

1.1. Einrichtung der Lernumgebung

Normalerweise ist ein Domino Server laut HCL Vorgaben auf einem Windows Server (oder einem der anderen möglichen Server-Betriebssystemen - z.B. Linux) zu installieren.

Da wir lediglich eine Lernumgebung implementieren, eignet sich auch Windows 10/11 Pro sehr gut. Ausgestattet mit einer halbwegs aktuellen CPU und mit 3-4 GByte RAM werden alle gezeigten Funktionen flüssig laufen.

Falls Sie auch bei sich eine Lernumgebung installieren möchten, benötigen Sie folgendes:

- **Windows 10/11 Pro**
(das müssen keine physischen PC's sein - eine virtuelle Maschine ist auch geeignet)

Einen Domino Server + Domino Administrator kann man gleichzeitig auf einer Windows Instanz installieren - falls es mehrere Domino Server werden sollen, gilt als Regel:

- 1 x Windows 10/11 Pro für jeden Domino Server

- **Notes Client (inkl. Administrator) und Domino Server Version 9.0.1.x bis 12.0.1**

Bevor jemand fragt: Notes und Domino sind kommerzielle Produkte der Firma HCL und können nicht »einfach so« irgendwo heruntergeladen werden.

Da Sie sich aber vermutlich als Mitarbeiter eines Unternehmens mit der Domino Administration beschäftigen (Notes/Domino wird kaum von Privatpersonen genutzt), sollte die Software in Ihrem Unternehmen verfügbar sein.

Hinweis

Um Funktionen wie in den Kapiteln [2. Arbeiten mit mehreren Domänen](#) auf Seite 11 oder [7. Domino Cluster](#) auf Seite 179 ausprobieren zu können, sind mindesten zwei Domino Server erforderlich.

Sprache des Betriebssystem und der Notes/Domino Software

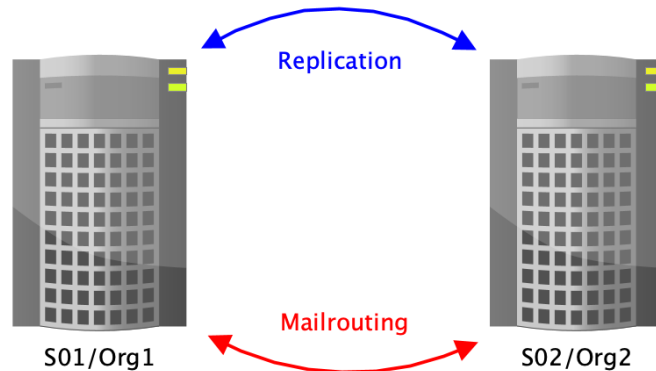
Auch in der deutschen Ausgabe dieses Buches wird sowohl das Windows Betriebssystem als auch die Notes/Domino Software in der Sprache **Englisch** genutzt. Dies hat primär folgende Gründe:

- Viele Administratoren bevorzugen mittlerweile bei Software die englische Sprache. Eine Suche nach Lösungsmöglichkeiten bei Problemen in englischer Sprache ist wesentlich erfolgreicher.
- Bei der Erstellung des Buches muss ich nicht alle Screenshots mehrfach erstellen.

2. Arbeiten mit mehreren Domänen

2.2. Kommunikation zwischen fremden Domänen

In diesem Kapitel wird gezeigt, wie man Domino Server aus unterschiedlichen Domänen/Organisationen miteinander verbindet. Da es sich um Domino Server handelt, geht es um die Replikation und das Mailrouting (NRPC Mailrouting, nicht SMTP).



Die Kommunikation zwischen Domino Servern aus verschiedenen Domänen/Organisationen unterscheidet sich grundsätzlich nicht von der Kommunikation, wie sie bei Domino Servern aus der gleichen Domäne/Organisation stattfindet.

Lediglich die Authentifizierung, also der »Handshake« bei der Verbindungsaufnahme der Domino Server, wird nicht »einfach so« funktionieren, denn die beteiligten Server-IDs stammen aus unterschiedlichen Organisationen (sind also Abkömmlinge unterschiedlicher cert.id's).

Wir erinnern uns:

Beim Einrichten des ersten Domino Servers wird ein Zertifikat (man könnte es als Stammzertifikat der Notes/Domino Umgebung bezeichnen) erstellt, welches in der Datei cert.id gespeichert und beim Registrieren von Servern oder Anwendern in deren ID Dateien übernommen wird.

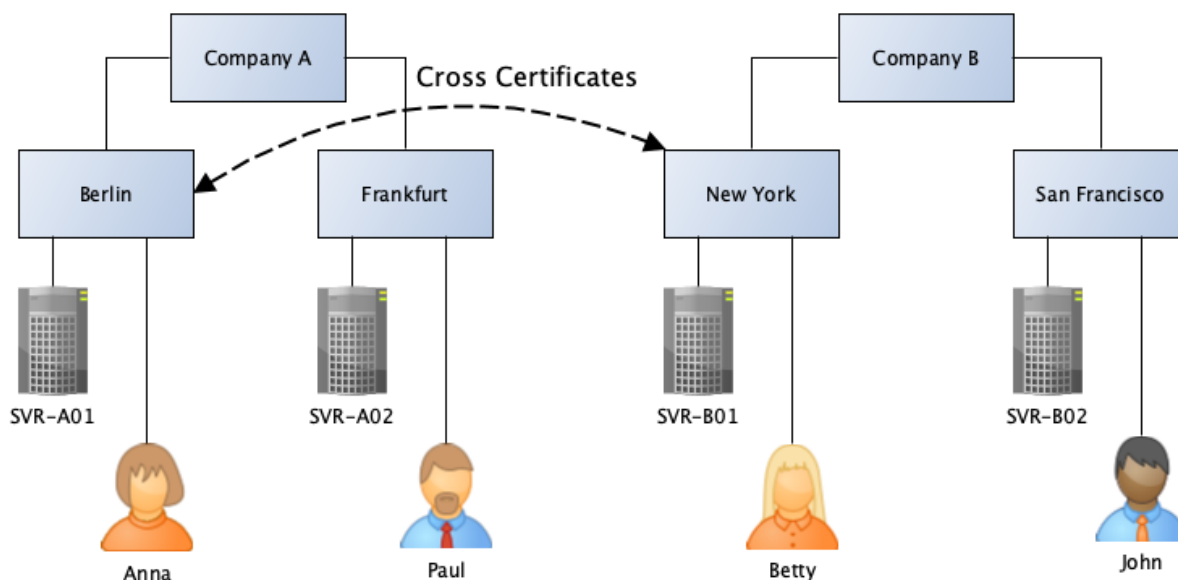
Erfolgt nun ein Verbindungsversuch zwischen zwei Domino Servern, so überprüft jeder der beteiligten Domino Server, ob die Gegenseite auch über dieses Zertifikat verfügt. Sofern dies der Fall ist, wird die nachfolgende Kommunikation problemlos stattfinden. Ansonsten kommt es auf der Domino Konsole (oder in der »log.nsf«) zu Fehlermeldungen und der Zugriff wird verweigert.

Domino Server und Notes Clients kommunizieren grundsätzlich nur untereinander, wenn die verwendeten Server- oder Benutzer-IDs die gleichen Stammzertifikate in sich tragen, also von der gleichen Datei cert.id (oder einer damit erstellten Abteilungs-ID) abstammen.

Um eine Kommunikation zwischen fremden Domino Servern und/oder Notes Clients zu ermöglichen, müssen auf beiden beteiligten Systemen sogenannte Gegenzertifikate erstellt werden.

Dies kann auf unterschiedlichen Ebenen (Organisation, Abteilung, Server- oder Personen-ID) erfolgen. Die Details hierzu werden im nächsten Kapitel vorgestellt.

2.3.2. Gegenzertifikate auf der Abteilungsebene (OU)



Hier erfolgt die Gegenzertifizierung auf der Ebene von **Abteilungen**.

Durch die Erstellung der Gegenzertifikate auf Abteilungsebene sind schon erheblich weniger Domino Server oder Notes Anwender in der Lage, auf Domino Server der Gegenseite zuzugreifen.

Am Standort Berlin sind nur für Anna und den Server SVR-A01 ein Zugriff auf den Domino Server SVR-B01 am Standort New York möglich. Betty und der Domino Server SVR-B01 am Standort New York erhalten einen Zugriff auf den Domino Server SVR-A01 in Berlin.

Die Anzahl der Kommunikationspartner wird somit gegenüber einer Gegenzertifizierung auf Organisationsebene erheblich reduziert. Trotzdem muss der zuständige Administrator zumindest mit Zugriffen von fremden Personen rechnen - deren Anzahl ist nicht ohne weiteres abschätzbar und somit nicht die auf den eigenen Domino Servern beanspruchten Ressourcen.

Ebenso müssen die ACLs aller Anwendungen sorgfältig gepflegt werden, damit die Mitarbeiter der fremden Unternehmung nicht unkontrolliert auf nicht für sie vorgesehene Informationen zugreifen können.

Fazit

Obgleich die Gegenzertifizierung auf Abteilungsebene im Gegensatz zur Organisationsebene die Anzahl der möglichen Kommunikationspartner reduziert, stellt sich doch die grundlegende Frage, ob Mitarbeiter mit Ihrem Notes Client überhaupt einen Zugriff auf die Gegenseite erhalten?

Die Domino Server tauschen via Replikation und Mailrouting alle erforderlichen Informationen aus und somit ist i.d.R. überhaupt kein individueller Zugriff für einzelne Mitarbeiter erforderlich.

2.4. Einrichtung der Gegenzertifizierung

In diesem Kapitel wird gezeigt, wie ein Gegenzertifikat schnell und komfortabel erstellt werden kann.

Hinweis

Zusätzlich zu der hier gezeigten Variante der Erstellung der Gegenzertifikate kann dies auch durch den Austausch von ID-Dateien (ggf. via Mailrouting) erfolgen. Diese Varianten sind umständlicher und aufwändiger. Deshalb werden sie im Buch nicht vorgestellt.

Nachfolgend wird ein Gegenzertifikat auf der Ebene von Server IDs erstellt.

2.4.1. Verbindungsaufbau zwischen Domino Servern ohne Gegenzertifikat

```

S01/Org1,Release 12.0.1 - HCL Domino Console
File Edit View Help
User: localAdmin
Platform: Windows/11/64 10.0
Server: S01/Org1,Release 12.0.1
Resume

trace S02/Org2
[0B34:0006-0DAC] Determining path to server S02/ORG2
[0B34:0006-0DAC] Available Ports: TCPIP
[0B34:0006-0DAC] Checking normal priority connection documents only...
[0B34:0006-0DAC] Allowing wild card connection documents...
[0B34:0006-0DAC] Checking for S02/ORG2 at last known address 'S02' on TCPIP...
[0B34:0006-0DAC] Using address '192.168.179.102' for S02/ORG2 on TCPIP
[0B34:0006-0DAC] Connected to server S02/ORG2
[0B34:0006-0DAC] Attempting Authenticated Connection

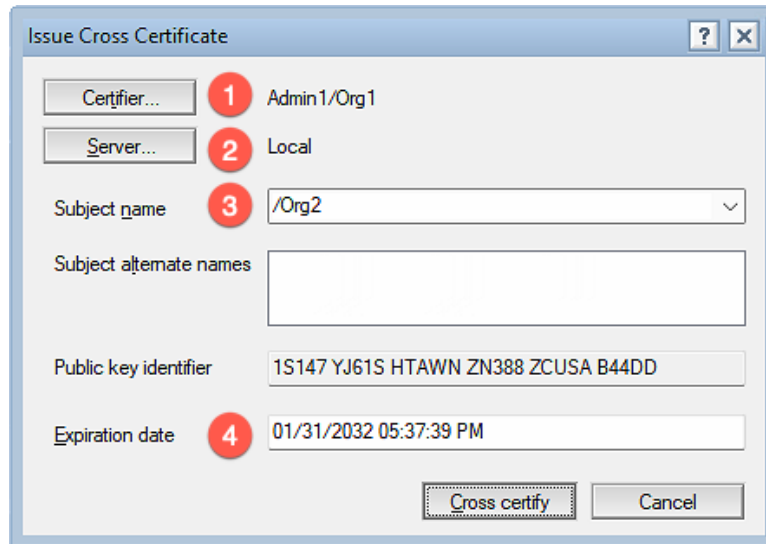
[0B34:0006-0DAC] 31.01.2022 16:58:31 Failed to authenticate with server S02/Org2: Your Address Book does not
contain any cross certificates capable of authenticating the server.
[0B34:0006-0DAC] 31.01.2022 16:58:31 Error connecting to server S02/ORG2: Your Address Book does not contain any
cross certificates capable of authenticating the server.
    
```

Eine Kommunikation zwischen Domino Servern aus **unterschiedlichen** Organisationen ist grundsätzlich nicht möglich. Versucht man, mit dem Konsolenbefehl »trace« eine Verbindung aufzubauen (eine Erreichbarkeit über das Netzwerk vorausgesetzt), so erscheinen die im Screenshot gezeigten Fehlermeldungen.

Meldung an der Domino Console	Erklärung
Attempting Authenticated Connection	Es wird versucht, eine Verbindung aufzubauen, hierbei überprüfen sich die beiden Partner (Authentifizierung).
Failed to authenticate with server S02/Org2: Your Address Book does not contain any cross certificates capable of authenticating the server.	Die Authentifizierung schlägt fehl, weil im Directory (»names.nsf«) kein Gegenzertifikat zur Bestätigung des fremden Domino Servers existiert.
Error connecting to server S02/Org2: Your Address Book does not contain any cross certificates capable of authenticating the server.	Es ist kein Verbindungsaufbau möglich, da im Directory (»names.nsf«) kein Gegenzertifikat zur Bestätigung des fremden Domino Servers existiert.

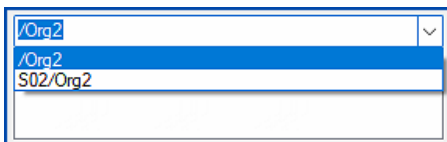
Dieses Gegenzertifikat würde bestätigen, dass die aktuell genutzte Anwender ID der Organisation »Org2« vertraut (der Notes Client akzeptiert Verbindungen zur Organisation »Org2«).

Für die Kommunikation der Domino Server ist ein solches, auf dem Notes Client lokal gespeichertes Gegenzertifikat nutzlos. Klicken Sie daher auf die Schaltfläche »Advanced«.



Das sind die Vorgaben in diesem Dialog. Hier **nicht** sofort auf die Schaltfläche »Cross certify« klicken! Diese Vorgaben sind **nicht** für die Erstellung des Gegenzertifikates für die Domino Server geeignet.

1. Über die Schaltfläche »Certifier...« wählen Sie aus, wer aus Ihrer Domino Umgebung der Gegenseite vertraut. Dies sollte die Server ID des eigenen Domino Servers sein.
2. Wo soll das Gegenzertifikat gespeichert werden? Lokal in der »names.nsf« des Notes Clients (nicht sinnvoll) oder in der »names.nsf« auf dem eigenen Server? Wählen Sie durch die Schaltfläche »Server...« einen Ihrer Domino Server aus.
3. Auf welcher Ebene vertrauen Sie der Gegenseite? Vorab ausgewählt ist die Organisationsebene, aber Sie können durch einen Klick auf den Auswahlpfeil rechts explizit den Domino Server der Gegenseite festlegen.



4. Wie lange soll das Gegenzertifikat gültig sein? Voreingestellt ist eine Gültigkeitsdauer von 10 Jahren. Da man später durch das Löschen des Gegenzertifikats die Verbindung zur Gegenseite jederzeit beenden kann, können hier problemlos längere Laufzeiten angegeben werden.

Fazit

Als Ergebnis der zuvor ausgeführten Schritte ist ein neues Gegenzertifikat im Domino Directory (»names.nsf«) auf dem angegebenen eigenen Domino Server gespeichert.

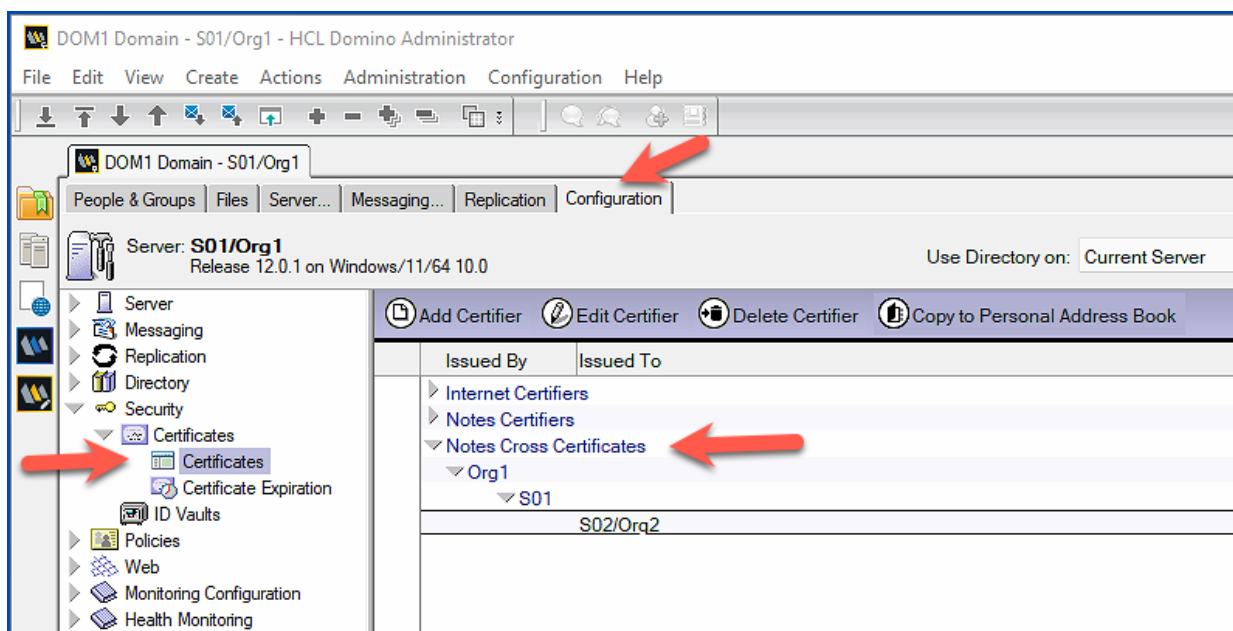
2.4.3. Gegenzertifikat im Domino Directory

Öffnen Sie im Domino Administrator den Tab »Configuration« und selektieren Sie links in der Navigation die Ansicht »Security« → »Certificates« → »Certificates«.

Hinweis

Sie finden die Ansicht »Certificates« auch auf dem Tab »People & Groups«.

Erweitern Sie die Kategorie »Notes Cross Certificates«.



Der Domino Server »S01/Org1« aus der Organisation »Org1« vertraut dem Domino Server »S02/Org2« aus der Organisation »Org2«. Dies wird in den beiden Spalten »Issued By« und »Issued To« angezeigt.

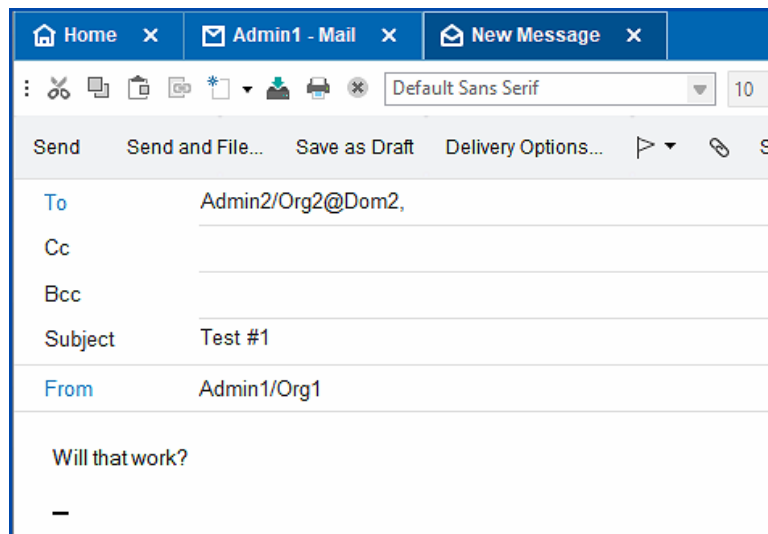
Damit sind alle erforderlichen Schritte in der Organisation »Org1« abgeschlossen.

Hinweis

Gegenzertifikate funktionieren nur, wenn Sie in **beiden** Notes/Domino Umgebungen existieren. Der zuständige Administrator der Gegenseite muss folglich ebenfalls diese Schritte ausführen.

2.5. Mailrouting zwischen fremden Domänen

Sobald Domino Server aus verschiedenen Domänen/Organisationen aufgrund der Gegenzertifikate kommunizieren, wird das NRPC Mailrouting trotzdem nicht funktionieren.

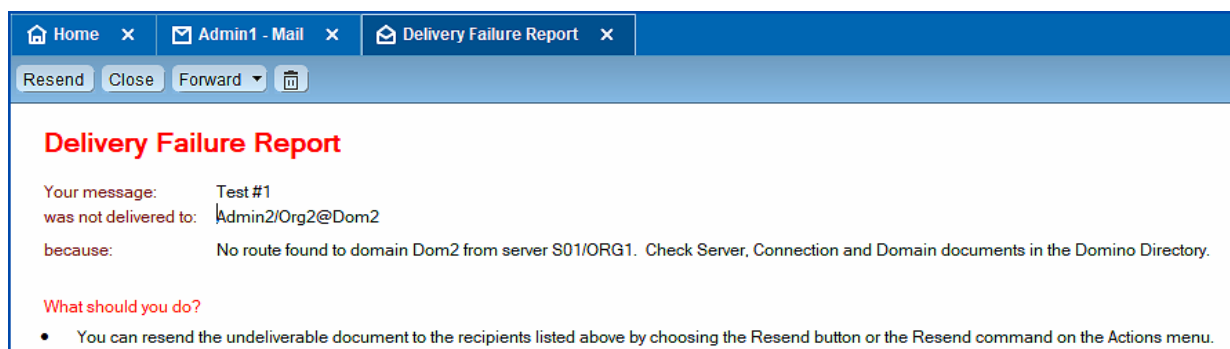


Eine Mail wird von »Admin1/Org1@Dom1« an die Person »Admin2/Org2@Dom2« gesendet.

Hinweis

Der Empfänger lässt sich **nicht** durch den Link »To« aus dem eigenen Domino Directory auswählen - dort existiert ja kein Personendokument für diese Person.

Im Kapitel 2.8. [Aktivierung fremder Directories](#) auf Seite 35 lernen Sie, wie man fremde Directories zur komfortablen Auswahl von Empfängern in die eigene Domino Umgebung einbindet.



Der Absender erhält diesen »Delivery Failure Report« - die Mail kann nicht zugestellt werden.

Der Hinweis »Check Server, Connection and Domain documents in the Domino Directory« ist korrekt - es fehlen im Moment die erforderlichen Verbindungsdokumente.

Server Connection: S01/Org1 to S02/Org2

Basics | Replication/Routing | **Schedule** | Comments | Administration

Scheduled Connection

Schedule:	Enabled ▾
Connect at times:	12:00 AM - 11:59 PM ▾ each day
Repeat interval of:	5 ▾ minutes
Days of week:	Sun, Mon, Tue, Wed, Thu, Fri, Sat ▾

Das Mailrouting sollte rund um die Uhr aktiviert sein.

Speichern Sie das neue Verbindungsdokument. Nachdem der Server die Einstellungen übernommen hat (siehe Kapitel [9.9. Warum werden Änderungen nicht sofort übernommen?](#) auf Seite [220](#)), werden Mails zur fremden Domäne geroutet.

An der Domino Konsole können Sie mit dem Befehl »show schedule« überprüfen, ob der Domino Server die Einstellungen aus dem Verbindungsdokument verwendet.

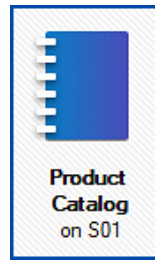
```
sh sch
[235C:0006-12B4] Scheduled   Type   Next schedule
[235C:0006-12B4] S02/Org2           Mail Routing           02.02.2022 14:05:00
```

2.5.2. Funktionsprüfung durch Mails

Senden Sie eine weitere Mail an einen Empfänger in der fremden Notes/Domino Domäne.

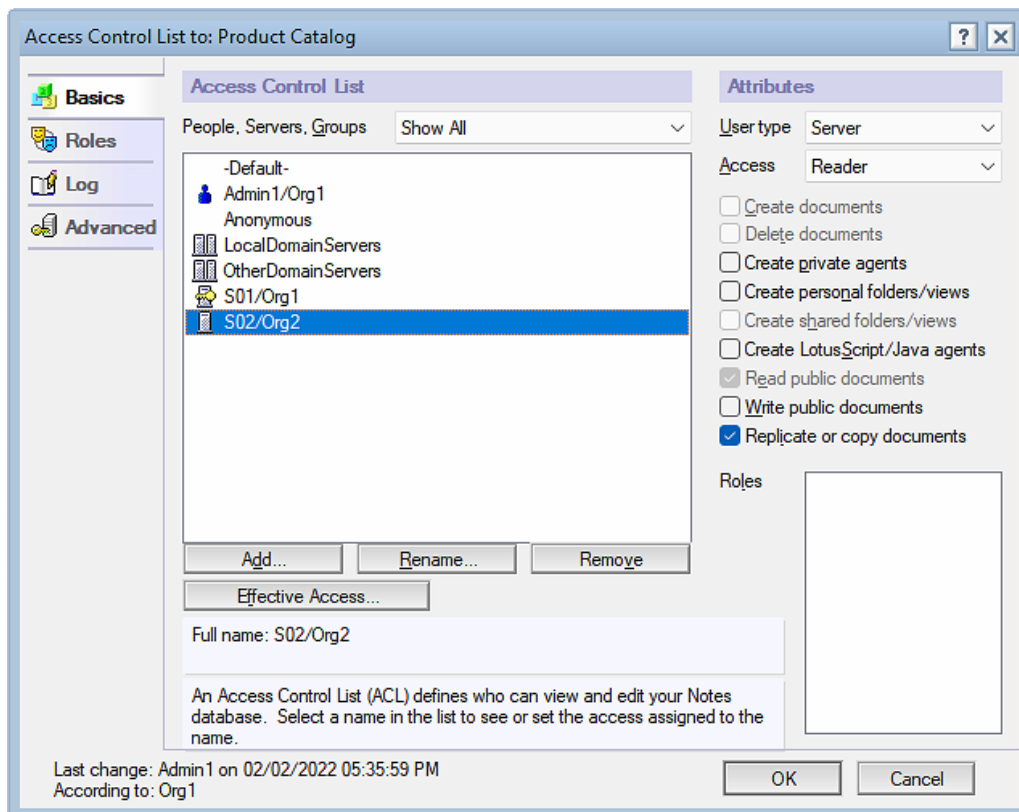
Sofern alle Einstellungen im Verbindungsdokument korrekt sind und der Domino Server diese übernommen hat, wird die Mail ohne Probleme zugestellt.

```
[2110:000C-0E6C] 02.02.2022 14:19:19 Router: Transferring mail to S02/ORG2 via Notes
[2110:000C-0E6C] 02.02.2022 14:19:19 Router: Transferred 1 messages to S02/ORG2 via Notes
[2110:0006-1F2C] 02.02.2022 14:19:20 Router: Message 00287519 transferred to S02/ORG2 for Admin2/Org2@Dom2 via Notes
```



Wir haben einen (fiktiven) Produkt Katalog, welchen wir mit einer Partnerfirma replizieren möchten.

Beispiel 1: Weitergabe von Informationen

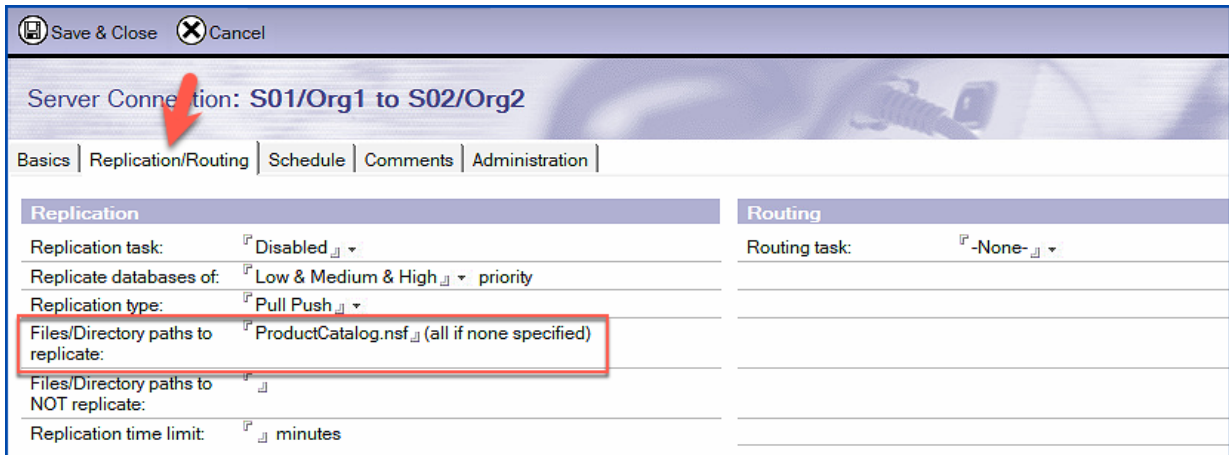


Der fremde Domino Server »S02/Org2« erhält die ACL Ebene »Reader«. Damit kann der Domino Server der Gegenseite alle Informationen aus unserer Anwendung zu sich replizieren, aber keine neuen Dokumente, Änderungen oder Löschungen an unsere Anwendung weitergeben.

Hinweis
 Alternativ zum Servernamen »S02/Org2« könnte man die vordefinierte Gruppe »OtherDomainServers« verwenden (»S02/Org2« muss dann Mitglied dieser Gruppe sein).
 Ich persönlich bevorzuge Einträge mit dem Servernamen. So sieht man auf einen Blick, welche fremden Domino Server mit welcher Ebene zugreifen - das ist aber sicher eine Geschmacksfrage.

Auf dem Tab »Basics« werden der Quell- und Zielserver sowie die Quell- und Zieldomäne benannt.

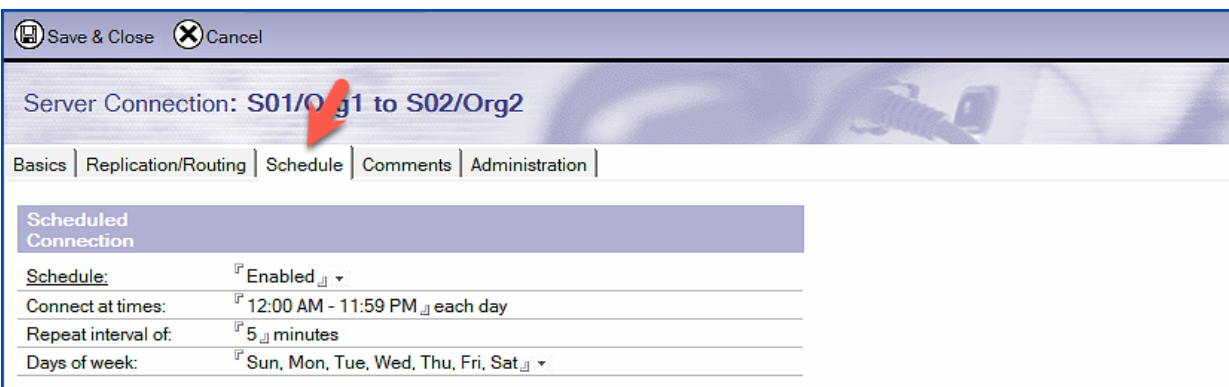
Tab Replication/Routing



Das Mailrouting ist auf dem Tab »Replication/Routing« deaktiviert.

Wichtig
 Geben Sie im Feld »Files/Directory paths to replicate« unbedingt die relevanten Anwendungen an!
 Wenn Sie das Feld leer lassen, werden alle Anwendungen und **Templates** repliziert. HCL liefert die Templates weltweit mit den gleichen Replik IDs aus. Falls auf dem fremden Domino Server modifizierte Templates existieren, könnten sich diese Änderungen in Ihren Templates wiederfinden. Verlassen Sie sich nicht darauf, dass die ACLs der Templates so eingestellt sind, dass dies nicht passiert!

Tab Schedule



```
[0A90:0002-0FE0] 02.02.2022 19:26:38 Starting replication with server S02/Org2
[0A90:0002-0FE0] 02.02.2022 19:26:38 Access control is set in S02/Org2 ProductCatalog.nsf to not replicate forms or
views from ProductCatalog.nsf
[0A90:0002-0FE0] 02.02.2022 19:26:38 Replicator added 1 document(s) to ProductCatalog.nsf from S02/Org2
ProductCatalog.nsf
[0A90:0002-0FE0] 02.02.2022 19:26:38 Finished replication with server S02/Org2
```

Die Replikation kann erfolgreich durchgeführt werden.

2.7.2. Domänendokument für benachbarte Domänen

Tab **Basics**

Domain Dom2

Basics | Restrictions | Calendar Information | Comments | Administration

Basics

Domain type: 1

Adjacent domain name: 2

Domain description: 3

Auf dem Tab »Basics« werden die folgenden Einstellungen festgelegt.

1. Im Feld »Domain type« wählen Sie die Option »Adjacent Domain«.
2. Im Feld »Adjacent domain name« geben Sie den Namen der benachbarten Domäne ein.
3. Die Angabe im Feld »Domain description« ist optional und beschreibt die benachbarte Domäne allgemein.

Tab **Restrictions**

Domain Dom2

Basics | Restrictions | Calendar Information | Comments | Administration

Restrictions

Allow mail only from domains: 1

Deny mail from domains: 2

Durch die Felder auf dem Tab »Restrictions« steuern Sie, wer Mails an die benachbarte Domain (in unserem Beispiel »Dom2«) senden darf.

Hinweis

Wir werden die Details erst im folgenden Kapitel genauer besprechen, aber grundsätzlich können Mails durch eine benachbarte Domäne zu einer anderen, nicht benachbarten Domäne geroutet werden. Damit die Domäne »in der Mitte« dies erlauben oder verbieten kann, gibt es diese beiden Felder.

1. Im Feld »Allow mail only from domains« legen Sie fest, welche anderen Domänen zu der auf dem Register »Basics« benannten Domäne Nachrichten durch die eigene Domäne routen dürfen. Die hier eingetragenen Domänen erhalten dafür eine Erlaubnis. Bleibt das Feld leer, gibt es keine Einschränkung.
2. Das Feld »Deny mail from domains« steuert, welche anderen Domänen keine Nachrichten zu der auf dem Register »Basics« angegebene Domäne senden dürfen. Bleibt das Feld leer, gibt es keine Einschränkung.

Die Mailadresse einer Mail, welche von einem Sender aus Domäne »Dom1« an einen Empfänger in Domäne »Dom3« gesendet wird, muss in folgender Form aufgebaut sein:

Admin3/Org3@Dom3@**Dom2**

Eine solche Notes Mailadresse sieht ungewöhnlich aus. Sie funktioniert aber trotzdem, da der Router eines Domino Servers die Mailadresse von rechts beginnend auswertet.

Der Router auf dem Domino Server der Domäne »Dom1« sieht, dass die Mail zunächst an »Dom2« gesendet werden soll. Da Verbindungsdokumente zwischen Domäne »Dom1« und »Dom2« existieren, wird die Mail erfolgreich zur Domäne »Dom2« geroutet.

Der Domino Server in Domäne »Dom2« erhält die Mail und betrachtet die Mailadresse abzüglich der letzten Domäne (@Dom2) und versucht die Mail an den Empfänger »Admin3/Org3@Dom3« zu routen. Da zwischen Domäne »Dom2« und »Dom3« ebenfalls geeignete Verbindungsdokumente existieren, wird die Nachricht an die Zieldomäne weitergegeben.

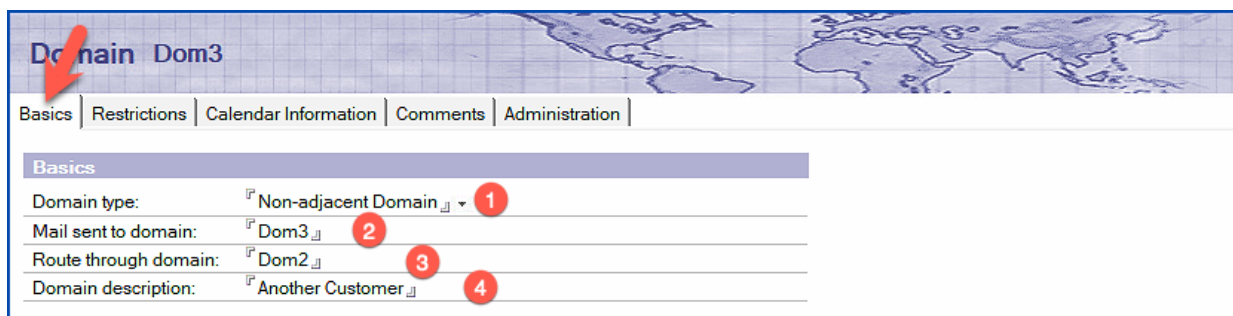
Eine Adressierung von Mails mit der Angabe von mehreren Domino Domänen ist den Anwendern nicht zumutbar, daher werden nicht benachbarte Domänenendokumente eingesetzt, welche die Adressierung von Mails mit nur einer Domäne ermöglichen.

Hinweis

Im folgenden Beispiel wird davon ausgegangen, dass wir ein Domänenendokument in der Domäne »Dom1« erstellen.

2.7.4. Domänenendokument für nicht benachbarte Domänen

Tab **Basics**



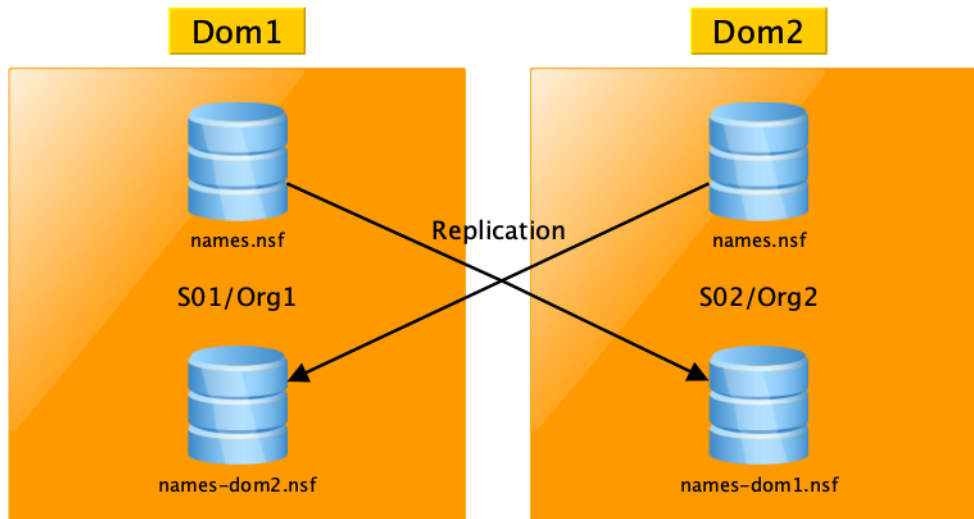
Auf dem Tab »Basics« legen Sie die folgenden Optionen fest:

1. Im Feld »Domain type« wählen Sie die Option »Non-adjacent Domain«.
2. An diese Domäne werden Mails gesendet. Dies ist die Domäne (nicht benachbart), zu der keine direkte Verbindung besteht.
3. Über diese Domäne werden die Mails geroutet.
4. Die Angabe im Feld »Domain description« ist optional.

2.8. Aktivierung fremder Directories

Für Anwender ist es beim Erstellen von Mails umständlich, wenn Sie Empfänger nicht per Klick aus einem Domino Directory (»names.nsf«) auswählen oder die Schnelladressierung verwenden können. Daher bietet es sich an, fremde Directories in die eigene Notes/Domino Umgebung einzubinden.

2.8.1. Replikation

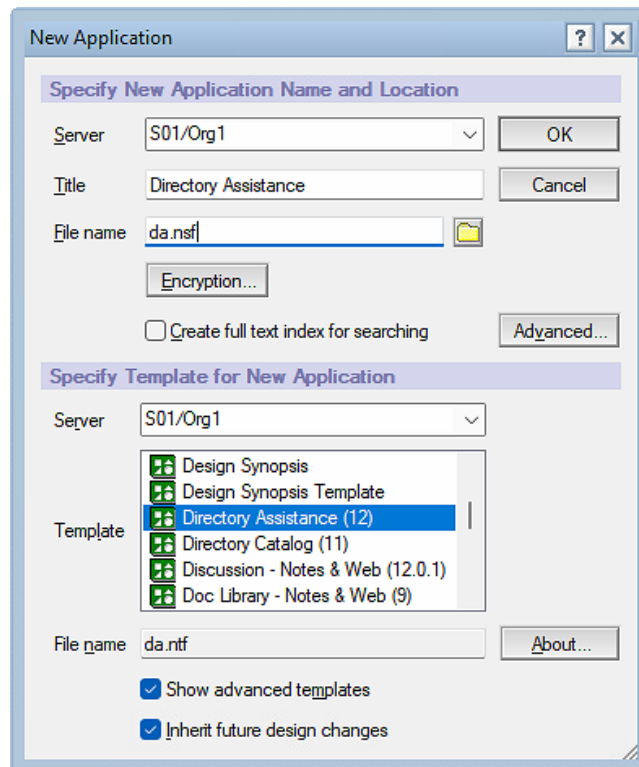


Im Beispiel gibt »Dom1« ihr Directory als Replik an »Dom2« und erhält im Gegenzug das Directory von »Dom2« als Replik.

Es bietet sich an, das jeweils fremde Directory entsprechend zu benennen. So könnte »Dom1« das fremde Directory als »names-dom2.nsf« auf den eigenen Domino Servern speichern. Es gibt keine Verwechslungen und die Zuordnung ist eindeutig.

Wichtig

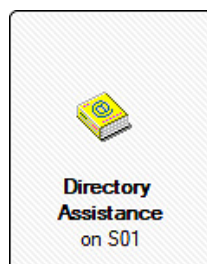
- **Replikation**
Die Inhalte der Repliken müssen auf dem aktuellen Stand gehalten werden. Vergessen Sie daher nicht, das fremde Directory (bei »Dom1« z.B. »names-dom2.nsf«) in das für die Replikation mit der Gegenseite erstellte Verbindungsdokument aufzunehmen.
- **ACL Einstellungen**
Die Gegenseite sollte auf das eigene Directory die Ebene »Reader« erhalten - so werden im eigenen Directory unerwünschte Änderungen verhindert. Für das Directory, welches man von der Gegenseite erhalten hat, sollte der fremde Domino Server einen »Editor« Zugriff erhalten. Hierdurch werden alle Änderungen von Dokumenten repliziert. Replikation von Designänderungen und ACL Änderungen sind damit ausgeschlossen.



Erstellen Sie zunächst die neue Anwendung »Directory Assistance« mit den im Screenshot angegebenen Parametern und wählen Sie die korrekte Schablone aus.

Hinweis

- Der Titel und Dateiname sind frei wählbar. Die Anwendung wird mit dem vergebenen Dateinamen im Serverdokument eingetragen.
- Damit Ihnen das Template angezeigt wird, müssen Sie unten im Dialog die Option »Show advanced templates« aktivieren.



Da der Titel und Dateiname der Anwendung frei wählbar ist, muss die Anwendung »Directory Assistance« dem Domino Server im Serverdokument bekannt gemacht werden.

Tab Basics

DIRECTORY ASSISTANCE

Basics | Naming Contexts (Rules) | Domino

Basics

Domain type: 1 Notes

Domain name: 2 Dom2

Company name: 3 Dom2 Inc.

Search order: 4 1

Make this domain available to: 5 Notes Clients & Internet Authentication/Authorization
6 LDAP Clients

Group authorization: 6 No

Enabled: 7 Yes

Auf dem Tab »Basics« existieren die folgenden Felder:

1. Domain type

Wählen Sie aus, ob es sich bei dem fremden Directory um ein Notes/Domino oder um ein LDAP Directory handelt.

2. Domain name

Der Name der fremden Domäne (im Beispiel: »Dom2«).

3. Company name

Der Name der Firma, zu dem das fremde Directory gehört (im Beispiel »Dom2 Inc.«).

4. Search order

Für den Fall, dass man weitere fremde Directories nutzt, wird hier die Suchreihenfolge festgelegt. Der Startwert ist »1«.

5. Make this domain available to

Die Option »LDAP Clients« ist nur erforderlich, wenn der eigene Domino Server als LDAP Server genutzt wird und Informationen aus dem fremden Directory für LDAP-Abfragen zur Verfügung stehen sollen.

6. Group authorization

Sofern gewünscht, können Gruppen im fremden Directory zur Zugriffssteuerung von Notes Clients in ACLs oder für die Zugriffssteuerung bei Nutzung des HTTP-Dienstes genutzt werden.

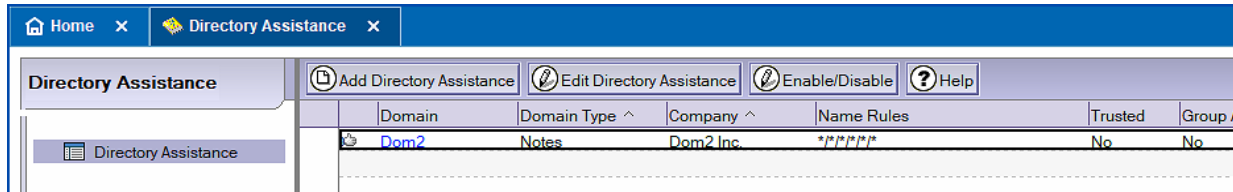
7. Enabled

Falls das fremde Directory temporär nicht zur Verfügung stehen soll, ändern Sie diese Option auf »No«.

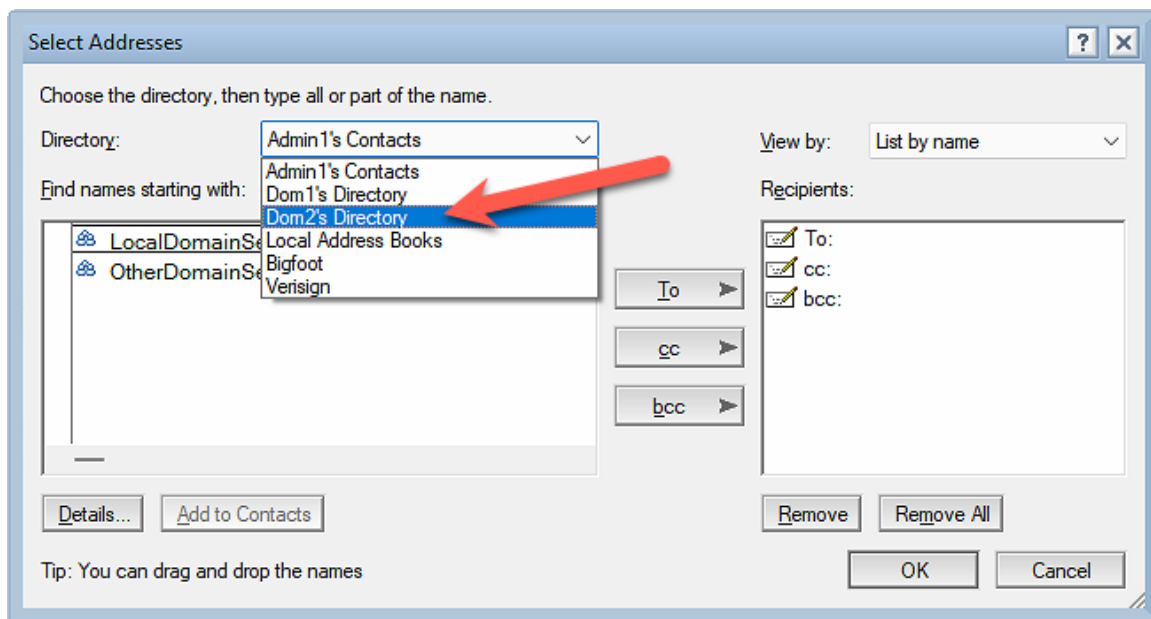
Auf dem letzten Tab »Domino« werden entweder Links² zum fremden Directory (Feld »Applications Links«) eingefügt, oder bis zu 5 Repliken des fremden Directories namentlich eingetragen.

Durch die Verwendung mehrerer Links oder die Angabe von bis zu 5 Repliken kann der Domino Server bei Problemen mit einem fremden Directory auf eine andere Replik umschalten.

Speichern und schließen Sie das Dokument.



Die »Directory Assistance« für die Domäne »Dom2« ist nun aktiv. Überprüfen Sie im Notes Client, ob dieses Directory bei der Adressierung von Empfängern für neue Mails zur Auswahl angeboten wird.



Hinweis

Mit hoher Wahrscheinlichkeit ist für den Domino Server und den Notes Client (inkl. Domino Administrator und Domino Designer) ein Neustart erforderlich.

² Es handelt sich um spezifische Links (Notes DocLink, NDL) zu Anwendungen, nicht um Internet-Links.

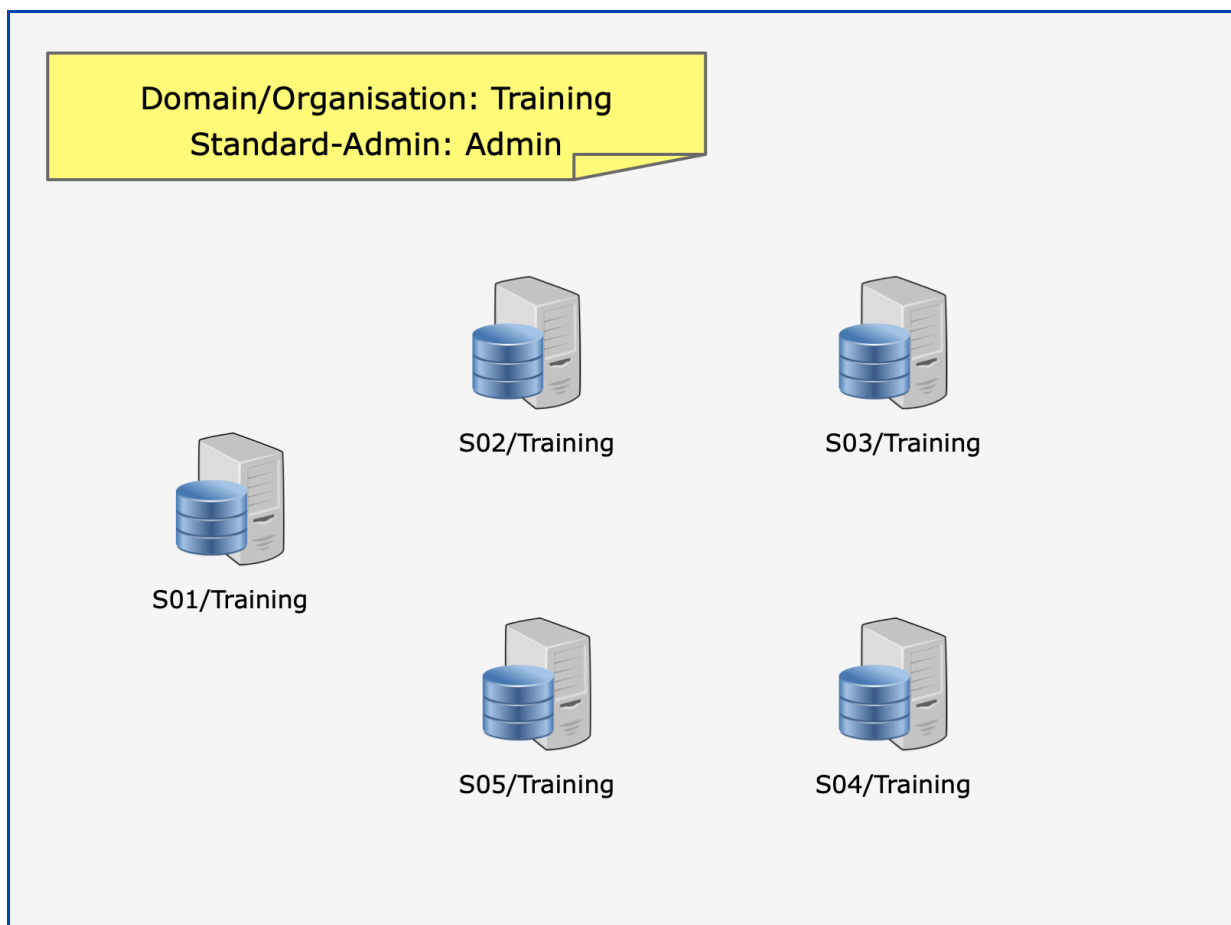
2.10. Lernumgebung für alle weiteren Kapitel in diesem Buch

Um in folgenden Kapiteln den »Domino Cluster« oder »ID Vault« (diese funktionieren nicht über Domänen/Organisationen hinweg) ausprobieren zu können, müssen wir die aktuelle Lernumgebung austauschen.

Sofern Sie der Empfehlung im Kapitel [2.1. Lernumgebung für Kapitel zu diesem Thema](#) auf Seite [12](#) gefolgt sind und ein Backup der Installationsdateien erstellt haben, müssen Sie die folgenden Schritte ausführen:

- Beenden Sie den Domino Server (zusätzlich den Dienst in Windows) und alle Notes Clients.
- Löschen Sie (oder benennen die Ordner um) die Installationsordner für den Domino Server und Notes Client (in meinem Fall ist das der Ordner »D:\HCL«).
- Kopieren Sie die Ordner aus dem Backup zurück an die gleiche Position im Dateisystem.
- Passen Sie die Datei »hosts« entsprechend den neuen Namen an.
- Führen Sie das Setup für die Domino Server aus und nehmen Sie die Notes Clients in Betrieb.

Die folgenden Namen sind geeignet:



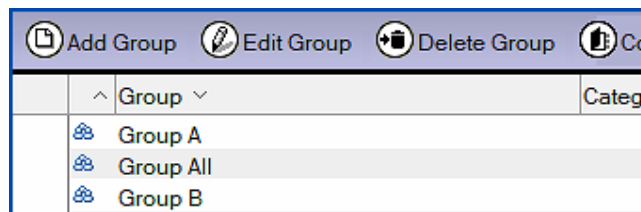
Die Anzahl der Domino Server ist frei wählbar - es sind mindestens **2** für die Lernumgebung erforderlich.

3.1. Auflösung von verschachtelten Gruppen

Gruppen dürfen ineinander verschachtelt werden. Nutzt man dies mit vielen Gruppen über mehrere Ebenen, verliert man leicht den Überblick.

Die Frage, in welchen Gruppen ein Anwender enthalten ist (direkt oder verschachtelt), lässt sich kaum mehr beantworten.

Nehmen wir an, es gibt folgende Konstellation.

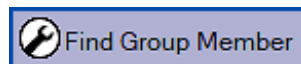


Aufbau der Gruppen:

Name	Mitglied(er)	Anmerkung
Group A	Admin/Training	
Group B	Betty Jones/Training	
Group All	Group A Group B	Verschachtelung

In welchen Gruppen ist »Betty Jones/Training« direkt oder indirekt Mitglied?

Ein Suche im Directory (Menü »View« → »Search This View«) findet nur Gruppen, in denen die Person direkt eingetragen ist.



Auch eine Suche über Aktion »Find Group Member« (oben in der Aktionsleiste) liefert nur direkte Mitgliedschaften (hier ist zu beachten, das der Vor- **und** Nachname verwendet werden muss - ansonsten gibt es überhaupt keine Treffer).

Lösung: Selektieren Sie rechts das Tool »Groups« → »Manage...«.

Dieses Tool dient grundsätzlich der Verwaltung von Gruppen, kann aber auch Mitgliedschaften über alle Ebenen der Verschachtelung auflösen.

3.2. Service generiert Out-of-Office Meldungen

In älteren Notes/Domino Versionen wurden Out-of-Office Meldungen durch einen Agenten, welcher im Postfach der Anwender gespeichert ist, generiert.

Da der Zeitplan für die Ausführung dieses Agenten auf ein Intervall von mehreren Stunden (Vorgabe) eingestellt war, konnte man nicht von einer zeitnahen Benachrichtigung des Absenders einer Mail sprechen. Zudem war die minimal einstellbare Zeitspanne für eine Abwesenheit auf einen Tag festgelegt.

Seit Notes/Domino Version 8.x ist die Generierung der Abwesenheitsnachrichten durch einen Service (Mailrouter) möglich. Es ergeben sich folgende Vorteile:

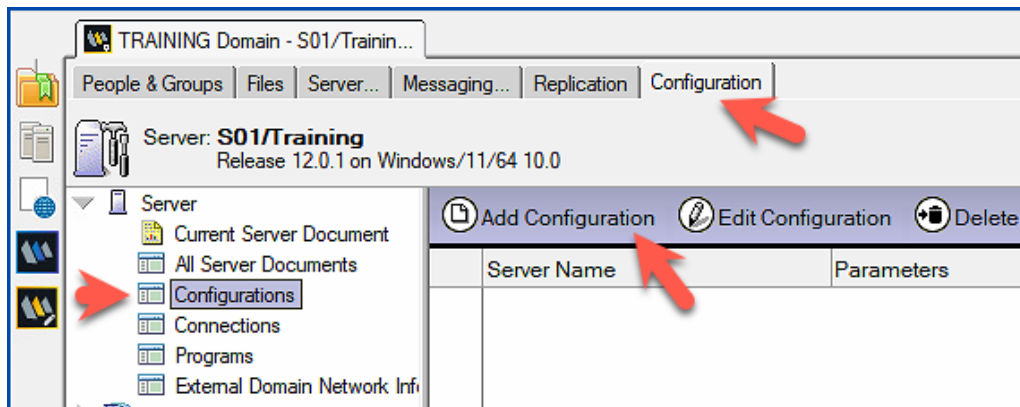
- Out-of-Office Meldungen werden in Echtzeit, also unmittelbar nach Eingang einer neuen Mail verschickt.
- Die minimal einstellbare Zeitspanne für die Abwesenheit beträgt 1 Stunde.

Hinweis

Die Nutzung des Out-of-Office Service ist optional und nach der Installation einer neuen Notes/Domino Umgebung nicht automatisch aktiviert.

3.2.1. Aktivierung im Konfigurationsdokument

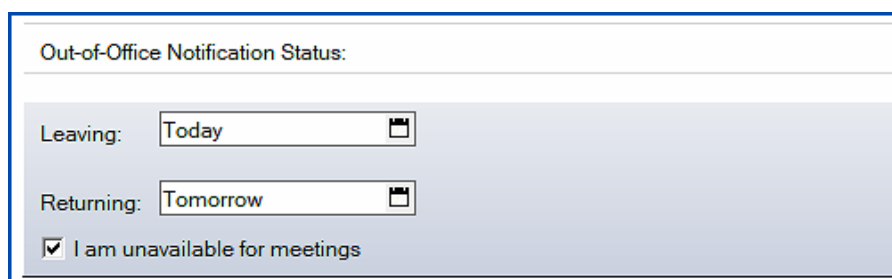
Öffnen Sie im Domino Administrator der Tab »Configuration« und selektieren Sie links die Ansicht »Configurations«.



Klicken Sie auf die Aktion »Add Configuration« (oder öffnen Sie eine bestehende Konfiguration, sofern verfügbar).

3.2.2. Geänderte Einstellmöglichkeiten beim Anwender

Wenn ein Anwender in seinem Postfach die Out-of-Office Einstellungen festlegt, sieht er grundsätzlich folgende Einstellmöglichkeiten:



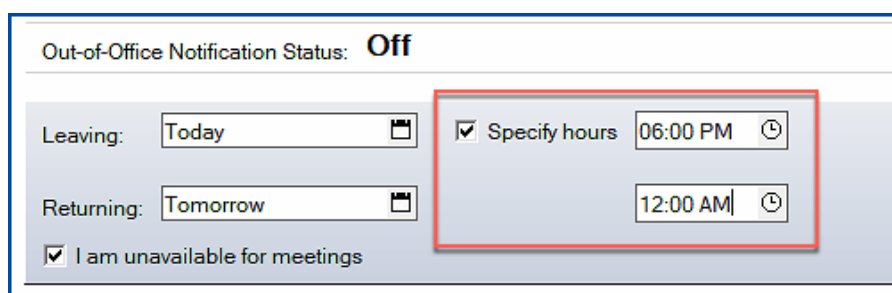
Out-of-Office Notification Status:

Leaving: Today

Returning: Tomorrow

I am unavailable for meetings

Es existieren die Felder »Leaving« und »Returning«. Eine Einstellung für eine gewünschte Zeitspanne in Stunden fehlt.



Out-of-Office Notification Status: **Off**

Leaving: Today

Returning: Tomorrow

Specify hours 06:00 PM

12:00 AM

I am unavailable for meetings

Sobald der Out-of-Office Service auf dem Domino Server aktiv ist, kann zusätzlich eine Zeitspanne (Minimum: 1 Stunde) eingestellt werden.

3.3.1. Was ist der ID Vault?

- ID Vault ist eine Domino Anwendung, welche geschützte Kopien der User IDs vorhält.
- Administratoren und Benutzer erhalten mit dem ID Vault ein Werkzeug zur Verwaltung von Anwender ID Dateien.
- Möglichkeit der Wiederherstellung von Anwender IDs und der Kennwortrücksetzung durch autorisierte Benutzer (ausser den Administratoren zusätzlich Personen aus dem Helpdesk, Poweruser, etc.).
- Unterstützung für 3rd Party Programme (C, Java, JavaScript oder LotusScript).
- Automatische Synchronisation mehrerer Anwender ID-Dateien (z.B. beim Einsatz von Notebook und Desktop PC).
- Wenig bis keine Benutzeraktivität erforderlich.
- Anwender ID-Dateien lassen sich extrahieren, um auf die im ID Vault verschlüsselt gespeicherten IDs zuzugreifen (Rolle »Auditor« in der Vault Anwendung).
- Der Anmeldedialog im Notes Client zeigt auf Wunsch selbst definierte Hinweise zur Vorgehensweise bei vergessenem Kennwort an (grünes »+« Symbol direkt im Anmeldedialog).
- Die Zuordnung von Anwendern zu einem ID Vault wird durch Policies in Verbindung mit Einstellungsdokumenten vom Typ »Security« umgesetzt.

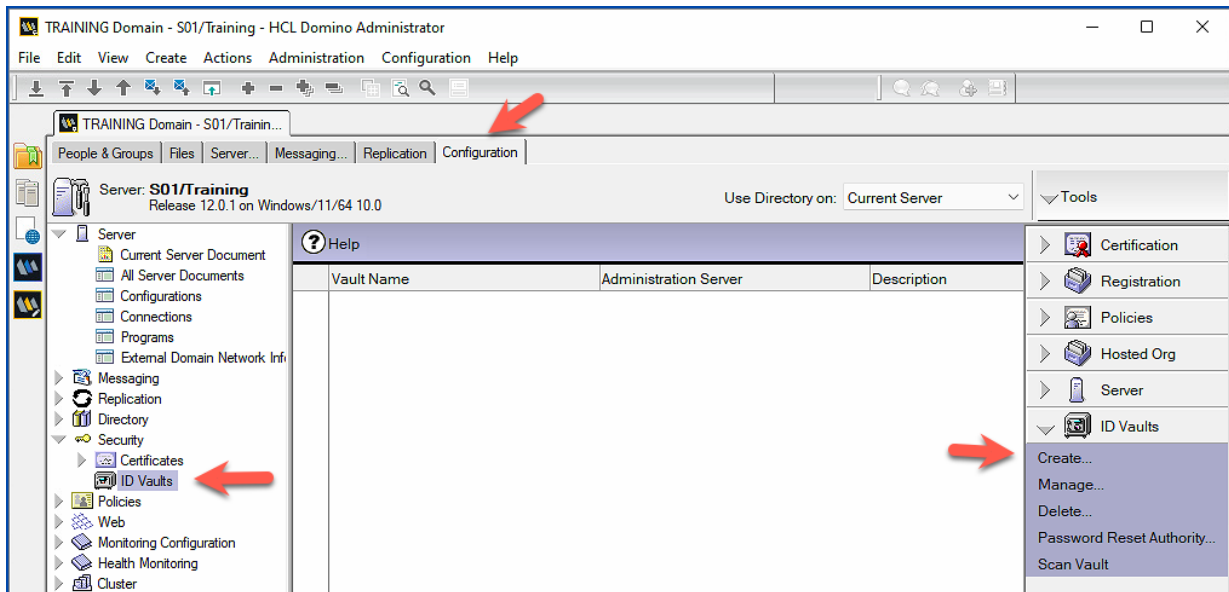
3.3.2. Voraussetzungen für den ID Vault

- Notes Client und Domino Server Version 8.5 oder höher.
- Vault Trust Certificates (werden automatisch erstellt).
- Policies in Verbindung mit Einstellungsdokumenten vom Typ »Security« (beide Dokumente werden auf Wunsch während der Einrichtung des ID Vaults automatisch erstellt).
- Der Notes Client benötigt zwingend einen gültigen Eintrag für den Home-/Mailserver in den Arbeitsumgebungen.

3.3.3. Wie funktioniert der ID Vault?

- **Aktive Notes Anwender**
Nachdem die Policies wirksam sind, wird die Anwender ID Datei beim ersten Anmelden des Anwenders in den Vault kopiert (zufallsgesteuerter Zeitpunkt, kann bis zu 8 Stunden dauern).

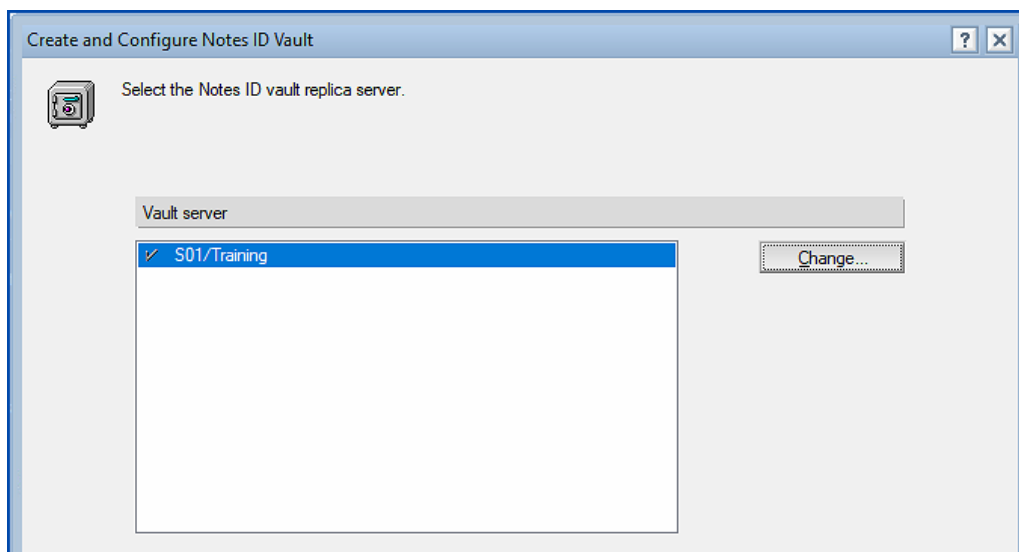
3.3.7. Einrichtung des ID Vaults



Öffnen Sie im Domino Administrator den Tab »Configuration« und selektieren Sie links die Ansicht »Security« → »ID Vaults«. Klicken Sie rechts auf das Tool »ID Vaults« → »Create...«.

Die Konfiguration wird in den folgenden Dialogen (zuerst wird ein Dialog mit weiteren Informationen angezeigt) in insgesamt 10 Schritten umgesetzt.

Schritt 3

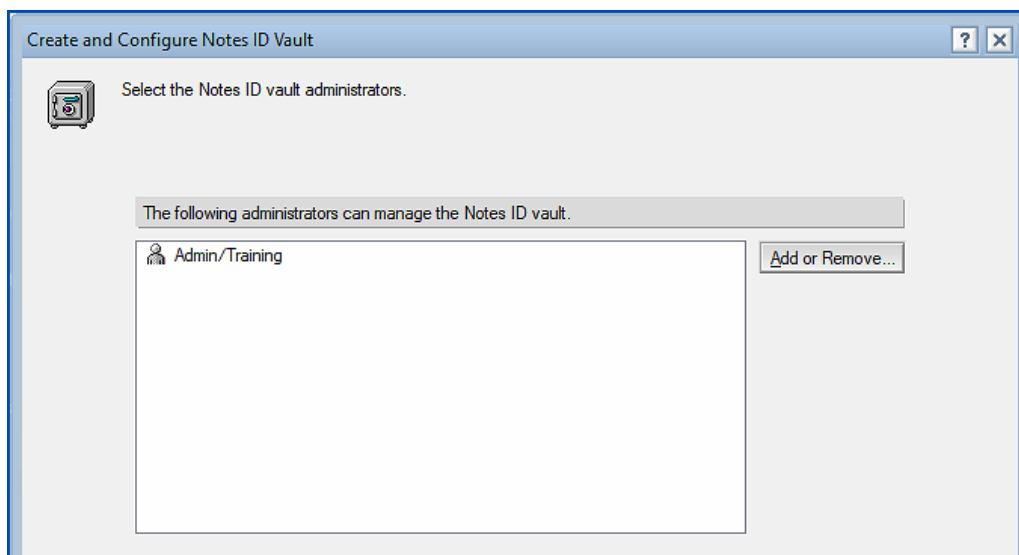


Die ID Vault Anwendung wird auf diesem Domino Server gespeichert. Durch die Schaltfläche »Change...« kann ein anderer Domino Server ausgewählt werden.

Hinweis

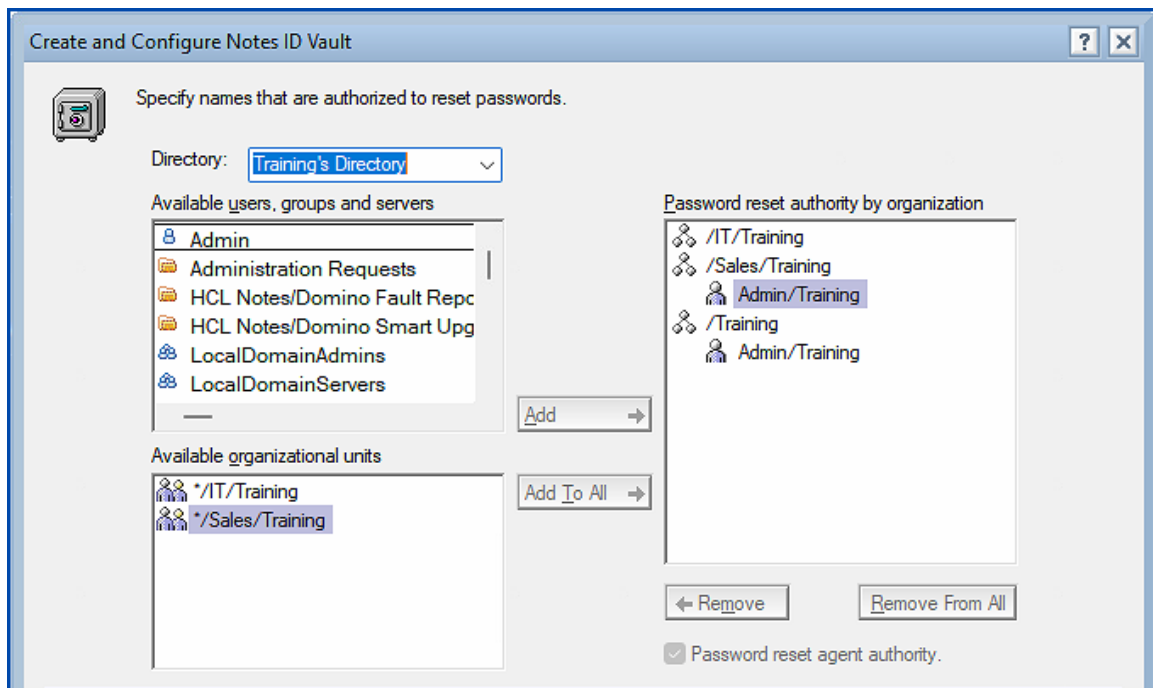
Es lässt sich immer nur **ein** Domino Server selektieren. Sie können später durch das Tool zur Verwaltung des ID Vaults Repliken auf weiteren Domino Servern erstellen.

Schritt 4



Die hier gezeigte Person darf den ID Vault verwalten. Durch die Schaltfläche »Add or Remove...« können weitere Personen (keine Gruppen) ausgewählt werden. Zur Auswahl stehen nur Personen, welche im Serverdokument auf dem Tab »Security« im Feld »Administrators« direkt oder als Mitglied einer Gruppe eingetragen sind.

Schritt 6



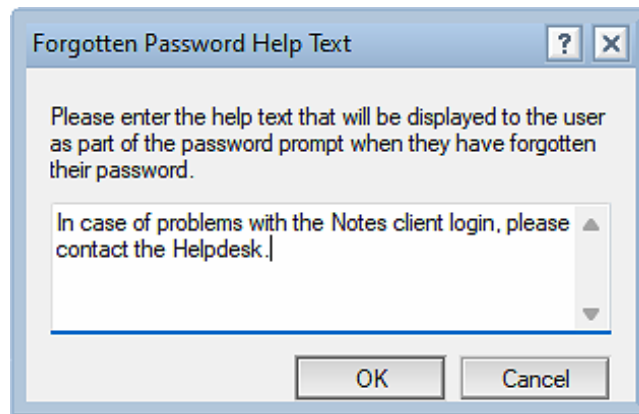
Wählen Sie hier für jede im rechten Fenster gelistete Organization oder Organizational Unit, welche Person eine Rücksetzung von Passwörtern durchführen darf. Sofern Sie eine Gruppe auswählen, wird für jedes Mitglied der Gruppe ein eigenes Kennwort-Rücksetzungszertifikat erstellt.

Hinweis

Es existiert später keine Verbindung mehr zu den Mitgliedern der Gruppe. Ändern sich die Mitglieder, hat dies keinen Einfluss auf aktuell erstellen Kennwort-Rücksetzungszertifikate.

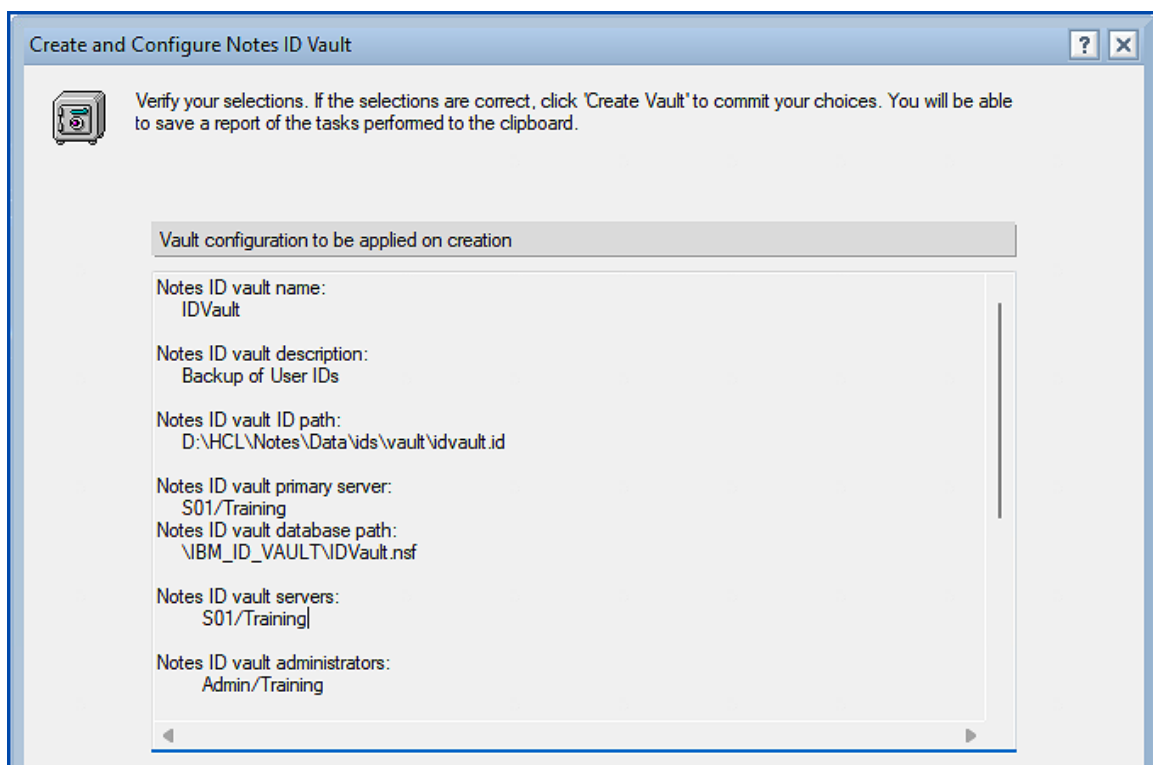
Wichtig

Bei Nutzung der Option »Available organizational Units« ist Vorsicht geboten. Würde man als Beispiel »*/Sales/Training« verwenden, darf jeder Anwender aus dieser Organizational Unit Passwörter zurücksetzen.



Der eingegebene Text wird beim Anmeldedialog im Notes Client angezeigt, wenn man auf das grüne »+« Symbol klickt.

Schritt 9



Hier werden alle zuvor festgelegten Parameter zur Überprüfung angezeigt. Bestätigen Sie den Dialog durch die Schaltfläche »Create Vault«.

3.3.8. Überprüfung der ID Vault Einrichtung

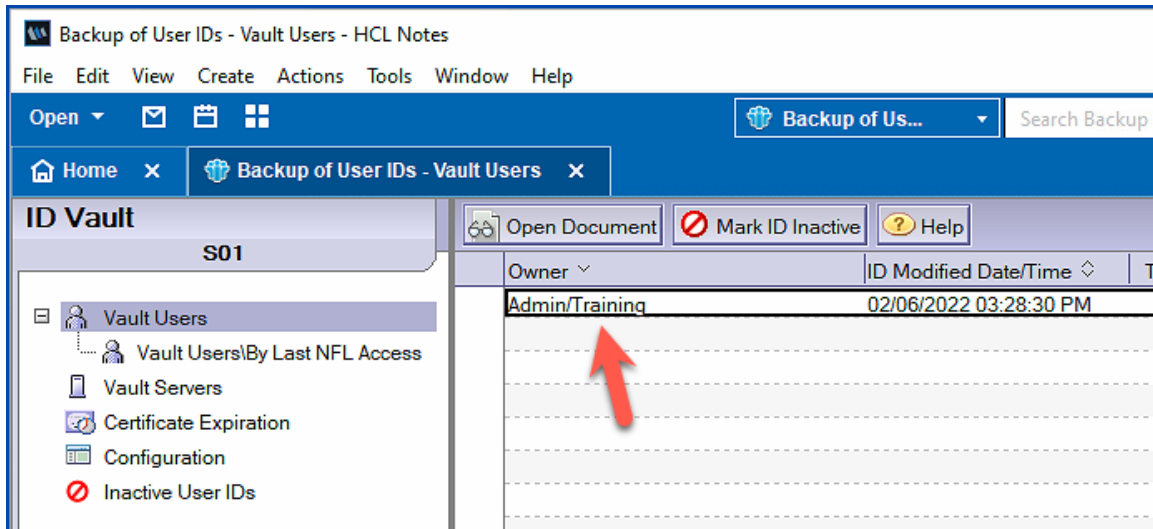
Nach der Einrichtung des ID Vaults finden Sie die folgenden, neu erstellten Elemente.

- **ID Vault Application**
Die Anwendung wurde im Verzeichnis »IBM_ID_FAULT« unterhalb des Verzeichnisses »Data« gespeichert.
- **ID Vault Document** (im Directory gespeichert)
Wählen Sie im Domino Administrator den Tab »Configuration« und dann links in der Navigation den Punkt »Security« → »ID Vaults«.
- **Password Reset Certificates** (im Directory gespeichert)
Wählen Sie im Domino Administrator den Tab »Configuration« und dann links in der Navigation den Punkt »Security« → »Certificates« → »Certificates«.
- **Vault Trust Certificates** (im Directory gespeichert)
Wählen Sie im Domino Administrator den Tab »Configuration« und dann links in der Navigation den Punkt »Security« → »Certificates« → »Certificates«.
- **Policy-/Settingsdocuments** (im Directory gespeichert)
Wählen Sie im Domino Administrator den Tab »People & Groups« und dann links in der Navigation den Punkt »Policies« oder »Settings«.

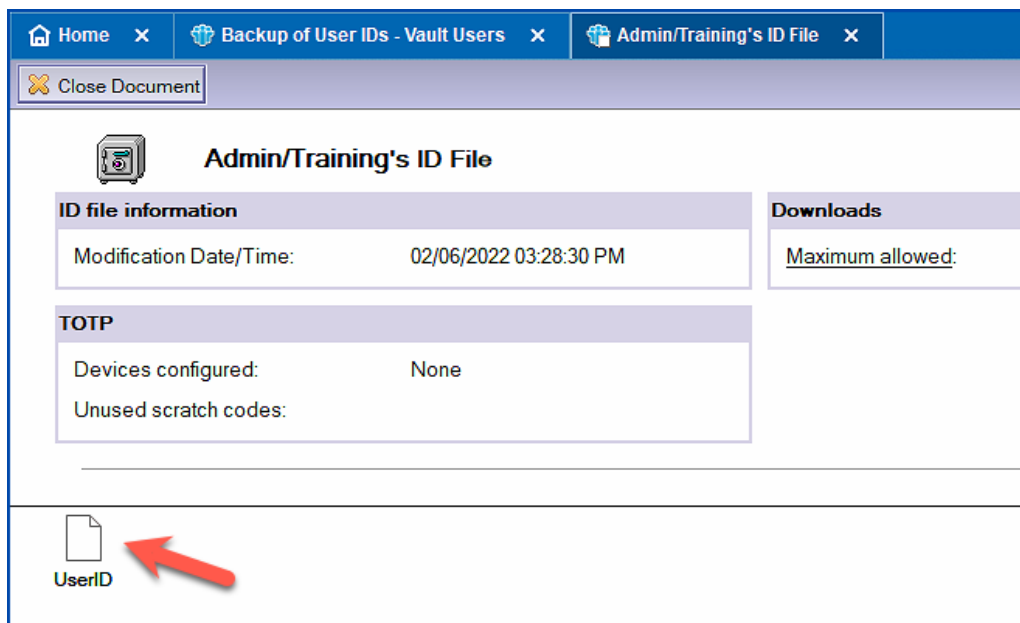
3.3.9. Hochladen der Anwender IDs in den ID Vault

Damit die Anwender ID-Dateien in die ID Vault Anwendung hochgeladen werden, muss die bei der Einrichtung des ID Vaults neu angelegte oder geänderte Richtlinie wirksam sein. Dies kann man (siehe folgenden Screenshot) im Anmeldedialog beim Start des Notes Clients überprüfen.

Wenn Sie auf das grüne Plus (+) bei der Meldung »Forgot your password?« klicken und es wird dann Ihre selbst festgelegte Meldung angezeigt, dann ist die Richtlinie für den im Anmeldedialog benannten Anwender wirksam.



Das Dokument sollte sofort verfügbar sein.



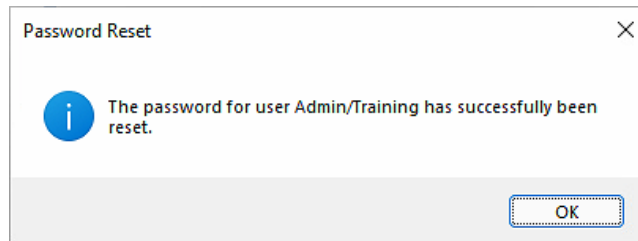
Im geöffneten Dokument sehen Sie die angehängte Anwender ID Datei.

(z.B. den Vorgesetzten) an, an die ein per Zufall generiertes Passwort per Mail gesendet wird.

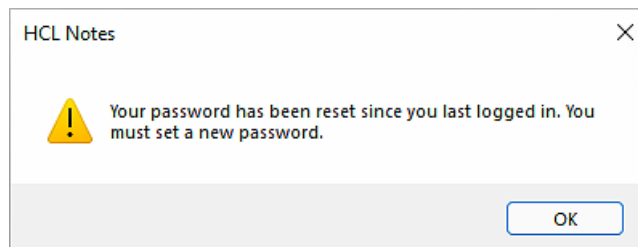
4. New password und Confirm new password

Eingabe und Bestätigung des selbst festgelegten Passworts.

Bestätigen Sie die Rücksetzung des Passworts durch die Schaltfläche »Reset Password«.



Nach der Eingabe des zurückgesetzten Passworts im Anmeldedialog des Notes Clients, wird der Anwender aufgefordert, ein neues und dauerhaft gültiges Passwort zu vergeben.



Bestätigen Sie den Dialog mit »OK«.

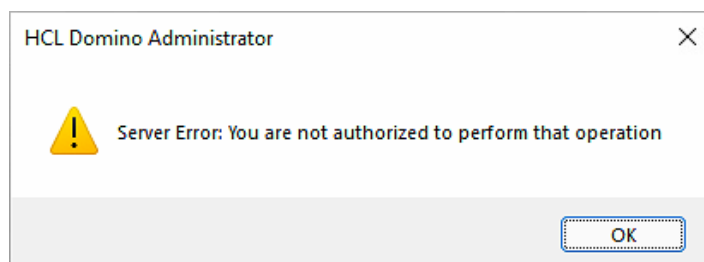


Geben Sie ein neues Passwort ein. In der Grundkonfiguration des Domino Servers darf dies das zuvor verwendete Passwort sein.

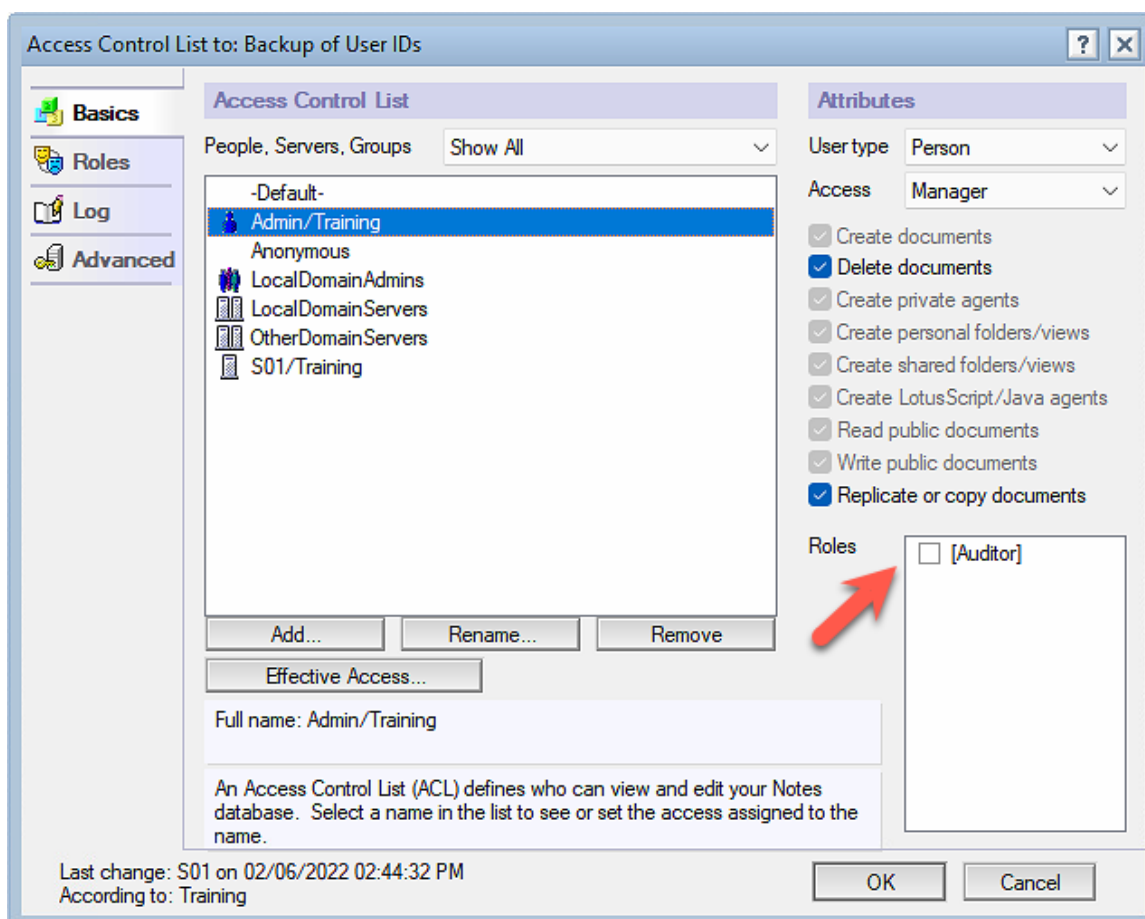
3.3.12. Nutzung des ID Vaults - Anwender ID-Datei extrahieren

Eine Anwender ID kann manuell aus dem ID Vault heruntergeladen und einem Anwender zur Verfügung gestellt werden.

Hierzu ist in der ACL der Anwendung »ID Vault« die Rolle »Auditor« erforderlich.



Ohne diese Rolle erhalten Sie die im Screenshot gezeigte Fehlermeldung. Öffnen Sie den Dialog zur Verwaltung der ACL für Ihren ID Vault.



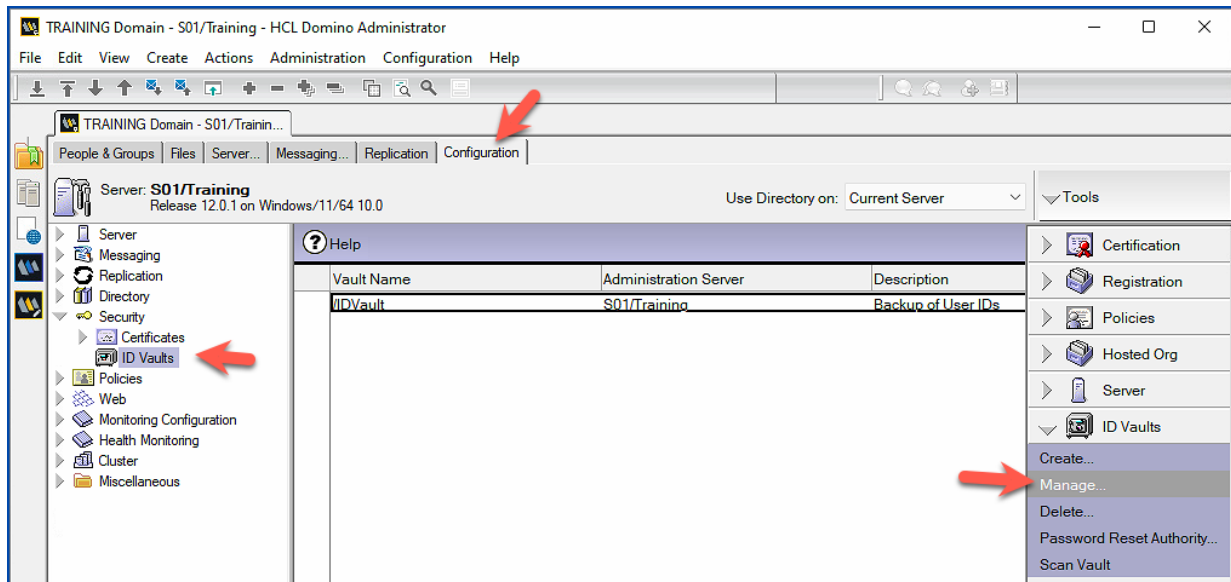
Aktivieren Sie für ihren Anwender die Rolle »Auditor« und bestätigen Sie den Dialog mit »OK«.

Öffnen Sie im Domino Administrator den Tab »People & Groups« und selektieren Sie links die Ansicht »People«. Nachdem Sie den gewünschten Anwender ausgewählt haben, klicken Sie auf das Tool »ID Vaults« → »Extract ID From Vault...«.

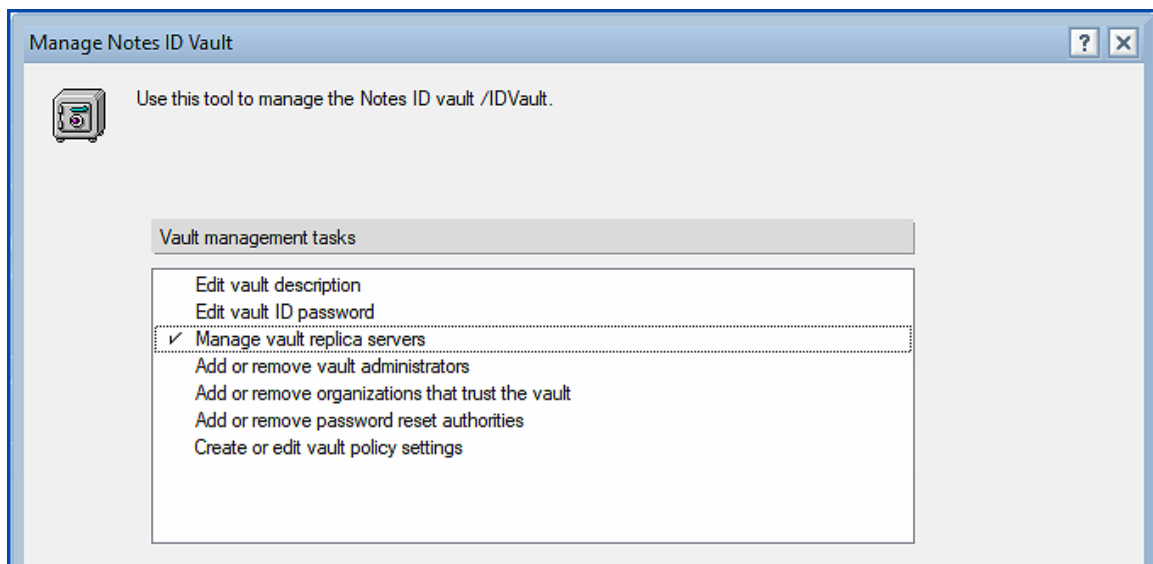
3.3.13. Änderungen an der ID Vault Konfiguration durchführen

Die Konfiguration des ID Vaults kann nach der initialen Einrichtung geändert werden.

Öffnen Sie im Domino Administrator den Tab »Configuration«. Wählen Sie links in der Navigation die Ansicht »Security« → »ID Vaults« und selektieren Sie in der Übersicht den gewünschten ID Vault. Klicken Sie rechts auf das Tool »ID Vaults« → »Manage«.



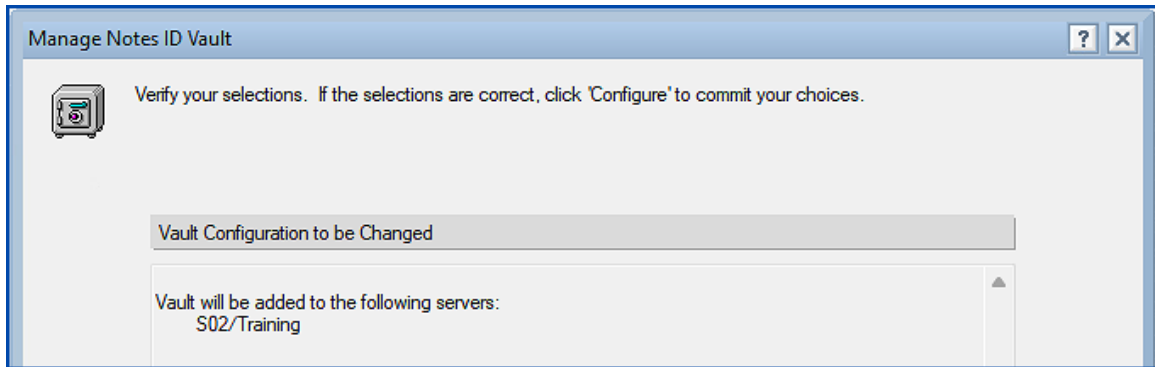
Es erscheint zuerst (falls Sie dies beim Erstellen des ID Vaults nicht deaktiviert haben) ein Informationsdialog. Im folgenden Dialog wählen Sie aus, was Sie in der Konfiguration (eine Mehrfachauswahl ist möglich) ändern möchten.



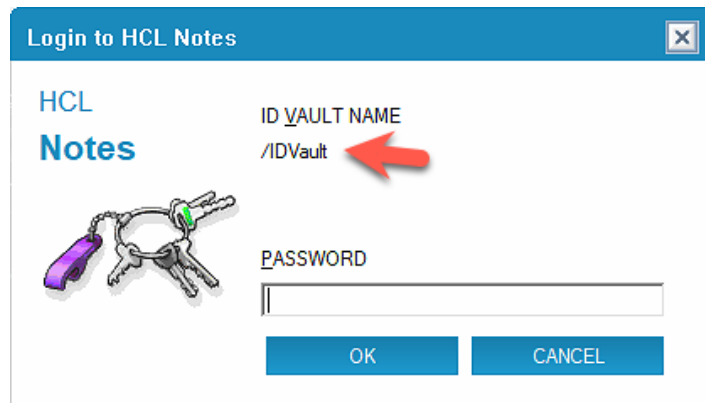
Als Beispiel werden wir den ID Vault zusätzlich als Replik auf einem weiteren Domino Server verfügbar machen. Grundsätzlich sollte der ID Vault auf allen Domino Servern verfügbar sein, welche als Homeserver für Anwender genutzt werden.

Bestätigen Sie den Dialog mit der Schaltfläche »Next«.

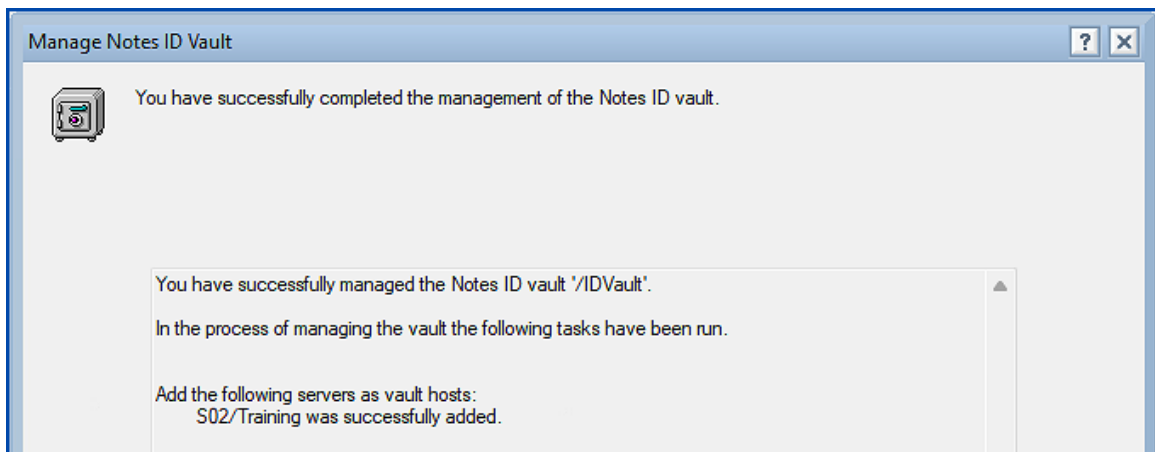
Bestätigen Sie den Dialog durch die Schaltfläche »Next«.



Die gewählte Konfiguration wird zur Kontrolle angezeigt. Bestätigen Sie diesen Dialog mittels der Schaltfläche »Configure«.



Bevor die neue Replik erstellt wird, müssen Sie das Passwort zur ID Datei des ID Vaults eingeben.



Die Replik des ID Vault wurde auf dem Domino Server »S02/Training« erstellt.

Hinweis
 Weitere Änderungen an der Konfiguration des ID Vault verlaufen ähnlich komfortabel. Probieren Sie gerne zusätzliche Optionen in Ihrer Lernumgebung aus!

3. Beim nächsten Versuch einer Synchronisierung wird das zuvor genutzte Dokument des Anwenders wegen der Umbenennung nicht mehr im ID Vault gefunden und die Anwender ID wird erneut hochgeladen. Hiernach sollte die Synchronisation wieder einwandfrei funktionieren.

Neustart der Synchronisation: Verwaltung

Durch den Konsolenbefehl »qvault« (query vault) sowie durch eine neue Option im Domino Administrator können verschiedene Optionen beim Management des ID-Vault genutzt werden.

Zunächst muss der Datei »notes.ini« der folgende Eintrag hinzugefügt werden:

```
IDV_Enable_Vault_Scan=1
```

Jetzt kann der Konsolenbefehl »qvault« verwendet werden (ggf. ist zur Nutzung ein Neustart des Domino Servers erforderlich). Durch die Ergänzung des Befehls um die Option »/?« werden die zulässigen Parameter gelistet.

```
load qvault /?
[1C1C:0002-1250] Query Vault Tool.
[1C1C:0002-1250] Usage: load qvault [-x <vaultname> [-u <username> [-r | -a | -d] -i | -v] -p]] | [-d] -p]]
[1C1C:0002-1250] Usage: Usage: Add quotes around <vaultname> or <username> if the name contains a space
[1C1C:0002-1250] -x <vaultname> Scan O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> Scan O=VaultName for UserName
[1C1C:0002-1250] -x <vaultname> -u <username> -r Revert Archived UserName in O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> -a Archive UserName in O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> -i Inactivate UserName in O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> -v Reactivate UserName in O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> -d Delete Archived UserName in O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> -p Update User Data in O=VaultName
[1C1C:0002-1250] -x <vaultname> -d Delete All Archived Users in O=VaultName
[1C1C:0002-1250] -x <vaultname> -p Update All User Data in O=Vaultname
[1C1C:0002-1250] e.g. load qvault -x <vaultname> -p Update All User Data in O=Vaultname
```

Beispiel (Achten Sie auf die Nutzung von kanonischen Notes Namen):

```
load qvault -x O=IDVault -u "CN=Admin/O=Training"
```

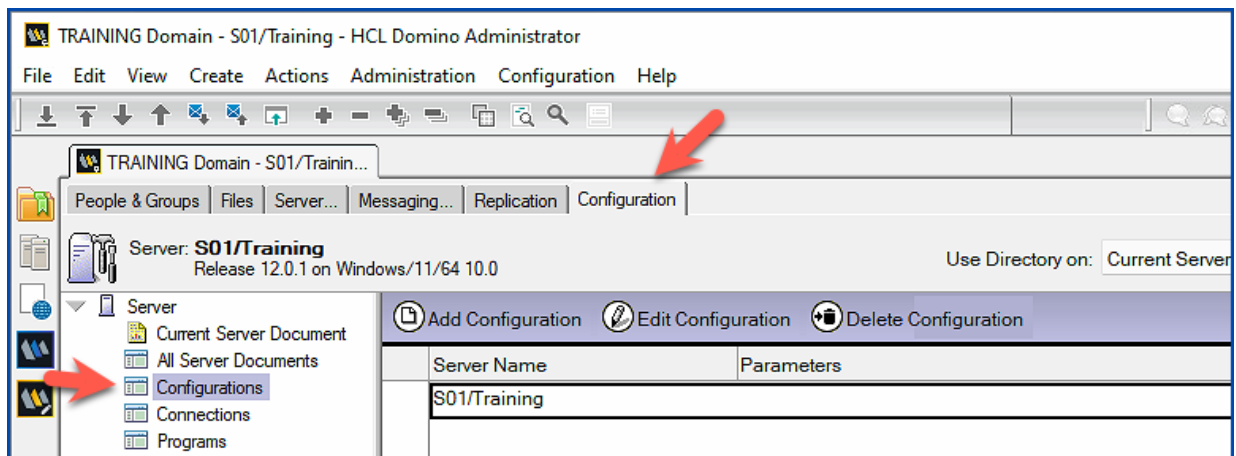
```
load qvault -x O=IDVault -u "CN=Admin/O=Training"
[2344:0002-0348] QVR: Vault O=IDVault
[2344:0002-0348] QVR: User CN=Admin/O=Training
[2344:0002-0348] Scan Vault : O=IDVault, Total 1, Updated 0, No Update Needed 1, Update failures 0
[0448:005B-0FD4] 06.02.2022 18:59:04 Opened session for S01/Training (Release 12.0.1)
[0448:005B-0FD4] 06.02.2022 18:59:04 Closed session for S01/Training Databases accessed: 1
```

3.4. Lizenzverfolgung

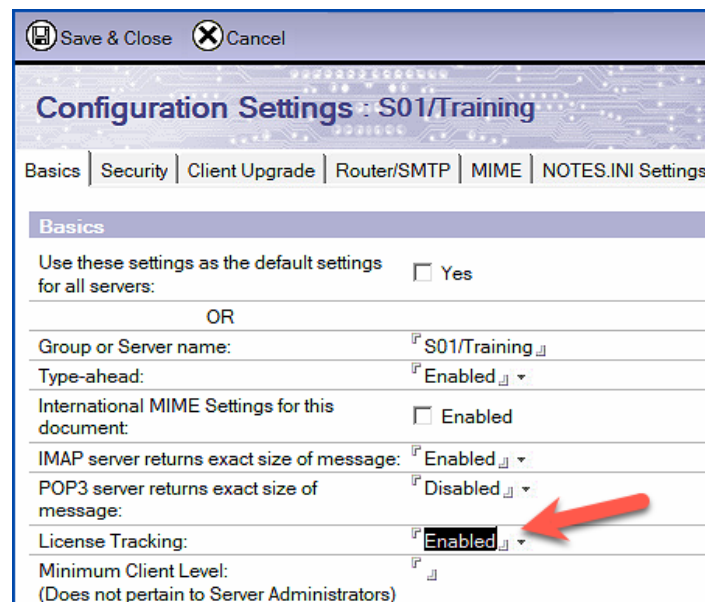
Die Lizenzverfolgung ermöglicht die Überwachung der aktiv von Anwendern genutzten Lizenzen. Nach der Aktivierung werden Zugriffe auf den Domino Server erfasst und in der Anwendung **Domino User License Tracking** (»userlicenses.nsf«) gespeichert.

3.4.1. Aktivierung der Lizenzverfolgung

Öffnen Sie im Domino Administrator den Tab »Configuration« und wählen Sie links die Ansicht »Server« → »Configurations«.



Erstellen Sie ein neues oder öffnen Sie ein existierendes Konfigurationsdokument.

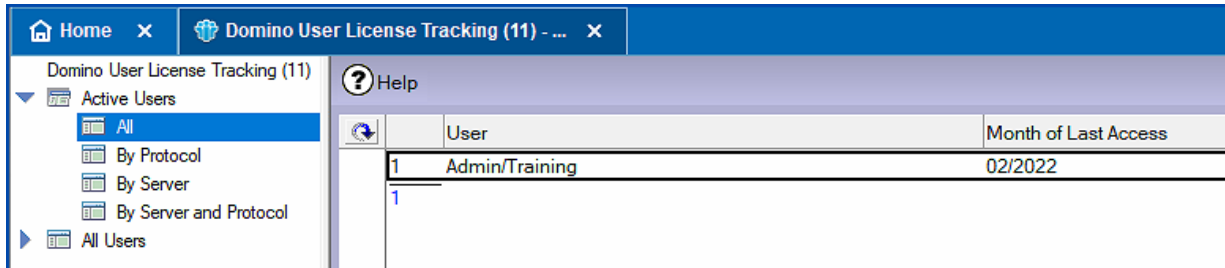


Aktivieren Sie die Lizenzverfolgung im Feld »License Tracking« auf dem Tab »Basics«. Speichern und schließen Sie das Dokument.

Sobald die Lizenzverfolgung aktiviert ist, wird jede authentifizierte Verbindung (Notes NRPC, HTTP, IMAP, POP3, SMTP und LDAP) eines Anwenders registriert und zunächst temporär in der Datei »license.ncf« gespeichert. Hierbei wird der vollständige Benutzername, das verwendete Protokoll sowie Datum und Uhrzeit erfasst.

3.4.2. Dokumente in der Anwendung userlicenses.nsf

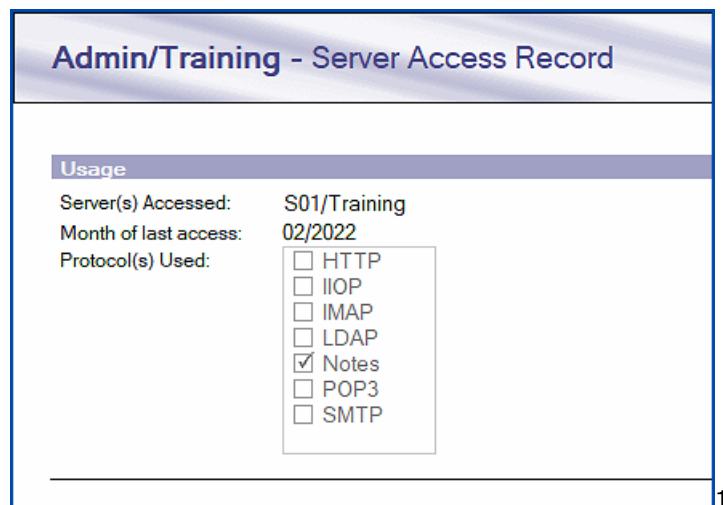
Sobald die Anwendung Domino User License Tracking («userlicenses.nsf») erstellt wurde, kann Sie geöffnet und die Dokumente für die einzelnen Anwender betrachtet werden. Zur Auswertung stehen verschiedene Ansichten zur Verfügung.



Hinweis

Wenn Sie diese Anwendung im Notes Client öffnen möchten, müssen Sie den Dateinamen »userlicenses.nsf« selbst im Dialog zum Öffnen von Anwendungen eintippen - die Anwendung wird wegen eines spezifischen Flag nicht automatisch angezeigt.

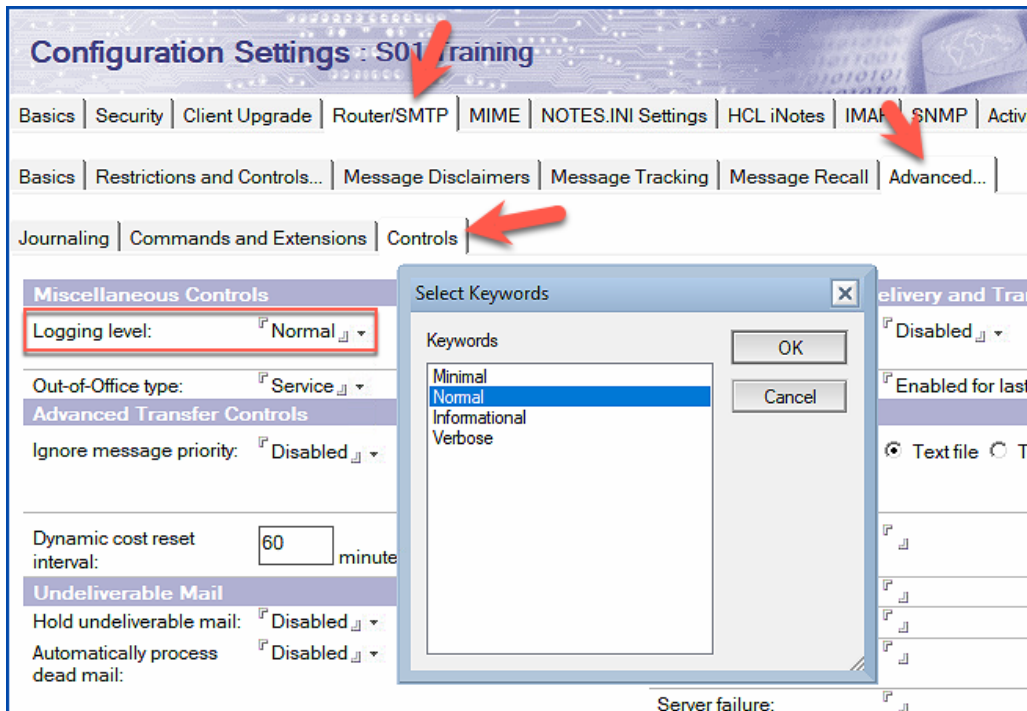
Öffnen Sie eines der Dokumente.



Im geöffneten Dokument werden die vom Anwender genutzten Domino Server, der Monat des letzten Zugriffs und die verwendeten Protokolle angezeigt.

4. Mailrouting

Erstellen Sie ein neues oder öffnen Sie ein existierendes Konfigurationsdokument. Wählen Sie den Tab »Router/SMTP« → »Advanced...« → »Controls«.



Im Feld »Logging level« stehen diverse Optionen zur Auswahl - die Vorgabe ist »Normal«. Die Option »Minimal« zeigt an der Domino Konsole noch weniger Informationen und scheidet daher aus.

Für eine Nutzung in der Praxis erscheint die Option »Informational« sinnvoll - sie liefert an der Domino Konsole folgende Informationen zu einer gesendeten Mail:

- [064C:0006-0E28] 07.02.2022 16:55:11 Router: Message 0050BD9B transferred to S02/TRAINING for Betty Jones/Training@Training **from Admin/Training Size: 1K** via Notes

Zusätzlich werden der Absender und die Größe der Mail angezeigt. Bei Nutzung der Option »Verbose« kommen weitere Meldungen des Router Dienstes hinzu - teilweise ohne einen großen Mehrwert für den Administrator.

Probieren Sie es aus!

zurückgerufen werden, welche der Empfänger schon gelesen hat.

3. Do not allow recall of messages older than

Für die hier ausgewählte Zeitspanne in Minuten, Stunden, Tagen oder Wochen ist der Rückruf einer Mail möglich. Vorgabe: 14 Tage.

Hinweis

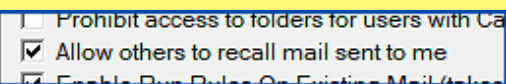
Sofern keine Policy mit Vorgaben für den Nachrichtenrückruf wirksam ist (siehe nächstes Kapitel), gilt die hier getroffene Einstellung für alle Anwender, deren Postfächer auf diesem Domino Server gespeichert sind.

Speichern und schließen Sie das Konfigurationsdokument.

Wichtig

Sofern dies nicht durch eine Policy vorgegeben ist, dürfen Anwender in den Vorgaben des Postfachs selbst entscheiden, ob eine an den Anwender gesendete Mail zurückgerufen werden darf.

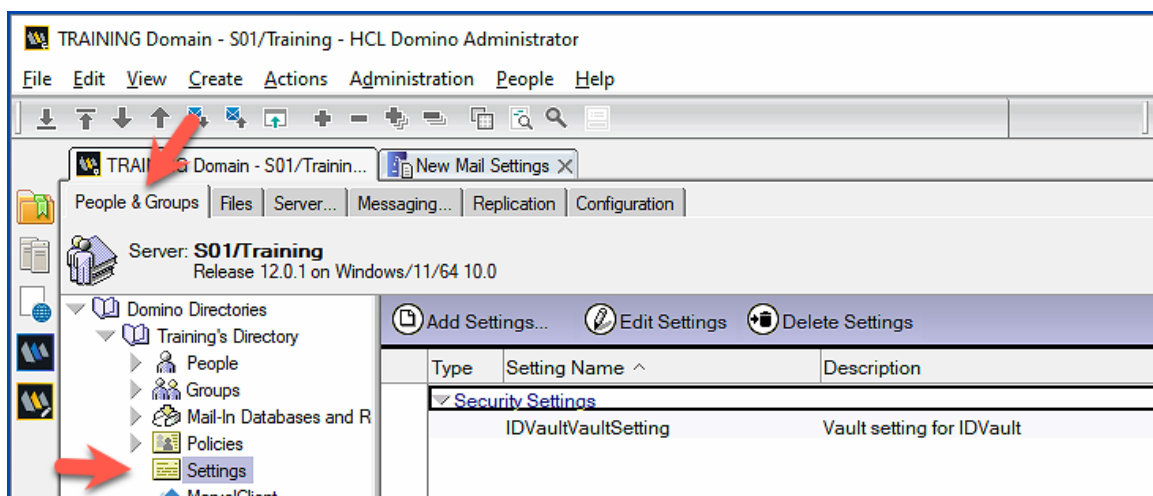
Sie finden diese Einstellung im Dialog »Preferences« (im geöffneten Postfach die Aktion »More« → »Preferences« anklicken) auf dem Tab »Mail« → »Basics« im Abschnitt »View and Folder Management«.



4.2.2. Konfiguration durch Policies

Durch eine Policy in Kombination mit einem Einstellungsdocument für den Bereich »Mail« können die Einstellungen im Konfigurationsdocument **überschrieben** werden.

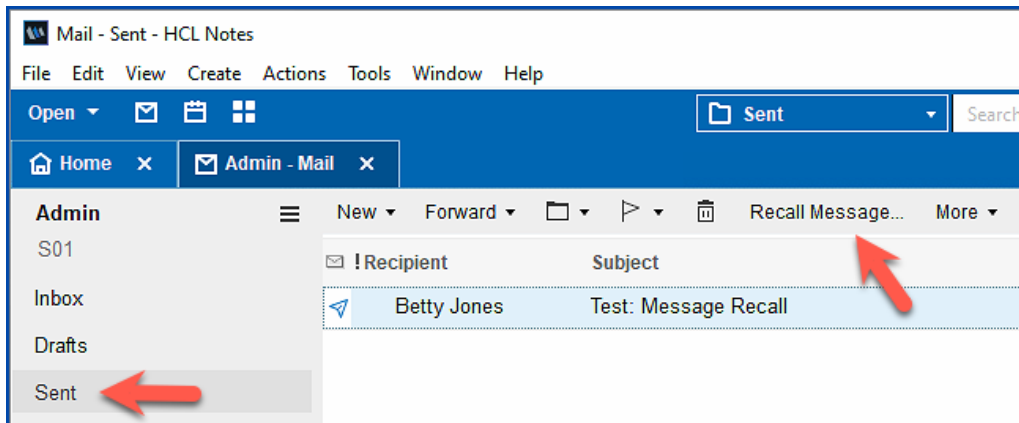
Öffnen Sie im Domino Administrator den Tab »People & Groups« und selektieren Sie links die Ansicht »Settings«.



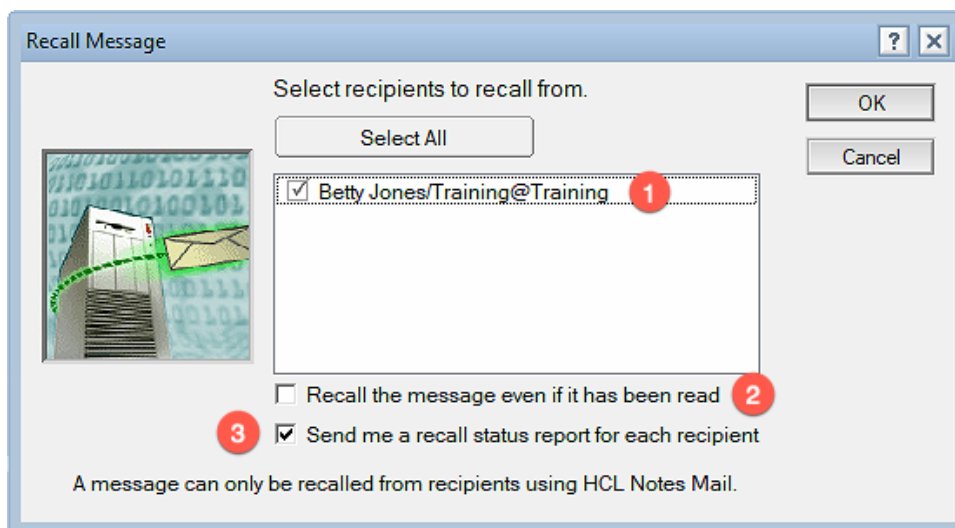
4.2.3. Rückruf von Mails durch den Anwender

Sofern die administrativen Einstellungen einen Rückruf von Mails zulassen, kann der Anwender den Nachrichtenrückruf direkt aus seinem Postfach heraus starten.

Öffnen Sie Ihr Postfach und selektieren Sie die Ansicht »Sent«.



Klicken Sie auf die Aktion »Recall Message...«.



Die folgenden Optionen stehen zur Verfügung:

- 1. Select recipients to recall from**
Sofern die Mail an mehrere Empfänger adressiert war, können durch die Schaltfläche »Select All« alle Empfänger ausgewählt werden.
- 2. Recall the message even if it has been read**
Diese Option funktioniert **nur**, wenn der Rückruf von gelesenen Nachrichten im Konfigurationsdokument oder der Policy erlaubt ist.
- 3. Send me a recall status report for echt recipient**
Auf Wunsch erhält man vom Domino Server für jede auswählte Person einen Statusreport in Form einer Mail.

4.3. Mailverfolgung

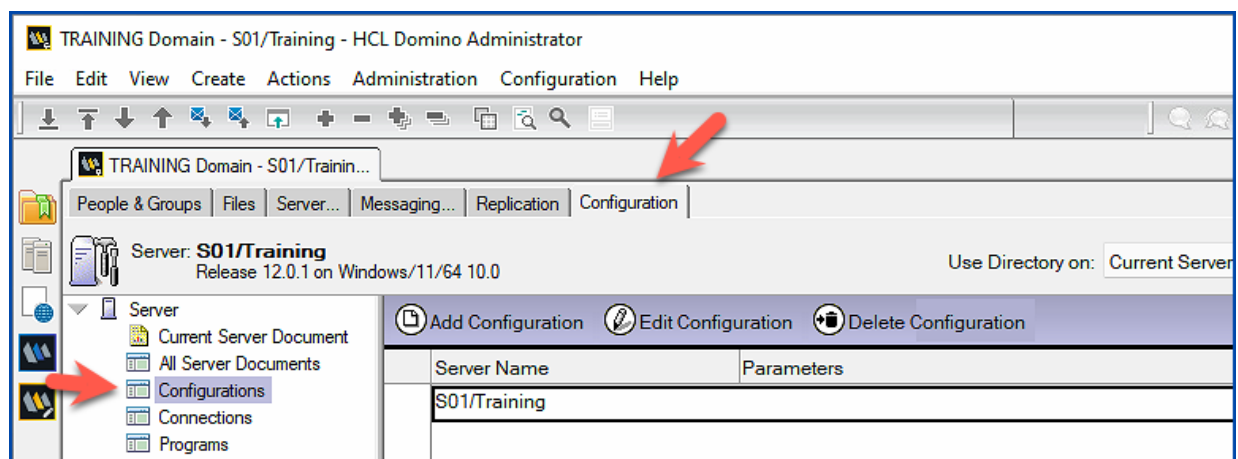
Durch die Mailverfolgung kann der Transfer von Mails vom Absender bis zum Empfänger nachverfolgt werden. Zusätzlich erhält man die Information, ob der Empfänger die Mail gelesen oder gelöscht hat.

Wer selbst schon einmal durch die Informationen in den LOG Anwendungen (>log.nsf«) versucht hat, eine Mail über mehrere Domino Server zu verfolgen, wird die Mailverfolgung lieben.

Die Verfolgung von Mails funktioniert grundsätzlich nur innerhalb der eigenen Notes/Domino Umgebung.

4.3.1. Einstellungen im Konfigurationsdokument

Öffnen Sie im Domino Administrator den Tab »Configuration« und wählen Sie links die Ansicht »Server« → »Configurations«.



Erstellen Sie ein neues oder öffnen Sie ein existierendes Konfigurationsdokument. Wählen Sie den Tab »Router/SMTP« → »Message Tracking«.

in dieses Feld eingetragen werden, wenn Mails über mehrere Domino Server hinweg verfolgt werden sollen.

Wichtig

Die Mailverfolgung muss auf **allen** Domino Servern aktiviert werden, die am Transfer von Mails beteiligt sind. Ansonsten ist keine Verfolgung über mehrere Domino Server möglich.

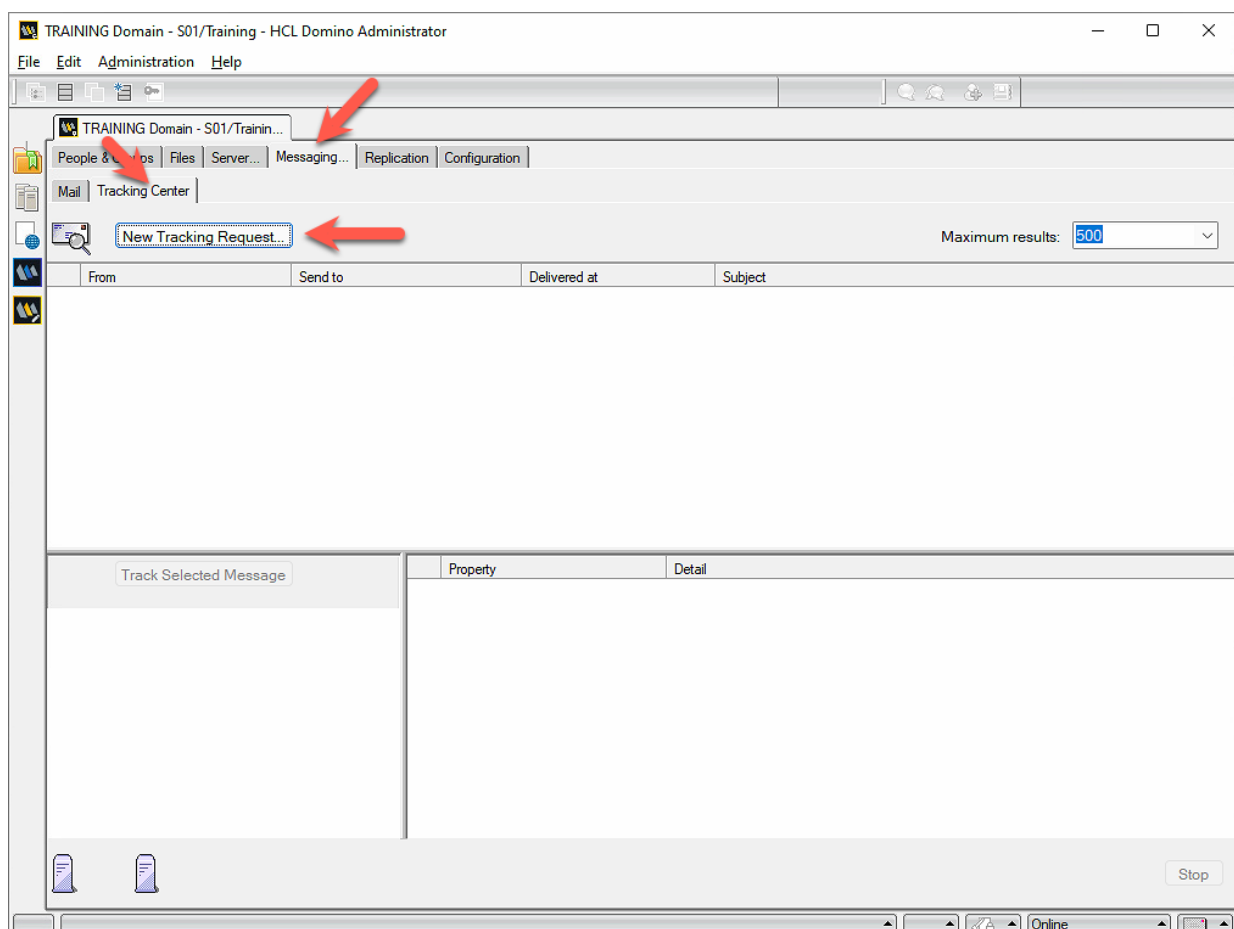
Speichern und schließen Sie das Konfigurationsdokument.

Hinweis

Nach Aktivierung der Mailverfolgung müssen Sie den Domino Server neu starten. Es wird dann unterhalb des Data Verzeichnisses der Ordner »mtdata« angelegt und darin die Anwendung Domino MailTracker Store (»mtstore.nsf«) erstellt.

4.3.2. Nutzung der Mailverfolgung

Öffnen Sie im Domino Administrator den Tab »Messaging...« → »Tacking Center«.

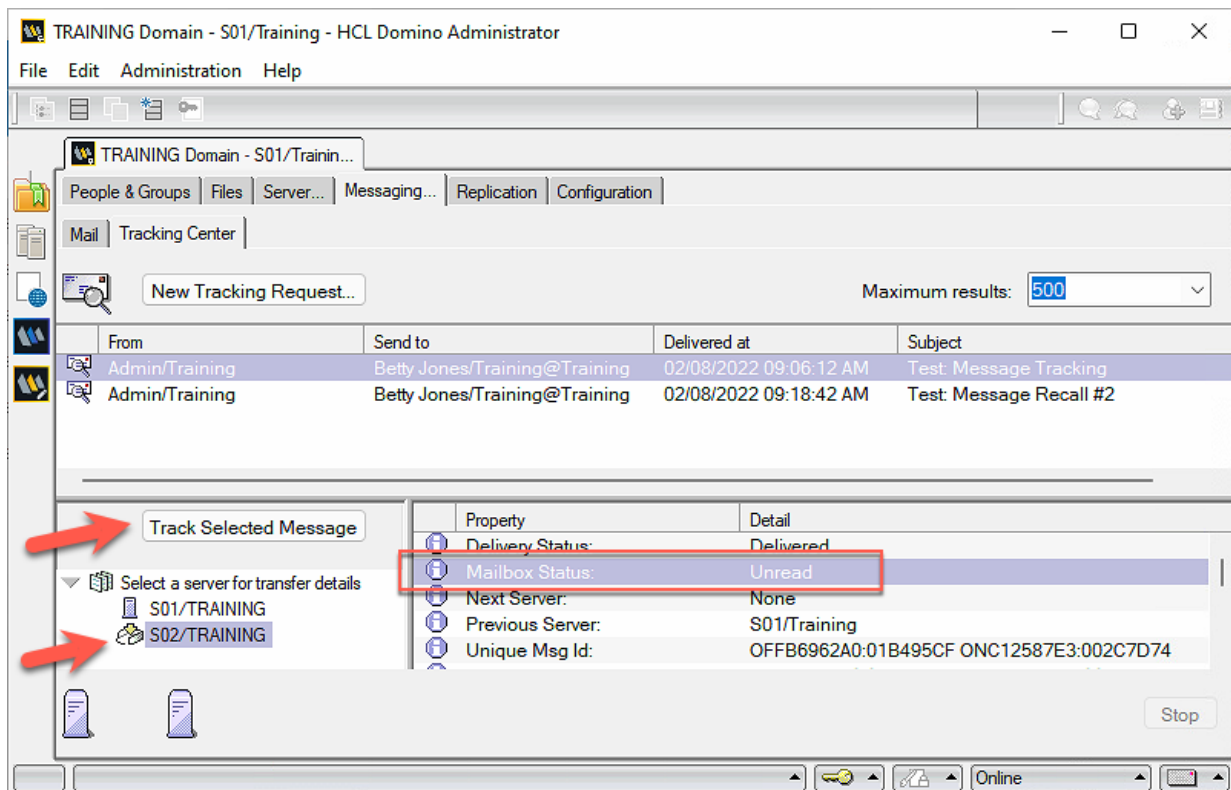


Klicken Sie auf die Schaltfläche »New Tracking Request«.

6. Message ID

Jede Mail, welche über Domino Server geroutet wird, erhält eine eindeutige »Message ID«. Diese wird aber nur an der Domino Konsole (oder in der Anwendung LOG) angezeigt und steht einem Administrator meist nicht zur Verfügung.

Bestätigen Sie den Dialog mit »OK«.



Selektieren Sie die gewünschte Mail und klicken Sie auf die Schaltfläche »Track Selected Message« (oder Sie führen alternativ einen Doppelklick direkt auf die Mail aus).

Im unteren linken Bereich können Sie die einzelnen Domino Server anklicken und es werden rechts viele Details zur Mail angezeigt. Der im Screenshot markierte Domino Server »S02/Training« wird mit einem anderen Symbol als die zuvor gelisteten Server angezeigt, da er final die Mail im Anwender Postfach zugestellt hat.

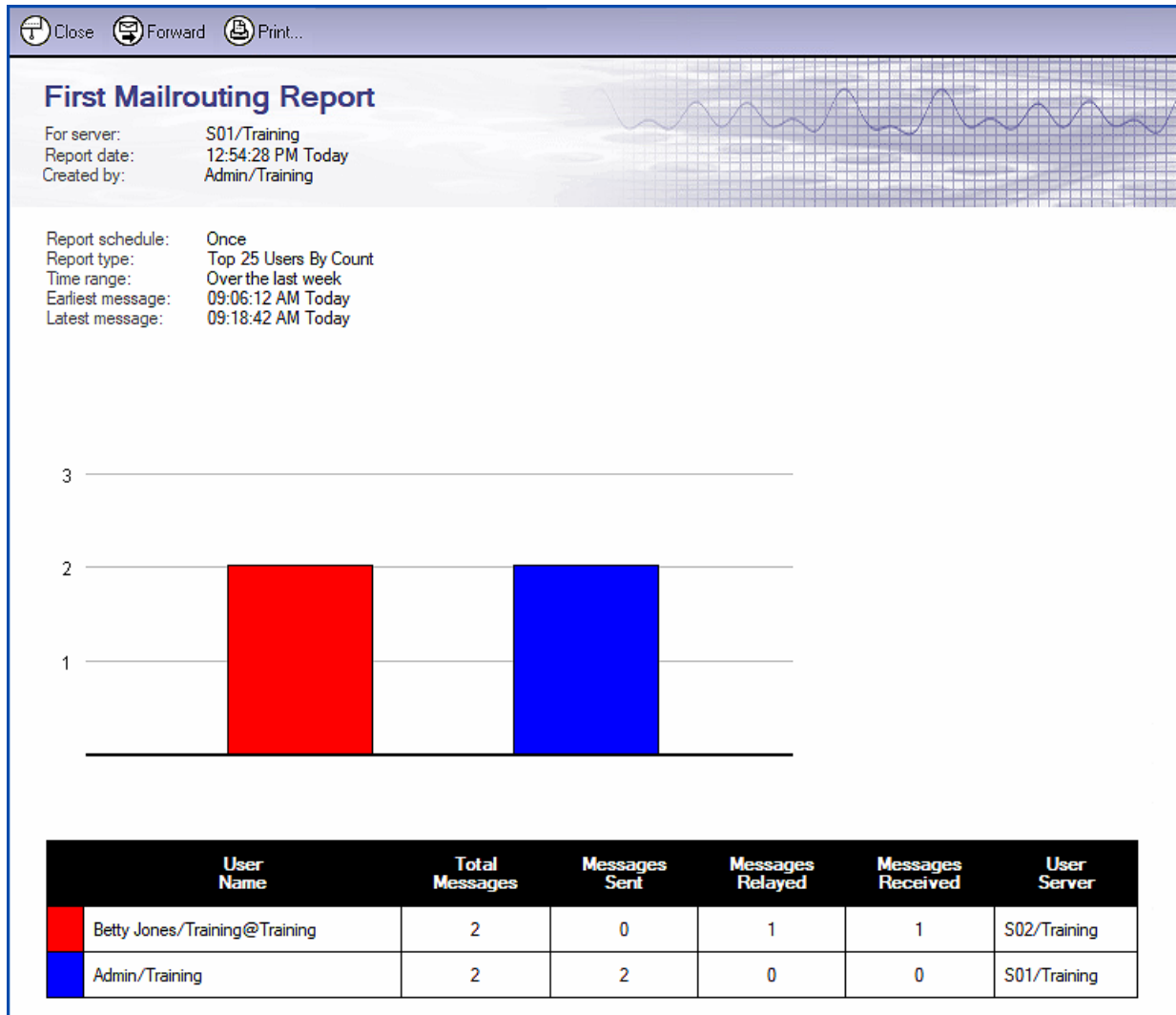
Hinweis

Besonders beim final zustellenden Domino Server ist der »Mailbox Status« interessant. Hier wird sogar der Status »Deleted« angezeigt, wenn der Anwender die Mail gelöscht hat.

In der Praxis kann man so leicht nachweisen, dass die Mail zugestellt wurde - falls der Anwender behauptet, er hätte die Mail nie erhalten.

Auf dem Tab »Basics« lassen sich neben einer Benennung auch die Parameter »Report Type«, »Time Range«, »Run this report« (einmalig oder wiederkehrend) und »Report should be« (der Report wird in der Anwendung gespeichert oder per Mail verschickt) selektieren.

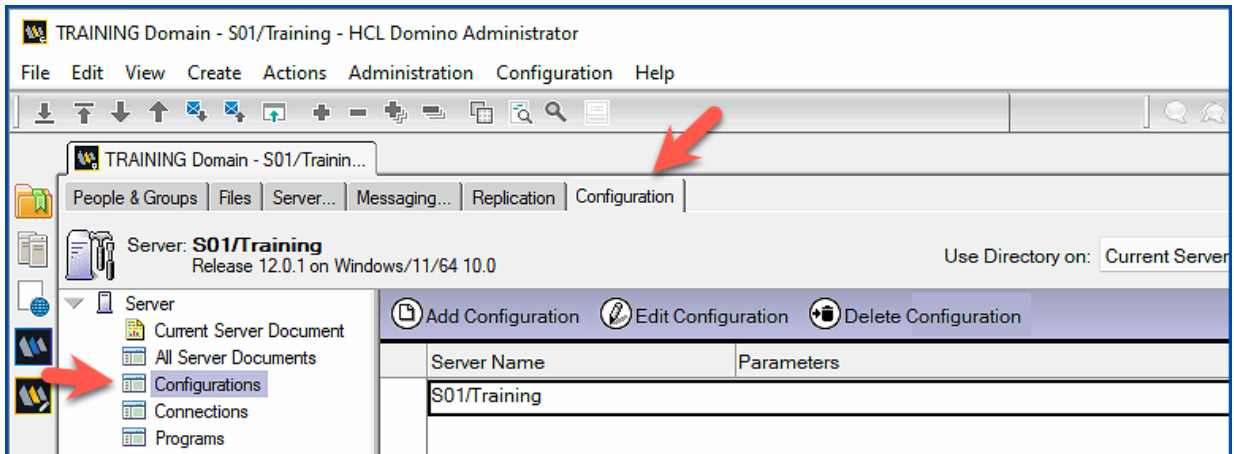
Auf dem Tab »Conditions« lassen sich Filter nach den Kriterien »Sender’s Name«, »Recipient’s Name«, »Delivery Status« und »Message Size« aktivieren.



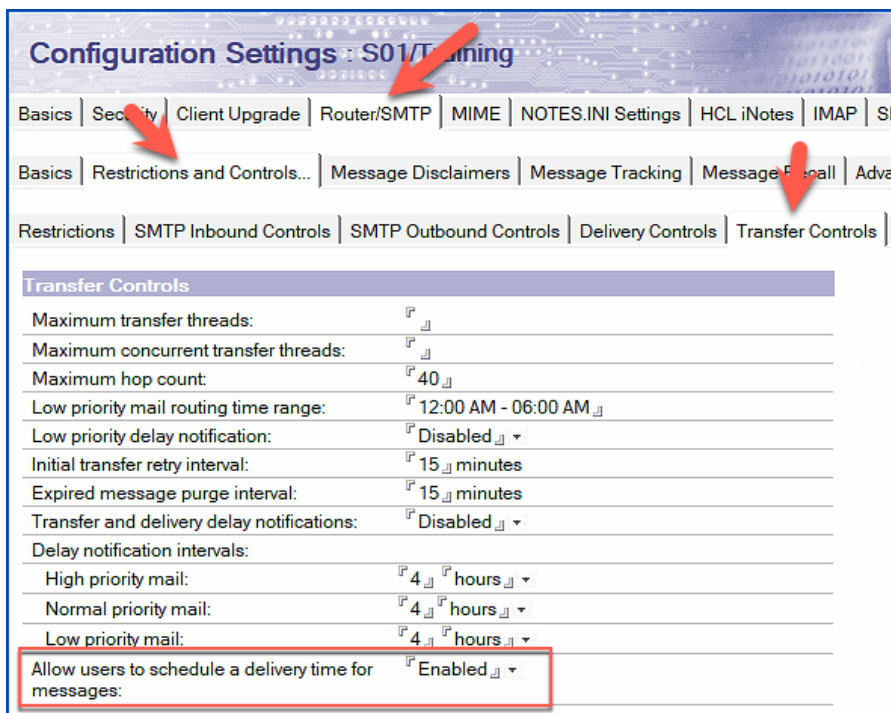
Dies ist ein Beispiel mit den Standard Vorgaben. Probieren Sie gerne weitere Reports aus!

4.4.2. Einstellung im Konfigurationsdokument

Öffnen Sie im Domino Administrator den Tab »Configuration« und wählen Sie links die Ansicht »Server« → »Configurations«.



Erstellen Sie ein neues oder öffnen Sie ein existierendes Konfigurationsdokument. Wählen Sie den Tab »Router/SMTP« → »Restrictions and Controls...« → »Transfer Controls«.



Sie können den zeitgesteuerten Versand im Feld »Allow users to schedule a delivery time for messages« ein- oder ausschalten.

Hinweis

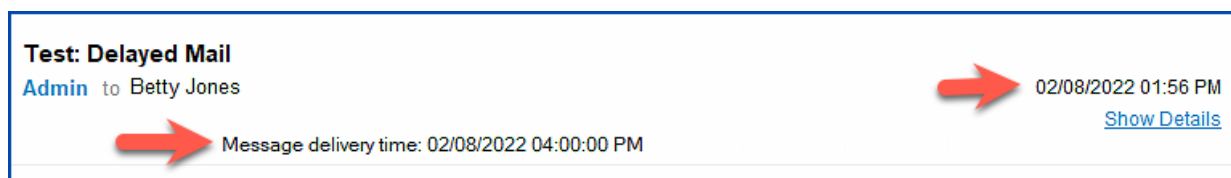
Es kann bis zu 12 Stunden dauern, bis ein Notes Client diese Einstellung übernimmt. Damit die Änderung sofort wirksam wird, verwenden Sie folgenden Befehl an der Domino Konsole:

»tell admin process mailpolicy«

4.4.4. Zeitgesteuerten Versand im Notes Client nutzen

Sofern der Zeitgesteuerte Versand auf einem Domino Server aktiv ist, können Anwender beim Erstellen einer Mail, einer Antwort oder beim Weiterleiten von Mails einen Sendezeitpunkt in der Zustelloptionen festlegen.

Öffnen Sie eine verschickte Mail, welche einen Sendezeitpunkt aufweist.



In gesendeten Mails wird angezeigt, wann die Mail erstellt wurde und wann der Sendezeitpunkt eingeplant war.

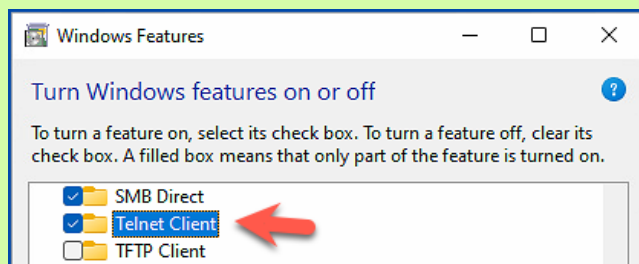
4.5.1.2. Funktionstest

Sie können einen Funktionstest durch den Befehl »telnet« des Betriebssystems durchführen.

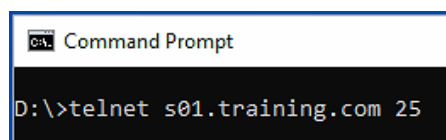
Hinweis

Falls bei Ihrem Windows Betriebssystem der Befehl »telnet« nicht zur Verfügung steht, müssen Sie ihn als »Windows Feature« aktivieren.

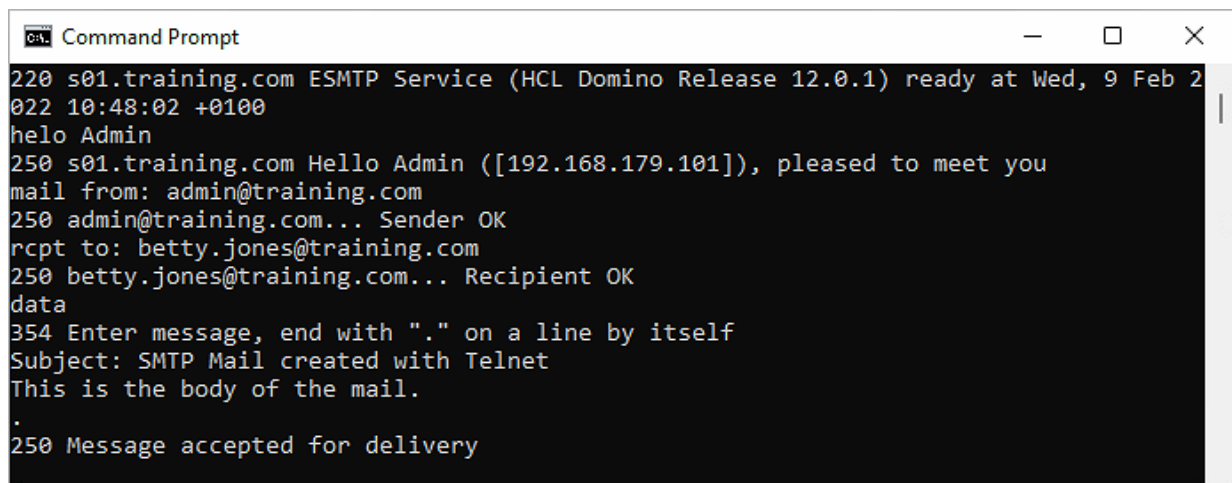
Geben Sie in der Windows Suche »Feature« ein und aktivieren Sie dann den »Telnet Client«.



Öffnen Sie eine Windows Eingabeaufforderung.



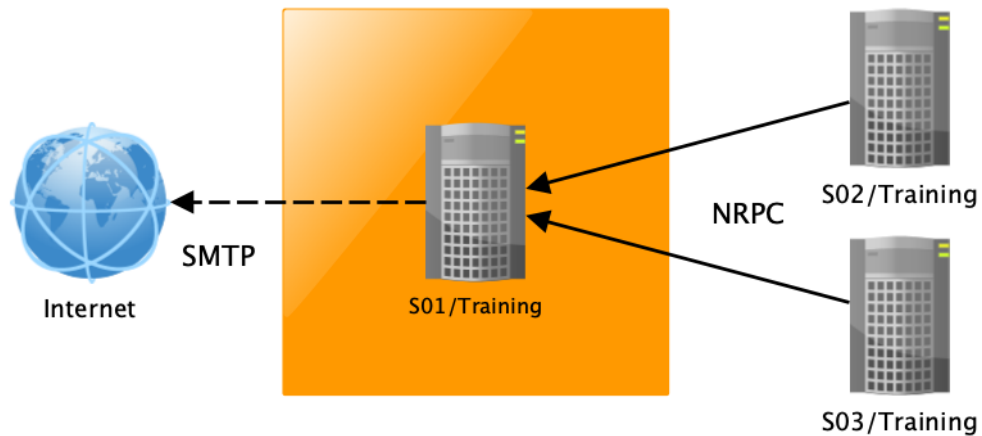
Geben Sie den Befehl »telnet s01.training.com 25« ein. Ein Domino Server agiert beim SMTP Protokoll grundsätzlich auf den Port 25 (dies kann im Serverdokument eingestellt werden).



Hinweis

Die gezeigten Kommandos sind für das SMTP Protokoll dokumentiert und können über eine Internet Suchmaschine leicht gefunden werden.

4.5.3. Ausgehende SMTP Mails beim Einsatz mehrerer Domino Server

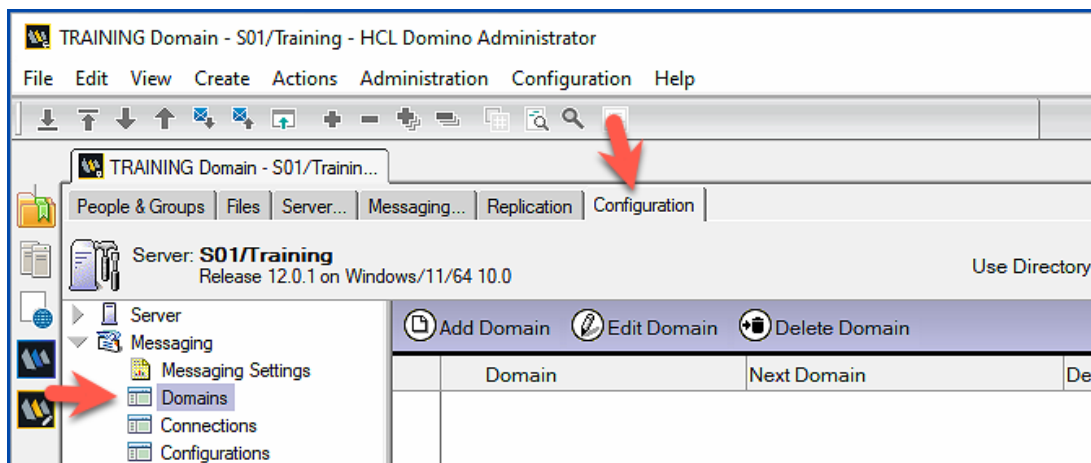


Betreibt ein Unternehmen mehrere Domino Server, so wird das ausgehende SMTP Mailrouting oftmals nur auf einem Domino Server aktiviert (siehe vorheriges Kapitel).

Andere Domino Server transferieren SMTP Mails für die weitere Zustellung zu diesem Domino Server (via Notes NRPC Routing). Zur Konfiguration sind 2 Schritte erforderlich.

4.5.3.1. Domänenendokument

Öffnen Sie im Domino Administrator den Tab »Configuration« und wählen Sie links die Ansicht »Messaging« → »Domains«.



Erstellen Sie ein neues oder öffnen Sie ein existierendes Domänenendokument. Wählen Sie den Tab »Basics«.

2. Domain name

Geben Sie hier den frei wählbaren Namen einer fiktiven Domäne (die Domäne darf nicht als Domino Domäne existieren) ein.

Wenn ein Domino Server eine SMTP Mail erkannt hat, versucht er diese Mail an die hier benannte Domäne zu senden. Dies funktioniert nur, wenn ein korrespondierendes »SMTP Verbindungsdokument« (siehe nächstes Kapitel) existiert.

3. Internet host

Alternativ zur Angabe im Feld »Domain name« kann im Feld »Internet host« ein Hostname oder IP-Adresse angegeben werden.

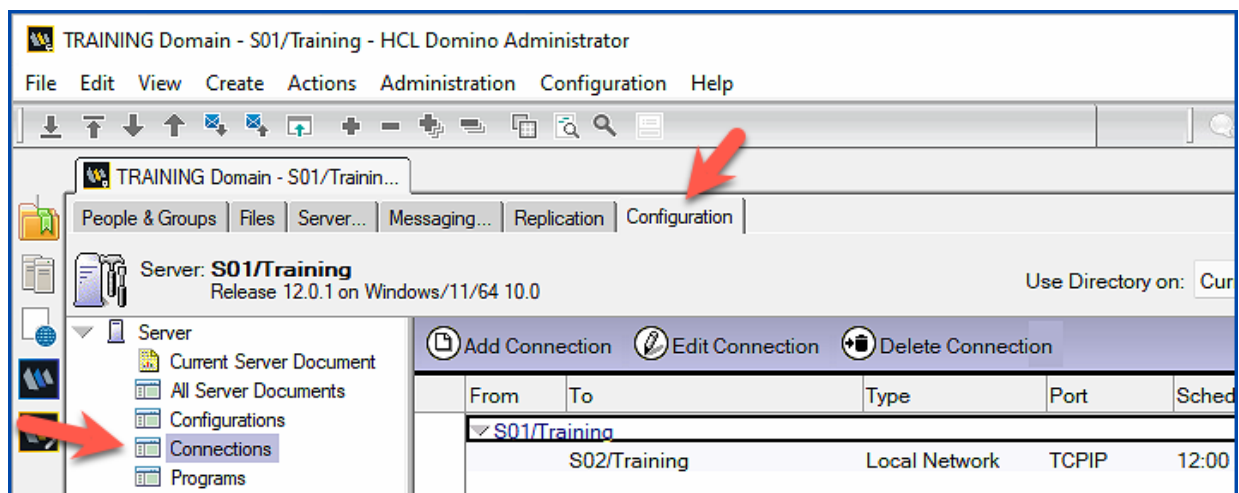
Dies bedeutet aber, dass jeder Domino Server versucht, dorthin seine SMTP Mails zu transferieren. Wenn alle Domino Server ihre SMTP Mails bei einer Firewall abgeben, ist das eine zusätzliche Option.

Speichern und schließen Sie das Dokument.

4.5.3.2. SMTP Verbindungsdokument

Damit die Domino Server wissen, wohin sie eine an die fiktive Domain (siehe Kapitel Domänenendokument) adressierte Mail weiterleiten, wird ein Verbindungsdokument vom Typ »SMTP« benötigt.

Öffnen Sie im Domino Administrator den Tab »Configuration« und wählen Sie links die Ansicht »Server« → »Connections«.

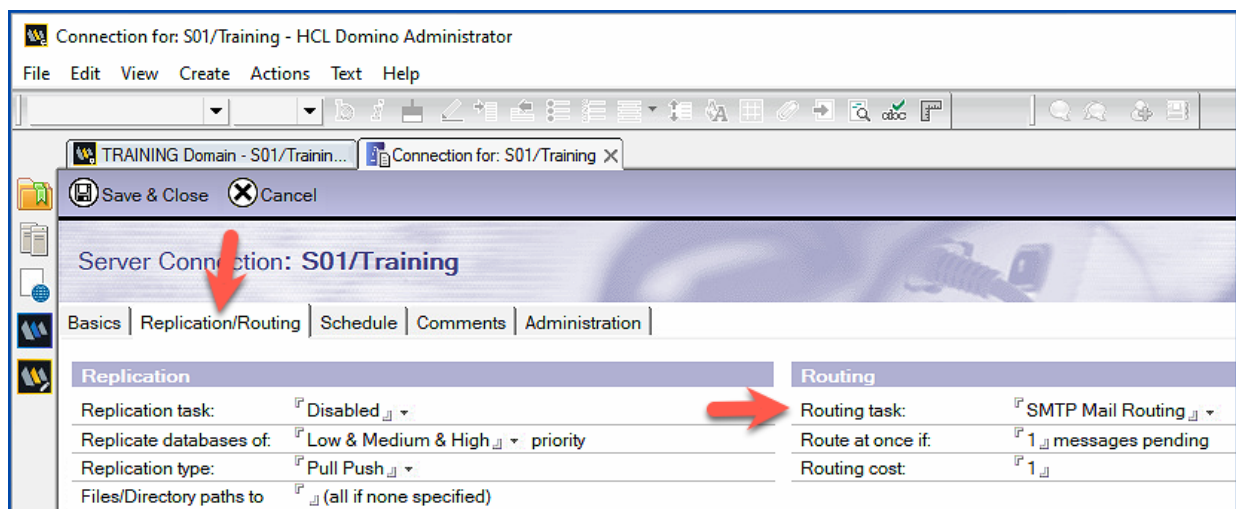


Erstellen Sie ein neues Verbindungsdokument.

Hinweis

Ich werde nachfolgend nur die für das SMTP Routing relevanten Tabs im Verbindungsdokument besprechen. Die anderen Einstellmöglichkeiten (Replikation) sind nicht relevant oder Ihnen schon bekannt.

Tab **Replication/Routing**



Hier ist nur das Feld »Routing Task« relevant. Selektieren Sie dort die Option »SMTP Mail Routing«.

Speichern und schließen Sie das Verbindungsdokument.

Hinweis

Das SMTP Routing in Zusammenspiel aller Domino Server wird erst funktionieren, wenn **alle** beteiligten Domino Server die Dokumente via Replikation erhalten und die Einstellungen übernommen haben.

5.1. ODS (On Disk Structure)

5.1.1. Was ist die ODS?

Die ODS (On Disk Structure) beschreibt den inneren Aufbau und somit die Struktur einer Notes/Domino Anwendung. Über die verschiedenen Domino Versionen wurde die ODS weiterentwickelt und dadurch leistungsfähiger und robuster.

Folgende Aspekte gelten im Bezug auf die ODS:

- **Die ODS hat keinen Bezug zum Design einer Anwendung**
Das Ändern der ODS hat keinen Einfluss auf die in der Anwendung befindlichen Designelemente. Ebenso wirken sich Änderungen am Design nicht auf die ODS einer Anwendung aus. Auch in älteren ODS Versionen können aktuelle Designs gespeichert werden.
- **Die ODS wird nicht repliziert**
Kommen auf verschiedenen Domino Servern unterschiedliche ODS Versionen zum Einsatz, so hat dies keinen Einfluss auf die Replikation einer Anwendung - bei der Replikation werden die Inhalte (Dokumente, Design und ACL) abgeglichen, aber nicht die Struktur der Anwendung geändert.

Was bringt einen der Einsatz einer bestimmten ODS Version?

Als Beispiel möchte ich die Erweiterungen der ODS 51 (Domino Version 8.5) nennen:

- **Komprimierung von Dokumenten**
Dokumente (keine Dateianhänge) können komprimiert werden - somit belegt eine Anwendung weniger Speicherplatz im Dateisystem.
- **Komprimierung von Designelementen**
Die Größe eines leeren Postfachs lag bei Domino Version 8.5 bei ca. 30 MByte. Durch die Komprimierung des Designs kann die Größe um nahezu 50% reduziert werden.
- **Einsatz von DAOS** (Domino Attachment and Object Services)
Redundant in Anwendungen vorhandene Dateianhänge werden konsolidiert - somit nur einmal im Dateisystem gespeichert. Hierdurch kann in der Praxis Speicherplatz eingespart werden. Genauere Informationen finden Sie im Kapitel [5.3. DAOS \(Domino Attachment and Object Services\)](#) auf Seite 120.

Hinweis

Alleine durch die Aktivierung einer höheren ODS Version sind die meisten Erweiterungen nicht automatisch aktiviert.

Die zusätzlich erforderlichen Schritte sind in den folgenden Kapitel beschreiben.