DOCUMENTS

LDAP DIRECTORY

Integration

Ab Version 1.3.0

Inhaltsverzeichnis

1. Voraussetzungen

Für die erfolgreiche Verbindung von **DOCUMENTS 5** mit einem *LDAP*-Verzeichnis müssen folgende Voraussetzungen erfüllt sein:

- Ein LDAP-Browser ist installiert. Auf diesem Wege können *Distinguished Names (DNs)* ausgelesen und aus dem Verzeichnis kopiert werden, ohne Schreibfehler zu verursachen.
- Die folgenden XML-Dateien müssen in einem Verzeichnis abgelegt werden, welches vom DOCUMENTS-Manager aus erreichbar ist:
    - `01_LDAP_Scripts.xml`
    - `02_LDAP_ConfigurationFiletype.xml`
    - `03_LDAP_ConfigurationFolder.xml`
- Die folgenden beiden Dateien müssen in das Verzeichnis `..\server\locale` der **DOCUMENTS 5** - Installation kopiert werden. Im Dateinamen muss der Begriff "*dopaag*" durch den Namen des jeweiligen Mandanten ersetzt werden:
    - `portalstrings_dopaag_de.properties`
    - `portalstrings_dopaag_en.properties`
- Wenn Ihre **DOCUMENTS 5** - Installation nicht mit einem **EASY Archive** verbunden ist, muss die Checkbox *Neue Benutzer automatisch mit Archiv-Zugriff* deaktiviert werden. Diese Einstellung erfolgt im **DOCUMENTS-Manager** im Menü *Documents -> Einstellungen* auf dem Register *Archiv (Basis)* (Abb. 1).

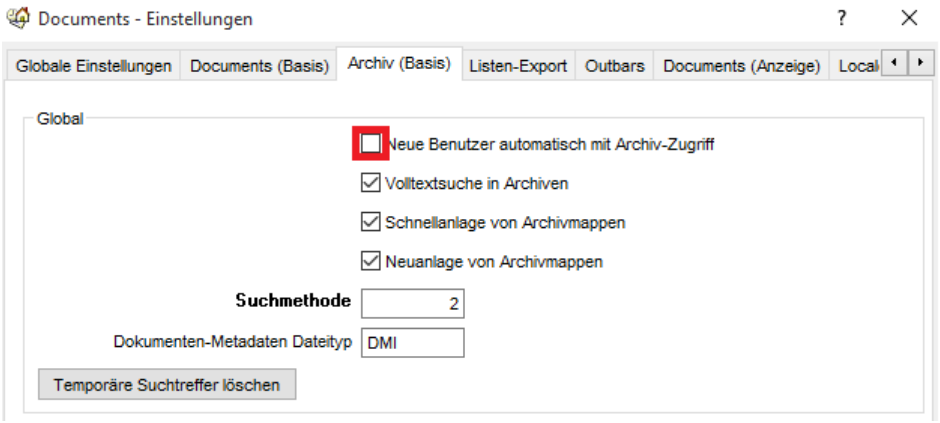

Abb. 1: Einstellung für den Betrieb ohne Anbindung an ein EASY-Archiv

2. Installation der LDAP-Integration

Führen Sie folgende Schritte in der genannten Reihenfolge durch:

- Melden Sie sich als `admin` unter Angabe des Mandanten am **DOCUMENTS-Manager** an.
- Importieren sie folgende Datei über das Menü *Servereinstellungen -> XML-Import*:
    - `01_LDAP_Scripts.xml`

Sie können nun bereits die LDAP-Integration mit Hilfe der soeben importierten Skripte konfigurieren.

Optional besteht die Möglichkeit, die Einstellungen über eine (Singleton-) Mappe direkt in **DOCUMENTS 5** vorzunehmen. Hierzu müssen Sie noch einen vorkonfigurierten *Mappentyp* sowie einen *öffentlichen Ordner* importieren.

Führen Sie folgende XML-Importe in der richtigen Reihenfolge durch:

- `02_LDAP_ConfigurationFiletype.xml`
- `03_LDAP_ConfigurationFolder.xml.`

*Beachten Sie bitte, dass diese Objekte nach dem Import im **DOCUMENTS-Manager** manuell mit* Mappen- und Ordnerzugriffsrechten *eingeschränkt werden sollten. Vergeben Sie exklusive Schreib- und Leserechte für ein administratives Zugriffsprofil.*

Die Installation der benötigten Komponenten ist damit abgeschlossen.

3. Konfiguration der LDAP-Integration

3.1 Einrichtung mit Hilfe der Konfigurationsmappe

Stellen sie sicher, dass folgende Dienste gestartet sind:

- `Documents5Server`
- `Documents5Tomcat`

3.1.1 Basis-Zugangskonfiguration LDAP

Melden Sie sich an **DOCUMENTS 5** an und öffnen Sie in der Ordnerstruktur den Eintrag *LDAP-Konfiguration.* Abb. 2 zeigt ein Beispiel für die Konfigurationsmappe, die daraufhin geöffnet wird.

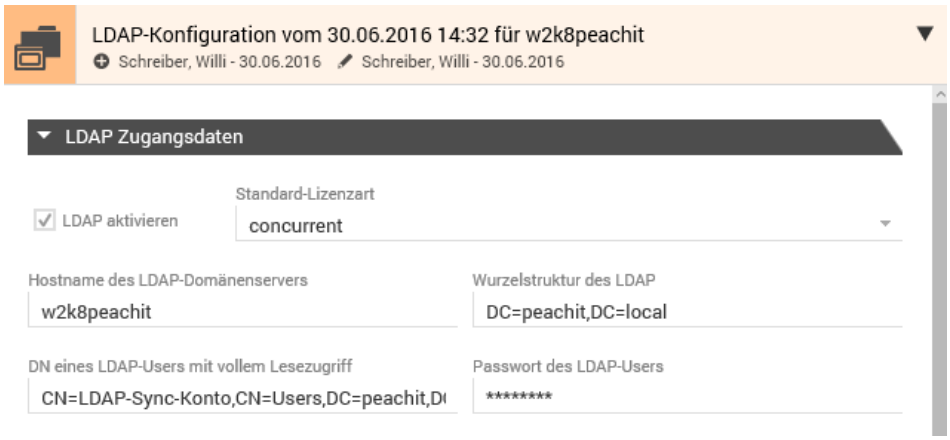

Abb. 2: LDAP-Konfigurationsmappe

Folgende Einstellungen sind auf der Mappe zu berücksichtigen.

Default-Lizenzart (LdapLicenseType)

Abhängig von den vorhandenen Lizenzen kann entschieden werden, welche *Lizenzart* (`named`, `concurrent_standard`, `concurrent_open` oder `concurrent_named`) neu synchronisierten Benutzern standardmäßig zugewiesen wird.

Hostname des LDAP-Domänenservers

Vollständiger Name (*FQDN*) des LDAP-Domänenservers. Beispiel:

```
myDC.peachit.de
```

Wurzelstruktur des LDAP (LdapBaseDN)

Geben Sie hier einen *Startknoten* bzw. ein *Wurzelverzeichnis* im LDAP-System an. Mit dieser Einstellung legen Sie eine *Suchbasis* für sämtliche LDAP-Strukturen fest. Möglichkeiten zur Eingrenzung der zu durchsuchenden Strukturen erfolgen bei der Konfiguration der Benutzer und Gruppen (vgl. das folgende Kapitel 3.1.2).

Beispiel:

```
DC=peachit,DC=de
```

DN eines LDAP-Users mit vollem Lesezugriff

Für den Zugriff auf das LDAP-System wird ein Benutzer benötigt, der Lesezugriff auf die gesamte LDAP-Struktur hat.

Beispiel:

```
CN=Master,CN=Users,DC=peachit,DC=de
```

Password des LDAP-Users

Tragen Sie hier das *Passwort* des oben genannten Benutzers ein. Dieses wird während der Eingabe im Klartext angezeigt und erst beim Speichern durch Platzhalter ersetzt. Es muss daher bei jeder Bearbeitung der Mappe erneut eingetragen werden.

Diese Minimalkonfiguration würde alle Benutzer innerhalb des Root Directory und eine Ebene darunter importieren.

3.1.2 Einstellungen für die Synchronisation

Es können weitere Einschränkungen auf Strukturen hinterlegt werden. Dies ist für zu importierende *Benutzer* und *Gruppen* gleichermaßen möglich (Abb. 3).

Abb. 3: Einstellungen für die Synchronisation

Gruppe für Benutzerimport (LdapSwitchingGroupDN)
An dieser Stelle können Sie eine Gruppen-DN hinterlegen. Auf diesem Wege erreichen Sie, dass alle Benutzer, die Mitglied in dieser Gruppe sind (und ausschließlich diese Benutzer), importiert werden.

Gruppenmodus

Wird eine Benutzerfilter-Gruppe DN angegeben aber kein *Wurzelverzeichnis für Benutzer, werden alle Mitglieder der Gruppe automatisch importiert. Dies geschieht unabhängig davon, in welche OU sie eingeteilt sind.*

Gruppe für Documents-Zugang (LdapDocumentsGroup)
Siehe Abschnitt 3.1.3 „Gruppen für Rechtevergabe“

Gruppe für Archiv-Zugang (LdapArchiveGroup)
Siehe Abschnitt 3.1.3 „Gruppen für Rechtevergabe“

Benutzer aus Untergruppen importieren (groupInGroup.recursiveUserSearch)
Ist diese Option gewählt, werden Benutzer (rekursiv) auch aus Untergruppen importiert, die in der Gruppe für den Benutzerimport Mitglied sind.

Untergruppen als Zugriffsprofile zuweisen (groupInGroup.recursiveAccessProfiles)
Ist diese Option gewählt, werden den Benutzern auch dann importierte Zugriffsprofile zugewiesen, wenn sie nicht direkt darin Mitglied sind sondern nur in einer im LDAP untergeordneten Gruppe. Die Zuweisung der Zugriffsprofile erfolgt rekursiv.

Beispiel:

Benutzer Bernhard Buch ist Mitglied in der LDAP-Gruppe *Vertieb_Team_1*. Diese Gruppe ist wiederum Mitglied in der LDAP-Gruppe *Vertieb_Gesamt.* Beide Gruppen sind Mitglied in der Gruppe *Gruppenimport*, die als *Gruppe für Gruppenimport* verwendet wird. Herr Buch erhält in Documents nun *Vertieb_Team_1* und *Vertrieb_Gesamt* als Zugriffsprofile.

Organisationseinheit (OU) für Benutzer (LdapUserDN)
Wenn der Import der Benutzer auf eine OU eingeschränkt werden soll, können Sie hier den DN einer OU angeben, der alle zu importierende Benutzer enthält. Benutzer aus anderen Bereichen werden nicht synchronisiert. Die Angabe der Gruppe für den Benutzerimport kann dann entfallen.

Aus Performance-Gründen ist die Angabe einer Gruppe für den Benutzerimport der Angabe einer OU vorzuziehen und sollte nur verwendet werden, wenn die Anlage und Pflege einer separaten Gruppe im LDAP nicht möglich ist. Werden sowohl die Gruppe als auch die OU angegeben, werden nur Benutzer importiert die in der OU hinterlegt sind UND Mitglied in der Gruppe sind.

Gruppe für Gruppenimport (LdapGroupFilterGroupDN)
Tragen Sie hier den DN einer Gruppe ein, in der alle Gruppen Mitglied sind, die als Zugriffsprofile in **DOCUMENTS 5** übernommen werden sollen.

*Gruppenmodus für den Import von Zugriffsprofilen (**Ab Version 1.3.0 der LDAP-Kopplung**)*

Wird eine Gruppenfilter-Gruppe DN angegeben aber kein *Wurzelverzeichnis für Gruppen, werden alle Zugriffsprofile, die in der Gruppe Mitglied sind, automatisch importiert. Dies geschieht unabhängig davon, in welche OU sie eingeteilt sind.*

Organisationseinheit (OU) für Gruppen (LdapGroupDN)
Analog zu den Benutzern wird hier der DN einer OU eingetragen, in der alle Gruppen enthalten sind, die als Zugriffsprofile in **DOCUMENTS 5** übernommen werden sollen. Bei Angabe einer OU kann die Angabe einer Gruppe für den Gruppenimport entfallen.

3.1.3 Gruppen für Rechtevergabe

Diese Einträge steuern die Zugangsrechte der Benutzer auf die Anwendungsbereiche **DOCUMENTS 5** und **Archiv**.

Legen Sie in diesem Zusammenhang zwei neue Gruppen in der LDAP-Struktur an, denen alle Benutzer nach diesem Gesichtspunkte zugeordnet werden.

Je nach Mitgliedschaft in diesen beiden Gruppen werden die Zugangsrechte der Benutzerkonten beim Import automatisch gesetzt.

Abb. 4 zeigt, was letztlich in diesem Zusammenhang erfolgt: Auf den Benutzerkonten werden die Checkboxen *Archiv-Zugang* und *Documents-Zugang* entsprechend aktiviert.

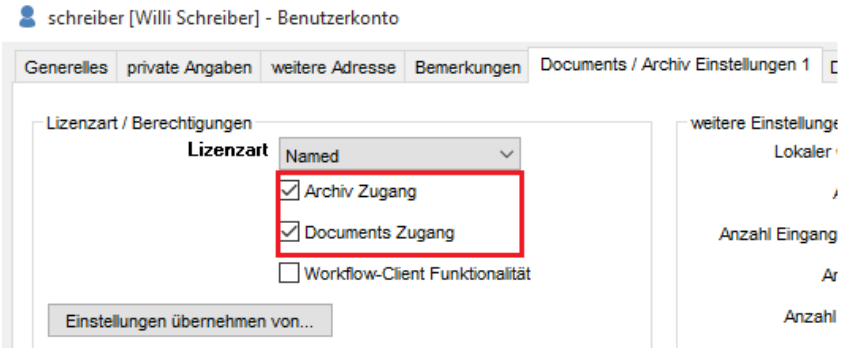

Abb. 4: Zugangsrechte eines Benutzerkontos

Sollen alle Benutzer sowohl Zugang zu **DOCUMENTS 5** als auch zum **Archiv** erhalten, kann in beiden Feldern die gleiche Gruppe hinterlegt werden. In jedem Fall muss jedoch einer der beiden Einträge vorgenommen werden.

Gruppe für Documents-Zugang

Geben Sie hier den DN der Gruppe an, deren Mitglieder *Documents-Zugang* erhalten sollen. Sollen alle importierten Benutzer *Documents-Zugang* erhalten, kann hier die gleiche Gruppe verwendet werden wie bei *Gruppe für Benutzerimport.*

Gruppe für Archiv-Zugang

Geben Sie hier den DN der Gruppe an, deren Mitglieder *Archiv-Zugang* erhalten sollen. Soll dies für alle importierten Benutzer gelten, kann hier die gleiche Gruppe verwendet werden wie bei *Gruppe für Benutzerimport***.**

3.1.4 Unterstützung für Single-SingnOn (SSO)

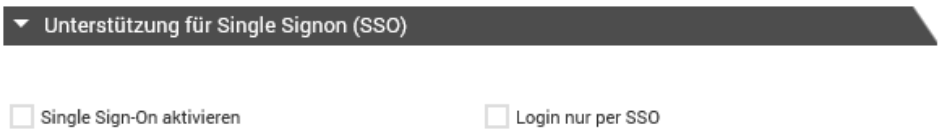

Abb. 5: Einstellungen für die Synchronisation

SSO (Single Sign-On)

Es ist möglich, SSO in Verbindung mit LDAP zu verwenden. Die Konfiguration wird in einer separaten Dokumentation beschrieben. Nach der erfolgreichen Konfiguration von SSO kann diese Checkbox und damit die Verwendung von SSO in Verbindung mit LDAP aktiviert werden.

Login nur per SSO
Wenn diese Checkbox aktiviert ist, können sich Benutzer ausschließlich per SSO anmelden. Voraussetzung hierzu ist die korrekte Einrichtung von SSO.

3.1.5 Einrichtung einer automatischen Synchronisation

Die Synchronisation kann über ein Job-Skript automatisiert werden. Tragen Sie im Bereich aus Abb. 6 ein, ob dies automatisch erfolgen soll (Checkbox *Job aktiviert*) und legen Sie eine Uhrzeit fest, zu der die Synchronisation täglich erfolgen soll.

Abb. 6: Einrichtung eines Synchronisationsjobs

3.1.6 Testen der Konfiguration

Die Verbindung zum LDAP-Server wird beim Speichern der Konfiguration mit dem hinterlegten LDAP-Benutzer getestet. Nach dem Speichern werden oben in der Konfigurationsmappe zwei Schaltflächen eingeblendet, mit denen sowohl der LDAP-Job als auch der Login getestet werden können.

Klicken Sie auf die Schaltfläche *LDAP-Job ausführen*, so können Sie weitere Details im folgenden Dialog aus Abb. 7 abstimmen.

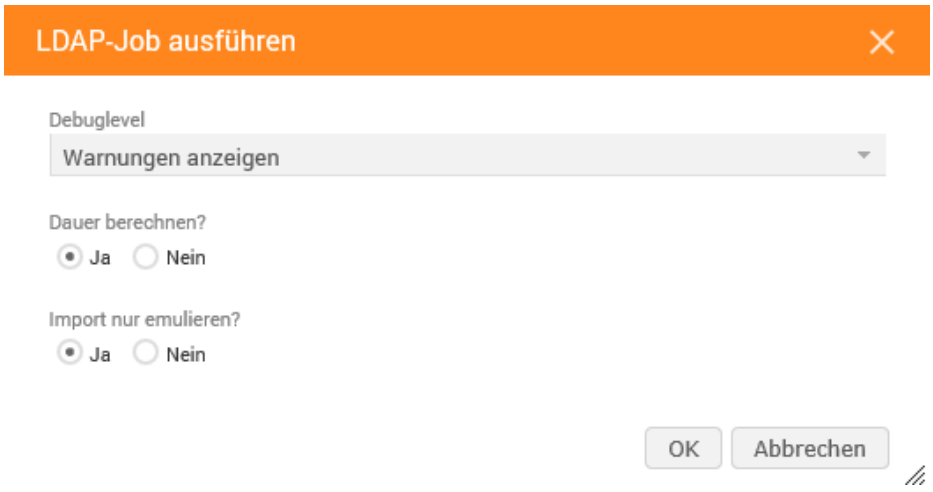

Abb. 7: Details des Konfigurationstests

Für den ersten Lauf des Skripts verwendet Sie bitte die voreingestellten Parameter. Beim Ausführen des Skripts sollte eine ähnliche Ausgabe erzeugt werden wie die folgende aus Abb. 8:

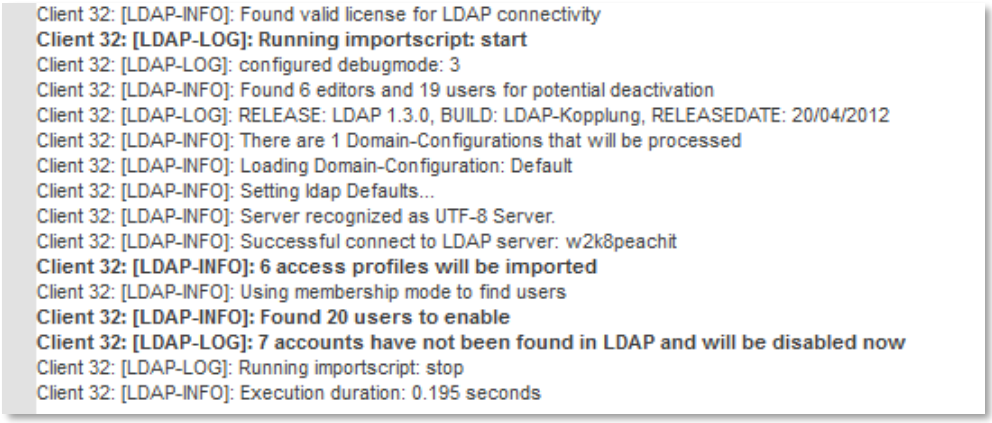

Abb. 8: Ausgabemeldungen des Verbindungstests

Wenn die hier angezeigten Werte plausibel erscheinen, können sie den LDAP-Job erneut ausführen und dieses Mal die Option *Import emulieren* auf *Nein* setzen. Erst jetzt erfolgt ein tatsächlicher Import, und es werden die Benutzerkonten und Zugriffsprofile angelegt.

Wenn das LDAP-Job Skript erfolgreich ausgeführt wurde, können Sie in der Konfigurationsmappe den Bereich *Konfiguration des Synchronisationsjobs* ausfüllen und aktivieren.

3.2 Einrichtung durch Konfigurationsskripte

Bei bestimmten Konfigurationen der LDAP-Struktur ist eine Einrichtung der Anbindung über die oben beschriebene Mappe nicht möglich. Dies ist bspw. dann der Fall, wenn die Benutzer über mehrere OUs verteilt sind und die Benutzer nicht in eine Gruppe zusammen geführt werden können. In solchen Fällen einer erweiterten Konfiguration muss diese zwingend auf der Ebene von Skripten realisiert werden.

Die Konfiguration über Skripte bietet im Vergleich zur Einrichtung über die Mappe verschiedene Erweiterungsmöglichkeiten. Bspw. kann eine Benutzer-Struktur als Array mehrerer OUs eingetragen werden. Im Wesentlichen ist das Vorgehen zur Konfiguration aber in beiden Fällen identisch. Aus diesem Grund werden im Folgenden nicht mehr alle Informationen zu den bereits beschriebenen Aspekten gegeben.

Die Konfiguration findet im Skript `LdapParamDomain statt`.

Das Skript `LdapCallbackFunctions` stellt eine Programmierschnittstelle zur Verfügung, mit der die Funktionalität der LDAP-Schnittstelle erweitert werden kann.

Das wichtigste Konfigurationsskript ist `LdapParamDomain`. Es enthält bereits auskommentierte Beispielwerte um die Konfiguration zu vereinfachen. Um eine Option zu aktivieren müssen nur die „//“ am Anfang der Zeile entfernt werden und der gewünschte Wert eingetragen werden.

LdapParamDomain

Öffnen Sie das Skript `LdapParamDomain` im **DOCUMENTS-Manger** und passen Sie die folgenden Parameter an ihre LDAP-Umgebung an:

- `ldapConfig.LdapLogin`: Für den Zugriff auf das LDAP-System wird ein Benutzer benötigt, der Lesezugriff auf die gesamte LDAP-Struktur hat. Beispiel:

```
CN=Master, CN=Users, DC=peachit, DC=de
```

- `ldapConfig.LdapPassword`: Das Passwort des Benutzers.
- `ldapConfig.LdapHostname`: Vollständiger Name des LDAP-Domänenservers z.B. `myDC.peachit.de`. Diese Option wird als Array-Struktur gespeichert. Es ist möglich, hier mehrere LDAP-Server anzugeben.
- `ldapConfig.LdapBaseDN`: Knoten im LDAP-System, der als Suchbasis für sämtliche LDAP-Strukturen verwendet wird. Im Beispiel:

```
DC=peachit,DC=de
```

- `ldapConfig.useLdapBaseDN` (`true/false`): Wenn dieser Wert auf *true* gesetzt wird, wird die `LdapBaseDN` an jede weitere DN-Option automatisch angehängt.
- `ldapConfig.licenseType`**:** Abhängig von den vorhandenen Lizenzen kann entschieden werden, welche Lizenzart (`named` oder `concurrent`) neu synchronisierten Benutzern zugewiesen wird.
- `ldapConfig.cutPrefix` und `ldapConfig.groupPrefix`: Es ist möglich, **DOCUMENTS**-spezifische Gruppen im LDAP mit einem Präfix zu versehen. Um dieses bei der Synchronisation als Zugriffsprofil in **DOCUMENTS 5** wieder zu entfernen, können diese beiden Optionen verwendet werden.
- `ldapConfig.withSuperior` (`true/false`): Synchronisiert die in LDAP eingestellte *Superior*-Rolle mit der *Vorgesetzten*-Funktion in **DOCUMENTS 5**.
- `ldapConfig.withSupervisor (true/false)`: Synchronisiert den in LDAP eingestellten „*Supervisor*“ einer Gruppe als Attribut des Zugriffsprofils in **DOCUMENTS 5**.
- `ldapConfig.LdapGroupFilterGroupDN`: Die DN einer Gruppe. Alle Gruppen, die Mitglied dieser Gruppe sind, werden importiert. (Es sei denn, sie werden durch die Einstellung in LdapGroupDN eingeschränkt).

Attribute	Value
uSNChanged	102799
uSNCreated	102799
whenCreated	20060403085736.0Z
whenChanged	20060403085736.0Z
instanceType	4
objectCategory	CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=toastup,DC=local
distinguishedName	OU=Zugriffsprofile,OU=Distribution Groups,OU=MyBusiness,DC=toastup,DC=local
objectGUID	Qn□□□□□H□□J□□□
name	Zugriffsprofile
ou	Zugriffsprofile
objectClass	organizationalUnit
objectClass	top

Abb. 9: Auslesen des DN mit einem LDAP-Browser

- `ldapConfig.syncProfiles (true/false)`: Legt fest, ob die im LDAP zugewiesenen Gruppen als Zugriffsprofile in **DOCUMENTS 5** synchronisiert werden sollen (Standard: `true`)
- `ldapConfig.LdapGroupDN` (Array-Struktur): Eine oder mehrere DNs von OUs mit Gruppen, die als Zugriffsprofile in **DOCUMENTS 5** übernommen werden sollen (vgl. Abb. 9).
- `ldapConfig.LdapSwitchingGroupDN`**:** Die DN einer Gruppe. Nur Benutzer, die Mitglied dieser Gruppe sind, werden importiert.
- `ldapConfig.LdapDocumentsGroupDN`: Die DN einer Gruppe. Nur Mitglieder dieser Gruppe erhalten Zugriff auf **DOCUMENTS 5**. Hinweis: Wenn alle importierten Benutzer Zugriff erhalten sollen, kann hier die gleiche Gruppe verwendet werden wie bei `LdapSwitchingGroupDN`.
- `ldapConfig.groupInGroup.recursiveUserSearch (true/false)`: Legt fest, ob auch Benutzer aus Untergruppen der LdapSwitchingGroupDN importiert werden sollen. (Standard: `false`)
- `ldapConfig.groupInGroup.recursiveAccessProfiles (true/false)`: Legt fest, Benutzer auch die Gruppen als Zugriffsprofile enthalten sollen, in denen sie nur indirekt Mitglied sind. (Standard: false)
- `ldapConfig.LdapArchiveGroupDN`: Die DN einer Gruppe. Nur Mitglieder dieser Gruppe erhalten Zugriff auf das Archiv. Hinweis: Wenn alle importierten Benutzer Zugriff erhalten sollen, kann hier die gleiche Gruppe verwendet werden wie bei `LdapSwitchingGroupDN`.
- `ldapConfig.LdapUserDN` (Array-Struktur): Eine oder mehrere DNs von OUs welche UNMITTELBAR User enthalten, die mit **DOCUMENTS 5** synchronisiert werden sollen (vgl. **Fehler! Verweisquelle konnte nicht gefunden werden.**).
- `ldapConfig.singleSignon` (true/false): Bei Verwendung in Kombination mit SSO muss dieser Parameter auf `true` gesetzt werden.
- `ldapConfig.loginOnlyWithSSO` (true/false): Bei Verwendung in Kombination mit SSO steuert dieser Parameter, ob ein Login nur mit SSO möglich ist (`true`) oder auch eine manuelle Anmeldung möglich ist (`false`).

Bitte speichern Sie die Änderungen am Skript und schließen Sie den Dialog.

LdapJob

Öffnen Sie das Skript `LdapJob` und wechseln in das Register *Test*. Geben Sie hier den Login-Namen eines administrativen **DOCUMENTS 5**-Benutzers ein. Auf dem Register *Job* kann eingestellt werden, in welchen zeitlichen Abständen der Synchronisationsjob automatisch gestartet werden soll.

Um die Synchronisation manuell zu starten, verwenden Sie die Schaltfläche *Skript ausführen*.

Um letztlich den Login mit LDAP-Verbindung zu aktivieren, muss noch eine Eigenschaft `loginScript` mit dem Wert `LdapLogon` am Mandanten hinzugefügt werden (Abb. 10).

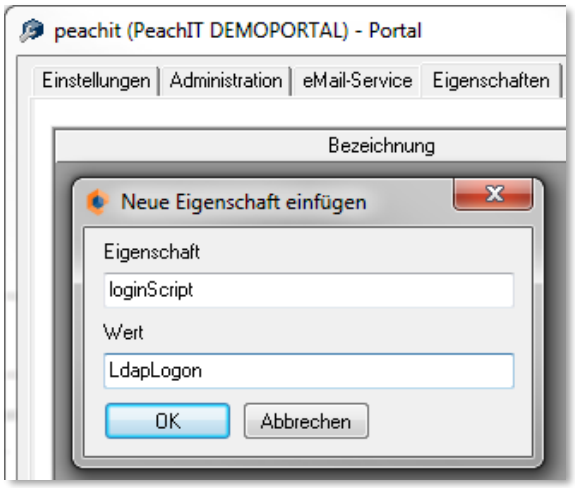

Abb. 10: Neue LDAP-Eigenschaft am Mandanten

3.3 Konfiguration mehrerer Domänen

Wenn Benutzer aus mehreren verschiedenen Domänen importiert werden sollen, so ist dies nicht über die Konfigurationsmappe möglich. Für jede Domäne muss ein eigenes Skript angelegt werden, das die Einstellungen aus Abschnitt 3.2 enthält. Hierzu kann auch der Inhalt des Skripts `LdapParamDomain` als Vorlage verwendet werden.

Wurde für jede Domäne ein Skript angelegt, müssen diese Skripte nun im Skript `LdapDomainInclude` eingetragen werden. Der Inhalt von `LdapDomainInclude` ist standardmäßig wie folgt:

```
ldapConfigContainer = new Array();


ldapConfigContainer[0] = {
        configurationName: "Default",
        loadDefaults: true,
        loadConfiguration: function(){
                #import "LdapParamDomain"
        }
}
```

Um eigene Domänen hinzuzufügen, muss lediglich der grün markierte Teil angepasst und /oder dupliziert werden. Eine Konfiguration mit drei Domänen könnte bspw. so aussehen:

```
ldapConfigContainer = new Array();


ldapConfigContainer[0] = {
        configurationName: "ActiveDirectory1",
        loadDefaults: true,
        loadConfiguration: function(){
```

```
                #import "LdapConfig_AD1"
        }
}

ldapConfigContainer[1] = {
        configurationName: "ActiveDirectory2",
        loadDefaults: true,
        loadConfiguration: function(){
                #import "LdapConfig_AD2"
        }
}

ldapConfigContainer[2] = {
        configurationName: "EDirectory",
        loadDefaults: true,
        loadConfiguration: function(){
                #import "LdapConfig_ED"
        }
}
```

Der Wert für *configurationName* vergibt einen Namen für diese Konfiguration, die später in den log Dateien angezeigt wird. Hinter dem *#import* Befehl muss der Skriptname des jeweiligen Konfigurationsskripts angegeben werden.

WICHTIG!

*Es muss unbedingt sichergestellt werden, dass die Benutzernamen der importierten Benutzer über **alle Domänen hinweg eindeutig** sind. Das heisst, ein Benutzer „schmidt“ darf nur in einer einzigen Domäne vorkommen. Kommt ein Benutzername mehrmals vor, kann dies zu schwerwiegenden Fehlern im Login-Prozess dieser Benutzer führen.*

3.4 Abschließende Schritte

Um die Verbindung zum LDAP Server zu testen, starten Sie Ihren Browser und öffnen Sie die Seite **http://server:8080/documents.html.** Versuchen sie sich mit einem Benutzer anzumelden, der aus dem LDAP importiert wurde.

Wenn der Import durch `LdapJob` oder der Login durch `LdapLogon` nicht korrekt funktioniert, gibt die Ausgabe im Serverfenster Aufschluss über das Problem.

4. Zugang ohne Synchronisation

Im Standardverhalten wird die Verwaltung von Benutzern und Gruppen nach der Einrichtung der Konfiguration vollständig an die LDAP-Struktur übertragen.

Bei der Synchronisation erfolgt daher nicht nur ein Import, sondern auch ein Abgleich der gefundenen Objekte. Werden in diesem Zusammenhang in **DOCUMENTS 5** Objekte gefunden, zu denen es keinen passenden Eintrag in der LDAP-Struktur gibt, verhält das System sich folgendemaßen:

- Wird in **DOCUMENTS 5** ein *Zugriffsprofil* gefunden, welches sich in der LDAP-Struktur nicht widerspiegelt, so wird dieses bei der Synchronisation entfernt.
- Wird ein *Benutzer* oder *Redakteur* in **DOCUMENTS 5** ohne passenden Eintrag im LDAP gefunden, so wird dieser gesperrt.

In bestimmten Fällen kann es durchaus sinnvoll oder erforderlich sein, dass ein solches Element ausschließlich in **DOCUMENTS 5** existiert. Die Synchronisation kann daher für diese Ausnahmen ausgeschaltet werden. Legen Sie dann für das Zugriffsprofil, den Redakteur oder Benutzer folgende Eigenschaft an:

```
noLdapCheck=true
```

Vor der Version 1.1.7 der LDAP-Kopplung lautet die Eigenschaft für Zugriffsprofile:

```
onlyInPortal=true
```

5. Zusätzliche Einstellungen

Folgende Einstellungen können verwendet werden, sind aber im Normalfall nicht erforderlich:

- `ldapConfig.LdapServerType` im Skript `LdapParamDomain`: Legt den Servertyp fest. Erlaubt sind:
    - ADS (Standard)
    - Novell
    - Domino
    - OpenLDAP
    - Samba
- `ldapConfig.tcpPort` im Skript `LdapParamDomain`: Der Standard LDAP – Port ist 389. Wenn ein anderer Port verwendet werden soll, kann dieser hier angegeben werden.
- `ldapConfig.searchScope` im Skript `LdapParamDomain`: Diese Eigenschaft verändert das Verhalten der Suche. Erlaubte Werte sind:
    - `0`: Sucht nur in der Basis
    - `1`: Sucht in der Basis und eine Ebene darunter
    - `2`: Sucht rekursiv in Basis und allen Ebenen darunter (Default)
- `ldapConfig.LdapUserLoginName` im Skript `LdapParamDomain`: Der Standard `sAMAccountName` wird von den meisten LDAP Servern verwendet. Domino und Samba Server benötigen hier hingegen den Wert `uid`.
- `ldapConfig.LdapUsersGroupArray` im Skript `LdapParamDomain`: Der Standard `memberOf` wird von den meisten LDAP Servern verwendet. Domino benötigt hier den Wert `dominoAccessGroups`.
- `ldapConfig.LdapDNAttributeName` im Skript `LdapParamDomain`: Die meisten LDAP Server benutzen den Standard `distinguishedName`. In manchen Fällen kommt es vor, dass keine DNs vorhanden sind. Der hier angegebene Wert muss ein Attribut des LDAP-Benutzers sein, welches einen eindeutigen Benutzernamen enthält (bspw. Die E-Mail Adresse).
- `ldapConfig.syncUsers=false` im Skript `LdapParamJob`: Schaltet die Synchronisierung der Benutzer ab.
- `ldapConfig.disableGroupCache=true` im Skript `LdapParamJob` oder `LdapParamLogin`: Schaltet den internen Caching-Mechanismus aus, der die Zugriffe auf die LDAP-Struktur reduziert.

6. Häufige Konfigurationsprobleme

- Wenn die Verbindung mit dem LDAP Server komplett fehlschlägt, liegt dies meistens daran, dass die Parameter `ldapConfig.LdapLogin`, `ldapConfig.LdapPassword` und/oder `ldapConfig.LdapHostnameK` falsch angegeben wurden.
- Als Benutzername muss unter `ldapConfig.LdapLogin` der vollständige *distinguishedName (DN)* des Benutzers angegeben werden.
- `ldapConfig.LdapPassword` muss das Passwort des Benutzers in Klartext enthalten.
- Es hängt von der jeweiligen Netzwerkstruktur ab, ob `ldapConfig.LdapHostname` als IP-Adresse, einfacher Hostname oder FQDN angegeben werden kann.
- Wenn die Verbindung zum LDAP Server erfolgreich ist, aber keine Benutzer oder Gruppen importiert werden (Debug-Ausgaben im Server-Fenster beachten!), liegt es wahrscheinlich daran, dass die Parameter `ldapConfig.LdapGroupDN` und/oder `ldapConfig.LdapUserDN` falsch angegeben wurden.
- Wenn die Gruppen korrekt importiert wurden, aber trotzdem keine Benutzer gefunden wurden (Debug-Ausgaben beachten), kann es sein, dass `ldapConfig.LdapSwitchingGroup` falsch angegeben wurde oder dass es keine Benutzer im LDAP gibt, die sowohl Mitglied der *SwitchingGroup* als auch in einer der OUs in `ldapConfig.LdapUserDN` zu finden sind.
- Wenn weiterhin keine Benutzer importiert werden, überprüfen Sie, ob der angegebene LDAP-Benutzer ausreichend Leserechte besitzt, um auf die wichtigen Strukturen im LDAP zugreifen zu können.
- Aufgrund von Restriktionen in *MS Active Directory* können auf diesem System aktuell nicht mehr als 1000 Gruppen pro OU importiert werden. Dies gilt auch für Benutzer. Im Gruppenmodus können auch mehr Benutzer importiert werden.
- Stellen Sie sicher, dass im **DOCUMENTS-Manager** ein korrekter *Job-Benutzer* angegeben wurde. Diese Einstellung kann im Menüpunkt *Documents -> Einstellungen -> Documents (Basis)* vorgenommen werden. Andernfalls kann es passieren, dass Benutzer und Gruppen zwar synchronisiert aber deren Attribute nicht korrekt übernommen werden.
- Stellen Sie sicher, dass der *Standard-Benutzer* unter *Documents -> Einstellungen -> Documents (Basis)* die Eigenschaft `noLdapCheck` *nicht* besitzt.
  Wenn diese Eigenschaft am *Standard-Benutzer* auf `true` gesetzt ist, wird diese an alle neu angelegten Benutzer vererbt. Eine Authentifizierung der Benutzer über LDAP erfolgt dann zwangsläufig nicht mehr.
- Für den Fall, dass Sie Sonderzeichen wie bspw. runde Klammern in DNs einstellen müssen, muss jedem Sonderzeichen ein „\“ (Backslash) vorangestellt werden.
- DNs von Benutzern und Gruppen dürfen keine „/“ und keine Umlaute enthalten, da es sonst zu diversen Problemen mit der Synchronisation kommen kann. Dies betrifft vor allem die Mitgliedschaft von Benutzern in Gruppen.
- Namen von Gruppen dürfen ebenfalls keine Umlaute enthalten, da diese in Zugriffsprofilen in **DOCUMENTS 5** ebenfalls nicht erlaubt sind.

7. Callback API

Die **Callback-API** stellt einige Umgebungsvariablen und Methoden bereit, mit deren Hilfe die Funktionalität der LDAP-Kopplung an vielen Stellen erweitert werden kann.

Das Auslieferungspaket enthält das Script `ldapCallbackFunctions`, welches bereits alle bisher vorhandenen Methoden enthält. Einige enthalten bereits sinnvollen Beispielcode, der als Referenz verwendet werden kann.

7.1 Verfügbare Umgebungsvariablen

- `ldapConfig` (Object):
  Globales Objekt, welches die Konfiguration der LDAP-Kopplung enthält.
- `lang` (String):
  Der zwei Zeichen lange Sprachcode der aktuell vom Benutzer eingestellten Sprache.
- `lngIndex` (Integer)
  Die Nummer der aktuell vom Benutzer gewählten Portalsprache (0-5).

7.2 Verfügbare Callback-Methoden

Die Methoden sind in der Reihenfolge ihrer Ausführung (während des Jobs und während des Logins) aufgelistet.

- `callbackConnectionError(string dcErrorMessage)`:
  Wird aufgerufen, wenn keine Verbindung zum LDAP Server aufgebaut werden kann. `dcErrorMessage` enthält die Fehlermeldung die vom Server zurückgegeben wurde.
- `callbackProfileSyncPre(string profileName)`:
  Die Funktion erlaubt es, den Profilnamen vor der Synchronisierung eines Zugriffsprofils zu manipulieren. Dies ist sinnvoll, wenn im LDAP bspw. ein Präfix für Gruppennamen verwendet wird, das in den Zugriffsprofilen entfernt werden soll.
- `callbackProfileCreatedPost(AccessProfile apObj, LDAPGroup ldapGroupObj)`:
  Wird ausgeführt, nachdem ein Zugriffsprofil synchronisiert wurde. Mit dieser Funktion können bspw. nachträglich noch zusätzliche Eigenschaften am Zugriffsprofil gesetzt werden.
- `callbackProfileFoundPost(AccessProfile apObj, LDAPGroup ldapGroupObj)`:
  Diese Funktion wird ausgeführt, nachdem ein Zugriffsprofil anhand einer LDAP Gruppe im **DOCUMENTS-Manager** gefunden wurde.
- `callbackUserHandleLogin(string login)`:
  Wird immer dann aufgerufen, wenn der Name eines LDAP-Benutzers aus dem LDAP gelesen wird. Für den Fall, dass bspw. E-Mail Adressen als eindeutige Identifizierung verwendet werden, kann diese Funktion dazu dienen, den Benutzernamen (vor dem @) aus der E-Mail Adresse zu extrahieren.

Wichtiger Hinweis: Wenn diese Funktion verwendet wird, ist die automatische Erstellung von Benutzern beim Login nicht mehr möglich. Es muss also immer zuerst der LDAP-Job gelaufen sein.

- `callbackUserSetUserAttributes(string login, SystemUser user, LdapUser ldapUser)`:
  Überschreibt das Standardverhalten zur Synchronisation der Attribute des Benutzers zwischen LDAP und **DOCUMENTS 5.**
- `callbackUserProfileSyncPre(string login, SystemUser user, LDAPUser ldapUser)`:
  Wird ausgeführt, bevor die Profile eines Benutzers mit dem LDAP synchronisiert werden.
- `callbackUserProfileSyncPost(string login, SystemUser user, LDAPUser ldapUser)`:
  Wird ausgeführt, nachdem die Profile eines Benutzers mit dem LDAP synchronisiert wurden. Dies kann bspw. verwendet werden, um dem Benutzer ein festes, LDAP unabhängiges, Zugriffsprofil zuzuweisen.
- `callbackUserDisablePost(string login)`:
  Wird ausgeführt, wenn ein Benutzer bei der Synchronisation gesperrt wurde.
- `callbackAfterJobSync()`:
  Wird nach erfolgreicher Synchronisation aufgerufen.
- `callbackNoLdapAuthRequired(String login)`:
  DWird aufgerufen, wenn sich ein Benutzer anmeldet, der nicht mit dem LDAP synchronisiert werden muss (`noLdapCheck=true`).
- `callbackSetSuperiorPost(SystemUser suObj, String supLogin)`:
  Wird ausgeführt, wenn ein Benutzer (`supLogin`) als Superior eines anderen Benutzers (`suObj`) eingetragen wird.
- `callbackUserLoginPost(String login)`:
  Wird aufgerufen, nachdem ein Benutzer erfolgreich gegen das LDAP authentifiziert und seine Eigenschaften synchronisiert wurden.
- `callbackDisableLdapConfig(currentFile)`:
  Wird aufgerufen, wenn die LDAP Verbindung deaktiviert wurde (sofern diese mithilfe des Mappentypen konfiguriert wurde). Die Auslieferung enthält bereits eine Implementierung, die alle LDAP-Benutzer sperrt, sobald die Verbindung deaktiviert wird.

8. Abbildungsverzeichnis