

UCS Domänenkonzept: Listener/Notifier-Mechanismus

Thema:	Der UCS-Replikationsmechanismus dient als Grundlage der domänenweiten Administration. In diesem Dokument werden die Funktionsweise und Bestandteile des Listener/Notifier-Mechanismus und Ansätze zur Fehleranalyse beschrieben.
Datum:	3. April 2011
Seitenzahl:	10
Versionsnummer:	8343
Autoren:	Univention GmbH feedback@univention.de

Inhaltsverzeichnis

1	Einleitung	3
2	Beteiligte Dienste	3
2.1	Univention Directory Manager	3
2.2	OpenLDAP-Server - slapd	4
2.3	Univention Directory Notifier	5
2.4	Univention Directory Listener	5
3	Funktionsweise	6
3.1	Voraussetzung - Beitritt zur UCS-Domäne	6
3.2	Informationsfluss zwischen den Diensten	6
3.3	Schema-Replikation	7
3.4	Syncrepl zur Anbindung von Nicht-UCS OpenLDAP-Servern	8
4	Fehleranalyse	8
4.1	Log-Datei des Univention Directory Listeners	8
4.2	Vergleich der Transaktions-IDs	8
4.3	Einspielen nicht replizierter Daten (failed.ldif)	9
4.4	Re-Initialisieren der Listener-Module	10

1 Einleitung

Univention Corporate Server ist eine der wenigen Linux-Distributionen, die auf einem Domänen-Konzept aufbauen. Dieses Domänen-Konzept ermöglicht unter anderem die zentrale Konfiguration und Administration von Ressourcen und Diensten, die von den verschiedenen Mitgliedern der Domäne bereitgestellt werden. Dabei wird der größte Teil der Administration einer UCS-Umgebung im Univention Directory Manager über ein Web-Frontend oder eine Kommandozeilen-Schnittstelle vorgenommen.

Alle Informationen, die in Univention Directory Manager verwaltet werden (z.B. Objekte für Benutzer, Gruppen und Rechner, Richtlinien, Konfigurationen für Dienste) werden im Verzeichnisdienst OpenLDAP gespeichert. Die Verteilung dieser Daten innerhalb der UCS-Umgebung erfolgt über den Listener/Notifier-Mechanismus, der als flexibler und erweiterbarer Ersatz für den früher in OpenLDAP enthaltenen Replikationsdienst *slurpd* entwickelt wurde. *slurpd* wurde mittlerweile auch in OpenLDAP durch ein neues Verfahren abgelöst.

Der Listener/Notifier-Mechanismus führt als Reaktion auf Veränderungen von Daten Programme auf Systemen der UCS-Umgebung aus. Diese Programme können wiederum lokale Veränderungen am System vornehmen, z.B. Konfigurationsdateien auf Grundlage der veränderten Daten neu schreiben oder Dienste neu starten. Wird zum Beispiel ein neuer Drucker in Betrieb genommen, legt der Administrator in Univention Directory Manager ein Drucker-Objekt an, in dem vorgegeben wird, um welches Modell mit welchem Treiber es sich handelt und auf welchem UCS-Server die Warteschlange angelegt wird. Über den Listener/Notifier-Mechanismus wird auf dem UCS-Server die Konfiguration des Druck-Dienstes *cups* erweitert und der Drucker ohne weitere Interaktion des Administrators aktiviert. Der Drucker kann umgehend von Clients verwendet werden.

2 Beteiligte Dienste

Der Listener/Notifier-Mechanismus ist ein verteilter Dienst. Univention Directory Manager dient zur Erfassung von Daten, der Administrator nimmt Veränderungen über die Frontends vor. Die Daten werden im Verzeichnisdienst OpenLDAP gespeichert. Die Veränderungen im Verzeichnisdienst werden vom zentralen Notifier-Dienst registriert. Die Listener-Dienste werden auf allen UCS-Systemen ausgeführt und fragen Veränderungen vom Notifier-Dienst ab. Über den Listener-Dienst werden lokale Anpassungen auf den Systemen vorgenommen.

2.1 Univention Directory Manager

Univention Directory Manager ist ein Bestandteil des UCS-Managementsystems und nur auf einem UCS-Domänencontroller Master verfügbar. Über diesen Dienst werden alle Einstellungen vorgenommen, die sich auf die gesamte Domäne beziehen. Neben Benutzern, Gruppen und Rechnern werden ebenfalls zentrale Dienste und Netzwerkeinstellungen verwaltet. Alle Daten werden dabei im lokalen LDAP-Verzeichnisdienst gespeichert.

Der Administrator kann Univention Directory Manager über zwei Frontends bedienen. Das Web-Frontend bietet neben einem LDAP-Browser über Wizards auch einen intuitiven, einheitlichen Zugriff auf Objekte. Zusätzlich können alle Funktionen, die das Web-Frontend unterstützt, auch über das Kommandozeilen-Interface `univention-directory-manager` verwendet werden, was beispielsweise in administrativen Shell-Skripten oder Migrations-Szenarien ein Vorteil sein kann. Weitergehende Informationen zum Univention Directory Manager sind im gleichnamigen Kapitel des UCS-Handbuchs zu finden.

2.2 OpenLDAP-Server - slapd

Der Verzeichnisdienst OpenLDAP wird von Univention Directory Manager als Datenspeicher eingesetzt. Verzeichnisdienste sind hierarchisch strukturierte Datenbanken, auf die über ein Netzwerkprotokoll zugegriffen wird. Manche Dienste - wie **Samba** oder der Mail-Dienst **Cyrus** - können unmittelbar einen LDAP-Verzeichnisdienst abfragen. Dienste ohne LDAP-Anbindung werden über den Listener/Notifier-Mechanismus indirekt an den Verzeichnisdienst angebunden.

In einem Verzeichnisdienst werden Daten, zusammengefasst zu Objekten, strukturiert abgelegt. Jedes Objekt hat einen eindeutigen Namen, den **Distinguished Name** (DN), der dem Pfad zum Objekt innerhalb des Verzeichnisses entspricht. Ein Objekt besteht aus Objektklassen und Attributen. Dabei sind Attribute Schlüssel-Wert Paare und Objektklassen geben vor, welche Attribute an einem Objekt verwendet werden können. Jedes Attribut kann bei der Suche im Verzeichnisdienst als Suchkriterium verwendet werden. Wird bei einer Suche ein Attribut angegeben, das an mehreren Objekten verwendet wird, werden alle diese Objekte in der Ergebnisliste ausgegeben.

In Schema-Definitionen wird festgelegt, welche Objektklassen existieren und welche Attribute darin enthalten sind - mit anderen Worten, welche Daten in einem Verzeichnisdienst gespeichert werden können. Schema-Definitionen liegen als Text-Dateien vor und werden über die Konfigurationsdatei des OpenLDAP-Servers eingebunden.

Die Verwendung von OpenLDAP ist eine der Grundlagen für die leichte Erweiterbarkeit des UCS-Managementsystems. Über das Einbinden zusätzlicher Schema-Definitionen können an Objekten weitere Attribute verwendet werden, die im Auslieferungszustand nicht zur Verfügung stehen. Durch die Erweiterung von Univention Directory Manager um benutzerdefinierte Attribute können diese Attribute konsistent zu bestehenden Attributen im Web-Frontend und in der Kommandozeilen-Schnittstelle verwaltet werden.

OpenLDAP unterstützt die Verteilung von Daten auf mehrere Server durch Replikation. In einer UCS-Umgebung werden schreibende Veränderungen nur auf dem OpenLDAP-Server des Domänencontroller Master vorgenommen. Alle OpenLDAP-Server auf weiteren Domänencontroller-Systemen werden über den Listener/Notifier-Mechanismus aktualisiert. Der LDAP-Server **slapd** schreibt dazu jede Veränderung im Verzeichnis als Transaktion in eine Log-Datei.

In UCS-Umgebungen wird nicht das OpenLDAP-Replikationsverfahren SyncRepl verwendet, sondern der Univention Listener/Notifier-Mechanismus. Die Eigenschaft des LDAP-Servers, Transaktionen in Log-Dateien zu schreiben, wird auch vom Listener/Notifier-Mechanismus verwendet. Die einzelnen Transaktionen werden dabei durch den Notifier registriert.

Das OpenLDAP-Replikationsverfahren SyncRepl lässt sich zusätzlich zum Listener/Notifier-Mechanismus zur Anbindung von OpenLDAP-Servern aktivieren, die nicht auf UCS-Systemen ausgeführt werden. Im Zusammenhang mit der Replikation von Verzeichnisdienst-Inhalten ermöglicht der Listener/Notifier-Mechanismus auch die Schema-Replikation - eine Eigenschaft, die OpenLDAP nicht besitzt.

UCS verwendet ein Berechtigungskonzept, das auf OpenLDAP basiert. In der Konfiguration des LDAP-Servers kann über Access Control Lists (ACLs) detailliert festgelegt werden, wie auf Objekte und einzelne Attribute zugegriffen werden kann. Auf Grundlage dieses Berechtigungskonzepts kann über den Listener/Notifier-Mechanismus die selektive Replikation realisiert werden. Dadurch besteht die Möglichkeit nur ausgewählte Daten auf die Standort-Server zu verteilen, bspw. nur Benutzer einer bestimmten Gruppe.

2.3 Univention Directory Notifier

Der Univention Directory Notifier nimmt die Rolle des Vermittlers zwischen OpenLDAP-Server und Univention Directory Listener ein. Er registriert alle Transaktionen des OpenLDAP-Servers und speichert in einer Log-Datei eine aufsteigende Transaktions-ID, den DN des veränderten Objekts und die Änderungsart (neu, verändert oder gelöscht).

Die aktiven Univention Directory Listener stehen in permanenter Verbindung zum Univention Directory Notifier. Registriert der Univention Directory Notifier eine neue Transaktions-ID, übermittelt er diese zusammen mit dem DN des Objekts und der Änderungsart. Da der Univention Directory Notifier Kenntnis über den Zustand der Univention Directory Listener-Dienste hat, kann er unterscheiden, welcher Univention Directory Listener informiert werden muss

Der Listener/Notifier-Mechanismus arbeitet transaktionsbasiert. Ein Univention Directory Listener, der mehrere Transaktionen verpasst hat - weil zum Beispiel der Rechner ausgeschaltet war - kann vom Univention Directory Notifier alle fehlenden Transaktionen abfragen. Sobald der Univention Directory Listener eine Verbindung zum Notifier aufgebaut hat, informiert der Univention Directory Listener den Univention Directory Notifier über seine höchste Transaktions-ID. Der Univention Directory Listener erhält vom Univention Directory Notifier die nächste Transaktions-ID, meldet diese dem Notifier und bekommt so lange vom Univention Directory Notifier die nächsthöhere Transaktions-ID, bis er auf dem neuesten Stand ist.

2.4 Univention Directory Listener

Mit jeder UCS-Systemrolle außer Thin Clients und Basissystemen wird der Univention Directory Listener installiert. Er hat die Aufgabe, nach Erhalt einer neuen Transaktion vom Univention Directory Notifier das Objekt dieser Transaktion aus dem LDAP-Server auszulesen. Im Gegensatz zum Univention Directory Notifier speichert der Univention Directory Listener nur die letzte verarbeitete Transaktions-ID. Dabei besitzt der Univention Directory Listener selbst keine Programmlogik, die auf Grundlage der Attribute eines Objektes Aktionen ausführen kann. Diesen Teil übernehmen die Listener-Module.

Listener-Module sind Erweiterungen des Univention Directory Listeners, die mit UCS-Komponenten installiert werden. Bei diesen Modulen handelt es sich um Programme, welche die Verarbeitung der veränderten Objekte aus dem LDAP-Server ausführen.

Der Aufbau aller Listener-Module ist identisch. Jedes Listener-Modul enthält einen Suchfilter, mit dem anhand der Attribute überprüft wird, ob das aktuelle Objekt behandelt werden soll. Die Programmlogik unterscheidet drei Fälle: das Objekt ist neu, das Objekt wurde verändert, das Objekt wurde gelöscht.

3 Funktionsweise

3.1 Voraussetzung - Beitritt zur UCS-Domäne

Bevor auf einem System der Listener-Dienst ausgeführt werden kann, muss das System der UCS-Domäne beitreten. Der Beitritt zur UCS-Domäne wird in der Regel zum Abschluss der Installation automatisch vorgenommen. Eine ausführliche Beschreibung dieses Vorgangs ist im Abschnitt Domänenbeitritt des UCS-Handbuchs zu finden.

3.2 Informationsfluss zwischen den Diensten

Die einzelnen Schritte im Listener/Notifier-Mechanismus sind in Abbildung 1 schematisch dargestellt. Beispielhaft soll der Ablauf anhand des Hinzufügens einer Samba-Freigabe in Univention Directory Manager verdeutlicht werden.

1. Der Administrator legt in Univention Directory Manager eine neue Samba-Freigabe an. Alle Einstellungen (Name der Freigabe, Server, Pfad...) werden in einem LDAP-Objekt gespeichert. Beim Anlegen des Objekts im LDAP-Server wird der DN des Objekts mit dem Typ der Änderung in die Replikations-Log-Datei geschrieben.
2. Der Notifier-Dienst liest den neuen Eintrag aus.
3. Ein aus Transaktions-ID, DN und dem Typ der Änderung bestehender neuer Eintrag wird in der Transaktions-Log-Datei angelegt.
4. Der Notifier-Dienst entfernt die registrierten Einträge aus der Replikations-Log-Datei des OpenLDAP-Servers. Der Notifier-Dienst übergibt die neue Transaktion einschließlich DN und Typ der Änderung an die angebundenen Listener-Dienste.
5. Der Listener-Dienst ruft das LDAP-Objekt mit allen Objektklassen und Attributen über eine LDAP-Suche vom OpenLDAP-Server ab.
6. Der Listener-Dienst trägt daraufhin die Transaktions-ID in seine Transaktions-Log-Datei ein.
7. Um festzustellen, für welche Listener-Module das neue Objekt relevant ist, wird der Such-Filter jedes Listener-Moduls gegen das neue Objekt getestet. Passt der Such-Filter eines Listener-Moduls auf das Objekt, wird das Listener-Modul ausgeführt.
8. Durch das Listener-Modul werden die erforderlichen Anpassungen am System vorgenommen.

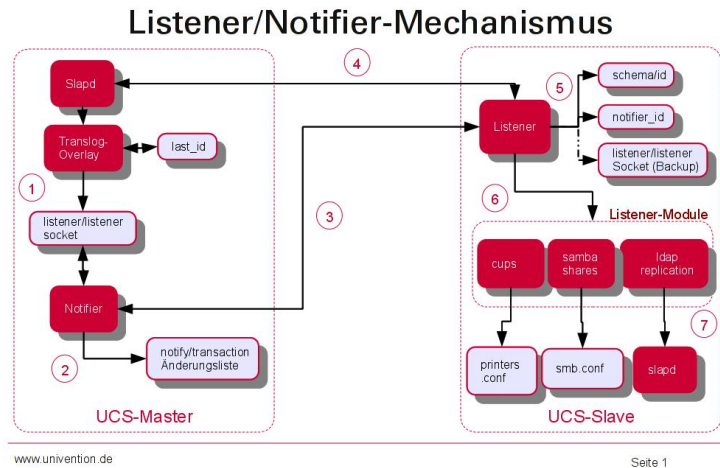


Abbildung 1: Schematische Darstellung Informationsfluss

3.3 Schema-Replikation

Über den Listener/Notifier-Mechanismus wird auch die Replikation der LDAP-Schemata automatisiert. Dies entbindet den Administrator von der Notwendigkeit, Schema-Änderungen auf allen OpenLDAP-Servern der Domäne manuell nachzupflegen. Mit der Ausführung der Schema-Replikation vor der Replikation von LDAP-Objekten wird sichergestellt, dass diese nicht aufgrund fehlender Objektklassen oder Attribute scheitert. Ähnlich der Replikation von LDAP-Objekten werden bei der Schema-Replikation aufsteigende IDs verwendet, um den Zustand der teilnehmenden Systeme abzubilden.

Auf dem Domänencontroller Master wird beim Starten des OpenLDAP-Servers über alle Verzeichnisse mit Schema-Definitionen eine Prüfsumme erzeugt. Diese Prüfsumme wird mit der letzten in der Datei `/var/lib/univention-ldap/schema/md5` gespeicherten Prüfsumme verglichen. Wurden neue Schema-Definitionen in die Konfiguration aufgenommen, stimmt sie nicht überein. In diesem Fall wird die aktuelle Schema-ID, die in der Datei `/var/lib/univention-ldap/schema/id/id` gespeichert ist, erhöht und die gespeicherte Prüfsumme aktualisiert.

Die eigentliche Replikation der Schema-Definitionen wird vom Univention Directory Listener initiiert. Vor jeder Abfrage einer neuen Transaktions-ID durch den Univention Directory Notifier wird dessen aktuelle Schema-ID abgefragt. Ist diese höher als die Schema-ID auf der Listener-Seite, wird über eine LDAP-Suche vom LDAP-Server des Notifier-Systems dessen aktuell verwendetes Subschema bezogen. Grundlage dieses Vorganges ist die Eigenschaft von OpenLDAP, alle über die Konfigurationsdatei eingebundenen Schema-Definitionen während des Startens einzulesen und in einem Bereich des Verzeichnisses für operative Informationen abzulegen.

Das ausgelesene Subschema wird auf dem Listener-System im LDIF-Format in die Datei `/var/lib/univention-ldap/schema.conf` geschrieben. Sie ist in der Konfigurationsdatei des OpenLDAP-Servers über eine **include**-Anweisung eingebunden. Nachdem die Datei **schema.conf** geschrieben wurde, wird die lokale Schema-ID erhöht und der lokale OpenLDAP-Server neu gestartet. Dabei werden die neuen Schema-Definitionen aus `schema.conf` aktiviert. Ist die Schema-Replikation mit diesem Schritt abgeschlossen, wird die Replikation der LDAP-Objekte fortgeführt.

3.4 Syncrepl zur Anbindung von Nicht-UCS OpenLDAP-Servern

Für die Anbindung von nicht auf UCS-Systemen installierten OpenLDAP-Servern an das UCS-Managementsystem kann parallel zum Notifier-Dienst der Syncrepl-Replikations-Dienst aktiviert werden. Dieser ist Bestandteil von OpenLDAP, registriert Veränderungen im lokalen Verzeichnisdienst und überträgt diese auf weitere OpenLDAP-Server.

Die Einrichtung ist in der Univention Supportdatenbank unter <http://sdb.univention.de/1120> beschrieben.

4 Fehleranalyse

4.1 Log-Datei des Univention Directory Listeners

Die Log-Datei des Univention Directory Listeners `/var/log/univention/listener.log` ist von zentraler Bedeutung bei der Fehleranalyse im Listener/Notifier-Mechanismus. Sowohl der Listener-Dienst selbst, als auch die Listener-Module schreiben Statusmeldungen in diese Datei. Diese beziehen sich überwiegend auf Starten und Stoppen des Dienstes, Verbindungen zum Notifier und Initialisierungen der Listener-Module. Von den Listener-Modulen werden Meldungen innerhalb der Programmlogik erzeugt. Jede Meldung ist in eine von fünf Kategorien eingeordnet. Die Kategorien sind **ERROR**, **WARN**, **NOTIFICATION**, **INFO** und **DEBUG**. Sie entsprechen jeweils einem Debug-Level, der über die Univention Configuration Registry-Variable `listener/debug/level` auf Werte von **0** (nur Meldungen der Kategorie **ERROR**) bis **4** (Meldungen aller Kategorien) eingestellt wird. Für die Fehleranalyse kann es hilfreich sein, den Debug-Level vorübergehend zu erhöhen. Nachdem der Debug-Level geändert wurde, muss der Univention Directory Listener neu gestartet werden.

4.2 Vergleich der Transaktions-IDs

Im Standard-Betrieb der Domänen-Replikation (keine hohe Last auf den Systemen, keine Störungen im Netzwerk) ist die Verzögerung zwischen der Änderung in Univention Directory Manager bis zur Änderung auf dem Listener-System kaum merkbar. Innerhalb einiger Sekunden

können mehrere Transaktionen vom Listener durchgeführt werden. Werden auf einem Listener-System Auffälligkeiten beobachtet, die mit dem Listener/Notifier-Mechanismus in Zusammenhang stehen könnten, kann der Vergleich der Transaktions-IDs von Listener- und Notifier-Dienst einen ersten Hinweis liefern.

Auf dem Domänencontroller Master werden die vom Notifier-Dienst registrierten Transaktionen in aufsteigender Reihenfolge in die Datei `/var/lib/univention-ldap/notify/transaction` geschrieben:

```
root@dcmaster:~# tail -1 /var/lib/univention-ldap/notify/transaction
836 cn=dcslave3,cn=dc,cn=computers,dc=firma,dc=de m
root@dcmaster:~#
```

Auf dem Listener-System wird die zuletzt vom Listener empfangene Transaktion in der Datei `/var/lib/univention-directory-listener/notifier_id` gespeichert:

```
root@dcslave1:~# cat /var/lib/univention-directory-listener/notifier_id
836
root@dcslave1:~#
```

Weichen die Transaktions-IDs voneinander ab, kann das Problem im Umfeld des Listeners gesucht werden. Es können sich in der der Log-Datei des Listener-Dienstes weitere auffällige Einträge finden, z.B. **'connection to notifier was closed'**. Über das Nagios-Plugin `check_univention_replication` können ebenso Replikationsauffälligkeiten sichtbar gemacht werden.

4.3 Einspielen nicht replizierter Daten (failed.ldif)

Die Replikation von Verzeichnisdienst-Inhalten erfolgt über den Listener/Notifier-Mechanismus. Auf den UCS-Systemrollen Domänencontroller Backup und Domänencontroller Slave wird mit dem Paket ***univention-directory-replication*** das Listener-Modul `replication.py` installiert. Alle Objekte werden über dieses Listener-Modul dem lokalen Verzeichnisdienst hinzugefügt. Sollte der lokale LDAP-Server nicht erreichbar sein, werden alle Objekte im LDIF-Format in eine Datei geschrieben, um die Änderungen, wenn der LDAP-Server wieder erreichbar ist, nachträglich einspielen zu können.

Ist der LDAP-Server für den Univention Directory Listener nicht erreichbar, wechselt er nach mehreren erfolglosen Versuchen in den LDIF-Mode. In der Log-Datei des Listeners (`/var/log/univention/listener.log`) findet sich ein Eintrag mit Datum und der Meldung ***going into LDIF mode***. Die Datei `/var/lib/univention-directory-replication/failed.ldif` wird angelegt und es werden alle folgenden LDAP-Objekte in diese Datei geschrieben. Auch wenn der lokale LDAP-Server während des Betriebs im LDIF-Modus wieder erreichbar sein sollte, werden Veränderungen weiterhin in die Datei `failed.ldif` geschrieben. Die Replikation kann nur manuell wieder in den normalen Betrieb überführt werden:

Dies kann entweder über den Neustart des LDAP-Servers,

```
/etc/init.d/slaped restart
```

oder mit dem folgenden Befehl erreicht werden:

```
univention-directory-replication-resync \  
/var/lib/univention-directory-replication/failed.ldif
```

Durch den Befehl wird vorübergehend der Listener-Dienst angehalten, um weitere Schreibvorgänge in die Datei `failed.ldif` zu verhindern. Die gespeicherten LDAP-Objekte werden dem LDAP-Server nacheinander hinzugefügt. War die Übernahme erfolgreich, wird die Datei `failed.ldif` gelöscht und der Listener-Dienst erneut gestartet.

Sollten einzelne Objekte z.B. bei ausgebliebener Schema-Replikation oder bei bereits existierenden Objekten nicht eingespielt werden können, werden diese wiederum in eine LDIF-Datei unterhalb des `/tmp`-Verzeichnisses geschrieben. In diese Datei werden auch Meldungen geschrieben, die Hinweise auf den Grund für die Ablehnung durch den LDAP-Server geben. Der Pfad zur Datei wird von `univention-directory-replication-resync` ausgegeben. Nach Prüfung der einzelnen gespeicherten Objekte und entsprechenden Korrekturen können die ausstehenden Objekte über das Kommando `ldapmodify` wieder eingespielt werden.

4.4 Re-Initialisieren der Listener-Module

Falls es zu Problemen bei der Abarbeitung eines Listener-Moduls gekommen ist, so besteht die Möglichkeit, das Listener-Modul neu zu initialisieren. Dabei werden alle Objekte, auf die der Filter des Listener-Modul passt, als neue Objekte übergeben.

Dem Befehl zum erneuten Initialisieren muss der Name des Listener-Moduls übergeben werden. Die Namen aller installierten Listener-Module sind im Verzeichnis `/var/lib/univention-directory-listener/handlers/system` zu finden.

Mit dem folgenden Befehl kann beispielsweise das Druckermodul neu initialisiert werden:

```
univention-directory-listener-ctrl resync cups-printers
```