichteten Zugriffs auf Daten unterschiedlichster Art dar. Für diesen Zugriff müssen bestimmte Voraussetzungen erfüllt sein.

Diese Voraussetzungen verbergen sich hinter „LDAP“, was die Abkürzung für „Lightweight Directory Access Protocol“ ist. Für die Insider unter uns: LDAP leitet sich vom X.500-Standard ab, der 1998 von einem Konsortium entwickelt wurde, um Informationen verschiedener Systeme in einer Datenbank zu integrieren. Diese gleichartigen Informationen werden allgemein als „Entities“ bezeichnet.

Die Funktionsweise von LDAP ist zwar recht komplex, lässt sich aber für den Anfang mit der nachfolgenden Grafik recht gut beschreiben.

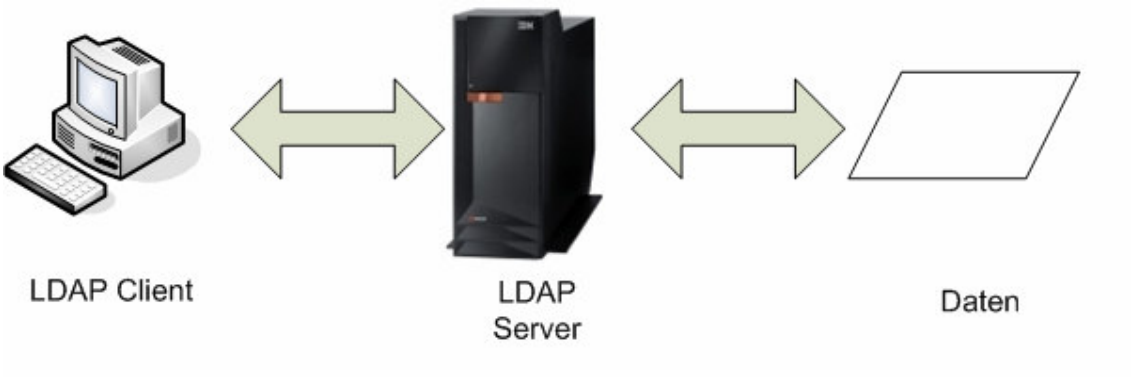

Abbildung 001: LDAP-Ablauf

Ein Client stellt an einen LDAP Server die Anforderung, bestimmte Informationen aus einem Daten-Pool zu ermitteln. Der LDAP Server enthält die „Wegbeschreibung“ zu den Informationen, die in einer weiteren Datenbank gespeichert sind und kann diese recht schnell dem Benutzer oder der anfordernden Anwendung zur Verfügung stellen.

Wir wollen an dieser Stelle nicht in die Details von LDAP eingehen, sondern uns mit der Möglichkeit beschäftigen, LDAP-Dienste in Domino zu integrieren bzw. zu aktivieren.

Domino verfügt selbst über einen integrierten LDAP Server, der auf dem Domino Server als eigenständiger Task ausgeführt wird. Die LDAP-Funktionen können im Zuge der Domino Server-Installation mitinstalliert werden. Sollte auf einem bereits existierenden Server dieser LDAP-Dienst nicht installiert sein, dann kann er jederzeit nachinstalliert werden.

Den LDAP-Dienst finden wir im Domino-Administrator in der Auswahl: „Server -> Status -> LDAP“.

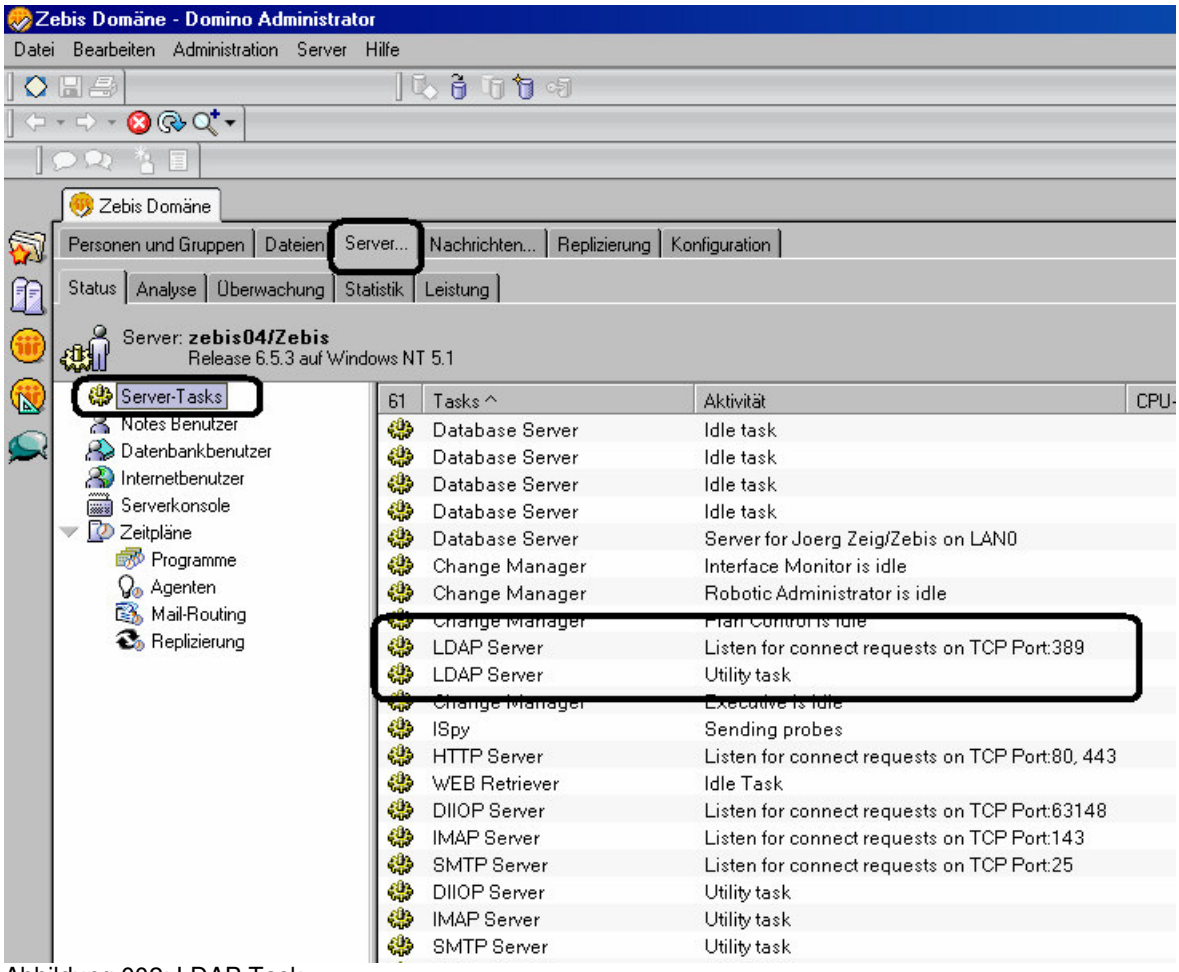

Abbildung 002: LDAP Task

Wie bei den meisten Server Tasks lässt sich der LDAP Server Task auch manuell aus der Administrations-Konsole starten, erneut starten und beenden:

- Load LDAP
- Restart Task LDAP
- Tell LDAP Quit

Alternativ dazu kann der LDAP-Dienst auch über die Auswahl „Task -> Neuen Task starten“ aktiviert werden.

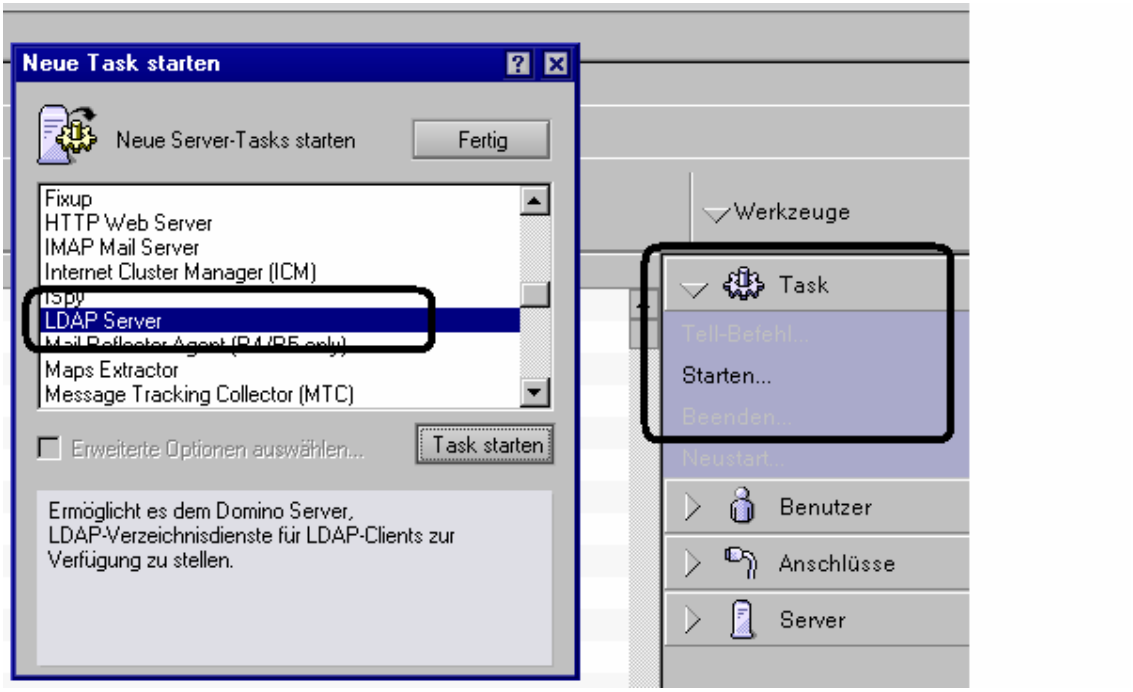

Abbildung 003: Task starten

In der Regel können die Standard-Einstellungen übernommen werden, die IBM für die LDAP-Einrichtung vorschlägt. Per Standard-Definition verwendet der LDAP-Dienst, der über TCP/IP ausgeführt wird, den Port 389. Dabei wird nicht zwischen einem anonymen Zugriff und einem autorisierten Zugriff unterschieden, wie es bei einigen anderen TCP/IP-Diensten der Fall ist.

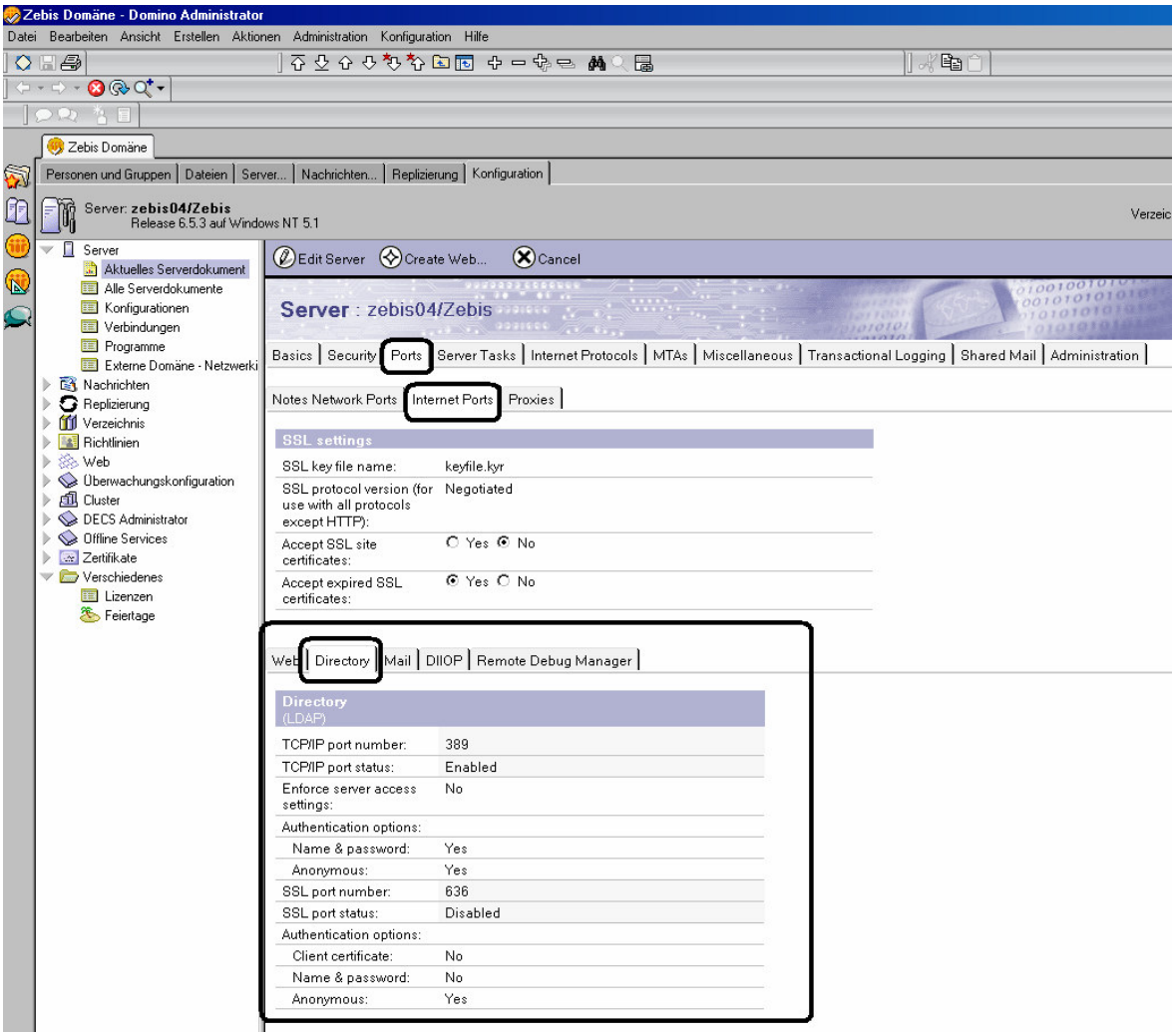

Abbildung 004: LDAP Port-Einstellungen

Die Einstellungen zu diesem Bereich befinden sich im Server-Dokument unterhalb des Eintrages „Ports → Internet Ports -> Directory“.

Ändern Sie diese Angaben aber wirklich nur ab, wenn sich das nicht vermeiden lässt!

Die Verwendung von LDAP in Verbindung mit Domino birgt noch einige Besonderheiten, die ich Ihnen im Nachfolgenden kurz skizzieren möchte.

LDAP Volltext-Index

LDAP arbeitet mit Hilfe von versteckten Ansichten im Domino Directory, um die gewünschten Informationen auffinden zu können. Zum Teil wird für das Auffinden der Informationen ein Volltext-Index benötigt. Damit diese Indexierungen nicht zu viel Performance während der aktuellen Verarbeitung benötigen, kann in Domino definiert werden, dass eine automatische Index-Erstellung für alle LDAP-relevanten Informationen stattfindet.

Die Aktivierung der Volltext-Indexe ist dringend zu empfehlen und kann mit dem nachfolgenden Verfahren durchgeführt werden. Natürlich verwenden wir dazu den Domino-Administrator und öffnen dort unterhalb des gewünschten Domino Servers die Registerkarte „Konfiguration“.

Auf der linken Seite befindet sich der Eintrag „Verzeichnis“, den wir mit einem Klick erweitern und anschließend den Bereich „LDAP -> Einstellungen“ auswählen.

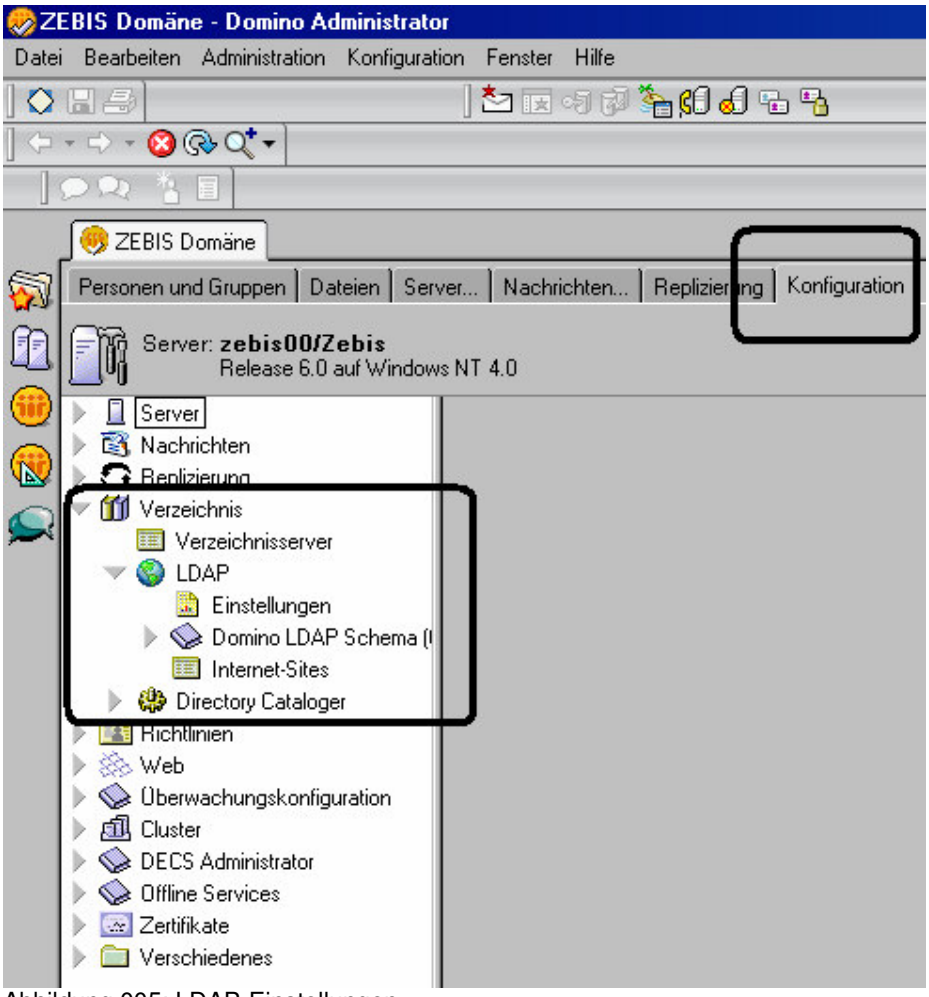

Abbildung 005: LDAP-Einstellungen

Nach der Auswahl öffnet sich der LDAP-Einstellungsbereich. Sollte dieser Bereich nur zur Anzeige geöffnet sein, dann klicken Sie doppelt in den Bereich hinein, damit er im Verwaltungsmodus geöffnet wird.

Unter anderem können in dieser Anzeige auch die Angaben für die Volltext-Indexierung angegeben werden.

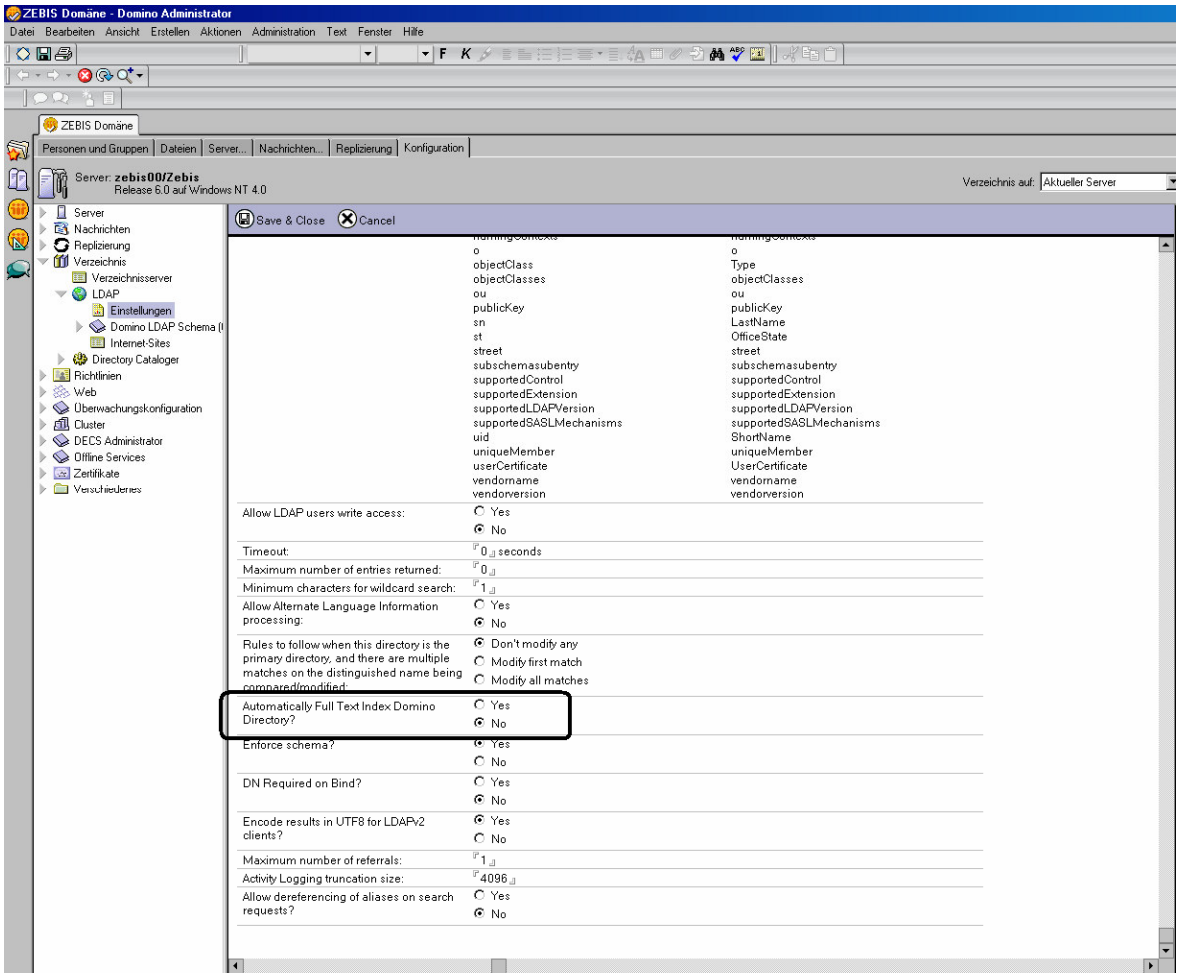

Abbildung 006: Angaben für Volltext-Index

Die Standard-Einstellung ist „NO“; wir ändern sie auf „YES“ ab und schließen diese Anzeige, nachdem wir die Einstellungen gespeichert haben.

LDAP-Schreibzugriff

Im Zusammenhang der Verwendung von LDAP und Domino ist es wichtig, dass per Standard keine Schreibzugriffe für den LDAP Client erlaubt sind. Damit können auch keine Einträge in das LDAP-Verzeichnis geschrieben werden. Das ist aber eine Funktion, die in der Praxis häufig benötigt wird.

Mit einer kleinen Anpassung können wir diesen Schreibzugriff auf das LDAP-Verzeichnis ermöglichen. Dazu verwenden wir wieder die bereits zuvor beschriebene Konfigurationsumgebung für LDAP innerhalb des Domino-Administrators. In derselben Anzeige, in der wir auch die Volltext-Indexierung aktiviert haben, befindet sich der Parameter für die Aktivierung der Schreibrechte. Diesen Parameter verändern wir mit einem Mausklick von „No“ auf „Yes“. Damit ist der Schreibzugriff nun möglich.

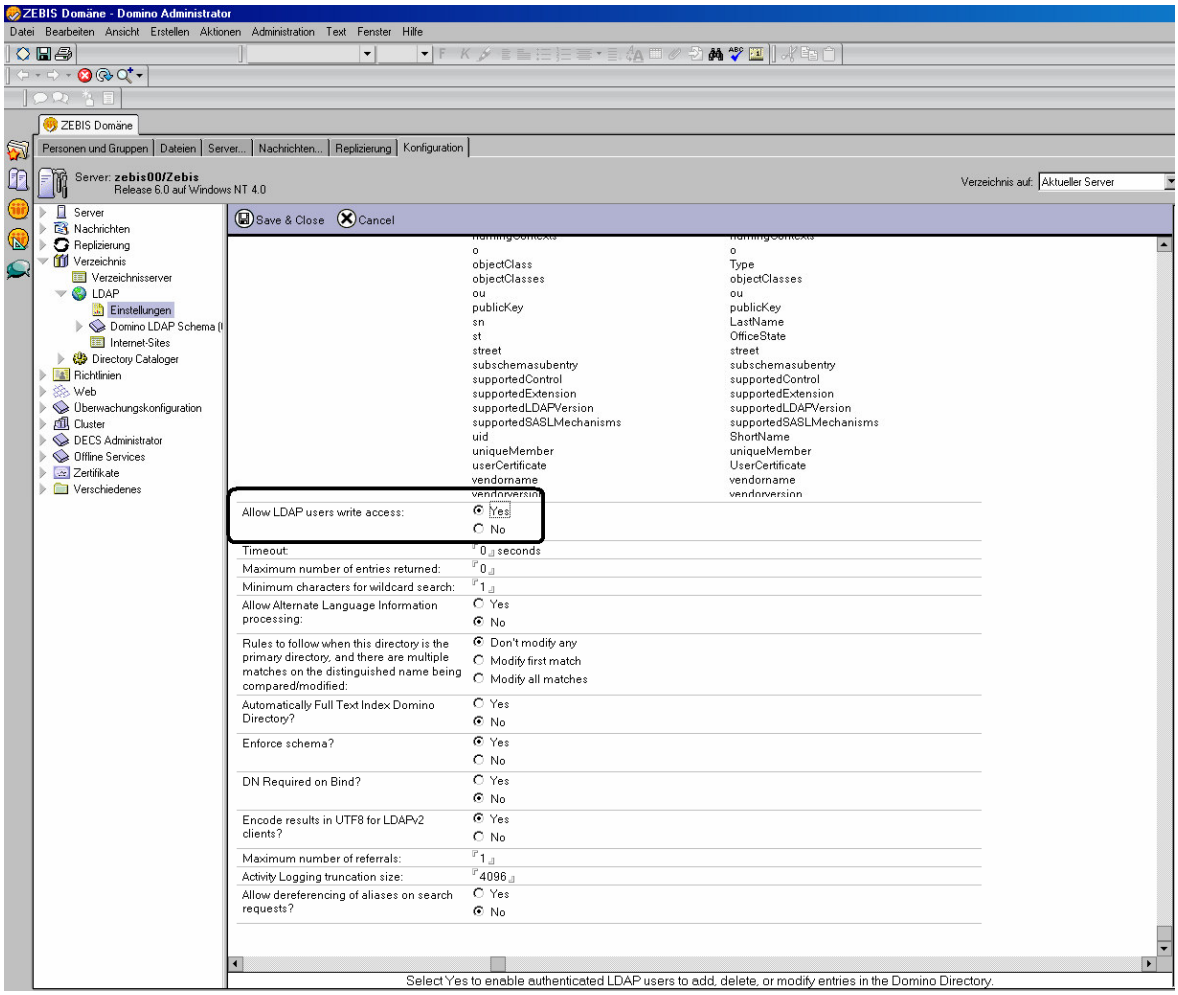

Abbildung 007: LDAP-Schreibzugriff

LDAP und doppelte Namen

Es kann durchaus vorkommen, dass Suchanfragen im Umfeld von LDAP mehrere Einträge – also doppelte Einträge – finden. Dies kann durchaus auch bei so genannten „eindeutigen“ Einträgen der Fall sein, wobei dann die Eindeutigkeit natürlich nicht mehr gegeben ist.

In solchen Fällen muss definiert werden, wie diese zu behandeln sind.

Wie Domino bzw. LDAP in einem solchen Fall reagieren soll, kann ebenfalls in den allgemeinen Konfigurationseinstellungen für LDAP definiert werden. Dabei stehen drei unterschiedliche Auswahlmöglichkeiten zur Verfügung:

- Keinen Eintrag ändern (Standard-Einstellung)
    - Mit dieser Auswahl wird festgelegt, dass keine doppelten Namen verwendet werden. Damit werden auch keine Fehler erzeugt, wenn LDAP doppelte Namen findet. Mit dieser Einstellung besteht dann die Möglichkeit, eine Analyse der doppelten Einträge durchzuführen.
- Ersten Eintrag ändern

- Mit dieser Auswahl wird der erste Eintrag, der gefunden wird, mit diesem Vorgang verarbeitet.

- Alle Einträge ändern
  - Mit dieser Auswahl werden alle gefundenen Einträge mit diesem Vorgang verarbeitet.

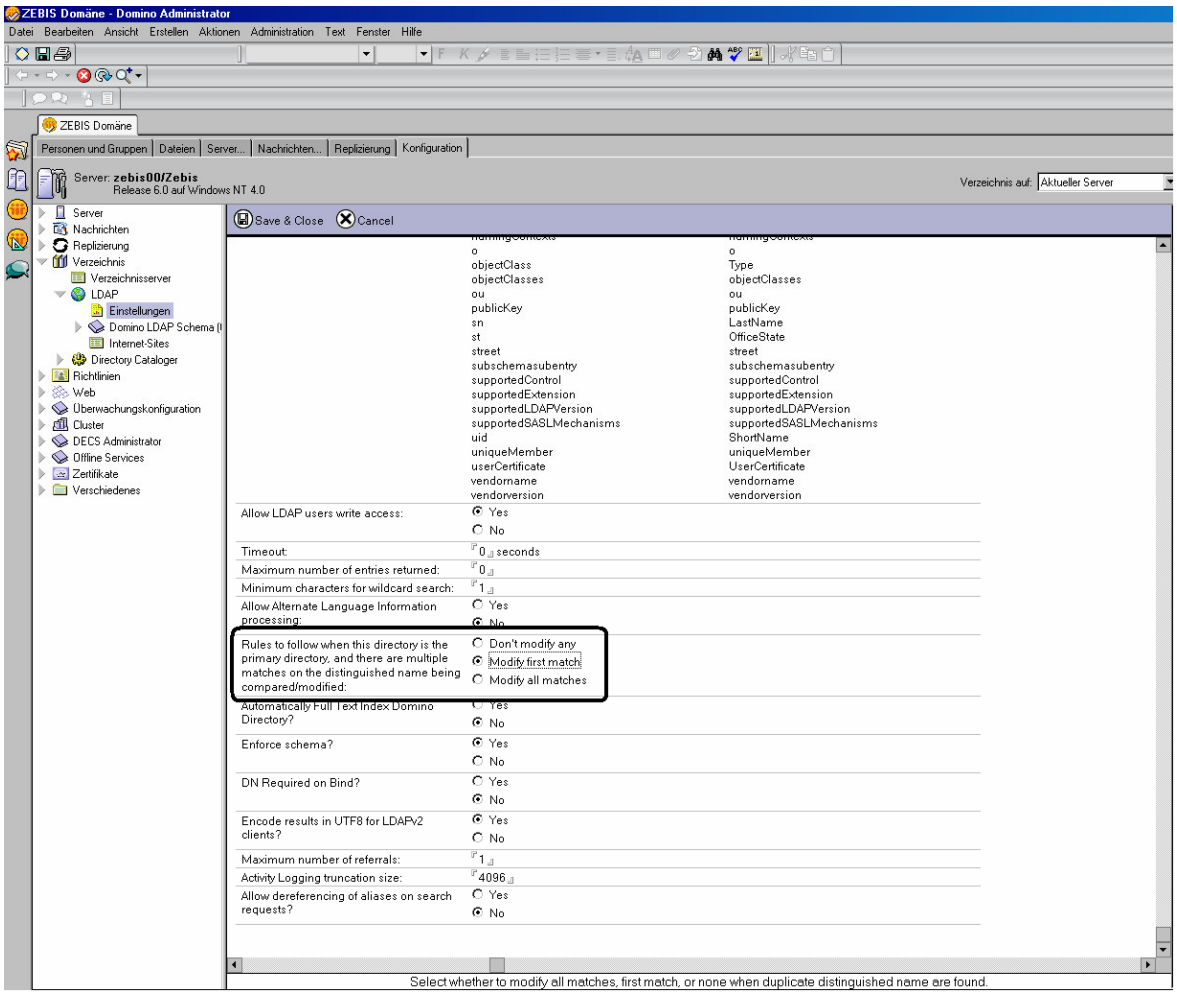

Abbildung 008: Behandlung doppelter Namenseinträge

In der nächsten Ausgabe beschäftigen wir uns nochmals – dann allerdings auch abschließend – mit LDAP. Dabei geht es dann um die Modifikationen des Schemas.