



HCL Domino 12 Systemadministration 2

Weiterführende Themen der Domino Administration

Autor
Manfred Dillmann

Herzlich Willkommen!

Sie sind bereits mit den Grundlagen der HCL Domino Administration vertraut und möchten sich in weiterführende Themen einarbeiten? Dann ist dieses Buch für Sie genau richtig!

- Es handelt sich nicht um eine Einführung in die Domino Administration - die Inhalte aus meinem Buch »HCL Domino 12 Systemadministration 1« oder vergleichbare Kenntnisse werden vorausgesetzt.
- In diesem Buch werden ausgewählte Themen der Domino Administration vorgestellt und in einer Lernumgebung implementiert. Es will kein Ersatz für das Handbuch zur HCL Notes/Domino Software sein - eine vollständige Dokumentation bietet HCL selbst an (siehe Kapitel [9.11. Offizielle HCL Produktdokumentation](#) auf Seite 223).
- Aufgrund seiner Struktur und den detaillierten Anleitungen ist dieses Buch sehr gut als ausführliches Handout für den Einsatz in Seminaren oder für das Selbststudium geeignet.

Ich möchte Sie eindringlich dazu ermutigen, alle vorgestellten Schritte in einer eigenen Lernumgebung nachzuvollziehen. »Learning by doing« ist immer noch eine der besten Möglichkeiten, sich in neue Themen einzuarbeiten.

Ich wünsche Ihnen einen tollen Lernerfolg und ganz viel Freude bei der Nutzung der Software HCL Notes/Domino!

Manfred Dillmann

März 2022



Inhaltsverzeichnis

1. Einführung	8
1.1. Einrichtung der Lernumgebung	9
1.2. Rechtliche Hinweise	10
2. Arbeiten mit mehreren Domänen	11
2.1. Lernumgebung für Kapitel zu diesem Thema	12
2.2. Kommunikation zwischen fremden Domänen	13
2.3. Auswahl der Ebene für die Gegenzertifizierung	14
2.3.1. Gegenzertifikate auf der Organisationsebene (O)	14
2.3.2. Gegenzertifikate auf der Abteilungsebene (OU)	15
2.3.3. Gegenzertifikate auf der Ebene einer ID Datei	16
2.4. Einrichtung der Gegenzertifizierung	17
2.4.1. Verbindungsaufbau zwischen Domino Servern ohne Gegenzertifikat	17
2.4.2. Erstellung des Gegenzertifikates	18
2.4.3. Gegenzertifikat im Domino Directory	21
2.4.4. Erfolgreiche Verbindungsaufnahme mit Gegenzertifikaten	22
2.5. Mailrouting zwischen fremden Domänen	23
2.5.1. Verbindungsdokumente	24
2.5.2. Funktionsprüfung durch Mails	25
2.6. Replikation zwischen fremden Domänen	26
2.6.1. Verteilung der gewünschten Anwendungen	26
2.6.2. ACL Einstellungen	26
2.6.3. Verbindungsdokumente	28
2.7. Domänenendokumente	30
2.7.1. Benachbarte Domänen	30
2.7.2. Domänenendokument für benachbarte Domänen	31
2.7.3. Nicht benachbarte Domänen	32
2.7.4. Domänenendokument für nicht benachbarte Domänen	33
2.8. Aktivierung fremder Directories	35
2.8.1. Replikation	35
2.8.2. Aktivierung via notes.ini	36
2.8.3. Aktivierung via Directory Assistance	36
2.8.4. Dokumente der Directory Assistance Anwendung	38
2.9. Zusammenführung von Domänen/Organisationen	42
2.10. Lernumgebung für alle weiteren Kapitel in diesem Buch	43
3. Anwenderverwaltung	44
3.1. Auflösung von verschachtelten Gruppen	45
3.2. Service generiert Out-of-Office Meldungen	47
3.2.1. Aktivierung im Konfigurationsdokument	47
3.2.2. Geänderte Einstellmöglichkeiten beim Anwender	49
3.3. ID Vault	50
3.3.1. Was ist der ID Vault?	51
3.3.2. Voraussetzungen für den ID Vault	51
3.3.3. Wie funktioniert der ID Vault?	51

3.3.4. Synchronisation der lokalen Anwender IDs	52
3.3.5. Synchronisation von Anwender IDs bei Nutzung mehrerer Arbeitsplätze	52
3.3.6. Wiederherstellung von gelöschten Anwender IDs	52
3.3.7. Einrichtung des ID Vaults	53
3.3.8. Überprüfung der ID Vault Einrichtung	61
3.3.9. Hochladen der Anwender IDs in den ID Vault	61
3.3.10. Nutzung des ID Vaults - Anwender hat sein Passwort vergessen	64
3.3.11. Nutzung des ID Vaults - Anwender ID-Datei wurde gelöscht	66
3.3.12. Nutzung des ID Vaults - Anwender ID-Datei extrahieren	67
3.3.13. Änderungen an der ID Vault Konfiguration durchführen	69
3.3.14. Neuerungen des ID Vaults ab Domino Version 10	72
3.4. Lizenzverfolgung	75
3.4.1. Aktivierung der Lizenzverfolgung	75
3.4.2. Dokumente in der Anwendung userlicenses.nsf	77
3.5. Ab Domino 12: Entitlement Tracking	78
4. Mailrouting	79
4.1. Mehr Details zu Mails in der LOG Anwendung	80
4.1.1. Vorgabe bei einem neuen Domino Server	80
4.1.2. Einstellungen im Konfigurationsdokument	80
4.2. Rückruf von Mails	82
4.2.1. Einstellungen im Konfigurationsdokument	82
4.2.2. Konfiguration durch Policies	83
4.2.3. Rückruf von Mails durch den Anwender	85
4.3. Mailverfolgung	87
4.3.1. Einstellungen im Konfigurationsdokument	87
4.3.2. Nutzung der Mailverfolgung	89
4.3.3. Reports	92
4.4. Zeitgesteuerter Versand von Mails	94
4.4.1. Technische Details	94
4.4.2. Einstellung im Konfigurationsdokument	95
4.4.3. Konfiguration durch Policies	96
4.4.4. Zeitgesteuerten Versand im Notes Client nutzen	97
4.5. SMTP Mailrouting	98
4.5.1. Eingehende SMTP Mails	98
4.5.1.1. Konfiguration im Serverdokument	98
4.5.1.2. Funktionstest	99
4.5.2. Ausgehende SMTP Mails beim Einsatz eines Domino Servers	100
4.5.3. Ausgehene SMTP Mails beim Einsatz mehrerer Domino Server	101
4.5.3.1. Domänendokument	101
4.5.3.2. SMTP Verbindungsdokument	103
5. Anwendungen	106
5.1. ODS (On Disk Structure)	107
5.1.1. Was ist die ODS?	107
5.1.2. ODS Versionen	108
5.1.3. Ändern der ODS	108
5.1.3.1. Eintrag in der Datei notes.ini	108
5.1.3.2. Aktivierung der ODS für bestehende Anwendungen	109
5.1.4. Ändern der ODS für alle Anwendungen	110
5.1.5. Ändern der ODS für Templates und Mailboxen	110

5.1.6. Design- und Nutzdatenkomprimierung.....	110
5.1.6.1. Aktivierung für einzelne Anwendungen.....	111
5.1.6.2. Aktivierung für mehrere Anwendungen.....	111
5.2. Transactional Logging.....	113
5.2.1. Was ist Transactional Logging?.....	113
5.2.2. Aktivierung des Transactional Logging.....	114
5.2.2.1. Aktivierung auf dem Domino Server.....	114
5.2.2.2. Aktivierung für einzelne Anwendungen.....	117
5.2.2.3. Aktivierung für mehrere Anwendungen.....	117
5.2.3. Bedeutung der Database Instance ID (DBIID).....	118
5.3. DAOS (Domino Attachment and Object Services).....	120
5.3.1. Voraussetzungen für die Nutzung von DAOS.....	120
5.3.2. Einsatz von DAOS bei Domino Servern mit unterschiedlichen Versionen.....	120
5.3.3. DAOS aktivieren.....	121
5.3.3.1. Aktivierung auf dem Domino Server.....	121
5.3.3.2. Aktivierung für einzelne Anwendungen.....	123
5.3.3.3. Aktivierung für mehrere Anwendungen.....	123
5.3.4. Reduzierung des erforderlichen Speicherplatzes (Beispiel).....	124
5.3.5. Speichern von älteren Dateianhängen im DAOS Pool.....	125
5.3.6. DAOS Catalog.....	126
5.3.7. DAOS Konsolenbefehle.....	126
5.3.8. DAOS Tipps.....	127
5.3.8.1. Server Mailboxen.....	127
5.3.8.2. Drei .nlo Dateien für den gleichen Dateianhang?.....	127
5.4. Domänenkatalog und Domänensuche.....	129
5.4.1. Die Anwendung Catalog (catalog.nsf).....	129
5.4.2. Aktivieren der Domänensuche auf dem Domino Server.....	130
5.4.3. Aktivierung der Domänensuche in Anwendungen.....	132
5.4.4. Erstellung des Suchindex durch den Domänen Indexer Task.....	133
5.4.5. Problemlösung: Aufnahme von Anwendungen in den Domänensuchindex.....	134
5.4.6. Domänensuche im Notes Client.....	135
5.4.6.1. Arbeitsumgebung anpassen.....	135
5.4.6.2. Durchführen einer Domänensuche.....	136
5.5. Domino Backup & Restore.....	138
5.5.1. Komponenten.....	138
5.5.2. Konfiguration.....	139
5.5.2.1. Global Configuration.....	139
5.5.2.2. Backup Configuration Dokument.....	141
5.5.3. Backup (Beispiel).....	142
5.5.4. Restore einer Anwendung(Beispiel).....	143
6. Monitoring.....	146
6.1. Domino Konsolen.....	147
6.1.1. Globale Einstellungen für Domino Server Konsolen.....	147
6.1.2. Konsole im Domino Administrator.....	149
6.1.3. HCL Domino Console.....	149
6.1.4. Log Anwendung.....	150
6.1.5. Log Filter.....	151
6.2. Monitoring klassisch: Statistik- und Ereignisüberwachung.....	153
6.2.1. Statistikwerte des Domino Servers.....	153
6.2.2. Statistikwerte in der Anwendung Monitoring Results.....	154

6.2.2.1. Starten des Tasks Collect	154
6.2.2.2. Definition des Sammelintervalls	155
6.2.2.3. Erfasste Statistikwerte	157
6.2.3. Überwachung selbst definierter Statistik Grenzwerte	158
6.2.4. Benachrichtigungen durch Event Handler	162
6.2.4.1. Selbst definierte Statistik Grenzwerte	163
6.2.4.2. Weitere Optionen des Event Handlers	166
6.2.5. Überwachung weiterer Ereignisse	169
6.2.6. Zusätzliche Ansichten der Monitoring Configuration	170
6.3. DDM (Domino Domain Monitoring)	171
6.3.1. Was ist Domino Domain Monitoring?	171
6.3.2. DDM Probes	172
6.3.3. DDM Ereignisse	174
6.3.4. DDM Filter	176
6.3.5. Hierarchische Strukturen für das Sammeln der DDM Ereignisse	177
7. Domino Cluster	179
7.1. Übersicht	180
7.1.1. Konzept	180
7.1.2. Voraussetzungen	180
7.1.3. Komponenten	181
7.2. Erstellen eines Clusters / Hinzufügen von Servern zum Cluster	182
7.3. Was ändert sich nach der Einrichtung eines Clusters?	184
7.3.1. Cluster Tasks	184
7.3.2. Cluster Directory (clbdir.nsf)	184
7.3.3. Local Free Time Info (clusbusy.nsf)	185
7.4. Manuelles Verteilen der Anwendungen im Cluster	186
7.5. Test des Clusters	187
7.5.1. Cluster Replicator	187
7.5.2. Cluster Failover	187
7.6. Spezielle Einstellungen / Befehle	188
7.6.1. server_restricted - Manuelles Failover erzwingen	188
7.6.2. server_availability_threshold - Lastverteilung im Cluster	188
7.6.3. rtr_logging - Mehr Details zum Cluster-Replikation	189
7.6.4. crepl - Konsolenbefehl	189
7.7. Neu ab Domino 10: Symmetrischer Cluster	190
7.7.1. Voraussetzungen	190
7.7.2. Funktionsweise	191
7.7.2.1. Fehlende Anwendungen	191
7.7.2.2. Beschädigte Anwendungen	191
7.7.2.3. Aufgaben des Reparatur Dienstes	192
7.7.3. Einrichtung des symmetrischen Clusters	192
7.7.3.1. notes.ini Eintrag	192
7.7.3.2. Tasks	192
7.7.3.3. Cluster Configuration Dokumente	193
7.7.3.4. Test des Symmerischen Clusters	196
7.8. Domino Cluster auflösen	197
7.8.1. Entfernen einzelner oder aller Domino Server	197
7.8.2. Manuelle Aufgaben	198

8. Extras	199
8.1. Domino Server als LDAP Server - Änderung des LDAP Schemas	200
8.2. Automatischer Neustart nach Abstürzen	203
8.3. Domino Server konsolidieren - Stilllegungsanalyse	204
8.4. DCT - Domino Configuration Tuner	206
9. Gut zu wissen	209
9.1. Abkürzung von Befehlen an der Domino Konsole	210
9.2. Dateiname in den Anwendungssymbolen anzeigen	211
9.3. Einsatz von Tools vs. Aktionen	212
9.4. Hilfefunktion zu einzelnen Feldern	214
9.5. Notes Clients schneller machen	215
9.6. Sortierte Liste aller notes.ini Einträge	217
9.7. Spielt es eine Rolle, auf welchem Server ich administriere?	218
9.8. Warum fehlen im Domino Administrator Dokumente?	219
9.9. Warum werden Änderungen nicht sofort übernommen?	220
9.10. Zeilenumbrüche in der Domino Console	222
9.11. Offizielle HCL Produktdokumentation	223

1. Einführung

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.

1.2. Rechtliche Hinweise

Autor

Dipl.-Ing. Manfred Dillmann
<https://www.madicon.de>

Ausgabe

Ausgabe 1 vom 01.03.2022

Copyright – Urheberrechtshinweise

Alle Inhalte dieser Dokumentation, insbesondere Texte, Fotografien und Grafiken, sind urheberrechtlich geschützt. Das Urheberrecht liegt, soweit nicht ausdrücklich anders gekennzeichnet, bei Manfred Dillmann.

Bitte fragen Sie mich, falls Sie die Inhalte dieser Dokumentation verwenden möchten.

© Manfred Dillmann. Alle Rechte vorbehalten.

Hinweise

Der Autor dieser Dokumentation ist nicht verantwortlich für die Funktion oder Fehler der in dieser Dokumentation beschriebenen Software.

Bei der Erstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen - trotzdem können Fehler nicht vollständig ausgeschlossen werden.

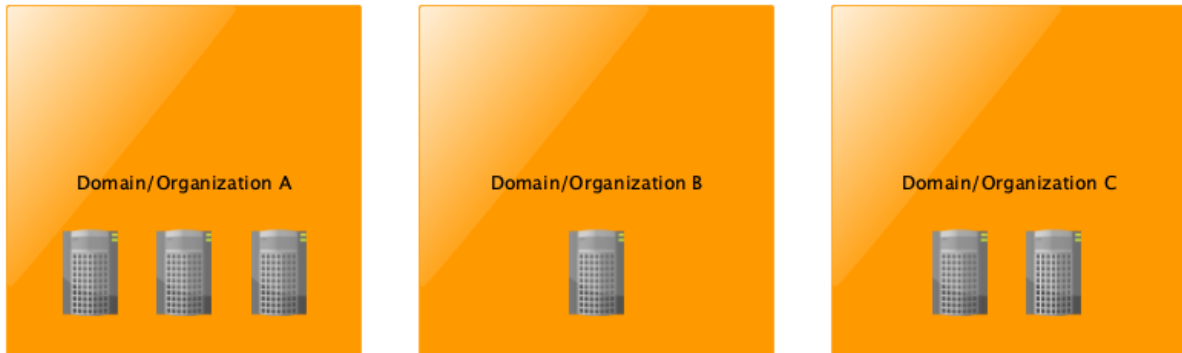
Der Autor kann für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen. Für Verbesserungsvorschläge und Hinweise auf Fehler ist der Autor dankbar.

In dieser Dokumentation werden Warennamen ohne die Gewährleistung der freien Verwendbarkeit und ohne besondere Kennzeichnung benutzt. Es ist jedoch davon auszugehen, dass viele der Warennamen gleichzeitig eingetragene Warenzeichen oder als solche zu betrachten sind.

2. Arbeiten mit mehreren Domänen

2.1. Lernumgebung für Kapitel zu diesem Thema

Um später eine Besonderheit bei den Domänenenddokumenten (Kapitel 2.7. Domänenenddokumente auf Seite 30) ausprobieren zu können, ist eine Umgebung mit 3 Domänen wünschenswert.



Die Anzahl der Domino Server innerhalb einer Domäne spielt keine Rolle - ein einzelner Domino Server wäre ausreichend.

Hinweis

Um die genannte Besonderheit demonstrieren zu können, werde ich die Lernumgebung mit 3 Domino Servern einrichten.

Wir verwenden folgende Namen:

Domino Server	Domäne	Organisation	Administrator
S01	Dom1	Org1	Admin1
S02	Dom2	Org2	Admin2
S03	Dom3	Org3	Admin3

Was ist jetzt zu tun?

- Installation der Domino Server auf jeweils einer Windows Maschine
- Installation des Notes Clients (inkl. Domino Administrator) auf jeweils einer Windows Maschine
- Konfiguration der Domino Server
- Inbetriebnahme der Domino Server
- Inbetriebnahme des Notes Clients

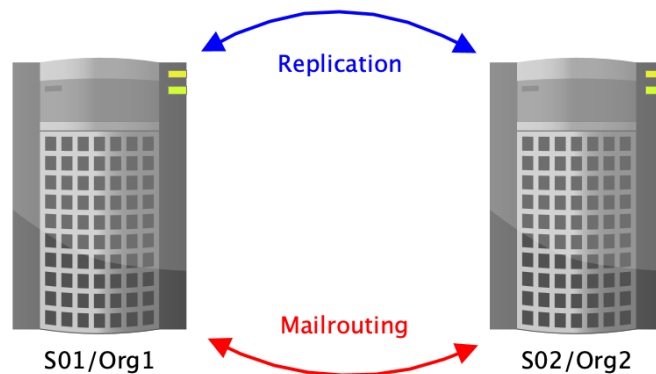
Wichtig

Wir werden gegen Ende des Kapitels »Arbeiten mit mehreren Domänen« die aktuelle Installation zurücksetzen und in den weiteren Kapiteln nur noch mit einer Domäne/Organisation arbeiten.

Erstellen Sie daher **vor** der Konfiguration der Domino Server und der Inbetriebnahme der Notes Clients eine Kopie des jeweiligen Installationsverzeichnisses. Sie ersparen sich so den Zeitaufwand für eine ansonsten erforderliche, neue Installation.

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.

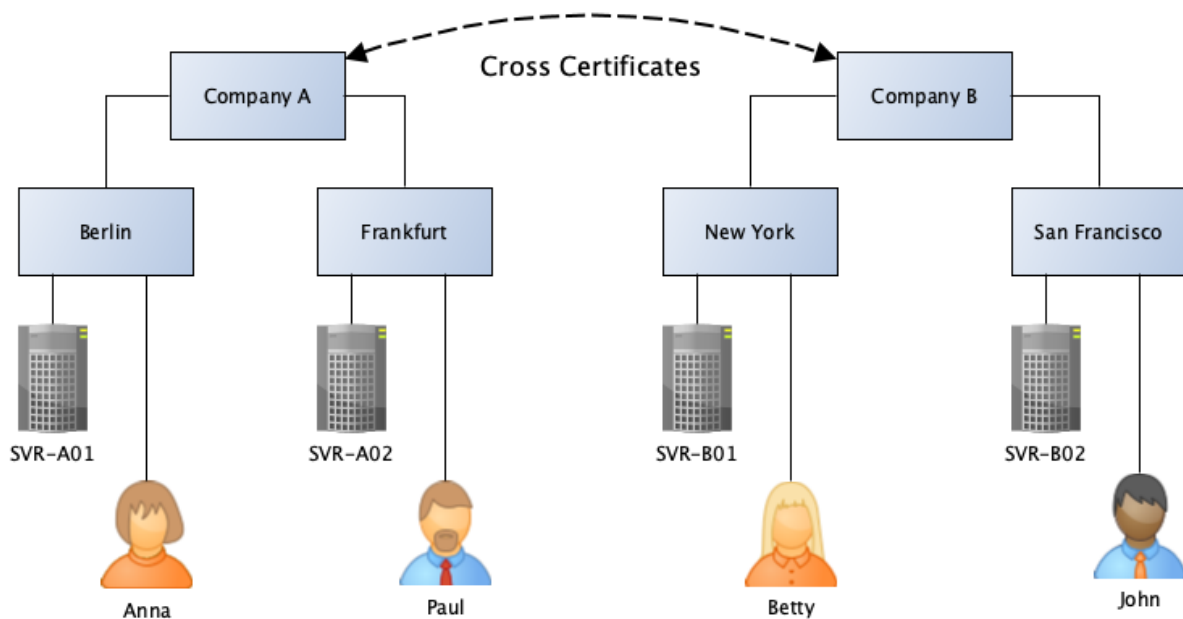
Dies kann auf unterschiedlichen Ebenen (Organisation, Abteilung, Server- oder Personen-ID) erfolgen. Die Details hierzu werden im nächsten Kapitel vorgestellt.

2.3. Auswahl der Ebene für die Gegenzertifizierung

In diesem Kapitel erfahren Sie, auf welcher Ebene (Organisation, Abteilung, Server- oder Personen-ID) eine Gegenzertifizierung möglich ist. Die konkreten Schritte zur Erstellung der Gegenzertifikate werden dann im nächsten Kapitel gezeigt.

Nachfolgend werden 3 Beispiele vorgestellt, welche eine Gegenzertifizierung jeweils auf einer der Ebenen zeigen. Beliebige weitere Varianten (z.B. Server-ID wird mit der »cert.id« gegenzertifiziert) sind möglich.

2.3.1. Gegenzertifikate auf der Organisationsebene (O)



Hier wird die Gegenzertifizierung auf der Ebene der **Organisation** durchgeführt.

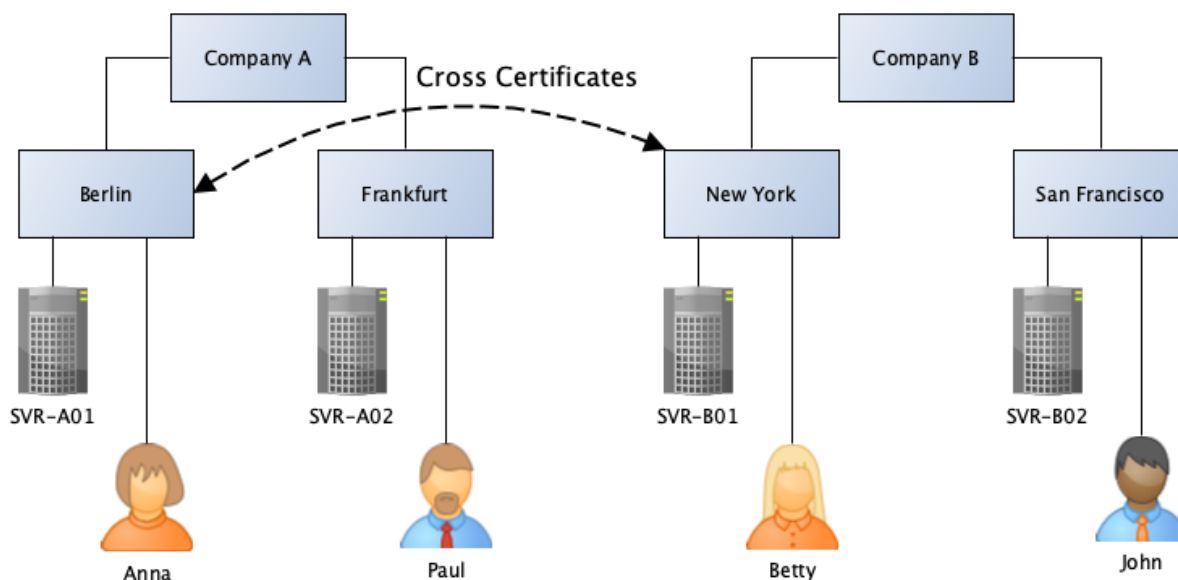
Dies bedeutet, dass sich die Organisationen vollständig vertrauen. Jeder Domino Server von Company A (SVR-A01, SVR-A02) kann mit jedem Domino Server von Company B (SVR-B01, SVR-B02) kommunizieren. Sogar jeder Mitarbeiter kann auf jeden Domino Server der Gegenseite zugreifen.

Man muss sich bei einer Gegenzertifizierung auf der Ebene der Organisation fragen, ob man die zuvor existierende Trennung zwischen den Organisationen in der Praxis soweit aufheben möchte. Wenn zwei Firmen fusionieren und damit eine Einheit darstellen, ist eine Gegenzertifizierung auf dieser Ebene denkbar, ansonsten ist Vorsicht geboten.

Fazit

Möchte man mit einem Kooperationspartner Informationen via Replikation oder Mailrouting austauschen, erscheint die Gegenzertifizierung auf Organisationsebene zu hoch. In diesem Fall empfiehlt sich die Gegenzertifizierung höchstens auf der OU Ebene oder - besser, weil sicherer - auf der Ebene einzelner Server IDs.

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.

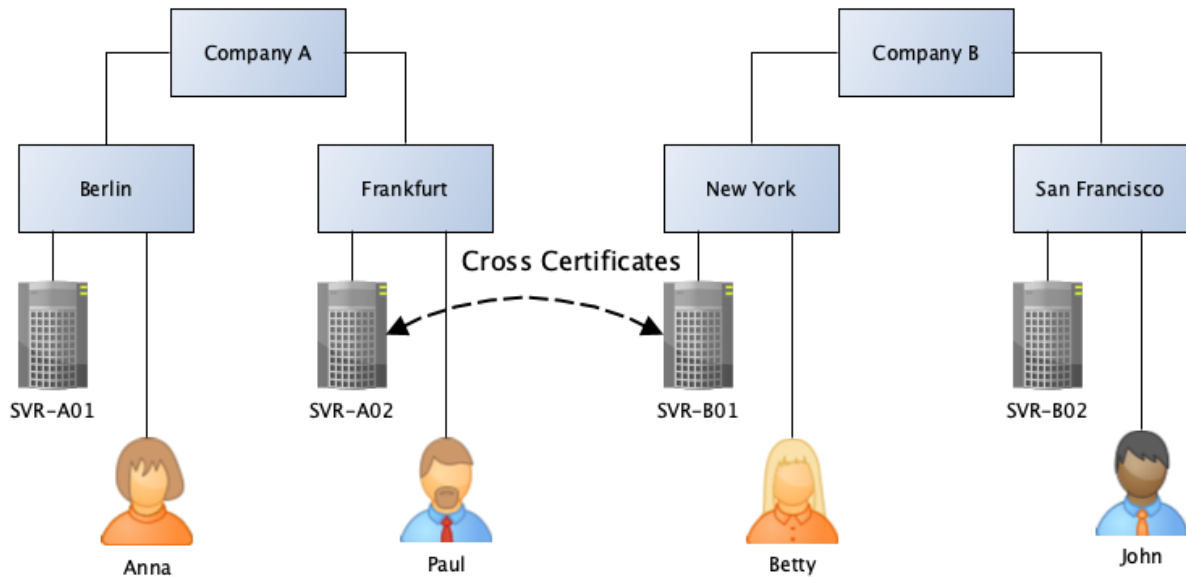
Ebenso müssen die ACLs aller Anwendungen sorgfältig gepflegt werden, damit die Mitarbeiter der fremden Unternehmung nicht unkontrolliert auf nicht für sie vorgesehene Informationen zugreifen können.

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.

2.3.3. Gegenzertifikate auf der Ebene einer ID Datei



Hier erfolgt die Gegenzertifizierung auf der Ebene von **Server ID Dateien**.

Im Beispiel kann nur der Domino Server SVR-A02 am Standort Frankfurt mit dem Domino Server SVR-B01 in New York kommunizieren. Dies sieht auf den ersten Blick nach einer massiven Einschränkung der Kommunikationsmöglichkeiten aus. Da aber der gesamte Informationsfluss (Replikation, Mailrouting) in einer Notes/Domino Umgebung immer über Domino Server erfolgt, ist dies keine Einschränkung.

Wenn nur die Server aus Frankfurt und New York miteinander kommunizieren, kann die zwischen den Firmen ausgetauschte Information innerhalb der jeweiligen Firma ebenfalls via Replikation weitergegeben werden.

Fazit

Erfolgt die Gegenzertifizierung auf der Ebene von Server ID Dateien, ist genau bekannt, wer mit wem kommuniziert. Es wird nach diesem Konzept nicht passieren, dass unkontrolliert fremde Anwender auf die eigenen Domino Server zugreifen.

Auf der anderen Seite gibt es keine Einschränkung bei der Verteilung von Informationen und man weiß zu jedem Zeitpunkt, über welche Wege sie ausgetauscht werden.

Aus diesen Gründen erscheinen die Gegenzertifikate auf der Ebene der ID Dateien die erste Wahl für sicherheitsbewusste Administratoren zu sein.

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.
  
```

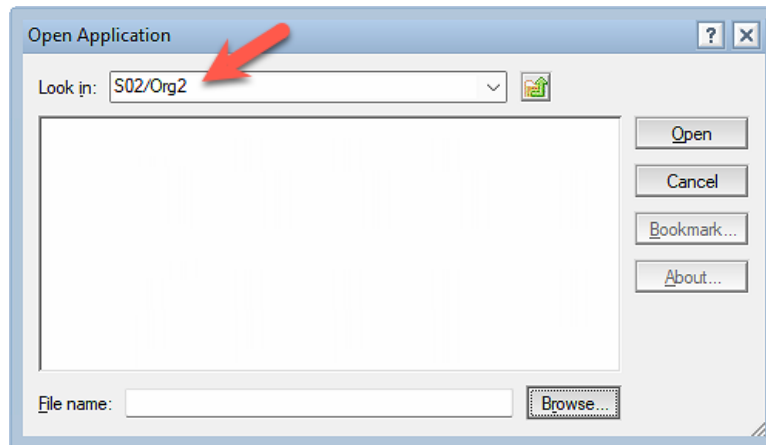
Eine Kommunikation zwischen Domino Servern aus **unterschiedlichen** Organisationen ist grundsätzlich nicht möglich. Versucht man, mit dem Konsolenbefehl »trace« eine Verbindung aufzubauen (eine Erreichbarkeit über das Netzwerk vorausgesetzt), so erscheinen die im Screenshot gezeigten Fehlermeldungen.

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.

2.4.2. Erstellung des Gegenzertifikates

Wie schon erwähnt, werden wir die Gegenzertifikate nicht durch den Austausch von Dateien erstellen. Es geht einfacher und schneller durch folgende Vorgehensweise.

Im Domino Administrator (welcher für »Org1« genutzt wird) wählen Sie den Menüpunkt »File« → »Application« → »Open« (Hotkey: Ctrl + O).

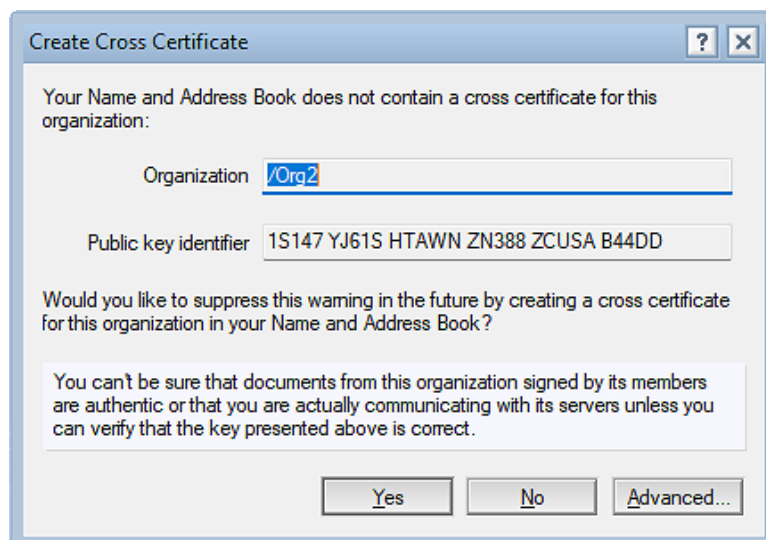


Im oberen Eingabefeld »Look in« geben Sie den Namen des Domino Servers ein, auf welchen Sie zugreifen möchten.

Hinweis

Hierzu muss eine Erreichbarkeit über das Netzwerk gegeben sein. Die Namensauflösung muss funktionieren und in der Firewall muss auf der Gegenseite der TCP Port 1352 geöffnet sein.

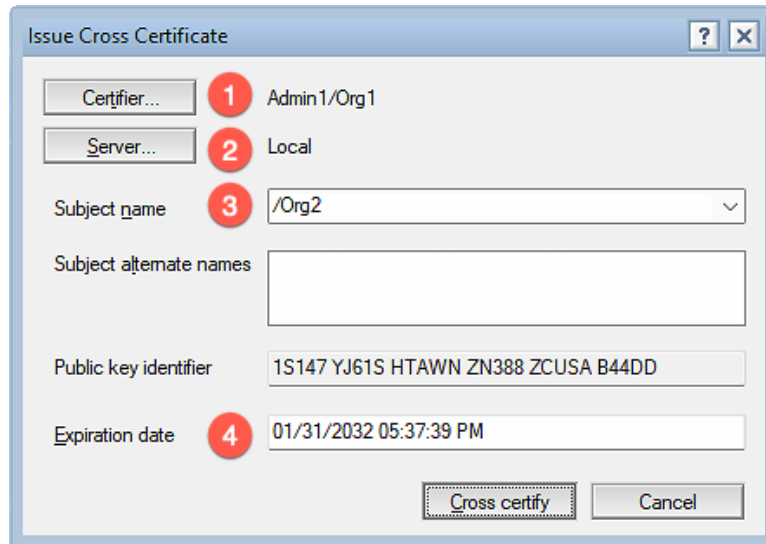
Bestätigen Sie den Dialog mit »Open«.



Klicken Sie hier **nicht** auf die Schaltfläche »Yes«. Das Ergebnis wäre ein Gegenzertifikat, welches in der lokalen Anwendung Kontakte (»names.nsf«) des Notes Clients gespeichert würde.

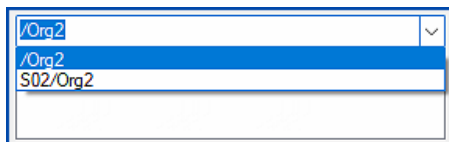
Dieses Gegenzertifikat würde bestätigen, dass die aktuell genutzte Anwender ID der Organisation »Org2« vertraut (der Notes Client akzeptiert Verbindungen zur Organisation »Org2«).

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



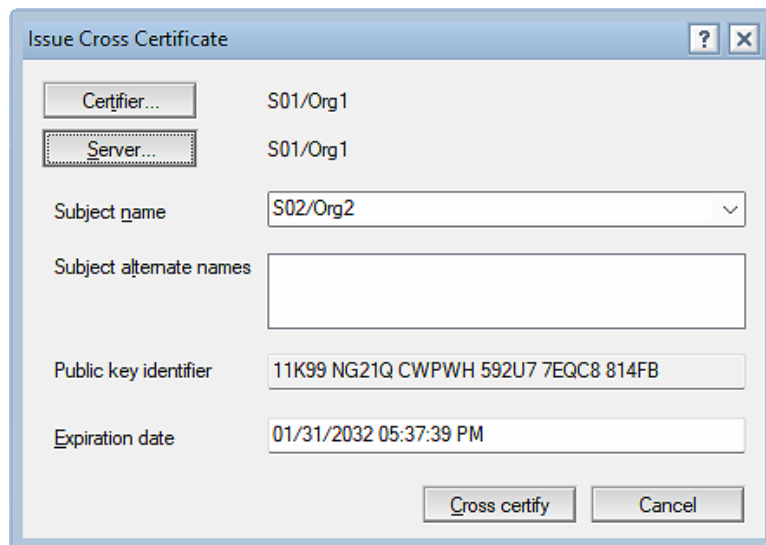
Das sind die Vorgaben in diesem Dialog. Hier **nicht** sofort auf die Schaltfläche »Cross certify« klicken! Diese Vorgaben sind **nicht** für die Erstellung des Gegenzertifikates für die Domino Server geeignet.

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.



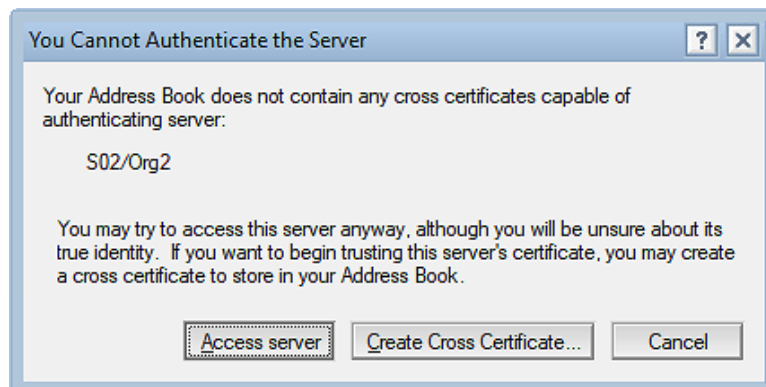
4. Wie lange soll das Gegenzertifikat gültig sein? Voreingestellt ist eine Gültigkeitsdauer von 10 Jahren. Da man später durch das Löschen des Gegenzertifikats die Verbindung zur Gegenseite jederzeit beenden kann, können hier problemlos längere Laufzeiten angegeben werden.

Nach der Änderung der Parameter sieht der Dialog so aus:

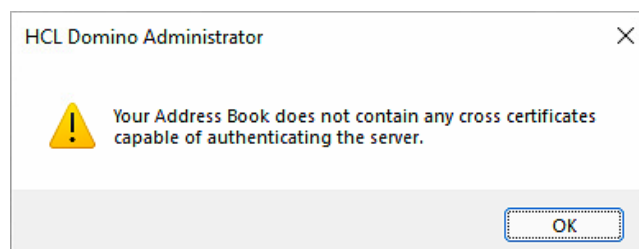


Mit diesen Einstellungen vertraut der eigene Domino Server »S01/Org1« dem fremden Domino Server »S02/Org2« und das Gegenzertifikat ist bis zum 31.01.2032 gültig.

Bestätigen Sie diesen Dialog mit der Schaltfläche »Cross certify«. Mit hoher Wahrscheinlichkeit erscheint folgender Dialog.



Der Domino Administrator möchte Sie darauf hinweisen, dass (aus seiner Sicht) noch kein Gegenzertifikat in der lokalen »names.nsf« gespeichert ist. Da wir ein solches Zertifikat nicht benötigen, können Sie diesen Dialog über die Schaltfläche »Cancel« schließen.



Ein weiterer Hinweis, dass in der Anwendung »names.nsf« des Notes Clients kein Gegenzertifikat vorhanden ist.

Fazit

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

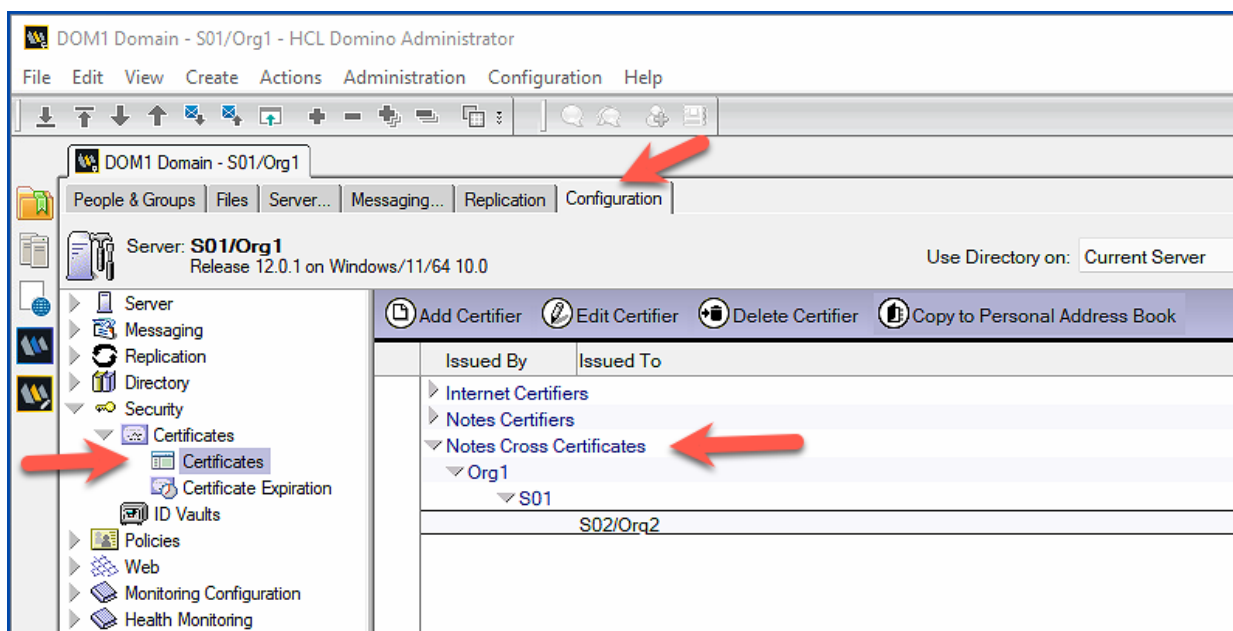
2.4.3. Gegenzertifikat im Domino Directory

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.

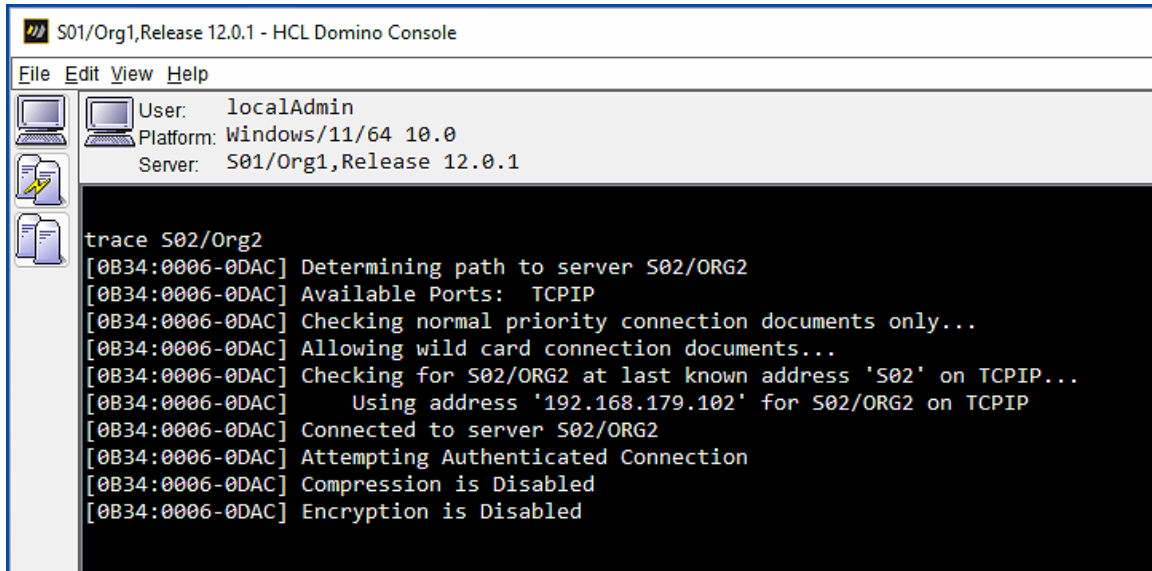
Hinweis

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

2.4.4. Erfolgreiche Verbindungsaufnahme mit Gegenzertifikaten

Sofern alle Schritte korrekt ausgeführt wurden, steht einer Verbindungsaufnahme der beteiligten Server nichts mehr im Wege.

An der Domino Konsole sieht der Verbindungsaufbau mittels »trace« Befehl so aus:



```
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

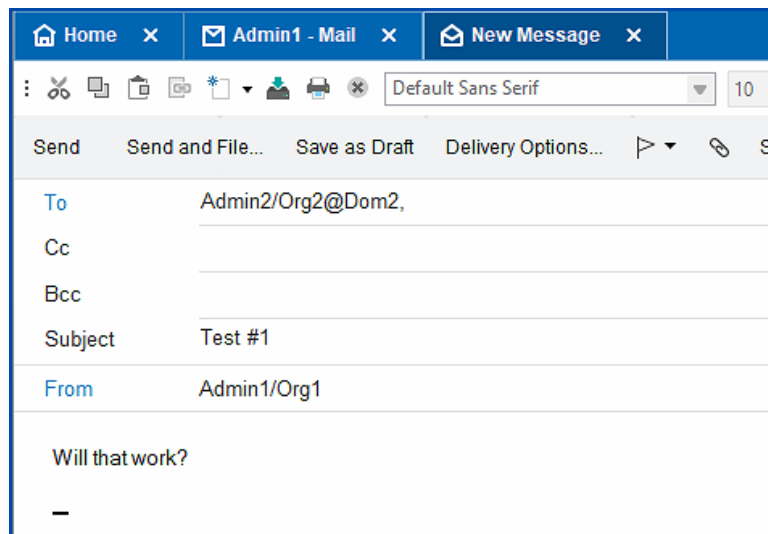
trace S02/Org2
[0B34:0006-0DAC] Determining path to server S02/ORG2
[0B34:0006-0DAC] Available Ports: TCPIP
[0B34:0006-0DAC] Checking normal priority connection documents only...
[0B34:0006-0DAC] Allowing wild card connection documents...
[0B34:0006-0DAC] Checking for S02/ORG2 at last known address 'S02' 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] Compression is Disabled
[0B34:0006-0DAC] Encryption is Disabled
```

Es gibt keine Fehlermeldungen, die Authentifizierung erfolgt korrekt und die beteiligten Server können ab diesem Zeitpunkt die Replikation und das Mailrouting einwandfrei miteinander ausführen.

Welche zusätzlichen Schritte zur Konfiguration von Replikation und Mailrouting erforderlich sind, erfahren Sie in den folgenden Kapiteln.

2.5. Mailrouting zwischen fremden Domänen

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

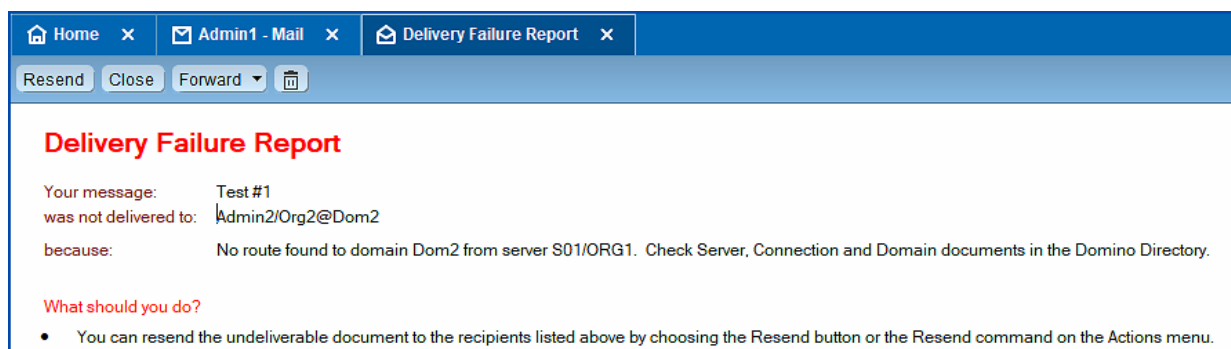


Eine Mail wird von »Admin1/Org1@Dom1« an die Person »Admin2/Org2@Dom2« gesendet.

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.

2.5.1. Verbindungsdokumente

Erstellen Sie ein neues Verbindungsdokument.

Server Connection: S01/Org1 to S02/Org2

Basics | Replication/Routing | Schedule | Comments | Administration

Basics	
Connection type:	Local Area Network
Source server:	S01/Org1
Source domain:	Dom1
Use the port(s):	TCPIP
Usage priority:	Normal
Destination server:	S02/Org2
Destination domain:	Dom2
Optional network address:	

Choose Ports...

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

Hinweis

Vielleicht haben Sie sich bislang auch schon gefragt, warum in den Verbindungsdokumenten immer die Quell- und Zieldomäne angegeben wird - diese ist ja bei intern gesendeten Mails immer gleich.

Sobald aber Mails via NRPC zu fremde Domänen gesendet werden, wissen die eigenen Domino Server durch die Angabe im Feld »Destination domain«, welcher Domino Server sich um den Transfer kümmern. Hat man mehrere Domino Server im Einsatz (in mehreren benannten Netzwerken), liefern diese alle an die fremde Domäne gerichteten Mails beim im Feld »Source server« ausgewählten Domino Server ab.

Save & Close Cancel

Server Connection: S01/Org1 to S02/Org2

Basics | Replication/Routing | Schedule | Comments | Administration

Replication	Routing
Replication task:	Routing task:
Replicate databases of:	Route at once if:
Replication type:	Routing cost:
Files/Directory paths to replicate:	Router type:
Files/Directory paths to NOT replicate:	
Replication time limit:	

Die Replikation ist auf dem Tab »Replication/Routing« deaktiviert und die Einstellungen im Abschnitt »Routing« entsprechen den Vorgaben.

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
```