

Christian Buchacher

HCL Domino 11-Administration

Christian Buchacher

HCL Domino 11-Administration für Windows

1. Auflage, August 2021 (V5)

© Christian Buchacher

Goltzgasse 2–4/13

1190 Wien

Österreich

E-Mail: fachbuch@cob.at

Cover: Agnes Schubert, www.agneschubert.at

Korrekturat: Dorrit Korger, dorrit.korger@icloud.com

Diese Publikation ist urheberrechtlich geschützt. Weiterverarbeitung, Vervielfältigung und öffentliche Wiedergabe sind ausdrücklich untersagt und können zivil- und/oder strafrechtliche Folgen nach sich ziehen.

Trotz der Sorgfalt, mit der die Informationen in diesem Buch erarbeitet wurden, sind Fehler nicht auszuschließen. Der Autor kann für Folgen, die auf fehlerhafte Angaben zurückgehen, weder eine juristische Verantwortung noch irgendeine Haftung übernehmen. Für Hinweise auf Fehler ist der Autor jedoch dankbar.

Die in diesem Werk wiedergegebenen Gebrauchsnamen, Handelsnamen und Warenzeichen können auch ohne besondere Kennzeichnung Marken sein und als solche den gesetzlichen Bestimmungen unterliegen.

Aus Gründen der besseren Lesbarkeit wird in diesem Buch auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Inhalt

1. Vorwort	19
2. Über dieses Buch	21
2.1. An wen richtet sich dieses Buch?	21
2.2. Was dieses Buch NICHT ist	21
2.3. Welche Voraussetzungen SIE mitbringen müssen	21
2.4. Ein paar Worte zur Sprache	22
2.5. Gerne höre ich von Ihnen	22
3. Architektur und Konzepte	23
3.1. Was ist HCL Notes und Domino?	23
3.1.1. Merkmale im Detail	23
3.2. Von Zertifizierern und hierarchischen Namen	25
3.2.1. Am Anfang war das Zertifikat	25
3.2.2. Hierarchische Namen	25
3.2.3. Arten von ID-Dateien	26
3.2.4. Soll ich Organisationseinheiten verwenden?	27
3.2.5. Querzulassung	28
3.2.6. Soll ich Ländercodes verwenden?	28
3.3. Das Domino-Verzeichnis	28
3.4. Von Domänen und Netzwerken	29
3.4.1. Die Domino-Domäne	29
3.4.2. Benannte Notes-Netzwerke	30
3.4.3. Verbindungsdokumente	30
4. Serverinstallation	31
4.1. Voraussetzungen für die Installation	31
4.1.1. Unterstützte Betriebssysteme	31
4.1.2. Speicher	32
4.1.3. Wie viele »Platten« braucht Domino?	32
4.1.4. DAS, NAS oder SAN: Interessiert das Domino?	32
4.2. Einen Domino-Server installieren	33
4.2.1. Übersicht	33
4.2.2. Vorgangsweise	34
4.3. Fehlerkorrekturen einspielen	40
4.3.1. A Notes/Domino related process is still running ...	41
4.3.2. Ein Fix Pack entfernen	41
4.4. Sprachen installieren	41

4.4.1. Alternativen zum Language Pack	42
4.4.2. Installation des Sprachpakets am Server	42
4.5. Einen ersten Domino-Server einrichten	50
4.5.1. Voraussetzungen	50
4.5.2. Schritt-für-Schritt-Anleitung	50
4.5.3. Über den Konfigurationsablauf	54
4.6. Einen Domino-Server starten und beenden	55
4.6.1. Einen Domino-Server als Applikation starten	56
4.6.2. Einen Domino-Server als Dienst starten	57
4.6.3. Server-Controller und Domino-Console	59
4.6.4. Der Domino-Server startet nicht als Dienst	60
4.6.5. Verwendung einer Community-Server-Lizenz	61
4.7. Domino-Ports in der Windows-Firewall öffnen	61
4.8. Einen Domino-Administrator installieren	64
4.8.1. Den Admin-Client einrichten	69
4.8.2. Administrationsvorgaben setzen	71
4.9. Einen zusätzlichen Domino-Server einrichten	74
4.9.1. Wozu zusätzliche Server?	74
4.9.2. Einen zusätzlichen Server registrieren	75
4.9.3. Einen zusätzlichen Domino-Server konfigurieren	77
4.10. Eine ältere Domino-Version aktualisieren	80
4.10.1. Eine ältere Version auf 9.0.1 aktualisieren	80
4.10.2. Aktualisieren von Domino 9.x (oder höher) auf Version 11.x	81
4.10.3. Das Ausrollen der neuen Version planen	82
4.11. Domino und AntiVirus	84
5. Serverkonfiguration	85
5.1. Serverkonsolen	85
5.1.1. Die direkte Serverkonsole	85
5.1.2. Die Entfernte Konsole im Domino-Administrator	86
5.1.3. Die Domino-Console	88
5.1.4. Konsolen im Domino-Webadministrator	90
5.1.5. Wichtige Befehle für alle Konsolen	90
5.1.6. Thread-ID	91
5.2. Die Datei notes.ini	91
5.2.1. Die Datei notes.ini direkt bearbeiten	91
5.2.2. Über das Konfigurationsdokument in die notes.ini schreiben	92
5.2.3. Über die Serverkonsole in die notes.ini schreiben	93
5.2.4. Im Domino-Webadministrator in die notes.ini schreiben	93
5.3. Domino-Serverprogramme	94
5.3.1. Programme über die Serverkonsole starten	95

5.3.2. Programme auf Betriebssystemebene starten	96
5.3.3. Programme über die Datei notes.ini starten	96
5.3.4. Programme über Programmdokumente starten	97
5.4. Konfigurationsdokumente	99
5.4.1. Eine Vorgabekonfiguration erstellen	100
5.4.2. Gruppenkonfigurationsdokumente erstellen	100
5.4.3. Individuelle Konfigurationsdokumente erstellen	101
5.5. Datenbankcache und Transaktionsprotokoll	101
5.5.1. Der Datenbankcache	101
5.5.2. Die Transaktionsprotokollierung	103
5.6. Die verschiedenen Domino-Administratoren	108
5.6.1. Administratoren	109
5.6.2. Datenbankadministratoren	109
5.6.3. Administratoren mit voller Remote-Konsolen-Berechtigung	109
5.6.4. Leseberechtigte Administratoren	109
5.6.5. Systemadministratoren	110
5.6.6. Eingeschränkte Systemadministratoren	110
5.6.7. Sonderfall Administratoren mit voller Berechtigung	110
5.7. Der Administrationsprozess	112
5.7.1. Die Datenbank für Administrationsanforderungen	113
5.7.2. Administrationsserver	113
5.7.3. Planungstypen	114
5.7.4. Das Zertifizierungsprotokoll	115
5.7.5. Den Administrationsprozess einrichten	115
5.8. Domino-Server neu installieren oder verschieben	119
5.8.1. Den Domino-Server auf derselben Maschine neu installieren	119
5.8.2. Den Domino-Server auf eine andere Maschine verschieben	119
5.8.3. Verschieben auf Betriebssystemebene	119
5.8.4. Verschieben via Replikation	120
6. Benutzerverwaltung	123
6.1. Richtlinien	123
6.1.1. Überblick	123
6.1.2. Organisationsbezogene Richtlinien	124
6.1.3. Explizite Richtlinien	125
6.1.4. Wirksame Richtlinie	126
6.1.5. Das Ausrollen von Richtlinien planen	127
6.1.6. Eine organisationsbezogene Richtlinie erstellen	127
6.1.7. Hinweise zu Richtlinieneinstellungen	128
6.1.8. Die Registrierungseinstellung	131
6.1.9. Übersicht über weitere Richtlinieneinstellungen	134

6.2. Der ID-Vault	137
6.2.1. Einen ID-Vault einrichten	138
6.2.2. Die ID-Synchronisierung überwachen	146
6.2.3. Den ID-Vault durchsuchen	147
6.3. Eine serverbasierende Zulassungsstelle einrichten	149
6.3.1. Einen Notes-Zertifizierer migrieren	149
6.4. Notes-Benutzer anlegen	152
6.4.1. Benutzer einzeln registrieren	152
6.4.2. Benutzer aus einer Datei registrieren	156
6.5. Roaming-Benutzer	157
6.5.1. Roaming aktivieren	157
6.5.2. Roaming deaktivieren	160
6.6. Notes-ID-Kennwörter zurücksetzen	160
6.6.1. Kennwörter über den Domino-Administrator zurücksetzen	161
6.6.2. Kennwörter über eine Self-Service-Anwendung zurücksetzen	162
6.7. Notes-IDs verlängern	163
6.7.1. Verlängern über den Administrationsprozess	163
6.7.2. Verlängern der ID-Datei	164
6.7.3. Die Administrator-ID ist abgelaufen	165
6.8. Benutzer umbenennen	165
6.8.1. Voraussetzungen	166
6.8.2. Ändern des Allgemeinen Namens	166
6.8.3. Das Tempo der Umbenennung steuern	168
6.8.4. Wechsel zu neuem Zertifizierer anfordern	169
6.9. Benutzer verschieben	171
6.10. Benutzer sperren	172
6.11. Benutzer löschen	173
6.12. Gruppen verwalten	175
6.12.1. Gruppentypen	176
6.12.2. Wer darf Gruppen erstellen?	176
6.12.3. Gruppen erstellen	176
6.12.4. Automatisch befüllte Gruppen	177
6.12.5. Gruppen delegieren	178
6.12.6. Gruppen umbenennen	178
6.12.7. Gruppen löschen	178
6.12.8. Geschützte Gruppen (Protected Groups)	178
6.12.9. Das Werkzeug Gruppen verwalten	179
6.13. Externe Verzeichnisse einbinden	180
6.13.1. Eine Verzeichnishilfe-Datenbank erstellen	180
6.13.2. Zusätzliche Domino-Verzeichnisse einbinden	182
6.13.3. LDAP-Verzeichnisse einbinden	184

7. Kalender und Zeitplanung	189
7.1. Übersicht	189
7.2. Die Zeitplanungsdatenbank	190
7.2.1. Zeiten innerhalb derselben Domäne abfragen	190
7.2.2. Zeiten zwischen verschiedenen Domänen abfragen	191
7.2.3. Zeitplanung zwischen Domänen ermöglichen	191
7.2.4. Serverbefehle zur Wartung der Zeitplanungsdatenbank	191
7.3. Die Anwendung Ressourcenreservierung	192
7.3.1. Die Datenbank erstellen	193
7.3.2. Ein Standortprofil erstellen	194
7.3.3. Eine Ressource erstellen	194
7.3.4. Ändern und Löschen von Ressourcen	195
7.3.5. Die Agenten in der Ressourcenreservierung aktivieren	196
7.3.6. Die Anwendung Ressourcenreservierung verschieben	196
7.3.7. Detaillierte Planungsinformationen extrahieren	198
7.4. Feiertage verwalten	199
7.4.1. Die Feiertage aktualisieren	199
8. Mail-Routing	201
8.1. Die Mailkomponenten	201
8.1.1. Mailer	201
8.1.2. Mailbox	202
8.1.3. Router	202
8.1.4. SMTP-Server	202
8.1.5. Wo Mailadressen hinterlegt sind	202
8.2. Notes-Mail	203
8.2.1. Der Mailer	203
8.2.2. Der Router	203
8.2.3. Benannte Notes-Netzwerke	204
8.3. Internet-Mail	208
8.3.1. Das SMTP-Protokoll	208
8.3.2. Internet-Mailrouting aktivieren	209
8.3.3. Den SMTP-Server starten	210
8.3.4. Internetdomänen zulassen	211
8.3.5. Die Absenderadresse konfigurieren	213
8.3.6. HTML-Mails ermöglichen	214
8.3.7. Der SMTP-Server lässt grüßen	215
8.3.8. Auf Spurensuche im MIME-Header	216
8.3.9. TLS für SMTP aktivieren	217
8.4. Weitere Maileinstellungen	219
8.4.1. Anzahl Mailboxen	219

8.4.2. Transaktionsprotokollierung für Mailboxen abschalten	219
8.4.3. Adresssuche	220
8.4.4. Relay-Host	220
8.4.5. Smart-Host	221
8.4.6. Absenderadresse aus dem Personendokument erzwingen	221
8.5. Mail-In-Datenbanken	222
8.6. Sinnvolle Mailvorgaben setzen	223
8.6.1. Papierkorb	223
8.6.2. Einheitliche Sortierung für Ordner und Ansichten	223
8.6.3. Umgang mit Empfangsbestätigungen	224
8.7. Beschränkungen beim Senden von Mails setzen	225
8.7.1. Vorgangsweise	226
8.8. Geplante Nachrichten versenden	227
8.8.1. Geplante Nachrichten serverweit aktivieren	228
8.8.2. Geplante Nachrichten für bestimmte Benutzer aktivieren	228
8.8.3. Zustellungszeit einer geplanten Nachricht ändern	229
8.8.4. Überwachen geplanter Nachrichten	230
8.9. Auf Zustellungsfehler reagieren	230
8.10. Auf unzustellbare Nachrichten reagieren	231
8.10.1. Manuelle Verarbeitung nicht zustellbarer Mails	231
8.10.2. Automatische Verarbeitung nicht zustellbarer Mails	232
8.10.3. Verarbeitung von nicht zustellbaren Mails überwachen	233
8.11. Die Größen von Maildatenbanken beschränken	233
8.11.1. Was passiert beim Überschreiten der Maximalgröße?	234
8.11.2. Wann werden Größenbeschränkungen überprüft?	234
8.11.3. Mailzustellung bei Überschreiten der Maximalgröße	234
8.11.4. Größenbeschränkungen ändern/aufheben	235
8.12. Abwesenheitsnachrichten einrichten	236
8.12.1. Übersicht	236
8.12.2. Den Abwesenheitstyp konfigurieren	237
8.12.3. Setzen von Rechten für Abwesenheitsagenten	237
8.13. Einen Verzeichniskatalog erstellen	238
8.13.1. Einen Verzeichniskatalog erstellen	238
8.13.2. Einen Verzeichniskatalog einrichten	238
8.13.3. Befüllen des Verzeichniskatalogs	240
8.13.4. Verteilen des Verzeichniskatalogs an Notes-Clients	240
9. Datenbanken verwalten	243
9.1. Übersicht	243
9.2. Datenbanken organisieren	244
9.3. Neue Datenbanken erstellen	245

9.3.1. Eine Anwendung basierend auf einer Schablone erstellen	245
9.3.2. Eine Anwendung basierend auf einer Kopie erstellen	246
9.4. Das Dateiformat	246
9.4.1. Warum Sie ODS 53 aktivieren sollten	247
9.4.2. Das Dateiformat am Server aktualisieren	248
9.4.3. Das Dateiformat am Client ändern	250
9.4.4. Das Dateiformat mit der Dateieindung steuern	251
9.5. Komprimieren von Datenbanken	252
9.5.1. Den belegten Platz eruieren	252
9.5.2. Eine Komprimierung anfordern	252
9.5.3. Die verschiedenen Komprimiermethoden	253
9.5.4. Beschränkungen bei Feldgrößen	256
9.6. Das Database-Maintenance-Tool	256
9.6.1. DBMT und Systemdatenbanken	258
9.6.2. Komprimieren	259
9.6.3. DBMT starten	259
9.7. Datenbanken reparieren	260
9.7.1. Das Programm Fixup	260
9.7.2. Fixup über DBMT ausführen	261
9.8. Ansichten verwalten	261
9.8.1. Nicht genutzte Ansichten finden	262
9.8.2. Ansichtsindizes aktualisieren	263
9.8.3. Kritische Ansichten priorisieren	263
9.8.4. Den temporären Ordner für Indexaktualisierungen ändern	264
9.8.5. Verschieben der Ansichtsindizes ins Dateisystem (NIFNSF)	265
9.9. Volltextindizes verwalten	266
9.9.1. Einen Volltextindex erstellen	267
9.9.2. Volltextindex aktualisieren	269
9.9.3. Volltextindex löschen	270
9.9.4. Volltextindex verschieben	270
9.10. Die Servertasks Update und UpdAll	271
9.10.1. Der Servertask Update	271
9.10.2. Die Leistung von Update verbessern	271
9.10.3. Der Servertask UpdAll	272
9.11. Kompressionsverfahren anwenden	274
9.11.1. Gestaltungskomprimierung	274
9.11.2. Zentralschablone	275
9.11.3. Komprimieren von Dokumentdaten	276
9.11.4. Anhangskomprimierung	277
9.12. Domino Attachment and Object Service	277
9.12.1. Den DAOS zur Mailweiterleitung einrichten	278

9.12.2. Ein paar Worte zur Verschlüsselung	278
9.12.3. Ein paar Worte zur Anhangskomprimierung	278
9.12.4. Voraussetzungen für den DAOS	278
9.12.5. Einen DAOS einrichten	278
9.12.6. Der DAOS-Manager	280
9.12.7. Den DAOS deaktivieren	281
9.12.8. Den DAOS-Speicher verschieben	282
9.12.9. DAOS-Tier 2-Speicher	282
9.13. Datenbanken verschieben	283
9.13.1. Händisches Verschieben einzelner Dateien	283
9.13.2. Verschieben von Datenbanken über AdminP	286
9.13.3. Auslagern von Datenbanken über Datenbank-Links	286
9.13.4. Auslagern von Verzeichnissen über Ordner-Links	286
9.14. Benutzeraktivitäten überwachen	287
9.15. Dokumentlöschungen protokollieren	289
9.16. Der Datenbankkatalog	290
9.16.1. Den Catalog-Task händisch starten	291
10. Replikation	293
10.1. Übersicht	293
10.1.1. Replik-ID	293
10.1.2. Replik	294
10.1.3. Kopie	294
10.1.4. Servertask Replikator	294
10.1.5. Replizierkonflikte	295
10.1.6. Repliziertypen	295
10.1.7. Die Server-zu-Server-Replikation	296
10.1.8. Die Client-zu-Server-Replikation	296
10.1.9. Replizierprotokoll	296
10.1.10. Löschinfos	296
10.2. Eine neue Replik erstellen	297
10.2.1. Über das Menü	297
10.2.2. Über das Werkzeug Replik(en) erstellen	298
10.2.3. Über den Konsolenbefehl cl copy	299
10.2.4. Lokale Repliken und Rechte	299
10.3. Datenbanken replizieren	300
10.3.1. Replizieren über das Datenbanksymbol	300
10.3.2. Replizieren auf der Serverkonsole	300
10.4. Eine automatische Replizierung einrichten	301
10.4.1. Einen Replizierzeitplan erstellen	301
10.5. PIRC	303

10.5.1. Aktivieren von PIRC via Replizieroptionen	303
10.5.2. Aktivieren von PIRC via Domino-Administrator	303
10.5.3. Aktivieren von PIRC via Comapct-Task	303
11. Anwendungsentwicklung	305
11.1. Wozu dieses Kapitel?	305
11.2. Anwendungsschablonen	305
11.2.1. Eine Schablone erstellen	306
11.2.2. Schablonen signieren	307
11.2.3. Die Gestaltung von Anwendungen aktualisieren	308
11.2.4. Die Schablone wechseln	310
11.3. Agenten	312
11.3.1. Was sind Agenten?	312
11.3.2. Der Agentenmanager	313
11.3.3. Einen einfachen Formel-Agenten erstellen	315
12. Verschlüsselung und Zertifikate	319
12.1. Kurze Einführung in die Kryptografie	319
12.1.1. Verschlüsselungsverfahren	319
12.1.2. Sicherheitsstandards	320
12.1.3. Digitale Signatur	321
12.2. Netzwerkverschlüsselung	321
12.3. Datenbankverschlüsselung	323
12.3.1. Lokale Verschlüsselung	323
12.3.2. Verschlüsselung am Server	324
12.4. Dokumentverschlüsselung	325
12.5. Spezialfall Mailverschlüsselung	325
12.5.1. Mails beim Senden verschlüsseln	325
12.5.2. Behalten einer verschlüsselten Kopie	326
12.5.3. Mails beim Zustellen verschlüsseln	326
12.6. Feldverschlüsselung	327
12.7. Signieren	328
12.7.1. Signieren von Mails	328
12.7.2. Signieren von Dokumentänderungen	328
12.8. Verschlüsselung in ID-Dateien	328
12.8.1. Interne Verschlüsselung	329
12.8.2. RSA-Verschlüsselung	332
13. Das Domino-Sicherheitsmodell	335
13.1. Übersicht über die einzelnen Sicherheitsebenen	335
13.2. Serversicherheit	336
13.2.1. Authentifizierung	336

13.2.2. Querzulassung	337
13.2.3. Den Serverzugriff steuern	340
13.2.4. Abgänger ausschließen	341
13.3. ID-Sicherheit	342
13.3.1. Allgemeines zu Kennwörtern	342
13.3.2. Kennwortlänge und Komplexität	343
13.3.3. Kennwortqualität	343
13.3.4. Kennwort überprüfen oder ablaufen lassen	344
13.3.5. Benutzerdefinierte Kennwortrichtlinie	347
13.4. Gemeinsame Notes-Anmeldung	350
13.4.1. Einrichten der Gemeinsamen Notes-Anmeldung	351
13.4.2. Einschränkungen	351
13.5. Nachruf: Einmalige Notes-Anmeldung	352
13.5.1. Was nützen die ganzen Schlösser, wenn sie keiner absperrt?	352
13.6. Das Internetkennwort	353
13.6.1. Den Speicherort des Internetkennworts konfigurieren	353
13.6.2. »Sichere« und »sicherere« Internetkennwörter	354
13.6.3. Sperren des Internetkennworts erzwingen	355
13.6.4. Passwort-Synchronisierung	357
13.7. Verzeichnissicherheit	357
13.8. Datenbanksicherheit	358
13.8.1. Benutzerrollen	359
13.8.2. Konsistente Zugriffskontrollliste	361
13.9. Ausführungskontrolllisten	362
13.9.1. Die Vorgabe-ECL bearbeiten	364
13.9.2. Änderungen in der Administrations-ECL ausrollen	364
13.9.3. Mehrere Administrations-ECLs erstellen	365
13.9.4. ECL–Empfehlungen	366
13.10. Gestaltungssicherheit	366
13.10.1. Leserfelder	366
13.10.2. Autorenfelder	367
13.10.3. Öffentlicher Zugriff	367
13.10.4. Feldverschlüsselung	368
14. Der Webserver	371
14.1. Fähigkeiten des Domino-Webservers	371
14.1.1. Domino Webserver-Features im Detail	371
14.2. Einrichten eines Domino-Webservers	372
14.2.1. Bevor Sie einen Webserver einrichten	372
14.2.2. Den Webserver starten	373
14.2.3. Eine Webseite einrichten	373

14.2.4. Mehrere Websites einrichten	375
14.3. Benutzeranmeldung im Web	376
14.3.1. Anonyme Benutzer	376
14.3.2. Arten der Authentifizierung	376
14.3.3. Welche Anmeldenamen sind erlaubt?	379
14.3.4. Benutzer ohne Zugriff auch für HTTP sperren	380
14.4. Webserver-Konfiguration	380
14.4.1. Eine Anmeldemaske bereitstellen	381
14.4.2. Eine Maske zur Kennwortänderung bereitstellen	382
14.4.3. Fehlermeldungen des Webserver anpassen	382
14.5. Ein Webserverprotokoll einrichten	383
14.5.1. Protokollierung in einer Notes-Datenbank	383
14.5.2. Protokollierung in Textdateien	385
14.6. Einen sicheren Webserver aufbauen	387
14.6.1. Transport Layer Security (TLS)	388
14.6.2. Die eigene Webseite überprüfen	388
14.6.3. Was Sie nach einem Upgrade überprüfen sollten	393
14.6.4. HTTP Strict Transport Security (HSTS)	393
14.6.5. Server Name Indication – SNI	394
14.7. TLS-Zertifikate erstellen	394
14.7.1. Die einzelnen Komponenten	394
14.7.2. Ein Zertifikat bei einer offiziellen CA anfordern	395
14.7.3. Das TLS-Zertifikat einspielen und aktivieren	399
14.7.4. TLS-Zertifikate mit Let's Encrypt erstellen	401
14.7.5. Eigene Zertifikate erstellen	403
14.7.6. Zertifikate für mehrere Hostnamen erstellen	406
14.8. Der Domino-Webadministrator	409
14.8.1. Einrichten des Webadministrators	409
14.9. Einen Credential Store einrichten	410
14.9.1. Einen Credential Store auf einem einzelnen Server einrichten	410
14.9.2. Einen Credential Store in einem Cluster einrichten	411
14.10. Webmail einrichten	411
14.10.1. iNotes Redirect einrichten	412
14.10.2. Eine Websiteregeln erstellen	412
14.11. Auf HCL Verse umstellen	413
14.11.1. Was ist HCL Verse?	413
14.11.2. Voraussetzungen	413
14.11.3. Installation von Verse	414
14.11.4. Verse als eigenständige Anwendung ausführen	416

15. Mobile Endgeräte	417
15.1. Übersicht	417
15.2. Installation des Traveler-Servers	418
15.2.1. Vorgaben	418
15.2.2. Vorgangsweise	418
15.3. Den Traveler starten und beenden	423
15.4. Traveler-Benutzer hinzufügen	424
15.5. Traveler-Benutzer löschen	425
15.6. Geräte verwalten	425
15.6.1. Den Geräten Vorgaben zuweisen	425
15.6.2. Wie Vorgaben gesetzt werden	427
15.6.3. Geräte löschen oder zurücksetzen	428
15.6.4. Entferntes Löschen	428
15.6.5. Ein Remote Wipe zurücknehmen	430
15.7. Das Traveler-Protokoll	431
15.8. Die Derby-Datenbank	432
15.8.1. Die Datenbank manuell defragmentieren	433
15.8.2. Die Datenbank nach Zeitplan defragmentieren	433
16. Domino-Cluster	435
16.1. Was ist ein Cluster?	435
16.2. Einen Cluster einrichten	437
16.2.1. Voraussetzungen	437
16.2.2. Vorgangsweise	438
16.2.3. Überprüfen, ob der Cluster korrekt eingerichtet ist	440
16.2.4. Einen eignen Cluster-Port einrichten	440
16.2.5. Das Cluster-Verzeichnis	441
16.3. Lastverteilung einrichten	442
16.3.1. Lastverteilung über die Maximalzahl von Benutzern	442
16.3.2. Lastverteilung über einen Verfügbarkeitsschwellenwert	443
16.3.3. Wie die Client-Umleitung funktioniert	443
16.3.4. Zugriff auf einen Cluster-Server beschränken	444
16.3.5. Mail-Routing im Cluster konfigurieren	444
16.4. Symmetrische Cluster	445
16.4.1. Erkennung und Reparatur fehlender Datenbanken	445
16.4.2. Erkennung und Reparatur defekter Datenbanken	445
16.4.3. Bedingungen für einen symmetrischen Cluster	446
16.4.4. Einen symmetrischen Cluster aufsetzen	446
16.4.5. Den Reparaturdienst tunen	448
16.4.6. Der Befehl Repair	449

17. Serverüberwachung	451
17.1. Übersicht	451
17.2. Das Domino-Serverprotokoll	451
17.2.1. Steuern, wie lange Protokolleinträge aufgehoben werden	452
17.2.2. Protokollfilter	453
17.3. Statistiken	453
17.3.1. Das Sammeln von Statistiken konfigurieren	454
17.3.2. Historische Statistiken abfragen	456
17.3.3. Veröffentlichen von Statistiken bei externen Diensten	457
17.4. Server-Ereignisse	458
17.4.1. Ereignishandler	458
17.4.2. Einen Eventhandler für eine bestimmte Meldung einrichten	459
17.4.3. Ereignisgeneratoren	461
17.5. Domino-Domänenüberwachung	462
17.5.1. Erweiterte und einfache Ereignisse	463
17.5.2. Problembearbeitung	463
17.5.3. Erfassungshierarchie	465
17.5.4. Probing	465
18. Anwender-Clients	467
18.1. Übersicht	467
18.2. HCL Notes	467
18.2.1. Basic- und Standard-Client	467
18.2.2. Die verschiedenen Client-Pakete	468
18.2.3. Notes-Clients ausrollen	469
18.3. HCL Nomad: Notes auf iPad, iPhone und Co.	473
18.4. POP- und IMAP-Clients	474
18.4.1. Vergleich zwischen POP3 und IMAP4	474
18.4.2. POP3	474
18.4.3. IMAP	475
18.4.4. Benutzer für POP3 oder IMAP4 anlegen	477
18.4.5. SMTP für POP3- oder IMAP-Clients erlauben	477
18.4.6. Beispiel: IMAP-Konfiguration für Microsoft Outlook 2019	478
18.4.7. Öffentliche Ordner einbinden	482
18.4.8. Auch IMAP verrät die Identität Ihres Servers	485
18.4.9. Konfiguration von LDAP am Beispiel von Outlook 2019	485
18.5. Microsoft Outlook über HTMO anbinden	487
18.5.1. Eigenschaften im Detail	488
18.5.2. Konfiguration des Traveler-Servers für Outlook	489
18.5.3. Aktivieren von REST-Services	489
18.5.4. Verwenden von TLS-Zertifikaten	491

18.5.5. Einstellungen für Outlook anpassen	492
18.5.6. Installation des HTMO-Outlook-Add-Ins	495
18.5.7. Outlook mit dem Traveler verbinden	497
18.5.8. HTMO-Benutzer überwachen	500
19. Anhänge	501
Anhang A: Serverkonsolenbefehle (Auswahl)	501
Anhang B: Domino-Serverprogramme (Auswahl)	503
Anhang C: Parameter für Konfigurationsdateien	505
20. Index	507
21. Danksagungen	519

1. Vorwort

Ich bin seit 1992 Notes-Spezialist. Ich stieg mit Version 2 ein, ein halbes Jahr darauf (im Mai 1993) kam Lotus Notes 3 heraus. Anfangs hielt ich Kurse mit dem Lotus Notes-Server für Windows für Workgroups 3.11, der zehn Benutzer versorgen konnte, was für durchschnittlich acht Kursteilnehmer ausreichte. Bei mir im Büro lief der Notes-Server als NLM unter Netware. Heute weiß kaum noch jemand, was das ist, aber es funktionierte toll – und kam mit 8 MB RAM aus.

Unter Notes 4.5 stellte zunächst OS/2 die leistungsfähigste Plattform, Notes-Clients und der mittlerweile in Domino unbenannte Server kommunizierten via NETBIOS oder IPX/SPX, das Protokoll TCP/IP war noch nicht weit verbreitet.

Unter Version 4.x erfolgte auch meine erste Zertifizierung, ich erlangte den Status CLP (Certified Lotus Professional) und CLI (Certified Lotus Instructor). Der Status CLI war damals schwer zu erreichen (und teuer), man musste erst bei der Firma Lotus in München eine Gesichtskontrolle über sich ergehen lassen. Von den vier Bewerbern im Zertifizierungskurs lehnte Lotus zwei ab – so streng ging es damals zu.

Nach dem Erscheinen von R5 im Jahr 1999 wurde Notes zum Renner. Ich stand fast täglich in der Klasse und für viele Kurse gab es Wartelisten. Der Fokus verlagerte sich langsam auf Windows NT und als Netzwerkprotokoll kam zunehmend TCP/IP zum Einsatz.

Nach der Eingliederung der Firma Lotus in die IBM wurden die Zertifizierungsregeln noch einmal verschärft, ich musste beinahe für jeden Kurs, den ich halten wollte, eine Prüfung ablegen. Im Jahr 2008 war ich mit IBM Notes und Domino 8 für jeden Notes-Kurs zertifiziert, den die IBM anbot, sowohl als Administrator als auch als Entwickler. Ich hatte mittlerweile über 1.000 Schulungstage hinter mir, und als das Schulungsgeschäft mit Version 8.5 stark nachließ, verschob sich mein Schwerpunkt in Richtung Projekte und Anwendungsentwicklung.

Dabei war 8.5 eine tolle Version – hier gab es mehr Änderungen als in 7 und 8 zusammen! Nach der Einführung von ID-Vault, DAOS und XPages fragten wir uns damals alle, wie wir ohne diese Features arbeiten können ... Ed Brill, der damalige Chef der IBM Collaboration Solutions, bemühte sich redlich, Notes und Domino weiter zu modernisieren, schied aber plötzlich aus der Firma IBM aus. Man wollte Domino, so munkelte man damals zumindest, »wegen interner Konkurrenz« keine bahnbrechenden Neuerungen mehr gönnen – wer kauft denn noch Websphere oder Connections, wenn der Domino-Server schon alles kann?

Nach Eds Abgang im Jahr 2013 wurde aus Lotus Notes 8.5.4 plötzlich IBM Notes 9 (mit rund 1.300 Korrekturen und Neuerungen etwas schmalbrüstig – die Wartungs-Updates 8.5.1 bis 8.5.3 hatten zuvor fast 4.500 Änderungen enthalten). Kurz danach entschied sich die IBM, gar keine neuen Versionen mehr auszuliefern, sondern nur noch sogenannte »Feature Packs« herauszubringen, die neben Korrekturen auch einige Neuerungen enthielten. Man konnte das durchaus als gelungene Produktpflege bezeichnen, zwischen 9.0 und 9.0.1 FP10 liegen rund 3.000 Änderungen, darunter auch viele interessante. Doch es fehlten echte Innovationen, und die Kunden fühlten sich in Ermangelung neuer

Versionen zunehmend verunsichert. In dieser mehrere Jahre dauernden Sauregurkenzeit migrierten viele Firmen zu anderen Herstellern, und diejenigen, die bei Notes blieben, betrieben es nur noch auf Sparflamme.

Dann kam unerwartet die Firma HCL ins Spiel und frischer Wind auf. So mancher Kunde, der bereits laut über eine Migration nachgedacht hatte, blieb bei Notes. Mit der Einführung von Notes und Domino 10 im Jahr 2018 konnte ich erstmals ein paar Punkte auf meiner persönlichen Mängelliste abhaken – das war seit der Einführung von Version 8.5 im Jahr 2008 nicht mehr passiert. Die vielen Neuerungen wirkten sich auch auf die Auftragslage aus: Für mich als Domino-Experte gab es plötzlich wieder viel zu tun!

Was mir in Kursen oder bei Kundenbesuchen jedoch ständig vorgehalten wurde, war das Fehlen jeglicher deutscher Dokumentation. Und noch schlimmer: So unglaublich es auch klingen mag, es gab überhaupt kein aktuelles Domino-Buch auf dem Markt, nicht einmal auf Englisch! Also habe ich rasch dieses Buch geschrieben. Es ist kein »Kompodium« geworden, in dem alles steht, dafür hätte ich viel länger gebraucht, aber ich wollte das Buch über Domino 11 doch veröffentlichen, bevor Domino 12 erscheint. Dafür plane ich, für jede neue Version nicht nur eine aktualisierte, sondern auch erweiterte Auflage herauszubringen, das Buch über Domino 12 ist bereits in Arbeit! Wie es danach weitergeht, hängt von Ihrem Interesse ab. Lassen Sie mich hören, was Sie lesen wollen!

Wien, im Mai 2021

2. Über dieses Buch

2.1. An wen richtet sich dieses Buch?

Sie sind angehender Domino-Administrator, der HCL Notes und Domino neu einführt, um es entweder als Applikationsplattform zu nutzen oder damit ein anderes Mailsystem ablöst? – Dann ist dieses Buch für Sie genau richtig!

Sie sind schon länger Domino-Administrator, der eine HCL Notes und Domino-Umgebung betreibt und auf Version 11 aktualisieren möchte? – Dann ist dieses Buch für Sie genau richtig!

Auch wenn sich dieses Buches auf HCL Domino 11 bezieht, können Sie es ebenso als Anleitung für die Versionen 10 und 9 verwenden.

Im Mittelpunkt steht Domino für Windows; abgesehen von der Installation unterscheidet sich die Administration auf anderen Plattformen jedoch kaum, sodass Sie dieses Buch auch zurate ziehen können, wenn Sie Domino auf Linux, AIX oder System i betreiben.

2.2. Was dieses Buch NICHT ist

Dieses Buch stellt keinen Anspruch auf Vollständigkeit. Ich habe jene Informationen zusammengetragen, die mir für den Betrieb einer Domino-Umgebung in einem kleinen oder mittelständigen Unternehmen als wichtig erscheinen.

Dieses Buch ist kein Update-Buch, in dem alle Neuerungen der Version 11 vollständig aufgelistet sind. Ich schlage immer jene Methode vor, die mir am sinnvollsten erscheint, egal mit welcher Version sie eingeführt wurde. Damit auch Administratoren älterer Versionen das Buch verwenden können, mache ich jedoch darauf aufmerksam, wenn ein Feature erst mit Version 10 oder 11 eingeführt wurde.

Dieses Buch behandelt den Domino-Server und bietet keine Unterstützung für den Client-Support und schon gar keine Anleitungen für Endanwender. Ich beschränke mich darauf, aufzuzeigen, wie Sie Domino konfigurieren müssen, um verschiedene Clients anzubinden.

2.3. Welche Voraussetzungen SIE mitbringen müssen

Sie müssen kein Domino-Administrator sein, genau dieses Wissen will das Buch ja vermitteln. Sie sollten jedoch mit den grundlegenden Funktionen von Notes vertraut sein, denn ich erkläre hier nicht, wie man eine Datenbank öffnet, einen Kalendereintrag erstellt oder ein Mail verschickt.

Sie müssen auch kein Windows-Administrator sein, sollten jedoch auf den Servern über ausreichende Rechte verfügen (vor allem über das Recht, Software zu installieren!) und über grundlegende Themen Bescheid wissen. In diesem Buch verlange ich von Ihnen, ein Programm als Administrator

auszuführen, eine Kommandozeile zu öffnen und zu einem bestimmten Verzeichnis zu navigieren sowie einen Dienst zu starten und zu beenden. Mehr nicht.

2.4. Ein paar Worte zur Sprache

Dieses Buch ist nicht nur auf Deutsch geschrieben, es verweist auch auf die deutsche Software, d. h. Sie sehen auf allen Abbildungen einen deutschen Notes-Client, eine deutsche Mail-Schablone und ein deutsches Domino-Verzeichnis. Der deutschsprachige Raum gilt (zusammen mit Japan) als größte Notes-Hochburg, in der Notes und Domino mittlerweile weiter verbreitet sind als in den USA. Darauf nimmt auch der Hersteller der Software, die Firma HCL, zunehmend Rücksicht und hält viele Großveranstaltungen in Deutschland ab. Bei Updates erscheinen die deutschen Versionen zeitgleich mit den englischen und seit Neuestem werden sogar Beta-Versionen zum Testen auf Deutsch angeboten.

Damit Sie leichter eine Verbindung zur englischen Dokumentation des Herstellers im Internet herstellen können, werden in Klammern immer auch die englischen Begriffe genannt und sind auch via Index auffindbar.

2.5. Gerne höre ich von Ihnen

Alle Informationen in diesem Buch wurden gewissenhaft recherchiert und getestet, dennoch können Fehler passiert sein. Auch ändern sich Features durch das Einspielen von Updates und sogar von Fix Packs. Sollten Sie auf einen Fehler oder ein geändertes Verhalten stoßen, freue ich mich über einen Hinweis. Selbstverständlich können Sie mich auch gerne kontaktieren, wenn Sie Änderungsvorschläge haben oder einfach nur einen Kommentar abgeben möchten. Senden Sie dazu eine E-Mail an fachbuch@cob.at. Bitte haben Sie jedoch Verständnis, dass ich keinen Gratis-Support für Notes und Domino leisten kann.

3. Architektur und Konzepte

- > 3.1 Was ist HCL Notes und Domino?, Seite 23
- > 3.2 Von Zertifizierern und hierarchischen Namen, Seite 25
- > 3.3 Das Domino-Verzeichnis, Seite 28
- > 3.4 Von Domänen und Netzwerken, Seite 29

3.1. Was ist HCL Notes und Domino?

HCL Domino ist, wie man in Wikipedia nachlesen kann, ein dokumentenorientiertes, verteiltes Datenbanksystem mit enger E-Mail-Anbindung. HCL Domino stellt weiters eine Plattform zur Entwicklung von Anwendungen bereit. Einige dieser Anwendungen sind als fertige, quelloffene Schablonen bereits im Lieferumfang enthalten und können mit wenig Aufwand an den eigenen Bedarf angepasst werden.

Für Anwendungen finden sich sowohl die Bezeichnungen Notes-Datenbank als auch Domino-Datenbank bzw. auch Notes- oder Domino-Anwendung (oder Applikation). In Folge ist hier von Notes-Datenbanken die Rede.

Neben dem Domino-Server gibt es noch verschiedene Clients. Der Client für Anwender heißt HCL Notes, jener für Entwickler HCL Domino-Designer und jener für Administratoren HCL Domino-Administrator. Anwender-Clients mit reduziertem Funktionsumfang existieren außerdem für Tablets (HCL Nomad) und Mobiltelefone (HCL Verse).

3.1.1. Merkmale im Detail

3.1.1.1. Plattformen

Domino 11 ist für eine Reihe von Plattformen verfügbar, darunter Windows, Linux, AIX und IBM i (AS/400). Ältere Domino-Versionen laufen auch auf Solaris, z/OS und zLinux. In diesem Buch wird ausschließlich auf die Plattform Windows eingegangen.

Notes 11 steht für Windows und Mac OS in einer schlankeren Basic-Version mit reduziertem Funktionsumfang und einer voll ausgestatteten, aber wesentlich mehr Ressourcen benötigenden Standardversion zur Verfügung. (Für Linux existiert ein älterer Standard-Client auf Stand Version 9.) Der Domino-Designer und der Domino-Administrator laufen nur unter Windows. Der unter iOS und Android laufende HCL Nomad entspricht weitestgehend dem Basic-Client und kann als solcher auch Mail und Applikationen ausführen. Zusätzlich kommen der Webbrowser und Clients für Mobiltelefone (HCL Verse) zum Einsatz.

3.1.1.2. Dienste

Domino stellt eine Reihe von Diensten zur Verfügung. Der Server ist zunächst ein Datenbankserver, der Notes-Dokumente an Notes-Clients liefert. Weiters ist er ein Mailserver, der sowohl das native Domino-Routing-Protokoll NRPC (Notes Remote Procedure Calls) als auch SMTP (Simple Mail Transport Protokoll) zum Senden von Mails ins Internet beherrscht. Auch externe Mail-Clients können mit gängigen Mailprotokollen wie POP3 oder IMAP angebunden werden. Ferner gehört ein Webserver zum Lieferumfang, der alle üblichen Verschlüsselungsstandards (TLS – Transport Layer Security) und SNI (Server Name Indication) beherrscht, sowie ein Server für die Anbindung mobiler Endgeräte (HCL Traveler). Ein weiterer Server stellt den Verzeichnisdienst LDAP zur Verfügung.

3.1.1.3. Sicherheit

Eine integrierte Public-Key-Infrastruktur (PKI) sorgt für hohe Sicherheit: Ein Notes-Benutzer benötigt für den Zugriff eine Notes-ID, welche Zertifikate, einen Öffentlichen und dazu passenden Privaten Schlüssel und gegebenenfalls weitere Schlüssel enthält. Dasselbe gilt für Server. Die in einer PKI sonst aufwendige Administration der Öffentlichen Schlüssel in Verzeichnissen ist bei Notes/Domino im LDAP-fähigen Domino-Verzeichnis bereits enthalten.

3.1.1.4. Notes-Datenbanken

Notes-Datenbanken sind **Client-Server-Anwendungen**. Dabei werden – vereinfacht dargestellt – die Daten auf dem Domino-Server gespeichert, die Benutzerinteraktionen finden jedoch auf dem Client statt. Daten können vom Client aber auch lokal verwaltet werden, entweder als regelmäßige oder manuell abgeglichene Version einer Server-Datenbank (lokale Replik) oder als eigenständige Datenbank.

Daraus ergibt sich eine volle **Offline-Funktionalität**: Eine Notes-Anwendung, die auf einem Domino-Server betrieben wird, kann in der Regel identisch ohne Serververbindung auf einem Laptop benutzt werden. Sobald wieder eine Verbindung zwischen Client und Server besteht, werden die Änderungen je nach Konfiguration entweder automatisch – gemäß den definierten Verbindungsintervallen – oder auch manuell abgeglichen. Dieser Vorgang wird als **Replikation** bezeichnet.

In Datenbanken werden die Daten gemeinsam mit der Anwendungslogik und der Benutzeroberfläche abgelegt. Im Lieferumfang sind in Form von quelloffenen **Schablonen** bereits mehrere Anwendungen enthalten, unter anderem E-Mail, Kalender, Aufgaben, Adressverwaltung, Diskussion und TeamRoom, die mit relativ geringem Aufwand an eigene Bedürfnisse angepasst werden können.

3.1.1.5. RADD (Rapid Application Development & Deployment)

Mit der mitgelieferten Entwicklungsumgebung im HCL Domino-Designer können Anwendungen für den Notes-Client oder den Webbrowser mit relativ wenig Aufwand entwickelt und gewartet werden. Mittels **Gestaltungsaktualisierung** können Designelemente (Masken, Ansichten, Agenten etc.) von einer **Schablone** auf abhängige Datenbanken auf demselben Server übertragen und dann via **Replikation** auf andere Server und Clients weiterverteilt werden. Diese Fähigkeit vereinfacht die Entwicklung, Wartung und Administration.

3.1.1.6. Ausfallsicherheit und Lastverteilung

Domino-Server können zu **Clustern** verbunden werden, wobei weder das darunterliegende Betriebssystem noch die Version eine Rolle spielt. So ist es möglich, einen Domino-Server der Version

10 auf Windows mit einem Domino-Server der Version 11 auf Linux zu einem Cluster zu verbinden. Domino-Cluster haben nichts mit Clustern auf Betriebssystemebene zu tun. Bei Ausfall eines Domino-Servers übernimmt der Client selbstständig den Wechsel auf einen anderen Domino-Server im Cluster. Cluster werden nicht nur eingesetzt, um die **Ausfallsicherheit** zu erhöhen, sondern auch, um durch **Lastverteilung** die Leistungsfähigkeit zu maximieren.

3.2. Von Zertifizierern und hierarchischen Namen

Notes-Clients kommunizieren mit Domino-Servern sowie Domino-Server untereinander über das Protokoll NRPC (Notes-RPC, einer Variante von RPC – Remote Procedure Calls). NRPC kann über TCP/IP (Port 1352), NETBIOS und andere Protokolle geroutet werden.

Das Besondere an NRPC ist eine Benutzerauthentifizierung über einen Schlüsselaustausch und nicht – wie bei den meisten anderen Protokollen – über Namen und Kennwort. Diese **Authentifizierung** stellt Vertrauen zwischen beiden Seiten (Client – Server oder Server – Server) her. Erst wenn die Vertrauensstellung etabliert ist, werden der Name und die damit verbundenen Zugriffsrechte überprüft. Dieser zweite Schritt wird **Autorisierung** genannt.

Die Authentifizierung wird also rein über **Zertifikate** abgewickelt, welche die jeweils andere Stelle nicht nur ausweist, sondern auch überprüft. Das Zertifikat ist ein eindeutiger, elektronischer Schlüssel, erhalten von einem **Zertifizierer** und gespeichert in einer **ID-Datei** (mit der Endung *.id). Auch der Schlüssel des Zertifizierers ist in einer ID-Datei abgelegt, die beim Registrieren einer Organisation oder Unterorganisation bzw. beim Konfigurieren des ersten Domino-Servers erstellt wird.

Der Zertifizierer selbst gewährt keinen Zugriff, sondern fungiert nur als elektronischer Stempel zum Validieren anderer IDs.

3.2.1. Am Anfang war das Zertifikat

Am Beginn steht immer die Erstellung eines Zertifizierers. Damit verbunden ist die Generierung des sogenannten **Unternehmensschlüssels** (manchmal auch als Allgemeiner Schlüssel – Common Certificate bezeichnet), der in der ersten Zertifizierer-ID (Vorgabe: cert.id) abgelegt wird. Erst mit dieser Datei können Server und Benutzer erstellt werden.

ID-Dateien von Servern und Benutzern erhalten neben dem Unternehmensschlüssel noch ein mathematisch aufeinander abgestimmtes Schlüsselpaar zum Ver- und Entschlüsseln von Mails, Dokumenten oder ganzen Datenbanken. (Mehr über Schlüsselarten und Verschlüsselungsverfahren finden Sie in Kap. 12 Verschlüsselung und Zertifikate, ab Seite 319.)

Ein Teil der Authentifizierung ist die hierarchische Namensgebung.

3.2.2. Hierarchische Namen

Um Namenskollisionen zu vermeiden, verwendet Domino eine hierarchische Namensgebung; damit kann jedes Unternehmen seinen Server »Server1« nennen und der Name bleibt trotzdem eindeutig. Die Hierarchie beruht auf X400-Namenskonventionen, einem etwas in die Jahre gekommenen Standard zum Übertragen elektronischer Nachrichten.

Registriert der Zertifizierer /O=COB/C=AT eine Person mit dem Namen Admin, wird daraus CN=Admin/O=COB/C=AT. Minimum sind also Nachname und Organisation. Üblicherweise

werden bei der Angabe von Namen die Qualifizierer weggelassen, und man bedient sich der abgekürzten (abbreviated) Darstellung: `Admin/COB/AT`. Dafür gibt es in Notes sogar einen eigenen Feldtyp, das sogenannte Namensfeld, in dem der Name abgekürzt angezeigt, aber vollständig (in kanonischer Form) gespeichert wird.

Eine Übersicht über die einzelnen Namenskomponenten liefert die folgende Tabelle:

Komponente	Anzahl Zeichen	Bedeutung
CN (Common Name)	1–80	Der Allgemeine Name, bei einer Person die Kombination aus Vor-, Mittel- und Nachname, bei einem Server der Servername.
OU (Organizational Unit)	0–32	Optional. Eine Organisationseinheit, üblicherweise eine Abteilung oder ein Standort. Es sind bis zu vier OU-Ebenen möglich, dann als OU1, OU2 etc. bezeichnet.
O (Organization)	3–64	Der Name der Organisation – oft abgekürzt.
C (Country)	0 oder 2	Optional. Ländercode zweistellig nach ISO 3166; z. B.: DE für Deutschland, AT für Österreich

Tabelle 3.1: Namenskonventionen

Alle Namenskomponenten zusammen müssen einen eindeutigen Namen ergeben, d. h. der Allgemeine Name kann öfters vorkommen, wenn sich die Personen in mindestens einer anderen Namenskomponente unterscheiden, z. B.:

`Franz Meier/IT/COB/AT`

`Franz Meier/HR/COB/AT`

In der Praxis verwenden zumindest große Organisationen ihren Unternehmenszertifizierer zurückhaltend zum Registrieren von Benutzern, sondern erstellen damit zunächst Unternehmenseinheiten (`/OU=`), meist Abteilungen. Erst mit diesen registrieren sie dann Server und Benutzer.

Auch Vertrauen funktioniert zwischen Zertifizierern hierarchisch. Ähnlich wie bei Internetzertifikaten vertrauen jene IDs einander, die vom selben Stammzertifikat abstammen (also denselben Unternehmensschlüssel besitzen). Es ist jedoch auch möglich, einem fremden Zertifizierer zu vertrauen – siehe Kap. 13.2.2 Querkzulassung, ab Seite 337.

3.2.3. Arten von ID-Dateien

Es gibt drei Arten von ID-Dateien:

- > Zertifizierer (auf `/O-` und `/OU-`Ebene sowie ID-Vaults)
- > Server
- > Personen

Allen drei ID-Typen ist gemeinsam, dass sie nicht ewig gültig bleiben, sondern irgendwann ablaufen. Zertifizierer-IDs (auch als **Zulassungsdateien** bezeichnet) und Server-IDs sind per Vorgabe hundert Jahre gültig, Benutzer-IDs nur zwei. Eine Ihrer Aufgaben besteht also darin, diese immer wieder zu verlängern. Aber auch bei Servern und Zertifizierern könnte Arbeit anfallen – etwa, wenn Sie die Schlüssellänge erhöhen wollen.

Dass alle ID-Arten die Dateierdung `*.id` verwenden, erfordert zur besseren Unterscheidung eine entsprechende Kennzeichnung auf Dateiebene. Hat sich der Administrator diese Mühe nicht

gemacht, können Sie die ID auch inspizieren – solange Sie das Kennwort wissen. Navigieren Sie im Domino-Administrator zum Register (umgangssprachlich oft auch als »Reiter« bezeichnet) **Konfiguration** und wählen Sie in den Werkzeugen den Befehl **Zertifizierung > ID-Eigenschaften**. Hier ein Beispiel für einen Zertifizierer:



Abbildung 3.1: Eigenschaften eines Hierarchischen Zertifizierers

Es erübrigt sich fast zu sagen, dass vor allem Zertifizierer-IDs (und deren Kennwörter!) nicht verloren gehen dürfen. Erstellen Sie also Sicherheitskopien und legen Sie diese an einen sicheren Ort. Aber auch Benutzer-IDs, die zum Verschlüsseln von Datenbanken verwendet wurden, dürfen nicht abhandenkommen. Deshalb stellt Domino für das Speichern von Benutzer-IDs einen **ID-Tresor** (ID-Vault) zur Verfügung, aus dem Sie ID-Dateien unter Vergabe eines neuen Kennworts extrahieren können. Diesen ID-Tresor müssen Sie allerdings erst einmal aufsetzen! (Die Anleitung dazu finden Sie in Kap. 6.2.1 Einen ID-Vault einrichten, ab Seite 138.)

3.2.4. Soll ich Organisationseinheiten verwenden?

Ob Sie in Ihrem Unternehmen eine oder gar mehrere Organisationseinheiten (Organizational Units, OUs) einführen sollen, ist nicht leicht zu beantworten. In sehr kleinen Firmen (mit ein paar Duzend bis hundert Benutzern) lässt man sie in der Regel weg, weil der Mehraufwand den Vorteil klar überwiegt. In Unternehmen mit mehreren tausend Benutzern führt man sie hingegen meist ein. Die Zuordnung zu OUs (Abteilungen und/oder Standorte) lässt nicht nur die Herkunft der Benutzer erkennen, sondern bietet auch mehr Möglichkeiten beim Zuweisen von Rechten oder beim Zuordnen von Richtlinien. So können Sie etwa in eine Zugriffskontrollliste den folgenden Eintrag aufnehmen:

```
*/Verkauf/COB/AT
```

Damit werden allen von diesem Zertifizierer abstammenden Benutzern dieselben Rechte zugeordnet, ohne dass Sie dafür ein statisches Gruppendokument warten müssen!

Andererseits muss die ID des Benutzers bei jedem Abteilungswechsel umbenannt werden, was bis heute einen beträchtlichen Aufwand erzeugt. Sie erkaufen sich die größere Flexibilität bei der Konfiguration also durch einen größeren Aufwand bei der Wartung.

Sie sehen schon, es ist nicht leicht, eine klare Anleitung zu bieten, zu viele Details sind zu berücksichtigen. Sollten Sie sich für die Einführung von OUs entscheiden, kann ich Ihnen nur raten, dabei nicht zu übertreiben. Namen wie den folgenden würde ich tunlichst vermeiden, auch wenn dahinter eine sorgfältige Planung stecken mag:

```
Franz Ritter/Verkauf/Germany/EMEA/ABC
```

Beschränken Sie sich auf eine OU-Ebene, in großen Unternehmen maximal auf zwei.

Und noch etwas: Da Server normalerweise nicht exklusiv Abteilungen zur Verfügung stehen, ist es unüblich, sie in OUs zu stellen, sie unterstehen besser direkt der Organisation.

3.2.5. Querzulassung

Sollten Sie sich, weil Ihnen das ganze Rezertifizieren zu aufwendig erscheint, für die Einführung mehrerer Organisationen entscheiden, so ist auch das möglich. Mehrere Stammzertifizierer (also Organisationen) im selben Domino-Verzeichnis vertrauen einander per se zwar nicht, können aber über den Weg der Querzulassung eine Vertrauensstellung zueinander aufbauen. Und da das Ganze hierarchisch funktioniert, genügt es, diese auf oberster Ebene auszutauschen, alle »Nachfahren« (also OU-Zertifizierer, Server und Benutzer) vertrauen einander dann auch. (Die Anleitung zum Austauschen einer Querzulassung finden Sie in Kap. 13.2.2 Querzulassung, ab Seite 337.)

3.2.6. Soll ich Ländercodes verwenden?

Die Verwendung einer Länderkennung bietet sich an, wenn Sie in verschiedenen Ländern aktiv sind und in jedem Land eine eigene Organisation aufbauen wollen. Wenn Sie einen Ländercode vergeben, wird er Teil des Organisationsnamens. Das Verwenden einer Länderkennung verringert auch die Wahrscheinlichkeit, dass ein anderes Unternehmen gleich heißt – was allerdings nur bei der Verbindung über NRPC ein Problem wäre.

Wenn Sie nur darstellen wollen, aus welchem Land ein Benutzer stammt, können Sie zur Länderkennung alternativ auch die OU heranziehen. Welche Methode Sie verwenden, hat Auswirkungen auf die Sicherheit, respektive auf die Zugriffsrechte der Benutzer und Server.

	/AT/COB	/COB/AT
/DE/COB	✓	✗
/COB/DE	✗	✗

Tabelle 3.2: Zugriffsmatrix OU/OU – O/O (Erklärung im Text)

Benutzer und Server aus /AT/COB gehören zur selben Organisation wie Benutzer und Server aus /DE/COB und haben daher aufeinander Zugriff. (Dieser Zugriff kann später über die **Serverzugriffskontrollliste** eingeschränkt werden – siehe Kap. 13.2.3 Den Serverzugriff steuern, ab Seite 340.) Benutzer und Server von /COB/AT gehören hingegen zu einer anderen Organisation als Benutzer und Server von /COB/DE und erhalten daher keinen Zugriff. (Dieser Zugriff kann über eine Querzulassung gewährt werden – siehe Kap. 13.2.2 Querzulassung, ab Seite 337.)

3.3. Das Domino-Verzeichnis

Mit Domino-Verzeichnis (Domino Directory) ist kein Verzeichnis im Dateisystem gemeint, sondern eine Notes-Datenbank mit dem Namen names.nsf, die die folgenden Eigenschaften aufweist:

- > ein domänenweites Verzeichnis aller Namen zum Nachschlagen von Adressen
- > ein domänenweites Verzeichnis aller Öffentlichen Schlüssel
- > Richtlinien zur Benutzerverwaltung und der Client-Konfiguration
- > die Serverkonfiguration (zusammen mit der Datei notes.ini)

In früheren Domino-Versionen wurde das Domino-Verzeichnis »Öffentliches Adressbuch« (Public Address Book oder auch Name & Address Book, NAB) genannt – im Gegensatz zum lokalen Adressbuch des Notes-Clients, welches »Persönliches Adressbuch« oder seit einiger Zeit nur noch

»Kontakte« heißt. Beide verwenden den Dateinamen `names.nsf`, das Domino-Verzeichnis basiert jedoch auf der Schablone `pubnames.ntf`, die Kontakte-Anwendung auf `pernames.ntf`.

Alle Server innerhalb einer Domäne verwenden Repliken ein und desselben Domino-Verzeichnisses, die zwischen den Servern regelmäßig abgeglichen (repliziert) werden müssen – wofür Sie als Administrator zu sorgen haben. (Siehe auch Kap. 10 Replikation, ab S. 293.)

Dabei kann eine Verteilte oder eine Zentrale Verzeichnisarchitektur aufgebaut werden. Bei einer **Verteilten Verzeichnisarchitektur** verfügen alle Server in der Domäne über eine vollständige Replik des Domino-Verzeichnisses. Eine vollständige Replik wird auch **Primäres Domino-Verzeichnis** genannt. Ein Primärverzeichnis enthält Personen, Gruppen, Mail-In-Datenbanken (siehe Kap. 8.5 Mail-In-Datenbanken, ab Seite 222) und Ressourcen (siehe Kap. 7.3.3 Eine Ressource erstellen, ab Seite 194) sowie die gesamte Konfiguration.

Bei einer **Zentralen Verzeichnisarchitektur** verfügen nur einige Server (mindestens zwei) in einer Domäne über ein Primäres Domino-Verzeichnis, die restlichen Server verwenden eine selektive Replik, die nur Konfigurationsdokumente enthält und deshalb **Konfigurationsverzeichnis** genannt wird. Ein Server mit einem Konfigurationsverzeichnis verbindet sich bei Bedarf mit dem primären Verzeichnis auf einem anderen Server, um Benutzerinformationen abzurufen.

Eine Zentrale Verzeichnisarchitektur empfiehlt sich nur in großen Domino-Umgebungen mit vielen Servern und einem entsprechend großen Domino-Verzeichnis. Da Server mit Konfigurationsverzeichnissen nicht mehr darauf warten müssen, bis Änderungen in Personen-, Gruppen- oder Mail-In-Dokumenten per Zeitplan zu ihnen repliziert werden, verfügen sie über aktuellere Informationen. Ein häufiges Nachschlagen dieser Informationen in den Primärverzeichnissen anderer Server kann jedoch auch zu einer größeren Netzwerkbelastung führen, weshalb Sie Server, die auf eine häufige Namenssuche angewiesen sind, eher mit einem Primärverzeichnis ausstatten sollten.

Jede Domino-Domäne verfügt über mindestens einen **Administrationsserver** für das Domino-Verzeichnis. Der Administrationsserver ist für die Ausführung von Administrationsanforderungen verantwortlich, die Aufgaben wie etwa das Umbenennen oder das Löschen von Benutzern automatisieren. Standardmäßig ist der zuerst eingerichtete Server auch der Administrationsserver für das Domino-Verzeichnis.

Server in unterschiedlichen Domänen verwenden unterschiedliche Domino-Verzeichnisse, können die Verzeichnisse der jeweils anderen Domänen jedoch als Adressbücher zum Nachschlagen von Adressen und auch zur Authentifizierung einbinden.

Der Schablonenname des Domino-Verzeichnisses lautet bis heute »StdR4PublicAddressBook« – nicht zu verwechseln mit dem Dateinamen der Schablone `pubnames.ntf`.

3.4. Von Domänen und Netzwerken

3.4.1. Die Domino-Domäne

Die Domäne ist in Notes – im Gegensatz zu Windows – eine reine Verwaltungseinheit. Mehrere Domänen innerhalb eines Unternehmens sind schwierig zu administrieren und selten sinnvoll. Mail-Austausch und Replikation zwischen Domänen erfordert einen größeren Verwaltungsaufwand, gestattet allerdings auch mehr Kontrolle.

Der Unterschied zwischen Domino-Organisationen und Domino-Domänen sorgt häufig für Verwirrung – es ist nämlich durchaus üblich, beide gleich zu benennen. Die übliche Notation ist, dass man

vor die Organisation einen Schrägstrich setzt, in unserem Beispiel also /COB, und vor die Domäne ein At-Zeichen, also @COB. Und Achtung: Nennen Sie Ihre Domino-Domäne NIEMALS so wie Ihre Internet-Domäne – also keinen Punkt (.) im Namen verwenden. Leerschritte sind zwar erlaubt, sollten aber ebenfalls vermieden werden.

Die Domänenzugehörigkeit steht nicht in der ID, sondern in einem Feld im Server, respektive im Personendokument. Deshalb kann der Domänenname später auch geändert werden. (Leider kommt er auch im lokalen Adressbuch (der Kontakte-Anwendung) des Notes-Clients vor, weshalb eine Umbenennung nicht ganz so einfach ist.)

3.4.2. Benannte Notes-Netzwerke

Benannte Notes-Netzwerke (Notes Named Networks, NNN), auch als Domino Named Networks, DNN bezeichnet, sind definiert als »eine Gruppe von Servern, die dasselbe Netzwerkprotokoll verwenden und einander deshalb sehen«. Ein Server kann theoretisch Teil mehrerer NNNs sein, braucht dazu aber mehrere IP-Adressen (außer es handelt sich um unterschiedliche Protokolle). Innerhalb eines NNNs funktioniert das Mail-Routing automatisch, und genau aus diesem Grund wollen Sie einige Server vielleicht in verschiedene NNNs stellen – Sie können dann nämlich die Verbindungswege bei der Mailweiterleitung beeinflussen.

Wenn ein Domino-Server über zwei Netzwerkadressen verfügt, kann er als Application Level Firewall fungieren: Indem man zwei NNNs konfiguriert, erlaubt man nur noch die Weiterleitung von NRPC-Paketen, während jede andere Art von Netzwerk-Traffic hier endet.

3.4.3. Verbindungsdokumente

Verwenden Sie innerhalb Ihrer Domäne nur ein NNN (was die Regel ist), müssen Sie gar nichts tun. Für die Verbindung zu Servern in anderen NNNs brauchen Sie einen Plan – und Verbindungsdokumente. Diese Dokumente liegen am Server im Domino-Verzeichnis, am Notes-Client in der Kontakte-Anwendung.

In Verbindungsdokumenten wird der Notes-Name des Ziels (immer ein Server, Notes-Clients kennen keine Peer-to-Peer-Verbindungen) mit einer Netzwerkadresse verbunden. Dabei handelt es sich fast durchwegs um TCP/IP-Adressen, Notes kann aber auch mit DNS-Namen umgehen – sofern diese aufgelöst werden können. (IP-Adressen bieten den Vorteil, ohne DNS-Server arbeiten zu können, DNS-Namen bieten die Freiheit, jederzeit die physische IP-Adresse ändern zu können – so lange der Eintrag im DNS richtiggestellt wird.) Verbindungsdokumente können außerdem auf bestimmte Zeiten und Standorte (= Arbeitsumgebungen) eingeschränkt werden.

Bei NNNs geht es wohlgermerkt nur um Notes-Mail (Protokoll NRPC) – Internet-Mail und damit die Verbindung zu Internet-Domänen über Internet-Protokolle (z. B. SMTP) ist ein ganz anderes Thema. Mehr Details dazu finden Sie in Kap. 8.3 Internet-Mail, ab S. 208.

4. Serverinstallation

- > 4.1 Voraussetzungen für die Installation, Seite 31
- > 4.2 Einen Domino-Server installieren, Seite 33
- > 4.3 Fehlerkorrekturen einspielen, Seite 40
- > 4.4 Sprachen installieren, Seite 41
- > 4.5 Einen ersten Domino-Server einrichten, Seite 50
- > 4.6 Einen Domino-Server starten und beenden, Seite 55
- > 4.7 Domino-Ports in der Windows-Firewall öffnen, Seite 61
- > 4.8 Einen Domino-Administrator installieren, Seite 64
- > 4.9 Einen zusätzlichen Domino-Server einrichten, Seite 74
- > 4.10 Eine ältere Domino-Version aktualisieren, Seite 80
- > 4.11 Domino und AntiVirus, Seite 84

4.1. Voraussetzungen für die Installation

4.1.1. Unterstützte Betriebssysteme

HCL Domino 11 unterstützt eine Vielzahl von Betriebssystemen, neben Windows auch Linux (Red Hat, SUSE, CentOS), AIX und IBM i. In diesem Buch wird in erster Linie auf Windows eingegangen.

Die folgenden Windows-Versionen sind für Domino 11 zertifiziert:

Unterstützte Windows-Versionen	Bit
Windows Server 2019 Standard Edition	64-Bit
Windows Server 2019 Datacenter Edition	64-Bit
Windows Server 2016 Standard Edition	64-Bit
Windows Server 2016 Datacenter Edition	64-Bit
Windows Server 2012 R2 Standard Edition	64-Bit
Windows Server 2012 R2 Datacenter Edition	64-Bit

Tabelle 4.1: Die für Domino 11 zertifizierten Windows-Versionen

Ist eine Windows-Version hier nicht aufgelistet (z. B. Windows Server 2008 R2) bedeutet das nicht zwangsweise, dass Domino darauf nicht läuft. In meinen Schulungen installieren wir Domino sogar auf Windows 10, für den Einsatz als Produktivsystem empfiehlt sich ein Desktop-Betriebssystem jedoch nicht.

4.1.2. Speicher

Die minimale Speicherausstattung beträgt laut HCL für Domino 512 MB pro Prozessor. Da Speicher derzeit nicht viel kostet, würde ich zumindest 16 GB RAM einplanen. Domino verwendet in den meisten Fällen zwar bedeutend weniger, aber das Betriebssystem braucht auch noch etwas und der übrige Speicher kann für den Dateisystemcache verwendet werden, was die Performance unerhört steigert. (Ich habe schon Dateiserver mit 32 GB RAM gesehen, die alle verwendeten NSF-Dateien im Speicher hielten und im normalen Betrieb komplett ohne Plattenzugriffe auskamen!)

Hat der Domino-Server mehr Speicher zur Verfügung, verwendet er ihn außerdem für seinen Datenbank-Cache, was zumindest auf Servern mit großen Mail- oder Anwendungsdateien zusätzlich für Performance sorgt.

4.1.3. Wie viele »Platten« braucht Domino?

Für die Installation von Domino unter Windows benötigen Sie mindestens 3 GB Speicherplatz. Im Betrieb kommt Domino dann mit etwa 1,5 GB aus, zuzüglich des Platzbedarfs für neu erstellte Datenbanken, allen voran der Maildateien.

Wie wir sehen werden, schlägt der Installationsassistent als Speicherort für die Daten ein Unterverzeichnis des Programmverzeichnis vor, Domino »braucht« also nur eine Platte. Aber ist das auch die beste Vorgangsweise? – Natürlich nicht! Programme von Daten zu trennen bringt einige Vorteile wie mehr Sicherheit, ein leichteres Backup und – unter gewissen Voraussetzungen – eine bessere Performance. Idealerweise erhält daher alles – Betriebssystem, Auslagerungsdatei, Domino-Programme, Domino-Daten, Transaktionsprotokolle, DAOS, Volltextindizes, Ansichtsindizes (NDX) u. a. – eigene Speicherbereiche, was aber ein eher unwahrscheinliches Szenario darstellt. Meine Minimalanforderung lautet daher: eine Platte für Betriebssystem mit Auslagerungsdatei plus Domino-Programme, eine zweite für die Domino-Daten und eine Dritte für die Transaktionsprotokolle.

Aber was heißt überhaupt »Platte«? – Es gibt ja die unterschiedlichsten Speichersysteme: Interne Festplatten/SSDs, DAS (Direct Attached Storage), NAS (Network Attached Storage), SAN (Storage Area Network), VDIs in virtuellen Umgebungen ...

Und was bedeutet »verschiedene« Platten? – Auch das hängt vom verwendeten Speichergerät ab:

- > Bei lokalen Festplatten = verschiedene Partitionen (aus Performancegründen auf verschiedenen physischen Platten)
- > Bei lokalen RAIDs = verschiedene RAID-Volumes
- > Bei SAN = verschiedene Logical Units (LUNs)
- > Bei NAS = hängt von Größe und Fähigkeiten des NAS ab (besitzt ein eigenes Dateisystem)
- > Bei VMware ESX = separate VMDKs – auch wenn sie im selben Disk-Volume liegen

4.1.4. DAS, NAS oder SAN: Interessiert das Domino?

Die kurze Antwort darauf lautet: nein. Der Domino-Server interagiert nur mit dem zugrunde liegenden Betriebssystem und verfügt über keine Kenntnisse über die bereitgestellten Speichergeräte. Domino setzt einen schnellen und zuverlässigen Zugriff voraus und trifft keinerlei Vorkehrungen, um eine verlorene Laufwerksverbindung wiederherzustellen oder die Antwortzeiten zu optimieren.

Entsprechend sind auch DAS, NAS oder SAN zulässige Speichergeräte – wenn sie von einem unterstützten Betriebssystem bereitgestellt werden. Für NAS wird die Verwendung von NFS gegenüber CIFS empfohlen, da es bei einer CIFS-Konfiguration zu Datenverlusten kommen kann.

Außerdem sollten NAS-Speichergeräte über ein dediziertes, privates Netzwerk mit dem Domino-Server verbunden sein.

4.1.4.1. Empfehlungen Domino-Daten

- > Verwenden Sie unbedingt RAID10 (statt RAID5).
- > High-End-SAN-Hardware sollte immer RAID10 sein.
- > Erfordert für zufällig verteilte Zugriffe ein rasches Schreiben. Performance hängt ab von Cache, Anzahl der Platten, Performance pro Platte.

4.1.4.2. Empfehlungen Transaktionsprotokoll

- > Erfordert ein schnelles sequenzielles Schreiben.
- > Stellen Sie sicher, dass der Schreibcache aktiviert ist!
- > Hat auf einem NAS nichts zu suchen.
- > Üblicherweise wird dafür ein RAID1 oder eine separate VDisk herangezogen.

Für virtualisierte Umgebungen gilt, dass mehrere kleine Disks besser sind als eine Mega-Disk (Virtualisierung ist mit mehreren kleineren Dateien in der Regel schneller als mit einer großen ...)

4.1.4.3. Empfehlungen DAOS

Im DAOS-Speicher werden ausgelagerte Dateianhänge abgelegt.

- > Dazu brauchen Sie keine besondere Performance, sondern sollten eher eine große sequenzielle Lese-/Schreibleistung bieten.
- > Könnte ein RAID5 oder sogar ein NAS sein.

Details zum DAOS finden Sie in Kap. 9.12 Domino Attachment and Object Service, ab Seite 277.

Um den Großteil der obigen Empfehlungen brauchen wir uns jetzt noch nicht zu kümmern – der Installationsassistent fragt vorerst ja nur Programm- und Dateiverzeichnis ab. Aber wir sollten den Bedarf an weiteren »Platten« nicht aus den Augen verlieren!

4.2. Einen Domino-Server installieren

4.2.1. Übersicht

Die Installation eines Domino-Servers erfolgt in zwei Schritten:

1. Installation der Server-Software
2. Konfiguration des Servers via Setup-Dialog

Bevor Sie Ihren Domino-Server installieren und konfigurieren, sollten Sie sich mit der Namensgebung in Ihrer Organisation auseinandergesetzt haben (siehe Kap. 3.2 Von Zertifizierern und hierarchischen Namen, ab Seite 25). Weiters sollten Sie Ihre Netzwerkkonfiguration kennen und wissen, wie Sie den Domino-Server in das Netzwerk eingliedern.

Zum Aktualisieren einer älteren Domino-Version lesen Sie Kap. 4.10 auf Seite 80.

4.2.2. Vorgangsweise

Laden Sie die Installationsdatei aus dem HCL FlexNet herunter. (Die Datei für HCL Domino 11.0.1 für Windows heißt Domino_1101_Win_English.exe.)

Starten Sie die Installationsdatei lokal und nicht von einem Netzwerklaufwerk, da dies zu Problemen beim Berechnen des vorhandenen Speicherplatzes führen kann.

Haben Sie die Benutzerkontensteuerung aktiviert, deaktivieren Sie diese oder führen Sie die Installation als Administrator aus, indem Sie mit der rechten Maustaste auf die ausführbare Datei klicken und dann im Kontextmenü **Als Administrator ausführen** wählen.

InstallAnywhere bereitet die Installation vor:

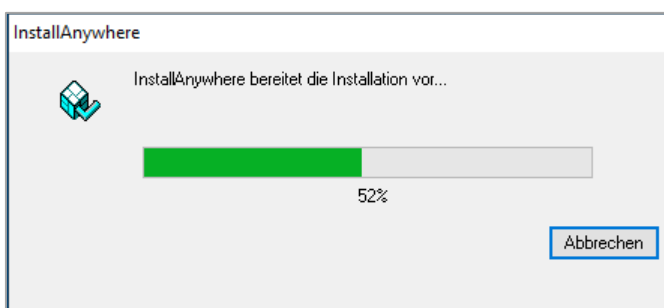


Abbildung 4.1: Server-Installation – Installation wird vorbereitet

Wählen Sie die Installationsssprache und klicken Sie auf **OK**.



Abbildung 4.2: Server-Installation – Auswahl der Installationsssprache

Selbst wenn Sie Deutsch wählen, werden einige Dialoge auf Englisch angezeigt.

Wenn Sie die Einführungsseite sehen, klicken Sie auf **Weiter**:

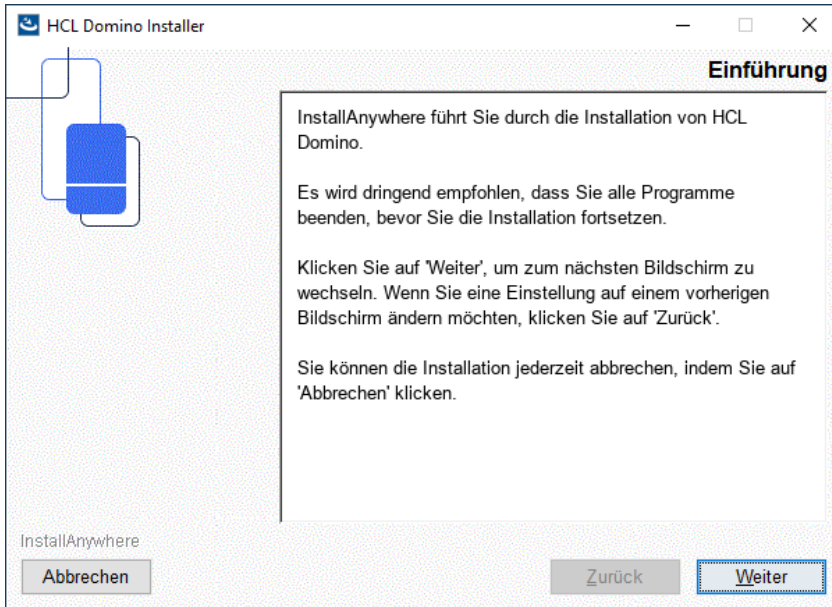


Abbildung 4.3: Server-Installation – Willkommenseite

Klicken Sie auf **Weiter**. Der Lizenzvertrag wird angezeigt:

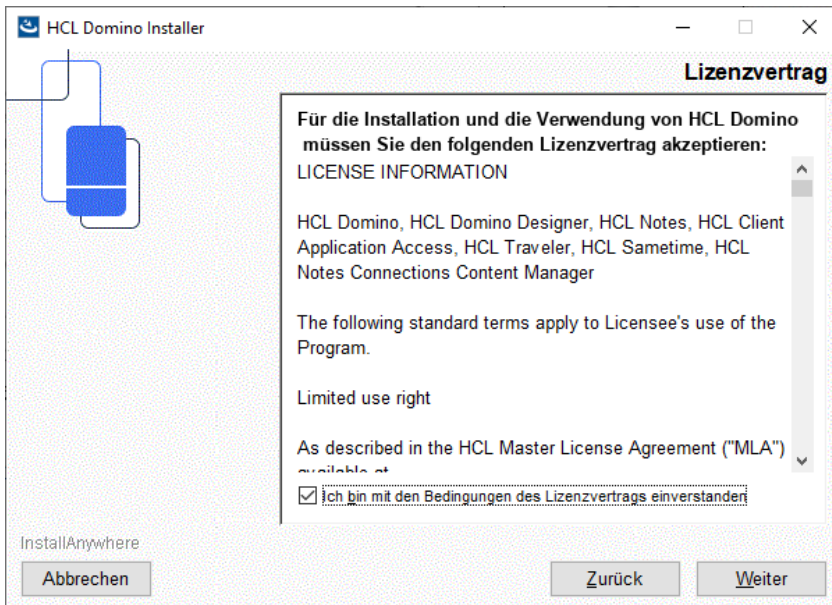


Abbildung 4.4: Server-Installation – Lizenzvertrag

Aktivieren Sie das Kontrollkästchen **Ich bin mit den Bedingungen des Lizenzvertrags einverstanden** und klicken Sie auf **Weiter**.

Wählen Sie nun das Verzeichnis aus, in dem der Server installiert werden soll. Vorgabe ist C:\Program Files\HCL\Domino:

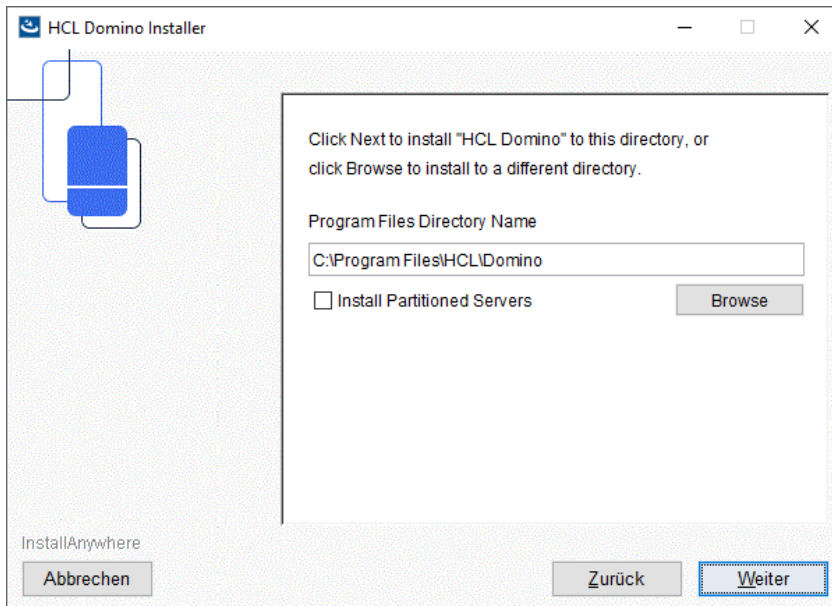


Abbildung 4.5: Server-Installation – Auswahl des Programmverzeichnisses

Aktualisieren Sie eine ältere Version in einem anderen Verzeichnis, schlägt Domino dieses vor. Klicken Sie anschließend auf **Weiter** und wählen Sie das Datenverzeichnis aus:

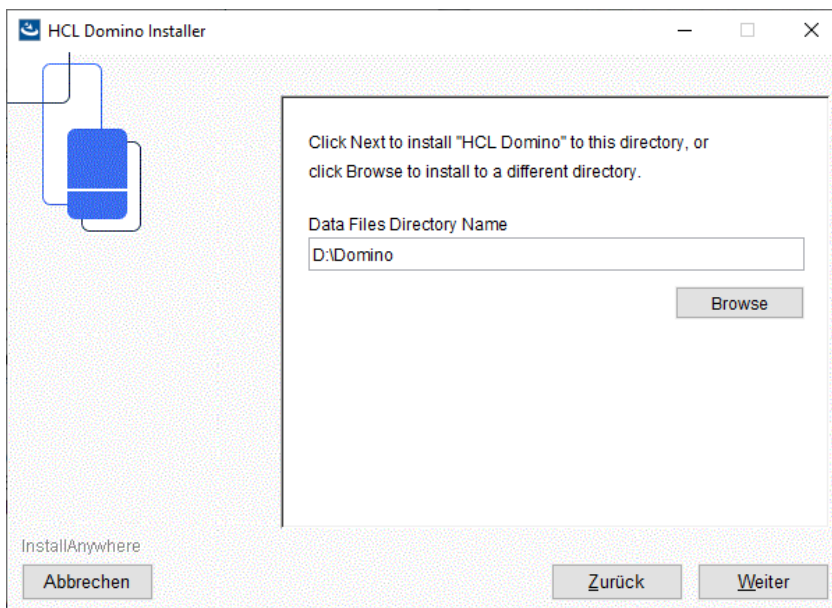


Abbildung 4.6: Server-Installation – Auswahl des Datenverzeichnisses

Tip: Installieren Sie den Domino-Server nie auf einem Dateiserver!

- > Sicherheitsfunktionen könnten bei gemeinsam benutzten Datenverzeichnissen von Benutzern des Netzwerk-Dateiservers umgangen werden.
- > Die Leistung des Dateiservers oder des Domino-Servers geht zurück, wenn einer von beiden lange Verarbeitungszeiten benötigt.
- > Die Stabilität des Dateiservers oder des Domino-Servers wird eventuell beeinflusst.

Wählen Sie möglichst eine eigene Partition. Klicken Sie danach auf **Weiter** und wählen Sie den sogenannten Installationssatz:

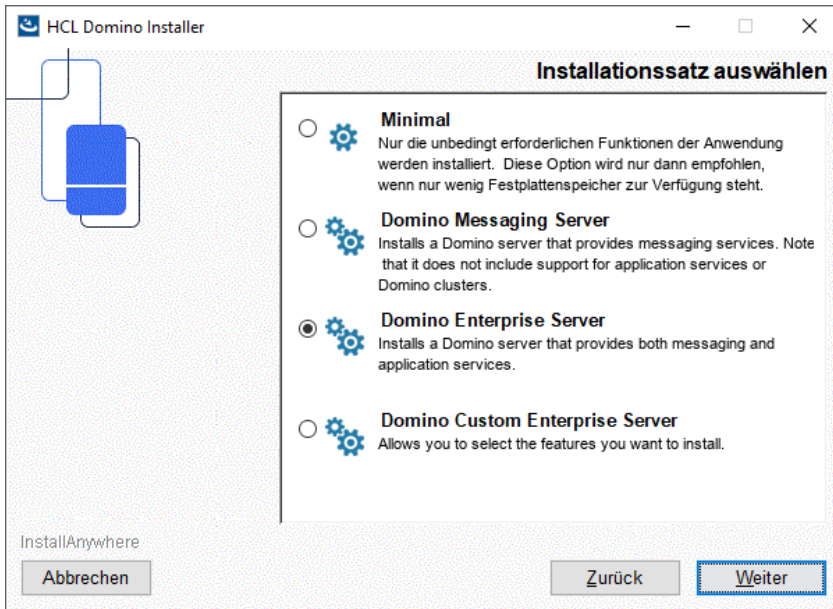


Abbildung 4.7: Server-Installation – Auswahl des Installationssatzes

Die Erklärung der einzelnen Optionen finden Sie in der folgenden Tabelle:

Installationssatz	Erklärung
Minimal	Installiert einen Domino-Server, der nur Unterstützung für Anwendungsdienste bietet. Dieser Installationstyp unterstützt Domino-Cluster, erlaubt jedoch keine Nachrichtendienste (außer Mail-In-Datenbanken).
Domino Messaging Server	Installiert einen Domino-Server, der Nachrichtendienste (Mail, Instant Messaging) bietet. Dieser Installationstyp unterstützt keine Anwendungsdienste oder Domino-Cluster.
Domino Enterprise Server	Installiert einen Domino-Server, der sowohl Nachrichtendienste, als auch Anwendungsdienste bietet und Domino-Cluster unterstützt.
Custom	Entspricht vom Lizenztyp einem Enterprise Server, bei dem jedoch die Features einzeln ausgewählt werden können.

Tabelle 4.2: Die verschiedenen Installationssätze

Welchen Servertyp Sie wählen, hängt natürlich auch von Ihrem Lizenzmodell ab. Lizenzieren Sie etwa pro Benutzer (wie z. B. beim CCB-/CCX- Lizenzmodell), spielt es keine Rolle wie viele und welche Domino-Server Sie betreiben. Wählen Sie in diesem Fall »Domino Enterprise-Server«.

Die folgenden Komponenten sind verfügbar (Situation nach Auswahl von »Minimal«):

- Anwendungen
- Program Files
 - Billing Support
 - Clustering Support
 - Optional Network Drivers
 - Symbols Files
 - Java Support
 - Messaging Server Files
 - Utility Server Files
 - Enterprise Server Files
- Data Files
 - Required Templates
 - Administration Templates
 - Optional Templates
 - Certificate Management
 - Readme Files
 - Dojo
 - Xpages
- Domino Enterprise Connection Services
- iNotes
 - Web Services Data Files
- Domino Directory Sync Services
- Domino As A Windows Service
- Performance Monitoring
- Resource Modeling Engine
- Hilfe
- OS Integration

Abbildung 4.8: Server-Installation – Auswahl der Installationskomponenten

Klicken Sie auf **Weiter**. Der Domino-Server ist nun zur Installation bereit:

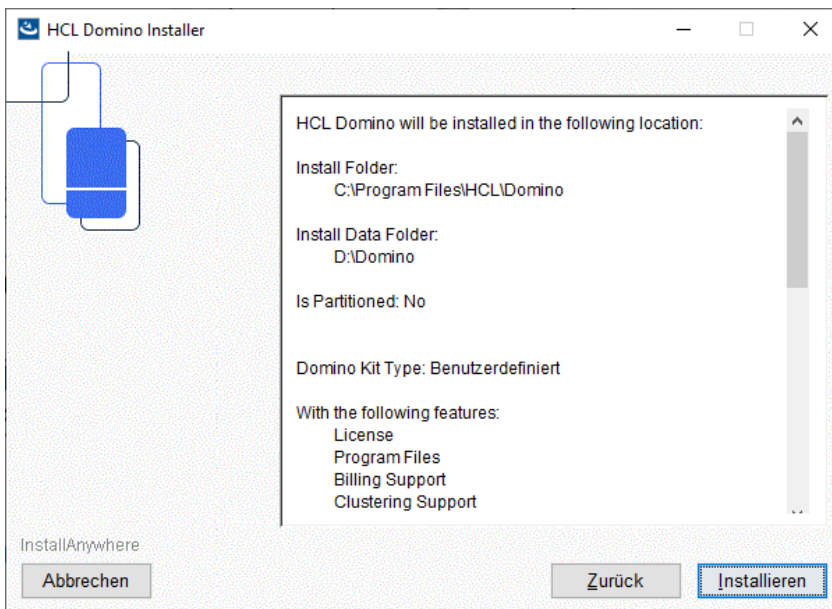


Abbildung 4.9: Server-Installation – Zusammenfassung

Klicken Sie auf **Installieren**, um die Installation zu starten. Die Installationsroutine informiert Sie über den Fortschritt der Installation:

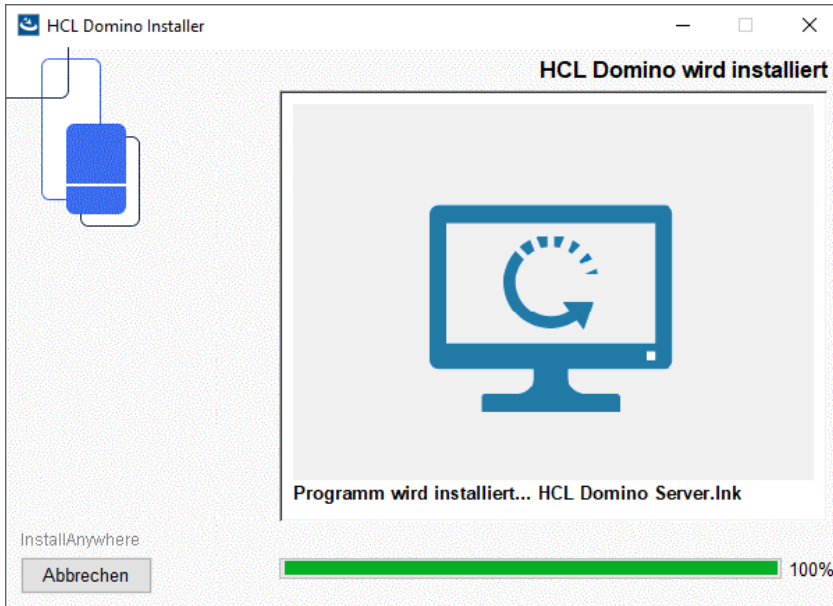


Abbildung 4.10: Server-Installation – Installationsfortschritt

Klicken Sie am Ende der Installation auf **Fertig**:

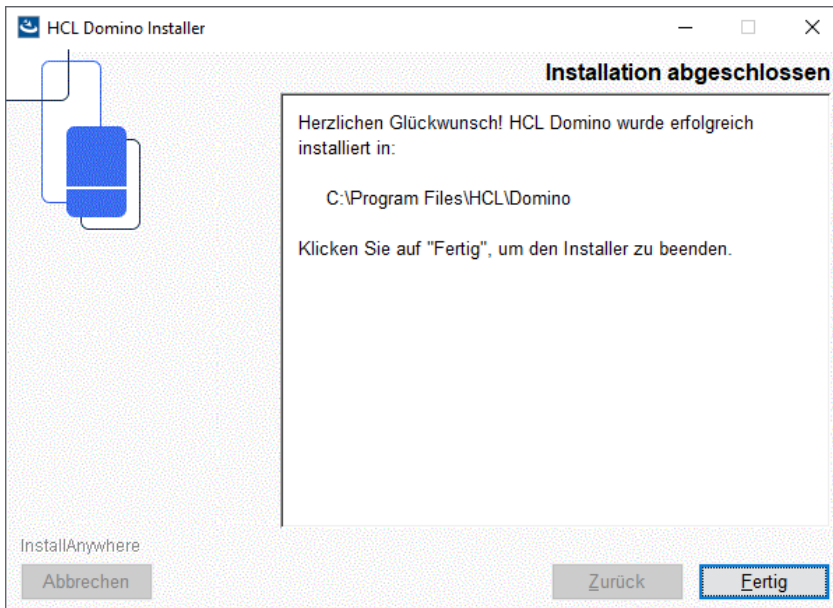


Abbildung 4.11: Server-Installation – Installation ist abgeschlossen

Gibt es für Ihre Version Fehlerkorrekturen (sogenannte Fix Packs - für Domino 11.0.1 gibt es bereits drei), sollten Sie diese sofort einspielen. Mehr dazu erfahren Sie im nächsten Kapitel.

4.3. Fehlerkorrekturen einspielen

HCL stellt bei Bedarf Fehlerkorrekturen zur Verfügung, die **Fix Packs** (FPs) genannt werden. Fix Packs besitzen die folgenden Eigenschaften:

- > werden in regelmäßigen Abständen veröffentlicht (meist einmal pro Quartal, bei Bedarf öfter)
- > existieren als getrennte Downloads für Clients und Server
- > korrigieren verbreitete Kundenprobleme, kritischen Bugs etc.
- > schließen Sicherheitslücken
- > enthalten keine neuen Features
- > sind kumulativ und enthalten auch die Korrekturen der vorhergehenden Fix Packs (außerdem Korrekturen der mit früheren Fix Packs eingeschleppten Fehlern – den sogenannten **Regressi-
onen**).
- > sind immer auch in nachfolgenden **Maintenance Releases** (z. B. 11.0.1) enthalten
- > sind nicht sprachspezifisch, d. h. Sie verwenden ein und dasselbe Fix Pack für den englischen oder deutschen Client
- > ändern keine Schablonen, die mit installierten Sprachpaketen kollidieren würden, d. h. sie korrigieren auch keine Fehler. Schablonen von Systemdatenbanken, die nur auf Englisch vorliegen, sowie der iNotes Web Access (Webmail) werden bei Bedarf jedoch ersetzt und müssen über das Serverprogramm Design (siehe Kap. 11.2.3.2 Der Servertask Design, ab Seite 309) verteilt werden.
- > werden zwar getestet (Bug-Fix-Verifikation, Regressionstests, Interoperabilitäts-Tests mit anderen Produkten), aber nicht so ausführlich wie neue Versionen

Wie Sie in obiger Liste lesen können, sind Fix Packs kumulativ, d. h. jedes Fix Pack enthält auch die Korrekturen der vorhergehenden, sodass Sie immer nur die letzte Version installieren müssen. Für Version 11.0.1 gibt es derzeit vier Fix Packs, für Domino 10.0.1 sechs. Wenn Sie also einen Domino 11.0.1-Server betreiben und noch kein Fix Pack eingespielt haben, müssen Sie nicht zuerst FP1 installieren und danach FP2 usw., sondern können gleich mit FP4 beginnen.

Bei dringenden (Sicherheits-) Problemen stellt die HCL manchmal auch **Interim Fixes** (IFs) oder **Hot Fixes** (HFs) zur Verfügung. Diese werden nicht so umfangreich getestet und sollten nur eingespielt werden, wenn ein dringendes Problem besteht. Außerdem wird man sie nachher unter Umständen nicht mehr so leicht los.

Fix Packs besitzen ihren eigenen Installer, der gelegentlich auch Probleme macht. Beachten Sie daher die folgenden Regeln:

- > Fahren Sie vor der Installation den Server herunter und beenden Sie alle auf Notes und Domino bezogenen Prozesse.
- > Installieren Sie nie von einem Netzwerklaufwerk aus.
- > Führen Sie auf Servern mit aktivierter Benutzerkontensteuerung den Fix Pack-Installer unbedingt als Administrator aus.

4.3.1. A Notes/Domino related process is still running ...

Sollte bei Ihnen der folgende Fehler angezeigt werden: »Lotus Notes/Domino or a Notes / Domino related process is still running. Please close it before pressing OK to continue«, dann starten Sie den Task Manager und überprüfen Sie, ob noch Notes- oder Domino-Prozesse laufen. Sollte das der Fall sein, beenden Sie diese Prozesse. Manchmal ist das jedoch nicht der Fall und dann ist der Schuldige meist der Dienst **Windows Management Instrumentation Service** (auf Deutsch: **Windows-Verwaltungsinstrumentation**). Stoppen Sie den Dienst und beeilen Sie sich mit der Installation, da er von selbst wieder startet ...

Ein anderer Trick besteht darin, das Domino-Programmverzeichnis umzubenennen (z. B. in C:\Program Files\HCL\DominoX), den Rechner neu zu starten und dann das Verzeichnis wieder zurückzubenennen. Wenn Sie dann den Fix Pack-Installer ausführen, sollte die Installation durchlaufen.

4.3.2. Ein Fix Pack entfernen

Um ein Fix Pack zu entfernen, müssen Sie es erneut installieren. Der Fix Pack-Installer erkennt, dass das Fix Pack bereits installiert ist und bietet an, es zu entfernen.

Achtung: Sollte die Installation eines Fix Packs scheitern, wird sie vom Installer normalerweise rückgängig gemacht. Nach einem Abbruch kann es aber auch passieren, dass der Installer die Version nicht mehr erkennt und das Fix Pack weder erneut installiert noch entfernt werden kann. In diesem Fall müssen Sie die letzte Domino-Version erneut installieren.

4.4. Sprachen installieren

Den Domino-Server selbst gibt es nur auf Englisch. Es ist jedoch möglich, anderssprachige Schablonen zu installieren, welche von HCL in Form von **Server Language Packs** bereitgestellt werden. HCL ordnet Sprachen verschiedenen Gruppen mit verschiedenen Prioritäten zu. Für Version 11 sind die folgenden Sprachen verfügbar:

Gruppe	Sprachen
G1	Englisch, Deutsch, Japanisch, Brasilianisches Portugiesisch, Französisch, Italienisch, Spanisch, Koreanisch, Chinesisch
G2	Arabisch, Niederländisch, Schwedisch, Tschechisch, Polnisch, Russisch
G3	Dänisch, Finnisch, Norwegisch, Katalanisch, Hebräisch, Ungarisch, Slowenisch, Thailändisch, Türkisch

Tabelle 4.3: Sprachgruppen

Sprachpakete sind versionsspezifisch, d. h., Sie müssen mit jedem Update des Domino-Servers auf die Verfügbarkeit des passenden Sprachpakets warten – auch bei so kleinen Versionsprüngen wie von 11.0 auf 11.0.1! Die G1-Sprachen erscheinen meist gleichzeitig mit einer neuen Version, die anderen Gruppen in der Regel einige Wochen später.

Hier nochmals der Hinweis, dass Fix Packs die Auswahl des Sprachpakets nicht beeinflussen, das heißt, Sie installieren bei 11.0.1 dasselbe Sprachpaket wie bei 11.0.1 FP3.

Die Installation des Sprachpakets kann gleich nach der Installation des Domino-Servers erfolgen oder auch später.

4.4.1. Alternativen zum Language Pack

Manche Admins installieren kein Sprachpaket, sondern kopieren die mit dem deutschen Notes-Client mitgelieferten Schablonen unter geänderten Datei- und Schablonennamen auf den Server, z. B. die Mailschablone als mail11de.ntf. Diese Methode bewährt sich vor allem dann, wenn Sie nur ganz bestimmte Datenbanken auf Deutsch zur Verfügung stellen wollen – etwa nur die Maildatenbank. Außer dass Sie dann mit mehreren Schablonen hantieren müssen, ist mir kein Nachteil bekannt.

4.4.2. Installation des Sprachpakets am Server

Laden Sie das Sprachpaket für die aktuelle Domino-Version von FlexNet herunter (zum Zeitpunkt der Veröffentlichung dieses Buchs war das Domino_1101_SLP_German.tar) und extrahieren Sie es in einen Ordner im lokalen Dateisystem des Domino-Servers.

Die Setup-Routine startet nicht automatisch, öffnen Sie daher den Ordner und suchen Sie nach der ausführbaren Datei für Windows. Diese heißt sowohl für Version 11 als auch für Version 11.0.1 WINDomLP1100.exe.

Um das Sprachpaket zu installieren, gehen Sie wie folgt vor:

1. Beenden Sie den Domino-Server.
2. Starten Sie die ausführbare Datei als Administrator (mit der rechten Maustaste auf die Datei klicken und im Kontextmenü **Als Administrator ausführen** wählen). Starten Sie die Installationsdatei niemals aus einem Netzwerkordner, da sie den notwendigen Speicherplatz sonst nicht ermitteln kann.
3. Der Startbildschirm wird angezeigt:



Abbildung 4.12: Installation Sprachpakete – Auswahl Installationsprache

4. Wählen Sie die Installationsprache und klicken Sie auf **OK**.

5. Der Willkommensbildschirm wird angezeigt:

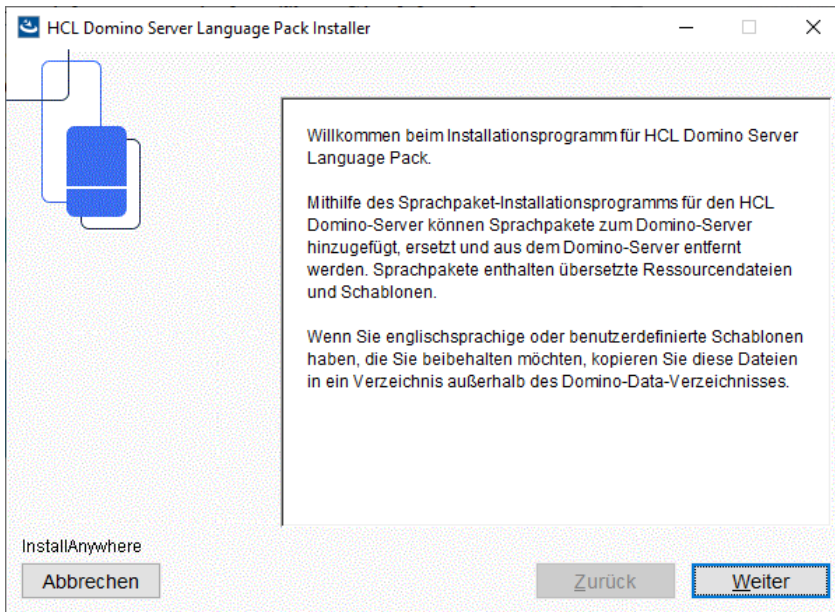


Abbildung 4.13: Installation Sprachpakete – Willkommensseite

6. Klicken Sie auf **Weiter**. Der Lizenzvertrag wird angezeigt:



Abbildung 4.14: Installation Sprachpakete – Lizenzvertrag

7. Aktivieren Sie das Kontrollkästchen **Ich bin mit den Bedingungen des Lizenzvertrags einverstanden** und klicken Sie auf **Weiter**.
8. Sie werden nach dem Programmverzeichnis des Domino-Servers gefragt. Es wird das Installationsverzeichnis aus der Windows-Registrierdatenbank vorgeschlagen:

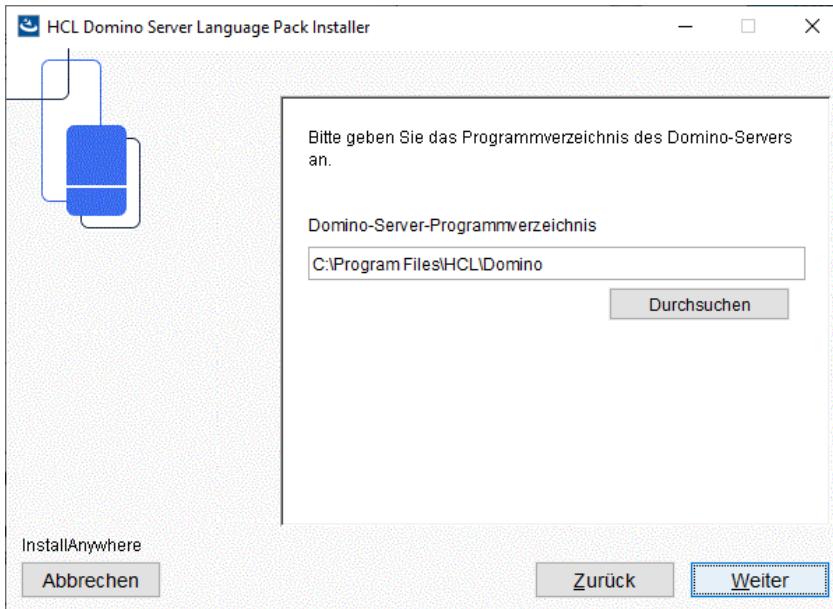


Abbildung 4.15: Installation Sprachpakete – Auswahl Programmverzeichnis

9. Klicken Sie auf **Weiter**. Das Datenverzeichnis wird abgefragt:

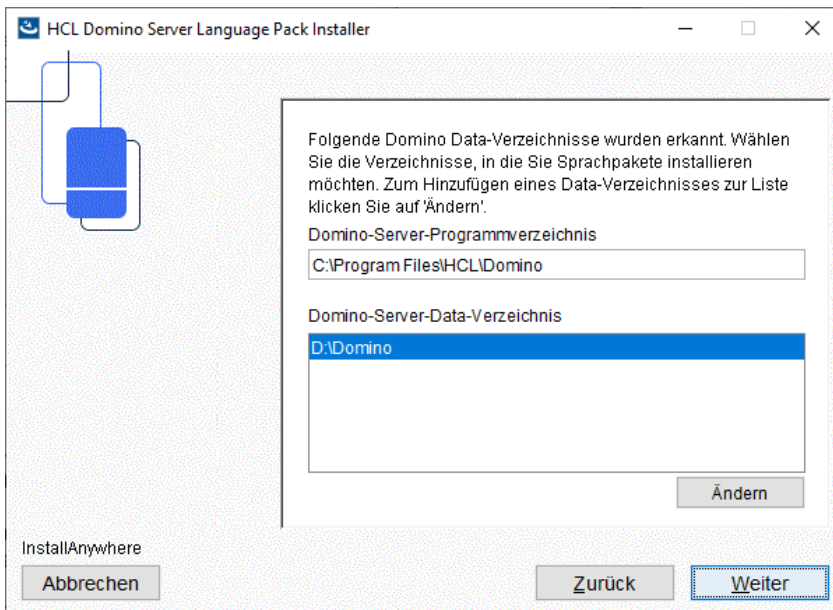


Abbildung 4.16: Installation Sprachpakete – Auswahl Programm- und Datenverzeichnis

Auch hier sollte die Vorgabe passen. Ist es nicht der Fall, etwa, weil Sie das Datenverzeichnis nach der letzten Installation verschoben haben, korrigieren Sie es. Klicken Sie auf **Weiter**.

10. Wählen Sie einen Installationssatz aus,

Wählen Sie die Option »Sprachpaket hinzufügen«, wenn deutsche Gestaltungselemente zu den ausgelieferten englischen Schablonen hinzugefügt werden sollen. Diese Datenbanken liegen dann zweisprachig auf Englisch und Deutsch vor.

Die meisten Systemdatenbanken und somit auch das Domino-Verzeichnis bleiben englisch. Deutsch wird nur zu Schablonen mit einem Benutzerkontext hinzugefügt, sodass Sie beim Erstellen einer neuen Anwendung entscheiden können, ob Sie nur Deutsch, nur Englisch oder beide Sprachen enthalten soll. Enthält eine Datenbank zwei oder mehrere Sprachen, entscheidet die im Client eingestellte **Inhaltssprache** (Content Language), in welcher Sprache die Gestaltungselemente angezeigt werden. (Die Inhaltssprache ändern Sie im Menü unter **Datei > Vorgaben... > Ländereinstellungen**)

Wählen Sie die Option »Sprachpaket ersetzen«, wenn die mit dem Domino-Server ausgelieferten englischen Schablonen durch deutsche ersetzt werden sollen.

Damit werden nicht nur Datenbanken mit Benutzerkontext, sondern auch die meisten Systemdatenbanken wie das Domino-Verzeichnis deutsch. Nur Systemdatenbanken, für die es keine deutsche Schablone gibt, z. B. »Monitoring Configuration« oder »Domino Backup«, bleiben englisch.

Wählen Sie die Option »Sprachpaket entfernen«, wenn ein zuvor installiertes Sprachpaket entfernt werden soll.

Natürlich sollten alle Datenbanken, mit denen Endanwender zu tun haben, wie Mail, Diskussion oder TeamRoom auf Deutsch verfügbar sein. Es spricht jedoch einiges dafür, Systemdatenbanken wie das Domino-Verzeichnis auf Englisch zu belassen:

- > Englische Schablonen sind besser getestet, enthalten weniger Fehler und werden mit mehr Sorgfalt erstellt (Spalten und Tasten sind immer breit genug für Beschriftungen und Einstellungen etc.)
- > Deutsche Schablonen enthalten häufiger Fehler
- > Unterstützung und Anleitungen finden sich im Internet praktisch nur auf Englisch

Für das Ersetzen durch Deutsch gilt:

- > Keine Sprachmischungen!
- > Keine Akzeptanz durch Endanwender!
- > Manchmal geht es gar nicht darum, ob Ihre Mitarbeiter Englisch *können*, sondern ob sich eine deutsche, österreichische oder Schweizer Firma mit einer englischsprachigen Software auseinandersetzen *will*.

Alle Darstellungen in diesem Buch wurden mit deutschen Schablonen erstellt (außer eine Datenbank liegt nur auf Englisch vor).

Sehen wir uns nun je nach Auswahl von »Sprachpaket ersetzen« oder »Sprachpaket hinzufügen« die Unterschiede bei der weiteren Installation an (immer beginnend mit 11.).

4.4.2.1. Sprachpaket ersetzen

Sehen wir uns zuerst an, was passiert, wenn wir die mitgelieferte Sprache Englisch durch Deutsch ersetzen:

11. Wählen Sie auf der Seite **Installationssatz auswählen** die Option »Sprachpaket ersetzen«:

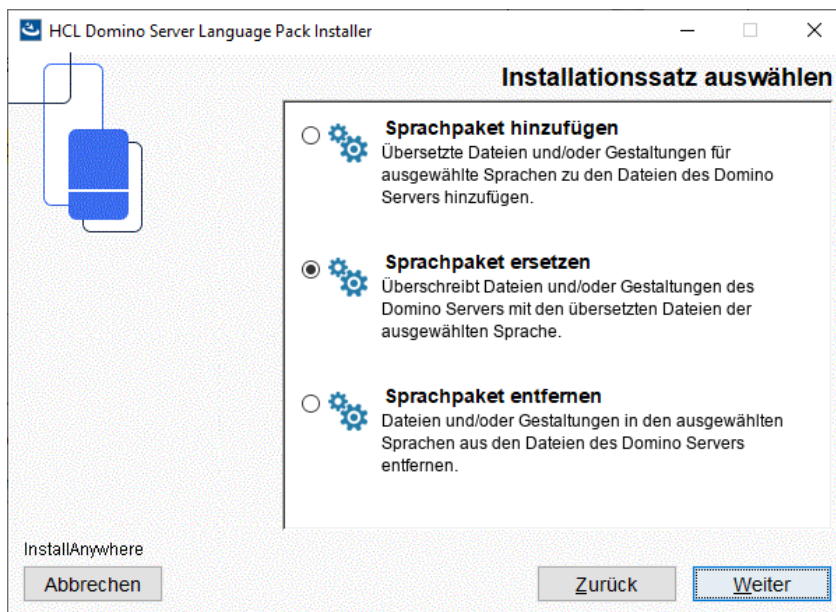


Abbildung 4.17: Installation Sprachpakete – Installationssatz wählen

12. Klicken Sie auf **Weiter**. Im nächsten Schritt wird die Version überprüft:

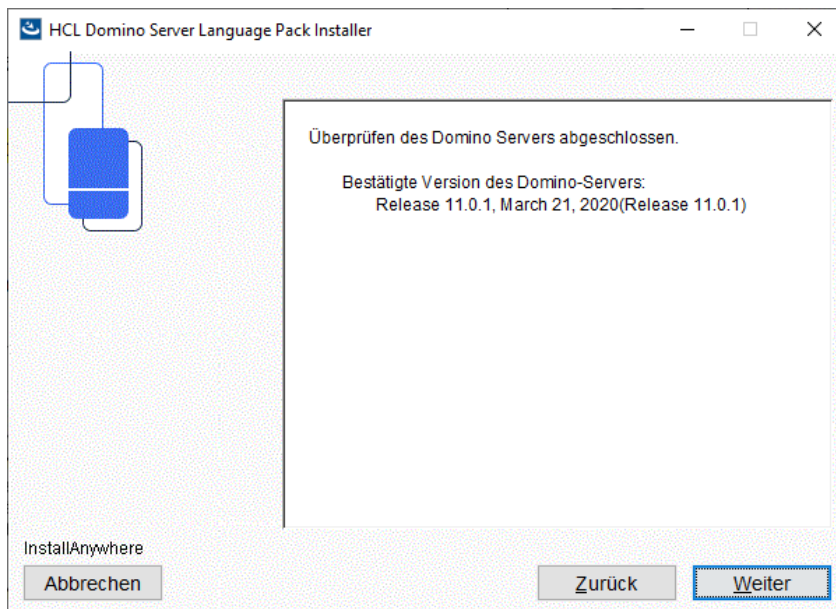


Abbildung 4.18: Installation Sprachpakete – Überprüfen der Version

13. Klicken Sie auf **Weiter**. Da man die Vorgabesprache Englisch nur durch eine andere Sprache ersetzen kann, ist diese bereits ausgewählt:

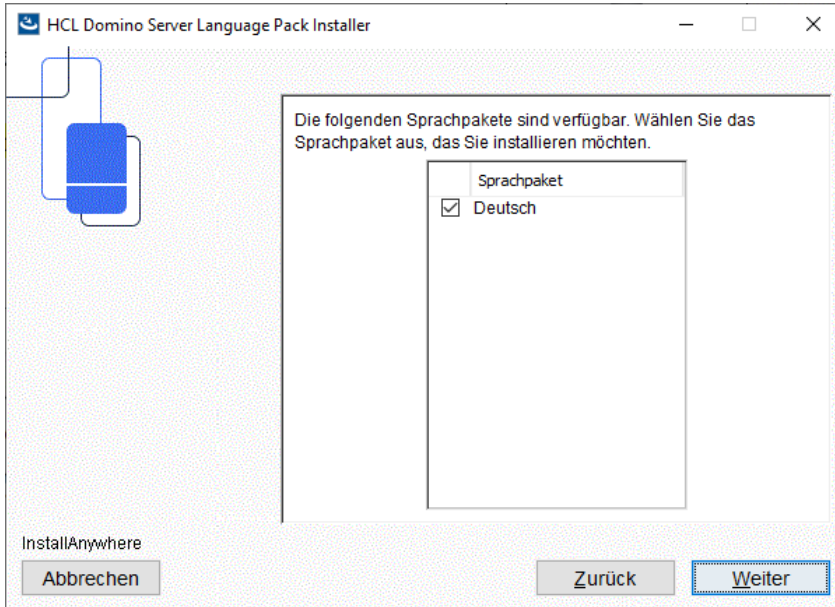


Abbildung 4.19: Installation Sprachpakete – Sprache wählen

14. Klicken Sie auf **Weiter**.

4.4.2.2. Sprachpaket hinzufügen

11. Wählen Sie auf der Seite **Installationssatz auswählen** die Option »Sprachpaket hinzufügen«:

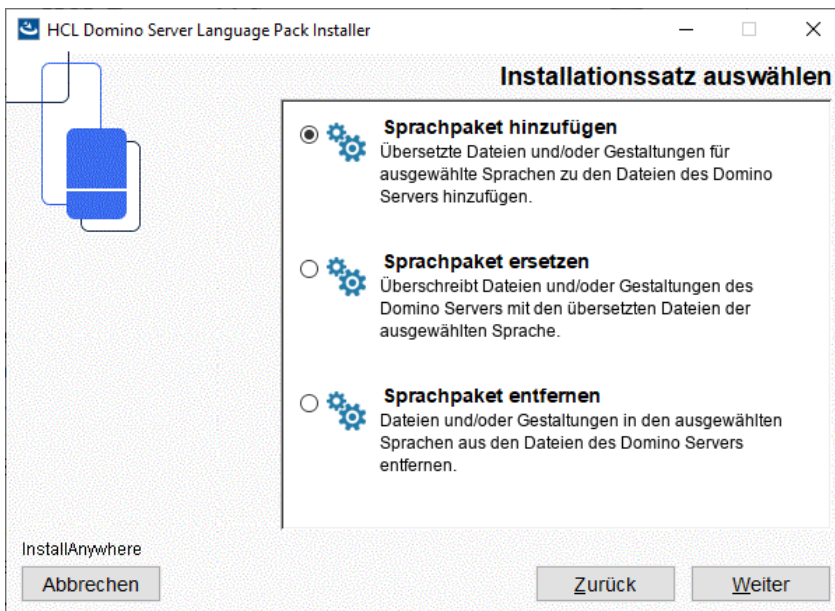


Abbildung 4.20: Installation Sprachpakete – Installationssatz wählen

12. Im nächsten Schritt wird die Version überprüft. Da die Sprachdateien kurzfristig im Dateisystem abgelegt werden, wird dafür Platz benötigt.

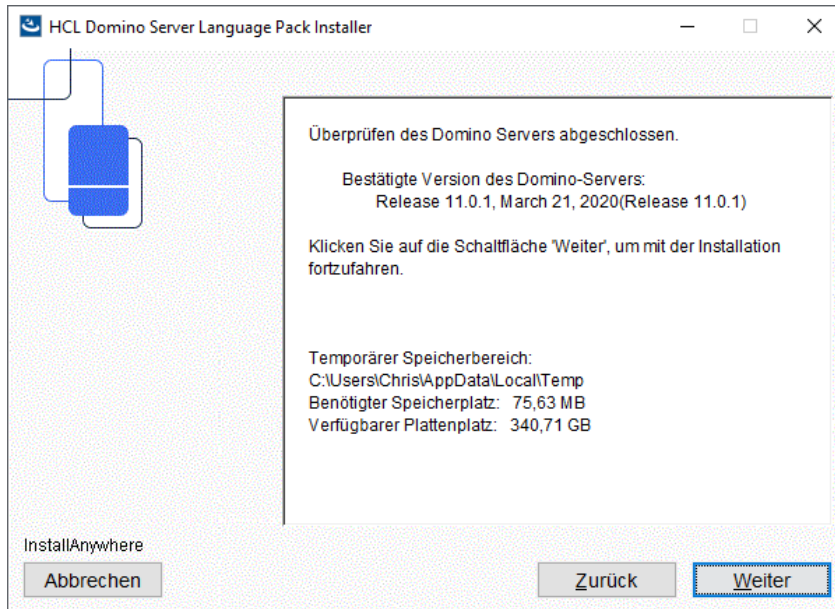


Abbildung 4.21: Installation Sprachpakete – Zusammenfassung

13. Es können prinzipiell mehrere Sprachen hinzugefügt werden, daher müssen Sie, selbst wenn das Sprachpaket nur eine Sprache enthält, diese auswählen:

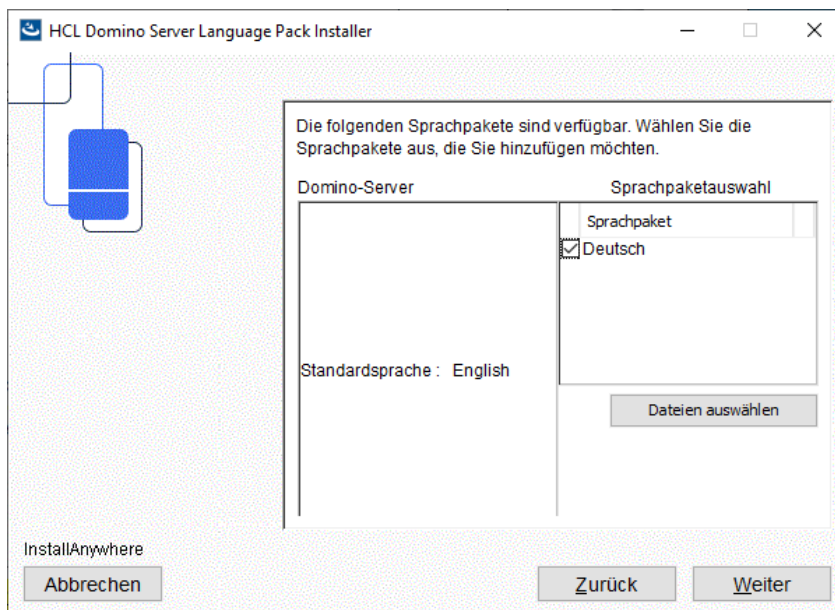


Abbildung 4.22: Installation Sprachpakete – Auswahl Sprachen

Beachten Sie, dass Englisch Standardsprache bleibt, d. h. alle Systemdatenbanken inklusive des Domino-Verzeichnisses bleiben englisch!

(Optional) Klicken Sie auf die Schaltfläche **Dateien auswählen**, um zu erfahren, welche Schablonen auf Deutsch verfügbar sind:

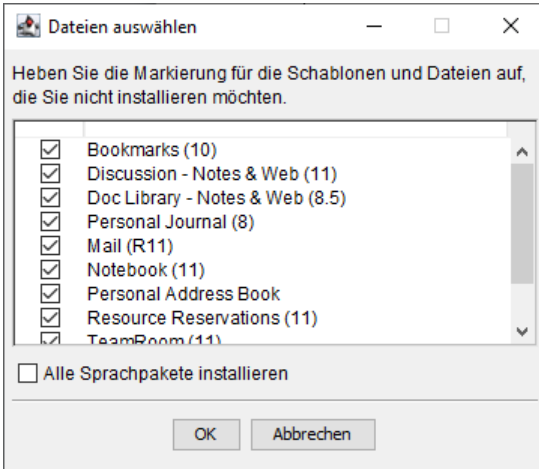


Abbildung 4.23: Installation Sprachpakete – Auswahl Schablonen

Wie Sie zweifelsfrei erkennen können, wird Deutsch nur zu Schablonen hinzugefügt, die einen Benutzerbezug aufweisen.

14. (Optional) Sollten Sie eine bestimmte Schablone nicht installieren wollen, entfernen Sie das Häkchen vor dem Eintrag und klicken Sie auf **OK**.
15. Klicken Sie auf **Weiter**.
16. Im nächsten Schritt wird der Speicherplatz ermittelt:

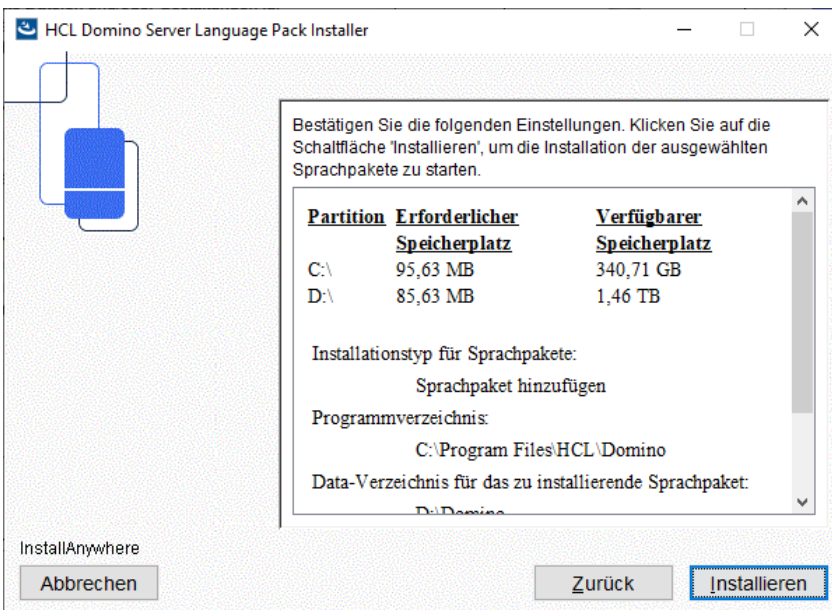


Abbildung 4.24: Installation Sprachpakete – Berechnung Speicherplatz

17. Klicken Sie auf **Installieren**.
18. Klicken Sie nach Installation des Sprachpakets auf **Fertig**:

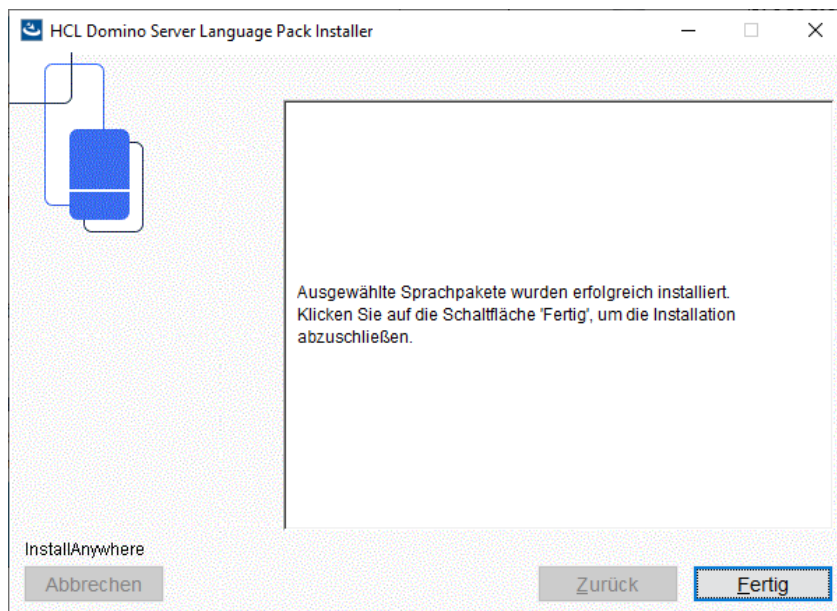


Abbildung 4.25: Installation Sprachpakete – Installation abschließen

Achtung: Haben Sie »Sprachpaket ersetzen« gewählt und somit die englischen Originalschablonen mit den Schablonen des Sprachpakets überschrieben, können Sie nur zu Englisch zurückkehren, indem Sie die Server-Software erneut installieren.

Treten während der Installation grobe Fehler auf (z. B. eine falsche Serverversion, nicht genug Platz auf dem Speichermedium u. a.) wird die Installation abgebrochen. Einige Fehler führen jedoch nicht zu einem Abbruch, etwa wenn eine Schablone eine falsche Sprache enthielt und Deutsch nicht hinzugefügt werden konnte. Diese »kleineren« Fehler werden in der Datei LPlog.txt im Domino-Programmverzeichnis protokolliert.

4.5. Einen ersten Domino-Server einrichten

4.5.1. Voraussetzungen

Sie haben sich mit Themen wie Organisation und Domäne wie in Kap. 3.2 Von Zertifizierern und hierarchischen Namen, ab Seite 25 beschrieben, auseinandergesetzt.

Sie haben den Server, den Sie jetzt einrichten wollen, wie in Kap. 4.2 Einen Domino-Server installieren, ab Seite 33 beschrieben, bereits installiert.

Wenn es bereits einen Domino-Server in Ihrem Unternehmen gibt, und Sie jetzt einen zusätzlichen Server einrichten wollen, lesen Sie stattdessen Kapitel 4.9 Einen zusätzlichen Domino-Server einrichten, ab Seite 74.

4.5.2. Schritt-für-Schritt-Anleitung

1. Doppelklicken Sie das Symbol HCL Domino-Server, um die Einrichtung zu starten:



2. Das Server-Setup wird geladen und der Setup-Dialog (nur auf Englisch verfügbar) angezeigt. Auf der ersten Seite können Sie bei Bedarf die Schriftart anpassen. Klicken Sie auf **Next >**, um zur nächsten Seite zu gelangen.
3. Wir konfigurieren den ersten Server des Unternehmens und wählen daher die Option »Set up the first server or a stand-alone server«:

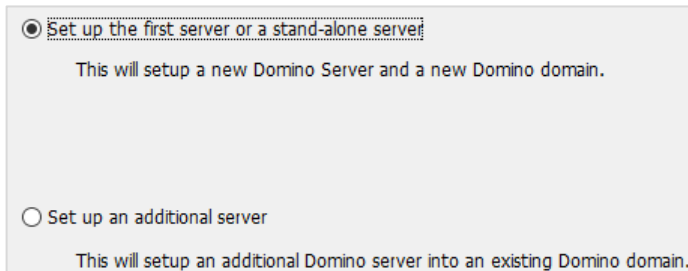


Abbildung 4.26: Installationsmodus wählen

Das bedeutet, dass beim Einrichten des Servers auch Organisation und Domäne erstellt werden.

4. Geben Sie auf der nächsten Dialogseite den Servernamen und gegebenenfalls einen Servertitel ein:

Abbildung 4.27: Servername eingeben

Der Titel hat rein informativen Charakter und kann jederzeit geändert werden. Der Servername kann später nicht geändert werden, Sie können nur einen neuen Server registrieren. Überlegen Sie sich daher nicht nur den Namen selbst, sondern auch seine Schreibweise.

5. Geben Sie einen Namen für Ihr Unternehmen ein.
Der Name kann zwischen drei und 64 Zeichen lang sein.

Überlegen Sie sich nicht nur den Namen selbst, sondern auch seine genaue Schreibweise, denn er kann später nicht geändert werden!

Für das Unternehmen wird im Datenverzeichnis des Servers eine Zulassungsdatei mit dem Namen cert.id abgelegt. Diese Datei sollte gleich nach dem Einrichten in einem sicheren Bereich kopiert und danach aus dem Datenverzeichnis entfernt werden.

6. Geben Sie ein Kennwort zum Schutz der Zertifizierer-ID ein.

Kennwörter dürfen maximal 32 Zeichen inklusive Leerzeichen enthalten. Beachten Sie, dass zwischen Groß- und Kleinschreibung unterschieden wird.

An dieser Stelle gibt es nur eine Minimalanforderung von fünf Zeichen, Sie sollten jedoch ein komplexeres Kennwort wählen.

7. Klicken Sie auf **Customize...**, um weitere Optionen anzuzeigen.

8. (Optional) Geben Sie den Namen einer Unterorganisation (OU) ein. Wenn Sie eine zusätzliche OU eingeben:

1. wird der Server innerhalb dieser OU registriert (erhält also einen zweiten Schrägstrich im Namen, z. B.: `Server1/SRV/COB/AT`, wenn der Name der OU `SRV` lautet)
2. wird eine OU-Zulassungsdatei mit dem Namen `oucert.id` erstellt und im Datenverzeichnis des Servers gespeichert.

9. (Optional) Wählen Sie eine Länderkennung aus:

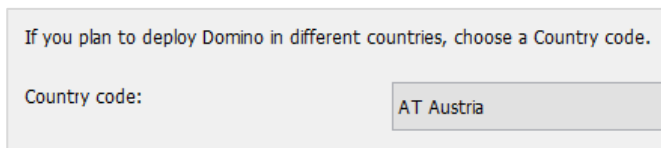


Abbildung 4.28: Wählen Sie eine Länderkennung

Wenn Sie eine Länderkennung auswählen, gehört diese untrennbar zum Namen der Organisation!

10. Klicken Sie auf **OK** und navigieren Sie durch Klicken auf **Next** > zur nächsten Dialogseite.

11. Geben Sie den Namen der Domäne ein.

Domänennamen sollten möglichst aus einem einzelnen Wort bestehen und keine Punkte enthalten. Kleinen Unternehmen empfehle ich, den Namen der Organisation zu verwenden.

Der Name der Domäne kann später geändert werden, was jedoch mit relativ viel Aufwand verbunden ist.

12. Geben Sie den Namen des zuständigen Administrators ein.

Tragen Sie generische Namen wie »Admin« im Feld Nachname ein. Verwenden Sie Vor- und Nachname, so dürfen beide nicht länger als 80 Zeichen lang sein.

13. Geben Sie ein Kennwort zum Schutz der Administrator-ID ein. Mindestanforderung ist fünf Zeichen.

14. Setzen Sie ein Häkchen bei **Also save a local copy of the ID file** wird die Administrator-ID zusätzlich unter dem Namen `admin.id` im Domino-Datenverzeichnis abgelegt. Das ist später hilfreich, wenn Sie mehrere Admin-Clients mit dieser ID einrichten wollen; Sie sollten jedoch nicht vergessen, die Datei später aus dem Datenverzeichnis des Servers zu entfernen.

15. Navigieren Sie zur nächsten Seite und wählen Sie die Dienste (Services), die beim Hochfahren des Servers automatisch gestartet werden sollen:



Abbildung 4.29: Wählen Sie die benötigten Dienste aus

16. Wählen Sie »Web Browsers« und »Internet Mail Clients« und klicken Sie dann auf **Customize...**, um Tasks, die Sie nicht brauchen, abzuwählen (z. B. POP3 oder IMAP):

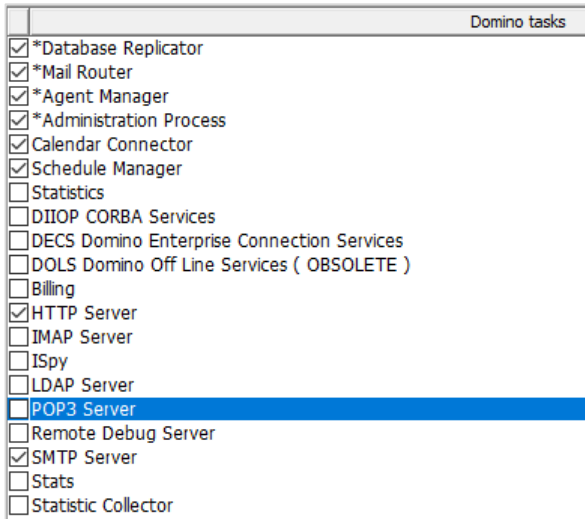


Abbildung 4.30: Liste der verfügbaren Dienste bzw. Server-Tasks

17. Navigieren Sie weiter zu den **Domino Network Settings** und klicken Sie auf **Customize...**, um zu den Details zu gelangen:

Notes Port Driver	Notes Network (Editable)	Host Name (Editable)	Encrypt	Compress
<input checked="" type="checkbox"/> TCP/IP	TCP/IP Network	WS01	<input type="checkbox"/>	<input type="checkbox"/>

Abbildung 4.31: Netzwerkeinstellungen

Host Name: Doppelklicken Sie dieses Feld, um den Namen des Hostrechners einzutragen. Ob Sie ein Domänensuffix angeben, hängt von der Verfügbarkeit Ihres DNS-Servers ab. Läuft er verlässlich, ist die Angabe des voll qualifizierten Hostnamens flexibler. (Mit eingeschalteter NETBIOS-Namensauflösung können Sie gegebenenfalls auch auf das Domänensuffix verzichten.) Läuft der DNS-Server nicht verlässlich, geben Sie lieber die IP-Adresse an.

Encrypt: Aktivieren Sie dieses Feld, wenn die Kommunikation über NRPC verschlüsselt ablaufen soll. Wenn Sie keinen triftigen Grund haben, würde ich eher davon absehen. Weitere Details dazu finden Sie in Kap. 12.2 Netzwerkverschlüsselung, ab Seite 321.

Compress: Die Netzwerkkomprimierung sollten Sie auf jeden Fall einschalten – es gibt kaum eine einfachere Weise, die Performance zu steigern. (Die Möglichkeit, das auszuschalten, stammt noch aus Zeiten, als ein 80836er eine Highend-Maschine darstellte.)

18. Geben Sie einen voll qualifizierten Internet-Hostnamen für Ihren Server ein:

Type the fully qualified internet host name for this Domino server:

For example: host1.acme.com

Abbildung 4.32: Voll qualifizierter Internet-Hostname

19. Klicken Sie auf **Next**. Geben Sie an, ob »Anonymous« (für nicht authentifizierte Benutzer) mit dem Recht »Kein Zugriff« in die Zugriffskontrolllisten aller Datenbanken und Schablonen aufgenommen werden soll. Diese Aktion wird unbedingt empfohlen!

Geben Sie außerdem an, ob die Gruppe »LocalDomainAdmins« mit Managerzugriff in die Zugriffskontrolllisten aller Datenbanken und Schablonen aufgenommen werden soll. Diese Aktion ist nicht zu aktivieren, wenn Ihre Administratorengruppe anders heißt.

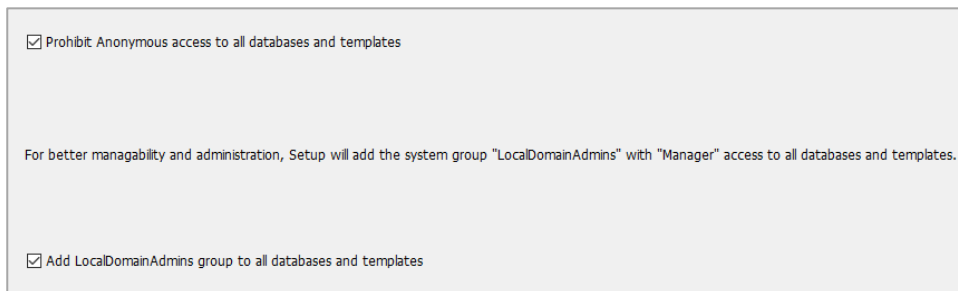


Abbildung 4.33: Optionen zum Eintragen von Anonymous und der Gruppe LocalDomainAdmins

20. Eine Zusammenfassung wird angezeigt. Klicken Sie auf **OK**, um die Konfiguration zu starten.

4.5.3. Über den Konfigurationsablauf

Der folgende Dialog zeigt den Fortschritt bei der Konfiguration des ersten Servers:

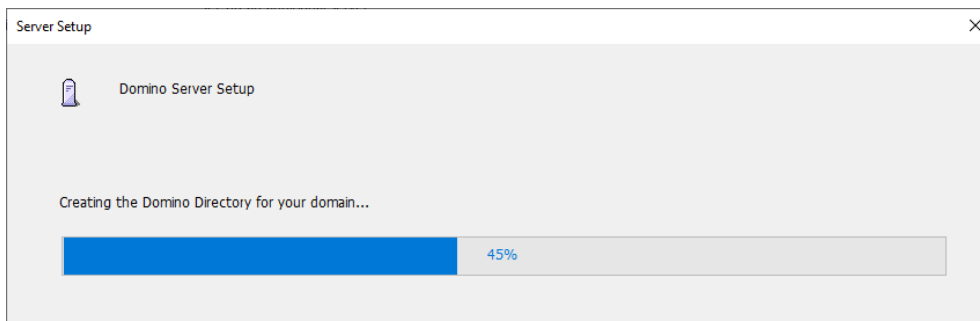


Abbildung 4.34: Verlaufs balken während der Konfiguration

Während der Konfiguration werden ...

- > das Domino-Verzeichnis (names.nsf) im Datenverzeichnis des Servers erstellt.
- > das Zertifizierungsprotokoll (certlog.nsf) im Datenverzeichnis des Servers erstellt.
- > die Unternehmenszulassungsdatei (cert.id) im Datenverzeichnis generiert. Sie wird mit dem bei der Konfiguration angegebenen Kennwort verschlüsselt. Erstellt zusätzlich ein Dokument für den Zertifizierer im Domino-Verzeichnis.
- > (wenn ausgewählt) der Zertifizierer für die angegebene Unternehmenseinheit (oucert.id) erstellt und im Datenverzeichnis abgelegt. Zusätzlich wird ein Dokument für den Zertifizierer im Domino-Verzeichnis erstellt.
- > die Server-ID (server.id) erstellt und im Datenverzeichnis abgelegt. Die Server-ID wird mit der Zulassungs-ID zertifiziert.
- > das Serverdokument im Domino-Verzeichnis erstellt und die von Ihnen während der Konfiguration angegebenen Informationen übertragen.
- > die Benutzer-ID für den Administrator (user.id) erstellt und mit der Zulassungs-ID zertifiziert.
- > das Personendokument für den Administrator im Verzeichnis erstellt und darin die user.id als Anhang gespeichert.
- > dem Administrator Managerzugriff in der Zugriffskontrollliste des Domino-Verzeichnisses gewährt.
- > der Server zur Gruppe LocalDomainServers hinzugefügt.

- > das Serverprotokoll (log.nsf) im Datenverzeichnis des Servers erstellt.
- > die Netzwerkeinstellungen im Serverdokument aktualisiert.
- > das angegebene Netzwerk aktiviert.
- > das Unterverzeichnis mail und die Maildatenbank des Administrators erstellt.
- > die Datenbank reports.nsf erstellt.
- > SMTP konfiguriert, falls es während der Konfiguration ausgewählt wurde.
- > die Einträge »Anonymous« und »LocalDomainAdmins« zu den Zugriffskontrolllisten aller Datenbanken und Schablonen hinzugefügt, falls es während der Konfiguration ausgewählt wurde.

4.6. Einen Domino-Server starten und beenden

Der erste Start nach der Konfiguration sollte erneut über einen Doppelklick auf das Serversymbol am Desktop erfolgen:



Sie werden gefragt, ob Sie den Domino-Server als Dienst (Service) oder als Applikation starten wollen:

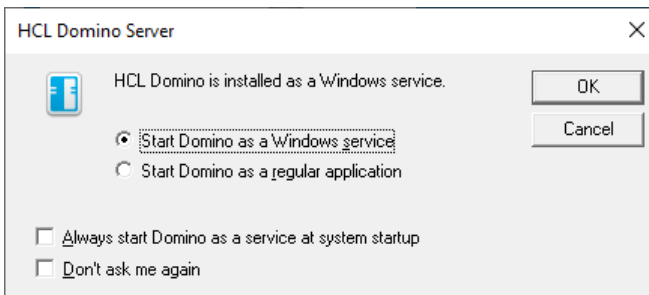


Abbildung 4.35: Dialog HCL Domino Server mit Startoptionen

Üblicherweise starten Sie den Domino-Server unter Windows als Dienst, da dies wesentlich mehr Vorteile bietet. Der Start als Applikation kann jedoch unter bestimmten Voraussetzungen nötig sein, etwa weil sonst der Zugriff auf eine bestimmte ODBC-Datenquelle nicht gegeben ist. Die Unterschiede zwischen Dienst und Applikation entnehmen Sie bitte Tabelle 4.4.

Start als Windows-Dienst	Start als Applikation
Domino läuft unsichtbar im Hintergrund.	Domino läuft in einem sichtbaren Fenster.
Sie können auf den Server nur über die Entfernte Konsole oder die Java-Konsole zugreifen.	Sie können direkt im Serverfenster Konsolenbefehle eintippen.
Dienste können nicht direkt mit dem Desktop interagieren, was sie weniger angreifbar macht.	Die GUI macht den Server angreifbar. In der Vergangenheit gab es mehrmals Sicherheitslücken, bei denen von Browsern auf die Serverkonsole zugegriffen werden konnte.

Start als Windows-Dienst	Start als Applikation
Systemdienste laufen unabhängig von angemeldeten Benutzern und ihren Sitzungen. Der Server »sieht« als Systemdienst nichts, wofür eine Anmeldung nötig wäre, wie Netzwerklaufwerke etc. (Dienste können jedoch auch Benutzerkonten verwenden.)	Hinter dem Server steckt ein Benutzer-Account, daher kann er alles nutzen, was auch ein Benutzer nutzen kann, wie Netzwerkfreigaben etc.
Ein Dienst kann auf ODBC-Datenquellen nur zugreifen, wenn sie als System-DSN konfiguriert wurden.	Der Server als Applikation kann auch auf eine Benutzer-DSN zugreifen.
Dienste können beim Hochfahren des Betriebssystems automatisch gestartet und vor dem Herunterfahren automatisch beendet werden.	Anwendungen können nur über zusätzliche Tools, z. B. die Windows-Aufgabenplanung automatisch gestartet und beendet werden.

Tabelle 4.4: Unterschiede zwischen Dienst und Applikation

4.6.1. Einen Domino-Server als Applikation starten

Starten Sie den Server als Applikation, sehen Sie ihn in einem eigenen Fenster hochfahren. In dieses Fenster können Sie direkt Konsolenbefehle eingeben und erhalten unmittelbar eine Antwort des Servers bzw. des betreffenden Tasks. Um den Server zu beenden, geben Sie einen der folgenden Befehle ein:

`quit`

`exit`

Die meisten Konsolenbefehle können abgekürzt werden, die mindestens einzugebenden Zeichen sind in diesem Buch unterstrichen dargestellt.

```

WS01/COB/AT: HCL Domino Server (64 Bit)

[1D90:0002-30D4] HCL Domino (r) Server (64 Bit), Release 11.0, November 25, 2019
[1D90:0002-30D4] (C) Copyright HCL Technologies. 1987, 2019

[1D90:0005-30D4] 04.03.2020 17:46:42 Informational, rebuild view needed - invalid collection header (reading D:\Domino\names.nsf view note Title: '$ServerAccess')
[1D90:0005-30D4] 04.03.2020 17:46:42 Invalid collection data was detected.
[1D90:0005-30D4] 04.03.2020 17:46:43 Informational, rebuilding view - no container or index (reading D:\Domino\names.nsf view note Title: '$Connections')
[1D90:0005-30D4] 04.03.2020 17:46:43 Informational, rebuilding view - no container or index (reading D:\Domino\names.nsf view note Title: '$Programs')
[1D90:0005-30D4] 04.03.2020 17:46:43 Informational, rebuilding view - no container or index (reading D:\Domino\names.nsf view note Title: '$Groups')
[1D90:0005-30D4] 04.03.2020 17:46:44 Informational, rebuilding view - no container or index (reading D:\Domino\names.nsf view note Title: '$Certifiers')
[1D90:0005-30D4] 04.03.2020 17:46:46 Directory Assistance could not access Directory COBDOMINO01/COB/AT cob\crm.nsf, error: Unable to find path to server. Check that your network connection is working. If you have a working connection, go to Preferences - Notes Ports and click Trace to discover where it breaks down.
[1D90:0005-30D4] 04.03.2020 17:46:46 Directory Assistance could not find an alternate replica for domain COB KUNDEN
[1D90:0002-30D4] refreshing view $Users - 04.03.2020 17:46:46
[1D90:0002-30D4] finished refresh - 04.03.2020 17:46:46
[25B4:0002-1CB4] 04.03.2020 17:46:46 Event Monitor started
[1D90:0002-30D4] 04.03.2020 17:46:46 Begin scan of databases to be consistency checked
[1D90:0002-30D4] 04.03.2020 17:46:46 End scan of databases: 1 found
[1D90:0002-30D4] 04.03.2020 17:46:47 Server started on physical node WS01
[1D90:0005-296C] 04.03.2020 17:46:49 Informational, rebuilding view - no container or index (reading D:\Domino\names.nsf view note Title: '$Networks')
[25B4:0002-1CB4] 04.03.2020 17:46:49 Event: Upgrading the design and data of EVENTS4.NSF...
[1D90:0007-296C] 04.03.2020 17:46:51 NSF_QUOTA_METHOD changed to 2.
[1D90:0007-296C] 04.03.2020 17:46:51 FormulaTimeout changed to 120.
[1D90:0005-296C] 04.03.2020 17:46:51 Informational, rebuilding view - no container or index (reading D:\Domino\names.nsf view note Title: '$ExternalDomainNetworkAdresse')
    
```

Abbildung 4.36: Serverkonsole nach dem Starten des Domino-Servers als Applikation

4.6.2. Einen Domino-Server als Dienst starten

Starten Sie den Domino-Server als Dienst (Service), wird er im Hintergrund ausgeführt und es wird kein Serverfenster angezeigt. Sie können die Serverkonsole ausschließlich über die (mitinstallierte) Java-Konsole (siehe Abbildung 4.41) oder die Entfernte Konsole im Domino-Administrator einsehen.

Egal ob Sie die in Abbildung 4.35 dargestellte Option »Always start Domino as a service at system startup« wählen oder nicht, der Domino-Server-Dienst startet immer automatisch. Wollen Sie das aus irgendeinem Grund nicht, müssen Sie die Eigenschaften des Dienstes bearbeiten. Starten Sie dazu den **Dienstmanager** (Service Manager), indem Sie im Startmenü je nach Sprache Ihres Windows-Servers die Zeichenfolge »dienste« oder »services« eingeben.

Ein Aufruf ist auch über das Programm **Ausführen** (Run) möglich; drücken Sie gleichzeitig die Tasten [Windowsst]+[R], geben Sie »services.msc« ein und klicken Sie auf **OK**.

Suchen Sie in der Liste der Dienste nach dem Eintrag »HCL Domino Server (<Datenverzeichnis>« (bei älteren Domino-Versionen auch »IBM Domino Server (<Datenverzeichnis>«) und führen Sie einen Doppelklick aus, um die Eigenschaften zu öffnen.

Wollen Sie nicht, dass der Domino-Dienst beim Hochfahren von Windows automatisch gestartet wird, wählen Sie als Starttyp »Manuell« und klicken Sie auf **OK**:

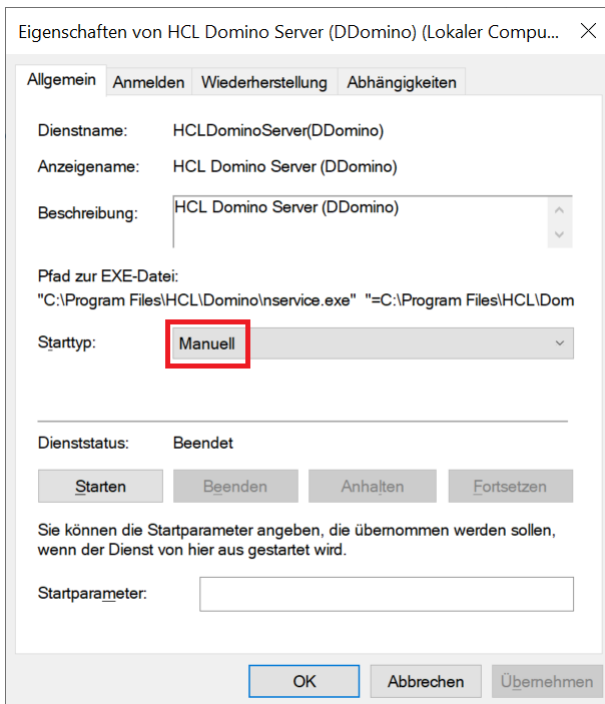


Abbildung 4.37: Die Eigenschaften des Dienstes »HCL Domino Server (DDomino)«

Im Dienstmanager können Sie den Domino-Server außerdem starten und beenden. Klicken Sie mit der rechten Maustaste auf den Namen, um das Kontextmenü aufzurufen; darin finden Sie alle verfügbaren Befehle:

Serverinstallation: Einen Domino-Server starten und beenden

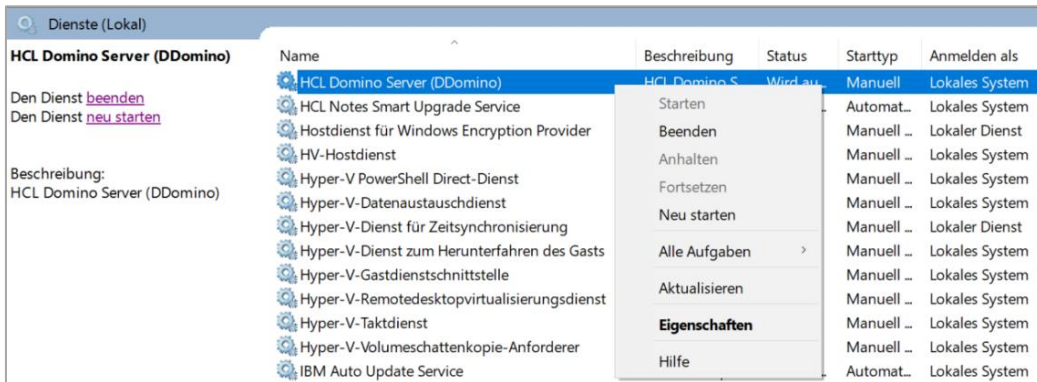


Abbildung 4.38: Der Dienst HCL Domino-Server im Dienstmanager

Sie können Dienste auch in der Kommandozeile über die Befehle »net start <Dienstname>« und »net stop <Dienstname>« starten und stoppen. Dazu müssen Sie die Eingabeaufforderung als Administrator gestartet haben, etwa durch Eintippen von »cmd« im Startmenü und dann Rechtsklick und Auswahl von **Als Administrator ausführen** im Kontextmenü:

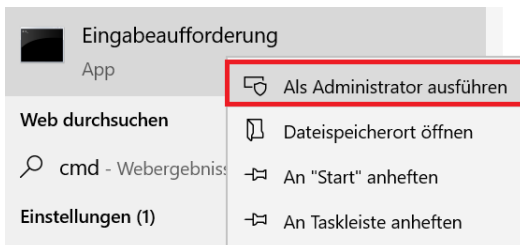


Abbildung 4.39: Die Eingabeaufforderung als Administrator ausführen

In unserem Beispiel verwenden wir als Datenverzeichnis D:\Domino, daher heißt der Dienst »HCL-DominoServer(DDomino)« bzw. »HCL Domino Server (DDomino)«. Geben Sie den Namen mit Leerzeichen ein, setzen Sie ihn in Anführungszeichen:

```
C:\>net stop "HCL Domino Server (DDomino)"
HCL Domino Server (DDomino) wird beendet.....
HCL Domino Server (DDomino) wurde erfolgreich beendet.
```

Sie können die Befehle net start und net stop auch in Batchdateien verwenden.

Wählen Sie die Option **Don't ask me again** und klicken danach auf **OK**, werden Sie beim nächsten Start nicht mehr gefragt.

Wollen Sie Ihre Auswahl später rückgängig machen, müssen Sie mit dem Registrierungs-Editor in der Windows-Registrierdatenbank den folgenden Schlüssel von 1 auf 0 zurücksetzen:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\HCL\Domino\1\DontAskAgain

Sollte Ihr Domino-Server als Dienst nicht starten, lesen Sie Kap. 4.6.4 Der Domino-Server startet nicht als Dienst, ab Seite 60.

4.6.3. Server-Controller und Domino-Console

Der Server-Controller ist ein Java-basierendes Programm, das den Domino-Server kontrolliert. Wird ein Domino-Server von einem Server-Controller gestartet, sehen Sie kein Konsolenfenster, sondern können nur noch über externe Konsolen mit dem Server kommunizieren. Verwenden Sie dazu entweder die Java-Konsole (Domino-Console), die Entfernte Konsole im Domino-Administrator oder die Live-Konsole im Webadministrator (sofern Sie einen Browser auftreiben, der Java unterstützt).

Um den Domino-Server, Server Controller und die Java-Konsole auf derselben Windows-Maschine zu starten, geben Sie über den Befehl **Ausführen** (Aufruf über [Windows]+[R]) oder auch in einer Windows-Eingabeaufforderung den folgenden Befehl ein:

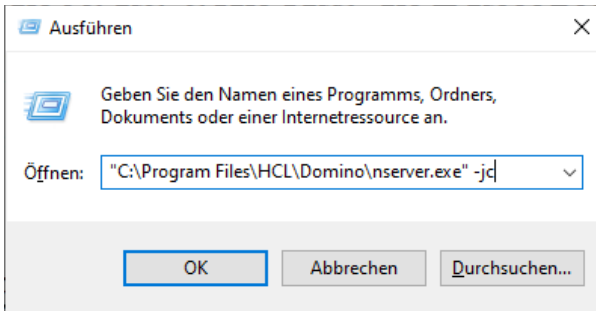


Abbildung 4.40: Der Dialog Ausführen

Die Java-Konsole wird angezeigt und Sie sehen den Server hochfahren:

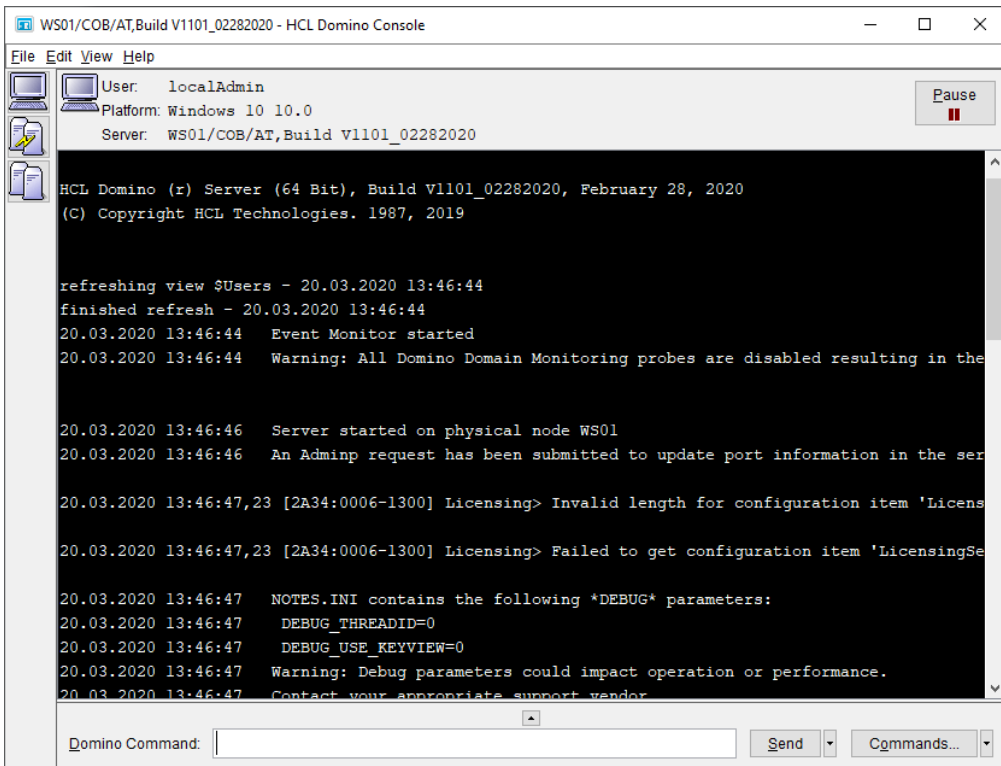


Abbildung 4.41: Die Domino-Console (Java-Konsole)

Serverinstallation: Einen Domino-Server starten und beenden

Die Java-Konsole gibt es nur auf Englisch.

Per Vorgabe hört der Domino-Server-Controller auf Anfragen auf Port 2050. Der Domino-Server-Controller kann auch allein laufen – ohne einen Domino-Server darunter.

Um den Domino-Server zu beenden, wählen Sie im Menü den Befehl **File > Exit** und aktivieren Sie im angezeigten Dialog die Option **Also stop Server Controller and server <Name>**:

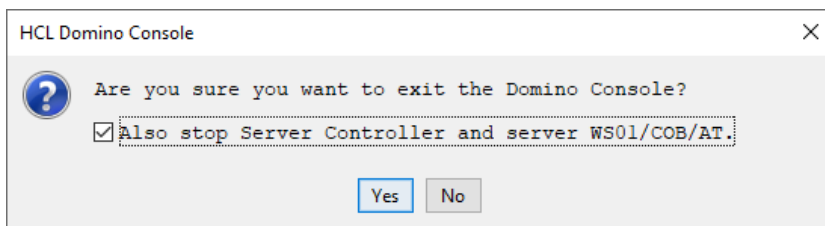


Abbildung 4.42: Dialog beim Beenden der Domino-Console

Beachten Sie die Regel, den Server stets so zu beenden, wie Sie ihn gestartet haben; wurde er als Dienst gestartet, beenden Sie ihn auch als Dienst. Wurde er über Ausführen oder die Befehlszeile zusammen mit der Java-Konsole gestartet, verwenden Sie den entsprechenden Befehl.

Wollen Sie den Domino-Server nur durchstarten, etwa, damit er seine Einstellungen neu lädt, können Sie auf der Konsole den folgenden Befehl eingeben:

```
restart server
```

4.6.4. Der Domino-Server startet nicht als Dienst

Manchmal startet der Domino-Server zwar als Applikation, nicht jedoch als Dienst:

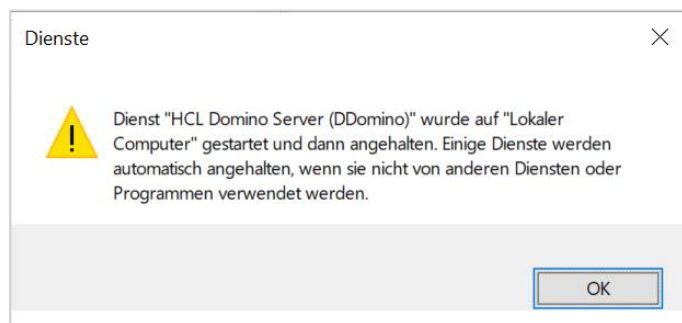


Abbildung 4.43: Fehlermeldung beim Starten des Dienstes

Dies kann verschiedene Gründe haben. Manchmal hat es nur damit zu tun, dass Sie zwar den Domino-Server beendet haben, nicht jedoch den Domino-Controller, etwa durch Eingabe des Befehls `quit`. Läuft die Domino-Console noch, können Sie das Beenden des Controllers nachholen, indem Sie wie oben beschrieben, den Befehl **File > Exit** auswählen und dann im angezeigten Dialog die Option **Also stop Server Controller and server <Name>** aktivieren.

Will der Dienst partout nicht starten, fügen Sie die folgenden Einträge zur Datei `notes.ini` hinzu und führen Sie anschließend einen Neustart durch:

```
ServerController=1  
TCPIP_ControllerTcplpAddress=nnn.nnn.nnn.nnn:2050
```

(Ersetzen Sie die Zeichenfolge »nnn.nnn.nnn.nnn« durch die IP-Adresse Ihres Servers!)

Hinweise zum Bearbeiten der Datei notes.ini finden Sie in Kap. 5.2 Die Datei notes.ini, ab Seite 91.

Sollte der Eintrag TCPIP_ControllerTcpIpAddress bereits vorhanden sein, überprüfen Sie, ob die IP-Adresse richtig ist.

Sollte der Dienst dann immer noch nicht starten, überprüfen Sie, ob in der Datei dcontroller.ini im Domino-Datenverzeichnis der richtige Hostname oder die richtige IP-Adresse eingetragen ist.

Wenn auch das nicht hilft, starten Sie den Domino-Server über eine Befehlszeile im Stand-Alone-Modus und hoffen Sie, dass er eine verwertbare Fehlermeldung ausgibt:

```
C:\ProgramFiles\HCL\Domino>nserver.exe -sa
```

Beenden Sie einen im Stand-Alone-Modus gestarteten Domino-Server stets durch Eingabe der Befehle `quit` oder `exit`.

4.6.5. Verwendung einer Community-Server-Lizenz

Es ist möglich, den Domino-Server mithilfe einer Community-Server-Lizenz zu testen. Die Version mit einem Evaluierungszertifikat hat ein anderes Installations-Kit als jene mit einer Produktlizenz. Wenn der Server beim ersten Hochfahren keinen Produktionsschlüssel vorfindet, erstellt er automatisch eine Community-Server-Lizenz und zeigt das auch auf der Konsole an.

Dieser Check findet bei jedem Serverstart statt. Findet der Server eine Produktionsversion, startet er normal. Findet der Server eine Community-Version, überprüft er, ob der Evaluierungszeitraum abgelaufen ist oder nicht. Sollte der Zeitraum abgelaufen sein, stoppt der Server und fordert Sie auf, eine Produktionsversion zu erwerben.

4.7. Domino-Ports in der Windows-Firewall öffnen

Installieren Sie den Domino-Administrator direkt auf der Server-Maschine, können Sie natürlich problemlos zugreifen. Versuchen Sie hingegen, von einem anderen PC aus auf den Domino-Server zuzugreifen, werden Sie nicht hinkommen, da die Windows-Firewall Ihren Zugriff abblockt. Das gilt nicht nur für NRPC, sondern auch für alle Internetprotokolle.

Sie können nun die Firewall entweder ganz abschalten, was in den meisten Fällen nicht ratsam ist, oder mit einigen eingehenden Regeln den Zugriff auf den Domino-Server erlauben.

Um den Zugriff auf den Domino-Server in der Firewall zu erlauben, gehen Sie wie folgt vor:

1. Tippen Sie im Windows-Startmenü »firewall« ein und starten Sie das vorgeschlagene Programm »Firewall & Netzwerkschutz«.
2. Wählen Sie den Befehl **Erweiterte Einstellungen**.
3. Klicken Sie auf **Eingehende Regeln** und dann rechts bei den Aktionen auf **Neue Regel...**
4. Der Assistent für neue eingehende Regel wird angezeigt.

5. Wählen Sie als Regeltyp »Programm« und klicken Sie auf **Weiter** >:

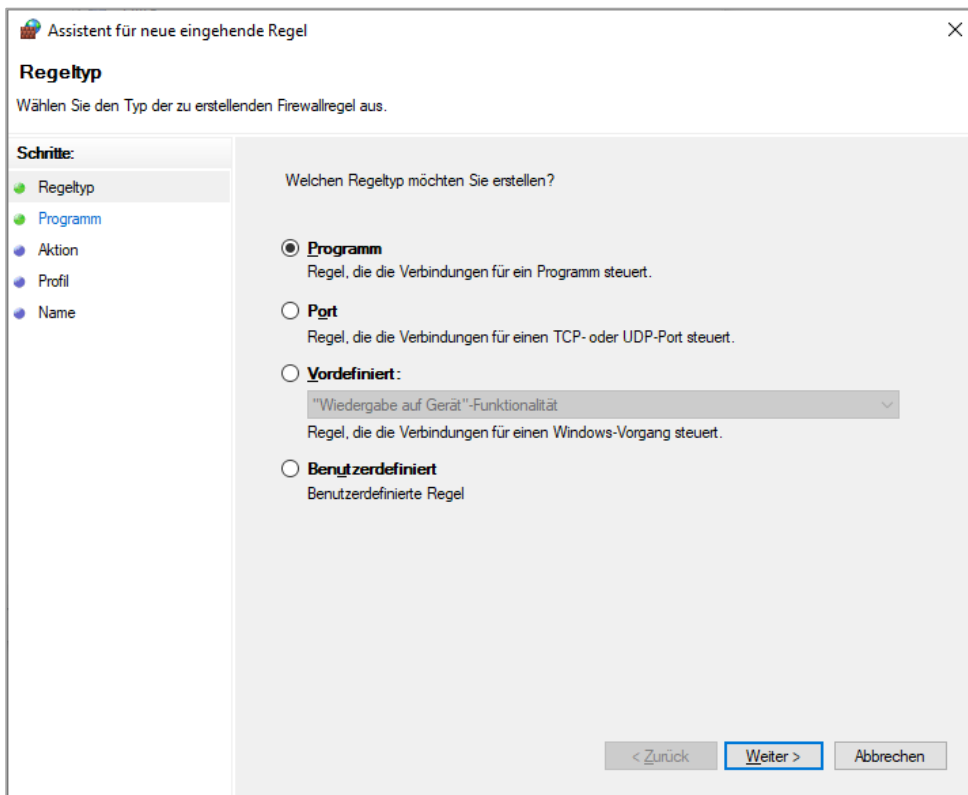


Abbildung 4.44: Windows-Firewall, eingehende Regel hinzufügen

6. Klicken sie auf **Durchsuchen...** und wählen Sie im Domino-Programmverzeichnis (Vorgabe C:\Programme\HCL\Domino) das Programm nserver.exe aus. Klicken Sie auf **Weiter** >:

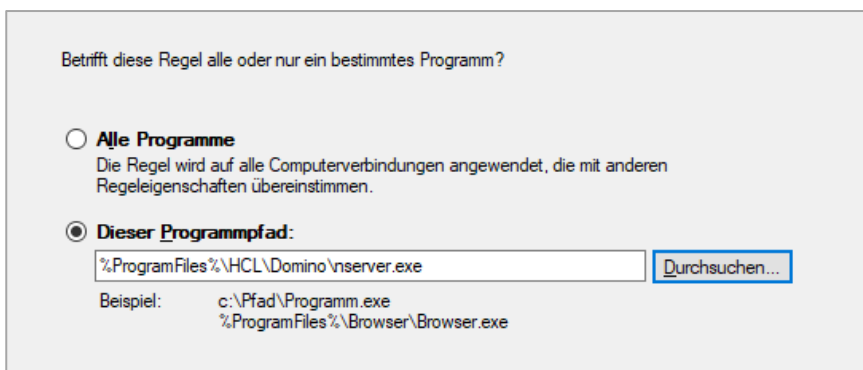


Abbildung 4.45: Windows-Firewall, eingehende Regel – Programm nserver.exe hinzufügen

7. Wählen Sie »Verbindung zulassen« und klicken Sie auf **Weiter** >.

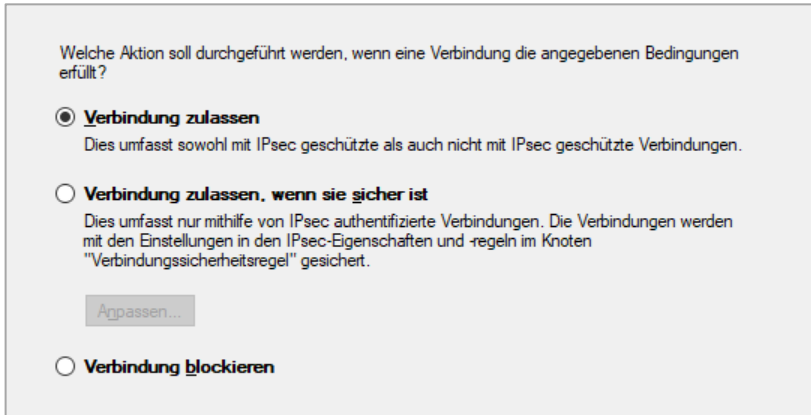


Abbildung 4.46: Windows-Firewall, eingehende Regel – Verbindung zulassen

8. Geben Sie an, für welchen Netzwerktyp die Regel gelten soll und klicken Sie auf **Weiter** >:

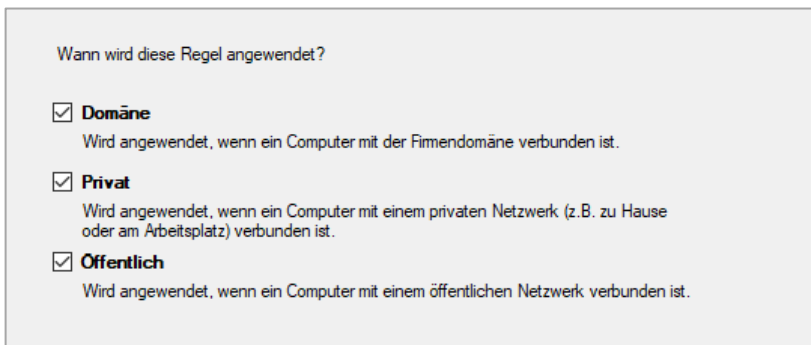


Abbildung 4.47: Windows-Firewall, eingehende Regel – Profile auswählen

9. Geben Sie einen Namen für die Regel ein und klicken Sie auf **Fertig stellen**.
10. Erstellen Sie auch für alle Ports, auf die ein Zugriff von außen möglich sein soll, eine eingehende Regel. Wählen Sie dazu als Regeltyp »Port« und geben Sie die gewünschte Port-Nummer ein:

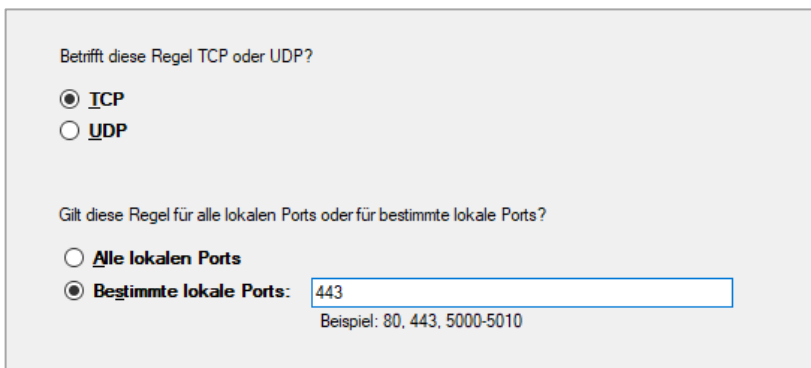


Abbildung 4.48: Windows-Firewall, eingehende Regel Port 443

4.8. Einen Domino-Administrator installieren

Zum Konfigurieren eines Domino-Servers benötigen Sie einen Administrator-Client. Laden Sie dazu das »All-Clients«-Installationspaket herunter, welches je nach Version und Sprache unterschiedlich bezeichnet wird:

Notes_Designer_Admin_11.0_Win_English.exe

Notes_Designer_Admin_11.0.1_Win_German.exe

Auf Betriebssystemseite werden alle Varianten von Windows 7 und Windows 10 unterstützt. Ich konnte auch keinen Nachteil darin finden, einen Domino-Administrator auch direkt auf einem Windows-Server zu installieren.

Eine Mehrbenutzerinstallation mit dem »Notes-Only«-Paket kann nicht direkt aktualisiert und muss vorher desinstalliert werden. Eine Einzelbenutzerinstallation mit dem All-Clients-Paket können Sie hingegen laut Angaben des Herstellers HCL zurückgehend bis Version 6.5 direkt mit Version 11 aktualisieren. Ich persönlich bevorzuge bei meinen Admin-Clients eine vorhergehende Deinstallation und Neuinstallation, um die ganzen Altlasten wie veraltete Schablonen etc. loszuwerden.

Eine Übersicht über die verschiedenen Notes-Clients finden Sie in Kap. 18.2.2 Die verschiedenen Client-Pakete, ab Seite 468.

Führen Sie nun das Installationspaket als Administrator aus. Sie werden gefragt, wohin die Software entpackt werden soll:

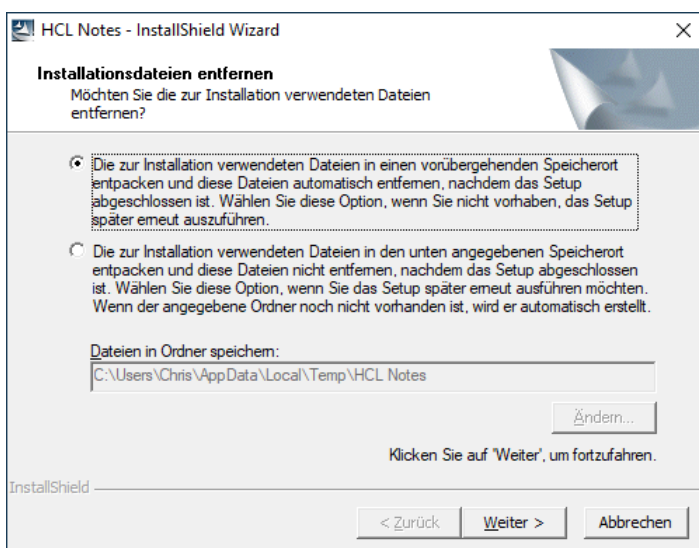


Abbildung 4.49: Client-Installation – Schritt Installationsdateien entfernen

Sollen die Installationsdateien in ein temporäres Verzeichnis entpackt und nach der Installation automatisch gelöscht werden, wählen Sie die erste Option.

Wollen Sie die bereits entpackte Software für weitere Installationen nutzen, wählen Sie die zweite Option und geben Sie einen Ordner an. Damit können Sie das Programm setup.exe später auch mit optionalen Parametern aufrufen und die Installation automatisieren, was jedoch nur beim Ausrollen von Notes-Clients zur Anwendung kommt (z. B. zur »Silent Installation« ohne Benutzereingabe).

Klicken Sie dann auf **Weiter** >.

Die Dateien werden entpackt und die Installation vorbereitet:

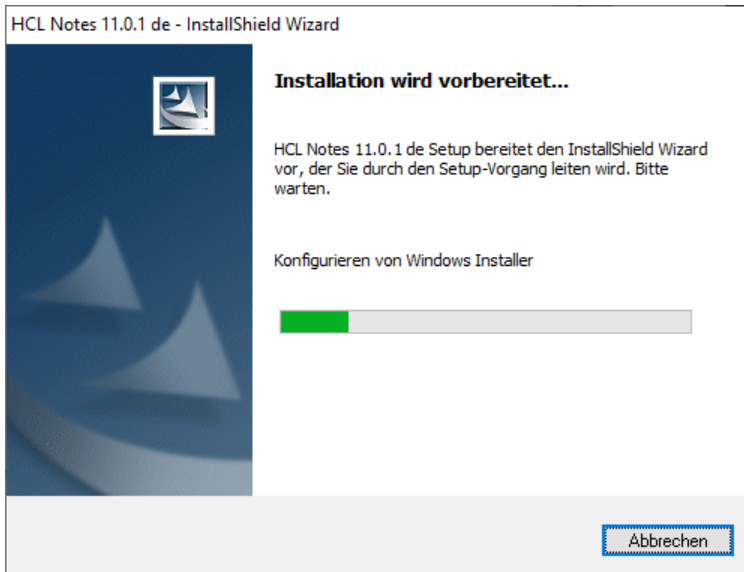


Abbildung 4.50: Client-Installation – Installation wird vorbereitet

Sobald die Willkommenseite angezeigt wird, klicken Sie auf **Weiter** >:

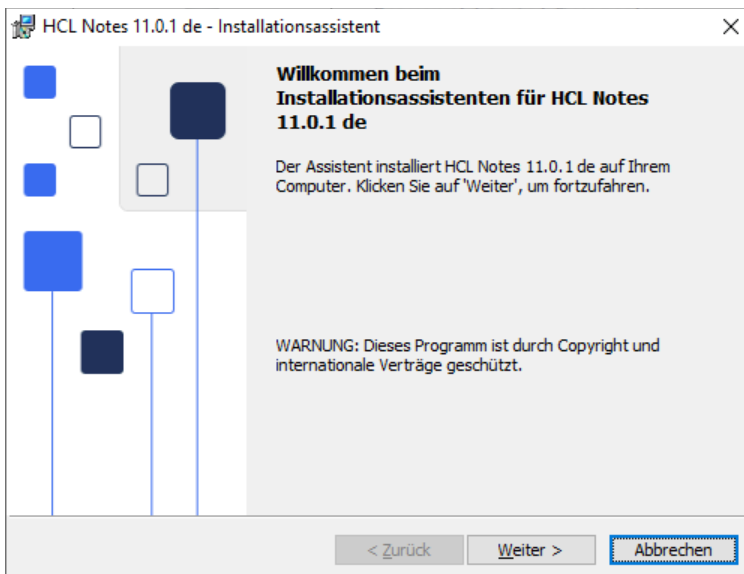


Abbildung 4.51: Client-Installation – Willkommenseite

Es werden die Lizenzbedingungen angezeigt. Wählen Sie »Ich akzeptiere die Bedingungen dieser Lizenzvereinbarung« und klicken Sie auf **Weiter** >.

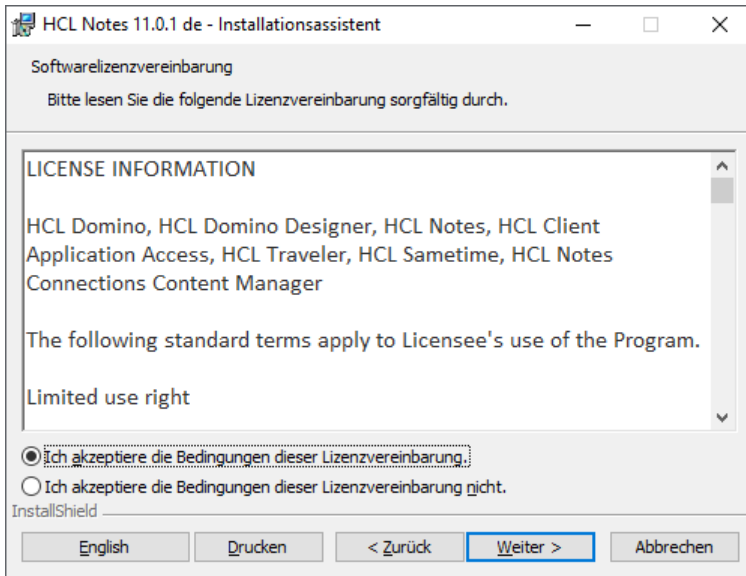


Abbildung 4.52: Client-Installation – Lizenzinformationen

Wählen Sie Programm- und Datenverzeichnis aus oder akzeptieren Sie die Voreinstellung und klicken Sie auf **Weiter >**:

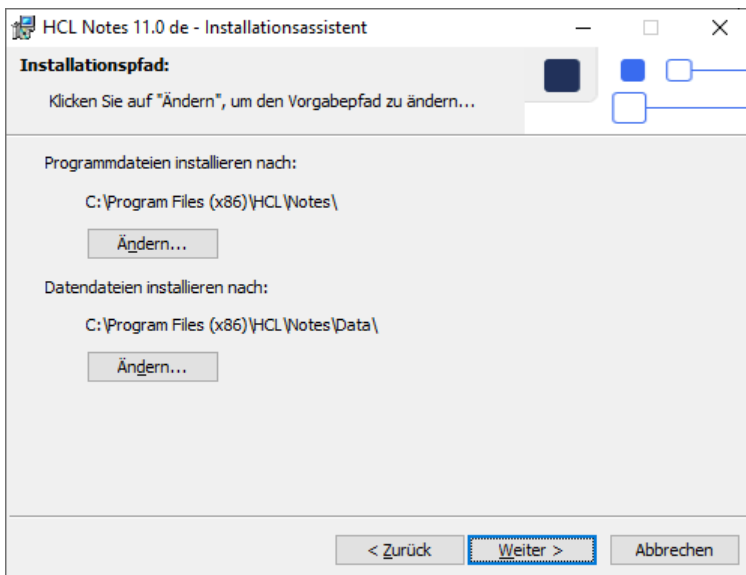


Abbildung 4.53: Client-Installation – Auswahl des Installationspfades

Aktualisieren Sie eine ältere Notes-Version, wird das Installationsverzeichnis automatisch ausgewählt. Beachten Sie, dass ältere Versionen das Verzeichnis »IBM« im Pfad verwenden.

Wählen Sie die zu installierenden Komponenten aus. Achten Sie darauf, neben den Notes-Client auch den Domino-Administrator und den Domino-Designer mit allen Features zu installieren.

Installieren Sie HCL Connections und Sametime hingegen nur, wenn Sie diese Produkte einsetzen oder ihren Einsatz planen:

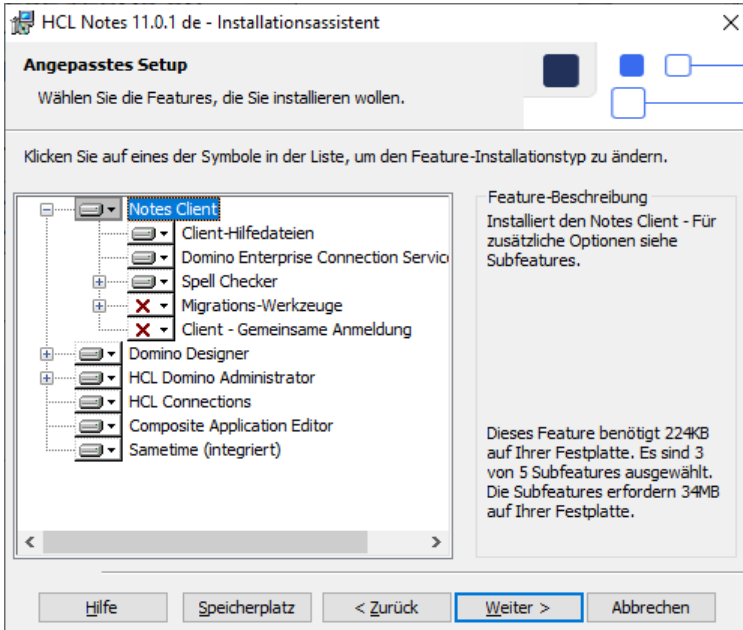


Abbildung 4.54: Client-Installation – Auswahl der Komponenten

Klicken Sie auf **Weiter >**.

Geben Sie an, ob Notes auch als Standard-Programm für E-Mail, Kalender und Kontakte verwendet werden soll (Vorgabe). Setzen Sie diese Einstellungen nur dann nicht, wenn Sie ein anderes E-Mail-Programm verwenden, und Notes nur zum Administrieren des Domino-Servers brauchen.

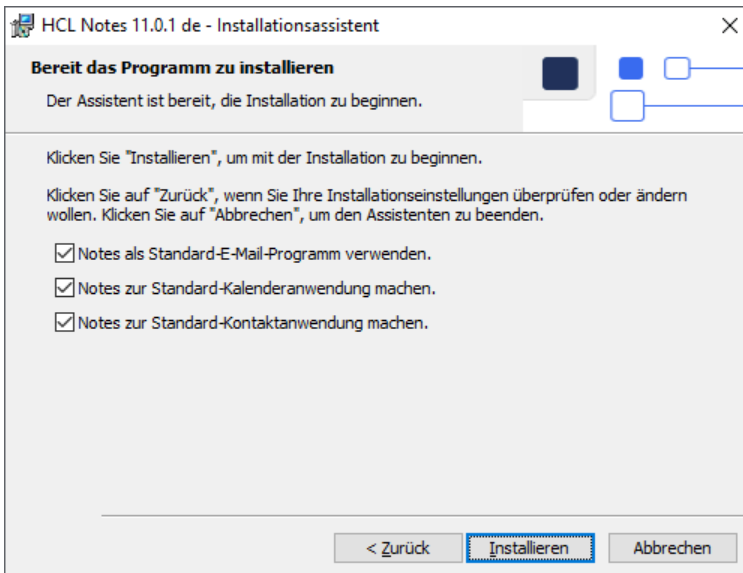


Abbildung 4.55: Client-Installation – Auswahl Vorgaben

Der Assistent ist nun bereit zur Installation.

Klicken Sie auf **Installieren**.

Serverinstallation: Einen Domino-Administrator installieren

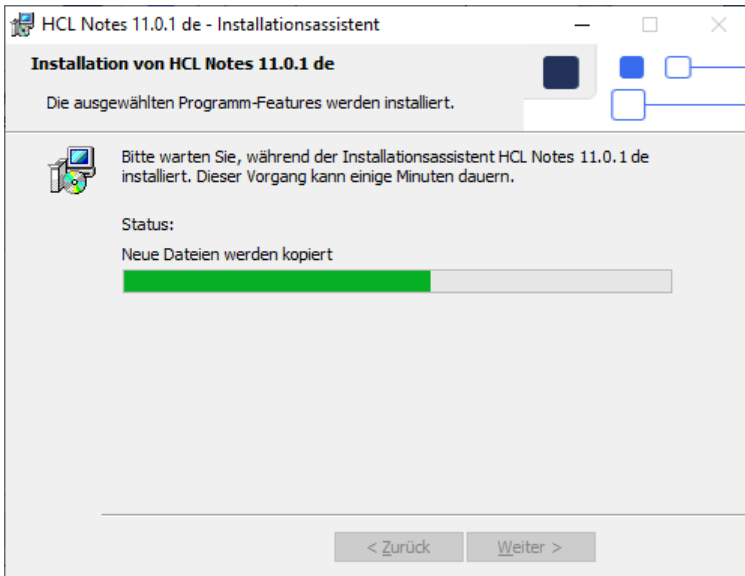


Abbildung 4.56: Client-Installation – Installationsverlauf

Die Installation kann bei einem aktivierten Viren-Scanner gegebenenfalls sehr lange dauern.

Wenn die Installation beendet ist, klicken Sie auf **Fertig stellen**:

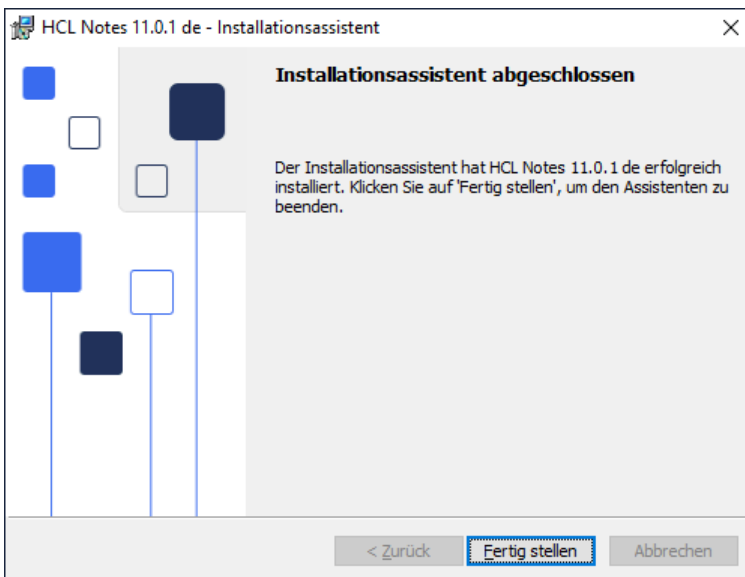


Abbildung 4.57: Client-Installation – Installation ist abgeschlossen

Der Assistent installiert, wie in Abbildung 4.58 ersichtlich, für jeden Client ein eigenes Symbol auf dem Desktop:

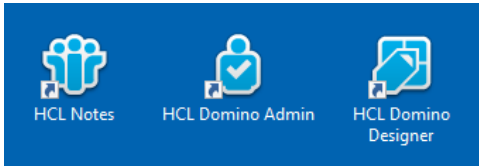


Abbildung 4.58: Die Symbole der drei Notes-Clients

4.8.1. Den Admin-Client einrichten

Bevor Sie Notes verwenden können, müssen Sie eine Client-Konfiguration durchführen. Dabei wird der Domino-Administrator mit einer Benutzer-ID verknüpft. In unserem Fall handelt es sich dabei um den beim Einrichten des Servers (siehe Kap. 4.5 Einen ersten Domino-Server einrichten, ab Seite 50) angegebenen Administrator. Seine Benutzer-ID hängt im Domino-Verzeichnis als Anhang im Personendokument und wird bei der Client-Konfiguration herausgelöst. Das bedeutet, dass diese ID zum Einrichten eines zweiten Domino-Administrators nicht mehr zur Verfügung steht und Sie diese aus dem Datenverzeichnis des Clients kopieren müssen.

Haben Sie beim Einrichten des Servers die Option »Also save a local copy of the ID file« gewählt, können Sie die ID des Administrators (die Datei heißt dann admin.id) auch aus dem Domino-Datenverzeichnis kopieren.

Um eine Client-Konfiguration durchzuführen, gehen Sie wie folgt vor:

1. Doppelklicken Sie auf ein beliebiges Symbol, etwa das für HCL Notes. Die Client-Konfiguration wird gestartet:

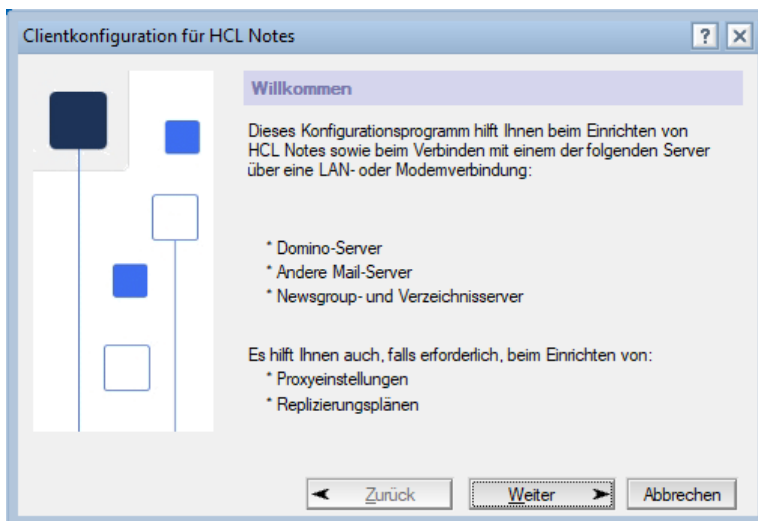


Abbildung 4.59: Notes-Client-Konfiguration

2. Geben Sie den Benutzernamen des Administrators ein. Der Name muss im Domino-Verzeichnis eindeutig sein – wenn bereits Ihr Vorname eindeutig ist, reicht dieser.
3. Geben Sie den Servernamen ein.

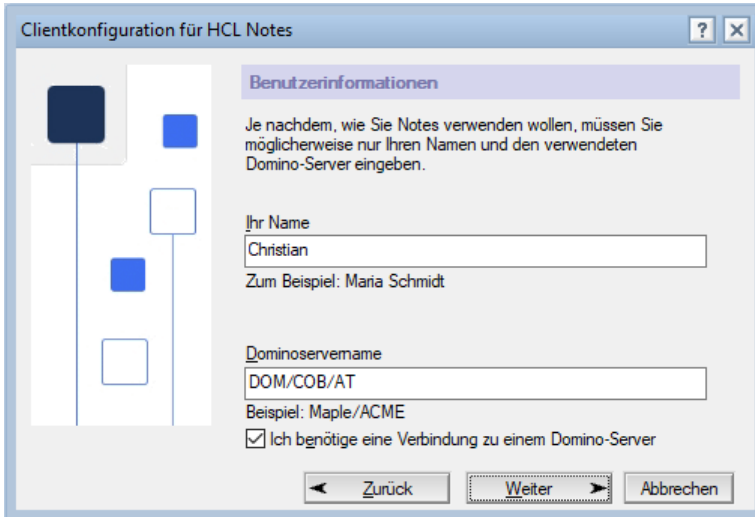


Abbildung 4.60: Notes-Client-Konfiguration – Eingabe von Benutzer und Server

4. Klicken Sie auf **Weiter** >.
5. Da die ID-Datei des ersten Administrators als Anhang im Personendokument gespeichert vorliegt, werden Sie sofort zur Kennworteingabe aufgefordert:

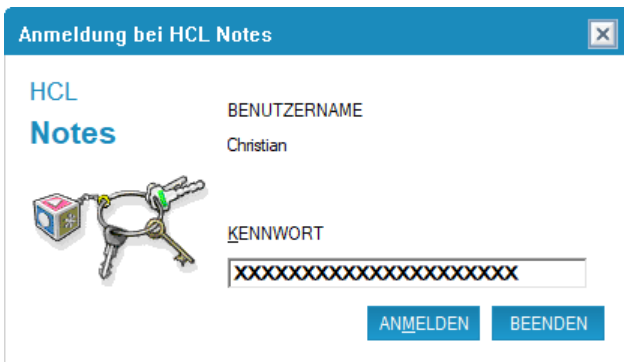


Abbildung 4.61: Notes-Client-Konfiguration – Kennworteingabe

Sollte im Personendokument keine ID-Datei mehr hängen, werden Sie dazu aufgefordert, eine ID-Datei aus dem Dateisystem auszuwählen.

Bei der ersten Client-Konfiguration wird die ID-Datei des Administrators aus Sicherheitsgründen aus dem Personendokument entfernt und steht zum Einrichten weiterer Clients nicht mehr zur Verfügung. Achten Sie daher darauf, rechtzeitig eine Sicherungskopie der Administrator-ID anzulegen.

6. Nach erfolgreicher Anmeldung werden Sie gefragt, ob Sie zusätzliche Dienste konfigurieren möchten. Dazu zählen etwa PO3 oder IMAP, um Mails von einem Internet-Provider abzuholen, oder LDAP, um auf ein externes Verzeichnis zuzugreifen. Klicken Sie auf **Weiter** > oder **Fertig**, um die Konfiguration zusätzlicher Services zu überspringen und die Installation zu beenden:

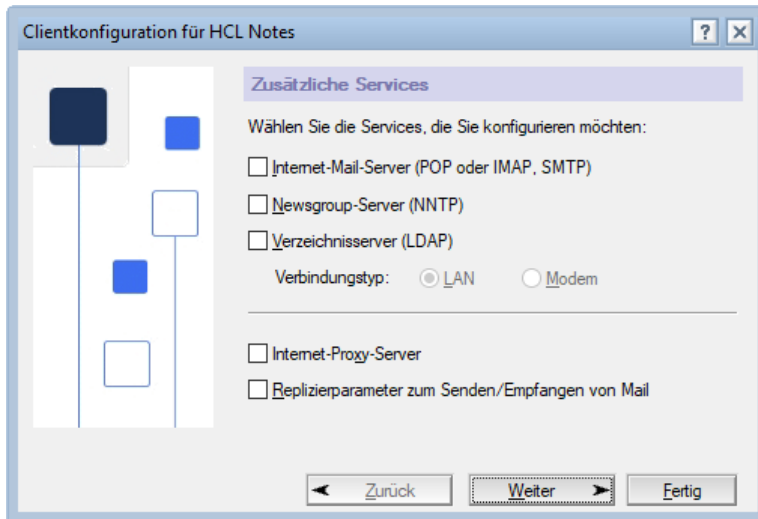


Abbildung 4.62: Notes-Client-Konfiguration – Auswahl zusätzlicher Services

4.8.2. Administrationsvorgaben setzen

Nach der Konfiguration des Admin-Clients empfiehlt es sich, zumindest einige grundlegende Administrationsvorgaben zu setzen. Einige der Vorgaben werden später nach dem Erstellen von Richtlinien obsolet. Zu den Vorgaben gehören:

- > Ordner zum Ablegen von ID-Dateien festlegen
- > Pfad zum Zertifizierer hinterlegen
- > Registriervorgaben für Benutzer setzen
- > Registriervorgaben für Server und Zertifizierer setzen

4.8.2.1. Ordner zum Ablegen der ID-Dateien festlegen

Als Erstes sollten Sie einen Speicherort für ID-Dateien festlegen, am besten einen Netzwerk-Ordner, auf den nur Administratoren Zugriff haben, z. B. T:\Notes\ids. Legen Sie die Unterverzeichnisse »certs« (für Zertifizierer), »servers« (für Server) und »people« (für Benutzer) an. (Später werden wir die Benutzer-IDs in einer eigenen Notes-Datenbank, dem sogenannten ID-Vault – siehe Kap. 6.2, ab Seite 137 – ablegen.)

Verschieben Sie die Zertifizierer-ID (cert.id) aus dem Domino-Datenverzeichnis in T:\Notes\ids\certs. Die Server-ID (server.id) muss im Datenverzeichnis verbleiben, Sie sollten jedoch eine Kopie in T:\Notes\ids\servers ablegen. Ich würde auch den Namen ändern, Sie sichern später ja wohl noch andere Server-IDs. Wenn Sie bei der Erstkonfiguration des Servers eine Kopie der Admin-ID angefordert haben (admin.id), sollten Sie diese jetzt auch aus dem Serverdatenverzeichnis in T:\Notes\ids\people verschieben. Wenn nicht, kopieren Sie die Admin-ID aus dem Datenverzeichnis des Domino-Administrators (dort heißt sie dann user.id).

Starten Sie den Domino-Administrator und rufen Sie im Menü **Datei > Vorgaben > Administration** die Administrationsvorgaben auf. Wählen Sie das Register **Registrierung**:

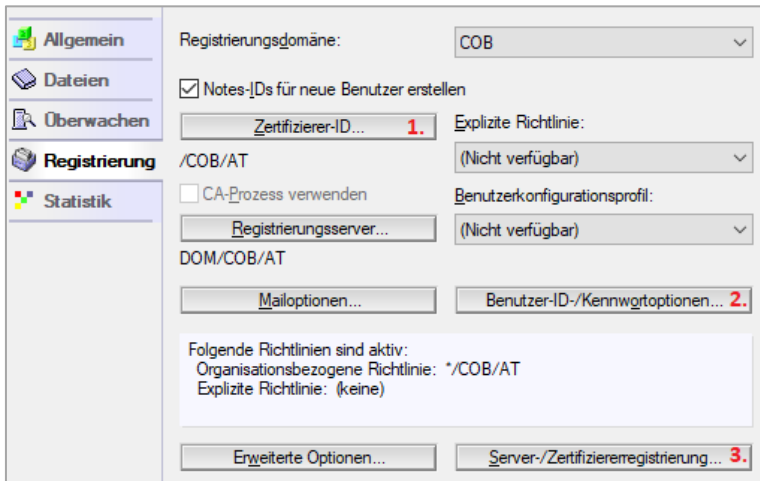


Abbildung 4.63: Administrationsvorgaben, Registerkarte Registrierung

1. Klicken Sie auf die Schaltfläche **Zertifizierer-ID...** und wählen Sie den Zertifizierer in dem von Ihnen angelegten Unterverzeichnis `\certs` aus.
2. Klicken Sie dann auf die Schaltfläche **Benutzer-ID-Konfigurationen...** und geben Sie das von Ihnen erstellte Verzeichnis `\people` als Ordner für die Personen-ID-Dateien an.

Achten Sie darauf, dass bei **Spezifikation des öffentlichen Schlüssels** die Option »Mit Version 7.0 und höher kompatibel (2048 Bit)« ausgewählt ist.

Im Feld **Lizentyp** sollte immer »Nordamerika« stehen:

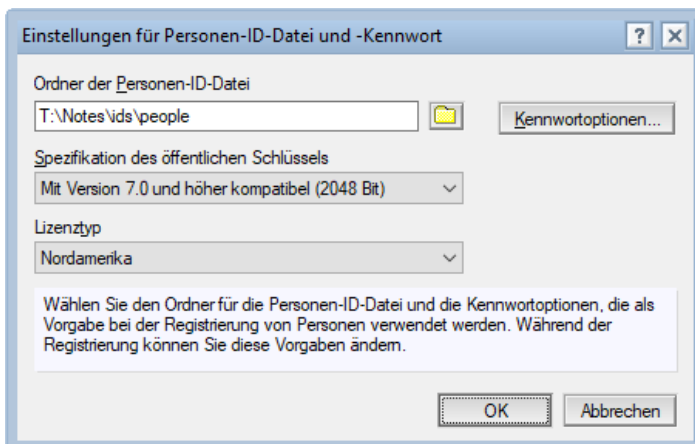


Abbildung 4.64: Vorgaben für Personen-ID-Datei und -Kennwort

Wählen Sie als **Lizentyp** »International«, werden kürzere Schlüssel generiert. Diese Einstellung stammt aus Zeiten, als der Export von Software mit »strong encryption« (damals 128 Bit und höher) aus den USA verboten war. Diese Beschränkung ist am 15.01.2000 gefallen und die IBM brachte mit Domino 5.0.4 die sogenannte »Global Edition« heraus, in der alle Länder den Lizenztyp »Nordamerika« einstellen dürfen. Haben Sie ein internationales Unternehmen zu administrieren, beachten Sie jedoch, dass in anderen Ländern andere Rege gelten können, z. B. in Frankreich.

Klicken Sie auf die Schaltfläche **Kennwortoptionen...** und ändern Sie bei Bedarf die Kennwortqualität. (Für Details zur Kennwortqualität lesen Sie Kap. 13.3.3 Kennwortqualität, ab Seite 343.)

Stellen Sie den **Verschlüsselungsgrad** auf »Mit Version 8.0 und höher kompatibel (256 Bit AES)« ein.

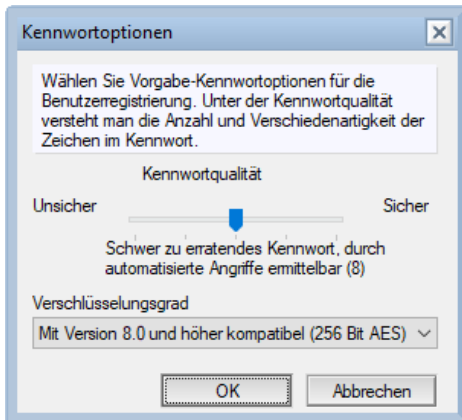


Abbildung 4.65: Vorgaben für Kennwortoptionen

3. Klicken Sie dann auf die Schaltfläche **Server-/Zertifiziererregistrierung...** und achten Sie auch hier darauf, den jeweils höchsten Verschlüsselungsgrad zu wählen: 2048 Bit für Server und 4096 Bit für Zertifizierer.

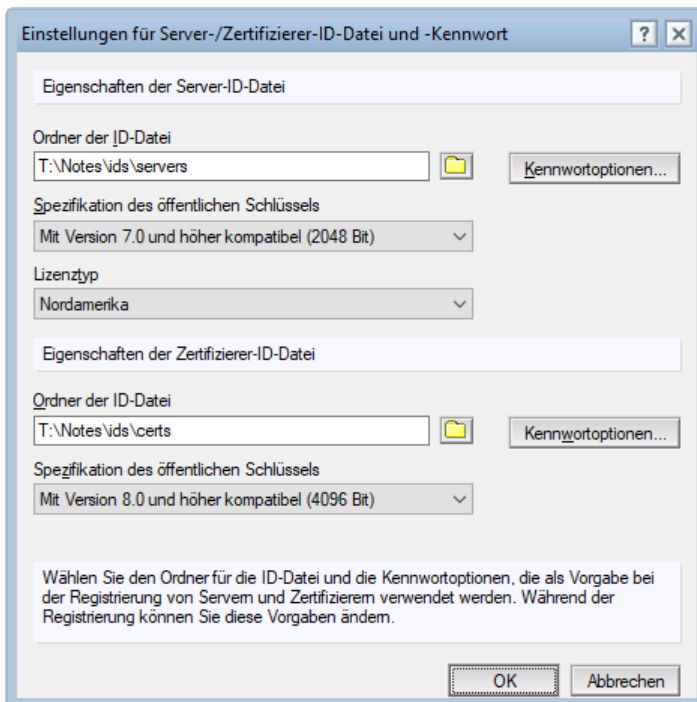


Abbildung 4.66: Vorgaben für Server-/Zertifizierer-ID-Datei und -Kennwort

Auch hier sollte im Feld **Lizenztyp** immer »Nordamerika« ausgewählt sein!

Klicken Sie sowohl für Server als auch für Zertifizierer auf die Schaltfläche **Kennwortoptionen...** und erhöhen Sie den Verschlüsselungsgrad auf 256 Bit AES.

Bei Servern sollte die Kennwortqualität auf »0 – Kennwort ist optional« eingestellt bleiben.

Serverinstallation: Einen zusätzlichen Domino-Server einrichten

Weiterführende Informationen zur Verschlüsselung finden Sie in Kap. 12 Verschlüsselung und Zertifikate, ab Seite 319.

4.9. Einen zusätzlichen Domino-Server einrichten

4.9.1. Wozu zusätzliche Server?

Wenn die Anzahl der Benutzer wächst, kann es nötig werden, weitere Server anzuschaffen und ihnen bestimmte Aufgaben zuzuweisen, um die Serverleistungen zu optimieren. Im Folgenden sind einige Servertypen aufgeführt, die Sie bei Ihrer Planung berücksichtigen sollten:

Mailserver

Mailserver speichern Mail-Datenbanken und sorgen für die Mailweiterleitung innerhalb des Netzwerks oder ins Internet. Außerdem pflegen sie die Zeitplanungsdatenbank und verarbeiten Anfragen nach freien Terminen an das Kalendersystem.

Anwendungsserver (Applikationsserver)

Ein Anwendungsserver stellt Anwendungen, also Notes-Datenbanken, zur Verfügung. Auf diesem Server laufen meist auch Agenten (Programme) und diverse Wartungstasks, die Datenbanken indizieren, komprimieren und reparieren.

Webserver

Webserver sind ebenfalls Anwendungsserver, verwenden aber das Protokoll HTTP/HTTPS und stellen ihre Dienste Webbrowsern zur Verfügung. Einen Sonderfall bilden Webserver, die Webmail zur Verfügung stellen – für den Zugriff von Webbrowsern oder Mobilgeräten. Bei Webservern liegt ein besonderer Fokus auf Sicherheit.

Einwählserver

Einwählserver (Dial-In-Server) sind Domino-Server, die von »außen«, also aus dem Internet, direkt über den Port 1352 erreichbar sind. Sie heißen so, weil man sich früher tatsächlich über eine Modemverbindung eingewählt hat. Aus Sicherheitsgründen wird heute ein direkter Zugriff aus dem Internet nur noch selten zugelassen und stattdessen von externen Benutzern erwartet, sich zuerst via VPN ins lokale Netzwerk einzuwählen. Einwählserver können sowohl Mailedienste als auch Anwendungen bereitstellen oder – aus Sicherheitsgründen – auch nichts anderes tun, als Notes-Clients im internen Netzwerk weiterzuverbinden; in diesem Fall nennt man sie auch Durchgangsserver.

Durchgangsserver

Ein Durchgangsserver (Path-Through-Server) fungiert als »Trittbrett«. Er leitet Clients im lokalen Netzwerk (LAN) zu anderen Servern weiter, die von außen nicht erreichbar sind. Das erhöht die Sicherheit, weil auf den Durchgangsservern selbst keine sensiblen Daten abgelegt werden, und ist praktisch, weil ein Benutzer über seinen Notes-Client nur eine einzige Verbindung aufbauen muss. Darüber hinaus können Durchgangsserver Verbindungen zwischen einem Client und einem Server oder zwischen zwei Servern herstellen, die unterschiedliche Netzwerkprotokolle nutzen.

Sicherungsserver/Archivserver

Auf Sicherungsservern können Repliken besonders wichtiger Datenbanken abgelegt werden. Auf Archivservern werden Datenbankarchive gespeichert.

Server-Cluster

Ein Grund für die Anschaffung weiterer Server kann auch der Aufbau eines Mail-Clusters sein. Cluster bieten eine höhere Ausfallsicherheit und eine bessere Lastverteilung.

4.9.2. Einen zusätzlichen Server registrieren

Bevor Sie einen weiteren Server konfigurieren können, müssen Sie ihn registrieren. Bei der Serverregistrierung werden zwei Aufgaben erfüllt: Es wird ein Serverdokument im Domino-Verzeichnis angelegt und es wird eine Server-ID erstellt. Diese ID kann entweder als Anhang im Serverdokument oder im Dateisystem gespeichert werden. Speichern Sie die Server-ID als Anhang, muss sie aus Sicherheitsgründen kennwortgeschützt sein und Sie müssen das Kennwort nach dem Einrichten des zusätzlichen Servers aus der ID-Datei löschen.

Zum Registrieren eines Servers müssen Sie im Domino-Verzeichnis zumindest über Editor-Rechte mit der Rolle [ServerCreator] verfügen. Weiters müssen Sie Zugriff auf den Unternehmenszertifizierer haben und sein Passwort kennen.

Um einen Domino-Server zu registrieren, gehen Sie wie folgt vor:

1. Starten Sie den Domino-Administrator und navigieren Sie zum Register **Konfiguration**. Klappen Sie die Werkzeuge auf und wählen Sie **Registrieren > Server**.
2. Wählen Sie einen Registrierungsserver und den Zertifizierer aus (falls noch nicht ausgewählt) und geben Sie das Kennwort ein.
3. Der Dialog **Server registrieren** wird angezeigt (siehe Abbildung 4.67).
4. Wählen Sie im Feld **Spezifikation des öffentlichen Schlüssels** »Mit Version 7.0 und höher kompatibel (2048 Bit)«.
5. Der Lizenztyp sollte »Nordamerika« sein.
6. (Optional) Ändern Sie das Ablaufdatum (es beträgt für Server standardmäßig hundert Jahre).
7. Klicken Sie auf **Weiter...**

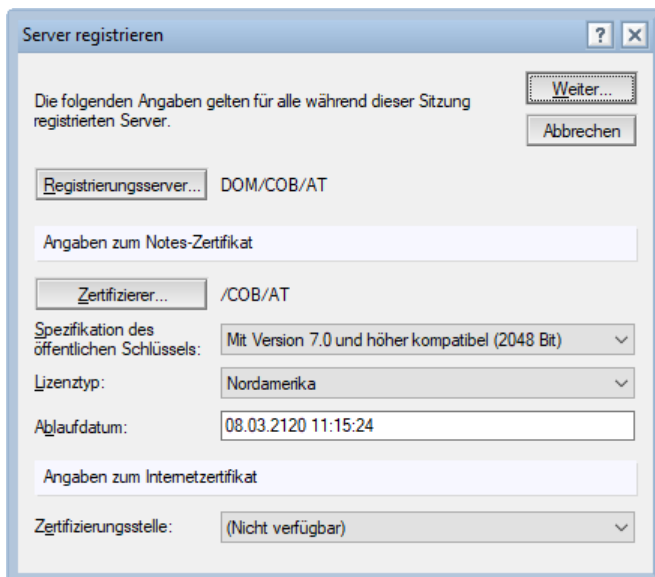


Abbildung 4.67: Dialog Server registrieren

8. Der Dialog **Neue Server registrieren** wird angezeigt:

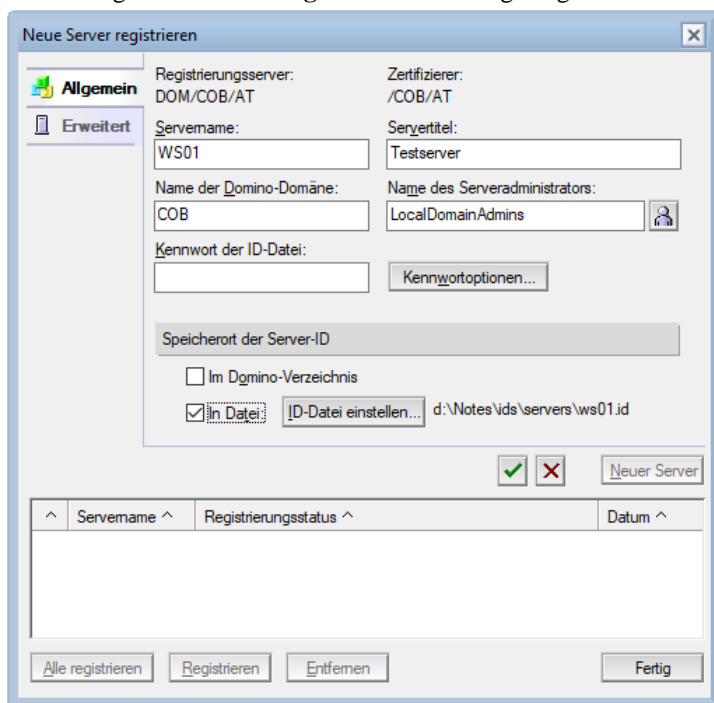


Abbildung 4.68: Der Dialog Neue Server registrieren

7. Geben Sie einen Servernamen ein. Beachten Sie dabei die Namenskonventionen, wie auf Seite 25 angegeben. Wenn möglich, verwenden Sie den Hostnamen des Windows-Servers.
10. (Optional) Ändern Sie bei Bedarf den Namen der Domäne.
11. Tragen Sie als Serveradministrator die vorgegebene Admin-Gruppe (meist LocalDomainAdmins) ein. Wählen Sie eine Person aus, muss diese bei der Konfiguration des Servers auf ihre Benutzer-ID zugreifen können.
12. Wählen Sie im Bereich **Speicherort der Server-ID**:
 - **Im Domino-Verzeichnis**: Dann müssen Sie zusätzlich ein Kennwort für die ID-Datei eingeben, da jeder mit Leserrechten im Domino-Verzeichnis die ID-Datei als Anhang im Serverdokument sehen und herunterladen kann.
 - **In Datei**: Dann ist kein Kennwort erforderlich, da davon ausgegangen wird, dass Sie die ID-Datei an einem sicheren Ort (den vorbereiteten Netzwerkordner) ablegen.
13. Klicken Sie auf das grüne Häkchen und dann auf **Registrieren**.

Wenn Sie ein Serverkennwort vergeben, achten Sie darauf, dass die Kennwortqualität auf 0 (Kennwort ist optional) eingestellt bleibt, damit Sie das Kennwort später löschen können!

Während des Registrierungsprozesses werden (unter anderen) die folgenden Schritte ausgeführt:

- > Es wird eine Server-ID für den neuen Server erstellt und mit der Zulassungsstelle zugelassen.
- > Das Serverdokument wird angelegt und der Name des Notes-Administrators im Feld **Administratoren** eingetragen.
- > Je nach Auswahl wird die Server-ID im Serverdokument und/oder als Datei gespeichert.

- > Der neue Server wird zur Gruppe LocalDomainServers hinzugefügt.
- > Es wird ein Eintrag für den neuen Server im Zertifizierungsprotokoll (certlog.nsf) angelegt.

4.9.3. Einen zusätzlichen Domino-Server konfigurieren

4.9.3.1. Voraussetzungen

Sie können einen zusätzlichen Domino-Server nur konfigurieren, wenn er bereits registriert wurde. Wählen Sie bei der Konfiguration »Setup an additional server«, wird eine Verbindung zu einem bestehenden Domino-Server derselben Domäne aufgebaut, um die notwendigen Informationen aus dem Domino-Verzeichnis auszulesen. Wenn eine Verbindung via Port 1352 nicht möglich ist, können Sie den zusätzlichen Server auch als Stand-Alone-Server (siehe Seite 33) konfigurieren. In diesem Fall müssen Sie Zugriff auf alle notwendigen Dateien (Server-ID, Zulassungsdatei und Domino-Verzeichnis) haben.

4.9.3.2. Schritt-für-Schritt-Anleitung

1. Starten Sie die Server-Software als Administrator.
2. Wählen Sie: »Setup an additional server«. Bei Auswahl dieser Option wird eine Verbindung zu einem bestehenden Domino-Server der Domäne aufgebaut.
3. Haben Sie beim Registrieren die Option »Speicherort der Server-ID: In Datei« gewählt, müssen Sie diese jetzt angeben. Wählen Sie dazu die Option: »The server ID file is stored on a floppy disk, CD or network drive« und klicken Sie auf **Browse...**, um die Datei auszuwählen:



Abbildung 4.69: Serverkonfiguration nach Auswahl der Option ID file is stored on a floppy ...

Nach der Auswahl wird im Feld **Server name** der Name des zusätzlichen Servers angezeigt:



Abbildung 4.70: Serverkonfiguration – Das Feld Server name nach Auswahl einer ID-Datei

Haben Sie beim Registrieren die Server-ID im Domino-Verzeichnis gespeichert, wählen Sie jetzt die Option »The server ID file is stored in the Domino Directory« und geben Sie das Kennwort ein:

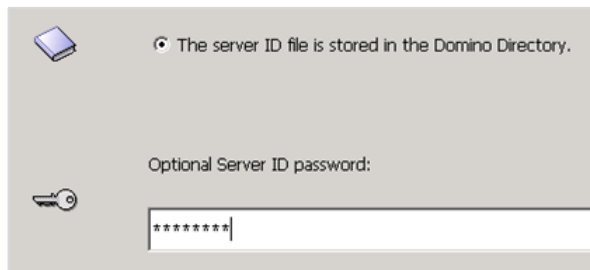


Abbildung 4.71: Serverkonfiguration – Eingabe des ID-Kennworts

In diesem Fall müssen Sie im Feld **Server name** den kompletten hierarchischen Namen des zusätzlichen Servers angeben:



Abbildung 4.72: Serverkonfiguration nach Auswahl der Option »ID file is stored in the Domino Directory«

4. Klicken Sie auf **Next**. Wählen Sie aus, welche Tasks auf dem Server laufen sollen. Wählen Sie »Web Browsers« und »Internet Mail Clients«:

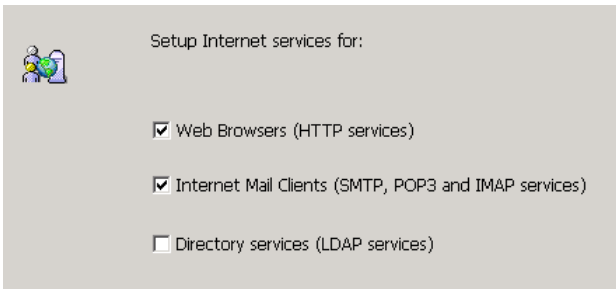


Abbildung 4.73: Serverkonfiguration – Setup Internet Services

5. Klicken Sie danach auf **Customize**, um eine Liste der verfügbaren Domino-Tasks einzusehen, und wählen Sie alle Internetdienste, die Sie nicht brauchen, wieder ab (z. B. POP3 oder IMAP):

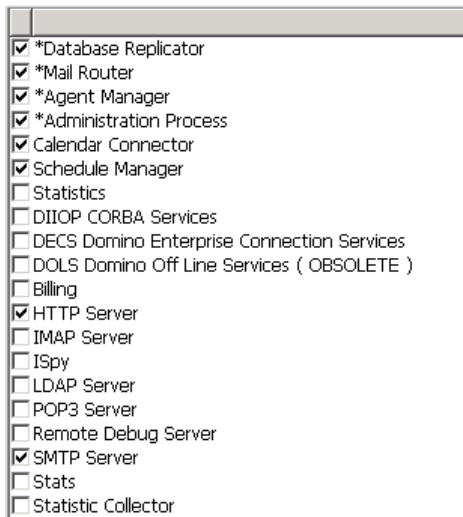


Abbildung 4.74: Serverkonfiguration – Liste der Server-Tasks

6. Geben Sie den Namen des Servers ein, von dem das Domino-Verzeichnis geholt werden soll. Wenn der Servername nicht aufgelöst werden kann, geben Sie zusätzlich die IP-Adresse an:

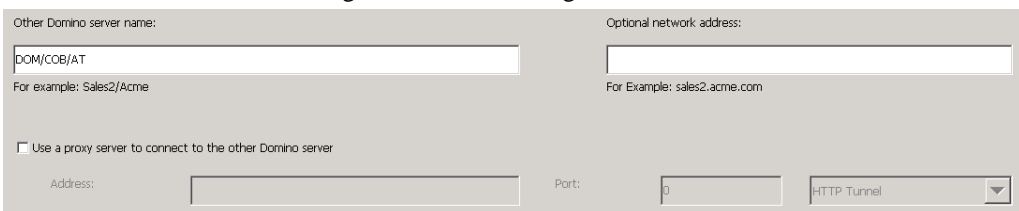


Abbildung 4.75: Serverkonfiguration – Eingabe des Verzeichnisservers

7. Navigieren Sie weiter zu den **Network settings** und klicken Sie auf **Customize**. Hinterlegen Sie den Hostnamen (das Feld kann mit einem Doppelklick bearbeitet werden).

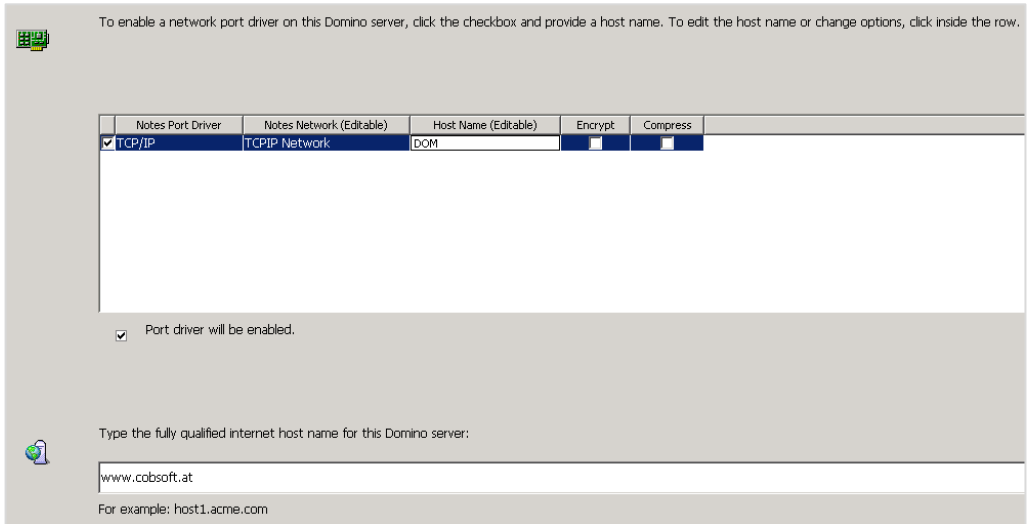


Abbildung 4.76: Serverkonfiguration – Network settings

Erwartet wird ein auflösbare Hostname oder eine IP-Adresse. Geben Sie außerdem einen voll qualifizierten Internet-Hostnamen ein. Klicken Sie auf **Next**.

8. Wählen Sie aus, welcher Verzeichnistyp verwendet werden soll:

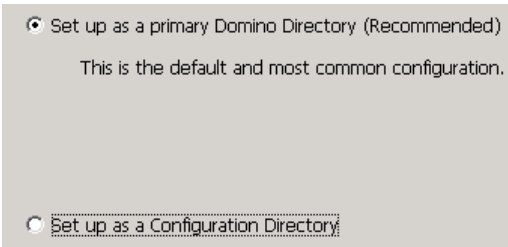


Abbildung 4.77: Serverkonfiguration – Auswahl Verzeichnistyp

Ein **Primary Domino Directory** ist ein vollständiges Verzeichnis, das die gesamte Konfiguration, aber auch alle Personen, Mail-In-Datenbanken, Ressourcen und Gruppen enthält. In kleinen Umgebungen mit wenigen Servern sollten Sie immer diesen Typ wählen.

Ein **Configuration Directory** enthält nur die Konfiguration und keine Benutzer, Mail-In-Datenbanken, Ressourcen und Gruppen. Diese Auswahl macht Sinn, wenn im selben LAN bereits mehrere Domino-Server mit Primärverzeichnissen verfügbar sind. Domino-Server mit einem Konfigurationsverzeichnis können deshalb trotzdem Rechte überprüfen, Gruppen auflösen oder Mails verschicken – sie fragen einfach einen Server mit einem kompletten Verzeichnis. (Die Namenssuchen (Name-Lookups) belasten allerdings auch das Netzwerk, überlegen Sie also genau, wo Sie das Feature einsetzen!)

9. Geben Sie bei Bedarf den Pfad zu den Systemdatenbanken (names.nsf u. a.) an.

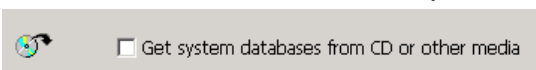


Abbildung 4.78: Serverkonfiguration – Auswahl Systemdatenbanken

10. Klicken Sie auf **OK**, um den Registrierungsprozess zu starten.

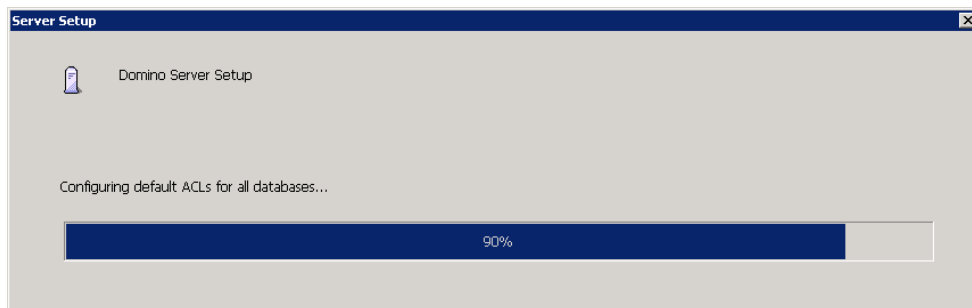


Abbildung 4.79: Serverkonfiguration – Verlaufs balken

Der Setup-Prozess ...

- > erstellt eine Replik des Domino-Verzeichnisses im Datenverzeichnis, wenn es nicht schon existiert.
- > kopiert die Server-ID von dem während des Setups angegebenen Ort ins Domino-Datenverzeichnis.
- > erstellt die Protokolldatei log.nsf.
- > erstellt die Datenbank für Administrationsanforderungen admin4.nsf und vergibt eine Replik-ID basierend auf der des Domino-Verzeichnisses.
- > repliziert die Datenbank Monitoring Konfiguration events4.nsf.
- > erstellt ein (deaktiviertes) Verbindungsdokument zum existierenden Domino-Server im Domino-Verzeichnis.
- > aktualisiert die Netzwerkeinstellungen im Serverdokument.
- > konfiguriert SMTP, wenn das während des Setups ausgewählt wurde.
- > aktualisiert je nach den Einstellungen während des Setups die Zugriffskontrolllisten aller Datenbanken und Schablonen im Datenverzeichnis, um anonymen Zugriff zu entfernen und die Gruppe LocalDomainAdmins hinzuzufügen.
- > repliziert die Änderungen im Serverdokument mit dem existierenden Server.
- > löscht, falls vorhanden, den Anhang server.id aus dem Serverdokument.

4.10. Eine ältere Domino-Version aktualisieren

Das Upgrade von Domino 9.x, 10.x und 11 auf Version 11.0.1 wurde vom Hersteller HCL getestet und zertifiziert. Das heißt für Sie, Sie können, wenn alle Voraussetzungen erfüllt sind (zertifiziertes Betriebssystem mit 64-Bit), einen Domino-Server der Version 9, 10 oder 11 direkt aktualisieren. Handelt es sich bei Ihrem alten Server um eine 32-Bit-Version, wird es jedoch komplizierter.

Ältere Versionen als 9 können nur bedingt direkt aktualisiert werden. Bei 8.5.x ist sehr wahrscheinlich, dass keine Probleme auftreten, bei noch älteren Versionen (7 oder 8) sollten Sie in einem Zwischenschritt zuerst auf Version 9.0.1 aktualisieren.

4.10.1. Eine ältere Version auf 9.0.1 aktualisieren

Nachfolgend eine Kurzfassung der Vorgangsweise für ein Interim-Upgrade auf Domino 9.0.1:

1. Beenden Sie den Domino-Server.

2. Erstellen Sie eine Sicherung aller Dateien (auch der Translogs, falls anwendbar).
3. Installieren Sie Version 9.0.1.
4. Installieren Sie Fix Pack 10.
5. Aktivieren Sie `DEBUG_OUTFILE=<Datei>` in der `notes.ini`, um die Ausgaben auf der Serverkonsole zu erfassen.
6. Wenden Sie Fixup auf alle Datenbanken an, um ihre Integrität zu prüfen und sie nötigenfalls zu reparieren. Öffnen Sie dazu eine Befehlszeile, navigieren Sie zum Domino-Programmverzeichnis (bei allen Versionen vor 11 üblicherweise `C:\Programm Files\IBM\Domino`) und geben Sie den folgenden Befehl ein:

```
C:\Program Files\IBM\Domino>nfixup.exe -f -j -v
```

Erklärung: `-f` steht für ein vollständiges Fixup, alle Dokumente werden überprüft. Ohne die Option `-j` repariert Fixup Datenbanken mit aktivierter Transaktionsprotokollierung nicht. `-v` bewirkt, dass Ansichten-Indizes ausgenommen werden (schneller). (Die Indizes werden nach dem Upgrade auf 11.0.1 ohnehin aktualisiert.)

Sie könne mehrere Fixup-Prozesse gleichzeitig starten und Indirect-Dateien (*.IND) verwenden, um den Vorgang zu beschleunigen. (Zur Anwendung von Fixup lesen Sie Kapitel 9.7 Datenbanken reparieren, ab Seite 260.)

7. Wenden Sie UpdAll auf alle Datenbanken Ihres Domino-Servers an:

```
C:\Program Files\IBM\Domino>nupdall.exe
```

Auch hier können Sie mit Indirect-Dateien (.IND) und mehreren UpdAll-Prozessen arbeiten, um den Vorgang zu beschleunigen.

8. Überprüfen Sie die in der Variable `DEBUG_OUTFILE` angegebene Datei nach Fehlern.
9. Starten Sie den 9.0.1-Domino-Server zumindest einmalig und überprüfen Sie, ob Fehler auftreten.

4.10.2. Aktualisieren von Domino 9.x (oder höher) auf Version 11.x

Bevor Sie das Upgrade auf 11.x durchführen, beachten Sie die folgenden Punkte:

- > Sollte es vor dem Upgrade schwerwiegende Probleme auf Ihrem Domino-Server gegeben haben, lösen Sie diese Probleme zuerst – gegebenenfalls mit Unterstützung der HCL. Erwarten Sie nicht, dass die Probleme durch das Upgrade gelöst werden.
- > Überprüfen Sie Anwendungen von Drittherstellern auf Kompatibilität mit Domino 11.x.
- > Erstellen Sie Sicherungen von allen Dateien und, falls anwendbar, auch des Transaktionsprotokolls.
- > Aktivieren Sie `DEBUG_OUTFILE=<Datei>` in der `notes.ini`, um die Ausgaben auf der Serverkonsole zu erfassen.
- > Wenden Sie Fixup auf alle Datenbanken an, um ihre Integrität zu prüfen und sie nötigenfalls zu reparieren. (Fällt aus, wenn Sie diesen Schritt bereits beim Interim-Upgrade auf 9.0.1 durchgeführt haben.) Öffnen Sie dazu eine Befehlszeile, navigieren Sie zum Domino-Programmverzeichnis (üblicherweise `C:\Programm Files\HCL\Domino`) und geben Sie den folgenden Befehl ein:

```
C:\ProgramFiles\IBM\Domino>nfixup.exe -f -j -v
```

Erklärung: -f steht für ein vollständiges Fixup, alle Dokumente werden überprüft. -j Ohne diese Option repariert Fixup Datenbanken mit aktivierter Transaktionsprotokollierung nicht. -v Ansichten-Indizes werden ausgenommen (schneller). (Die Indizes werden nach dem Upgrade auf 11.0.1 ohnehin aktualisiert.)

Sie könne Indirect-Dateien (*.IND) und mehrere Fixup-Prozesse verwenden, um den Vorgang zu beschleunigen. (Zur Anwendung von Fixup lesen Sie das Kapitel 9.7 Datenbanken reparieren, ab Seite 260.)

Überprüfen Sie danach die in DEBUG_OUTFILE angegebene Datei nach Fehlern.

- > Überprüfen Sie, ob alle Systemdatenbanken in den Eigenschaften, Register **Gestaltung**, die Eigenschaft »Gestaltung aus Master-Schablone übernehmen« gesetzt haben:

- names.nsf (StdR4PublicAddressBook)
- log.nsf (StdNotesLog)
- events4.nsf (StdR4Events)
- admin4.nsf (StdR4AdminRequests)

Dies ist nötig, damit der Design-Task die Gestaltung der Systemdatenbanken aktualisieren kann. (Sie können die Gestaltung aber auch später händisch aktualisieren.)

- > Wenn Sie mehrere Server aktualisieren, setzen Sie die Eigenschaft »Gestaltung nur auf Administrationsserver aktualisieren«. Damit verhindern Sie, dass ältere Domino-Server über Nacht, wenn der Design-Task läuft (siehe Kap. 11.2.3.2 Der Servertask Design, ab Seite 309), die Gestaltung des Domino-Verzeichnisses zurücksetzen:

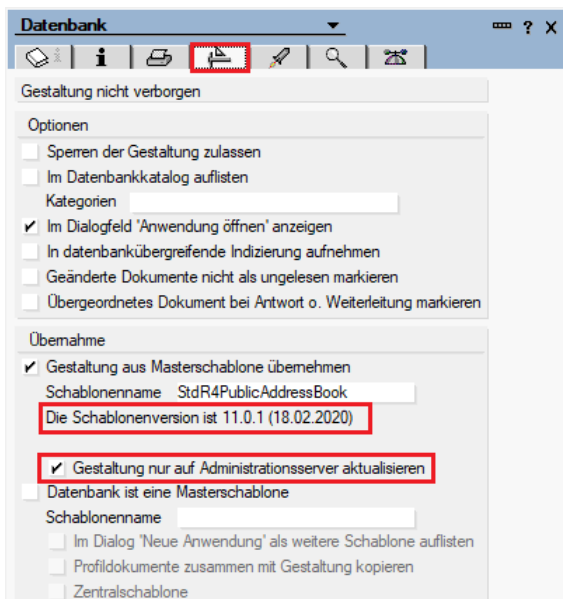


Abbildung 4.80: Datenbankeigenschaften, Register Gestaltung

4.10.3. Das Ausrollen der neuen Version planen

Halten Sie sich an die folgende Reihenfolge:

1. Aktualisieren Sie die Domino-Administrator-Clients.

2. Aktualisieren Sie den Administrationsserver des Domino-Verzeichnisses. (Bei diesem Schritt wird die Gestaltung des Domino-Verzeichnisses aktualisiert.)
3. Aktivieren Sie in den Datenbankeigenschaften des Domino-Verzeichnisses, Register Gestaltung, die Option **Gestaltung nur auf Administrationsserver aktualisieren.** ()
4. Aktualisieren Sie alle anderen Systemdatenbanken auf dem Administrationsserver.
5. Aktualisieren Sie die anderen Domino-Server, typischerweise zuerst Mail- und Webserver, dann alle übrigen.
6. Aktualisieren Sie die Notes-Clients.
7. Aktualisieren Sie die Gestaltung der Mail-Datenbanken und der anderen Anwendungen.
8. Stellen Sie – falls dies noch nicht geschehen ist – auf das neueste Dateiformat (ODS 53) um.

Die Schritte 1 bis 4 sollten unabhängig von Ihrer Upgrade-Strategie immer gleich ablaufen. Beim Upgrade von Version 9.0.1 ist es jedoch auch möglich, die Aktualisierung des Domino-Verzeichnisses vor dem eigentlichen Server-Upgrade vorzunehmen. Besorgen Sie sich dazu eine Kopie der Verzeichnisschablone (pubnames.ntf) und aktualisieren Sie die Gestaltung des Verzeichnisses auf allen 9.0.1er-Servern. Das Domino 11.x-Verzeichnisdesign ist bis Version 9.0.1 rückwärtskompatibel. Es enthält die folgenden Änderungen:

- > Das Branding wurde von IBM auf HCL umgestellt.
- > Die Konfiguration für AUT wurde vollständig implementiert, inklusive HCAA.
- > Hinzufügen von 4096-Bit-Schlüsseln in der Registriereinstellung
- > Hinzufügen von Einstellungen für die Active Directory Password Synchronisation zu den Server Tasks (Teilmaske \$ServerTasks).
- > Hinzufügen der Ansicht PWSyncProcessors, um Kennwort-Synchronisierungen zu ermöglichen
- > Korrektur der deutschen Feiertage
- > Neuordnung der Router-/SMTP-Einstellungen (Teilmaske \$RouterSMTPSettings)
- > Hinzufügen weiterer sicherer SSL-Verschlüsselungscodes (Ciphers) und Verschieben der als unsicher geltenden zu einer Liste von unsicheren Codes.
- > Entfernen von allen Hinweisen auf SSL v2
- > Vorgabe für den Abwesenheitsagent ist jetzt »Service« und nicht mehr »Agent«.
- > Hinzufügen der Möglichkeit, Querzulassungen von der Ansicht Zertifikate aus durchzuführen.
- > Überprüfen von Gruppennamen, um zu verhindern, dass sie denselben Namen bekommen wie Personen
- > Ermöglichen der Sortierung der Spalte Vault-Synchronisierung in der Ansicht Personen
- > Diverse Bug-Fixes

Die Schritte 5 bis 8 hängen stark von Ihrer Unternehmensstruktur ab und können speziell in großen Umgebungen mit Tausenden von Benutzern auch abweichen. So kann es etwa sinnvoller sein, zuerst alle Server eines Standortes zu aktualisieren und dann zum nächsten weiterzuwandern.

4.11. Domino und AntiVirus

Wenn Sie am Domino-Server eine AntiVirus-Software einsetzen müssen, verwenden Sie unbedingt eine Lösung, die mit Notes und Domino zusammenarbeitet. AV-Lösungen, die auf Betriebssystemebene operieren, wirken sich negativ auf die Serverperformance aus und können in bestimmten Fällen sogar zu Abstürzen führen. Kommen Sie um den Einsatz einer solchen Lösung nicht herum, deaktivieren Sie das Scannen des Datenverzeichnisses, der Transaktionsprotokolle, des DAOS-Speicherbereichs und aller Verzeichnisse, in denen Indexdateien aktualisiert oder gespeichert werden.

Wenn das nicht möglich ist, deaktivieren Sie zumindest das Scannen der folgenden Dateitypen:

- > *.nsf, *.ntf, *.box
- > *.ncf, *.ndk
- > *.TXN, *.NDX
- > *.DTF
- > *.nlo

5. Serverkonfiguration

- > 5.1 Serverkonsolen, Seite 85
- > 5.2 Die Datei notes.ini, Seite 91
- > 5.3 Domino-Serverprogramme, Seite 94
- > 5.4 Konfigurationsdokument, Seite 99
- > 5.5 Datenbankcache und Transaktionsprotokoll, Seite 101
- > 5.6 Die verschiedenen Domino-Administratoren, Seite 108
- > 5.7 Der Administrationsprozess, Seite 112
- > 5.8 Domino-Server neu installieren oder verschieben, Seite 119

5.1. Serverkonsolen

In der Domino-Welt findet ein Gutteil der Kommunikation über Konsolenbefehle statt. Für Sie als angehenden Administrator mag es anfangs schwierig sein, sich die Syntax zu merken, aber ich bin überzeugt, dass Sie die Flexibilität, die Ihnen die Konsole bietet, schnell zu schätzen lernen.

Je nach Modus präsentiert der Server einen Textbildschirm, in dem Sie direkt Befehle eintippen können, oder er läuft unsichtbar im Hintergrund. Im zweiten Fall können Sie die Befehle über entfernte Konsolen absetzen.

Es gibt vier verschiedene Serverkonsolen:

1. die direkte Serverkonsole (nach Start des Domino-Servers als Applikation bzw. im Stand-Alone-Modus)
2. die Entfernte Konsole im Domino-Administrator
3. die sogenannte Domino-Console (eine Java-Konsole)
4. die Live-Konsole im Domino-Webadministrator

Der Vollständigkeit halber sei erwähnt, dass Konsolenbefehle auch über Programmdokumente und Event-Handler abgesetzt werden können. Ein Beispiel für ein Programmdokument finden Sie in Kap. 5.3.4.3 Serverkonsolenbefehle über Programmdokumente absetzen, ab Seite 99.

5.1.1. Die direkte Serverkonsole

Diese steht nur zur Verfügung, wenn Sie den Domino-Server als Applikation bzw. im Stand-Alone-Modus gestartet haben und nicht als Dienst (Service):

```
C:\ProgramFiles\HCL\Domino>nserver.exe -sa
```

Zum Unterschied zwischen Dienst und Applikation lesen Sie den Vergleich auf Seite 55.

5.1.2. Die Entfernte Konsole im Domino-Administrator

Die Entfernte Konsole darf nur von Personen verwendet werden, die im Serverdokument, Register **Sicherheit**, in den Feldern **Administratoren mit voller Berechtigung**, **Administratoren** oder **Administratoren mit voller Remotekonsolen-Berechtigung** eingetragen sind. Personen, die im Feld **Leseberechtigte Administratoren** stehen, dürfen die Konsole eingeschränkt, nur zum Absetzen von Abfragen, benutzen.



Abbildung 5.1: Das Serverdokument mit den verschiedenen **Administratoren-Typen**

Tipp: Verwenden Sie zum Zuordnen von Rechten immer Gruppen!

5.1.2.1. Die Entfernte Konsole anzeigen

Wählen Sie im Domino-Administrator das Register **Server... > Status** und dann den Eintrag **Serverkonsole**.

5.1.2.2. Live-Konsole ein- und ausschalten

Die Entfernte Konsole zeigt die Ausgaben des Servers nur an, wenn Sie den Live-Modus aktivieren. Nach dem Wechsel auf ein anderes Register und wieder zurück geht der Live-Modus meist verloren und muss erneut aktiviert werden.

	Klicken Sie auf Live , wenn Sie Serverantworten unmittelbar sehen wollen.
	Klicken Sie auf Pause , um die Ausgabe anzuhalten. Klicken Sie auf Fortsetzen , um in den Live-Modus zurückzukehren.
	Klicken Sie auf Stopp , um die Live-Konsole zu beenden.

Tabelle 5.1: Live-Konsole ein- und ausschalten

Tipp: Sie können den Domino-Administrator bereits mit aktiviertem Live-Modus starten. Öffnen Sie im Menü **Datei > Vorgaben > Administration...** die Administrationsvorgaben und wählen Sie

im Bereich **Starteinstellungen** entweder einen Server aus oder die Option »Mit zuletzt verbundenem Server verbinden«. Setzen Sie dann ein Häkchen bei **Live-Konsole automatisch starten**.

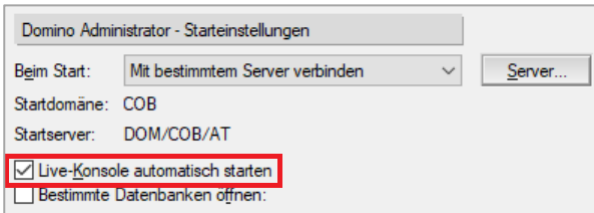


Abbildung 5.2: Administrationsvorgaben – Live-Konsole automatisch starten

5.1.2.3. Anpassen der Ausgabe

Klicken Sie mit der rechten Maustaste in den Hintergrund (ins Schwarze) und wählen Sie im Menü **Eigenschaften: Konsole...**

Ich empfehle Ihnen, auf eine besser lesbare serifenlose Schrift umzustellen und, zumindest wenn Sie wie ich eine Lesebrille brauchen, auch die Schriftgröße zu erhöhen:

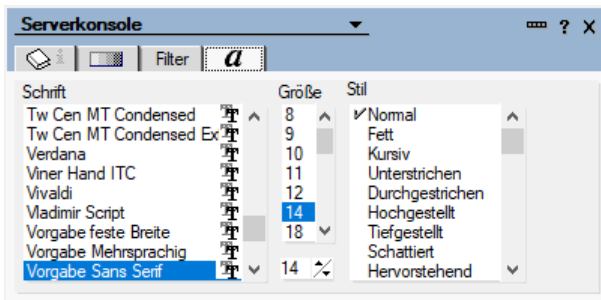


Abbildung 5.3: Eigenschaften der Serverkonsole, Register Schrift

Ein praktischer Einsteigertipp ist es, die Ausgaben entsprechend den zugeordneten Schwierigkeitsgraden in unterschiedlichen Farben darzustellen:

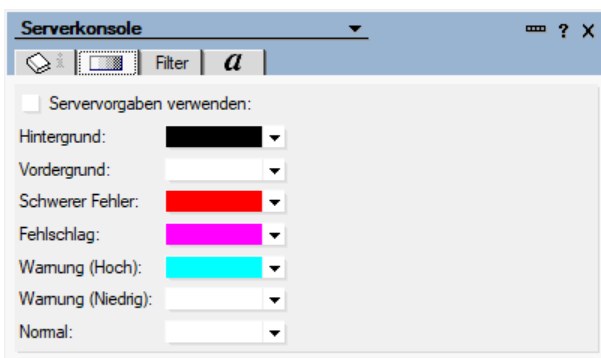


Abbildung 5.4: Eigenschaften der Serverkonsole, Register Farben

So erkennen Sie sofort, welche Fehler eine höhere Priorität aufweisen.

5.1.2.4. Bedienen der entfernten Konsole

> Tippen Sie den gewünschten Befehl ein und drücken Sie die Eingabe-Taste (ENTER).

- > Mit der Taste ESCAPE löschen Sie die Befehlszeile.
- > Mit den Pfeiltasten können Sie die zuletzt eingegebenen Befehle zurückholen.
- > Aus der Zwischenablage eingefügter Text löscht Ihre Eingabe.
- > Für alle Serverbefehle können Abkürzungen verwendet werden; diese sind in diesem Buch unterstrichen dargestellt.
- > Klicken Sie rechts oben auf **Pause**, um die Bildschirmausgabe anzuhalten. Klicken Sie auf **Fortsetzen**, um die Bildschirmausgabe fortzusetzen (siehe Tabelle 5.1).
- > Falls ein Befehlszeilenparameter einen Leerschritt enthält, setzen Sie diesen in Anführungszeichen, z. B.: pull "Server 1"
- > Bei einigen Befehlen gibt der Server keine Rückmeldung an die Konsole aus. Um das Ergebnis dieser Befehle nachzuprüfen, öffnen Sie das Serverprotokoll.
- > Greifen Sie mit Befehlen auf Datenbanken zu (etwa um diese zu replizieren oder zu komprimieren), geschieht dies mit den Rechten des Servers

Beispiel: Der Befehl `show users` zeigt die aktuellen Benutzersitzungen an:

```
> show user
Benutzername      Geöffnete Datenbanken   Minuten seit der letzten Verwendung
Admin/Buchacher
                  names.nsf                0
```

Abbildung 5.5: Die Ausgabe von `show users` auf der entfernten Serverkonsole

Mit dem Umleitungszeichen (>) kann die Ausgabe eines Befehls in eine Datei umgeleitet werden, z. B.:

```
show tasks >D:\Domino\Data\Tasks.txt
```

Alle Eingaben auf der Serverkonsole sind außerdem in der Protokolldatei (log.nsf), Ansicht »Verschiedene Ereignisse« sichtbar.

Eine Auswahl der wichtigsten Konsolenbefehle finden Sie in Anhang A.

5.1.3. Die Domino-Console

Die Domino-Console ist eine Java-basierende Konsole, die mit einem Server-Controller und in weiterer Folge mit einem oder mehreren Domino-Servern kommuniziert.

Wenn Sie sich über diese Konsole zu einem Domino-Server-Controller verbinden, sieht es genauso aus wie eine »traditionelle« Domino-Server-Konsole mit einem zusätzlichen Menü. Mit diesem Menü ähnelt sie dann der entfernten Konsole im Admin-Client.

Die Domino-Console kann als schlanker Konsolen-Client bezeichnet werden, der allein auf einem Server oder einem PC installiert wird. Sie funktioniert jedoch ausschließlich als Konsole, es sind keine weiteren Administrationsfähigkeiten verfügbar und es können keine Notes-Datenbanken geöffnet werden.

Die Java-Konsole bietet einige Vorteile:

- > Sie kann sich mit mehreren Servern verbinden und Befehle an mehrere Server gleichzeitig senden.

- > Man braucht keine Notes-ID, nur ein Personendokument mit einem Internetkennwort. Entsprechend kann man sich mit Servern aus anderen Organisationen verbinden, ohne eine Querkzulassung erstellen zu müssen.
- > Sie erlaubt verschiedene Anpassungen, etwa das Setzen von Filtern auf bestimmte Serverereignisse.
- > Die Serverausgabe kann in Protokolldateien gespeichert werden.
- > Es können auch Betriebssystembefehle abgesetzt werden.

Die Domino-Console ist als getrenntes Installationspaket für verschiedene Plattformen vorhanden, unter Windows wird sie mit dem Server mitinstalliert.

5.1.3.1. Anpassen der Domino-Console

Meldungen den Schweregraden entsprechend in unterschiedlichen Farben darzustellen, konfigurieren Sie in der Datenbank »Monitoring Configuration« (events4.nsf).

Wechseln Sie dazu im Domino-Administrator zum Register **Konfiguration** und wählen Sie **Überwachungskonfiguration** > **Console Attributes**. Editieren Sie das Dokument Ihres Servers oder erstellen Sie ein neues:

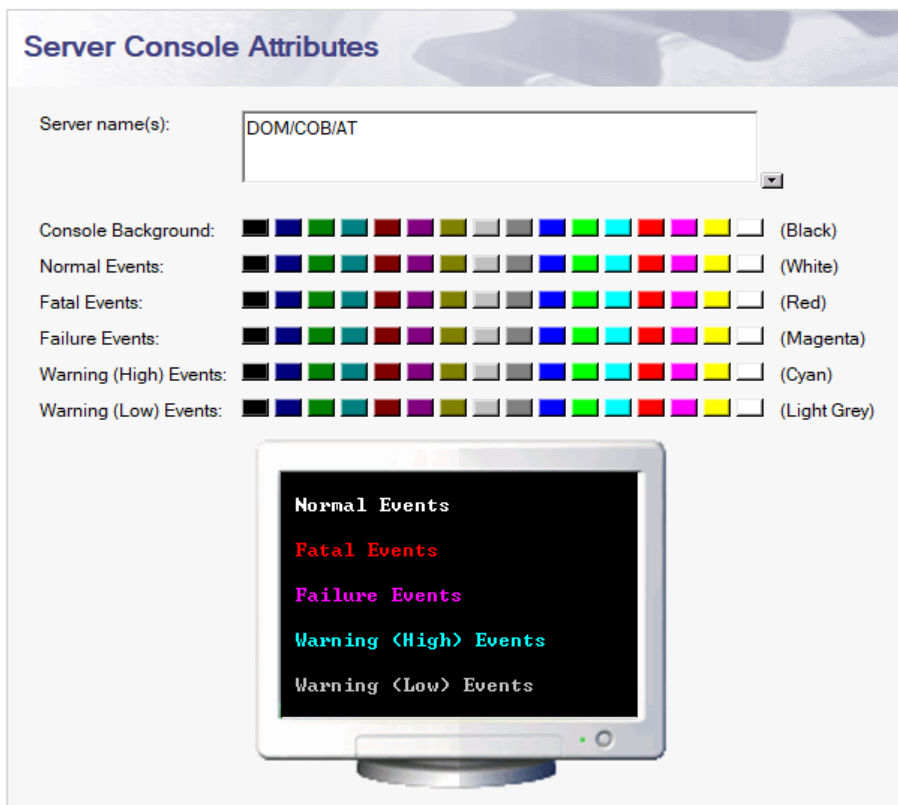


Abbildung 5.6: Server Console Attributes

Andere Eigenschaften, wie etwa die verwendete Schriftart, konfigurieren Sie direkt in der Konsole; wählen Sie dazu im Menü **Edit** > **Console Font...**

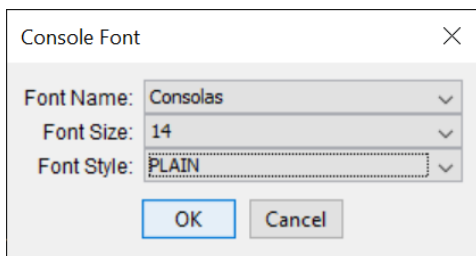


Abbildung 5.7: Einstellungen für die Konsolenschriftart

5.1.4. Konsolen im Domino-Webadministrator

Hinter diesem Feature steckt die Datenbank `webadmin.nsf`, die sich direkt im Datenverzeichnis des Servers befindet. Starten Sie den Domino-Webadministrator über die folgende URL:

<http://ihrservername/webadmin.nsf>

Über **Server... > Status > Quick Console** können Sie beliebige Befehle absetzen, erhalten jedoch keine Antwort.

Über **Server... > Status > Live Console** gelangen Sie zur Live-Konsole, welche in aktuellen Webbrowsern jedoch nicht mehr verfügbar ist, da dafür das Java-Plugin 1.4 oder höher installiert sein muss.

Details zum Domino-Web-Administrator finden Sie im Kap. 14.8 Der Domino-Webadministrator, ab Seite 409.

5.1.5. Wichtige Befehle für alle Konsolen

Hinweis: Kann ein Befehl abgekürzt werden, ist die Mindesteingabe unterstrichen dargestellt.

Über den Befehl `help` erhalten Sie eine Liste der wichtigsten Serverbefehle mit einer kurzen Erklärung.

Beenden Sie den Domino-Server mit den Befehlen:

`quit` oder `exit`.

Bedenken Sie, dass in der entfernten Konsole damit die Verbindung zum Server verloren geht!

Achtung: Wenn Sie den Domino-Server als Dienst gestartet haben, sollten Sie ihn auch als Dienst beenden (siehe Seite 55, Kap. 4.6 Einen Domino-Server starten und beenden).

Ein Neustarten des Servers ist über den folgenden Befehl möglich:

`restart server`

Diesen Befehl können Sie getrost auch in der entfernten Konsole eingeben; die Verbindung geht zwar verloren, wird nach dem Hochfahren aber neu aufgebaut.

Eine Aufstellung der wichtigsten Konsolenbefehle finden Sie in Anhang B auf Seite 501.

5.1.6. Thread-ID

Per Vorgabe wird jeder Ausgabe auf der Serverkonsole die Thread-ID vorangestellt. Dies erfolgt im Format: [ProcessID:Virtual Thread ID-Native Thread ID].

```
[0AB8:0002-0ABC] 30.12.2020 18:35:01 Starting replication with server COBDOMINO01/COB/AT
[0AB8:0002-0ABC] 30.12.2020 18:35:01 Access control is set in catalog to not allow replication fro
[0AB8:0002-0ABC] 30.12.2020 18:35:01 Access control is set in COBDOMINO01/COB/AT catalog
[0AB8:0002-0ABC] 30.12.2020 18:35:01 Finished replication with server COBDOMINO01/COB/AT
```

Abbildung 5.8: Konsolenausgabe mit vorangestellter Thread-ID

Die Thread-ID kann zum Aufspüren eines Prozesses, der eine Semaphore blockiert, hilfreich sein, braucht aber auch viel Platz, weshalb ich sie meist ausblende. Das ist mit folgendem Befehl möglich:

```
set configuration debug_threadid=0
```

```
se con DEBUG_THREADID=0
29.02.2020 19:11:22 Remote console command issued by Christian Buchacher/COB/AT:
29.02.2020 19:11:22 DEBUG_THREADID changed to 0.
```

Abbildung 5.9: Ausgabe des Befehls: set configuration debug_threadid=0

Analog blenden Sie die Thread-ID mit dem folgenden Befehl wieder ein:

```
set configuration debug_threadid=1
```

5.2. Die Datei notes.ini

Domino schreibt seine Einstellungen nicht etwa in die Windows Registrierdatenbank, sondern in eine schlichte Textdatei namens notes.ini. Diese befindet sich unter Windows im Programmverzeichnis des Servers, also per Vorgabe in C:\Program Files\HCL\Domino.

Achtung: Unsachgemäße Änderungen könnten Fehlverhalten von Domino verursachen.

5.2.1. Die Datei notes.ini direkt bearbeiten

Nach einem direkten Bearbeiten der Datei notes.ini muss immer der Server bzw. der betroffene Servertask neu gestartet werden. Zum Bearbeiten müssen Sie den Editor (notepad.exe) als Administrator ausführen. Tippen Sie dazu im Windows Startmenü »notepad« ein, klicken Sie mit der rechten Maustaste auf das gefundene Programm **Editor** und wählen Sie im Kontextmenü den Befehl **Als Administrator ausführen**:

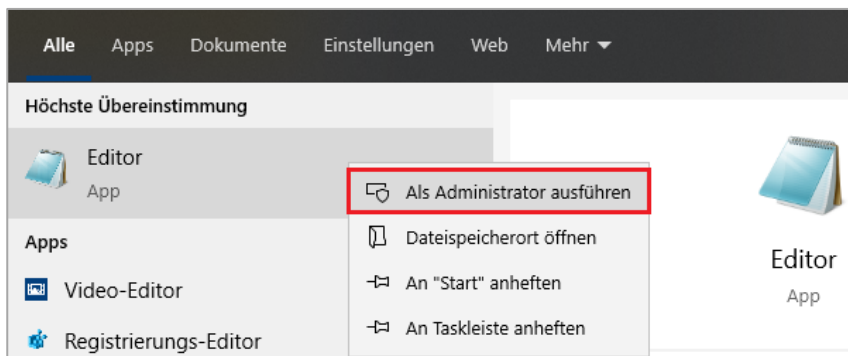


Abbildung 5.10: Ausführen des Editors als Administrator

Navigieren Sie nun zum Domino-Programmverzeichnis und öffnen Sie die Datei notes.ini. (Sie können im Öffnen-Dialog die Zeichenfolge *.ini eingeben, um auf Dateien mit dieser Endung zu filtern.)

Achtung: Erstellen Sie einen neuen Eintrag am Ende der Datei, fügen Sie danach durch Drücken der Eingabetaste noch eine Leerzeile hinzu.

5.2.2. Über das Konfigurationsdokument in die notes.ini schreiben

Einstellungen, die über das Konfigurationsdokument vorgenommen werden, haben Vorrang vor in der Datei notes.ini stehenden Einstellungen. Manche Einstellungen wirken dynamisch, bei anderen müssen Sie den Server bzw. nur den betroffenen Servertask neu starten.

Beim Hochfahren liest der Server das Konfigurationsdokument, durchsucht es nach betriebsrelevanten Informationen, liest die Einstellungen in den Arbeitsspeicher und aktualisiert die Datei notes.ini. Im Anschluss daran fragt der Server alle fünf Minuten Änderungen in den Konfigurationsdokumenten ab.

Um über ein Konfigurationsdokument in die Datei notes.ini zu schreiben, gehen Sie wie folgt vor:

1. Öffnen Sie ein vorhandenes Konfigurationsdokument oder erstellen Sie ein neues.
2. Wechseln Sie zum Register **NOTES.INI-Einstellungen** und klicken Sie auf die Schaltfläche **Parameter einstellen/ändern**.
3. Setzen wir in diesem Beispiel einen Parameter, den wir später brauchen werden, z. B. Create_R85_Log=1. Geben Sie bei **Element** den Text »Create_R85_Log« ein und bei **Wert** die Ziffer »1«. Klicken Sie auf die (schlecht lesbare) Schaltfläche **Hinzufügen/Aktualisieren**.

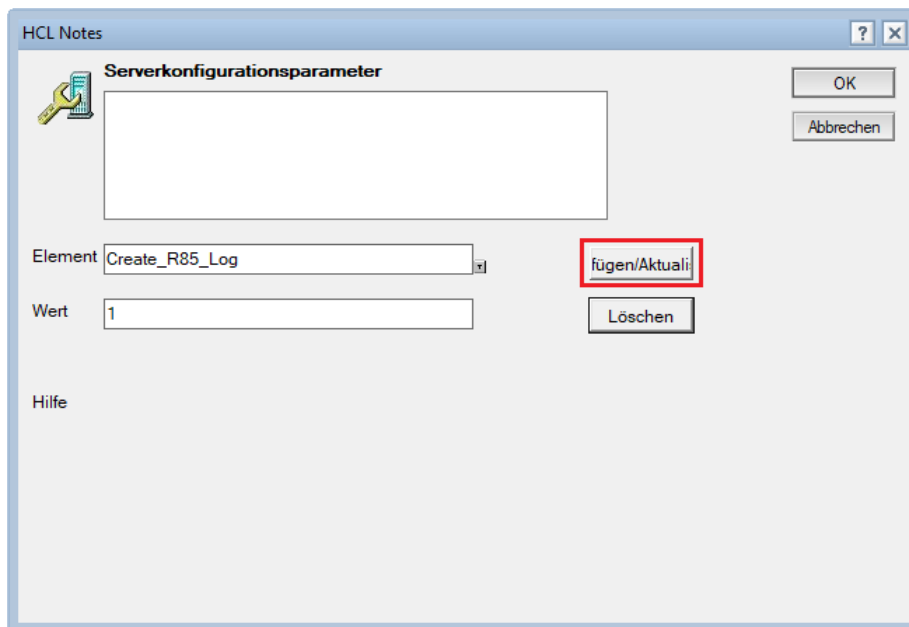


Abbildung 5.11: Dialog zum Hinzufügen von notes.ini-Einträgen im Konfigurationsdokument

4. In der Parameterliste steht jetzt Create_R85_Log=1. Klicken Sie auf **OK**. Der Parameter steht jetzt auch im Konfigurationsdokument:

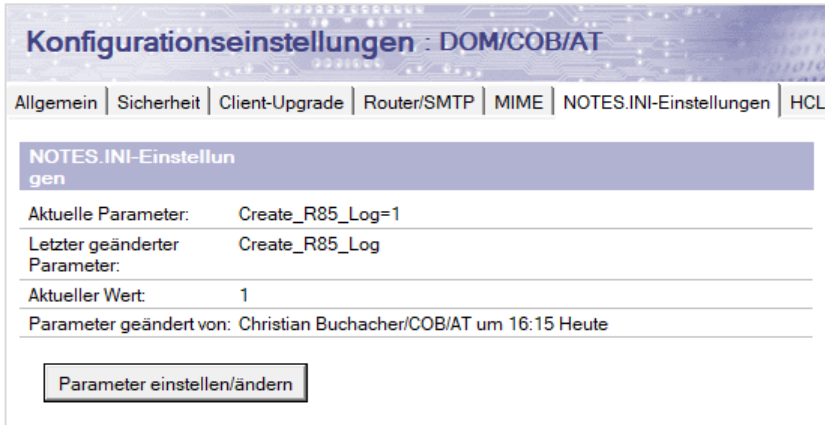


Abbildung 5.12: Das Konfigurationsdokument, Register NOTES.INI-Einstellungen

5. Speichern und schließen Sie das Dokument.

5.2.3. Über die Serverkonsole in die notes.ini schreiben

Auch beim Schreiben über Serverkonsolenbefehle gilt, dass manche Einstellungen dynamisch wirken, bei anderen müssen Sie den Server bzw. den betroffenen Servertask neu starten. Zum Schreiben in die Datei notes.ini kann folgender Konsolenbefehl verwendet werden:

```
set configuration <Variable>=<Wert>
```

Mit dem folgenden Befehl kann der gesetzte Wert einer Variablen abgefragt werden:

```
show configuration <Variable>
```

```
sh con servertasksat1
[0E48:005A-0E40] 29.02.2020 19:00:24 Remote console command issued
[0E48:0006-0D44] SERVERTASKSAT1=Catalog,Design
```

Abbildung 5.13: Ausgabe des Befehls show configuration

5.2.4. Im Domino-Webadministrator in die notes.ini schreiben

Gehen Sie im Domino-Webadministrator auf das Register **Configuration** und wählen Sie dort **Server > notes.ini file**.

Klicken Sie auf die Schaltfläche **Edit** und setzen Sie den gewünschten Eintrag.

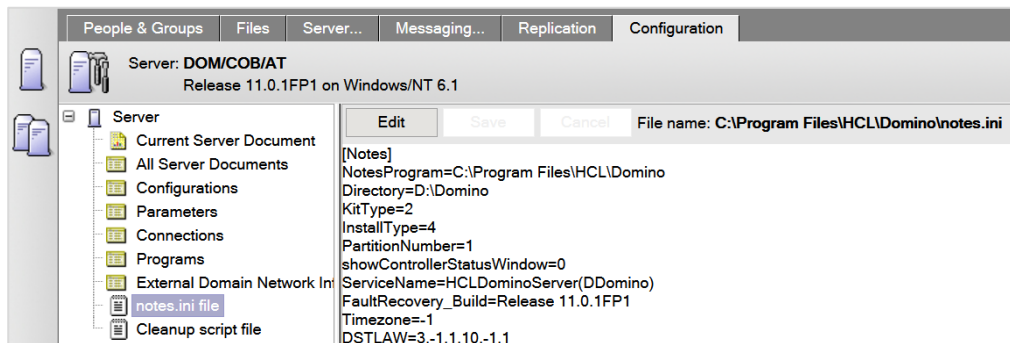


Abbildung 5.14: Bearbeiten der Datei notes.ini im Webadministrator

Wenn Sie fertig sind, klicken Sie auf die Schaltfläche **Save**.

Details zum Domino-Webadministrator finden Sie in Kap. 14.8, ab Seite 409.

5.3. Domino-Serverprogramme

Serverprogramme (auch als Servertasks bezeichnet) haben unterschiedlichste Aufgaben: Sie horchen auf bestimmten Ports auf Anfragen (IMAP, LDAP, SMTP u. a.), komprimieren Datenbanken oder aktualisieren Volltextindizes, automatisieren komplexe Verwaltungsaufgaben (Administrationsprozess), nehmen Mails entgegen oder leiten sie weiter.

Man unterscheidet zwei Arten von Programmen: jene, die immer laufen und auf Anfragen warten (wenn Sie gerade nichts zu tun haben, befinden sie sich im Leerlauf – auf Englisch »idle«), und jene, die Aufgaben zu erfüllen haben und sich selbst beenden, wenn sie damit fertig sind. Der zweite Typ kann nur manuell oder nach Zeitplan gestartet werden.

Vom ersten Typ sind alle Tasks, die auf einen Port auf Anfragen horchen (HTTP, SMTP, LDAP), aber auch der Mail-Router oder der Administrationsprozess. Ein Beispiel für den zweiten Typ ist der Compactor oder das Programm Fixup. Eine Übersicht über alle gerade am Server laufenden Programme liefert der Befehl:

`show tasks only`

```
show tasks only

      Task                Description
SMTP Server              Listen for connect requests on TCP Port:25
SMTP Server              Utility task
Process Monitor          Idle
Router                   Utility: Idle
Router                   MailEvent: Idle
Agent Manager            Executive '1': Idle
Router                   Dispatch: Idle
Router                   Dispatch: Idle
Router                   Sweep: Idle
Router                   Sweep: Idle
Router                   Mailbox: Idle
Statistic Collector      Idle
Admin Process            Idle
Rooms and Resources      Idle
SMTP Server              Control task
Schedule Manager         Idle
HTTP Server              Listen for connect requests on TCP Port:80
Inline Index             Inline Index
Directory Indexer        Idle
Indexer                  Idle
Agent Manager            Idle
Calendar Connector       Idle
Replicator               Idle
Router                   Main: Idle
Event Monitor            Idle
```

Abbildung 5.15: Ausgabe des Befehls `show tasks only`

(Lassen Sie das »only« weg, erhalten Sie zusätzlich eine Liste der aktiven Datenbankserver-Tasks, was die Ausgabe recht unübersichtlich gestaltet.)

Mit laufenden Tasks kommunizieren Sie über den Befehl `tell`. Wollen Sie wissen, welche Tell-Befehle ein laufender Task akzeptiert, können Sie ihn fragen:

```
tell <Task> -?
```

Beachten Sie, dass häufig ein anderer Name eingegeben werden muss, als angezeigt wird: So ist etwa der Agent Manager mit »amgr« anzusprechen, der Indexer mit »update«, der Replikator mit »replica«. Um z. B. den Agent Manager zu fragen, welche Befehle er unterstützt, geben Sie ein:

```
tell amgr -?
```

```
tell amgr -?
Purpose:  Runs scheduled agents in Domino database(s).
Usage:    Tell AMGR [options]...
[options]:
run db 'a'  Runs agent 'a' in database db (Quotes are required).
cancel db 'a' Cancels agent 'a' in database db (Quotes are required).
status     Show current queues and configuration information.
schedule   Shows todays scheduled agents, database, trigger and start time.
pause     Pauses scheduling of agent runs.
resume     Resumes paused scheduling of agent runs.
debug     Shows current debug control settings.
debug [n] Sets n debug control setting(s):
[options n]:
  m      Memory warnings
  e      Events
  c      Control parameters
  v      Verbose debug output
  r      Run reports
  s      Schedules of agents
  p      Performance statistics
  l      Loading reports
  -      Remove all debug flags
```

Abbildung 5.16: Ausgabe des Befehls `tell amgr -?`

Beenden Sie ein Programm mit dem Befehl:

```
tell <Taskname> quit
```

Sie können einen Task auch durchzustarten, etwa nach einer Konfigurationsänderung:

```
restart task <Taskname>
```

Serverprogramme können auf vier Arten gestartet werden:

1. auf der Serverkonsole (Server läuft)
2. in einer Eingabeaufforderung auf Betriebssystemebene (Server läuft nicht)
3. über Variablen in der Datei `notes.ini` des Servers
4. über Programmdokumente im Domino-Verzeichnis

5.3.1. Programme über die Serverkonsole starten

Auf der Konsole starten Sie Programme mit dem Befehl `load`. Um etwa den Datenbank-Compactor zu starten, geben Sie ein:

```
load compact <Schalter>
```

Wenn Sie wissen wollen, welche Schalter ein Programm unterstützt, das gerade nicht läuft, können Sie mit `load` und dem Parameter `-?` nachfragen:

```
load compact -?
```

In diesem Fall gibt das Programm die Liste der Optionen aus und beendet sich wieder.

5.3.2. Programme auf Betriebssystemebene starten

Auf Betriebssystemebene können Sie Programme in der Regel nur starten, wenn der Domino-Server nicht läuft, weil sonst der Zugriff auf Notes-Datenbanken gesperrt ist.

Da hinter allen Servertasks ausführbare Programme (also EXE-Dateien) stecken, geben Sie auf Betriebssystemebene kein `load` ein. Eine Besonderheit gibt es noch zu beachten: Sie müssen vor jeden Tasknamen ein zusätzliches `n` setzen. Aus: `load compact` wird somit: `ncompact.exe`.

Das zusätzliche `n` am Beginn des Programmnamens ist nur unter Windows einzugeben, auf allen anderen Plattformen (z. B. Linux) heißen die Servertasks auf Betriebssystemebene genauso wie auf der Serverkonsole.

Sie müssen das Programm `ncompact.exe` außerdem als Administrator ausführen. Das erreichen Sie am einfachsten, indem Sie bereits die Eingabeaufforderung als Administrator starten. Tippen Sie dazu `cmd` in die Suchleiste ein und klicken Sie dann mit der rechten Maustaste auf den Eintrag `Eingabeaufforderung` und wählen Sie `Als Administrator ausführen`.

Geben Sie nun den folgenden Befehl ein:

```
C:\Programme\HCL\Domino>ncompact.exe -C -* -ODS
```

Abbildung 5.17 zeigt die Ausgabe obigen Befehls:

```
C:\>cd programme\hcl\domino
C:\Programme\hcl\Domino>ncompact.exe -C -* -ODS
25.04.2020 11:06:54 Compacting activity.ntf (Activity Trends (8)), -C -* -ODS
25.04.2020 11:06:56 Compacted activity.ntf, 216K bytes recovered (13%), -C -* -ODS
25.04.2020 11:06:56 Compacting admin4.nsf (Administration Requests), -C -* -ODS
25.04.2020 11:06:59 Compacted admin4.nsf, 768K bytes recovered (23%), -C -* -ODS
25.04.2020 11:06:59 Compacting admin4.ntf (Administrationsanforderungen (11.0)), -C -* -ODS
25.04.2020 11:07:02 Compacted admin4.ntf, 0K bytes recovered (0%), -C -* -ODS
25.04.2020 11:07:02 Compacting AgentRunner.nsf (Java AgentRunner), -C -* -ODS
25.04.2020 11:07:03 Compacted AgentRunner.nsf, increased by 64K bytes (13%), -C -* -ODS
25.04.2020 11:07:03 Compacting alog4.ntf (Agent Log (8)), -C -* -ODS
25.04.2020 11:07:04 Compacted alog4.ntf, increased by 128K bytes (40%), -C -* -ODS
25.04.2020 11:07:04 Compacting archlg50.ntf (Archive Log (10)), -C -* -ODS
25.04.2020 11:07:05 Compacted archlg50.ntf, 24K bytes recovered (4%), -C -* -ODS
25.04.2020 11:07:05 Informational, LZ1 is enabled in database autcat.ntf.
25.04.2020 11:07:05 Compacting autcat.ntf (AUT-Katalog), -C -* -ODS
25.04.2020 11:07:07 Compacted autcat.ntf, 0K bytes recovered (0%), -C -* -ODS
25.04.2020 11:07:07 Informational, LZ1 is enabled in database autosave.ntf.
25.04.2020 11:07:07 Compacting autosave.ntf (Autosave), -C -* -ODS
25.04.2020 11:07:07 Compacted autosave.ntf, increased by 64K bytes (20%), -C -* -ODS
25.04.2020 11:07:07 Compacting billing.ntf (Billing), -C -* -ODS
25.04.2020 11:07:08 Compacted billing.ntf, 14240K bytes recovered (97%), -C -* -ODS
25.04.2020 11:07:08 Compacting bookmark.ntf (Lesezeichen (11)), -C -* -ODS
```

Abbildung 5.17: Starten von Compact auf Betriebssystemebene

5.3.3. Programme über die Datei notes.ini starten

Der folgende Abschnitt in der Datei `notes.ini` des Servers ist für den Programmstart zuständig:


```
ServerTasks=Replica,Router,Update,AMgr,Adminp,Sched,CalConn,RnRMgr
ServerTasksAt1=Catalog,Design
ServerTasksAt2=UpdAll
ServerTasksAt5=Statlog
```

Die über den Eintrag `ServerTaks` angegebenen Programme werden bereits beim Hochfahren des Servers gestartet. Die Variablen `ServerTasksAt#` startet Programme zu der angegebenen Uhrzeit – ersetzen Sie die Raute durch eine Ziffer zwischen 0 und 23, wobei 0 Mitternacht und 23 natürlich 23 Uhr entspricht.

Eine Liste aller in diesem Buch besprochenen Serverprogramme finden Sie in Anhang B.

5.3.4. Programme über Programmdokumente starten

Es ist wesentlich flexibler, Programme über Programmdokumente zu starten, als über die Datei `notes.ini`:

- > leichter und schneller zu bearbeiten
- > Man kann auf einen Blick erkennen, welche Programme auf welchem Server laufen
- > Mit Platzhalterzeichen kann ein Programm für eine Servergruppe oder sogar auf allen Servern gestartet werden

Programmdokumente erlauben nicht nur das Starten von `Servertasks`, sondern auch von Windows-Stapeldateien (mit der Endung `*.cmd`) entweder nach einem Zeitplan oder beim Hochfahren des Servers. Der Zeitplan umfasst maximal eine Woche, ein einmaliges oder auch mehrmaliges Starten pro Monat ist nicht möglich.

5.3.4.1. Ein Programmdokument erstellen

1. Öffnen Sie den Domino-Administrator.
2. Wählen Sie im Register **Konfiguration** die Ansicht **Server > Programme**.
3. Klicken Sie auf **Programm hinzufügen** oder wählen Sie im Menü **Erstellen > Server > Programm**.
4. Geben Sie den Namen des Programms ein, z. B.: `compact`
5. Geben Sie im Feld **Befehlszeile** zusätzliche Parameter ein, z. B.:
`mail -C -S 15`
6. Geben Sie einen Servernamen ein oder wählen Sie einen Server aus dem Domino-Verzeichnis. Das Feld darf enthalten:
 - einen hierarchischen Servernamen
 - ein Fragezeichen als Platzhalter für ein Zeichen, z. B. `Server??/COB/AT` für `Server01` bis `Server99`
 - einen Stern als Platzhalter für beliebig viele Zeichen, z. B. `*/VIE/COB/AT`
 - nur einen Stern (*) für alle Server
 - eine Servergruppe
 - einen Clusternamen

- Geben Sie eine Startzeit an oder wählen Sie im Feld **Aktiviert/Deaktiviert** »Nur bei Serverstart«, wenn das Programm bereits beim Hochfahren des Servers gestartet werden soll. Soll das Programm mehrmals pro Tag gestartet werden, geben Sie verschiedene Uhrzeiten (durch Semikolons voneinander getrennt) oder einen Zeitraum (z. B. »08:00 - 22:00«) und ein Intervall ein.

Im nachfolgenden Beispiel komprimiert Compact von Montag bis Freitag ab 21:00 alle Maildatenbanken mit der Methode »copy-style« (mithilfe einer Kopie), die mindestens 15% White Space enthalten:

Allgemein		Zeitplan	
Programmname:	compact	Aktiviert/deaktiviert:	Aktiviert
Befehlszeile:	mail -C -S 15	Anfangszeiten:	21:00 jeden Tag
Läuft auf Server:	DOM/COB/AT	Wiederholungsintervall:	0 Minuten
Kommentare:		Wochentage:	Mo, Di, Mi, Do, Fr

Abbildung 5.18: Compact mit Parametern, Erklärung im Text.

5.3.4.2. Starten aller Servertasks über Programmdokumente

Aufgrund der oben dargelegten Vorteile empfehle ich, Programme nicht mehr über die Datei notes.ini, sondern nur noch über Programmdokumente zu starten. Wählen Sie dazu für Programme aus der Zeile ServerTasks im Feld **Aktiviert/Deaktiviert** im Programmdokument die Option »Nur beim Serverstart« (siehe Abbildung 5.19). Wählen Sie für alle anderen Programme die Option »Aktiviert« und die entsprechende Uhrzeit.

Allgemein		Zeitplan	
Programmname:	router	Aktiviert/deaktiviert:	Nur beim Serverstart
Befehlszeile:			
Läuft auf Server:	DOM/COB/AT		
Kommentare:			

Abbildung 5.19: Programmdokument zum Laden eines Programms beim Serverstart

Tipp: Geben Sie für Programme, die auf allen Servern laufen sollen, im Feld **Läuft auf Server** einen Stern (*) ein.

Löschen Sie anschließend die Zeilen ServerTasks und ServerTasksAt# aus der Datei notes.ini.

Tipp: Zu Dokumentationszwecken können Sie Zeilen in der notes.ini auch mit einem Semikolon am Beginn (;) auskommentieren.

Bei der Installation eines Updates werden die Variablen ServerTasks und ServertasksAt# mit Standardwerten neu in die Datei notes.ini geschrieben. Wenn Sie das nicht wollen, nehmen Sie die folgende Zeile in die Datei notes.ini auf:

```
SetupLeaveServerTasks=1
```

5.3.4.3. Serverkonsolenbefehle über Programmdokumente absetzen

Wenn Sie einen beliebigen Serverkonsolenbefehl zu einer bestimmten Zeit an den Domino-Server senden wollen, müssen Sie als **Programmname** »nserver« angeben und in das Feld **Befehlszeile** »-c <Konsolenbefehl>« schreiben:

The screenshot shows the configuration page for a program named 'nserver'. It is divided into two tabs: 'Allgemein' and 'Administration'. The 'Allgemein' tab is active and contains two columns of settings: 'Allgemein' and 'Zeitplan'.

Allgemein		Zeitplan	
Programmname:	<input type="text" value="nserver"/>	Aktiviert/deaktiviert:	<input type="text" value="Aktiviert"/>
Befehlszeile:	<input http="" restart\""="" tell="" type="text" value="-c \"/>	Anfangszeiten:	<input type="text" value="04:00"/> jeden Tag
Läuft auf Server:	<input type="text" value="DOM/COB/AT"/>	Wiederholungsintervall:	<input type="text" value="0"/> Minuten
Kommentare:	<input type="text" value=""/>	Wochentage:	<input type="text" value="So, Mo, Di, Mi, Do, Fr, Sa"/>

Abbildung 5.20: Absetzen eines Serverkonsolenbefehls über ein Programmdokument

Tip: Geben Sie als Befehlszeile `-c "restart server"` ein, können Sie den Domino-Server über ein Programmdokument regelmäßig neu starten.

5.3.4.4. Eine Batch-Datei über ein Programmdokument starten

Um eine Batch-Datei (*.bat oder *.cmd) über ein Programmdokument zu starten, verwenden Sie das Programm `cmd.exe` mit dem Schalter `/c`:

The screenshot shows the configuration page for a program named 'cmd'. It is divided into two tabs: 'Allgemein' and 'Administration'. The 'Allgemein' tab is active and contains two columns of settings: 'Allgemein' and 'Zeitplan'.

Allgemein		Zeitplan	
Programmname:	<input type="text" value="cmd"/>	Aktiviert/deaktiviert:	<input type="text" value="Aktiviert"/>
Befehlszeile:	<input d:\domino\backup.cmd\""="" type="text" value="/c \"/>	Anfangszeiten:	<input type="text" value="23:00"/> jeden Tag
Läuft auf Server:	<input type="text" value="DOM/COB/AT"/>	Wiederholungsintervall:	<input type="text" value="0"/> Minuten
Kommentare:	<input type="text" value=""/>	Wochentage:	<input type="text" value="Sa"/>

Abbildung 5.21: Start einer Windows-Batch-Datei über ein Programmdokument

Tip: Der Befehl `show schedule` zeigt auf der Serverkonsole alle zeitplangesteuerten Ereignisse wie Programmstarts und Replikationen an. Haben Sie mehrere Uhrzeiten oder einen Zeitraum mit einem Intervall eingegeben, sehen Sie in der Liste nur die nächste Ausführungszeit.

5.4. Konfigurationsdokumente

Bei der Serverkonfiguration verfolgt die HCL ein dreistufiges Konzept, wobei die Priorität von oben nach unten zunimmt:

1. Vorgabe-Konfigurationsdokument für alle Server (*)
2. Konfigurationsdokumente für Servergruppen
3. individuelle Konfigurationsdokumente pro Server

Die höchste Priorität haben Einstellungen, die speziell für einen Server gelten (3.), danach folgen Einstellungen für eine Servergruppe (2.) und zuletzt Einstellungen, die im Vorgabedokument gesetzt wurden (1.).

Die Möglichkeit, Server entsprechend ihrer Funktion oder Hardwareausstattung zu Gruppen zuzuordnen, erhöht die Effizienz, da Sie diese in einem Arbeitsgang konfigurieren können.

5.4.1. Eine Vorgabekonfiguration erstellen

Setzen Sie in der Vorgabekonfiguration Einstellungen, die für alle oder zumindest die meisten Server gelten, z. B. die Verwendung des neuesten Dateiformats (ODS).

Da einige Einstellungen (z. B. die Register LDAP und Änderungsmanagement), nur in einem Vorgabe-Konfigurationsdokument zur Verfügung stehen, erstellen Sie auch dann ein Vorgabe-Konfigurationsdokument, wenn Sie nur einen Server in Betrieb haben.

Um ein Vorgabekonfigurationsdokument zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie im Admin-Client zum Register **Konfiguration** und wählen Sie **Server > Konfigurationen**.
2. Klicken Sie auf die Schaltfläche **Konfiguration hinzufügen**.
3. Aktivieren Sie das Kontrollkästchen **Diese Einstellung als Vorgabe für alle Server verwenden**:

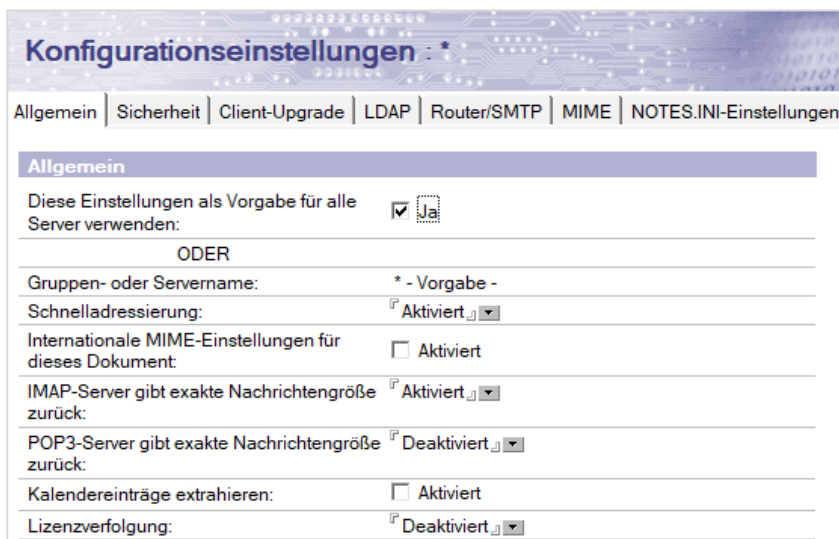


Abbildung 5.22: Das Vorgabe-Konfigurationsdokument

4. Speichern und schließen Sie das Dokument.

Wenn bereits ein Vorgabekonfigurationsdokument existiert, wird das Feld **Diese Einstellungen als Vorgabe für alle Server verwenden** ausgeblendet (siehe Abbildung 5.24).

5.4.2. Gruppenkonfigurationsdokumente erstellen

Gruppenkonfigurationsdokumente werden einer Servergruppe zugeordnet. Hier ein Beispiel:

Gruppe für Serverliste : MailServers	
Allgemein Kommentare Administration	
Allgemein	
Gruppenname:	MailServers
Gruppentyp:	Nur Server
Kategorie:	
Beschreibung:	Alle Mailserver
Maildomäne:	
Internetadresse:	
Methode zum automatischen Füllen:	Keine
Mitglieder:	DOM/COB/AT WS01/COB/AT

Abbildung 5.23: Servergruppe für alle Mailserver

Die Gruppe muss vom Typ »Nur Server« sein und darf auch nur Servernamen enthalten.

Tragen Sie beim Erstellen des Konfigurationsdokuments den Namen der Servergruppe ins Feld **Gruppen- oder Servername** ein:

Konfigurationseinstellungen	
Allgemein Sicherheit Client-Upgrade Router/SMTP MIME NOTES.INI-Einstellungen HCL	
Allgemein	
Gruppen- oder Servername:	MailServers
Schnelladressierung:	Aktiviert
Internationale MIME-Einstellungen für dieses Dokument:	<input type="checkbox"/> Aktiviert
IMAP-Server gibt exakte Nachrichtengröße zurück:	Aktiviert
POP3-Server gibt exakte Nachrichtengröße zurück:	Deaktiviert
Lizenzverfolgung:	Deaktiviert

Abbildung 5.24: Konfigurationsdokument für eine Servergruppe

5.4.3. Individuelle Konfigurationsdokumente erstellen

Individuelle Konfigurationsdokumente enthalten Einstellungen, die nur für einen bestimmten Server gelten. Tragen Sie beim Erstellen des Konfigurationsdokuments den Namen eines Servers ins Feld **Gruppen- oder Servername** ein.

5.5. Datenbankcache und Transaktionsprotokoll

5.5.1. Der Datenbankcache

Der Domino-Server implementiert aus Performancegründen einen Pufferspeicher (Cache) für Notes-Datenbanken. Dieser Cache wird als **NSF-Pufferpool** bezeichnet und vom **Unified Buffer Manager** verwaltet. Dieser implementiert einen Cache auf Dokumentebene, was für die von Domino

verarbeiteten Daten effizienter ist als ein Caching auf Dateisystemebene, wie es die meisten Betriebssysteme tun.

Beim NSF-Pufferpool handelt es sich um einen Read-Through- und Write-Back-Cache.

Read-Through bedeutet, dass wenn ein Benutzer oder Servertask eine Anforderung zum Öffnen eines Dokuments stellt, zuerst überprüft wird, ob das Dokument bereits im Cache vorhanden ist. Falls ja, wird die zwischengespeicherte Kopie aus dem Cache an den Benutzer weitergereicht. Ist es nicht der Fall, wird das Dokument aus der NSF-Datei zuerst in den Cache gelesen, und dann wieder die gecachte Kopie an den Benutzer geliefert. Das heißt, das Dokument wird in jedem Fall aus dem Cache bereitgestellt, ein Benutzer oder Servertask hat nie direkten Zugriff auf die NSF-Datei.

Write-Back bedeutet analog, dass beim Schreiben eines neuen Dokuments oder bei einer Änderung an einem vorhandenen Dokument die neuen Daten nur in den Cache geschrieben werden. Ein separater Hintergrund-Thread schreibt sie dann verzögert aus dem Cache in die NSF-Datei zurück. Diese Methode wird auch als verzögertes Schreiben bezeichnet.

5.5.1.1. Cache-Größe

Wie viele Datenbanken gleichzeitig in den Cache passen, hängt von ihrer Benutzung und von der Größe des Hauptspeichers ab. Der Domino-Server verwendet jedoch nie den ganzen verfügbaren Speicher, sondern setzt sich ein Limit, das auf der folgenden Regel beruht: entweder ein Wert größer 25 oder der Wert der Einstellung `NSF_Buffer_Pool_Size` in der Datei `notes.ini` geteilt durch 300 KB, je nachdem, welche Zahl größer ist.

Wie viele Datenbanken aktuell in den Cache passen, erfahren Sie über den Konsolenbefehl:

```
dbccache show
```

Sie können die Anzahl der maximal im Cache zugelassenen Datenbanken über den folgenden `notes.ini`-Eintrag steuern:

```
NSF_DbCache_Maxentries=<Wert>
```

Die tatsächliche Anzahl der im Cache zugelassenen Datenbanken entspricht dem 1,5-Fachen des angegebenen Wertes. Geben Sie 6000 an, ist die maximale Anzahl also 9000.

Wie können Sie feststellen, ob der Cache zu klein ist?

Die einzige Möglichkeit das festzustellen, besteht darin, die Cache-Statistiken zu überwachen. Ein manuelles Abrufen der Statistiken ist über folgenden Befehl möglich:

```
show statistic database.dbcache.*
```

Da es sich dabei um eine Momentaufnahme handelt, sollten Sie die Statistiken mit dem Statistic Collector mindestens eine Woche sammeln und erst dann auswerten. (Angaben zum Sammeln von Statistiken finden Sie auf Seite 454.)

Hier ein Beispiel von einem Kunden:

```
Database.DbCache.CurrentEntries = 4498
```

```
Database.DbCache.HighWaterMark = 4500
```

```
Database.DbCache.MaxEntries = 3000
```

```
Database.DbCache.OvercrowdingRejections = 15220
```

Die Werte von `CurrentEntries` und `HighWaterMark` sollten immer unter `MaxEntries` und der Wert von `OvercrowdingRejections` immer 0 sein!

Bei diesem Kunden habe ich den Wert dann auf 6000 erhöht:

```
NSF_DbCache_MaxEntries=6000
```

5.5.1.2. Wie Datenbanken aus dem Cache gelöscht werden

Bevor eine Datenbank aus dem Cache gelöscht wird, sorgt ein eigener Thread dafür, dass erforderliche Schreibvorgänge ausgeführt werden und der Arbeitsspeicher freigegeben wird. Dieser Prozess erfolgt spätestens nach 15 bis 20 Minuten. Ist das Maximum überschritten, aber noch nicht höher als das 1,5-Fache des zulässigen Maximums, werden Datenbanken bereits früher aus dem Cache gelöscht. Ist die aktuelle Anzahl der Datenbanken im Cache größer oder gleich dem 1,5-Fachen des zulässigen Maximums, legt Domino keine Datenbanken mehr im Cache ab. In diesem Fall liest Domino die Datenbanken von der Festplatte und nicht aus dem Cache, was langsamer ist.

5.5.1.3. Datenbanken händisch aus dem Cache entfernen

So lange eine Datenbank im Cache liegt, gilt sie als geöffnet und kann von Servertasks, die einen exklusiven Zugriff benötigen (z. B. dem Compactor) nicht bearbeitet werden. Geben Sie folgenden Befehl auf der Serverkonsole ein, um alle Datenbanken aus dem Cache zu entfernen:

```
dbcache flush
```

Sollte danach ein Benutzer oder ein Task auf die Anwendung zugreifen, wird sie sofort wieder in den Cache aufgenommen. Um das zu verhindern, müssen Sie den Cache deaktivieren.

5.5.1.4. Den Datenbankcache deaktivieren

Standardmäßig ist der Datenbankcache auf einem Server aktiviert. Um den Cache kurzfristig zu deaktivieren, geben Sie den folgenden Befehl auf der Serverkonsole ein:

```
dbcache disable
```

Der Datenbankcache bleibt dann bis zum nächsten Serverneustart deaktiviert.

Um den Cache bleibend zu deaktivieren, fügen Sie folgende Zeile zur Datei notes.ini hinzu:

```
NSF_DbCache_Disable=1
```

5.5.2. Die Transaktionsprotokollierung

Aus Performancegründen sollten Sie den Datenbankcache nur in Ausnahmefällen deaktivieren. Andererseits muss bei aktiviertem Cache der Zeitraum zwischen dem Schreiben in den Cache und dem Schreiben in die NSF-Datei aus Gründen der Datenintegrität so kurz wie möglich gehalten werden. Denn so lange die Änderungen nur im Cache, also im flüchtigen Hauptspeicher (RAM) existieren, nicht aber in der NSF-Datei, können bei einem Ausfall Daten verloren gehen und Datenbanken in einen inkonsistenten Zustand gelangen. Und genau das verhindert die **Transaktionsprotokollierung** (Transaction Logging). Ist sie aktiviert, wird jeder Schreibvorgang zweimal ausgeführt, einmal in den NSF-Pufferpool und ein zweites Mal ins **Transaktionsprotokoll**. Sollte es jetzt tatsächlich zu einem Ausfall kommen, können die Daten aufgrund der Informationen im Protokoll wiederhergestellt werden.

Eine **Transaktion** ist eine miteinander verbundene Reihe von Änderungen, die an einer Datenbank auf einem Server vorgenommen werden. So ist beispielsweise das Öffnen eines Dokuments, das Hinzufügen von Text und das Speichern des Dokuments eine Transaktion. In diesem Fall besteht

die Transaktion aus drei separaten impliziten API-Aufrufen: NoteOpen, NoteUpdate und NoteClose.

Aber zuvor habe ich Ihnen doch erklärt, dass das Schreiben auf die Festplatte relativ langsam ist und es zu einem großen Leistungseinbruch führen würde, wenn jeder Domino-Task darauf warten müsste, bis ein Schreibvorgang in eine NSF-Datei abgeschlossen ist. Führt das Schreiben ins Transaktionsprotokoll nicht zu einem ähnlichen Leistungsproblem? Nicht ganz!

In das Transaktionsprotokoll kann mit hoher Performance geschrieben werden, weil Suchvorgänge eliminiert und die Schreibvorgänge vereinfacht werden. Dies wird auf drei Arten erreicht:

- > Jeder Server erstellt ein einziges Transaktionsprotokoll, das die Änderungen aller Datenbanken erfasst, für die die Transaktionsprotokollierung aktiviert ist. Das Transaktionsprotokoll besteht aus einzelnen 64 MB großen Protokolldateien (auch als Extents bezeichnet) mit der Endung *.TXN. Domino schreibt die Daten immer nur in eine einzige TXN-Datei und geht erst zur nächsten weiter, wenn diese voll ist. Die Aufzeichnungen werden unter Verwendung eines herstellereigenen Byte-Stream-Formats gesichert.
- > Jede neue Transaktion wird an die aktive TXN-Datei angehängt. Dies bedeutet, dass in der aktuellen TXN-Datei nicht nach zufälligen Zugriffspositionen gesucht werden muss, jeder Schreibvorgang wird am Ende angefügt.
- > Werden die TXN-Dateien auf einen dedizierten Datenträger geschrieben, müssen Schreibzugriffe nicht mit jenen vom Betriebssystem, der Auslagerungsdatei oder anderen Domino-Servertasks konkurrieren.

Für Sie als Administrator gilt es vor allem, sich um den dritten Punkt zu kümmern. (Hinweise dazu finden Sie in Kap. 4.1.4.2 Empfehlungen Transaktionsprotokoll, ab Seite 33.) Speichern Sie das Transaktionsprotokoll im falschen Medium, etwa in demselben Laufwerk, auf dem auch die Datenbanken gespeichert werden, kann es tatsächlich zu einem Performanceverlust kommen.

5.5.2.1. Transaktionsprotokolle sichern

Zusätzlich zum Aufzeichnen von Datenbankänderungen zum Zweck der Wiederherstellung nach einem Systemabsturz kann das Protokoll auch zur Sicherung (Backup) genutzt werden. Sicherungen von Transaktionsprotokollen sind schneller als vollständige oder differenzielle Datenbanksicherungen und können in kurzen Abständen erstellt werden.

Um Transaktionsprotokolle für Sicherungen nutzen zu können, benötigen Sie ein Backup-Programm eines Fremdanbieters, das die Backup- und Wiederherstellungsmethoden des Domino C API-Toolkits unterstützt. Für eine Wiederherstellung beim Neustart wird hingegen kein Dienstprogramm eines Fremdanbieters benötigt. In diesem Fall wird die Protokollierung fortgesetzt, während Aktualisierungen vorgenommen werden. Wenn der Server abstürzt und anschließend neu gestartet wird, werden alle Aktualisierungen, die anderenfalls verloren gehen würden, in der Datenbank gespeichert. Dies führt zu deutlich weniger Datenverlust und Datenbankbeschädigungen aufgrund von Serverabstürzen und die für den Neustart insgesamt benötigte Zeit wird verkürzt, da eine Konsistenzprüfung der Datenbanken nicht mehr erforderlich ist.

Wenn Sie die Transaktionsprotokollierung aktivieren, weist Domino jeder Notes-Datenbank eine eindeutige Datenbankinstanz-ID (Database Instance ID – DBIID) zu. Zeichnet Domino eine Transaktion im Protokoll auf, so wird diese ID hinzugefügt. Während der Wiederherstellung verwendet Domino die DBIID, um Transaktionen im Protokoll aufzuspüren und mit den Datenbanken abzugleichen.

Bestimmte Datenbankaktivitäten, z. B. das Ausführen von Compact mit Optionen, bewirken, dass Domino die Datenbank so rekonstruiert, dass die Instanz-ID geändert und somit alte Transaktionsprotokoll Daten nicht mehr zuordenbar sind. Von diesem Zeitpunkt an verwenden alle Transaktionen die neue DBIID. Sollten Sie das Transaktionsprotokoll zum Zweck der Sicherung verwenden, müssen Sie nun ein vollständiges Backup der Datenbank erstellen, da sonst die im Protokoll gesammelten Einträge nicht mehr zum Backup passen.

Domino weist in folgenden Fällen eine neue DBIID zu:

- > Die Transaktionsprotokollierung wird erstmalig aktiviert.
- > Der Compact-Task wird mit einer Option ausgeführt, die eine neue Datei erzeugt, z. B. mit dem Schalter -C.
- > Der Fixup-Task wird für beschädigte Datenbanken ausgeführt.
- > Sie verschieben eine Notes-Datenbank auf einen Server, auf dem die Protokollierung aktiviert ist.

5.5.2.2. Protokollierungsarten im Vergleich

Umlaufend (Circular) bietet die beste Performance, ist aber auf 4 GB begrenzt. Wenn das Protokoll voll ist, überschreibt Domino alte Transaktionen, beginnend mit der ältesten, daher ist dieses Modell nicht zur Sicherung geeignet.

Wenn Sie mit Umlaufend nicht auskommen, verwenden Sie **Linear**. Die lineare Protokollierung ähnelt der umlaufenden, gestattet jedoch mehr als 4 GB. (Bedenken Sie beim Berechnen des Platzbedarfs, dass wirklich alles ins Protokoll rein muss, auch Anhänge!)

Bei **Archivierend** (Archived) wird das Protokoll nach Bedarf erweitert. In diesem Modus werden die Protokolldateien nie überschrieben, das heißt, das Protokoll wächst unaufhörlich, und Sie benötigen ein Backup-Dienstprogramm, um das Protokoll nach der Sicherung abzuschneiden und somit klein zu halten. Wenn Sie kein Backup-Dienstprogramm einsetzen, läuft das Speichermedium irgendwann voll und der Server bleibt stehen. Daher verwenden Sie diesen Modus ausschließlich, wenn Sie Transaktionsprotokolle sichern müssen.

5.5.2.3. Leistung zur Laufzeit bzw. zum Neustart festlegen

Die Einstellung »Vorrang für Laufzeit« liefert die beste Performance.

Bei »Vorrang für Wiederherstellung bei Neustart« startet der Server nach einem Absturz am schnellsten – gut etwa für Entwicklungs- oder Hubserver.

»Standard« – ist ein Kompromiss und daher nicht die effizienteste Methode.

5.5.2.4. Wo Sie Transaktionsprotokolle speichern

Transaktionsprotokolle müssen schnell geschrieben werden, sie haben also aus Performancegründen auf einem (langsamen) RAID 5 oder 10 oder auf einem NAS (Network Attached Storage) nichts zu suchen. Wenn Sie nicht vorhaben, die Transaktionsprotokolle für das Backup zu verwenden, ist alles, was Sie brauchen, ein Paar 4-GB-SSDs mit Spiegelung (RAID 1) und einem dedizierten Controller. Wenn Sie nur umlaufende Transaktionsprotokolle verwenden (siehe Seite 101), könnten Sie sogar riskieren, auf die Spiegelung zu verzichten.

Sollten Sie das nicht bereitstellen können, etwa in einer virtualisierten Umgebung oder wenn nur ein Plattensatz mit RAID 1 für alles verfügbar ist, würde ich aufgrund der Vorteile der höheren Datenintegrität und des wesentlich schnelleren Serverstarts trotzdem ein Transaktionsprotokoll einrichten – dann muss es sich den Platz eben mit Betriebssystem, Auslagerungsdatei und Programmverzeichnis teilen. Auf die separate Speicherung der Daten in einem RAID 5 / 10 oder bei Virtualisierung in einer eigenen VDisk würde ich jedoch bestehen.

5.5.2.5. Ein umlaufendes Transaktionsprotokoll einrichten

Wenn der Domino-Server eine andere Festplattenblockgröße als 512 Byte verwendet (was sehr wahrscheinlich ist), stellen Sie sicher, dass Sie das Transaktionsprotokoll im neueren, mit Version 8.5.3 eingeführten Format erstellen:

1. Öffnen Sie dazu das Vorgabekonfigurationsdokument (oder das spezifische Konfigurationsdokument des Servers) und fügen Sie auf dem Register **NOTES.INI-Einstellungen** den Parameter `Create_R85_Log=1` zur Liste hinzu.

Alternativ können Sie die Zeile `Create_R85_Log=1` auch direkt in die Datei `notes.ini` des Servers schreiben. Beachten Sie, dass der Server dann neu gestartet werden muss.

2. Öffnen Sie nun das Serverdokument im Bearbeitungsmodus und wechseln Sie zum Register **Transaktionsprotokollierung**.
3. Aktivieren Sie die Transaktionsprotokollierung. Sie erhalten die folgende Meldung:

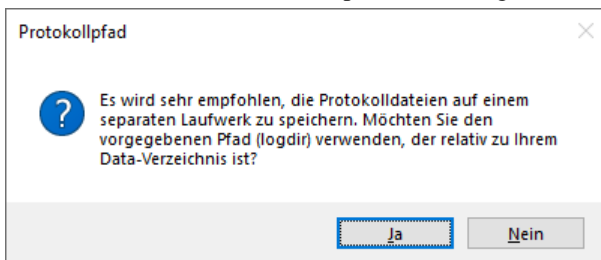


Abbildung 5.25: Bestätigung des Protokollpfades im Datenverzeichnis

4. Ändern Sie den Pfad nach Ihren Möglichkeiten (siehe Kap. 5.5.2.4).
5. Wählen Sie die Protokollierungsart »Umlaufend«.

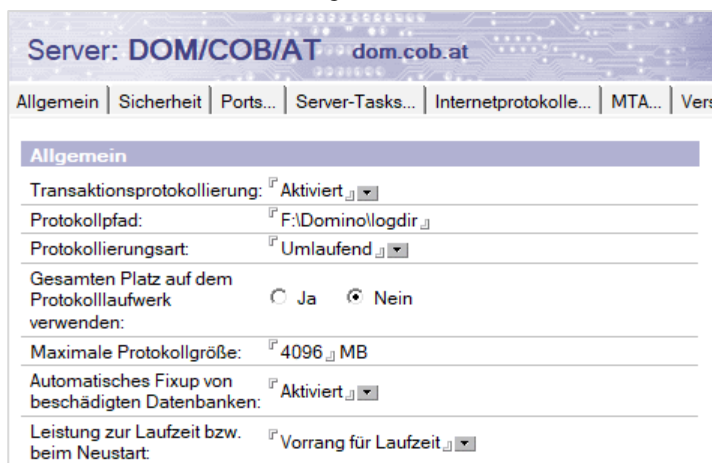


Abbildung 5.26: Serverdokument, Register Transaktionsprotokollierung

6. Wählen Sie im Feld **Gesamten Platz auf dem Protokolllaufwerk verwenden** den Wert »Nein« und geben Sie für die Protokollierungsart Umlaufend die Zahl »4096« ein. Das ist der höchste mögliche und zugleich einzig sinnvolle Wert.
7. Aktivieren Sie das automatische Fixup von beschädigten Datenbanken.
8. Wählen Sie bei **Leistung zur Laufzeit bzw. beim Neustart** den Wert »Vorrang für Laufzeit«.
9. Speichern und schließen Sie das Serverdokument.
10. Starten Sie den Server neu. Das Transaktionsprotokoll wird beim Neustart in voller Größe erstellt. Anschließend weist der Server jeder Datenbank, auf die er zugreift, eine neue DBIID zu.

Tipp: Wenn Sie die Zuweisung beschleunigen wollen, etwa weil Sie eine vollständige Datenbanksicherung durchführen wollen, aktualisieren Sie den Datenbankkatalog mit dem Befehl:
`load catalog`

5.5.2.6. Datenbanken aus dem Transaktionsprotokoll ausschließen

Nach dem Einrichten der Transaktionsprotokollierung auf Ihrem Server loggt Domino alle Datenbanken in einem einzigen Protokoll. Sie können aus Performancegründen die Protokollierung für einzelne Datenbanken abschalten. Wenn unprotokollierte Datenbanken korrupt werden, muss jedoch Fixup angewendet werden, wobei Daten verloren gehen können. Infrage kommt das Abschalten daher nur bei Datenbanken, die zwar häufige Schreibvorgänge aufweisen, jedoch jederzeit neu erstellt werden können. Dazu gehört neben den Mailboxen etwa auch das Serverprotokoll. (Bei aktiviertem DAOS ist es von der Performance besser, die Mailboxen für den DAOS zu aktivieren.)

Die Transaktionsprotokollierung muss aktiviert bleiben, wenn Sie in einer Datenbank den Domino Attachment und Object Service (DAOS) nutzen wollen, um Anhänge dedupliziert im Dateisystem zu speichern.

Sie können die Transaktionsprotokollierung in den Datenbankeigenschaften auf dem Register **Erweitert** (Propellerhut) abschalten:

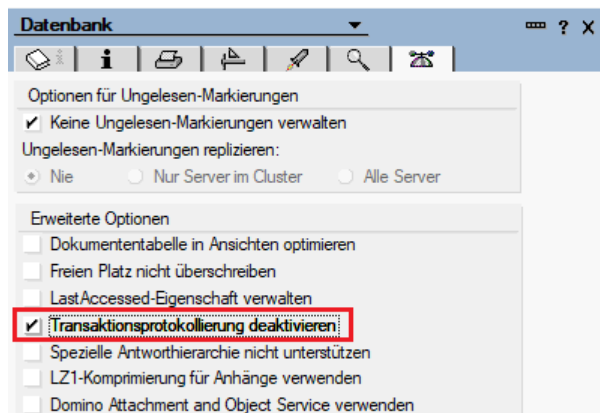


Abbildung 5.27: Datenbankeigenschaft Transaktionsprotokollierung deaktivieren

Wie bei allen erweiterten Datenbankeigenschaften muss die Datenbank danach komprimiert werden. Setzen Sie die Eigenschaft gleich daher gleich über `load compact -t` (Kleinbuchstabe!).

Die Transaktionsprotokollierung kann mit `load compact -T` (Großbuchstabe!) wieder aktiviert werden.

5.5.2.7. Ansichten protokollieren

Die Ansichtsprotokollierung (View Logging) hält Ansichten nach einem Serverabsturz konsistent. Die Ansichtsprotokollierung aktivieren Sie im Domino-Designer in den Eigenschaften der Ansicht:

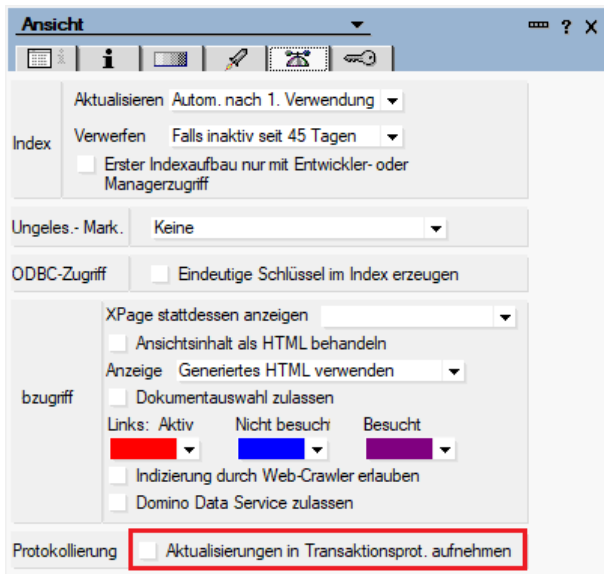


Abbildung 5.28: Ansichtseinstellung Aktualisierungen in Transaktionsprot. aufnehmen

Wenn die Eigenschaft **Aktualisierungen in Transaktionsprot. aufnehmen** im Register **Erweitert** (Propellerhut) aktiviert ist, benötigen Ansichten beim Serverneustart keine Aktualisierung, weil die Indexinformationen aus dem Transaktionsprotokoll wiederhergestellt werden können.

Tipp: Wenn Sie die Ansichtsprotokollierung bereits in der Schablone setzen, werden die Änderungen in alle damit erstellten Datenbanken übernommen.

5.6. Die verschiedenen Domino-Administratoren

Domino kennt mehrere Arten von Administratoren, die Sie im Serverdokument, Register **Sicherheit**, zuordnen können:

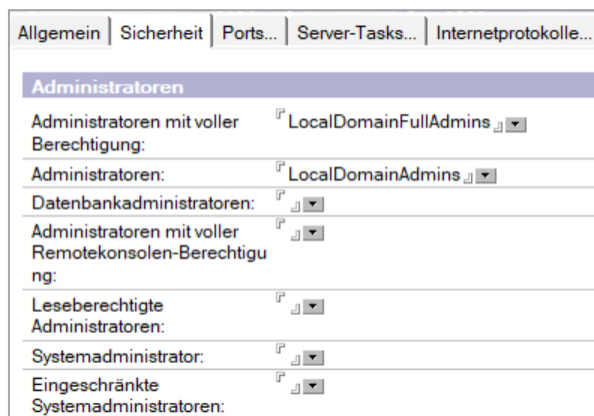


Abbildung 5.29: Die verschiedenen Administratoren im Serverdokument

5.6.1. Administratoren

Benutzer und Gruppen, die im Feld **Administratoren** stehen, dürfen:

- > die Entfernte Konsole verwenden und darauf alle Befehle absetzen
- > Datenbanken, Repliken und Schablonen erstellen
- > Datenbanken löschen
- > Datenbanken komprimieren (siehe Seite 252)
- > Volltextindizes erstellen, aktualisieren und löschen (siehe Seite 266)
- > bestimmte Datenbankeigenschaften setzen (z. B. Größenbeschränkungen)
- > Nachrichten verfolgen
- > die Zugriffskontrollliste einer Datenbank nur ändern, wenn sie dort als Manager eingetragen sind

Personen und Gruppen im Feld **Administratoren** verfügen bereits über alle Administrationsrechte. Die nachfolgenden Felder ordnen zusätzlichen Personen eine Teilmenge dieser Rechte zu, dienen also zur Delegation einzelner Aufgaben. Sie müssen also jemanden, der bereits Administrator ist, nicht auch noch die Rolle Datenbankadministrator geben.

Hier die Rechte der »Delegierungsadmins« im Einzelnen:

5.6.2. Datenbankadministratoren

Im Feld **Datenbankadministratoren** aufgelistete Benutzer oder Gruppen dürfen:

- > Ordner und Datenbanklinks erstellen, aktualisieren und löschen
- > Verzeichnislinks und -ACLs erstellen, aktualisieren und löschen
- > Datenbanken komprimieren und löschen
- > Volltextindizes erstellen, aktualisieren und löschen
- > Datenbanken, Repliken und Schablonen erstellen
- > bestimmte Datenbankeigenschaften ändern (z. B. Größenbeschränkungen)

Beachten Sie, dass Datenbankadministratoren keine Managerrechte erhalten, die oben aufgelisteten Aufgaben jedoch auch erledigen können, wenn sie auf eine Datenbank keinen Zugriff haben.

5.6.3. Administratoren mit voller Remote-Konsolen-Berechtigung

Benutzer oder Gruppen im Feld Administratoren mit voller Remote-Konsolen-Berechtigung dürfen auf der Entfernten Konsole im Domino-Administrator alle Arten von Befehlen absetzen.

5.6.4. Leseberechtigte Administratoren

Benutzer oder Gruppen im Feld Leseberechtigte Administratoren dürfen auf der Entfernten Konsole im Domino-Administrator nur Befehle absetzen, die einen Status abfragen, wie etwa `show tasks` oder `show server`. Befehle, die den Betrieb oder die Konfiguration ändern, dürfen nicht abgesetzt werden.

5.6.5. Systemadministratoren

Benutzer oder Gruppen im Feld **Systemadministratoren** können auf der Serverkonsole Betriebssystembefehle absetzen. (Das geht nur, wenn der Server über einen Serverkontroller gestartet wurde.)

5.6.6. Eingeschränkte Systemadministratoren

Benutzer oder Gruppen im Feld **Eingeschränkte Systemadministratoren** können auf der Serverkonsole nur jene Betriebssystembefehle absetzen, die im Feld **Beschränkte Systembefehle** angegeben wurden. (Das geht nur, wenn der Server über einen Serverkontroller gestartet wurde.)

5.6.7. Sonderfall Administratoren mit voller Berechtigung

Ein Spezialfall sind Administratoren mit voller Berechtigung (Full Access Administrators). Sie dürfen alles, was normale Administratoren dürfen, und zusätzlich:

- > Datenbanken öffnen und verwalten, selbst wenn sie in der ACL unter »Kein Zugriff« fallen
- > Dokumente mit Leserfeldern (siehe Kap. 13.10 Gestaltungssicherheit, ab Seite 366) sehen, selbst wenn sie nicht in den Leserfeldern stehen
- > Agenten erstellen, die mit vollen Administrationsrechten laufen

Achtung: Administratoren mit voller Berechtigung können keine verschlüsselten Datenbanken oder Dokumente lesen, wenn sie nicht über den passenden Schlüssel verfügen!

Beachten Sie, dass die Administration mit voller Berechtigung nicht automatisch zur Verfügung steht, sondern im Domino-Administrator erst angefordert werden muss. Wählen Sie dazu im Hauptmenü **Administration > Administration mit voller Berechtigung**:

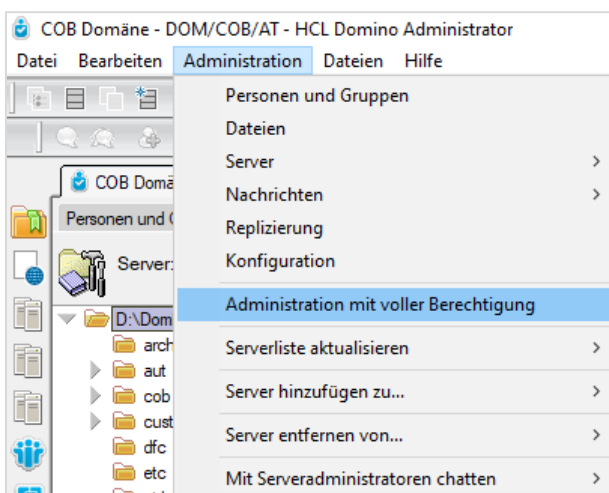


Abbildung 5.30: Administration mit voller Berechtigung aktivieren

Sollten Sie im Serverdokument nicht über uneingeschränkte Administratorrechte verfügen, erhalten Sie die Meldung:

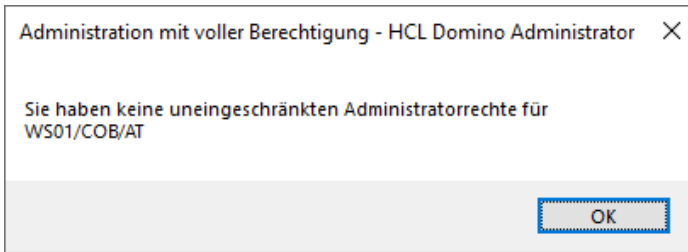


Abbildung 5.31: Meldung beim Fehlen von vollen Administrationsrechten

Die Zuweisung des Rechts bleibt so lange aufrecht, bis Sie das Häkchen wieder entfernen oder den Domino-Administrator schließen.

Solange der Domino-Administrator geöffnet ist, können Sie auch im Notes-Client und Domino-Designer mit vollen Administrationsrechten arbeiten.

Damit ein Mindestmaß an Nachvollziehbarkeit gegeben ist, wird die Anforderung im Serverprotokoll geloggt:

```
04.04.2020 17:26:08 Otto Huber/COB/AT was granted full administrator access.
```

5.6.7.1. Administration mit voller Berechtigung deaktivieren

Sollten Sie das Feature Administration mit voller Berechtigung deaktivieren wollen, tragen Sie in der Datei notes.ini die folgende Zeile ein:

```
SECURE_DISABLE_FULLADMIN = 1
```

Dieser Parameter kann nicht über die Serverkonsole, die Entfernte Konsole oder das Konfigurationsdokument des Servers gesetzt werden, sondern ausschließlich von einer Person mit physischem Zugriff auf die notes.ini im Dateisystem des Servers.

5.6.7.2. Strategien zur Vergabe von uneingeschränkten Adminrechten

Zur Nutzung dieses Features ergeben sich verschiedene Strategien:

1. Sie erstellen einen eigenen Benutzer, etwa `Full Admin/COB/AT`, und nehmen nur ihn in das Feld auf. In diesem Fall muss jeder, der uneingeschränkte Administrationsrechte braucht, zuerst zu dieser ID wechseln. Sie könnten die Sicherheit weiter verschärfen, indem Sie für die ID mehrere Kennwörter vergeben, die nur verschiedenen Personen bekannt sind.
Nachteil der Methode ist eindeutig, dass längerfristig gesehen nicht nachvollziehbar ist, wer das Feature verwendet hat.
2. Sie lassen das Feld Administration mit voller Berechtigung leer und fügen nur bei Bedarf den Namen eines vertrauenswürdigen Administrators ein. Nachdem das Problem behoben wurde, entfernen Sie den Namen wieder.
3. Sie fügen eine eigene Gruppe in das Feld Administration mit voller Berechtigung ein, etwa `LocalDomainFullAdmins`. In diese Gruppe nehmen Sie nur besonders vertrauenswürdige Administratoren auf.
4. Sie nehmen die übliche Admin-Gruppe (etwa `LocalDomainAdmins`) auch in das Feld Administration mit voller Berechtigung auf.

Tipp: Sie können das Verwenden dieses Features auch nachverfolgen, indem Sie sich jedes Mal eine Mail schicken lassen, wenn jemand die Administration mit uneingeschränkten Rechten anfordert: Konfigurieren Sie dazu in der Datenbank events4.nsf einen entsprechenden Event Handler (siehe Kap. 17.4.2 Einen Eventhandler für eine bestimmte Meldung einrichten, ab Seite 459).

5.7. Der Administrationsprozess

Der Servertask **Administrationsprozess** (Administration Process, AdminP) automatisiert mehr als 180 verschiedene Administrationsaufgaben. Dazu gehören unter anderem:

Benutzer verwalten

- > Den Namen eines Benutzers ändern
- > Benutzer neu zulassen
- > Benutzer innerhalb der Namenshierarchie verschieben
- > Benutzer und ihre Mail-Datenbanken löschen

Gruppen verwalten

- > Gruppen umbenennen
- > Gruppen löschen

Server verwalten

- > Server neu zulassen
- > Server löschen
- > Server zu einem Cluster hinzufügen oder aus einem Cluster entfernen

Datenbanken verwalten

- > Repliken mehrerer Datenbanken erstellen
- > Mail-Datenbanken erstellen
- > Leser- und Autorenfelder in Dokumenten ändern
- > Datenbanken innerhalb eines Clusters verschieben
- > Zugriffskontrolllisten bei Namensänderungen aktualisieren

Das Domino-Verzeichnis verwalten

- > Gruppen bei Namensänderungen aktualisieren
- > Ressourcen zum Adressbuch hinzufügen oder daraus löschen
- > Kennwortüberprüfung aktivieren

Unterstützung von Benutzern ohne Managerzugriff

- > Den Abwesenheitsagenten aktivieren
- > Mail- und Kalenderdelegation

Der Administrationsprozess wird per Vorgabe über die Zeile `ServerTasks` in der Datei `notes.ini` bereits beim Hochfahren des Servers gestartet und wartet auf Aufträge. Diese Aufträge werden in den meisten Fällen von einem Administrator über Befehle im Admin-Client gestellt, manche Anforderungen stammen jedoch auch von Endanwendern.

Jede Administrationsanforderung bedingt einen Eintrag in der Datenbank für Administrationsanforderungen (admin4.nsf). Den Zeitpunkt der Abarbeitung einer Anforderung bestimmt der zugeordnete Planungstyp, z. B. sofort oder einmal pro Stunde. Bei komplexeren Aufgaben (wie z. B. dem Umbenennen oder Löschen eines Benutzers) werden die Anforderungen in einzelne Schritte zerlegt, denen unterschiedliche Planungstypen zugeordnet sein können. Hier bedingt meist die Abarbeitung eines Schrittes den nächsten, in einzelnen Fällen ist auch ein Anmelden eines Benutzers oder die Bestätigung durch einen Administrator nötig.

5.7.1. Die Datenbank für Administrationsanforderungen

Der Administrationsprozess durchsucht in regelmäßigen Abständen die Datenbank »Administrationsanforderungen« (Administration Requests, admin4.nsf) nach neuen Anforderungen. Haben Sie mehrere Server, müssen Sie sicherstellen, dass diese Datenbank mit hoher Frequenz zwischen den einzelnen Servern repliziert wird. (Zum Aufsetzen der Replizierung lesen Sie Kap. 10.4 Eine automatische Replizierung einrichten, ab Seite 301.)

Die Datenbank admin4.nsf wird beim ersten Start jedes Servers automatisch erstellt. Damit eine Replikation gewährleistet ist, verwendet sie die Replik-ID des Domino-Verzeichnisses und tauscht eine Ziffer aus. (Lautet die Replik-ID des Domino-Verzeichnisses etwa C1278340:0073E9DF, so wird daraus C1278340:0373E9DF.)

Die Datenbank für Administrationsanforderungen enthält zwei Arten von Dokumenten: Die eigentlichen Anforderungsdokumente mit Angabe des zuständigen Servers und die dazugehörigen Protokolldokumente, über die der Administrationsprozess den aktuellen Status anzeigt (Datum und Uhrzeit der Verarbeitung, ausführender Server und Ergebnis). In den Protokolldokumenten kann das Ausführen eines Schritts durch Aktivieren des Feldes **Anforderung erneut durchführen?** wiederholt werden – etwa, wenn ein Fehler aufgetreten ist oder eine bestimmte Datenbank bei der letzten Ausführung keinen Administrationsserver zugewiesen hatte.

In den Anforderungsdokumenten stehen auch die Zuständigkeiten (Feld **Server, der/die die Aktion durchführen soll(en)**). Mögliche Zuständigkeiten sind:

- > Administrationsserver für das Domino-Verzeichnis
- > Alle Server (*)
- > Ein bestimmter Servername (meist der Mailserver)

Ist ein Server nicht zuständig, ignoriert der Administrationsprozess die Anforderung. Daher ist es wichtig, dass Anforderungen zum zuständigen Server repliziert werden.

5.7.2. Administrationsserver

Die Zuordnung der einzelnen Datenbanken zu Administrationsservern kontrolliert die Aufgabenverteilung; nur der Administrationsprozess des in der Zugriffskontrollliste eingetragenen Servers arbeitet anstehende Anforderungen ab. Damit werden ein mehrfaches Abarbeiten und damit Replizierkonflikte verhindert. Ist für eine Datenbank kein Administrationsserver eingetragen, wird sie vom Administrationsprozess auch nicht gewartet.

Eine besondere Rolle spielt der **Administrationsserver des Domino-Verzeichnisses**, der viele Aufgaben, wie etwa das Umbenennen von Benutzern, initiiert. Haben Sie mehrere Domino-Server im Einsatz, ist darauf zu achten, dass nicht nur das Domino-Verzeichnis, sondern auch die Datenbank für Administrationsanforderungen regelmäßig zwischen allen Servern abgeglichen wird.

Per Vorgabe wird der erste Server in der Domäne als Administrationsserver des Domino-Verzeichnisses festgelegt. Wollen Sie einen anderen Administrationsserver verwenden, ändern Sie den Namen in der Zugriffskontrollliste im Register **Erweitert**. Die richtige Einstellung für das Feld **Aktion** lautet »Namensfelder nicht ändern«:

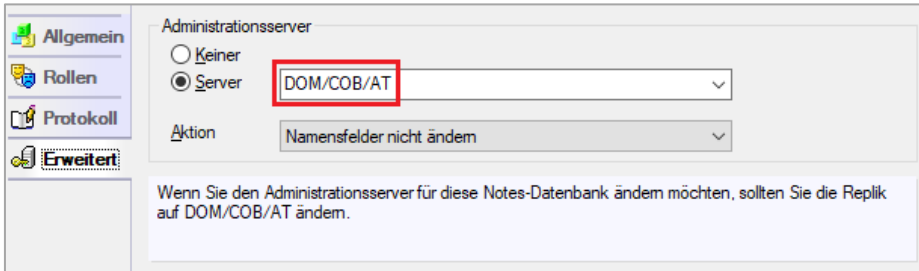


Abbildung 5.32: Zugriffskontrollliste, Register Erweitert – Administrationsserver auswählen

In der Zugriffskontrollliste der Datenbank admin4.nsf sollte derselbe Server eingetragen sein wie im Domino-Verzeichnis und ebenfalls die **Aktion** »Namensfelder nicht ändern«.

5.7.3. Planungstypen

Stellt der Administrator dem Administrationsprozess eine Aufgabe (etwa das Umbenennen einer Person), so wird diese in einzelne Schritte zerlegt und jedem Schritt ein eigener **Planungstyp** (Schedule Type) zugeordnet, der den Zeitpunkt der Ausführung bestimmt.

Die folgenden Planungstypen stehen zur Verfügung:






Symbol	Planungstyp (Schedule Type)	Vorgabe für Ausführung	Beschreibung
	Sofort (immediate)	jede Minute	Anforderungen werden innerhalb von einer Minute nach dem Erstellen verarbeitet. Das Intervall kann nicht geändert werden.
	Intervall (interval)	stündlich	Anforderungen werden per Vorgabe einmal stündlich verarbeitet. Das Intervall kann im Serverdokument geändert werden.
	Täglich (daily)	Täglich 24:00	Anforderungen werden per Vorgabe täglich um 24 Uhr verarbeitet. Die Zeit kann im Serverdokument geändert werden.
	Verzögert (delayed)	Sonntag 24:00	Anforderungen werden per Vorgabe am Sonntag um 24 Uhr verarbeitet. Tag und Zeit können im Serverdokument geändert werden.
	Bestätigung erforderlich		Anforderungen müssen vom Administrator bestätigt werden.

Tabelle 5.2: Die verschiedenen Planungstypen

Zum sofortigen Abarbeiten von Anforderungen stehen je nach Planungstyp die folgenden Konsolenbefehle zur Verfügung:

Befehl	Ergebnis
<code>tell adminp process all</code>	Verarbeitet alle neuen und geänderten unmittelbaren, täglichen, verzögerten und Intervall-Anforderungen.

Befehl	Ergebnis
	Wartet nicht, bis alle Anforderungen beendet sind. Dieser Befehl ist zu vermeiden, weil die einzelnen Schritte dann ev. nicht in der richtigen Reihenfolge ausgeführt werden.
<code>tell adminp process restart</code>	Verarbeitet und aktualisiert Anforderungen von jedem Zeitplantyp, so weit erforderlich, durch Simulation eines Neustarts des Administrationsprozesses. Wie der Befehl <code>process all</code> , wartet aber darauf, bis alle Anforderungen beendet sind, und baut die Warteschlangen neu auf.
<code>tell adminp process new</code>	Verarbeitet alle neuen Anforderungen vom Typ sofort oder Intervall.
<code>tell adminp process immediate</code>	Verarbeitet alle neuen Anforderungen vom Typ sofort.
<code>tell adminp process interval</code>	Verarbeitet alle sofortigen Anforderungen und alle Anforderungen, die normalerweise entsprechend der Einstellung »Intervall« verarbeitet werden.
<code>tell adminp process daily</code>	Verarbeitet alle neuen Anforderungen vom Typ täglich.
<code>tell adminp process delayed</code>	Verarbeitet alle neuen und geänderten verzögerten Anforderungen.
<code>tell adminp process people</code>	Verarbeitet alle neuen und geänderten Anforderungen zum Aktualisieren von Personendokumenten im Domino-Verzeichnis.
<code>tell adminp process time</code>	Verarbeitet alle neuen und geänderten Anforderungen zum Löschen von nicht verlinkten Maildateien.
<code>tell adminp show databases</code>	Zeigt alle Datenbanken an, für die der ausgewählte Server als Administrationsserver zugewiesen ist.
<code>tell adminp quit</code>	Beendet den Administrationsprozess.

Tabelle 5.3: Konsolenbefehle zum Abarbeiten von Administrationsanforderungen

5.7.4. Das Zertifizierungsprotokoll

Auf dem Server, auf dem Sie Umbenennungen oder Rezertifizierungen initialisieren, muss eine Replik des Zertifizierungsprotokolls (Certification Log, `certlog.nsf`) liegen. Das Zertifizierungsprotokoll wird beim Konfigurieren des ersten Servers automatisch erstellt und muss vom Administrator händisch auf andere Server repliziert werden.

5.7.5. Den Administrationsprozess einrichten

Zum Einrichten des Administrationsprozesses halten Sie sich an folgende Vorgangsweise:

- > Optional: Setzen Sie im Serverdokument Vorgaben für die Abarbeitung von Anforderungen und starten Sie den Administrationsprozess neu:

```
restart task adminp
```

- > Optional: Ändern Sie bei Bedarf den Administrationsserver für das Domino-Verzeichnis.
- > Optional: Haben Sie den Administrationsserver für das Domino-Verzeichnis geändert, ändern Sie auch den Administrationsserver in der Datenbank für Administrationsanforderungen.
- > Richten Sie die Replikation von names.nsf und admin4.nsf zwischen allen Servern ein. (Zum Einrichten einer zeitplangesteuerten Replikation lesen Sie Kap. 10.4 Eine automatische Replikation einrichten, ab Seite 301.)
- > Tragen Sie in den Zugriffskontrolllisten aller anderen Datenbanken einen Administrationsserver ein. Passen Sie außerdem bei Bedarf die Rechte an.

5.7.5.1. Vorgaben anpassen

Die Vorgabewerte sind zumindest für kleine Unternehmen mit wenigen Servern viel zu weit gesetzt, weshalb ich empfehle, sie anzupassen. Die Anpassung erfolgt im Serverdokument, auf dem Register **Server-Tasks... > Administrationsprozess**.

Hier können Sie die folgenden Parameter ändern:

Maximale Anzahl von Threads

Vorgabe sind 3, maximal möglich 10. Ein Thread wird zur Abwicklung der Anforderungen verwendet, die übrigen zum Abarbeiten. Sie können die Anzahl der Threads bereits bei bloßem Verdacht gefahrlos erhöhen, da sie erst bei Bedarf aktiviert werden.

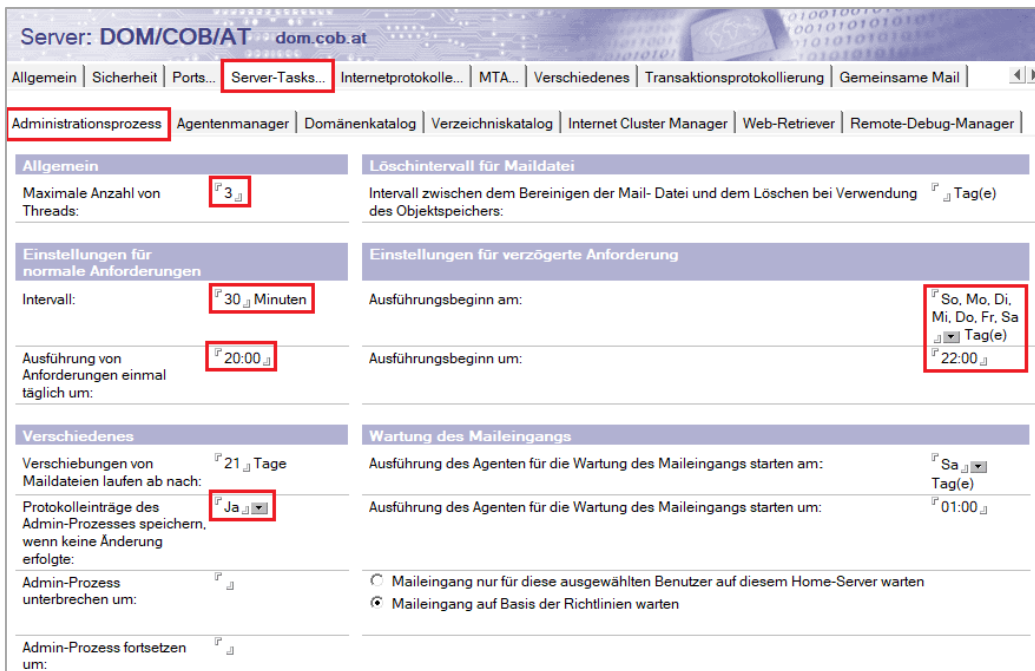


Abbildung 5.33: Serverdokument > Server-Tasks... > Administrationsprozess

Intervall

Wenn leer (Vorgabe) sind es 60 Minuten. Das Intervall kann problemlos verkürzt werden (auf dem Administrationsserver auf bis zu 15 Minuten, sonst nicht unter 30 Minuten). Bei Verkürzung muss auch das Replikationsintervall verkürzt werden!

Ausführung von Anforderungen einmal täglich um

Vorgabe für Anforderungen, die einmal täglich abgearbeitet werden, ist Mitternacht. Sie können die Ausführungszeit vorverlegen, da einige Anforderungen sehr prozessorintensiv sind, sollten Sie jedoch außerhalb der Arbeitszeiten bleiben.

Einstellungen für verzögerte Anforderung

Vorgabe für Anforderungen, die verzögert abgearbeitet werden, ist Sonntag um Mitternacht, damit auch in großen Umgebungen genügend Zeit zum Ausreplizieren bleibt. In kleineren Umgebungen mit wenigen Servern können verzögerte Anforderungen auch jeden Tag ausgeführt werden, womit Sie die Dauer vieler Administrationsanforderungen drastisch beschleunigen.

Protokolleinträge des Admin-Prozesses speichern, wenn keine Änderung erfolgte

Hier steuern Sie, ob der Administrationsprozess auch Protokolleinträge erstellen soll, wenn es nichts zu tun gab. Ich bevorzuge die Option »Ja«, weil man nur dann sehen kann, welcher Server die Anforderung bereits abgearbeitet hat und wann die Aufgabe fertig ist.

Dadurch entstehen jedoch auch wesentlich mehr Dokumente, was zumindest in einer großen Umgebung mit vielen Benutzern zu einer Vergrößerung der Datenbank um etwa 20 % führt.

Wahrscheinlich ist für Sie der geringe Größenunterschied ohnehin kein Thema und wenn doch, können Sie zumindest die Verweildauer der Dokumente in der Datenbank verkürzen. Öffnen Sie dazu die Datenbank admin4.nsf und wählen Sie im Hauptmenü den Befehl **Datei > Replizierung > Optionen für diese Anwendung...** Wechseln Sie im angezeigten Dialog **Replizierungsoptionen** zum Register **Platzsparer** und geben Sie im Feld **Dokumente entfernen, die seit (n Tagen) nicht geändert wurden** die Anzahl Tage ein, nach der die Dokumente gelöscht werden sollen:

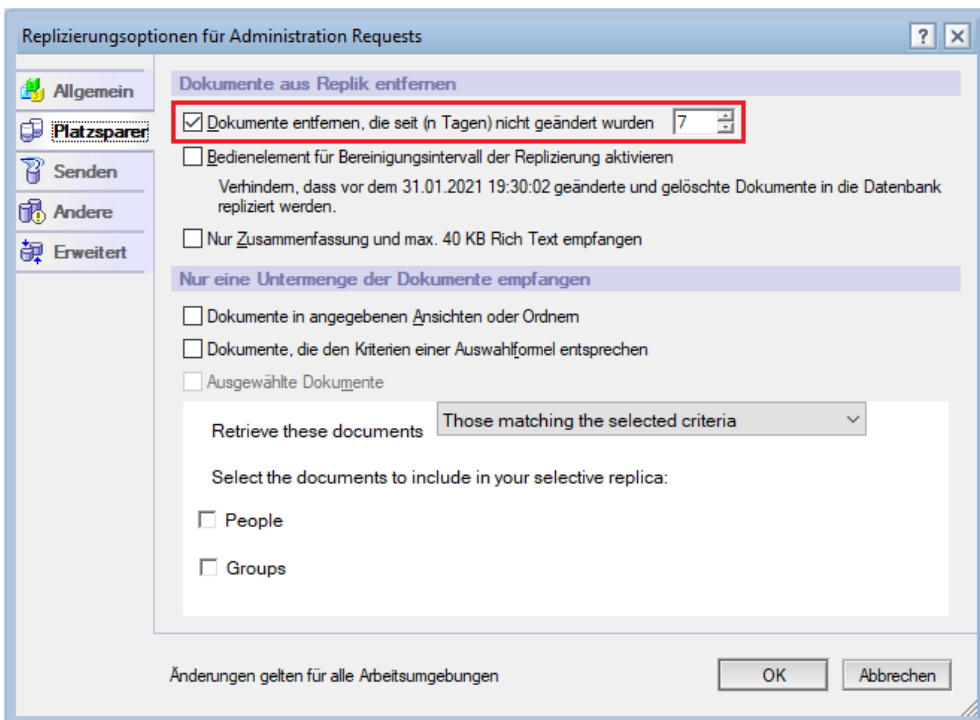


Abbildung 5.34: Replizeroptionen der Datenbank admin4.nsf

5.7.5.2. Administrationsserver in allen Datenbanken setzen

Achten Sie darauf, dass jede Datenbank in der Zugriffskontrollliste, Register **Erweitert**, einen Administrationsserver eingetragen hat. Überprüfen Sie, ob auf dem ausgewählten Server auch wirklich eine Replik der Datenbank existiert und diese Replik mit Repliken auf anderen Servern regelmäßig abgeglichen wird.

Um zu überprüfen, welche Datenbanken ein Administrationsprozess zugeordnet hat, können Sie auf der Serverkonsole den folgenden Befehl eingeben:

```
tell adminp show databases
```

Der Server zählt dann alle Datenbanken auf, bei denen er als Admin-Server eingetragen ist.

Wie bereits erwähnt, lautet die richtige Einstellung für das Feld **Aktion** in der Zugriffskontrollliste für das Domino-Verzeichnis »Namensfelder nicht ändern«. Welche Aktion Sie bei anderen Datenbanken auswählen, hängt von ihrer Datenstruktur ab. Sind etwa Autorenfelder vorhanden, können Autoren nach einer Umbenennung das Bearbeitungsrecht an Dokumenten verlieren; entsprechend sollten Sie hier die Aktion »Alle Leser- und Autorenfelder ändern« auswählen. Sollen auch Namensfelder richtiggestellt werden, dann wählen Sie die Aktion »Alle Namensfelder ändern« aus.

Achtung beim Löschen durch den Administrationsprozess. Wenn Sie die Aktion »Alle Namensfelder ändern« ausgewählt haben, werden die Benutzernamen aus allen Namens-, Leser- und Autorenfeldern entfernt, was zu unschönen und auch problematischen Effekten führen kann. Nicht nur, dass es komisch aussieht, wenn in einem Dokument im Feld »Genehmigt von« niemand mehr steht, das Löschen von Namen aus einem Leserfeld kann auch den Dokumentzugriff verändern. Wenn der gelöschte Benutzer etwa der einzige Eintrag war und das Leserfeld jetzt leer ist, sehen das Dokument wieder alle Leser und höher.

Leider wird die eingestellte Aktion vom Administrationsprozess für alle Aufgaben herangezogen, das heißt, wir haben es hier mit einem echten Dilemma zu tun: Bei Umbenennungen sollen alle Namensfelder geändert werden, aber bei Löschungen keines!

Alternativ zum Anpassen aller Zugriffskontrolllisten vor jedem Umbenennen oder Löschen können Sie, um das Löschen von Personen aus Namens- bzw. Leser- und Autorenfeldern zu verhindern, die beiden folgenden Einträge in die Datei notes.ini aufnehmen:

```
ADMINP_DISABLE_NAMEITEM_DELETE=1  
ADMINP_DISABLE_READAUTH_DELETE=1
```

5.7.5.3. Den Administrationsprozess mit einer Ansicht beschleunigen

Per Vorgabe durchsucht der Administrationsprozess alle Dokumente der Datenbank nach Leser-, Autoren- und Namensfeldern mit einem umzubennenden oder zu löschenden Namen. Dies ist sehr ressourcenintensiv und kann gegebenenfalls lang dauern. Sie können die Suche beschleunigen, indem Sie eine Ansicht mit dem Namen »\$AdminP« erstellen, die das Durchsuchen nach Leser-, Autoren- und Namensfeldern auf die enthaltenen Dokumente beschränkt. Ist die Ansicht leer, wird die Datenbank übersprungen.

5.8. Domino-Server neu installieren oder verschieben

5.8.1. Den Domino-Server auf derselben Maschine neu installieren

Wenn das Installationsprogramm ein Update nicht abschließen kann oder der Domino-Server abstürzt und die zugehörige Ursache bei der Fehlersuche nicht gefunden wird, kann es helfen, die Software neu zu installieren.

Verwenden Sie bei der Neuinstallation genau dieselben Pfade wie bei der Erstinstallation. Dabei werden die vorhandenen Systemdateien (names.nsf, admin4.nsf, certlog.nsf etc.) nicht überschrieben, und alle relevanten Informationen aus der vorhandenen Datei notes.ini übernommen.

Achtung: Haben Sie bereits ein Fix Pack installiert, müssen Sie es nach der Neuinstallation erneut einspielen.

5.8.2. Den Domino-Server auf eine andere Maschine verschieben

Wenn die Hardware für Domino nicht mehr ausreicht, können Sie entweder einen zweiten Domino-Server aufbauen und beide Server betreiben oder den vorhandenen Server auf eine leistungsfähigere Maschine verschieben.

Für das Verschieben bieten sich zwei Methoden an:

1. Verschieben auf Betriebssystemebene
2. Verschieben via Replikation

5.8.3. Verschieben auf Betriebssystemebene

Verwenden Sie diese Methode, wenn das Kopieren der Daten nicht lange dauert bzw. es kein Problem darstellt, wenn Ihr Domino-Server einige Zeit nicht erreichbar ist. Gehen Sie dazu wie folgt vor:

1. Erstellen Sie ein vollständiges Backup.
2. Deaktivieren Sie die Replizierung und das Mail-Routing auf dem Server, der verschoben werden soll.
3. Erstellen Sie die notwendigen Verzeichnisse auf dem neuen Server.
4. Kopieren Sie alle Dateien aus dem alten Datenverzeichnis ins neue. Kopieren Sie außerdem die Datei notes.ini ins neue Programmverzeichnis.
5. Verwenden Sie auf dem neuen Server andere Pfade, müssen Sie alle Verweise in der Datei notes.ini richtigstellen. Suchen Sie dazu mit der Tastenkombination [Strg]+[F] nach dem alten Pfad und ersetzen Sie ihn durch den neuen. Betroffen sind folgende Variablen:

Directory=D:\Domino\Data

KeyFileName=D:\Domino\Data\server.id

Wenn Sie auch das Programmverzeichnis ändern wollen, dann außerdem:

NotesProgram=C:\Program Files\HCL\Domino

6. Trennen Sie den alten Computer vom Netzwerk und ordnen Sie dem neuen Server denselben Hostnamen und dieselbe IP-Adresse zu wie dem alten.

Sollte das nicht möglich sein und der Server einen neuen Hostnamen und/oder eine andere IP-Adresse bekommen, müssen zusätzlich zu Datei notes.ini die Dateien dconsole.ini und dcontroller.ini richtiggestellt werden.

Wenn sich weiters die Netzwerkkonfiguration ändert, muss außerdem das Serverdokument aktualisiert werden, da hier als Netzwerkname entweder der Hostname oder die IP-Adresse eingetragen ist.

7. Installieren Sie die Domino-Server-Software auf dem neuen Computer. Verwenden Sie dabei exakt dieselben Pfade wie in der notes.ini angegeben. Die vorhandenen Systemdateien werden nicht überschrieben und alle relevanten Informationen aus der vorhandenen Datei notes.ini übernommen.
8. Starten Sie den neuen Server und prüfen Sie, ob er korrekt installiert und konfiguriert wurde.

Wenn Sie sehen wollen, welche Meldungen der Server beim Hochfahren ausgibt, können Sie ihn beim ersten Mal auch im Stand-Alone-Modus starten. Geben Sie dazu in einer Kommandozeile oder via Ausführen (Run) den folgenden Befehl ein:

```
"C:\Program Files\HCL\Domino\nserver.exe" -sa
```

5.8.4. Verschieben via Replikation

Verwenden Sie diese Methode, wenn das Kopieren der Datenbanken auf Betriebssystemebene sehr lange dauert und Sie nicht wollen, dass Ihr Server so lange offline bleibt.

1. Registrieren Sie einen neuen Domino-Server und kopieren Sie die server.id auf die neue Maschine.
2. Installieren Sie auf der neuen Maschine einen neuen Domino-Server. Wählen Sie während der Konfiguration die Option »Set up an additional server« und geben Sie die neue server.id aus Schritt 1 an.
3. Erstellen Sie ein Verbindungsdokument für den alten und den neuen Server und aktivieren Sie darin die Replikation.
4. Sorgen Sie dafür, dass der alte Server auf dem neuen Repliken erstellen darf. Das geht entweder damit, dass Sie den alten Server zu einem Administrator des neuen Servers machen (nehmen Sie am besten gleich die Gruppe LocalDomainServers in das Feld **Administratoren** auf), oder indem Sie den alten Server im Serverdokument des neuen Servers im Register Sicherheit im Abschnitt **Wer darf auf Server zugreifen** im Feld **Neue Repliken erstellen** aufnehmen.
5. Der neue Server muss in allen Datenbanken des alten Servers mindestens Leserrechte haben. Das erreichen Sie am besten, indem Sie bei allen Datenbanken die Gruppe »LocalDomainServers« zur ACL hinzufügen.
6. Replizieren Sie das Domino-Verzeichnis (names.nsf) und überprüfen Sie, ob alle Änderungen übertragen werden.
7. Nehmen Sie die Variable ADMINP_EXCHANGE_ALL_UNREAD_MARKS=1 in die notes.ini des alten Servers auf.
8. (Test) Erstellen Sie eine Replik einer Maildatenbank auf dem neuen Server, indem Sie im Domino-Administrator die Datenbank im Register Dateien markieren und dann in den Werkzeugen den Befehl **Datenbank > Replik(en) erstellen...** auswählen.

Setzen Sie auch ein Häkchen bei »Ungelesen-Markierungen beim Replizieren austauschen«. Damit stellen Sie sicher, dass die Ungelesen-Markierungen auf dem neuen Server nicht abweichen. (Diese Einstellung verlangsamt die Replikation.)

Beachten Sie, dass der Administrationsprozess mit dem Erstellen der Replik beauftragt wird.

9. Wenn Ihr Test erfolgreich war, können Sie mehrere Repliken mit einer Mehrfachauswahl erstellen. Nehmen Sie aber nicht gleich alle Datenbanken, sondern erstellen Sie die Repliken in mehreren Schritten.
10. Nachdem alle Datenbanken repliziert wurden, fahren Sie beide Server herunter und kopieren Sie die notes.ini und die server.id auf den neuen Server.
11. Ändern Sie den Hostnamen und die IP-Adresse des neuen Servers.
12. Starten Sie den neuen Server und testen Sie die Serververbindung, das Mail-Routing etc.

6. Benutzerverwaltung

- > 6.1 Richtlinien, Seite 123
- > 6.2 Der ID-Vault, Seite 137
- > 6.3 Eine serverbasierende Zulassungsstelle einrichten, Seite 149
- > 6.4 Notes-Benutzer anlegen, Seite 152
- > 6.5 Roaming-Benutzer, Seite 157
- > 6.6 Notes-ID-Kennwörter zurücksetzen, Seite 160
- > 6.7 Notes-IDs verlängern, Seite 163
- > 6.8 Benutzer umbenennen, Seite 165
- > 6.9 Benutzer verschieben, Seite 171
- > 6.10 Benutzer sperren, Seite 172
- > 6.11 Benutzer löschen, Seite 173
- > 6.12 Gruppen verwalten, Seite 175
- > 6.13 Externe Verzeichnisse einbinden, Seite 180

6.1. Richtlinien

6.1.1. Überblick

Richtlinien – auf »Neuhochdeutsch« manchmal schon als Policies bezeichnet – sind Teil der Benutzerverwaltung. Damit steuern Sie die Benutzeranlage, legen fest, wie sich Benutzer anzumelden haben, und setzen Einstellungen in Clients – um nur einige Möglichkeiten zu nennen. Richtlinien sind zwar nicht perfekt, aber es kommen mit jeder Domino-Version neue Möglichkeiten hinzu und sie werden immer besser!

Typisch für eine **richtlinienbasierte Verwaltung** (Policy Based Management) ist das Setzen von Einstellungen auf verschiedenen Ebenen. Das beginnt auf Serverebene, wo Sie Vorgaben im Konfigurationsdokument setzen. Bereits hier erfolgt die Konfiguration mehrstufig: Vorgabe-Konfiguration – Gruppenkonfiguration – Serverkonfiguration. Mehr über das Erstellen von Konfigurationsdokumenten lesen Sie in Kap. 5.4 Konfigurationsdokumente, ab Seite 99.

Eine Stufe tiefer geht es mit Richtlinien weiter, wo es wieder mehrere Ebenen geben kann: eine Richtlinie für die ganze Organisation, eine für einen Standort, eine weitere für eine funktionelle Gruppe (z. B. alle Notebook-Besitzer) und noch eine für ein Projektteam ...

Richtlinien bestehen aus zwei Komponenten, dem eigentlichen **Richtliniendokument** (Policy Master) und einem oder mehreren daran hängenden **Einstellungsdokumenten** (Policy Settings). Im Richtliniendokument erfolgt die Zuweisung zu einer Benutzergruppe und welche Einstellungs-

dokumente auf sie wirken sollen, nicht aber die Einstellungen selbst. Das heißt, das Erstellen einer Richtlinie allein bewirkt noch nichts, Sie müssen auch zumindest ein Einstellungsdokument zugeordnet haben. Derzeit stehen die folgenden Einstellungstypen zur Verfügung:

Einstellungstyp	Einstellungsname	
Registrierung:	<input type="checkbox"/> <input type="checkbox"/>	Neu...
Einrichtung:	<input type="checkbox"/> <input type="checkbox"/>	Neu...
Archivierung:	<input type="checkbox"/> <input type="checkbox"/>	Neu...
Desktop:	<input type="checkbox"/> <input type="checkbox"/>	Neu...
Sicherheit:	<input type="checkbox"/> <input type="checkbox"/>	Neu...
Mail:	<input type="checkbox"/> <input type="checkbox"/>	Neu...
Connections:	<input type="checkbox"/> <input type="checkbox"/>	Neu...
Notes Traveler:	<input type="checkbox"/> <input type="checkbox"/>	Neu...
Roaming:	<input type="checkbox"/> <input type="checkbox"/>	Neu...
Symphony:	<input type="checkbox"/> <input type="checkbox"/>	Neu...

Abbildung 6.1: Liste der Einstellungstypen im Richtliniendokument

Nicht alle Einstellungstypen sind gleich wichtig, manche sogar obsolet (z. B. Symphony). Zumindest die nachfolgenden Typen sollten Sie verwenden:

Einstellungstyp	Beschreibung
Registrierung	Legt Vorgaben für die Benutzerregistrierung fest.
Archivierung	Verbietet oder aktiviert die Archivierung und legt die Regeln dafür fest.
Desktop (auch Dynamischer Desktop genannt)	Enthält einerseits Client-Einstellungen (fast alles, was der Benutzer über Datei > Vorgaben... setzen kann) sowie Einstellungen, die dynamisch gesetzt werden müssen.
Sicherheit	Setzt Vorgaben für die Sicherheit.
Mail	Setzt Vorgaben für Mail, Kalender und Aufgaben.

Tabelle 6.1: Nützliche Richtlinieneinstellungen

Es gibt drei Möglichkeiten, eine Richtlinie zuzuweisen:

- > über die Hierarchie (Organisationsbezogene Richtlinie)
- > über eine Gruppe (Explizite Richtlinie)
- > über eine individuelle Zuordnung im Personendokument

6.1.2. Organisationsbezogene Richtlinien

Organisationsbezogene Richtlinien (Organizational Policies) beginnen immer mit einem Stern und einem Schrägstrich (*). Es sind mehrere Ebenen möglich, z. B.:

* /

* /AT

* /COB/AT

* /Verkauf/COB/AT

Das heißt, auf eine Person, die von der OUI Verkauf registriert wurde, wirken vier Richtlinien, wobei die Richtlinien vom Client von oben nach unten abgearbeitet werden. Die Sternrichtlinie (* /) ist somit die schwächste, weil ihre Einstellungen von den nachfolgenden Richtlinien überschrieben werden können, die OU-Richtlinie für Verkauf die stärkste, weil sie ihre Einstellungen nach allen anderen Richtlinien setzt.

Eine explizite Zuweisung ist bei organisationsbezogenen Richtlinien nicht nötig, die Benutzer werden basierend auf dem hierarchischen Namensschema automatisch zugeordnet. Bereits bei der Registrierung bestimmt die Wahl des Zertifizierers, welche organisationsbezogenen Richtlinien gelten:

The screenshot shows a registration form with the following fields and values:

- Registrierungsserver...: DOM/COB/AT
- Vorname: [Empty]
- Zweiter Vorname: [Empty]
- Nachname: [Empty]
- Kurzname: [Empty]
- Kennwort: [Empty]
- Mailsystem: HCL Notes
- Explizite Richtlinie: (keine expliz. Richtlinie zugewiesen)
- Kennwortoptionen...: [Button]
- Roaming für diese Person aktivieren:
- Notes-ID für diese Person erstellen:
- Organisationsbezogene Richtlinie: */COB/AT (highlighted with a red box)
- Richtlinienübersicht...: [Button]

Abbildung 6.2: Automatische Zuordnung von organisationsbezogenen Richtlinien beim Registrieren

6.1.3. Explizite Richtlinien

Explizite Richtlinien (Explicit Policies) beginnen mit einem Schrägstrich (/) und werden, wie der Name bereits andeutet, einer Personengruppe oder auch einer einzelnen Person explizit zugewiesen. Dies erfolgt entweder im Richtliniendokument selbst (Angabe von Benutzern oder Gruppen im Register **Richtlinienzuweisung**) oder über das Personendokument (Auswahl der Richtlinie im Feld **Zugewiesene Richtlinie** im Register **Administration**). Über das Personendokument kann nur eine einzige Richtlinie zugewiesen werden, über das Richtliniendokument auch mehrere Richtlinien.

The screenshot shows a policy document titled "Richtlinie : /Notebook-Anwender". The "Richtlinienzuweisung" tab is active, showing a list of users and groups. The group "Notebook-Anwender" is listed in the table.

Benutzer und Gruppen
Notebook-Anwender

Abbildung 6.3: Zuweisung im Richtliniendokument über die Gruppe »Notebook-Anwender«

Explizite Richtlinien werden nach organisationsbezogenen abgearbeitet, überschreiben also gegebenenfalls die dort gesetzten Einstellungen. Bei Zuordnung mehrerer expliziter Richtlinien, gewinnt jene mit der höchsten Priorität.

6.1.4. Wirksame Richtlinie

Die sogenannte **Wirksame Richtlinie** (auf Englisch: **Effective Policy**) ist die Summe aller Einstellungen, die auf einen Benutzer wirken. Bei der Abarbeitung der Richtlinien durch den Notes-Client wird dynamisch berechnet, welche Einstellungen gelten, wobei diese durchaus auch aus verschiedenen Richtliniendokumenten stammen können, etwa aus OU-Richtlinien, inklusive aus vererbten übergeordneten Richtlinien, und aus expliziten Richtlinien.

Hat der Client eine Richtlinieneinstellung abgearbeitet, erstellt er in der lokalen Kontakte-Anwendung (names.nsf) in der versteckten Ansicht (\$Policies) ein Dokument mit allen Einstellungen, die im Fall von computerspezifischen Formeln (siehe Kap. 6.1.7.2 Computerspezifische Formeln, ab Seite 129 auch individuell berechnet worden sein können:

Typ oder Name der Richtlinie	Richtliniename UNID
Effective Policy for: Peter Tester/COB/AT	Effective Policy for: Peter Tester/COB/AT 3CF835840CAE7BA11A947CDEB9B7FF2
Effective Policy for: Peter Tester/COB/AT	Effective Policy for: Peter Tester/COB/AT 57231875D0BA7F05CB29770875E0F013
Effective Policy for: Peter Tester/COB/AT	Effective Policy for: Peter Tester/COB/AT 928167F2B8722D68F9F00991B192A85A
Effective Policy for: Peter Tester/COB/AT	Effective Policy for: Peter Tester/COB/AT 9F658E206ACC4DC2D40ADE2268391265
Effective Policy for: Peter Tester/COB/AT	Effective Policy for: Peter Tester/COB/AT C05AD689F485AB631A99ED67F8FE64EA
PolicyDesktop	Effective Policy for: Peter Tester/COB/AT 57231875D0BA7F05CB29770875E0F013
PolicyMail	Effective Policy for: Peter Tester/COB/AT 3CF835840CAE7BA11A947CDEB9B7FF2
PolicyRegistration	Effective Policy for: Peter Tester/COB/AT 928167F2B8722D68F9F00991B192A85A
PolicySecurity	Effective Policy for: Peter Tester/COB/AT 9F658E206ACC4DC2D40ADE2268391265
PolicyTraveler	Effective Policy for: Peter Tester/COB/AT C05AD689F485AB631A99ED67F8FE64EA

Abbildung 6.4: Die versteckte Ansicht (\$Policies) in der lokalen Kontakte-Anwendung

Beim nächsten Zugriff überprüft der Client nur noch, ob die Richtlinieneinstellung am Server neuer ist als das von ihm angelegte Vergleichsdokument. Ist es der Fall, arbeitet er die Richtlinie erneut ab und aktualisiert das lokale Dokument. Ist es nicht der Fall, geht er zur nächsten Richtlinieneinstellung weiter.

Um zur Ansicht (\$Policies) zu gelangen, öffnen Sie die lokale Kontakte-Applikation (names.nsf) und wählen Sie im Menü den Befehl **Ansicht > Gehe zu...** bei gleichzeitigem Drücken der Tasten [Strg]+[Umschalten] aus.

Im Dialog **Gehe zu** werden die versteckten Ansichten nun eingeblendet. Wählen Sie die Ansicht (\$Policies) und klicken Sie auf **OK**:

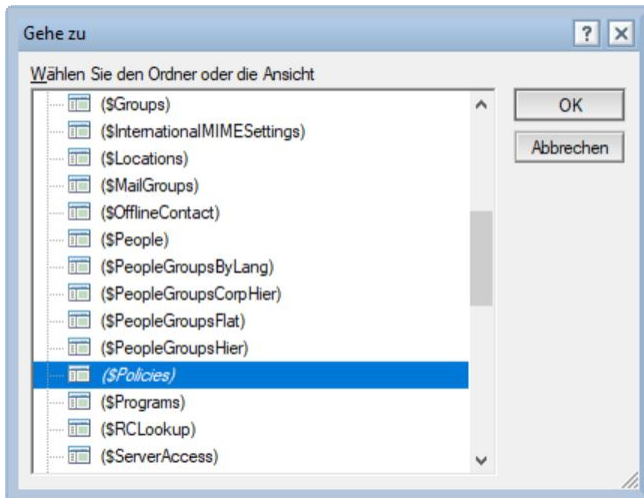


Abbildung 6.5: Der Dialog Gehe zu nach Drücken der Tasten [Strg]+[Umschalten]

Tipp: Sie können die versteckten Ansichten im Domino-Verzeichnis oder in der lokalen Kontakte-Anwendung auch einblenden, indem Sie die Tasten [Strg]+[Umschalten] gedrückt halten und dann den Doppelklick auf das Datenbanksymbol ausführen.

6.1.5. Das Ausrollen von Richtlinien planen

Sie sollten bei jeder Einstellung überlegen, wie Sie sie ausrollen. Betrifft die Einstellung die ganze Organisation oder ist sie standortbezogen? Steckt dahinter eine Abteilung, für die ein Zertifizierer existiert (organisationsbezogen) oder handelt es sich um eine funktionelle Gruppe, die sich quer durch ihre ganze Organisation zieht (explizite Zuordnung, z. B. Notebook-Benutzer).

6.1.6. Eine organisationsbezogene Richtlinie erstellen

Beginnen wir mit dem Erstellen einer Registrierungsrichtlinie, die uns später beim Anlegen von Benutzern viel Arbeit abnehmen wird. Da sich die Registrierung immer auf die Hierarchie bezieht (wir wählen zur Registrierung ja einen bestimmten Zertifizierer aus), hängen wir diese Einstellung vernünftigerweise auf einer organisationsbezogenen Richtlinie auf. Erstellen wir also zuerst eine Richtlinie für die ganze Organisation.

Zum Erstellen von Richtlinie und Richtlinieneinstellungen benötigen Sie im Domino-Verzeichnis zumindest Editor-Rechte sowie die Rollen [PolicyCreator] und [PolicyModifier].

Um eine organisationsbezogene Richtlinie zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Personen und Gruppen**.
2. Wählen Sie die Ansicht **Richtlinien** und klicken Sie auf die Schaltfläche **Neue Richtlinie**.
3. Wir wollen eine Richtlinie für die ganze Organisation erstellen, daher wählen wir im Feld **Typ der Richtlinie** »Organisationsbezogen«.
4. Tippen Sie im Feld **Richtliniename** nach dem Stern und dem Schrägstrich den Namen Ihres Zertifizierers ein. In unserem Fall heißt die Unternehmenszulassung /COB/AT, daher lautet der Name der Richtlinie: »*/COB/AT«.

Abbildung 6.6: Organisationsbezogene Richtlinie

5. Optional: Geben Sie eine kurze Beschreibung ein.
6. Optional: Weisen sie der Richtlinie eine Kategorie zu (hilfreich in der Ansicht **Nach Kategorie**).
7. Speichern und schließen Sie das Dokument.

Achtung: Die Richtigkeit Ihrer Eingabe wird nicht überprüft. Wenn Sie sich beim Namen Ihrer Organisation vertippen, greift die Richtlinie nicht!

6.1.7. Hinweise zu Richtlinieneinstellungen

Alle Einstellungsdokumente enthalten die Felder **Name** (das einzige Pflichtfeld) und **Beschreibung**, unterschiedlich viele Felder für die eigentlichen Einstellungen sowie Informationen, wie diese angewendet werden.

6.1.7.1. Wie Einstellungen angewendet werden

Manchmal wird in der Spalte **Wie diese Einstellung angewendet wird** nur ein Kontrollkästchen mit »Wert nicht festlegen« angeboten, manchmal eine Liste mit vier Optionen:

Option	Erklärung
Wert nicht festlegen	bedeutet, dass das Feld nicht gesetzt wird – als wäre es nicht vorhanden.
Anfangswert festlegen	bedeutet, dass der Wert am Client einmalig gesetzt und dann nie wieder geändert wird. Ideal, um Vorgaben zu setzen. Sollten Sie die Vorgaben jedoch später ändern wollen, müssen Sie (zumindest kurzfristig) auf »Wert nach jeder Änderung festlegen« umstellen.
Wert nach jeder Änderung festlegen	bedeutet, dass der Wert neu gesetzt wird, wenn das Richtliniendokument gespeichert wird. Diese Methode sollte vermieden werden, da der Benutzer sonst meint, die Kontrolle über die Einstellung zu haben, seine Änderung aber bei jedem Speichern zurückgesetzt wird.
Wert festlegen und Änderung verhindern	Hier wird die Einstellung einmalig gesetzt und das Feld dann gesperrt, sodass es der Benutzer nicht mehr ändern kann. Bezieht sich die Einstellung auf einen Menüpunkt, kann dieser auch ausgeblendet werden. Zusätzlich wird dem Benutzer angezeigt, dass der Administrator einige Vorgaben gesperrt hat.

Tabelle 6.2: Optionen im Listenfeld Wie diese Einstellung angewendet wird

Manche Einstellungen sind per Vorgabe deaktiviert (»Wert nicht festlegen«), da sie mit einer späteren Version von Notes und Domino eingeführt und nicht rückwärtskompatibel sind.

Für alle Einstellungen gilt prinzipiell, dass sie optional sind, d. h. wählen Sie nichts aus, wird auch kein Wert gesetzt. In diesem Fall kommen entweder die Einstellungen aus einer übergeordneten (schwächeren) Richtlinie zum Zug oder es wird keine Vorgabe gesetzt und es gelten die Client-Vorgaben. Hier ein Beispiel für eine gesperrte Einstellung in den Mailvorgaben:

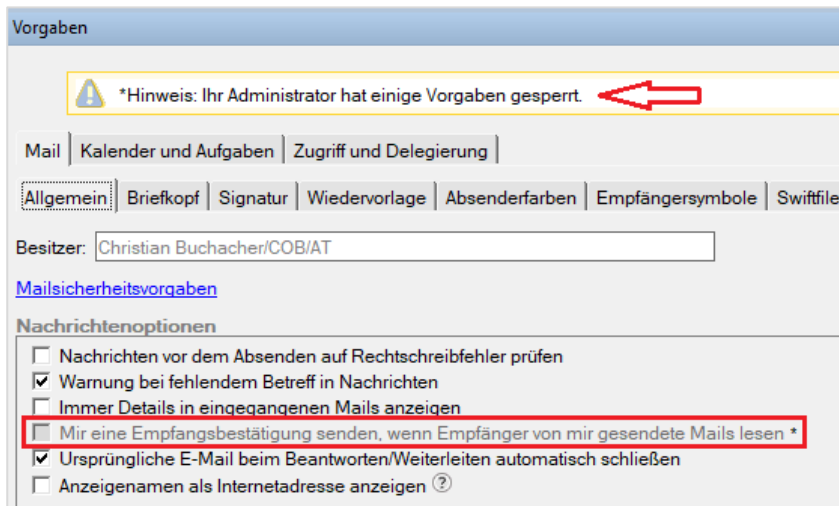


Abbildung 6.7: Vorgaben, Bereich Nachrichtenoptionen

6.1.7.2. Computerspezifische Formeln

In den Einstellungsdocumenten finden Sie an manchen Stellen zusätzlich die Schaltfläche **Computerspezifische Formel eingeben**, z. B. für das Erstellen von Verwalteten Repliken in der Desktoprichtlinie:

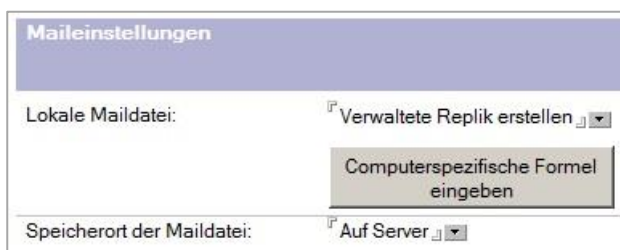


Abbildung 6.8: Schaltfläche **Computerspezifische Formel eingeben** in der Desktoprichtlinie, Register Mail

Klicken Sie auf diese Schaltfläche, wird ein Feld eingeblendet, in das Sie theoretisch jede beliebige @Formel eingeben können, die einen für die Einstellung passenden Wert zurückliefert (siehe Abbildung 6.9).

Die eingegebene Formel wird auf dem Client ausgeführt, wenn die Richtlinie verarbeitet wird, und das Ergebnis der Formel in der lokalen Kopie der Desktopeinstellung in der Kontakte-Anwendung gespeichert.



Abbildung 6.9: Das Feld **Computerspezifische Formel nachfolgend** in der Desktoprichtlinie, Register Mail

Die Funktion @GetMachineInfo

Meist kommt in diesem Feld die Funktion @GetMachineInfo zur Anwendung. Die Syntax der Funktion lautet:

```
@GetMachineInfo ([Schlüsselwort]; "Optionaler Text")
```

In dem in Abbildung 6.9 dargestellten Beispiel würde, wenn es sich um einen Stand-PC (Desktop) handelt, im lokalen Dokument der Wert »7« gespeichert, auf einem Notebook der Wert »8«. (Die Werte sind gegebenenfalls via Designer-Client in der Maske nachzuschlagen, im Fall des Feldes **Lokale Maildatei** lauten sie: »1« Lokale Replik erstellen, »3« Verwaltete Replik erstellen, »7« Verwaltete Replik erstellen oder lokale Replik in verwaltete Replik konvertieren oder »8« Lokale oder verwaltete Replik löschen.)

Weitere Schlüsselwörter für die Funktion @GetMachineInfo entnehmen Sie bitte Tabelle 6.3:

Schlüsselwort	Erklärung
IsLaptop	Liefert wahr zurück, wenn es sich beim aktuellen PC um einen Laptop/Notebook handelt.
IsDesktop	Liefert wahr zurück, wenn es sich beim aktuellen PC um einen Stand-PC/Desktop handelt. Beispiel: @If (@GetMachineInfo ([IsDesktop]); "7"; "8")
IsMultiUser	Liefert wahr zurück, wenn der Notes-Client als Mehrbenutzerinstallation vorliegt.
HasDesigner	Liefert wahr zurück, wenn ein Domino-Designer installiert ist.
HasAdmin	Liefert wahr zurück, wenn ein Domino-Administrator installiert ist.
IsStandard	Liefert wahr zurück, wenn ein Standard-Client installiert ist.
MachineName	Liefert wahr zurück, wenn der Maschinenname dem im Text angegebenen Namen entspricht. Beispiel: @If (@Left (@GetMachineInfo ([MachineName]); 2) = "WS"; "7"; "8")
Memory	Größe des lokalen Hauptspeichers (RAM). Beispiel: @If (@GetMachineInfo ([Memory]) >= 2048; "UseBasicNotes=0"; "UseBasicNotes=1")
DiskSpace	Größe des lokalen Plattenspeichers. Es kann zusätzlich das Laufwerk angegeben werden. Beispiel:

Schlüsselwort	Erklärung
	<code>@GetMachineInfo ([DiskSpace]; "d:")</code>
EnvVariable	Liefert den Wert der im Text angegebenen Variable in der lokalen Datei notes.ini zurück oder eine leere Zeichenfolge (""), wenn die Variable fehlt. Beispiel: <code>@GetMachineInfo ([EnvVariable]; "UseBasicNotes")</code>
SysEnvVariable	Liefert den Wert der im Text angegebenen Umgebungsvariable zurück oder eine leere Zeichenfolge (""), wenn dies fehlt. Beispiel Abfrage einer Citrix-Sitzung: <code>@If (@Left (@GetMachineInfo ([SysEnvVariable]; "SESSIONNAME"); 3) = "ICA"; @Unavailable; "7")</code>
IP	Liefert wahr zurück, wenn die IP-Adresse der im Text angegebenen entspricht. Beispiel: <code>@If (@Contains (@GetMachineInfo ([IP]); "192.168"); "7"; "8")</code>
MAC	Liefert wahr zurück, wenn die MAC-Adresse der im Text angegebenen entspricht.

Tabelle 6.3: Optionen der Funktion @GetMachineInfo

Computerspezifische Formeln stehen innerhalb der Richtlinien für folgende Einstellungen zur Verfügung:

- > Automatisches Update – Desktoprichtlinie: AUT
- > Lokales Verschlüsseln von Repliken – Desktoprichtlinie: Vorgaben > Replizierung
- > Setzen von notes.ini-Variablen – Desktoprichtlinie: Benutzerdefinierte Einstellungen > Notes.ini
- > Setzen von Einstellungen in Arbeitsumgebungen – Desktoprichtlinie: Benutzerdefinierte Einstellungen > Arbeitsumgebungen
- > Setzen von Verwalteten Einstellungen (Eclipse) – Desktoprichtlinie: Benutzerdefinierte Einstellungen > Verwaltete Einstellungen
- > Gemeinsame Notes-Anmeldung (Notes Shared Login) – Sicherheitsrichtlinie: Kennwortverwaltung > Gemeinsame Notes-Anmeldung
- > Föderierte Anmeldung (Federated Login) – Sicherheitsrichtlinie: Kennwortverwaltung > Föderierte Anmeldung

So viel zur Theorie. Stürzen wir uns nun in die Praxis!

6.1.8. Die Registrierungseinstellung

Die Registrierungseinstellung dient dazu, Vorgaben im Registrierdialog zu setzen. Es handelt sich also nicht um eine Richtlinie für Benutzer, sondern um eine für uns Administratoren. Die Vorgaben sind auch nicht verpflichtend, sondern können beim Registrieren angepasst werden. Ziel der Richtlinieneinstellung ist es also nicht, den Administrator zu etwas zu zwingen, sondern ihm die Arbeit zu erleichtern.

6.1.8.1. Die Einstellung erstellen

Die Richtlinieneinstellungen können an zwei Stellen erzeugt werden:

1. Im Richtliniendokument über die Schaltfläche **Neu...** Wählen Sie in diesem Fall die Schaltfläche neben dem Eintragstyp **Registrierung**.
2. In der Ansicht **Personen und Gruppen > Einstellungen** über die Schaltfläche **Einstellung hinzufügen...** Wählen Sie in diesem Fall die Option **Registrierung**.
3. Füllen Sie nun die Felder im Register **Allgemein** wie folgt aus:

Feld	Einstellung
Name	Vergeben Sie einen beliebigen Namen, am besten das Wort »Registrierung«, gefolgt vom Gültigkeitsbereich, in unserem Fall das ganze Unternehmen, also z. B. »Registrierung COB/AT«.
Beschreibung	Geben Sie eine Beschreibung ein. Erklären Sie, warum diese Richtlinie erstellt wurde und für wen. (Für längere Beschreibungen steht zusätzlich ein Kommentarfeld zur Verfügung.)
Registrierungsserver	Wenn die Benutzer zum überwiegenden Teil auf einem bestimmten Server registriert werden, wählen Sie ihn hier aus. Ist das nicht der Fall, lassen Sie das Feld leer, dann wird der im Domino-Administrator hinterlegte Registrierungsserver vorgeschlagen.
Kennwortqualität	Wählen Sie eine Kennwortqualität aus. Wenn eine Sicherheitseinstellung existiert, gelten die Kennwortregeln aus der Registriereinstellung nur für das erste Anmelden des Benutzers.
Internetkennwort festlegen	Aktivieren Sie diese Option, wenn das Internetkennwort anfangs gleich lauten soll wie das Notes-Kennwort. (Mehr Details zur Kennwortverwaltung finden Sie in Kap. 13.3 ID-Sicherheit, ab Seite 342)
Roaming-Benutzer	Wenn neue Benutzer das Roaming-Feature verwenden sollen, setzen Sie das Häkchen für Roaming-Benutzer . (Vergessen Sie die irreführende Angabe »vor 8.5«!) Ausführliche Informationen zum Thema Roaming finden Sie in Kap. 6.5 Roaming-Benutzer, ab Seite 157.

Tabelle 6.4: Registrierungseinstellung, Register Allgemein

4. Wechseln Sie zum Register **Mail** und füllen Sie die Felder wie folgt aus:

Feld	Einstellung
Mailsystem	Wählen Sie »HCL Notes«.
Mailserver	Wenn es Sinn macht, einen Mailserver vorzugeben, wählen Sie ihn hier aus – er kann später im Registrierdiallog bei Bedarf geändert werden. Lassen Sie das Feld leer, wird beim Registrieren der verbundene Server als Mailserver vorgeschlagen.
Mailschablone	Wenn Sie eine andere Mailschablone verwenden als vorgeschlagen, ändern Sie hier den Namen.
Maildatei jetzt / im Hintergrund erstellen	Wählen Sie »Maildatei jetzt erstellen«, wenn die Maildatenbank beim Registrieren erstellt werden soll. Wählen Sie »Maildatei im Hintergrund erstellen«, wenn die Verbindung beim Registrieren langsam ist (Sie etwa über das Internet zugreifen), dann wird der

Feld	Einstellung
	Administrationsprozess mit dem Erstellen der Maildatenbank betraut.
Internetdomäne	Hinterlegen Sie hier Ihre Internetdomäne.
Internetadressformat und Trennzeichen	Wählen Sie das Internetadressformat, üblicherweise: Vorname.Nachname@Domäne.
Mailrepliken erstellen auf	Legen Sie hier fest, auf welchen Servern Repliken der Maildatenbank erstellt werden sollen. Haben Sie einen Mail-Cluster, genügt es, die Option »Allen Mitgliedern des Mail-Server-Clusters« auszuwählen.
Zugriff für Besitzer der Maildatei	Normale Benutzer sollten nur über Editor-Rechte verfügen.
Manager der Maildatei	Wählen Sie die vorgesehene Admin- oder Support-Gruppe aus, die den Benutzer später bei Problemen unterstützen soll.
Volltextindex erstellen	Setzen Sie hier ein Häkchen, um die Maildatenbank von Anfang an mit einem Volltextindex zu versehen.
DB-Größenbeschränkung festlegen	Nach Aktivieren wird ein zusätzliches Feld eingeblendet, in dem Sie die Größenbeschränkung in MB eingeben können.
Warnschwellenwert festlegen	Nach Aktivieren wird ein zusätzliches Feld eingeblendet, in dem Sie den Warnschwellenwert in MB eingeben können.

Tabelle 6.5: Registrierungseinstellung, Register Mail

5. Wechseln Sie zum Register **ID/Zertifizierer** und füllen Sie die Felder wie folgt aus:

Feld	Einstellung
Sicherheitstyp	Hier wählen Sie normalerweise »Nordamerika«. Bei Auswahl von »International« werden kürzere Schlüssel generiert.
Spezifikation des öffentlichen Schlüssels	Sie sollten nur noch »Kompatibel mit Version 7.0 und höher (2018 Bit)« auswählen.
Kennwortschlüssellänge	Wählen Sie die Option »Mit 8.0 und höher kompatibel (256 Bit AES)«.
Ablaufdatum des Zertifikats	Wählen Sie die Option »Monate seit der Benutzerregistrierung« und geben Sie die Anzahl Monate ein, z. B. 24.
Speicherort der Benutzer-ID	Wählen Sie »In Datei« und wählen Sie über die Schaltfläche Verzeichnis für ID-Dateien festlegen... den Speicherort aus. Die ID-Datei im Domino-Verzeichnis abzulegen stellt ein Sicherheitsrisiko dar, da sie jeder Leser herunterladen kann. Stattdessen sollten Sie einen ID-Vault (ID-Tresor) einrichten, in dem die ID-Datei dann sicher gespeichert wird. (Zum Einrichten eines ID-Vaults lesen Sie Kap. 6.2.1 Einen ID-Vault einrichten, ab Seite 138.)

Tabelle 6.6: Registrierungseinstellung, Register ID/Zertifizierer

6. Wechseln Sie jetzt zum Register **Verschiedenes** und füllen Sie die Felder wie folgt aus:

Feld	Einstellung
Gruppenzuweisungen	Wählen Sie die Gruppe(n) aus, zu denen alle Benutzer hinzugefügt werden sollen.

Tabelle 6.7: Registrierungseinstellung, Register Verschiedenes

7. Speichern und schließen Sie die Registrierungseinstellung.

6.1.8.2. Die Einstellung einer Richtlinie zuweisen

1. Öffnen Sie die gewünschte Richtlinie – in unserem Fall die Unternehmensrichtlinie */COB/AT – und schalten Sie in den Bearbeitungsmodus um.
2. Klappen Sie in der Liste der Einstellungen neben dem Richtlinientyp **Registrierung** die Liste auf und wählen Sie die soeben erstellte Registrierungseinstellung »Registrierung COB/AT« aus:



Abbildung 6.10: Richtlinie, Zuordnung der Registrierungseinstellung

3. Speichern und schließen Sie die Richtlinie. Die neue Einstellung wirkt sofort beim nächsten Registrieren eines Benutzers.

Bevor Sie Benutzer im großen Stil registrieren, sollten Sie einen ID-Vault einrichten. Zum Einrichten eines ID-Vaults lesen Sie Kap. 6.2.1 auf Seite 138.

Wollen Sie jetzt einen Benutzer registrieren, blättern Sie weiter zu Kap. 6.4.1 auf Seite 152.

Zuvor ein paar Informationen über die anderen Richtlinieneinstellungen.

6.1.9. Übersicht über weitere Richtlinieneinstellungen

Bei den anderen Richtlinieneinstellungen gehe ich die einzelnen Felder nicht durch – das würde aufgrund der Fülle an Möglichkeiten vor allem in der Desktop- oder Sicherheitseinstellung den Rahmen sprengen. Stattdessen picken wir uns in den einzelnen Themenbereichen die wirklich brauchbaren Einstellungen heraus.

Achtung: Führen Sie Richtlinien nachträglich ein, bedenken Sie, dass diese nur von Personen gespeichert werden dürfen, denen in der ECL vertraut wird (Punkt »Änderungen in der Ausführungskontrollliste«), andernfalls ruft dies im Notes-Client die Anzeige einer Sicherheitswarnung hervor! Mehr Informationen zur Ausführungskontrollliste (ECL) finden Sie in Kap. 13.9 Ausführungskontrolllisten, ab Seite 362.

6.1.9.1. Sicherheit

Aufgabe

In der Sicherheitsrichtlinie gibt es mehrere große Themenbereiche:

- > Kennwortmanagement/-verwaltung – Kap. 13.3, ab Seite 342
- > Ausführungskontrollliste (Execution Control List) – Kap. 13.9, ab Seite 362
- > Schlüssel und Zertifikate – Kap. 12, ab Seite 319
- > Zuordnung des ID-Vaults – Kap. 6.2, ab Seite 137

Zuordnung

In der Regel organisationsbezogen ganz oben auf Ebene der Unternehmenszulassung, da Sicherheit alle gleich angeht. Ausnahmen für Benutzergruppen, für die strengere Regeln gelten sollen (etwa Administratoren), sind natürlich auch auf Gruppenbasis möglich.

Typ

Dynamische Richtlinie, wird bei jedem Client-Zugriff abgearbeitet.

6.1.9.2. Desktop**Aufgabe**

Setzen von Vorgaben für den Notes-Client, wobei diese als Vorschläge für den Benutzer oder auch zwingend konfiguriert werden können. Außerdem finden sich hier Einstellungen für Automatische Updates und Smart-Upgrade, Widgets, Maileinstellungen und mehr. Über den Bereich Benutzerdefinierte Einstellungen können Sie automatisiert Einträge zur Datei notes.ini der Clients hinzufügen sowie Einstellungen in den lokalen Arbeitsumgebungen setzen.

Zuordnung

In dieser Richtlinie gibt es sowohl standortabhängige Einstellungen (etwa Mail), Einstellungen, die am besten organisationsbezogen ausgerollt werden (die meisten Client-Vorgaben), als auch Einstellungen, die sich auf funktionale Gruppen beziehen (Notebook-Besitzer etc.). Wo Sie Ihre Desktopeinstellung aufhängen, hängt daher vom Bereich ab; bei Bedarf erstellen Sie einfach mehrere Einstellungsdokumente und ordnen Sie verschiedenen Bereichen zu.

Typ

Dynamische Richtlinie, wird bei jedem Client-Zugriff abgearbeitet.

6.1.9.3. Mail**Aufgabe**

Setzen von Vorgaben für die Maildatenbanken der Benutzer, wobei diese als Vorschläge oder auch zwingend konfiguriert werden können.

Zuordnung

Auf welchem Richtlinienbaum man die Maileinstellung am besten aufhängt, darüber könnte man länger diskutieren. Die Mailvorgaben sind eigentlich nicht standortbezogen, sondern variieren (wenn überhaupt) eher von Abteilung zu Abteilung (z. B. Größenbeschränkungen, Ausschlussklauseln). Trotzdem wird von den meisten Administratoren ein Bezug zu einem bestimmten Mailserver hergestellt und eine Zuordnung über eine sogenannte automatisch befüllte Gruppe (Regel Home-Server – siehe Seite 177) vorgenommen. Ich würde eher eine organisationsbezogene Zuordnung präferieren.

Typ

Die Richtlinie wird alle 12 Stunden vom Administrationsprozess aktualisiert bzw. jedes Mal, wenn Sie auf der Serverkonsole folgenden Befehl eingeben:

```
tell adminp proces mailpolicy
```

6.1.9.4. Archivierung

Aufgabe

Erlauben oder Verbieten einer lokalen Archivierung von Maildatenbanken sowie Konfiguration einer serverseitigen Archivierung nach Zeitplan.

Zuordnung

Diese Richtlinie ist eindeutig standortbezogen. Entsprechend können Sie die Archiveinstellung auf jeder Policy aufhängen, die einen Standort abbildet. Meist wird das eine automatisch befüllte Gruppe mit einer Home-Server-Regel sein (siehe Seite 177), eine Zuordnung macht jedoch auch organisationsbezogen Sinn, wenn hinter der OU-Richtlinie ein Standort mit einer bestimmten Serverlandschaft steckt, z. B. */VIE/COB/AT.

Typ

Dynamische Richtlinie, wird beim Client-Zugriff gesetzt

6.1.9.5. Traveler

Aufgabe

Setzt Einstellungen für den Verse-Client für mobile Geräte, meist auf Android oder iOS.

Zuordnung

Diese Richtlinie ist eindeutig standortbezogen. Entsprechend können Sie die Traveler-Einstellung jeder Policy zuordnen, die einen Standort abbildet.

Typ

Die Richtlinie wird alle 6 Stunden vom Administrationsprozess aktualisiert bzw. jedes Mal, wenn Sie auf der Serverkonsole folgenden Befehl eingeben:

```
tell adminp process traveler
```

6.1.9.6. Einrichtung

Aufgabe

Setzen von Vorgaben für den Notes-Client. Da damit nur ein einmaliges Setzen bei der Client-Konfiguration möglich ist und alle Einstellungen (und mehr) außerdem auch in der Desktoprichtlinie vorhanden sind, empfehle ich, eher diese zu verwenden.

Zuordnung

In dieser Richtlinieneinstellung gibt es sowohl standortabhängige Einstellungen (etwa Mail) als auch Einstellungen, die am besten organisationsbezogen ausgerollt werden (die meisten Client-Vorgaben). Wo Sie diese Einstellung aufhängen, hängt daher vom Bereich ab; bei Bedarf erstellen Sie einfach mehrere Einstellungsdokumente und ordnen Sie verschiedenen Bereichen zu.

Typ

Dynamische Richtlinie, wird einmalig bei der Client-Konfiguration abgearbeitet.

6.1.9.7. Connections

Aufgabe

Setzen von Vorgaben zur Anmeldung am Connections-Server.

Zuordnung

Die Einstellungen in dieser Richtlinie werden am besten organisationsbezogen ausgerollt.

Typ

Dynamische Richtlinie, wird bei jedem Client-Zugriff abgearbeitet.

6.1.9.8. Roaming

Aufgabe

Konfiguration eines Dateiserver-Roamings. Bei dieser Art von Roaming handelt es sich um ein typisches Außenstellenszenario, bei dem die Roaming-Dateien nicht auf einen Domino-Server, sondern auf einen Dateiserver hochgeladen werden. (Details zum Domino-Server-Roaming finden Sie in Kap. 6.5 Roaming-Benutzer, ab Seite 157.)

Zuordnung

Die Einstellungen in dieser Richtlinie beziehen sich auf einen Standort und werden in Ermangelung einer passenden OU meist explizit zugeordnet.

Typ

Dynamische Richtlinie, wird bei jedem Client-Zugriff abgearbeitet.

6.1.9.9. Symphony

Diese Richtlinieneinstellung ist seit Domino 9 obsolet, Symphony (ein auf OpenOffice basierendes Büropaket) wurde zuletzt mit Version 8.5.3 ausgeliefert.

6.2. Der ID-Vault

Vault heißt auf Deutsch Tresor, es handelt sich also um einen Tresor für ID-Dateien. (Ob man auf Deutsch *der* oder *die* Vault sagt, konnte ich nicht restlos klären – ich habe mich für die männliche Form entschieden.) Der ID-Vault erlaubt es Administratoren, Notes-IDs besser zu managen und so Supportkosten zu sparen. Nach Aktivierung werden automatisch Kopien aller Benutzer-IDs in den Vault hochgeladen. Damit das möglich ist, müssen zwei Bedingungen erfüllt sein: Erstens, der Zertifizierer der Benutzer-ID muss mit dem Vault ein Gegenzertifikat (Vault Trust Certificate) ausgetauscht haben. Und zweitens, der Benutzer muss via Sicherheitsrichtlinie einen Vault-Namen zugeordnet haben. Wenn der Benutzer die ID am Notes-Client ändert, etwa ein anderes Kennwort setzt oder ein Internet-Zertifikat hinzufügt, werden die Änderungen automatisch in den Vault hochgeladen. Wenn die Änderung in der Kopie im Vault passiert, etwa von einem Admin das Kennwort geändert wird, muss diese umgekehrt vom Notes-Client heruntergeladen werden. Dazu brauchen die Benutzer selbst keine Zugriffsrechte auf den Vault – der Server fungiert hier als Application-Proxy und leitet die Anfragen der Notes-Clients entsprechend weiter.

Die Vorteile des ID-Tresors auf einen Blick:

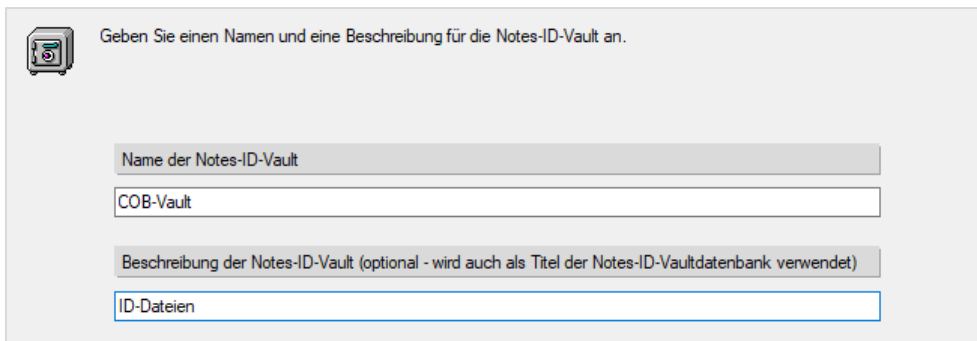
- > Einsammeln und zentrales Speichern aller verwendeten Benutzer-ID-Dateien
- > Bereitstellung der ID-Datei beim Client-Setup
- > Synchronisation von ID-Dateien zwischen Client und Vault (und damit zwischen verschiedenen Clients)
- > zentrale Kennwortzurücksetzung durch Administratoren im Domino-Administrator
- > Zurücksetzen des Kennworts über eine Anwendung (Beispielanwendung »Sample Web Agent - Reset User Password« – pwdresetsample.nsf wird mitgeliefert.)
- > automatisches Wiederherstellen verloren gegangener ID-Dateien beim Start des Notes-Clients
- > keine Benutzerbestätigung mehr beim Umbenennen oder beim Austauschen des Zertifikats (Key Rollover)
- > Extrahieren von ID-Dateien für Administratoren mit der Rolle [Auditor], etwa um den Zugriff auf verschlüsselte Daten zu ermöglichen

6.2.1. Einen ID-Vault einrichten

Wechseln Sie im Administrator-Client auf das Register **Konfiguration** und wählen Sie **Werkzeuge** > **ID-Vaults** > **Erstellen...** Der ID-Vault-Assistent wird aufgerufen.

Die erste Seite enthält eine Übersicht über die Funktionalität des ID-Vaults und kann durch Setzen eines Häkchens bei **Dieses Fenster zukünftig nicht mehr anzeigen** ausgeblendet werden.

Geben Sie auf der zweiten Seite (als Schritt 1 bezeichnet) einen Namen für Ihren ID-Vault ein:



Geben Sie einen Namen und eine Beschreibung für die Notes-ID-Vault an.

Name der Notes-ID-Vault
COB-Vault

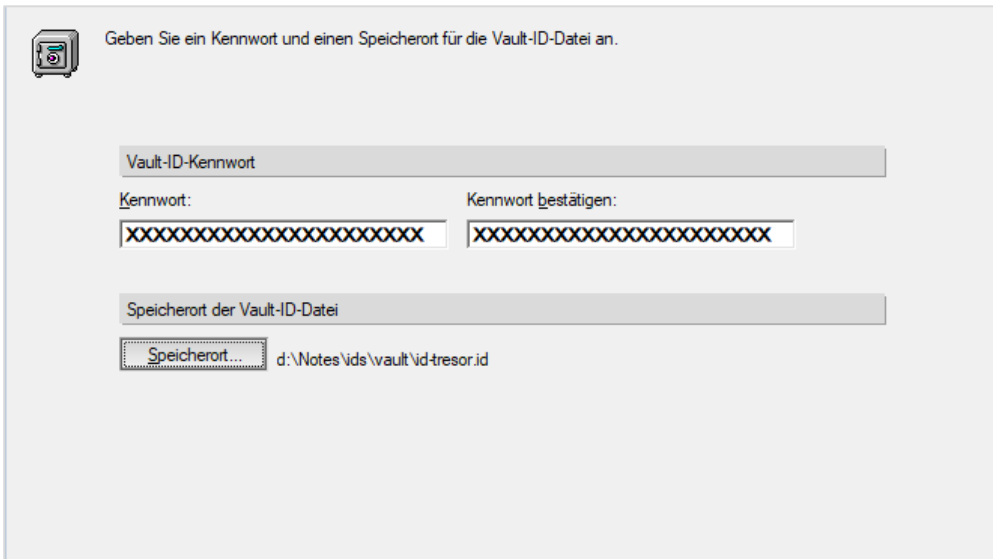
Beschreibung der Notes-ID-Vault (optional - wird auch als Titel der Notes-ID-Vaultdatenbank verwendet)
ID-Dateien

Abbildung 6.11: Schritt 1 – Name des ID-Vaults

Achtung: Da später eine Vertrauensstellung zwischen dem ID-Vault und Ihrer Notes-Organisation aufgebaut wird, müssen sich die beiden Namen voneinander unterscheiden.

Die Beschreibung ist optional; geben Sie hier etwas ein, wird es als Datenbanktitel verwendet. Geben Sie nichts ein, wird der Vault-Name als Datenbanktitel verwendet. Klicken Sie auf **Weiter** >.

Geben Sie ein Kennwort für die Vault-ID ein; dieses muss mindestens 10 Zeichen lang sein. Wählen Sie außerdem einen Speicherort für die Vault-ID-Datei aus:



Geben Sie ein Kennwort und einen Speicherort für die Vault-ID-Datei an.

Vault-ID-Kennwort

Kennwort: Kennwort bestätigen:

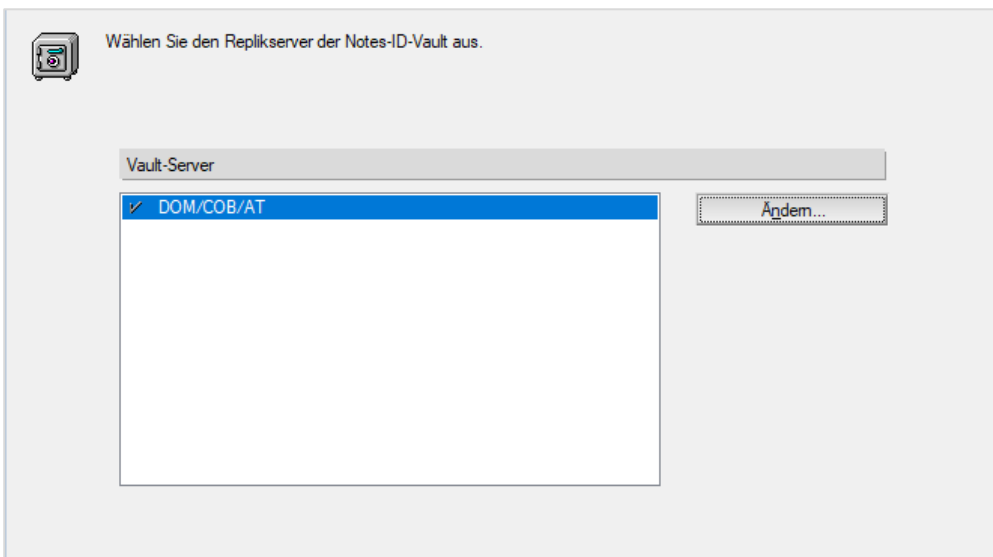
Speicherort der Vault-ID-Datei

Speicherort... d:\Notes\ids\vault\id-tresor.id

Abbildung 6.12: Schritt 2 – Kennwort für die Vault-ID

Klicken Sie auf **Weiter >**.

Wählen Sie im nächsten Schritt den ersten Replikserver für den ID-Vault aus. (Sie können später weitere Server hinzufügen; zumindest auf den Mailservern sollte eine Vault-Replik liegen.)



Wählen Sie den Replikserver der Notes-ID-Vault aus.

Vault-Server

DOM/COB/AT

Ändern...

Abbildung 6.13: Schritt 3 – Einen Replikserver wählen

Egal, mit welchem Server Sie im Admin-Client zurzeit verbunden sind, der ID-Vault wird immer zuerst auf dem Administrationsserver des Domino-Verzeichnisses eingerichtet.

In nächsten Schritt müssen Sie einen ID-Vault-Administrator auswählen:

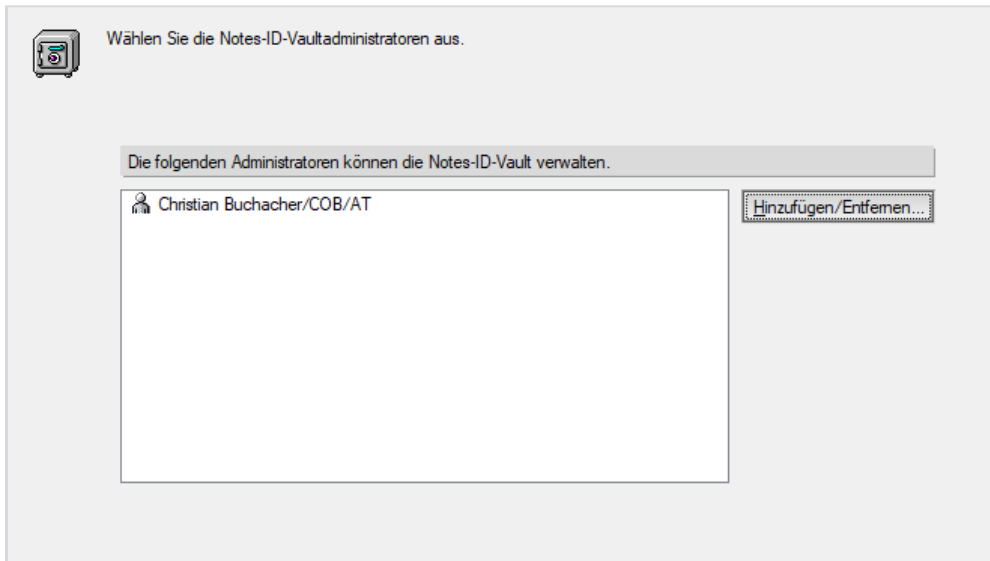


Abbildung 6.14: Schritt 4 – Die ID-Vault-Administratoren wählen

Es werden nur Personen angeboten, die gleichzeitig Serveradministratoren sind (also im Serverdokument im Feld **Administratoren** stehen).

Die gewählten Personen werden in der ACL als Manager eingetragen, gleichzeitig wird die Admin-Gruppe »LocalDomainAdmins« ohne Zugriff hinzugefügt. Damit wird verhindert, dass alle Mitglieder automatisch zu Vault-Administratoren werden.

Die gewählten Vault-Administratoren werden außerdem im Vault-Dokument eingetragen. Vault-Administratoren können Änderungen am Vault selbst vornehmen, einschließlich:

- > Hinzufügen oder Entfernen anderer Administratoren
- > Hinzufügen oder Entfernen von Zertifizierern
- > Erstellen oder Löschen von ID Vault-Repliken

Sie müssen niemandem Administratorrechte erteilen, wenn er lediglich Kennwörter für Benutzer zurücksetzen soll.

Klicken Sie auf **Weiter** >.

Wählen Sie nun die Organisation und alle Unterorganisationen, deren Notes-IDs in diesem ID-Vault verwaltet werden sollen.

Gibt es in Ihrem Unternehmen mehrere Notes-Organisationen, können Sie alle auswählen, bedenken Sie jedoch, dass dann die ID-Dateien der Benutzer aus allen Organisationen in ein und derselben Datenbank aufbewahrt werden.

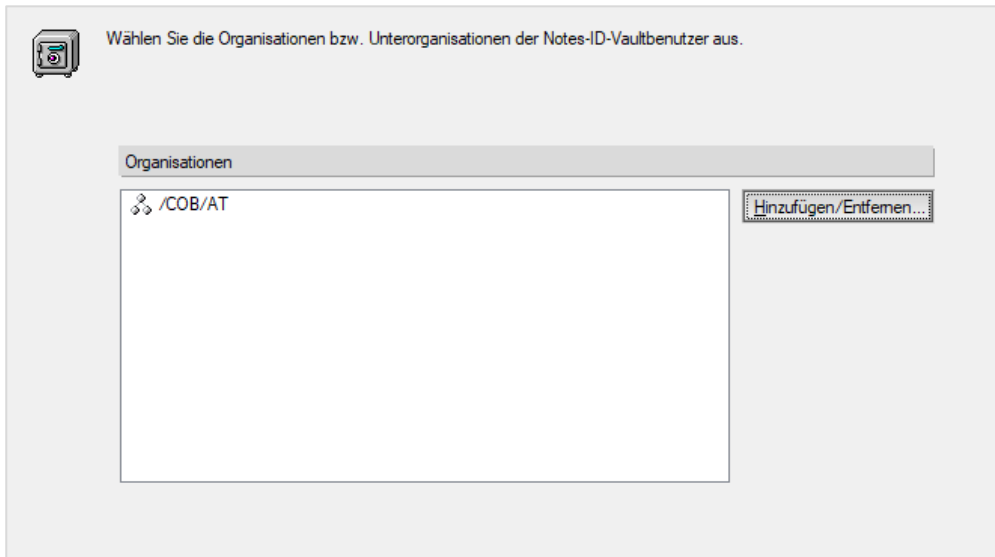


Abbildung 6.15: Schritt 5 – Die Organisation wählen

Beachten Sie auch, dass Sie zum Erstellen der Querkzulassung am Ende die ID-Dateien jeder gewählten Organisation und Unterorganisation einzeln öffnen und das Kennwort eintippen müssen.

Klicken Sie auf **Weiter** >.

In Schritt 6 definieren Sie, welche Personen für welche Organisationen (oder Unterorganisationen) Kennwörter zurücksetzen dürfen. Wählen Sie die gewünschten Personen aus und klicken Sie auf die Schaltfläche **Hinzufügen**:

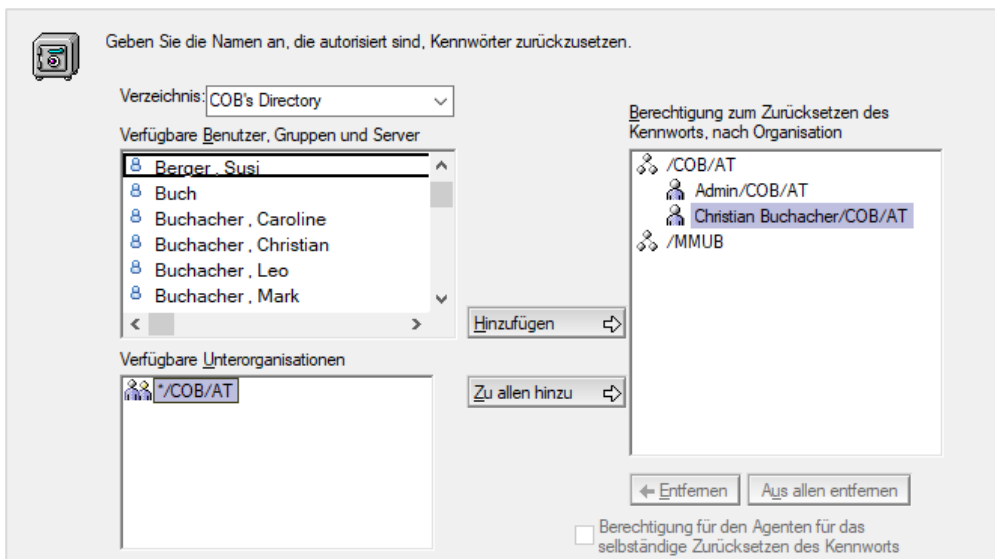


Abbildung 6.16: Schritt 6 – Kennwortzurücksetzungsstellen wählen

Die Betonung liegt auf Personen, denn es wird später eine Vertrauensstellung zwischen den gewählten Personen und dem ID-Vault aufgebaut (sogenannte Kennwortzurücksetzungszertifikate), und

dafür ist ein Schlüssel nötig. Gruppen verfügen über keine ID-Dateien und daher über keine Schlüssel. Wählen Sie trotzdem eine Gruppe aus, werden Sie informiert, dass diese in ihre Mitglieder aufgelöst wird:

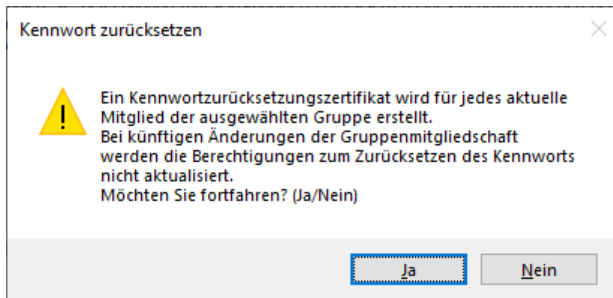


Abbildung 6.17: Infodialog beim Hinzufügen zu Gruppen

Setzen Sie zusätzlich ein Häkchen im Feld **Berechtigung für den Agenten für das selbständige Zurücksetzen des Kennworts**, kann der Benutzer später die Self-Service-Anwendung (siehe Kap. 6.6.2, ab Seite 162) benutzen, um selbst ein neues Kennwort zu vergeben.

Im nächsten Schritt werden Sie gefragt, ob der neue ID-Vault in eine bereits existierende Sicherheitsrichtlinie aufgenommen oder eine neue erstellt werden soll.

Wenn Sie noch keine Sicherheitsrichtlinie erstellt haben, wählen Sie die Option »Neue Richtlinie erstellen, die einer Organisation zugewiesen wird«. Wollen Sie den neuen ID-Vault in eine bestehende Sicherheitseinstellung aufnehmen, wählen Sie »Vorhandene Richtlinie bearbeiten«. Wollen Sie die Sicherheitseinstellung später selbst erstellen, wählen Sie »Ich werde eine Notes-ID-Vault-Richtlinie zu einem späteren Zeitpunkt erstellen«.

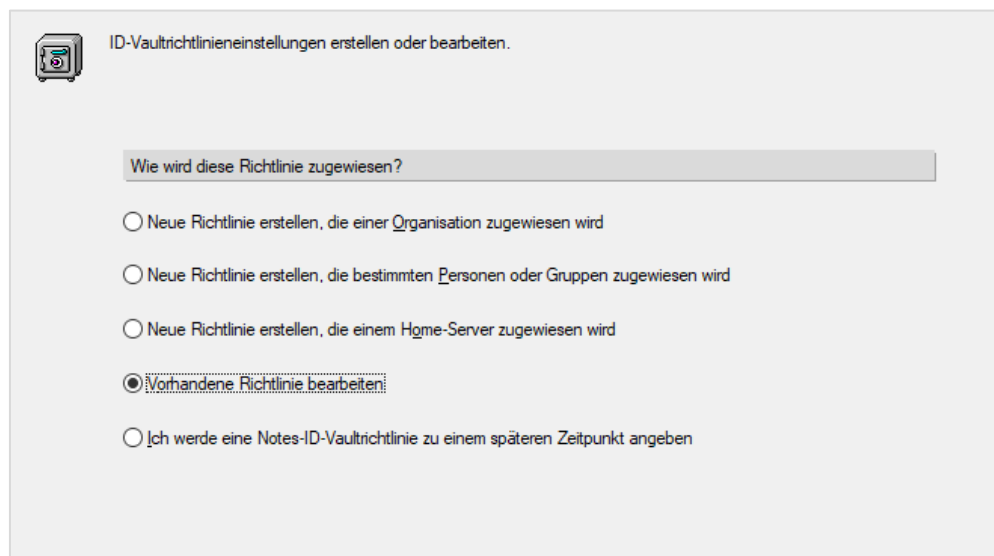


Abbildung 6.18: Schritt 7 – Richtlinie zuweisen

Haben Sie »Vorhandene Richtlinie bearbeiten« gewählt, können Sie diese im nächsten Schritt auswählen. Klicken Sie zuerst auf die Schaltfläche **Einstellungen erstellen**, damit die Schaltfläche **Weiter** angezeigt wird:

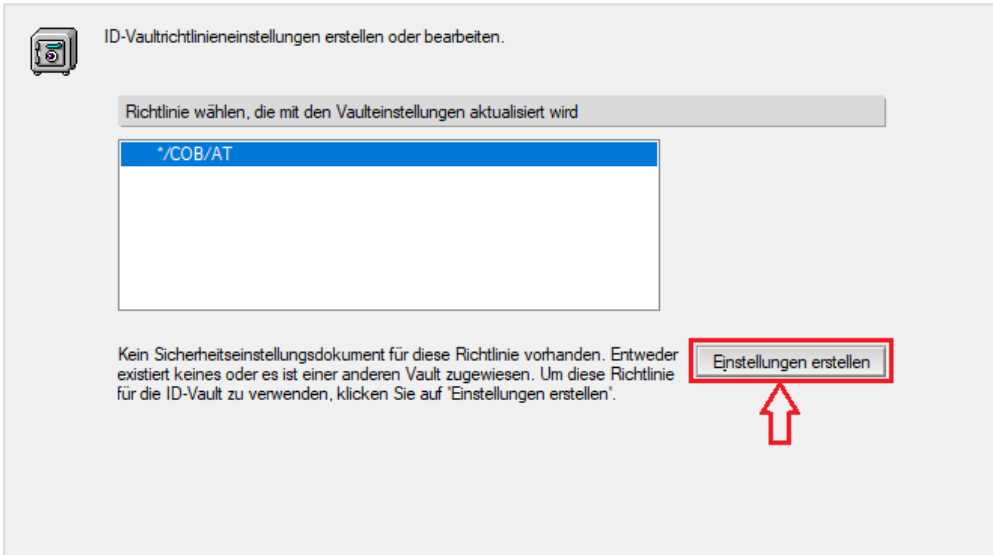


Abbildung 6.19: Schritt 8 – Mit Schaltfläche Einstellung erstellen

Klicken Sie auf **Vault erstellen**.

Sie werden aufgefordert, einen Hilfetext einzugeben, der Benutzern angezeigt wird, die ihr Kennwort vergessen haben:

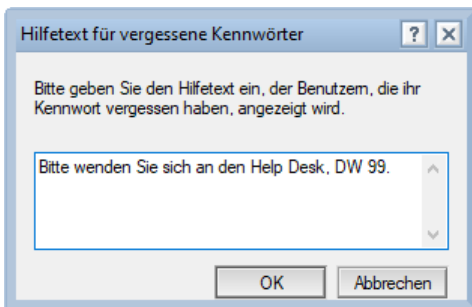


Abbildung 6.20: Schritt 8 – Hilfetext eingeben

Sie können bis zu 8 Zeilen (auch Leerzeilen) verwenden. Es ist auch möglich, mittels HTML-Link auf eine Anwendung zu verweisen, in der Benutzer ihr Kennwort selbst zurücksetzen können. (Ein Beispiel für eine solche Anwendung ist unter dem Namen PwdResetSmple.nsf im Lieferumfang enthalten.) Achten Sie darauf, dass der HTML-Code wohl formatiert ist:

```
<A HREF="http://IhrServer.de/passwordreset.nsf">Ihr Text</A>
```

Der Link wird dann im Anmeldedialog im Bereich **Kennwort vergessen?** angezeigt:

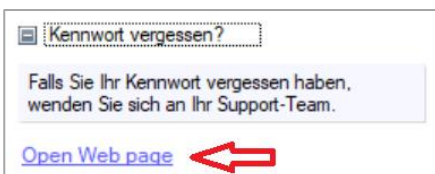


Abbildung 6.21: Der Bereich Kennwort vergessen im Anmeldedialog mit Weblink

Am Ende wird eine Zusammenfassung angezeigt. Überprüfen Sie Ihre Auswahl. Sollte etwas nicht passen, können Sie zurücknavigieren und die Einstellungen ändern. Sowie Sie die Zusammenfassung bestätigen, werden Sie aufgefordert, für jede einzelne angegebene Organisation und Unterorganisation die ID-Datei auszuwählen und das Kennwort einzugeben.

6.2.1.1. Den ID-Vault inspizieren

Den neuen ID-Vault finden Sie im Verzeichnis IBM_ID_VAULT unter dem von Ihnen angegebenen Dateinamen. Das dazu passende Vault-Dokument finden Sie im Domino-Administrator unter **Konfigurationen > Sicherheit > ID-Vaults**:

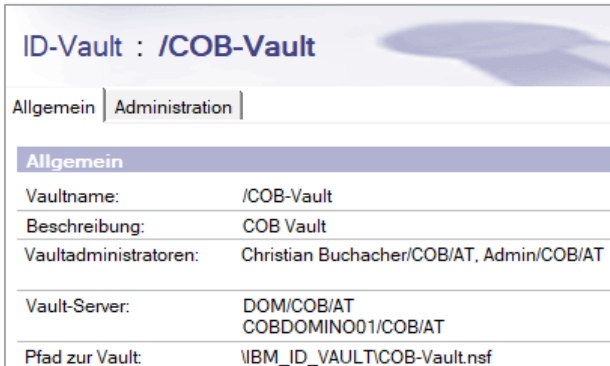


Abbildung 6.22: Das ID-Vault-Dokument im Domino-Verzeichnis

Weiters wurde in die von Ihnen ausgewählte Sicherheitsrichtlinie der Name des Vaults (beachten Sie den Schrägstrich am Beginn!) und der Hilfetext eingetragen:

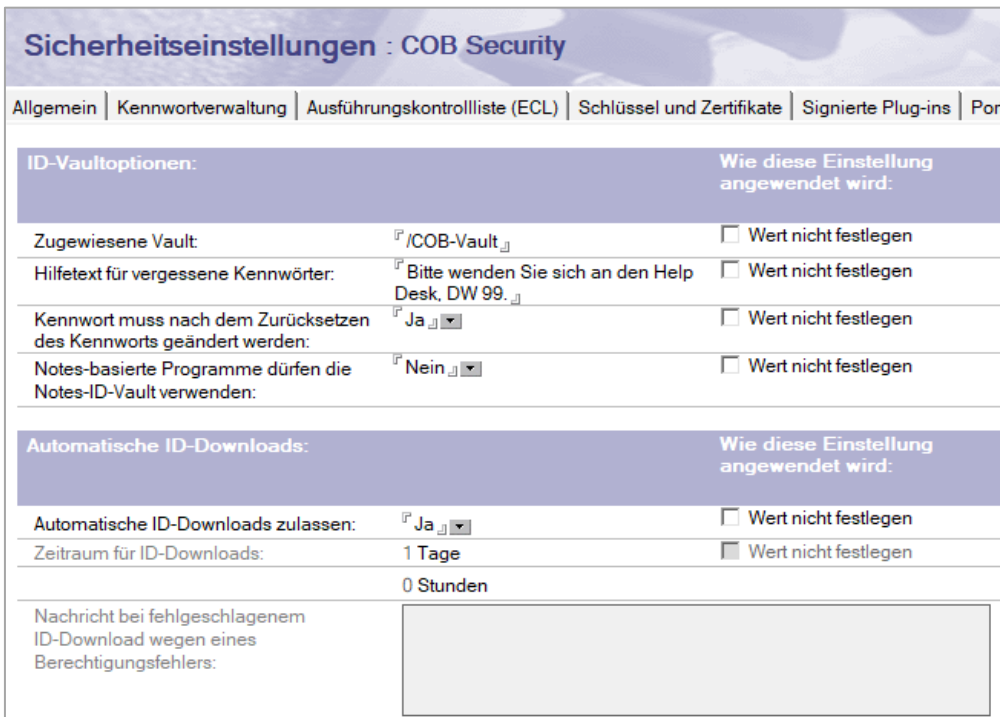


Abbildung 6.23: Sicherheitsrichtlinie, Register ID-Vault

6.2.1.2. Erstellte Zertifikate inspizieren

Die erstellten Zertifikate finden Sie im Domino-Verzeichnis, in der Ansicht **Sicherheit > Zertifikate**. Hier das Vault-Zertifikat (Vault Certificate):

Allgemein	
Zertifikatstyp:	Notes-Gegenzertifikat
Ausgestellt von:	/COB/AT
Ausgestellt auf:	/COB-Vault
Alternative Namen:	
Kombinierter Name:	O=COB/C=AT:VT:O=COB-Vault
Kommentar:	
Organisationen:	O=COB/C=AT:VT:O=COB-Vault
Bezeichner des primären Schlüssels:	1N92W D9KJC 8ATEX HCHTX UH4Y7 5741F
Bezeichner des internationalen Schlüssels:	1N92W D9KJC 8ATEX HCHTX UH4Y7 5741F
Aktuelle Schlüsselstärke:	Mit Version 7.0 und höher kompatibel (2048 Bit)

Abbildung 6.24: Vault-Zertifikat

Und hier das Kennworrücksetzungszertifikat (Password Reset Certificate):

Allgemein	
Zertifikatstyp:	Notes-Gegenzertifikat
Ausgestellt von:	/COB/AT
Ausgestellt auf:	Christian Buchacher/COB/AT
Alternative Namen:	
Kombinierter Name:	O=COB/C=AT:PR:CN=Christian Buchacher/O=COB/C=AT
Kommentar:	
Organisationen:	O=COB/C=AT:PR:O=COB/C=AT
Bezeichner des primären Schlüssels:	1NA82 SU2ZU 5SV9N 4P8PC 8D2UU A2413
Bezeichner des internationalen Schlüssels:	1NA82 SU2ZU 5SV9N 4P8PC 8D2UU A2413
Aktuelle Schlüsselstärke:	Mit Version 6.0 und höher kompatibel (1024 Bit)

Abbildung 6.25: Kennworrücksetzungszertifikat

Wenn Sie nicht mehr wollen, dass ein Benutzer weiterhin Kennwörter zurücksetzen kann, müssen Sie nur dieses Dokument löschen!

Nach der Aktivierung werden die ID-Dateien all jener Benutzer, die die Sicherheitsrichtlinie zugewiesen bekommen haben, nach und nach in den Vault aufgenommen. Damit nicht alle Notes-Clients gleichzeitig ihre IDs hochladen und den Server damit in die Knie zwingen, geschieht dies zu einer zufällig bestimmten Zeit innerhalb der ersten acht Stunden nach dem Client-Start.

Ein Hochladen der ID auf Knopfdruck gibt es nicht. Die einzige Methode, diesen Vorgang zu beschleunigen, besteht darin, zu einer anderen ID und wieder zurück zu wechseln. (Sofern Sie eine

andere ID haben.) Wählen Sie dazu den Befehl **Datei > Sicherheit > ID wechseln...** Meist steht danach nicht nur die andere ID, sondern auch die eigene im Vault.

Ist die ID einmal hochgeladen, können Sie ein Synchronisieren erzwingen: Öffnen Sie dazu über **Datei > Sicherheit > Benutzersicherheit** Ihre Sicherheitseinstellungen und klicken Sie im Bereich **Ihre Einstellungen zu Anmeldung und Kennwort** auf die Schaltfläche **Synchronisierung der ID-Vault**:

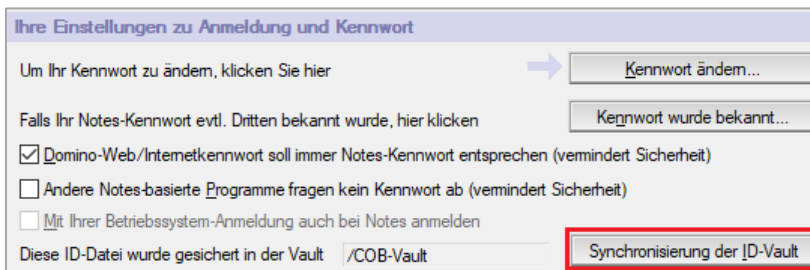


Abbildung 6.26: ID-Eigenschaften – Synchronisierung mit dem ID-Vault

6.2.2. Die ID-Synchronisierung überwachen

Einer der großen Vorteile des ID-Vaults ist die Kennwort-Synchronisation zwischen Client und Vault. Diese ermöglicht, dass der Benutzer das Kennwort auf einem Client ändert und dann auf einem anderen bereits das neue Kennwort eingeben kann. Wenn der Notes-Client feststellt, dass das eingegebene Kennwort nicht zur lokalen ID passt, aber zu derjenigen im Vault, lädt er diese automatisch herunter.

Wenn sich jedoch das Kennwort der ID im Vault vom Kennwort der ID am Notes-Client unterscheidet, stoppt die Synchronisation, und Neuerungen, etwa ein neu erworbener Geheimschlüssel, werden nicht mehr in den Vault übertragen.

Dass die Kennwörter nicht mehr übereinstimmen, kann folgende Gründe haben:

- > Der Administrator hat das Kennwort im ID-Vault geändert, der Benutzer aber das alte Kennwort weiterverwendet.
- > Der Benutzer hat das Kennwort geändert und auch erfolgreich mit dem ID-Vault synchronisiert, dann aber eine alte ID-Datei auf demselben oder einem anderen Notes-Client mit einem anderen Kennwort verwendet.

6.2.2.1. Die automatische ID-Archivierung aktivieren

Nach 7 Tagen ohne Synchronisation wird die alte ID-Datei archiviert (Name: »~<Benutzername>«) und die aktuelle ID-Datei wieder in den Vault aufgenommen. Jetzt geht die Synchronisierung weiter.

Dieses Verhalten ist jedoch nicht Standard, sondern wird erst durch Setzen der folgenden notes.ini-Variable aktiviert:

```
ENABLE_AUTORECOVERY_FROMBADPASSWORD=1
```

Wie das funktioniert? – Wenn die Synchronisation wegen eines abweichenden Passworts zum ersten Mal fehlschlägt, wird dieser Fehlschlag im Benutzerdokument in der Vault-Datenbank mit dem Datum markiert. Wenn die Synchronisation nach sieben Tagen immer noch fehlschlägt, wird der Name mit einer Tilde (~) versehen und das Dokument archiviert. Bei der nächsten Synchronisation stellt Notes fest, dass die ID im Vault fehlt und lädt die lokale hoch.

6.2.3. Den ID-Vault durchsuchen

Spätestens zwei Wochen nach Einführung des ID-Vaults fragt man sich als Administrator unweigerlich, ob alle Benutzer ihre IDs bereits hochgeladen haben. Früher hätte man sich zum Überprüfen einen Agenten geschrieben, seit Domino 10 können Sie auch das Programm **Query Vault** (qvault) beauftragen, einen Vault-Scan durchzuführen.

Query Vault durchsucht den angegebenen ID-Vault und aktualisiert für jeden gefundenen Benutzer das Personendokument im Domino-Verzeichnis. Das Ergebnis des Scans sehen Sie direkt in der Ansicht Personen, wo in der Spalte **ID-Vault** der Name des Vaults und in der Spalte **Vault-Synchronisierung** Datum und Uhrzeit der letzten erfolgreichen Synchronisation angezeigt werden:



E-Mail	Mail-Server ^	ID-Vault	Vault-Synchronisierung ^
Admin/COB/AT@COB	DOM/COB/AT	 /COB-Vault	08.10.2018 00:09
Susi Berger/COB/AT@COB	DOM/COB/AT		
Christian Buchacher/COB/AT@COB	DOM/COB/AT	 /COB-Vault	27.03.2020 17:12
Leo Buchacher/COB/AT@COB	DOM/COB/AT		

Abbildung 6.27: Ansicht Personen, Spalte ID-Vault nach einem Vault-Query

Der Scan kann via Konsolenbefehl bzw. im Domino-Administrator auch über die Werkzeuge beauftragt werden.

6.2.3.1. Das Scannen des ID-Vaults auf der Serverkonsole beauftragen

Aktivieren Sie diese Funktion zuerst durch Setzen des folgenden notes.ini-Parameters:

```
IDV_Enable_Vault_Scan=1
```

Geben Sie danach auf der Serverkonsole des ID-Vault-Administrationsservers einen der folgenden Befehle ein:

Schalter	Beschreibung
load qvault	Scannt alle Benutzer in allen Vaults, die im Verzeichnis IBM_ID_VAULT auf dem Server gefunden werden.
load qvault -x <Vault>	Scannt alle Benutzer in einem bestimmten Vault
load qvault -x <Vault> -u <Benutzer>	Scannt den angegebenen Benutzer im angegebenen Vault.
load qvault -x <Vault> -u <Benutzer> -a	Archiviert die angegebene Benutzer-ID im angegebenen Vault. Die ID wird bei der nächsten Synchronisation erneut in den Vault hochgeladen.
load qvault -x <Vault> -u <Benutzer> -r	Konvertiert die angegebene Benutzer-ID in ihren ursprünglichen Namen zurück
load qvault -x <Vault> -u <Benutzer> -d	Löscht die angegebene Benutzer-ID
load qvault -x <Vault> -d	Löscht alle archivierten Benutzer-IDs aus dem angegebenen Vault

Tabelle 6.8: Die verschiedenen Schalter des Tasks qvault.

6.2.3.2. Das Scannen des ID-Vaults im Domino-Administrator beauftragen

Das Scannen des ID-Vaults ist auch im Domino-Administrator möglich. Wenn Sie einen ganzen Vault scannen wollen, navigieren Sie zu **Konfiguration > Sicherheit > ID-Vaults** und wählen Sie das gewünschte ID-Vault-Dokument.

Klicken Sie auf **Werkzeuge > ID-Vaults > Tresor scannen**.

Wenn Sie nur einen einzelnen Benutzer scannen wollen, navigieren Sie zu **Personen und Gruppen > Personen** und wählen Sie die gewünschte Person in der Liste.

Klicken Sie auf **Werkzeuge > ID-Vaults > Tresor scannen**.

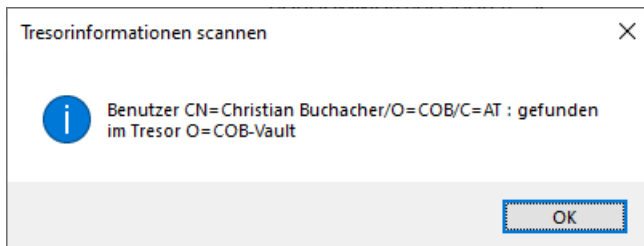


Abbildung 6.28: Tresorinformationen scannen

6.2.3.3. Protokollierung

Im Serverprotokoll (log.nsf) finden Sie in der Ansicht Sicherheits-Ereignisse (Security Events) Informationen zum ID-Vault. Hier wird unter anderem angezeigt:

- > Das Synchronisieren von ID-Dateien vom Client mit dem Vault
- > Das Extrahieren von ID-Dateien
- > Das Zurücksetzen von Kennwörtern

ID-Synchronisationen werden außerdem in der Protokolldatei (log.nsf) am Client angezeigt.

Zusätzlich können Sie auf der Serverkonsole mit dem folgenden Befehl Informationen über den ID-Vault abfragen:

```
show idvault
```

Sie erhalten eine Ausgabe ähnlich jener auf meinem Server:

```
ID Vault /COB-Vault (IBM_ID_VAULT\COB-Vault.nsf)
Control Vault Name: /COB-Vault
Control Vault Servers: DOM/COB/AT
Control Vault Servers: WEB/COB/AT
Vault Operations Key: VO-stel-bahq/DOM/COB-Vault
Servers: WEB/COB/AT
Servers: DOM/COB/AT
Vault Name: /COB-Vault
Description: COB Vault
Administrators: Christian Buchacher/COB/AT
Administrators: Admin/COB/AT
Servers: DOM/COB/AT
```

```

Servers: WEB/COB/AT
Administration Server: DOM/COB/AT
Administration Server: WEB/COB/AT
/COB/AT trusts this vault
/COB/AT trusts Christian Buchacher/COB/AT to reset passwords
/COB/AT trusts Admin/COB/AT to reset passwords
Setting COB Security uses this vault

```

6.3. Eine serverbasierende Zulassungsstelle einrichten

Bei der Konfiguration des ersten Servers wurde die Unternehmenszulassungsdatei cert.id im Domino-Datenverzeichnis abgelegt und sollte von dort schnellstmöglich in Sicherheit gebracht werden. Mit dieser Zertifizierer-ID können Organisationseinheiten oder auch direkt Personen und Server registriert werden. Dafür muss man allerdings Zugriff auf die ID-Datei haben und ihr Kennwort wissen, was nicht immer und überall leicht zu bewerkstelligen ist.

Alternativ können Sie eine serverbasierende **Domino-Zulassungsstelle** einrichten. Diese ermöglicht es, ohne Zugriff auf die Zertifizierer-ID und ohne Eingabe eines Kennworts Benutzer, Server und Organisationseinheiten zu registrieren. Beim Einrichten einer serverbasierenden Zulassungsstelle wird der gewünschte Notes-Zertifizierer aus der ID-Datei in eine Notes-Datenbank migriert, welche **ICL** (Issued Certificate List) genannt wird. Dabei können Sie festlegen, welche Administratoren für welche ICL eine Registrierungsberechtigung haben sollen. Nach der Migration ist eine Registrierung sogar über den Domino-Webadministrator möglich (siehe auch Kap. 14.8, ab Seite 409).

Die migrierten Zertifizierer werden von einem eigenen Servertask, dem **CA-Prozess** (für Certificate Authority) verwaltet. Auf jedem Server kann nur eine Instanz des CA-Prozesses laufen, dieser kann jedoch mit mehreren Zertifizierern verknüpft werden.

6.3.1. Einen Notes-Zertifizierer migrieren

Voraussetzung ist, dass Sie den Zertifizierer auf herkömmliche Weise registriert und Zugriff auf die dabei entstandene Zertifizierer-ID haben sowie ihr Passwort kennen.

Um einen Zertifizierer zu migrieren, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Konfiguration**.
2. Wählen Sie in den Werkzeugen den Befehl **Zertifizierung > Zertifizierer migrieren**.
3. Klicken Sie im angezeigten Dialog auf die Schaltfläche **Auswählen...**
4. Wählen Sie die gewünschte Zertifizierer-ID aus, z. B. die Datei cert.id, und klicken Sie auf **OK**.
5. Geben Sie das Kennwort für die ID-Datei ein.
6. Der Dialog **Migrieren** wird angezeigt (siehe Abbildung 6.29). Wählen Sie den Server aus, auf dem der gewählte Zertifizierer ausgeführt werden soll.
7. Es wird automatisch ein Name für die Datenbank im Unterverzeichnis ICL vergeben. Ändern Sie bei Bedarf den Dateinamen (z. B. in den Namen des Zertifizierers, etwa: icl\icl_cob.nsf), bleiben Sie jedoch im Unterverzeichnis ICL.
8. Wählen Sie eine der verfügbaren Schutzmaßnahmen für den Zertifizierer, entweder die Verschlüsselung über eine Sperr-ID oder ein Kennwort.

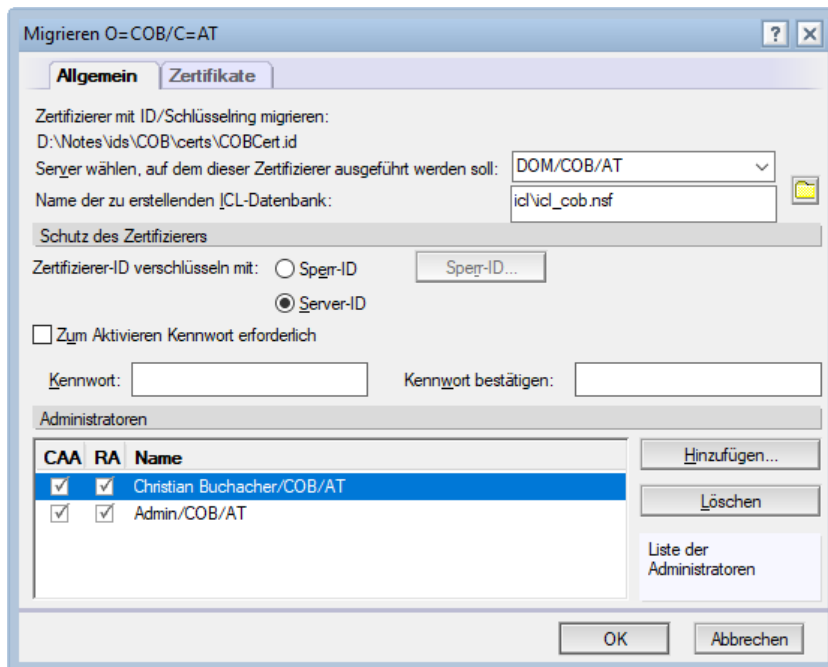


Abbildung 6.29: Notes-Zertifizierer migrieren, Register Allgemein

Wählen Sie die Verschlüsselung über die Server-ID, sind später keinerlei Maßnahmen zur Verwendung des Zertifizierers erforderlich.

Wählen Sie die Verschlüsselung über eine Sperr-ID, müssen Sie den Zertifizierer später vor jeder Verwendung mit dem folgenden Befehl entsperren:

```
tell ca unlock <Kennwort der ID-Datei>
```

Geben Sie ein Kennwort ein, müssen Sie den Zertifizierer später vor jeder Verwendung mit dem folgenden Befehl aktivieren:

```
tell ca activate <Kennwort>
```

9. Fügen Sie jene Administratoren hinzu, die das Recht haben sollen, mit diesem Zertifizierer Benutzer und Server zu registrieren.
10. (Optional) Wechseln Sie zum Register **Zertifikate** (siehe Abbildung 6.30).

Hier können Sie die Gültigkeitsdauer von Zertifikaten ändern. Unter EE-Zertifikaten (für End-Entity) versteht man Benutzer und Server.

11. Klicken Sie auf **OK**, um die Datenbank zu erstellen.

Der migrierte Zertifizierer steht erst zur Verfügung, wenn er vom Administrationsprozess im Domino-Verzeichnis in das Zertifiziererdokument eingetragen wurde. Diese Anforderung wird vom Administrationsserver des Domino-Verzeichnisses mit dem Planungstyp »sofort« abgearbeitet, muss aber, je nachdem wo Sie die Anforderung eingereicht haben, ev. erst dorthin repliziert werden.

12. Laden Sie den CA-Prozess, etwa durch den Befehl:

```
load ca.
```

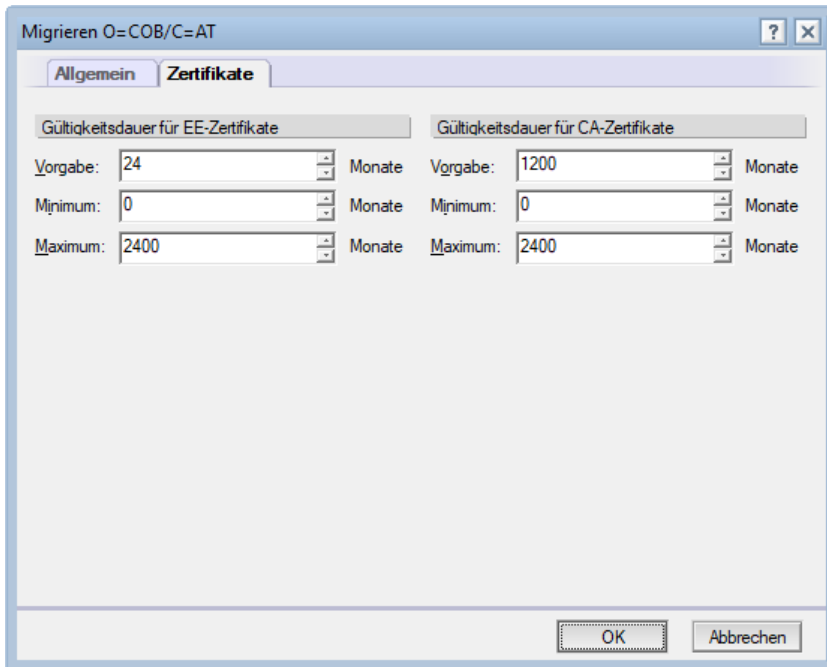


Abbildung 6.30: Notes-Zertifizierer migrieren, Register Zertifikate.

- Sorgen Sie dafür, dass der CA-Task bei jedem Neustart des Domino-Servers automatisch geladen wird, etwa durch Erstellen eines Programmdokuments oder durch Erweitern der Zeile `Servertasks=` in der Datei `notes.ini` des Servers.

Sowie der Administrationsprozess fertig ist, steht der migrierte Zertifizierer zum Registrieren von Benutzern, Servern und Organisationseinheiten bereit:

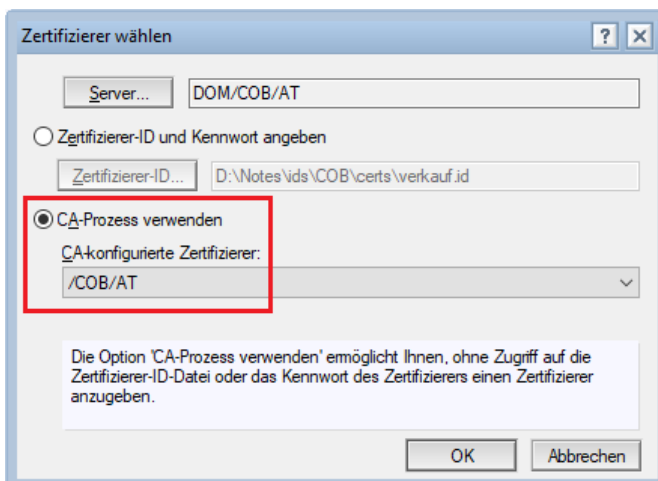


Abbildung 6.31: Dialog Zertifizierer wählen: CA-Prozess verwenden

Mit dem CA-Prozess können Sie Benutzer auch über den Webadministrator registrieren. (Mehr Details zum Domino-Webadministrator finden Sie Kap. 14.8 Der Domino-Webadministrator, ab Seite 409.)

6.4. Notes-Benutzer anlegen

Damit haben wir alle Voraussetzungen geschaffen, um Notes-Benutzer zu erstellen. Da Notes-Benutzer zum Anmelden im Notes-Client eine ID-Datei benötigen, können Sie im Domino-Verzeichnis nicht einfach über die Schaltfläche **Person hinzufügen** erstellt, sondern müssen mit einem gültigen Zertifizierer **registriert** werden.

Anders ist das bei Webbenutzern, etwa für die Protokolle HTTP, POP3 oder IMAP, diese können zwar ebenfalls über den Registrierdialog angelegt (Sie brauchen nur das Häkchen bei **Notes-ID für diesen Benutzer erstellen** wegnehmen), aber auch händisch im Verzeichnis erstellt werden. In diesem Fall müssen Sie jedoch wirklich alles selbst erledigen, etwa eine Maildatenbank für den Benutzer anlegen und die Rechte zuordnen.

6.4.1. Benutzer einzeln registrieren

1. Starten Sie den Domino-Administrator.
2. Navigieren Sie zum Register **Konfiguration**, klappen Sie die Werkzeuge auf und wählen Sie **Registrierung > Person...**
3. Haben Sie den Zertifizierer in den Admin-Vorgaben hinterlegt, werden Sie zur Eingabe des Kennworts aufgefordert.

Haben Sie den Zertifizierer nicht hinterlegt oder **Abbrechen** gewählt, werden Sie zur Auswahl einer Zertifizier-ID-Datei oder eines CA-konfigurierten Zertifizierers aufgefordert. Wählen Sie den gewünschten Zertifizierer über die Schaltfläche **Zertifizierer-ID...** oder wählen Sie wie in Abbildung 6.31 dargestellt die Option »CA-Prozess verwenden« und einen Eintrag aus der Liste der CA-konfigurierten Zertifizierer.

4. Der Dialog **Person registrieren** wird angezeigt (siehe Abbildung 6.32). Setzen Sie ein Häkchen bei **Erweitert**, um alle Registerkarten zu sehen.
5. Geben Sie den Namen des Benutzers ein. Bei generischen Benutzerkonten genügt die Angabe eines Nachnamens (z. B. »Office« oder »Admin«). Alle Namenskomponenten zusammen dürfen nicht länger als 80 Zeichen sein.
6. Geben Sie ein Kennwort ein. Länge und Komplexität müssen den voreingestellten Kennwortrichtlinien entsprechen (siehe dazu auch Kap. 13.3 ID-Sicherheit, ab Seite 342).
7. Bleiben Sie im Feld **Mailsystem** bei der Option »HCL Notes«.
8. Haben Sie eine **Explizite Richtlinie** erstellt, kann diese nun ausgewählt werden.
9. Setzen Sie bei Bedarf ein Häkchen im Feld **Roaming für diesen Benutzer aktivieren**. Mehr Informationen zum Thema Roaming finden Sie in Kap. 6.5 Roaming-Benutzer, ab Seite 157.

Haben Sie, wie in Kap. 6.1.8 auf Seite 127 beschrieben, eine Registrierungsrichtlinie erstellt, sollten alle weiteren Einstellungen bereits gesetzt sein. Wir wollen sie an dieser Stelle aber dennoch durchgehen.

10. Wechseln Sie zum Register **Mail** (siehe Abbildung 6.33).
11. Ändern Sie bei Bedarf über die Schaltfläche **Mail-Server...** den Server, auf dem die Maildatei des Benutzers gespeichert werden soll.

Wenn Sie über eine langsame Verbindung verfügen (sich z. B. über VPN eingewählt haben), aktivieren Sie **Im Hintergrund erstellen**.

Abbildung 6.32: Der Registrierdialog, Register Allgemein

12. Akzeptieren Sie den vorgeschlagenen Namen für die Maildatei (Vorgabe ist ein Zeichen des Vornamens plus maximal 7 Zeichen des Nachnamens) oder geben Sie einen neuen Namen ein. (Die Namensregeln zum Erstellen der Maildatenbank können derzeit nicht via Richtlinie vorgegeben werden.)
13. Akzeptieren Sie als Mailschablone »Mail 11« (mail11.ntf) oder wählen Sie eine andere aus der Liste.
14. Erstellen Sie bei Bedarf über die Schaltfläche **Maildateirepliken...** Repliken der Maildatenbank auf anderen Servern. In einem Cluster setzen Sie das Häkchen bei **Auf allen Mitgliedern des Mail Server Clusters**.
15. Wenn Sie über eine langsame Netzwerkverbindung verfügen (etwa via VPN), setzen Sie ein Häkchen bei **Mailreplik(en) im Hintergrund erstellen**.
16. Setzen Sie den **Zugriff für den Besitzer der Maildatei** auf »Editor« und tragen Sie als **Manager der Maildatei** eine Support- oder Admin-Gruppe (z. B. LocalDomainAdmins) ein.
17. Aktivieren Sie **Volltextindex aktivieren**.
18. Legen Sie bei Bedarf eine DB-Größenbeschränkung und einen Warnschwellenwert fest.
19. Wechseln Sie zum Register **Adresse** und legen Sie die Regeln zur Generierung der Internet-Mailadresse fest.
20. Wechseln Sie zum Register **ID-Info** (siehe Abbildung 6.34).

21. Wählen Sie im Feld **Spezifikation des öffentlichen Schlüssels** »Mit Version 7.0 und höher kompatibel (2048 Bit)« und als **Lizenztyp** »Nordamerika«.

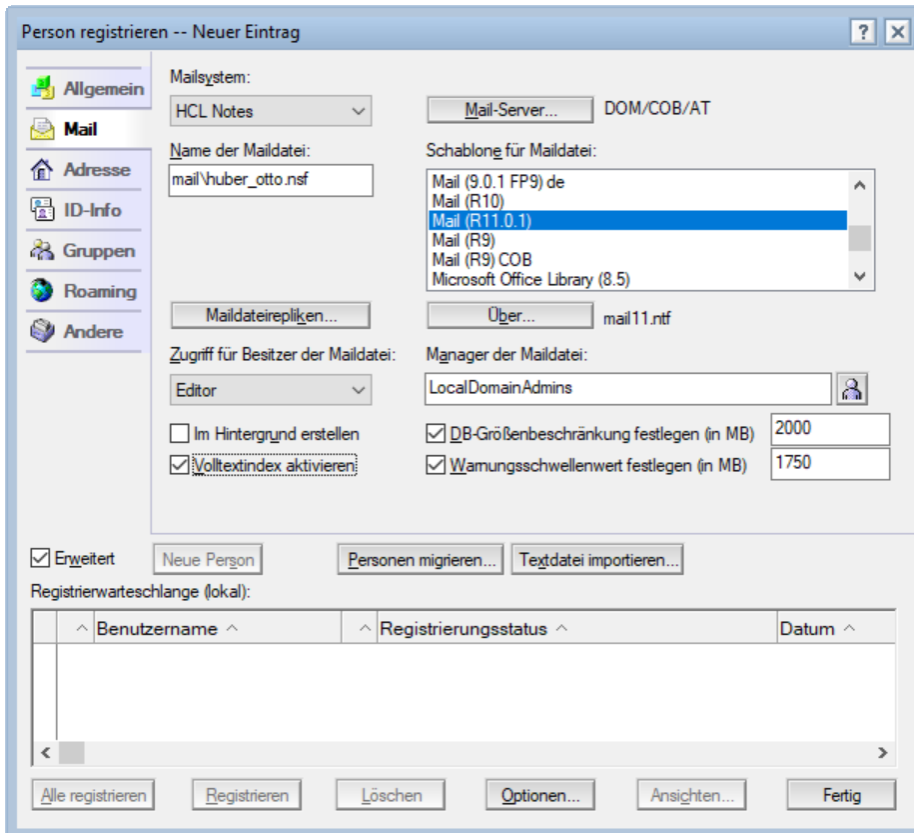


Abbildung 6.33: Der Registrierdialog, Register Mail

22. ID-Dateien werden im ID-Vault abgelegt. Haben Sie wie in Kap. 4.8.2.1 auf Seite 71 vorgeschlagen ein eigenes Verzeichnis für ID-Dateien konfiguriert, können Sie die ID-Datei auch dort ablegen.

Das Speichern von ID-Dateien im Domino-Verzeichnis ist nur möglich, wenn kein ID-Vault zugeordnet ist. Vergeben Sie in diesem Fall unbedingt für jede ID ein anderes Kennwort, da jeder Leser oder höher den Anhang sehen und herunterladen kann.

23. Wechseln Sie zum Register **Gruppen** und weisen Sie die vorgesehenen Gruppen zu.
24. Wechseln Sie zum Register **Roaming** und legen Sie fest, wo die Roaming-Dateien abgelegt werden sollen. Details zum Thema Roaming finden Sie in Kap. 6.5 Roaming-Benutzer, ab Seite 157.
25. Wechseln Sie zum Register **Andere**.
26. (Optional) Geben Sie einen Kommentar und die Position des Benutzers ein.
27. (Optional) Geben Sie eine Abteilungszuordnung an.

Mithilfe einer sogenannten **Eindeutigen Unterorganisation** (z. B. der Zuordnung zu einer Abteilung) kann zwischen Benutzern mit identischen CN-Namen, die von derselben Zulassungsstelle registriert wurden, unterschieden werden. Geben Sie eine zusätzliche Abteilungszuordnung an, wird diese zum Bestandteil des Namens:

Franz Huber/Verkauf/ABC

Franz Huber/Marketing/ABC

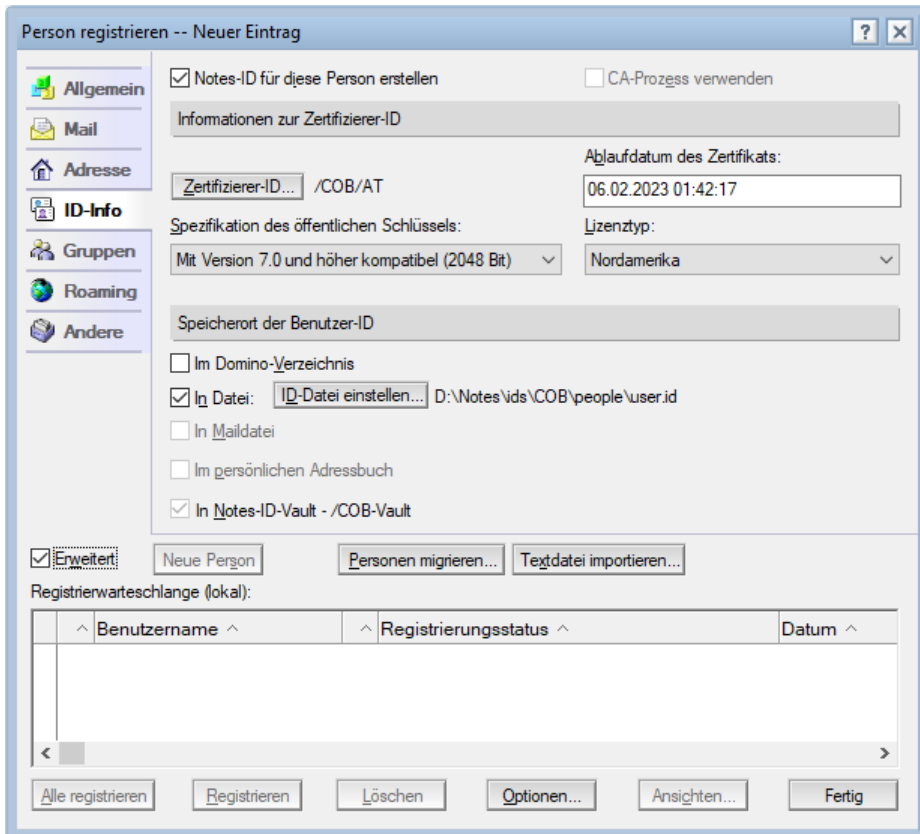


Abbildung 6.34: Der Registrierdialog, Register ID-Info

28. Wenn Sie fertig sind, klicken Sie auf die Schaltfläche mit dem grünen Häkchen. Die neue Person wird in der Registrierwarteschlange angezeigt.
29. (Optional) Klicken Sie auf die Schaltfläche **Neu**, um weitere Benutzer einzutragen und wiederholen Sie die Schritte 5 bis 26.
30. Klicken Sie auf **Alle registrieren**.

Existiert bereits eine Maildatei gleichen Namens, werden Sie gefragt, ob diese überschrieben werden soll. Klicken Sie auf **Nein**, erhalten Sie die Gelegenheit, den Namen zu ändern:

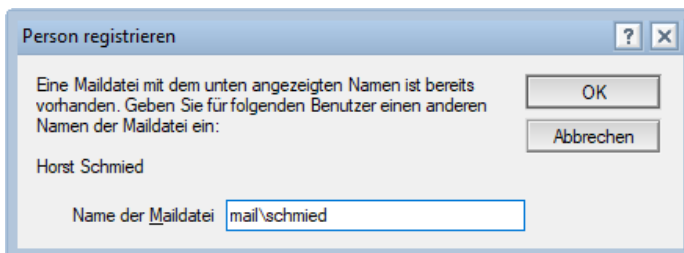


Abbildung 6.35: Dialog Name der Maildatei ändern

Geben Sie einen anderen Dateinamen ein und klicken Sie auf **OK**, um die Registrierung fortzusetzen, oder klicken Sie auf **Abbrechen**.

6.4.2. Benutzer aus einer Datei registrieren

Haben Sie die Benutzer aus einem anderen System exportiert, können Sie diese im CSV-Format in den Registrierdialog importieren. Wichtig ist, dass Sie als Trennzeichen das Semikolon (;) verwenden und die Spaltenreihenfolge genau einhalten. Eine Aufstellung der verfügbaren Spalten finden Sie in Tabelle 6.9:

Pos.	Parameter	Beschreibung
1	Nachname	Der Nachname des Benutzers (Pflichtfeld)
2	Vorname	Der Vorname des Benutzers
3	Mittlere Initiale	Die mittlere Initiale des Benutzers
4	Organisationseinheit	Der Name der Organisationseinheit des Benutzers
5	Kennwort	Das Kennwort des Benutzers (Pflichtfeld)
6	ID-Dateiverzeichnis	Das Verzeichnis, in dem die ID-Datei des Benutzers gespeichert wird. Dieser Parameter wird nur verwendet, wenn Sie als Speicherort der Benutzer-ID »In Datei« ausgewählt haben. Sie müssen das Verzeichnis vor der Registrierung angelegt haben.
7	ID-Dateiname	Der Name der ID-Datei des Benutzers. Dieser Parameter wird nur verwendet, wenn Sie bei der Option Speicherort der Benutzer-ID »In Datei« ausgewählt haben.
8	Mailservername	Der Name des Mailservers des Benutzers (Dieser Parameter übersteuert den im Registrierdialog angegebenen Server.)
9	Mailverzeichnis	Das Mailverzeichnis des Benutzers, z. B. mail\
10	Maildatei	Die Maildatei des Benutzers. Geben Sie keinen Namen an, wird die Maildatei nach dem Schema 1. Zeichen des Vornamens plus max. 7 Zeichen des Nachnamens erstellt.
11	Standort	Der Standort des Benutzers
12	Kommentar	Ein beliebiger Kommentar (wird in das Personendokument eingefügt)
13	Weiterleitungsadresse	Die Weiterleitungsadresse des Benutzers. Dieser Parameter wird nur verwendet, wenn als Mailsystem »Andere« oder »Andere Internet-Mail« angegeben wird.
14	Profil	Der Name des Konfigurationsprofils (obsolet)
15	Lokaler Administrator	Name der Person, die das Personendokument bearbeiten darf.
16	Internetadresse	Die Internet-Mailadresse des Benutzers (Pflichtfeld)
17	Kurzname	Der Kurzname des Benutzers
18	Alternativer Name	Ein alternativer Benutzername in einer anderen Sprache. Beachten Sie, dass der Zertifizierer die alternative Sprache enthalten muss.
19	Alternative Organisationseinheit	Eine Zeichenfolge, um zwei gleichlautende Benutzernamen voneinander zu unterscheiden

Pos.	Parameter	Beschreibung
20	Mailschablone	Der Dateiname der Mailschablone, die zum Erstellen der Maildatenbank verwendet werden soll

Tabelle 6.9: Parameter für Importdatei

Wenn Sie eine Registrierungsrichtlinie eingerichtet haben, müssen Sie die meisten Parameter nicht angeben; Minimalanforderung sind: Nachname, Vorname, Kennwort und die E-Mail-Adresse:

Buchacher;Christian;;;PasswOrd;;;;;;;c.buchacher@cob.at

Tipp: Sie können die Liste der Benutzer z. B. in Microsoft Excel erstellen und dann als CSV-Datei exportieren.

Wenn Sie die Datei erstellt haben, können Sie diese im Registrierdialog über die Schaltfläche **Textdatei importieren...** auswählen. Die Benutzer werden nicht sofort registriert, sondern zuerst in die Registrierwarteschlange eingelesen. Sie können diese in aller Ruhe inspizieren und – sollte das nötig sein – auch noch Änderungen vornehmen.

6.5. Roaming-Benutzer

Roaming-Benutzer (Roaming User) können von mehreren Notes-Clients auf verschiedenen Computern aus auf einen Domino-Server zugreifen und erhalten immer ihre benutzerdefinierten Einstellungen und persönlichen Informationen. (Die ID-Datei wird über das lokale Dateisystem oder den ID-Vault zur Verfügung gestellt.)

Zu den Roaming-fähigen Dateien gehören Kontakte, Lesezeichen, Notizbuch oder Journal und die Standard-Client-Einstellungen. Wenn der Benutzer an diesen Dateien Änderungen vornimmt, werden sie je nach Konfiguration nach Zeitplan oder spätestens beim Beenden des Notes-Clients auf einen Roaming-Server hochgeladen und beim Starten eines anderen Notes-Clients wieder heruntergeladen. Bei diesem Server kann es sich, je nachdem ob der Benutzer das **Domino-Server-Roaming** oder das **Dateiserver-Roaming** (nicht beide) nutzt, um einen Domino- oder Dateiserver handeln.

Das Domino-Server-Roaming kann für einen Benutzer bereits beim Registrieren aktiviert werden. Setzen Sie dazu im Registrierdialog, Register Allgemein ein Häkchen im Feld **Roaming für diese Person aktivieren** (siehe Abbildung 6.32). In diesem Fall werden während des Registriervorgangs am Server die Datenbanken Kontakte (names.nsf), Lesezeichen (bookmark.nsf), Notizbuch (notebook.nsf) oder Journal (journal.nsf), Feeds (localfeedcontent.nsf) und die Einstellungen des Notes-Standard-Clients (roamingdata.nsf) auf dem Server im angegebenen Verzeichnis erstellt und später bei der Client-Konfiguration von dort heruntergeladen.

Das Domino-Server-Roaming kann auch später im Domino-Administrator über die Roaming-Tools im Register **Personen und Gruppen** aktiviert bzw. deaktiviert werden.

Das Dateiserver-Roaming, welches für Außenstellen mit langsamer Anbindung an den Domino-Server gedacht ist, kann später via Roaming-Richtlinie eingerichtet werden. (Auf das Dateiserver-Roaming wird in diesem Buch nicht näher eingegangen.)

6.5.1. Roaming aktivieren

Um das Domino-Server-Roaming für ausgewählte Benutzer zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Domino-Administrator zum Register **Personen und Gruppen** und markieren Sie die Personen, für die Sie das Roaming aktivieren wollen.
2. Wählen Sie in den Werkzeugen den Befehl **Personen > Roaming...** Der Dialog **Roaming-Profil zuweisen** wird angezeigt:

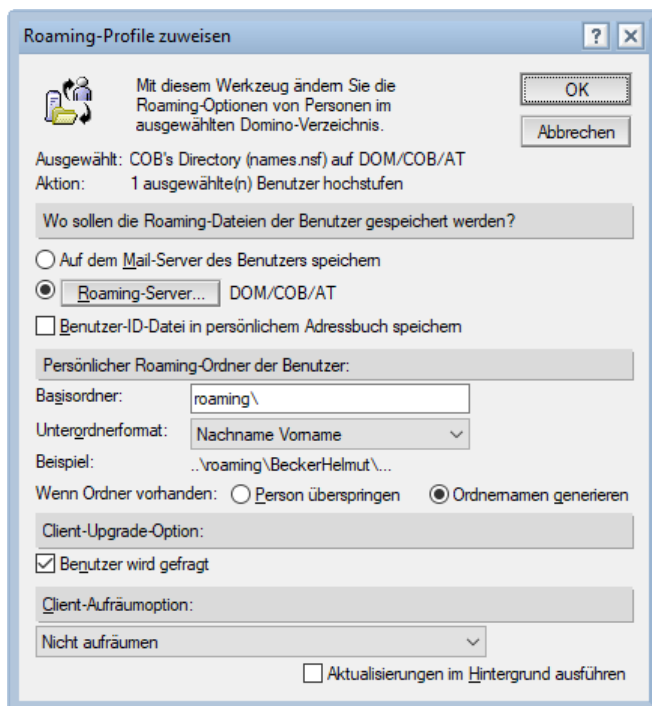


Abbildung 6.36: Dialog Roaming-Profil zuweisen

3. Wählen Sie den Server, auf dem die Roaming-Daten gespeichert werden sollen. In der Regel nehmen Sie hier den Mailserver der Person.
4. Aktivieren Sie die Option **Benutzer-ID-Datei in persönliches Adressbuch speichern** nur, wenn Sie keinen ID-Vault im Einsatz haben. (Sie sollten einen ID-Vault einsetzen!)
5. Geben Sie an, nach welchem Format das Roaming-Verzeichnis angelegt werden soll, z. B. nach dem Schema `roaming\NachnameVorname`.
6. Setzen Sie ein Häkchen im Feld **Benutzer wird gefragt**, wenn Sie wollen, dass der Benutzer entscheidet, wann er zum Roaming-Benutzer hochgestuft wird (empfohlen).
7. Wählen Sie im Feld **Client-Aufräumoption** den Wert »Nicht aufräumen« (Vorgabe).
8. »Aufräumen« bedeutet, dass die Roaming-Dateien nach dem Hochladen lokal gelöscht werden, was in der Regel unbrauchbar ist, weil der Client dann beim nächsten Start lange braucht, um alles wieder herunterzuladen.
9. Klicken Sie auf **OK**.

Der Administrationsprozess erhält die Anforderung »Status des Roaming-Benutzers im Personendokument aktualisieren«. Zuständig ist der Administrationsserver des Domino-Verzeichnisses. Wenn Sie die Anforderung auf einem anderen Server erstellt haben, vergessen Sie nicht, die Datenbank zu replizieren.

Sowie das geschehen ist, wird im Domino-Verzeichnis vor dem Benutzernamen eine Sanduhr angezeigt. Im Personendokument steht nun im Register **Roaming** im Feld **Roaming für Benutzer zulassen** »in Arbeit« und die Roaming-Datenbanken sind noch nicht eingetragen.

Beim nächsten Zugriff auf den Domino-Server (dafür können mehrere Neustarts nötig sein) wird der Benutzer gefragt, ob er in einen Roaming-Benutzer konvertiert werden möchte:

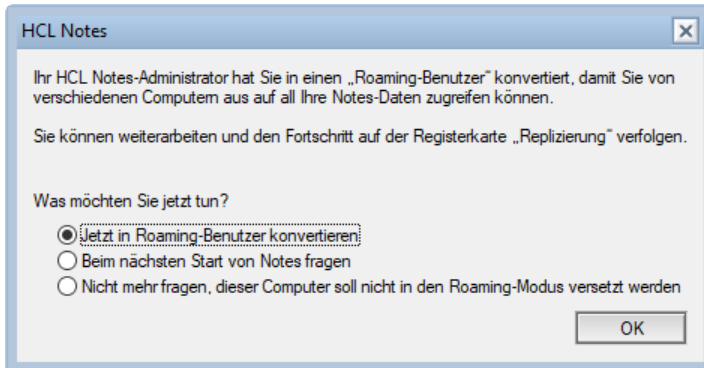


Abbildung 6.37: Frage zur Konvertierung in einen Roaming-Benutzer

Nach Bestätigen der Konvertierung erhält der Administrationsprozess des Roaming-Servers die Anforderung, »Replikrumpfe des Roaming-Benutzers erstellen«. Der Anwender muss den Client dann neu starten, damit die Datenbanken auf den Roaming-Server repliziert werden. Bereits beim Herunterfahren erhält der Benutzer die Meldung:

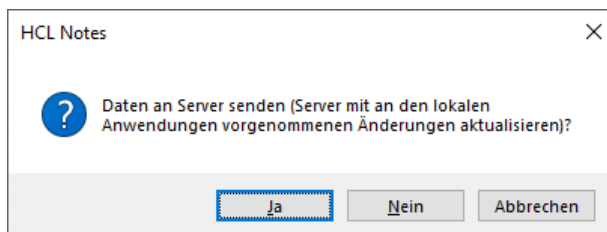


Abbildung 6.38: Frage zum Replizieren beim Beenden des Notes-Clients

Der Administrationsserver des Domino-Verzeichnisses erhält den Auftrag, die Roaming-Dateien in das Personendokument einzutragen (Anforderung »Angaben zum Roaming-Benutzer im Personendokument aktualisieren«). Die zusätzliche Anforderung »Replikrumpfe des Roaming-Benutzers überwachen« überprüft, ob alle Datenbanken repliziert wurden. Wenn dies der Fall ist (das kann mehrere Client-Starts erfordern und der Benutzer kann die Replikation zur Beschleunigung auch händisch anstoßen) wird der Roaming-Status des Benutzers vom Administrationsserver auf »Ja« gesetzt, wodurch in der Ansicht Personen das Symbol Weltkugel angezeigt wird. Der Benutzer erhält darauf die Meldung:

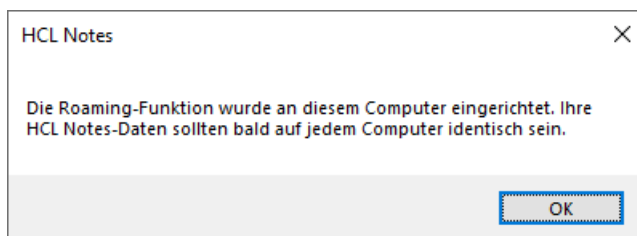


Abbildung 6.39: Info Roaming-Funktion ist eingerichtet

6.5.2. Roaming deaktivieren

Wenden Sie dasselbe Werkzeug **Personen > Roaming...** auf einen Benutzer mit aktiviertem Roaming an, werden Sie gefragt, ob das Roaming-Profil entfernt werden soll:

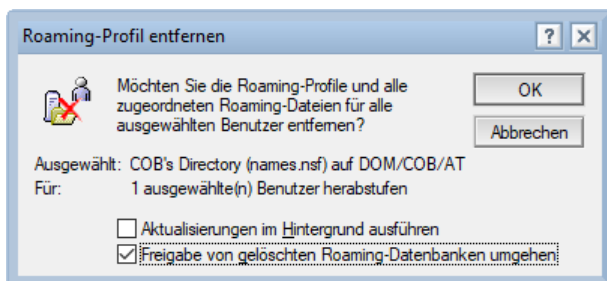


Abbildung 6.40: Dialog Roaming-Profile zuweisen

Setzen Sie unbedingt ein Häkchen bei **Freigabe von gelöschten Roaming-Datenbanken umgehen**, sonst müssen Sie in der Datenbank für Administrationsanforderungen das Löschen jeder einzelnen Datei bestätigen.

Die Roaming-Dateien werden vom Administrationsprozess gelöscht und der Status im Personendokument aktualisiert. Der Anwender erhält die Meldung:

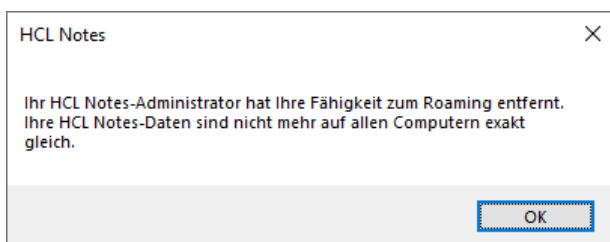


Abbildung 6.41: Info, dass Roaming deaktiviert wurde

Achtung: Das Wechseln der ID durch Auswahl von **Datei > Sicherheit > ID wechseln...** oder auch durch Auswahl einer Arbeitsumgebung, die zu einer anderen ID wechselt, wird für Roaming-Benutzer nicht empfohlen. Das Wechseln von Benutzer-IDs kann zu einem unbeabsichtigten Aktivieren oder auch Deaktivieren des Roamings führen, insbesondere wenn die ID, zu der gewechselt wird, die primäre ID-Datei eines anderen Roaming-Benutzers ist. Bei einer Installation mit mehreren Benutzern sollte jedem Roaming-Benutzer ein eigenes Windows-Anmeldeprofil zugeordnet sein.

6.6. Notes-ID-Kennwörter zurücksetzen

Wenn Notes-Benutzer ihr Kennwort vergessen haben, können Sie es mithilfe des Domino-Administrators mit wenig Aufwand zurücksetzen – sofern Sie einen ID-Vault eingerichtet haben ... Haben Sie keinen ID-Vault eingerichtet, können Sie dem Benutzer nur eine Kopie der ID-Datei mit dem Startkennwort aushändigen. Haben Sie diese auch nicht, müssen Sie den Benutzer neu anlegen. Erstellen Sie daher am besten sofort einen ID-Vault. (Eine Anleitung dazu finden Sie in Kap. 6.2.1 Einen ID-Vault einrichten, ab Seite 138.)

6.6.1. Kennwörter über den Domino-Administrator zurücksetzen

Damit Sie über den Admin-Client Kennwörter zurücksetzen können, muss sich die Notes-ID der Person, für die Sie das Kennwort zurücksetzen wollen, im ID-Vault befinden. Weiters müssen Sie das Recht besitzen, Kennwörter zurückzusetzen.

Um ein Kennwort zurückzusetzen, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Personen und Gruppen**.
2. Klicken Sie auf die Ansicht **Personen** und wählen Sie die gewünschte Person aus.
3. Wählen Sie jetzt in den Werkzeugen rechts **ID-Vaults > Kennwort zurücksetzen...**
4. Geben Sie zweimal das neue Kennwort ein:

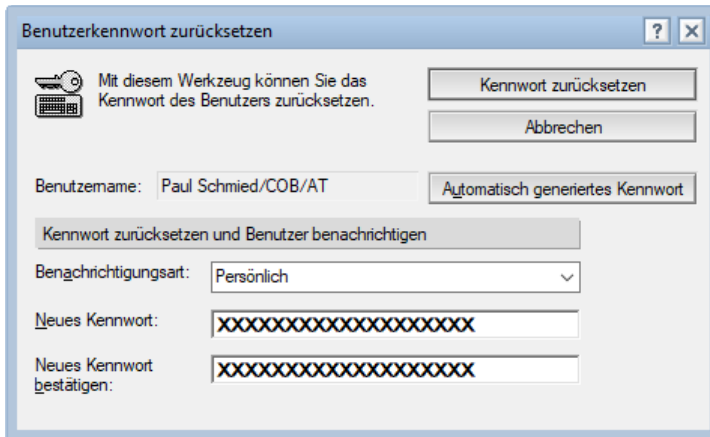


Abbildung 6.42: Dialog Benutzerkennwort zurücksetzen

Wählen Sie als Benachrichtigungsart »Persönlich«, wird davon ausgegangen, dass Sie dem Benutzer das Kennwort persönlich (etwa via Telefon) mitteilen. Wählen Sie hingegen »Über E-Mail an den Manager«, wird ein Zufallskennwort generiert und an die angegebene E-Mail-Adresse geschickt.

Haben Sie in den Sicherheitseinstellungen, Register **ID-Vault** das Feld **Kennwort muss nach dem Zurücksetzen des Kennworts geändert werden** auf »Ja« gesetzt, muss der Benutzer nach dem Zurücksetzen ein neues Kennwort vergeben.

5. Nach dem Zurücksetzen werden Sie über den Erfolg informiert:

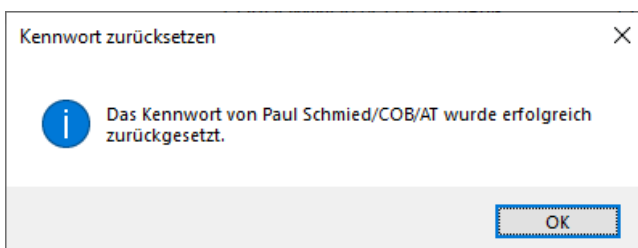


Abbildung 6.43: Kennwort zurücksetzen

6.6.2. Kennwörter über eine Self-Service-Anwendung zurücksetzen

6.6.2.1. Übersicht

Im Lieferumfang von Domino befindet sich die Beispielanwendung »Sample Web Agent - Reset User Password«, die Sie im Datenverzeichnis unter dem Namen PwdResetSample.nsf finden. Die Anwendung enthält einen in LotusScript programmierten Beispielagenten mit dem Namen »User-PasswordReset«, der es Benutzern ermöglicht, über einen Webbrowser ihr (vergessenes) Notes-ID-Kennwort selbst zurückzusetzen. Voraussetzungen dafür sind allerdings:

- > dass sich die ID-Datei des Benutzers im ID-Vault befindet
- > dass sich der Benutzer im Browser authentifizieren kann, entweder durch sein Internetkennwort oder durch eine andere Methode (z. B. SPNEGO)

Bei der mitgelieferten Anwendung handelt es sich nur um ein Beispiel, welches jedoch voll funktionsfähig ist. Verfügen Sie über die entsprechenden Ressourcen, können Sie den Code von einem Entwickler an Ihre Bedürfnisse anpassen lassen. Per Vorgabe wird in der Anwendung davon ausgegangen, dass sich Benutzer über ihr Internetkennwort auf einem Domino-Webserver anmelden. Der Agent bietet aber auch Möglichkeiten, ohne Authentifizierung auszukommen.

6.6.2.2. Einrichten der Anwendung

Öffnen Sie die Datenbank PwdResetSample.nsf auf dem gewünschten Server oder erstellen Sie eine Kopie, wenn Sie einen anderen Dateinamen verwenden möchten.

Geben Sie den Benutzern, die die Anwendungen nutzen sollen, zumindest Editorzugriff.

Signieren Sie den Agenten »UserPasswordReset« mit einer Benutzer-ID, die über das Recht verfügt, auf dem Webserver beschränkte LotusScript-Agenten zu signieren und auszuführen. (Zum Signieren von Agenten lesen Sie Kap. 11.2.2 Schablonen signieren, ab Seite 307.)

Wechseln Sie nun im Domino-Administrator zum Register **Konfiguration** und wählen Sie in **Werkzeuge > ID-Vaults** den Befehl **Berechtigung zum Zurücksetzen des Kennworts...**

Die Dialogseite zur Auswahl von Kennwortzurücksetzungsstellen wird angezeigt (siehe Abbildung 6.44).

Wählen Sie die folgenden Namen aus:

- > Den Benutzer, den Sie zum Signieren des Agenten verwendet haben. Achten Sie (wie in Abbildung 6.44 dargestellt) darauf, auch ein Häkchen bei: **Berechtigung für den Agenten für das selbständige Zurücksetzen des Kennworts** zu setzen.
- > Die Namen aller Server, die den Agenten zum Zurücksetzen des Kennworts ausführen.

Stellen Sie in den Sicherheitseinstellungen, Register **ID-Vault** das Feld **Kennwort muss nach dem Zurücksetzen des Kennworts geändert werden** auf »Nein«, damit Benutzer, die ihr Kennwort via Anwendung zurückgesetzt haben, ihr Kennwort in Notes nicht ein zweites Mal ändern müssen.

Zum Zurücksetzen des Kennworts können Benutzer die entsprechende URL entweder selbst im Browser eintippen, Sie können sie aber auch in den Anmeldedialog in den Bereich Kennwort vergessen integrieren, wie bereits in Kap. 6.2.1 Einen ID-Vault einrichten, ab Seite 138 dargestellt.

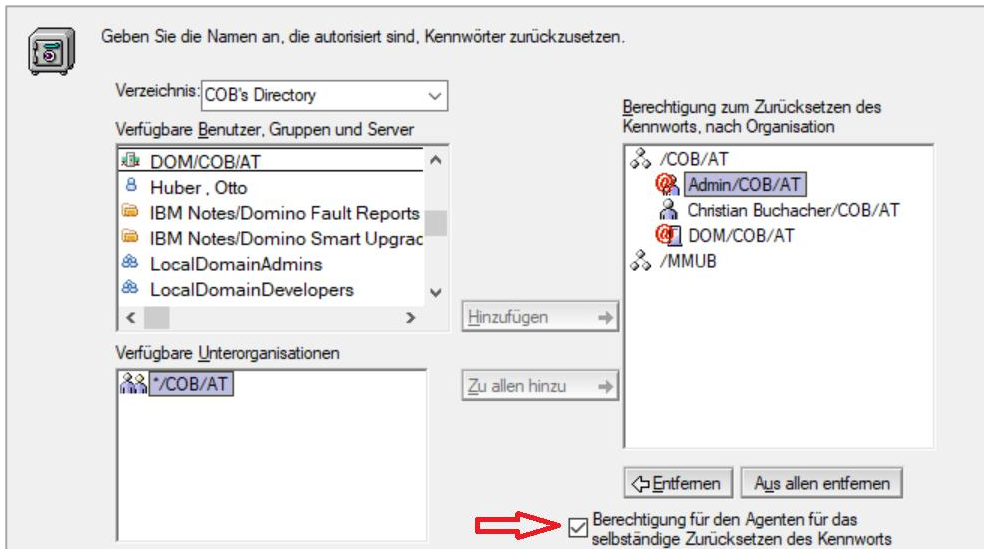


Abbildung 6.44: Berechtigung zum Zurücksetzen des Kennworts ändern

6.7. Notes-IDs verlängern

Das Ablaufdatum einer ID-Datei wird beim Registrieren festgelegt (Vorgabe für Benutzer ist zwei Jahre). Sie als Administrator sollten darauf achten, ID-Dateien zu verlängern, bevor die Benutzer eine Warnung erhalten:

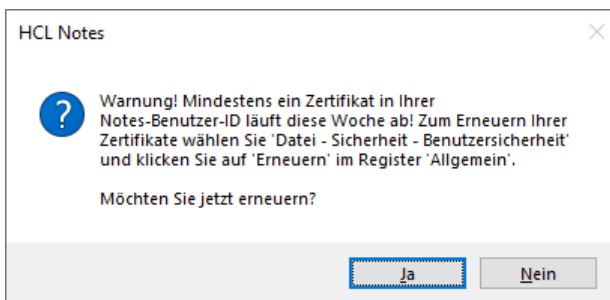


Abbildung 6.45: Warnung vor dem Ablauf der ID-Datei

6.7.1. Verlängern über den Administrationsprozess

Die einfachste Form der Verlängerung erfolgt im Domino-Administrator im Register **Konfiguration** über die Ansicht **Sicherheit > Zertifikate > Ablaufdatum des Zertifikats**.

In dieser Ansicht werden Benutzer nach dem Ablaufdatum kategorisiert dargestellt (»Läuft in den nächsten *nn* Tagen ab«), Sie können zur einfacheren Auswahl aber auch nach dem Zertifikatsaussteller oder dem Ablaufdatum sortieren.

Wählen Sie eine oder mehrere Personen aus (alle müssen auf demselben Zertifizierer beruhen) und klicken Sie auf die Schaltfläche **Ausgewählte Personen erneut zertifizieren**.

Wählen Sie im nächsten Schritt den Zertifizierer, mit dem die gewählten Personen ursprünglich zugelassen wurden.

Sie können jetzt ein neues Ablaufdatum eingeben:

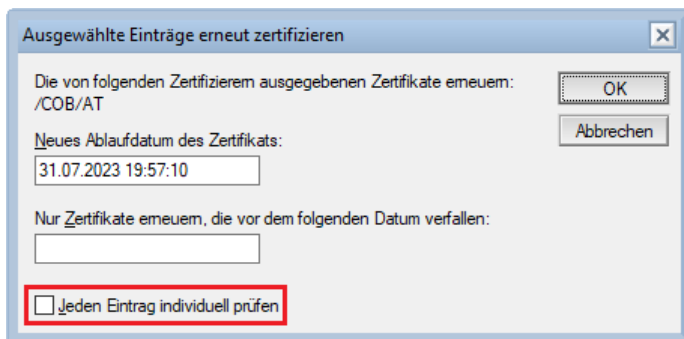


Abbildung 6.46: Ausgewählte Personen erneut zertifizieren – Eingabe des Ablaufdatums

Haben Sie mehrere Personen markiert, entfernen Sie unbedingt das Häkchen bei **Jeden Eintrag individuell prüfen**.

Die Aktualisierung wird im Hintergrund vom Administrationsprozess mit dem Planungstyp Intervall (also per Vorgabe einmal stündlich) ausgeführt. Soll es schneller gehen, geben Sie auf der Konsole den folgenden Befehl ein:

```
tell adminp process interval
```

Der Administrationsprozess aktualisiert zunächst die Zertifikate in den Personendokumenten, die Notes-IDs werden beim nächsten Zugriff der Benutzer mit dem neuen Ablaufdatum versehen und in den ID-Vault hochgeladen.

Diese Aktion wird vom Administrationsserver des Domino-Verzeichnisses ausgeführt. Wenn Sie den Antrag nicht auf diesem Server gestellt haben, muss er zuerst dorthin repliziert werden. Zum korrekten Aufsetzen des Administrationsprozesses lesen Sie Kap. 5.7 Der Administrationsprozess, ab Seite 112.

6.7.2. Verlängern der ID-Datei

Ein manuelles Verlängern einer ID-Datei ist im Domino-Administrator auch über den Befehl **Zertifizierung > Zertifizieren...** möglich. Wählen Sie in einem ersten Schritt den Zertifizierer, mit dem die ID-Datei neu zertifiziert werden soll, und dann die zu aktualisierende ID-Datei selbst.

Im Dialog **ID zertifizieren** (siehe Abbildung 6.47) können Sie neben dem Ablaufdatum auch die Kennwortqualität ändern.

Klicken Sie nach Eingabe des neuen Ablaufdatums auf die Schaltfläche **Zulassen**.

Das Neuzulassen einer ID-Datei hat jedoch einige Nachteile:

- > Sie müssen das Kennwort der ID-Datei wissen.
- > Die ID muss nach Verlängerung an den Benutzer ausgehändigt werden.
- > Das Prozedere ist aufwendig, wenn Sie mehrere ID-Dateien verlängern müssen.

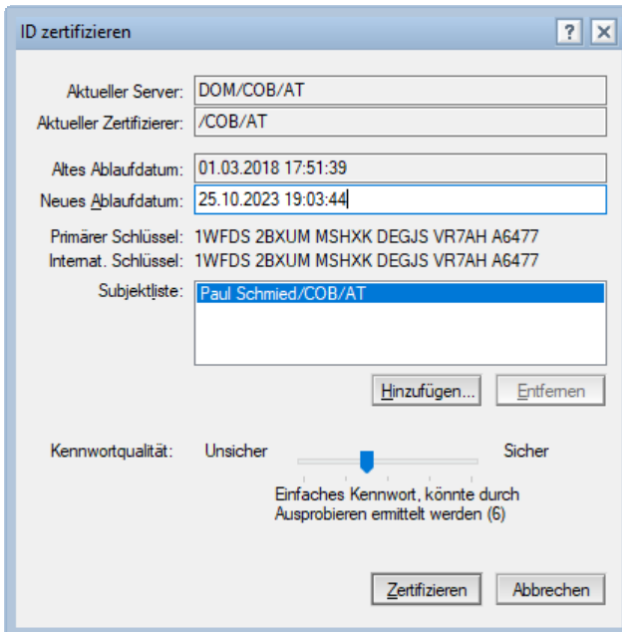


Abbildung 6.47: ID zertifizieren – Eingabe des Ablaufdatums

6.7.3. Die Administrator-ID ist abgelaufen

Selbst wenn Sie (oder Ihr Vorgänger) die ID des Administrators für einen längeren Zeitraum zugelassen haben, kann es passieren, dass Sie eines Tages feststellen, dass sie abgelaufen ist. Was tun Sie jetzt? – ein Zugriff auf den Server ist mit einer abgelaufenen ID nicht möglich!

Haben Sie einen anderen Benutzer zur Verfügung, der noch nicht abgelaufen ist, machen Sie ihn kurzfristig zum Admin! Das geht natürlich nicht, solange der Domino-Server läuft, fahren Sie also den Server herunter und kopieren Sie das Domino-Verzeichnis (names.nsf) auf einen PC, auf dem Notes installiert ist. Öffnen Sie die Datenbank dort lokal und fügen Sie den Benutzer zur Admin-Gruppe (in der Regel »LocalDomainAdmins«) hinzu. Kopieren Sie das Verzeichnis zurück und starten Sie den Server neu. Wechseln Sie über den Befehl **Datei > Sicherheit > ID wechseln...** zur hochgestuften Anwender-ID und verlängern Sie die abgelaufene Admin-ID wie in diesem Kapitel beschrieben. Beim Zurückwechseln zur Admin-ID und Zugriff auf den Server sollte diese verlängert werden und Sie können dem Benutzer die Administrationsrechte wieder entziehen.

Sollten alle IDs abgelaufen sein (dies kann unbemerkt passieren, wenn alle Benutzer mit Webmail arbeiten), dann können Sie im Client auch zu einer Server-ID zu wechseln. Bedenken Sie jedoch, dass die Zugriffskontrollliste per Vorgabe verhindert, dass eine Datenbank mit einer Server-ID im Client geöffnet wird (Benutzertyp »Server« oder »Servergruppe«). Kopieren Sie sich das Domino-Verzeichnis erneut lokal auf einen Client und ändern Sie dort den Benutzertyp für den Server auf »Unbestimmt«. Der Rest läuft gleich ab wie oben beschrieben.

6.8. Benutzer umbenennen

Lesen Sie zum korrekten Aufsetzen des Administrationsprozesses zuerst Kap. 5.7 Der Administrationsprozess, ab Seite 112.

Es gibt drei Arten von Umbenennungen:

1. Ändern eines flachen Namens (Otto Huber) auf einen hierarchischen (Otto Huber/COB/AT). (Dieser Vorgang ist seit Notes 3 obsolet.)
2. Ändern des sogenannten Allgemeinen Namens (also des Vor-, Mittel- oder Nachnamens), z. B. durch Heirat.
3. Ändern einer anderen Namenskomponente wie Organisationseinheit oder Organisation, etwa beim Wechsel in eine andere Abteilung oder in eine andere Firma.

Umbenennungen werden vom Administrationsprozess ausgeführt und erfolgen automatisiert im Hintergrund. Sie müssen die Umbenennung lediglich anstoßen. Starten Sie die Umbenennung am besten auf dem Administrationsserver des Domino-Verzeichnisses, da die ersten Schritte von diesem ausgeführt werden. Führen Sie Umbenennungen auf einem anderen Server aus, stellen Sie sicher, dass die Datenbank für Administrationsanforderungen (admin4.nsf) mit dem Administrationsserver repliziert.

6.8.1. Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein, damit Sie Benutzer umbenennen können:

- > Dem Domino-Verzeichnis ist ein Administrationsserver zugewiesen.
- > Es ist ein Zertifizierungsprotokoll (certlog.nsf) vorhanden. Sollte dieses fehlen, replizieren Sie es auf den Server, auf dem Sie Benutzer registrieren oder umbenennen wollen.
- > Alle Zertifizierer sind im Domino-Verzeichnis vorhanden.
- > Es besteht Zugriff auf die Zulassungs-ID-Datei oder auf einen CA-konfigurierten Zertifizierer.
- > Sie verfügen über ausreichende Zugriffsrechte im Domino-Verzeichnis und in der Datenbank für Administrationsanforderungen.

6.8.2. Ändern des Allgemeinen Namens

Am häufigsten werden Sie es mit Änderungen von Nachnamen zu tun haben. In unserem Beispiel heiratet Herr Otto Schmied und heißt von nun an Huber. Selbstverständlich will er seinen Namen auch in Notes geändert sehen. Für Sie als Administrator ergibt sich die folgende Vorgangsweise:

1. Wählen Sie im Administrator-Client im Register **Personen** zuerst den Benutzer und dann **Werkzeuge > Personen > Umbenennen....**
2. Klicken Sie auf die Schaltfläche **Allgemeinen Namen ändern...**

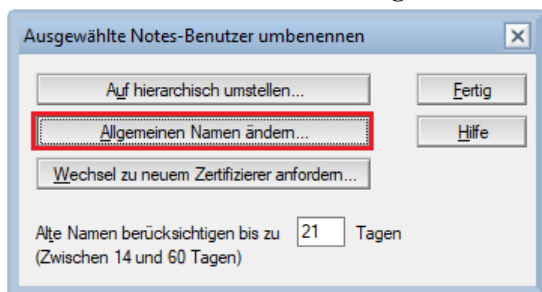


Abbildung 6.48: Dialog Ausgewählte Notes-Benutzer umbenennen

3. Wählen Sie die Zulassungsdatei aus und geben Sie das Kennwort ein oder klicken Sie auf **CA-Prozess verwenden** und wählen Sie einen CA-konfigurierten Zertifizierer:

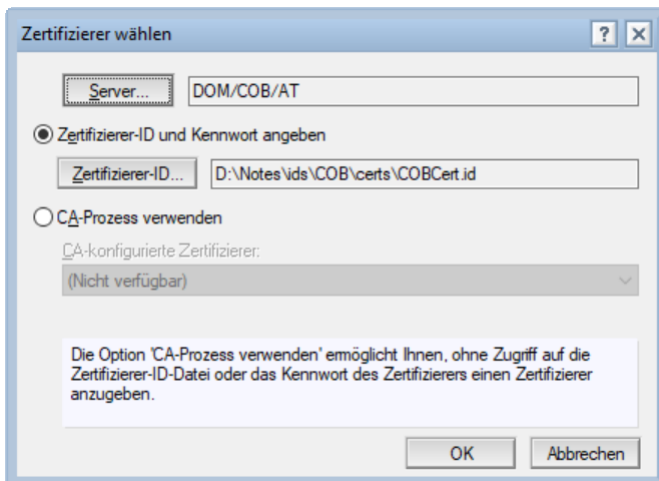


Abbildung 6.49: Dialog Zertifizierer wählen

4. Geben Sie bei Bedarf ein neues Ablaufdatum ein:

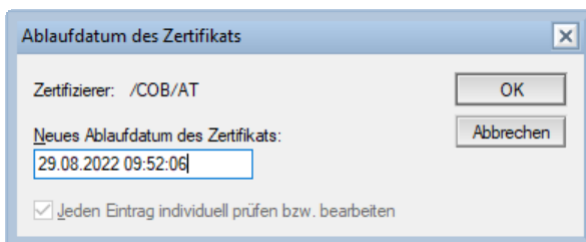


Abbildung 6.50: Dialog Ablaufdatum des Zertifikats

5. Sie erhalten nun Zugriff auf alle Namenskomponenten der Person:

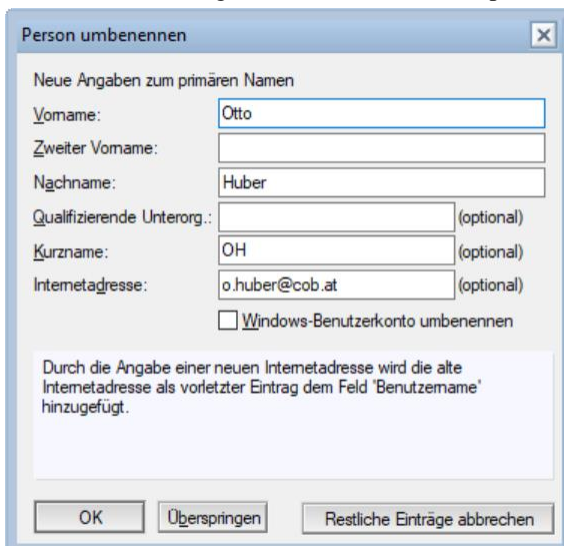


Abbildung 6.51: Dialog Person umbenennen

Geben Sie den neuen Nachnamen und/oder Vornamen ein.

Der Kurzname wird als Schlüssel verstanden und sollte nicht geändert werden; geben Sie einen neuen Kurznamen ein, wird dieser als Alias zum alten Kurznamen hinzugefügt.

Korrigieren Sie die Internetadresse.

Die alten Namen sowie die alte Mailadresse werden im Feld Benutzername als Aliasnamen weitergeführt, sodass der umbenannte Benutzer nach der Umbenennung auch unter seiner alten Mailadresse erreichbar bleibt.

6. Klicken Sie auf **OK**.
7. Wenn kein Fehler aufgetreten ist, erhalten Sie eine Erfolgsmeldung (»Verarbeitungsstatistik«).

6.8.3. Das Tempo der Umbenennung steuern

Der Administrationsprozess wird nun damit beauftragt, die Person umzubenennen. Das läuft vollautomatisch im Hintergrund ab, erfordert nur ein einmaliges Anmelden des umzubenennenden Benutzers. Den Fortschritt bei der Umbenennung sehen Sie in der Datenbank für Administrationsanforderungen (admin4.nsf) in der Ansicht **Alle Anforderungen nach Name (All Requests by Name)**, wo die Person unter ihrem alten Namen aufscheint. Darunter sollte nun der erste Schritt »Umbenennung im Domino-Verzeichnis veranlassen« zu sehen sein.

Wie schon in Kap. 5.7.3 Planungstypen, ab Seite 114 ausgeführt, ist in der Datenbank für Administrationsanforderungen (admin4.nsf) jedem Schritt ein bestimmter Planungstyp zugeordnet, der durch ein Symbol repräsentiert wird. Der erste Schritt wird nach Intervall abgearbeitet, also alle 60 Minuten, außer Sie haben im Feld **Intervall** im Serverdokument eine andere Zeit angegeben. Sie können nun darauf warten, bis das Intervall zuschlägt, oder den Administrationsprozess anweisen, den Schritt sofort abzarbeiten, indem Sie den zum Planungstyp passenden Befehl eintippen:

```
tell adminp process interval
```

Damit wird die Person im Personendokument umbenannt und der Administrationsprozess wartet darauf, dass sie sich anmeldet. Meldet sich die Person innerhalb des vorgegebenen Zeitraums nicht an (Vorgabe ist 21 Tage, kann auf 60 Tage hochgesetzt werden), geht die Umbenennung schief! Benennen Sie also keine Person um, die gerade auf Urlaub ist!

Nach Anmeldung der Person werden die nächsten Schritte in die Datenbank gestellt. Die vollständige Liste aller Schritte entnehmen Sie bitte Tabelle 6.10:

Anforderung	Planungstyp
Umbenennung im Domino-Verzeichnis veranlassen	Intervall
Personen im Domino-Verzeichnis umbenennen	Intervall
In Personendokument umbenennen	Täglich
In Liste der ungelesenen Dokumente umbenennen	Täglich
In Zugriffskontrollliste umbenennen	Intervall
In Gestaltungselementen umbenennen	Verzögert
In Datenbank für freie Zeit umbenennen	Sofort
Person in Kalendereinträgen und Profilen der Maildatei umbenennen	Sofort
Person in Kalendereinträgen und Profilen der Maildatei umbenennen erweitert	Verzögert
In Leser-/Autorenfeldern umbenennen	Verzögert

Tabelle 6.10: Schritte und Planungstypen beim Umbenennen einer Person

Beachten Sie, dass bei mehreren Schritten der Planungstyp »verzögert« zugeordnet ist, die Umbenennung daher per Vorgabe bis zu sechs Tage dauern kann. Daher sollten Sie, wie in Kap. 5.7.5 Den Administrationsprozess einrichten, ab Seite 115 dargestellt, die Vorgaben im Serverdokument an Ihre Bedürfnisse anpassen.

6.8.4. Wechsel zu neuem Zertifizierer anfordern

Ein Wechsel zu einem neuen Zertifizierer ist nur dann ein Thema, wenn Sie mehrere Unterorganisationen (OUs) erstellt haben. Stecken hinter den OUs Abteilungen, ist bei jedem Abteilungswechsel eine Umbenennung erforderlich.

6.8.4.1. Einen neuen OU-Zertifizierer erstellen

Falls der neue Abteilungszertifizierer noch nicht existiert, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Konfiguration** und wählen Sie in den Werkzeugen den Befehl **Registrierung > Unterorganisation...**

The screenshot shows a Windows-style dialog box titled "Zertifizierer für Unterorganisation registrieren". It contains several input fields and buttons. At the top, there are two fields: "Registrierungsserver..." with the value "DOM/COB/AT" and "Zertifizierer-ID..." with the value "/COB/AT". Below these is a text box with instructions: "Füllen Sie die erforderlichen Felder aus, um eine neue Unterorganisation zu erstellen. Bei der Registrierung einer Unterorganisation wird ein Zertifiziererdokument und eine Zertifizierer-ID-Datei erstellt." The main section has a "Unterorganisation" field with "Verkauf", a "Zertifizierer-Kennwort" field with "passw0rd#1" and a "Kennwortoptionen..." button, a "Dateiname der Zertifizierer-ID" field with "T:\Notes\ids\certs\verkauf.id" and an "ID-Datei einstellen..." button, a "Spezifikation des öffentlichen Schlüssels" dropdown menu set to "Mit Version 8.0 und höher kompatibel (4096 Bit)", a "Zertifizierungsanforderungen senden an (Admin.)" field with "Admin/COB/AT", and two optional fields: "Kommentar (optional)" and "Standort (optional)". At the bottom right are "Registrieren" and "Abbrechen" buttons.

Abbildung 6.52: Dialog Zertifizierer für Unterorganisation ändern

2. Geben Sie einen Namen für die Unterorganisation sowie ein Kennwort für die Zertifizierer-ID ein.
3. Haben Sie in Ihrem Admin-Client noch kein ID-Verzeichnis festgelegt (siehe Kap. 4.8.2.1 Ordner zum Ablegen der ID-Dateien festlegen, auf Seite 71), wählen Sie im Feld **Dateiname der Zertifizierer-ID** den Speicherort aus.
4. Setzen Sie die RSA-Schlüssellänge auf 4096 Bit.
5. Tragen Sie eine Person oder Gruppe ein, an die die Zertifizierungsanforderungen gesendet werden – etwa vor Ablauf der ID-Datei.

6. Klicken Sie auf **Registrieren**.

6.8.4.2. Eine Person umbenennen

Nehmen wir an, Frau Susanne Meier/Verkauf/COB/AT wechselt in die Abteilung Marketing, hinter der der OU-Zertifizierer /Marketing/COB/AT steckt, und will das auch in ihrem Namen widerspiegeln haben. Dazu gehen Sie wie folgt vor:

1. Wechseln Sie im Domino-Administrator zum Register **Personen und Gruppen** und wählen Sie die gewünschte Person(en) aus.
2. Wählen Sie in den Werkzeugen den Befehl **Personen > Umbenennen...**
3. Klicken Sie auf die Schaltfläche **Wechsel zu neuem Zertifizierer anfordern...**

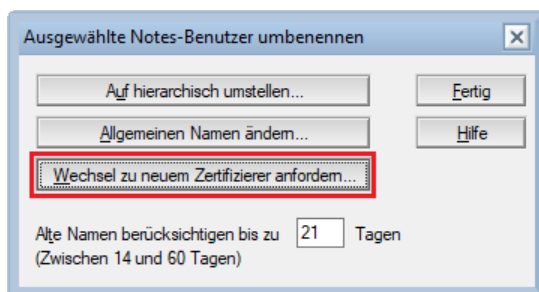


Abbildung 6.53: Dialog Ausgewählte Notes-Benutzer umbenennen

4. Wählen Sie zuerst den aktuellen Zertifizierer der Person aus, in unserem Beispiel den Zertifizierer für /Verkauf/COB/AT.
5. Sie werden gefragt, zu welchem Zertifizierer die gewählte Person wechseln wird, in unserem Beispiel zu /Marketing/COB/AT:

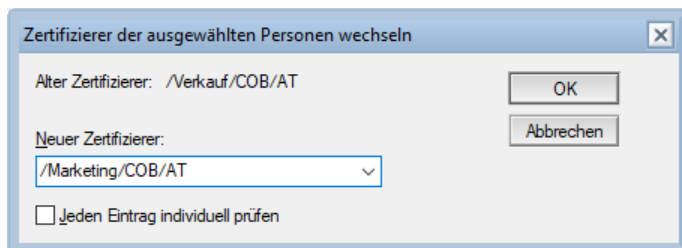


Abbildung 6.54: Dialog Zertifizierer der ausgewählten Personen wechseln

6. Entfernen Sie das Häkchen bei **Jeden Eintrag individuell prüfen**, sonst müssen Sie alle gewählten Personen einzeln bestätigen.
7. Klicken Sie auf **OK**.
8. Klicken Sie in der Erfolgsmeldung (»Verarbeitungsstatistik«) auf **OK**.
9. Wechseln Sie nun in die Datenbank für Administrationsanforderungen (admin4.nsf), um die Anforderung abzuschließen. Die Idee hinter dem zusätzlichen Schritt ist, dass Sie vielleicht gar nicht über die Zertifizierer-ID der Ziel-OU verfügen, weil ein anderer Administrator dafür zuständig ist.
10. Wählen Sie die Ansicht **Anforderungen zur Namensverschiebung** (Name Move Requests) und markieren Sie die zu verschiebenden Personen in der Ansicht.

Verschiebung für gewählte Einträge abschließen ? Hilfe	
Ziel-Zertifizierer	Gegenwärtiger Name
<input checked="" type="checkbox"/>	/Marketing/COB/AT Susanne Meier/Verkauf/COB/AT

Abbildung 6.55: Administrationsanforderungen, Ansicht Anforderungen zur Namensverschiebung

Stehen mehrere Einträge in der Liste, achten Sie darauf, nur Personen mit demselben Zielzertifizierer auszuwählen.

11. Klicken Sie auf die Schaltfläche **Verschiebung für gewählte Einträge abschließen** und wählen Sie die ID-Datei für die Ziel-OU aus, in unserem Beispiel `/Marketing/COB/AT`.
12. In die Datenbank für Administrationsanforderungen wird der Schritt »Umbenennung im Domino-Verzeichnis veranlassen« gestellt. Von nun an läuft die Verarbeitung gleich ab wie bei der Umbenennung des Allgemeinen Namens.

6.8.4.3. Spezialfall: Wechsel zu einer anderen Organisation

Ein Spezialfall des Wechsels zu einem neuen Zertifizierer ist das Verschieben in eine andere Organisation, etwa, weil sich eine Unterorganisation selbstständig gemacht hat oder Sie Ihren Firmennamen geändert haben. Voraussetzung zum Verschieben innerhalb desselben Domino-Verzeichnisses ist eine Querzulassung zwischen den Organisationen. (Zum Ausstellen einer Querzulassung lesen Sie Kap. 13.2.2 Querzulassung auf Seite 337.)

Die Vorgangsweise ist prinzipiell gleich wie im letzten Kapitel angegeben, aber achten Sie darauf, dass die Schritte 1. bis 9. unbedingt vom Administrator der ursprünglichen Organisation ausgeführt werden. Erst ab Schritt 10 ist der Administrator der neuen Organisation dran.

6.9. Benutzer verschieben

Unter dem Verschieben eines Benutzers versteht man das Verschieben der Maildatenbank auf einen anderen Server (oder auch nur das Umbenennen der Maildatenbank am selben Server). Dabei ist nicht nur die Maildatenbank selbst zu verschieben, sondern auch serverseitig das Personendokument und Client-seitig die Arbeitsumgebung zu korrigieren.

Um einen oder mehrere Benutzer zu verschieben, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Personen und Gruppen** und markieren Sie die Person(en), die verschoben werden soll(en).
2. Wählen Sie danach in den Werkzeugen **Personen > Verschieben...**
3. Der Dialog **Benutzer auf anderen Server verschieben** wird angezeigt (siehe Abbildung 6.56).
4. Wählen Sie den Zielservers und korrigieren Sie gegebenenfalls das Zielverzeichnis.
5. Klicken Sie auf **OK**.

Der Administrationsprozess wird mit dem Verschieben der Maildatenbank(en) beauftragt. Verfolgen Sie den Status in der Datenbank für Administrationsanforderungen (`admin4.nsf`). Dort müssen Sie auch das Löschen der Maildateien bestätigen.

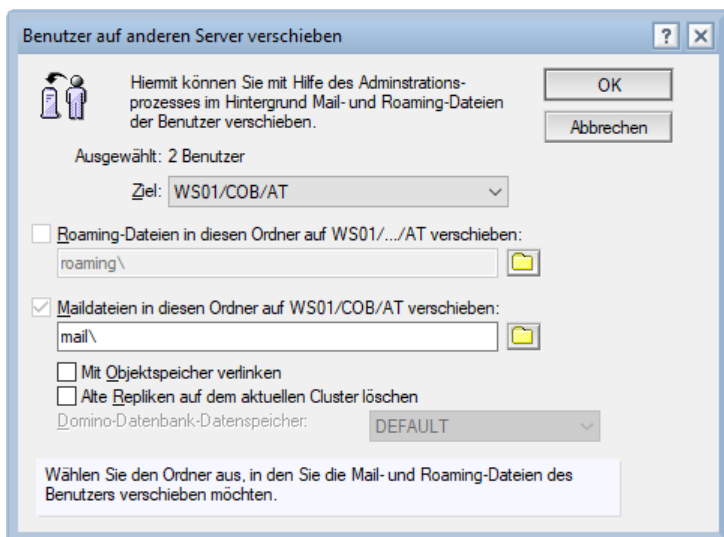


Abbildung 6.56: Dialog Benutzer auf anderen Server verschieben

6.10. Benutzer sperren

Vielleicht kennen Sie folgende Situation: Ihr Chef stürzt ins Zimmer und verlangt von Ihnen, einen Benutzer vom Domino-Server auszusperren. Und natürlich muss es schnell gehen ... Wie machen Sie das am besten?

Ich hoffe, Sie haben, wie in Kap. 13.2.4 (Seite 341) angeregt, eine Gruppe zum Sperren von Benutzern vorbereitet. Sonst geht es nämlich gar nicht schnell. Falls nein, legen Sie die Gruppe wie in Kap. 13.2.4 beschrieben an. (Sie wirkt leider erst nach einem Serverneustart!)

Haben Sie die Gruppe wie empfohlen angelegt und im Serverdokument eingetragen, fügen Sie jetzt den zu sperrenden Kollegen als Mitglied hinzu. Er wird dann sofort ausgeschlossen – außer er verfügt am Server noch über eine aktive Benutzersitzung, vielleicht, weil er vor seiner Entlassung noch rasch seine Mails löscht ... In diesem Fall wird er erst nach dem Beenden der Sitzung gesperrt.

Jetzt können Sie auf der Serverkonsole nur noch die folgenden Befehle absetzen:

```
drop "<Benutzername>", z. B. drop "Paul Schmied/COB/AT"
```

```
show nlcache reset
```

Damit haben Sie eine hohe Chance, dass der gesperrte Benutzer beim nächsten Drücken der Lösch-taste die folgende Meldung sieht:

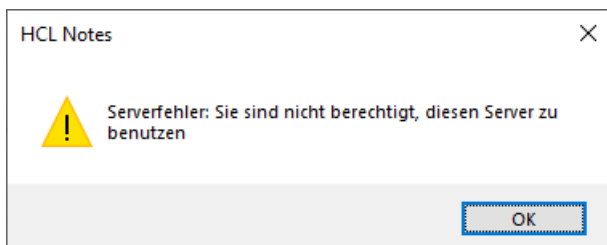


Abbildung 6.57: Fehlermeldung nach dem Sperren eines Benutzers

Achtung: Die Sperre gilt zunächst nur für das Protokoll NRPC, d. h. für den Zugriff über den Notes-Client. Über Internetprotokolle, also über Webmail (Protokolle HTTP/HTTPS) oder andere Mail-Clients (Protokolle POP3 oder IMAP) kann der Benutzer auch weiterhin zugreifen!

Wollen Sie auch den Zugriff über Internetprotokolle sperren, öffnen Sie das Serverdokument und navigieren Sie zum Register **Ports...** > **Internet-Ports...** und wählen Sie das betroffene Protokoll aus, etwa **Web**. Ändern Sie das Feld **Einstellungen zum Serverzugriff erzwingen** auf »Ja«. Verfahren Sie genauso mit allen anderen Protokollen, für die der Benutzer gesperrt werden soll.

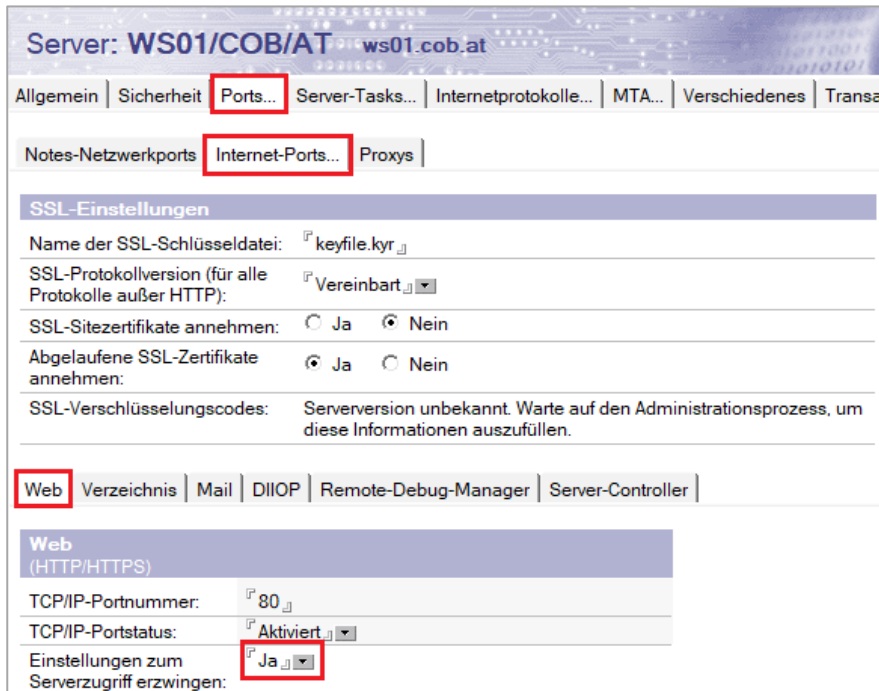


Abbildung 6.58: Einstellungen zum Serverzugriff erzwingen

Speichern und schließen Sie das Dokument.

6.11. Benutzer löschen

Auch das Löschen von Benutzern wird weitestgehend automatisiert vom Administrationsprozess erledigt. Haben Sie wie in Kap. 13.2.4 (auf Seite 341) vorgeschlagen eine Gruppe zum Ausschließen von Abgängern angelegt, können Sie die zu löschende Person auch gleich hinzufügen. Per Vorgabe kann eine gelöschte Person nämlich weiter zugreifen, so lange ihre ID-Datei nicht abgelaufen ist. (Die Einstellungen zum Serverzugriff finden Sie in Kap. 13.2.3 Den Serverzugriff steuern, ab Seite 340.)

Um einen Benutzer zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Admin-Client im Register **Personen und Gruppen** die zu löschende(n) Person(en) aus und klicken Sie auf **Werkzeuge > Personen > Löschen**.
2. Der Dialog Person löschen wird angezeigt (siehe Abbildung 6.59).

- Geben Sie an, ob die Maildatenbank gelöscht werden bzw. was mit der ID im Vault geschehen soll. Wählen Sie die Option »ID als inaktiv markieren und in der Vault belassen«, können Sie die ID später wieder aktivieren.

Zum Löschen einer ID aus dem Vault benötigen Sie die Rolle [Auditor].

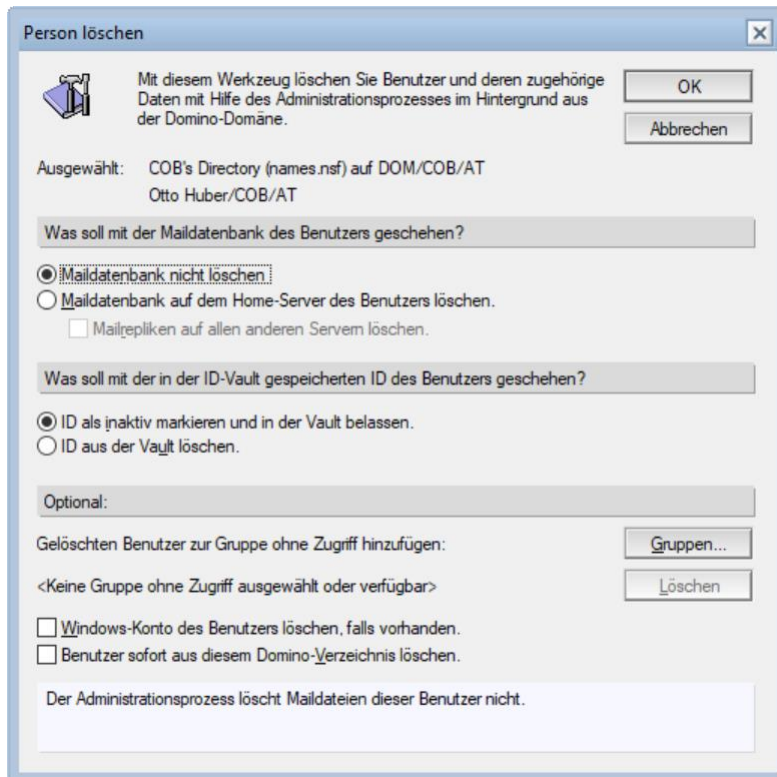


Abbildung 6.59: Dialog Person löschen

- Klicken Sie auf die Schaltfläche **Gruppen...**, um die zu löschende Person zu einer Gruppe ohne Zugriff hinzuzufügen.
- Klicken Sie auf **OK**.

Der Administrationsprozess wird beauftragt, die Person zu löschen. Ihre Anforderung wird wieder in einzelnen Schritten mit unterschiedlichen Planungstypen abgearbeitet:

Anforderung	Ausgeführt von	Planungstyp
Benutzer aus Vault löschen	Vault-Replikserver	Sofort
Person aus dem Domino-Verzeichnis löschen	Administrationsserver für das Domino-Verzeichnis	Intervall
In Personendokumenten löschen	Administrationsserver für das Domino-Verzeichnis	Täglich
In Zugriffskontrollliste löschen	Allen Servern (*)	Intervall
Person aus der Liste der ungelesenen Dokumente löschen	Allen Servern (*)	Intervall
Maildatei-Informationen zum	Mailserver	Sofort

Anforderung	Ausgeführt von	Planungstyp
Löschen abrufen		
Löschen der Maildatei bestätigen	Administrator	Bestätigung erforderlich
Löschen der Maildatei anfordern	Administrationsserver für das Domino-Verzeichnis	Sofort
Maildatei löschen	Mailserver	Intervall
In Gestaltungselementen löschen	Allen Servern (*)	Verzögert
In Leser-/Autorenfeldern löschen	Allen Servern (*)	Verzögert

Tabelle 6.11: Anforderungsschritte und Planungstypen beim Löschen einer Person

Hier nochmals der Hinweis, dass das Löschen von Benutzern aus Namens-, Leser- und Autorenfeldern zu unschönen und auch problematischen Effekten führen kann! Nicht nur dass es komisch aussieht, wenn in einem Dokument im Feld »Genehmigt von« niemand mehr steht, das Löschen von Namen aus einem Leserfeld kann auch den Dokumentzugriff verändern. Wenn der gelöschte Benutzer der einzige Eintrag war und das Leserfeld jetzt leer ist, sehen das Dokument wieder alle Leser und höher.

Wenn Sie nicht wollen, dass Personen aus Namensfeldern gelöscht werden, können Sie dies in der Zugriffskontrollliste einer Datenbank im Register **Erweitert** im Feld **Aktion** (auch kurzfristig) ändern:

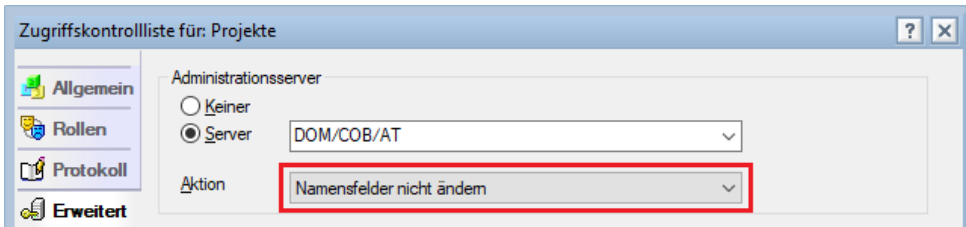


Abbildung 6.60: Einstellungen Administrationsserver in der Zugriffskontrollliste

Alternativ zum Ändern aller Zugriffskontrolllisten vor jedem Umbenennen oder Löschen können Sie auch die folgenden Einträge in die Datei notes.ini aufnehmen:

```
ADMINP_DISABLE_NAMEITEM_DELETE=1
ADMINP_DISABLE_READAUTH_DELETE=1
```

6.12. Gruppen verwalten

Mithilfe von Gruppen können Sie Mailverteiler aufbauen oder Zugriffsrechte zuordnen. Die Gruppenmitglieder können dabei händisch zugeordnet oder durch eine Formel berechnet werden. Da die Mitglieder in einem Gruppendokument stehen, spricht man auch von statischen Gruppen.

Das Feld **Mitglieder** (Members) weist – wie alle Felder mit eingeschalteter Summary-Eigenschaft (solche Felder können in Ansichten angezeigt werden) – eine Beschränkung von 15 Kilobyte auf, was je nach Länge der einzelnen Namen ein paar Hundert Einträge erlaubt. Sollten Sie damit nicht auskommen, schachteln Sie einfach mehrere Gruppen ineinander, d. h. machen Sie Gruppen zu Mitgliedern von anderen Gruppen. Für solche verschachtelte Gruppen (Nested Groups) gibt es ein Limit von 20 Ebenen, ich empfehle Ihnen allerdings, nicht mehr als vier zu verwenden.

Alternativ können Rechte auch mit einem Verweis auf die Hierarchie zugeordnet werden. So würde etwa der Eintrag */Verkauf/COB/AT in einer Zugriffskontrollliste allen Personen und Servern, die von dieser OU zertifiziert wurden, dasselbe Recht zuordnen. Diese Verweise werden auch **Dynamische Gruppen** genannt, weil kein Dokument dahintersteckt. Mit dynamischen Gruppen kann man allerdings keine Mailverteiler aufbauen ...

6.12.1. Gruppentypen

Es gibt in Domino die folgenden Gruppentypen:

Typ	Beschreibung
Mehrere Zwecke (Multi-purpose)	Können zur Rechtezuordnung und für Maillisten verwendet werden.
Nur Zugriffskontrollliste (Access Control List only)	Können zum Zuordnen von Zugriffsrechten in Zugriffskontrolllisten verwendet werden.
Nur Mail (Mail only)	Können nur für Maillisten verwendet werden.
Nur Server (Servers only)	Dürfen nur Server enthalten und können zum Replizieren und für Konfigurations- oder Programmdokumente verwendet werden.
Nur Negativliste (Deny List only)	Dienen zum Ausschluss von Personen vom Serverzugriff. Gruppen von diesem Typ werden in der Gruppenansicht nicht angezeigt und sind für Benutzer nicht sichtbar. Der Administrationsprozess löscht aus Gruppen dieses Typs keine Mitglieder.

Tabelle 6.12: Die verschiedenen Gruppentypen

6.12.2. Wer darf Gruppen erstellen?

Zum Erstellen von Gruppen müssen Benutzer im Domino-Verzeichnis über die folgenden Rechte verfügen:

- > das Grundrecht **Autor** mit der Zusatzrecht **Dokumente erstellen** oder höher
- > die Rolle [GroupCreator]

6.12.3. Gruppen erstellen

Um eine neue Gruppe zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Admin-Client zum Register **Personen und Gruppen** und dort zur Ansicht **Gruppen**. Klicken Sie auf die Taste **Gruppe hinzufügen**.
2. Geben Sie einen Namen für die Gruppe ein. Dieses Feld erlaubt Mehrfachwerte, d. h. Sie können bei Bedarf auch mehrere Synonyme durch Semikolons getrennt angeben. Der Gruppenname darf maximal 62 Zeichen lang sein. Verwenden Sie nur die folgenden Zeichen:
 - > Buchstaben (aA – zZ)
 - > Zahlen (0 – 9)
 - > Kaufmännisches Und (&)
 - > Bindestrich (-)
 - > Unterstrich (_)

- > Punkt (.)
- > Anführungszeichen (")
- > Leerzeichen

Wirklich verboten sind nur das At-Zeichen (@) und der doppelte Schrägstrich (//). Vermeiden Sie jedoch auch das Plus (+), die Raute (#) das Leer- und das Ist-gleich-Zeichen (=).

Handelt es sich bei der Gruppe um einen Mailverteiler, darf der Name nicht mit einem Vor- oder Nachnamen identisch sein. Sie können der Gruppe jedoch mit dem folgenden Eintrag in der notes.ini Priorität einräumen:

```
RouterExpansionAllowNonUniqueGroupMatch=1
```

3. Wählen Sie den Gruppentyp aus.
4. Optional: Wählen Sie eine Kategorie aus oder geben Sie eine neue ein.
5. Optional: Geben Sie eine kurze Beschreibung ein.
6. Bei Gruppen vom Typ **Mail** oder **Mehrere Zwecke**: Geben Sie die Domino-Domäne ein.
7. Optional (Bei Gruppen vom Typ **Mail** oder **Mehrere Zwecke**): Geben Sie eine Internetadresse ein. (Sie können nur eine Internetadresse angeben!)

Wenn Sie keine Internetadresse angeben, ist die Gruppe trotzdem via Internet erreichbar – außer Sie haben die Erreichbarkeit von Gruppen global abgeschaltet. In diesem Fall wird der Gruppenname mit der primären Internetdomäne kombiniert.

8. Wählen Sie entweder eine Methode zum automatischen Befüllen aus oder wählen Sie im Feld **Mitglieder** Personen und/oder Gruppen aus dem Adressdialog.

Beachten Sie das Limit von 15 K wie in der Einleitung beschrieben.

6.12.4. Automatisch befüllte Gruppen

Automatisch befüllte Gruppen (Auto-populated Groups) ermitteln und aktualisieren die Gruppenmitglieder anhand vordefinierter Kriterien. Zur Auswahl steht derzeit nur die Methode **Home-Server**, welche alle Personen berechnet, die den angegebenen Server als Mailserver eingetragen haben. Durch diese Methode eignen sich automatisch befüllte Gruppen besonders gut zum dynamischen Zuordnen von Benutzern zu Richtlinien.

In welcher Frequenz Gruppen aktualisiert werden, steuern Sie über das Verzeichnisprofil (Vorgabe ist 30 Minuten). Um das Verzeichnisprofil zu bearbeiten, wählen Sie im Domino-Verzeichnis in einer beliebigen Ansicht stehend den Befehl **Aktionen > Verzeichnisprofil bearbeiten**.

Um das Aktualisieren per sofort zu erzwingen, können Sie am Admin-Server des Domino-Verzeichnisses auch den folgenden Befehl eingeben:

```
tell autopop process
```

Autopop ist ein schweigsamer Task, der keinerlei Informationen anzeigt, egal, ob das Befüllen geklappt hat oder nicht. Sie können ihn mit dem folgenden Debug-Parameter in der Datei notes.ini jedoch zum Sprechen zwingen:

```
Debug_AutoPop=2
```

6.12.5. Gruppen delegieren

Um die Wartung einer Gruppe an jemanden zu delegieren, muss der Administrator die zuständige Person nach dem Erstellen des Gruppendokuments im Register **Administration** entweder im Feld **Administratoren** oder im Feld **Besitzer** eintragen. Um die Gruppe zu bearbeiten, reicht dann das Vorgaberecht Autor. Autoren mit der Rolle [GroupModifier] dürfen alle Gruppen bearbeiten.

6.12.6. Gruppen umbenennen

Ändern Sie den Namen der Gruppe nicht im Gruppendokument selbst, da sonst an anderen Stellen Referenzen auf den alten Namen bestehen bleiben. Beauftragen Sie stattdessen den Administrationsprozess mit der Umbenennung, der den Gruppennamen in allen ihm zugewiesenen Datenbanken korrigiert. Wählen Sie dazu im Domino-Administrator, Register **Personen und Gruppen**, die gewünschte Gruppe aus und klicken Sie auf den Befehl **Werkzeuge > Gruppen > Umbenennen...**

6.12.7. Gruppen löschen

Löschen Sie die Gruppe nicht einfach mit der Entferntaste, sondern wählen Sie im Domino-Administrator den Befehl **Werkzeuge > Gruppen > Löschen**. Die Gruppe wird dann vom Administrationsprozess gelöscht, der dafür sorgt, dass der Name überall verschwindet.

6.12.8. Geschützte Gruppen (Protected Groups)

Sie können Gruppen vor dem Löschen schützen, indem Sie diese im Verzeichnisprofil (Directory Profile) ins Feld **Löschen dieser Gruppen verhindern** aufnehmen. Bearbeiten Sie das Verzeichnisprofil mit dem Befehl **Aktionen > Verzeichnisprofil bearbeiten**:

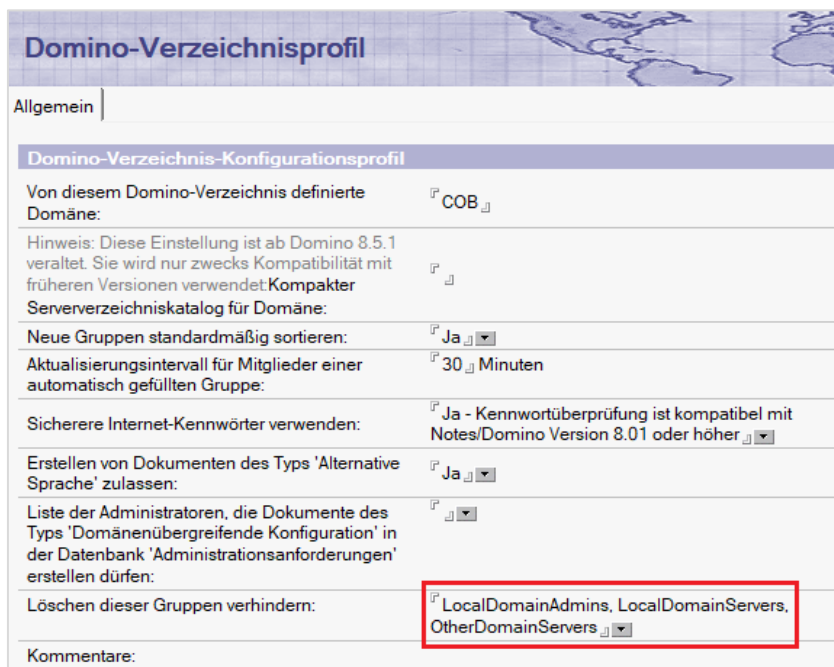


Abbildung 6.61: Domino-Verzeichnisprofil

6.12.9. Das Werkzeug Gruppen verwalten

Von vielen unterschätzt wird das Werkzeug **Gruppen verwalten**, welches sich im Domino-Administrator im Register **Personen und Gruppen** unter **Werkzeuge > Gruppen > Verwalten...** verbirgt. Hier können Sie einerseits die Gruppenzuordnung einer Person mit wenigen Klicks sichtbar machen und andererseits eine Person durch einfaches Ziehen und Ablegen einer Gruppe zuordnen oder aus einer Gruppe entfernen.

Das Werkzeug Gruppen verwalten bietet zwei verschiedene Arbeitsmodi an:

Im Modus **Alle Gruppenshierarchien** können Personen durch Ziehen auf den Gruppennamen (oder durch Klicken auf die Schaltfläche **Hinzu >>>**) einer Gruppe zugeordnet werden.

Ebenso ist es möglich, Personen durch Klicken auf die Schaltfläche **Entfernen** aus einer Gruppe zu entfernen.

Schalten Sie die Anzeige auf **Nur Mitgliedshierarchien** um, sehen Sie auf einen Blick, in welchen Gruppen eine Person Mitglied ist. Das funktioniert sogar bei verschachtelten Gruppen!

Ein Zuordnen zu Gruppen ist nach in diesem Modus allerdings nicht möglich.

Nachfolgend sehen Sie ein Beispiel für den Modus **Alle Gruppenshierarchien**:

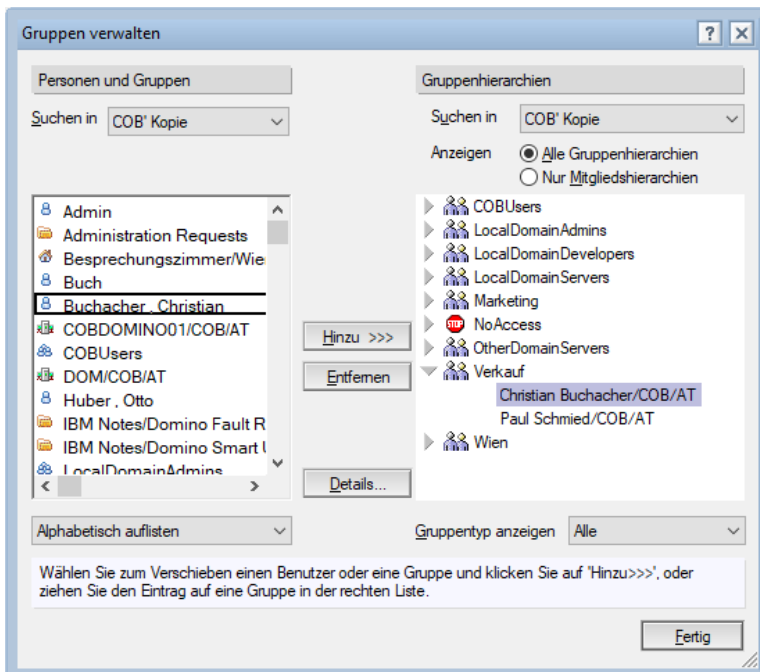


Abbildung 6.62: Gruppen verwalten – Alle Gruppenshierarchien

Und nachfolgend ein Beispiel für den Modus **Nur Mitgliedshierarchien**:

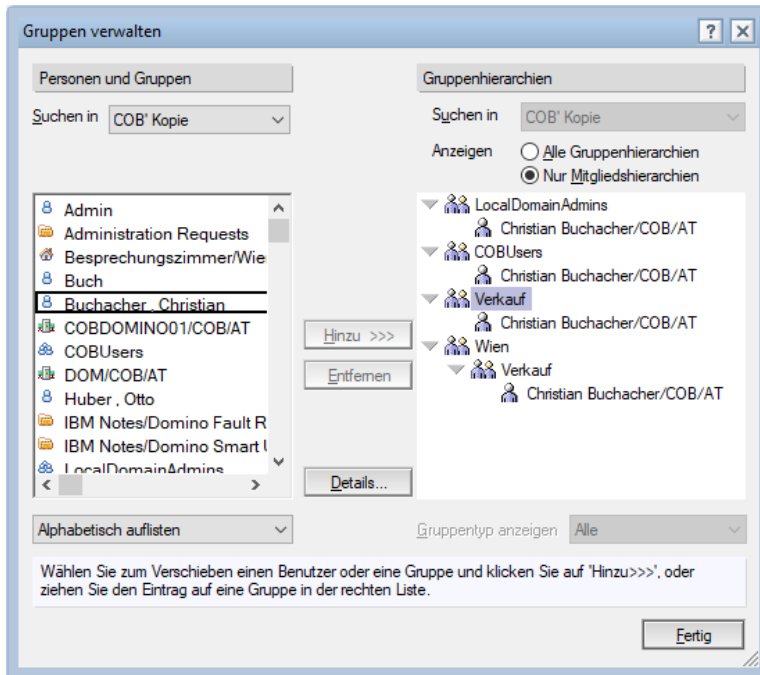


Abbildung 6.63: Gruppen verwalten – Nur Mitgliedshierarchien

6.13. Externe Verzeichnisse einbinden

Sie können fremde Domino- und LDAP-Verzeichnisse zum Nachschlagen von Mailadressen, aber auch zur Authentifizierung für externe Benutzer einbinden. Diese Fremdverzeichnisse können in Notes- und Web-Clients genutzt und über den LDAP-Task auch fremden LDAP-fähigen Clients (z. B. Microsoft Outlook) zum Nachschlagen von Mailadressen zur Verfügung gestellt werden. Zum Einbinden fremder Verzeichnisse benötigen Sie eine eigene Anwendung, die **Verzeichnishilfe** (Directory Assistance, DA) genannt wird. Über die Verzeichnishilfe kann außerdem eine Benutzersynchronisation zwischen dem Domino-Verzeichnis und einem fremden LDAP-Verzeichnis eingerichtet werden. Der häufigste Anwendungsfall dafür ist die Synchronisation mit dem Microsoft Active Directory.

6.13.1. Eine Verzeichnishilfe-Datenbank erstellen

Wenn die Datenbank Verzeichnishilfe noch nicht existiert, erstellen Sie diese zuerst. Gehen sie dazu wie folgt vor:

1. Wählen Sie dazu im Menü den Befehl **Datei > Anwendung > Neu...** oder drücken Sie [Strg]+[N]. Der Dialog **Neue Anwendung** wird angezeigt (siehe Abbildung 6.64).
2. Wählen Sie als Speicherort den gewünschten Server aus.
3. Geben Sie einen beliebigen Titel ein, z. B. »Verzeichnishilfe« oder »Directory Assistance« (die Datenbank gibt es nur auf Englisch).
4. Vergeben Sie einen beliebigen Dateinamen, z. B. »da.nsf«.
5. Wählen Sie als Schablonenserver den Server und setzen Sie ein Häkchen bei **Weitere Schablonen anzeigen**.

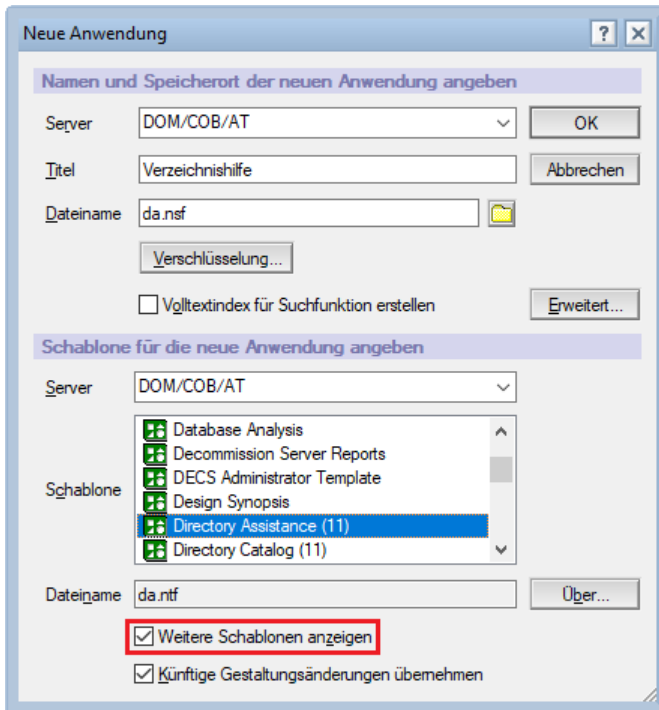


Abbildung 6.64: Die Anwendung Directory Assistance erstellen

6. Wählen Sie die Schablone »Directory Assistance (11)« (Dateiname: da.ntf) aus der Liste.
7. Klicken Sie auf **OK**, um die Datenbank zu erstellen.
8. Melden Sie die Verzeichnishilfe im Serverdokument, Register **Allgemein** an:

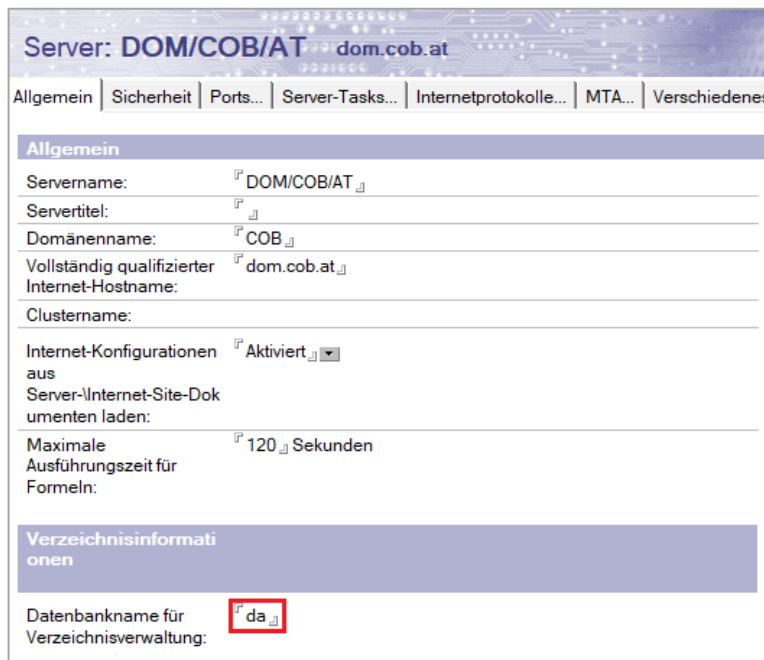


Abbildung 6.65: Die Anwendung Directory Assistance erstellen

6.13.2. Zusätzliche Domino-Verzeichnisse einbinden

6.13.2.1. Gründe für zusätzliche Domino-Verzeichnisse

Meist wird die Einführung eines zusätzlichen Verzeichnisses nötig, um den Anwendern externe Mailadressen von Kunden und/oder Lieferanten zentral zur Verfügung zu stellen. Die dazu verwendete Datenbank kann auf der Schablone des Domino-Verzeichnisses (pubnames.ntf) oder der Kontakte-Anwendung (pernames.ntf) basieren, es kann sich aber auch um eine eigene Anwendung (z. B. eine Kunden- oder CRM-Datenbank) handeln. Damit sich Ihre Anwendung in den Adressdialog integriert, müssen Sie (oder ein Entwickler) die dafür nötigen Ansichten aus dem Domino-Verzeichnis (bzw. der Schablone pubnames.ntf) hineinkopieren und für die dort verwendeten Feldnamen adaptieren.

Um eine Datenbank mit einem vom Domino-Verzeichnis abweichenden Design als Verzeichnis verwenden zu können, müssen die Ansichten (\$PeopleGroupsFlat), (\$PeopleGroupsHier), (\$PeopleGroupsByLang) und (\$PeopleGroupsCorpHier) vorhanden sein. Weitere Ansichten aus dem Domino-Verzeichnis (hier kommen alle mit der Ansichtsauswahl Type = "Person" infrage) können je nach Anwendungsfall hinzukommen, etwa die Ansicht (\$Users) zum Nachschlagen von Namen bei der Authentifizierung.

Ein zweiter Anwendungsfall ist das Einbinden von Benutzern und Gruppen aus fremden Domino-Verzeichnissen nach dem Austausch einer Querkulassung mit anderen Domino-Organisationen. In diesem Fall stellt das zusätzliche Verzeichnis nicht nur Mailadressen, sondern auch Öffentliche Schlüssel zum domänenübergreifenden Austausch von verschlüsselten Mails zur Verfügung.

Und letztendlich werden häufig zusätzliche Verzeichnisse eingeführt, um externe Benutzer getrennt von den eigenen speichern zu können, etwa Webbenutzer, die sich auf Ihrer Homepage registriert haben. In diesem Fall wird das zusätzliche Verzeichnis nicht nur zum Nachschlagen von externen Mailadressen, sondern auch zur Anmeldung (Authentifizierung) auf Ihrer Website verwendet.

6.13.2.2. Domino-Verzeichnisse einbinden

Um ein zusätzliches Domino-Verzeichnis oder eine entsprechend angepasste Domino-Anwendung als zusätzliches Verzeichnis einzubinden, gehen Sie wie folgt vor:

1. Öffnen Sie die Datenbank Verzeichnishilfe und klicken Sie auf die Schaltfläche **Add Directory Assistance**. (Die Anwendung ist nur auf Englisch verfügbar.)
2. Wählen Sie im Feld **Domain type** die Option »Notes« (Vorgabe).
3. Geben Sie im Feld **Domain name** den Namen der fremden Domäne ein.

Handelt es sich um das Verzeichnis einer fremden Domino-Organisation, geben Sie hier den tatsächlich verwendeten Domänennamen ein. Handelt es sich um ein zusätzliches Verzeichnis für alternative Mailadressen (etwa Ihre Kundendatenbank), geben Sie eine Fantasiedomäne an, z. B. »Kunden«.

Im Adressdialog wird später der Datenbanktitel angezeigt und nicht der hier angegebene Name.

4. (Optional) Geben Sie im Feld **Company name** einen Firmennamen ein. Der Firmenname hat rein informativen Charakter.
5. (Optional) Geben Sie im Feld **Search order** eine Zahl ein. Das ist nur relevant, wenn Sie mehrere Verzeichnisse via Directory Assistance einbinden und steuern wollen, in welcher Reihenfolge diese durchsucht werden sollen.

6. Wählen Sie im Feld **Make this domain available to** aus, welchen Clients die via Verzeichnishilfe eingebundenen Mailadressen zur Verfügung gestellt werden sollen.
Wählen Sie zumindest »Notes Client and Internet Authentication/Authorization«. Wählen Sie zusätzlich »LDAP Clients«, können auch externe LDAP-fähige Clients die via Verzeichnishilfe eingebundenen Mailadressen abfragen. Dazu muss der LDAP-Dienst auf Ihrem Domino-Server laufen.
7. (Optional) Wählen Sie im Feld **Group Authorization** die Option »Yes«, wenn Sie wollen, dass bei der Authentifizierung auch Gruppen aufgelöst werden. Dies ist nur relevant, wenn Sie das neue Verzeichnis auch zur Authentifizierung verwenden.
8. Achten Sie darauf, dass im Feld **Enabled** die Option »Yes« ausgewählt ist (Vorgabe).
9. (Optional) Geben Sie im Feld **Comments** einen Kommentar ein.

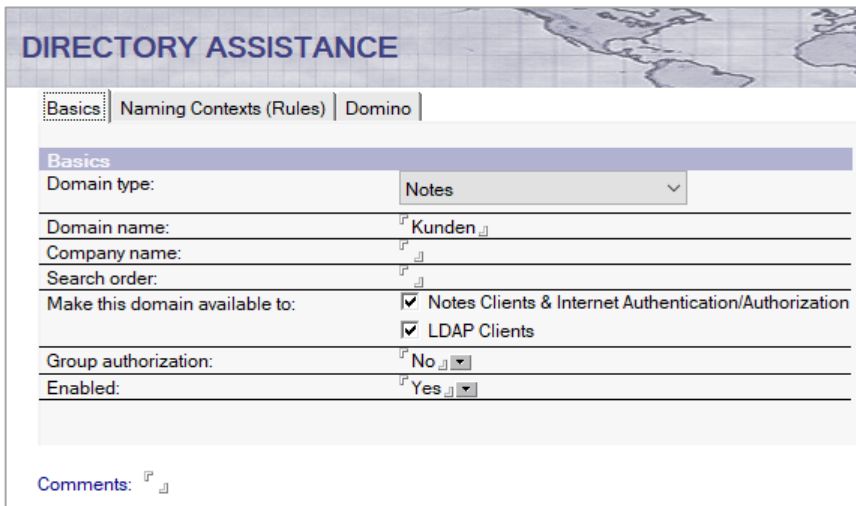


Abbildung 6.66: Directory Assistance, Register Basics

10. Wechseln Sie zum Register **Naming Contexts (Rules)**.
11. Ändern Sie die Regeln nur, wenn dies unbedingt nötig ist (z. B. zur Einschränkung auf eine bestimmte OU).
12. Achten Sie darauf, dass im Feld **Enabled** »Yes« ausgewählt ist (Vorgabe).
13. (Optional) Wollen Sie das neue Verzeichnis auch zur Authentifizierung verwenden, setzen Sie zusätzlich das Feld **Trusted for Credentials** auf »Yes«.

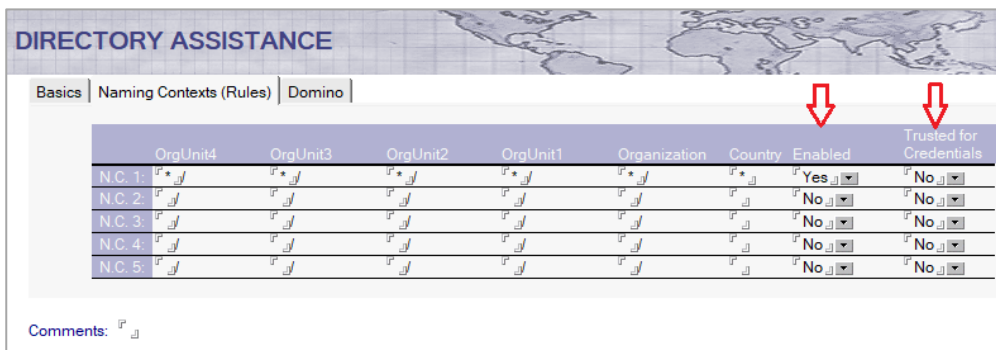


Abbildung 6.67: Directory Assistance, Register Naming Contexts (Rules)

14. Wechseln Sie zum Register **Domino**.
15. Geben Sie für das neue Verzeichnis bis zu fünf verschiedene Repliken an und vergessen Sie nicht, jeden Eintrag zu aktivieren (**Enabled** = »Yes«).

Wenn die erste Replik nicht verfügbar ist, etwa, weil der Server nicht läuft, wird automatisch zum nächsten Eintrag gewechselt.

Sie können alternativ auch Datenbank-Links in das Feld **Application-Links** einfügen, allerdings mit dem Nachteil, dass Sie nicht erkennen können, worauf die Links verweisen.

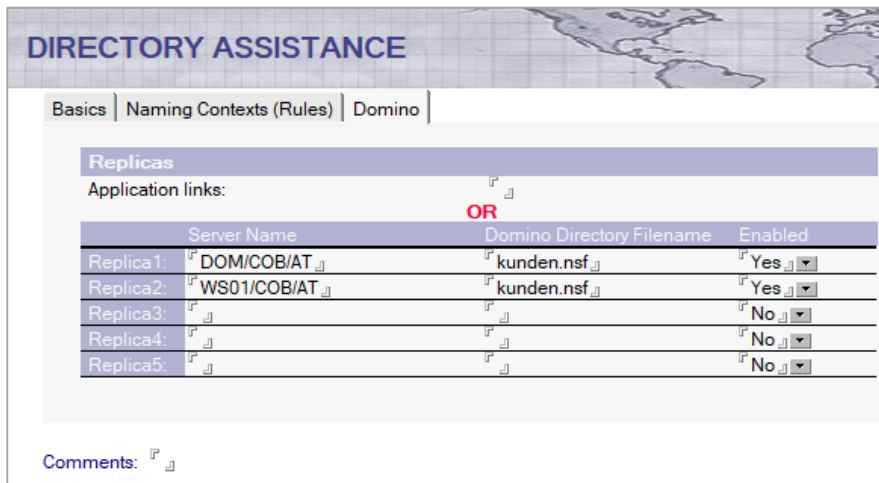


Abbildung 6.68: Directory Assistance, Register Domino

16. Speichern und schließen Sie das Dokument.
17. Nach einem Neustart des Servers und des Clients sollte im Adressdialog ein zusätzlicher Eintrag mit dem Titel des neu eingebundenen Verzeichnisses angezeigt werden.

6.13.3. LDAP-Verzeichnisse einbinden

Auch LDAP-Verzeichnisse werden via Verzeichnishilfe angebunden, die Einrichtung ist allerdings etwas aufwendiger. Externe LDAP-Verzeichnisse können sowohl zum Nachschlagen von Mailadressen als auch zur Authentifizierung verwendet werden.

Haben Sie die Anwendung Verzeichnishilfe noch nicht erstellt, folgen Sie den Anweisungen in Kap. 6.13.1 Eine Verzeichnishilfe-Datenbank erstellen, ab Seite 180.

Je nach Verzeichnistyp gibt es beim Einrichten mehrere Optionen. Im folgenden Beispiel soll ein Microsoft Active Directory zur Authentifizierung von Webbenutzern angebunden werden. Grundvoraussetzung dafür ist, dass sowohl der Windows-Server, der den Domino-Server hostet, als auch der Windows-PC, auf dem Ihr Domino-Administrator läuft, Mitglieder der Windows-Domäne sind.

Um ein Active Directory als fremdes LDAP-Verzeichnis einzubinden, gehen Sie wie folgt vor:

1. Öffnen Sie die Datenbank Verzeichnishilfe und klicken Sie auf die Schaltfläche **Add Directory Assistance**. (Die Anwendung ist nur auf Englisch verfügbar.)
2. Wählen Sie im Feld **Domain type** die Option »LDAP«.
3. Geben Sie im Feld **Domain name** einen beliebigen Namen für die fremde Domäne ein.

4. (Optional) Geben Sie im Feld **Company name** einen Firmennamen ein. Der Firmenname hat rein informativen Charakter.
5. (Optional) Geben Sie im Feld **Search order** eine Zahl ein. Das ist nur relevant, wenn Sie mehrere Verzeichnisse via Directory Assistance einbinden und steuern wollen, in welcher Reihenfolge diese durchsucht werden sollen.
6. Wählen Sie im Feld **Make this domain available to** aus, welchen Clients die via Verzeichnishilfe eingebundenen Mailadressen zur Verfügung gestellt werden sollen.
Wählen Sie zumindest »Notes Client and Internet Authentication/Authorization«. Wählen Sie zusätzlich »LDAP Clients«, können auch externe LDAP-fähige Clients die via Verzeichnishilfe eingebundenen Mailadressen abfragen. Dazu muss der LDAP-Dienst auf Ihrem Domino-Server laufen.
7. (Optional) Wählen Sie im Feld **Group Authorization** die Option »Yes«, wenn Sie wollen, dass bei der Authentifizierung auch Gruppen aufgelöst werden.
8. Achten Sie darauf, dass im Feld **Enabled** die Option »Yes« ausgewählt ist (Vorgabe).
9. (Optional) Geben Sie im Feld **Comments** einen Kommentar ein.

The screenshot shows the 'DIRECTOR ASSISTANCE' configuration window with the 'Basics' tab selected. The configuration is as follows:

Basics	
Domain type:	LDAP
Domain name:	cob.local
Company name:	COB
Search order:	
Make this domain available to:	<input checked="" type="checkbox"/> Notes Clients & Internet Authentication/Authorization <input type="checkbox"/> LDAP Clients <input type="checkbox"/> Directory Sync
Group authorization:	Yes
Use exclusively for group authorization or credential authentication:	No
Nested group expansion:	Yes
Enabled:	Yes
SSO Configuration	
Attribute to be used as name in an SSO token (map to Notes LTPA_UsrNm):	
Windows single sign-on for Web clients	<input type="checkbox"/> Enabled

Abbildung 6.69: Directory Assistance, Register Basics

10. Wechseln Sie zum Register **Naming Contexts (Rules)**.
11. Achten Sie darauf, dass im Feld **Enabled** »Yes« ausgewählt ist (Vorgabe).
12. Da wir das neue Verzeichnis auch für die Authentifizierung verwenden wollen, setzen Sie zusätzlich das Feld **Trusted for Credentials** auf »Yes«.
13. Wechseln Sie zum Register **LDAP**.
14. Geben Sie den Hostnamen des Active-Directory-Servers ein oder klicken Sie auf die Schaltfläche **Suggest**, um sich den Hostnamen vorschlagen zu lassen. (Die Schaltfläche Suggest funktioniert nur, wenn der Domino-Administrator auf einem Windows-PC läuft, der Mitglied in der Domäne ist.)

15. Wählen Sie im Feld **LDAP vendor** die Option »Active Directory«.
16. Geben Sie Anmeldedaten ein, mit denen ein Zugriff auf das Active Directory möglich ist. Klicken Sie anschließend auf die Schaltfläche **Verify**, um zu überprüfen, ob die Anmeldung erfolgreich war. (Die Schaltfläche Verify funktioniert nur, wenn der Domino-Administrator auf einem Windows-PC läuft, der Mitglied in der Domäne ist.)
17. Geben Sie im Feld **Base DN for search** (DN steht für Distinguished Name) den Speicherort an, unter dem die Benutzer in Ihrem AD abgelegt sind. Wie die Suchbasis genau aussieht, hängt von der Struktur Ihres Active Directories ab. Sie können auch auf die Schaltfläche **Suggest** klicken, um sich eine Suchbasis vorschlagen zu lassen.
18. Wählen Sie im Feld **Channel encryption** die Option »SSL«, wenn die Kommunikation mit dem Server verschlüsselt ablaufen muss, ansonsten bleiben Sie bei »None«.
19. Setzen Sie ein Häkchen bei **Enable name mapping** und geben Sie im Feld **Attribute to be used as Notes distinguished name** das Feld im AD an, das den Notes-Namen enthält, dem der Benutzer zugeordnet werden soll. Haben Sie ein solches Feld nicht angelegt, können Sie jedes im AD unbenutzte Feld verwenden, um den Namen einzugeben, z. B. das Feld »Info« (siehe Abbildung 6.71).
20. Wählen Sie im Feld **Type of search filter to use** die Option »Active Directory« aus.

DIRECTORY ASSISTANCE

Basics | Naming Contexts (Rules) | **LDAP**

Configure Directory Assistance access to a remote LDAP server.

LDAP Configuration

Hostname: dom.cob.local [Suggest] [Verify]

LDAP vendor: Active Directory

Optional authentication credential for search: Username: cob/Admin [Verify]
Password: *****

Base DN for search: DC=cob,DC=local [Suggest] [Verify]

Connection Configuration

Channel encryption: None

Port: 389

Advanced Options

Timeout: 60 seconds

Maximum number of entries returned: 100

Dereference alias on search: Always

Preferred mail format: Internet Mail Address

Enable name mapping

Attribute to be used as Notes distinguished name: Info [Verify]

Attribute is to be used for all lookups: No

Type of search filter to use: Active Directory [Suggest] [Verify]

Abbildung 6.70: Directory Assistance, Register LDAP

21. Speichern und schließen Sie das Dokument.
22. Tragen Sie im Active Directory den Namen des zugeordneten Notes-Benutzers ein, in unserem Beispiel in das Feld Info. Verwenden Sie die kanonische Schreibweise und achten Sie darauf, die einzelnen Namenskomponenten durch Kommas zu trennen.

Aus Max Mustermann/COB/AT wird somit CN=Max Mustermann, O=COB, C=AT.

Sie können einem Notes-Benutzer auch mehrere AD-Benutzer zuordnen.

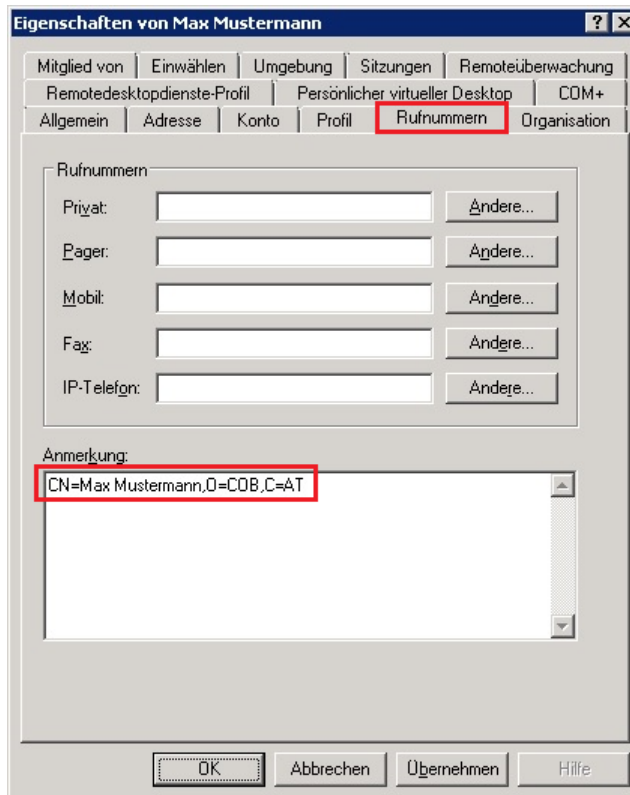


Abbildung 6.71: Active Directory, Benutzereigenschaften, Register Rufnummern

23. Starten Sie den Server neu.

Nach dem Neustart können Sie zu den Zugriffskontrolllisten der Datenbanken die zugeordneten Notes-Benutzer hinzufügen. LDAP-Benutzer können sich dann via Webbrowser mit ihren Namen und Kennwörtern aus dem Active Directory am Domino-Server anmelden und erhalten die Rechte des ihnen zugeordneten Notes-Benutzers zugewiesen.

Über folgenden Befehl auf der Serverkonsole erhalten Sie Informationen zu allen via Verzeichnis-hilfe angebotenen fremden Verzeichnissen:

```
show xdir
```


7. Kalender und Zeitplanung

- > 7.1 Übersicht, Seite 189
- > 7.2 Die Zeitplanungsdatenbank, Seite 190
- > 7.3 Die Anwendung Ressourcenreservierung, Seite 192
- > 7.4 Feiertage verwalten, Seite 199

7.1. Übersicht

Die Zeitplanungsfunktionen ermöglichen es Benutzern, die freie Zeit von Personen und Ressourcen abzufragen und so Besprechungen zu planen bzw. Ressourcen auch allein zu reservieren.

Das Abfragen von freien Zeiten wird durch das **Zeitplanungssystem** (Free Time System), eine Kombination aus den Servertasks **Schedule Manager** (Sched), **Calendar Connector** (Calconn) und nnotes zur Verfügung gestellt. Bei der Installation werden diese Tasks automatisch zur notes.ini-Variablen ServerTasks hinzugefügt und mit dem Domino-Server mitgestartet. Beim ersten Serverstart erstellt der Schedule Manager die Zeitplanungsdatenbank (busytime.nsf) und erstellt für jeden Benutzer mit einer Maildatenbank auf diesem Server ein Dokument. Entscheidend dafür ist ein hierarchischer Name im Kalenderprofil der Maildatenbank.

Im Kalenderprofil steuert der Benutzer, wer Zugriff auf seinen Zeitplan haben soll und welche Informationen anderen beim Planen von Besprechungen angezeigt werden sollen (nur Zeiten oder auch Orte, Räume etc.). Wenn ein Benutzer andere zu einer Besprechung einlädt, schlägt das Zeitplanungssystem die Verfügbarkeiten der Eingeladenen nach, wenn diese den Zugriff auf ihren Zeitplan freigegeben haben. Die Überprüfung erfolgt am Mailserver des Benutzers durch den Servertask Schedule Manager, serverübergreifend über den Calendar Connector, je nachdem wo die Maildatenbanken der Eingeladenen liegen. Innerhalb derselben Domäne funktioniert das automatisch – Sie als Administrator müssen dafür nichts konfigurieren.

Die Verfügbarkeiten von Ressourcen wie Räume und anderen Hilfsmittel (Projektoren, Tafeln u. a.) werden analog überprüft, dafür kommt am selben Server jedoch der Servertask **Rooms and Resources Manager** (RnRMgr) zum Einsatz.

Entscheidend sind bei Personen die Maildatenbanken mit einem Feld \$BusyName im Mailprofil bzw. die Ressourcen-Dokumente in der Anwendung Ressourcenreservierung und in jedem Dokument, das in die Datenbank busytime.nsf übertragen wird (Kalendereinträge, Reservierungen).

Als Administrator können Sie außerdem Feiertage verwalten. HCL Domino bringt für 35 Länder jeweils einen Satz von Feiertagen mit, die bearbeitet und ergänzt werden können. Endanwender können die vom Administrator bereitgestellten Feiertage in ihren Kalender importieren und abgleichen.

7.2. Die Zeitplanungsdatenbank

Die Datenbank busytime.nsf enthält also für alle Räume, die reserviert und alle Personen, die eingeladen werden können, einen Eintrag. Fehlt dieser Eintrag, kann der Raum nicht reserviert, die Person nicht eingeladen werden.

In geclusterten Umgebungen erstellt der Schedule Manager eine geclusterte Version der Zeitplanungsdatenbank mit dem Namen clubusy.nsf. Die geclusterte Version funktioniert prinzipiell gleich wie die normale, enthält aber alle Benutzer, deren Maildatenbank auf einem der Cluster-Server liegt. Jeder Cluster-Server besitzt eine Replik der clubusy.nsf, die Informationen werden via Cluster-Replikation rasch abgeglichen.

Der Vorteil der geclusterten Zeitplanverwaltung ist natürlich, dass Zeitplaninformationen auch zur Verfügung stehen, wenn ein Mailserver ausgefallen ist, weil die Benutzer eine Replik auf einem anderen Server durchsuchen können. Daraus ergeben sich auch Performancevorteile, weil der Benutzer auch die lokale Zeitplandatenbank durchsuchen kann, wenn die Maildatenbank eines Eingeladenen auf einem anderen Server liegt.

Fügen Sie einen ursprünglich nicht geclusterten Server zu einem Cluster hinzu, löscht der Schedule Manager die Datenbank busytime.nsf und erstellt stattdessen die Datei clubusy.nsf, die dann mit anderen Cluster-Servern repliziert. Wenn Sie einen Server aus einem Cluster entfernen, passiert das Gegenteil: Der Schedule Manager löscht clubusy.nsf und erstellt busytime.nsf. (In diesem Fall dauert es dann eine Weile, bis der Schedule Manager die Einträge aktualisiert hat.)

7.2.1. Zeiten innerhalb derselben Domäne abfragen

1. Ein Benutzer erstellt eine Besprechungseinladung und fragt die verfügbaren Zeiten eines Eingeladenen ab.
2. Eine Freie-Zeit-Abfrage wird an den Mailserver des Benutzers geschickt.
3. Das Zeitplanungssystem schlägt den Namen des Eingeladenen in der Zeitplanungsdatenbank (busytime.nsf oder clubusy.nsf) auf dem Mailserver des Benutzers nach.

Wenn beide denselben Mailserver haben oder wenn der Mailserver von beiden zum selben Cluster gehört, findet das Zeitplanungssystem die Information und sendet die Planungszeiten des Eingeladenen an den Benutzer zurück.

4. Wenn das Zeitplanungssystem keine Information über den Eingeladenen findet, konvertiert es den Namen des Eingeladenen in den voll qualifizierten Namen und sucht im Domino-Verzeichnis nach dem Personendokument. Wird das Personendokument gefunden, wird vom Calendar Connector eine Anfrage an den Mailserver des Eingeladenen geschickt.

Ist der Mailserver des Eingeladenen nicht erreichbar, wird eine Nachricht geschickt, dass der Server unerreichbar ist und die Informationen nicht verfügbar sind.

5. Das Zeitplanungssystem auf dem Mailserver des Eingeladenen schlägt in der Zeitplanungsdatenbank busytime.nsf nach und schickt via Calendar Connector die Informationen an den Benutzer zurück.

Findet das Zeitplanungssystem keine Information, geht die Freie-Zeit-Abfrage schief und die Informationen des Eingeladenen werden als nicht verfügbar angezeigt.

7.2.2. Zeiten zwischen verschiedenen Domänen abfragen

1. Ein Benutzer erstellt eine Besprechungseinladung und fragt dabei die verfügbaren Zeiten eines Eingeladenen ab.
2. Eine Freie-Zeit-Abfrage wird an den Mailserver des Benutzers geschickt.
3. Aufgrund der Adressierung stellt das Zeitplanungssystem fest, dass sich der Eingeladene in einer anderen Domäne befindet und sucht nach einem Domänenendokument.
4. Findet das Zeitplanungssystem ein benachbartes Domänenendokument mit einem eingetragenen Kalenderserver, schickt es die Anfrage an diesen weiter.

Findet das Zeitplanungssystem ein benachbartes Domänenendokument ohne Kalenderserver, schlägt die Freie-Zeit-Abfrage fehl und die Informationen des Eingeladenen werden als nicht verfügbar angezeigt.

Findet das Zeitplanungssystem ein nicht benachbartes Domänenendokument, leitet es die Anfrage an den im Feld **Anforderungen über diesen Kalenderserver übertragen** eingetragenen Server weiter.

Findet das Zeitplanungssystem ein nicht benachbartes Domänenendokument ohne Kalenderserver-Route schlägt die Freie-Zeit-Abfrage fehl und die Informationen des Eingeladenen werden als nicht verfügbar angezeigt.

Findet das Zeitplanungssystem überhaupt kein Domänenendokument, schlägt die Freie-Zeit-Abfrage fehl und die Informationen des Eingeladenen werden als nicht verfügbar angezeigt.

7.2.3. Zeitplanung zwischen Domänen ermöglichen

Für Benutzer innerhalb derselben Domino-Domäne funktioniert die Zeitplanung automatisch in geclusterten und nicht geclusterten Umgebungen. Sie müssen nur eine Datenbank zur Ressourcenreservierung erstellen, damit Benutzer Räume und andere Ressourcen reservieren können.

Für Benutzer aus benachbarten (Adjacent) Domino-Domänen (das sind Domänen, die direkt über ein Verbindungsdokument angebunden sind) müssen Sie ein Domänenendokument im Domino-Verzeichnis erstellen. Gehen Sie dazu wie folgt vor:

1. Starten Sie den Domino-Administrator und navigieren Sie zum Register **Konfiguration**.
2. Wechseln Sie zur Ansicht **Nachrichten > Domänen** und klicken Sie auf die Schaltfläche **Domäne hinzufügen**, um ein Domänenendokument zu erstellen. Wählen Sie im Feld **Domäentyp** »Benachbarte Domäne« (Adjacent Domain).
3. Wechseln Sie zum Register **Kalenderinformationen** und geben Sie im Feld **Kalenderservername** den Namen des Servers, an der die Zeitplanabfragen in der benachbarten Domäne verarbeiten soll.
4. Berücksichtigen Sie die Benutzer aus der benachbarten Domäne gegebenenfalls auch in der Zugriffskontrollliste der Ressourcenreservierung.

7.2.4. Serverbefehle zur Wartung der Zeitplanungsdatenbank

Die Befehle zur Wartung der Zeitplanungsdatenbank entnehmen Sie bitte Tabelle 7.1:

Befehl	Erklärung
<code>tell sched show <Benutzer></code> <code>tell rnmgr show <Ressource></code>	Dieser Befehl zeigt die gebuchten Zeiten. Er durchsucht busytime.nsf und listet alle Einträge für den betreffenden Benutzer/Raum auf.
<code>tell sched list <Benutzer></code> <code>tell rnmgr list <Ressource></code>	Dieser Befehl zeigt die Einstellungen aus dem Profildokument inklusive der verfügbaren Zeiten.
<code>tell sched check <Benutzer></code> <code>tell rnmgr check <Ressource></code>	Dieser Befehl gleicht die Einträge im Kalender mit jenen in der Datenbank busytime.nsf ab. Fehlende Einträge werden zu busytime.nsf hinzugefügt.
<code>tell sched validate <Benutzer></code> <code>tell rnmgr validate <Ressource></code>	Eine Validierung findet standardmäßig um 2:00 Uhr statt. Verwenden Sie diesen Befehl, um neue Ressourcen/Räume per sofort in die Datenbank busytime.nsf aufzunehmen oder nach dem Löschen daraus zu entfernen. Verwenden Sie diesen Befehl nicht, wenn Sie einen neuen Benutzer hinzufügen. (Der Administrationsprozess erstellt Personendokumente für Benutzer im Domino-Verzeichnis und legt erst dann die Maildatei der Benutzer an. Der Schedule Manager überwacht das Erstellen von Datenbanken und findet automatisch die Maildateien neuer Benutzer.)

Tabelle 7.1: Befehle zur Wartung der Zeitplanungsdatenbank

Verwenden Sie für die Platzhalter <Benutzer> und <Ressource> immer hierarchische Namen, also nach dem Format Vorname Nachname/OU/O/C bzw. Ressourcenname/Standort.

Alle Befehle funktionieren auch ohne Angabe eines Benutzers / Raums. In diesem Fall werden alle Profile auf dem Server berücksichtigt. Vor allem der Befehl check kann sehr lange dauern und sollte nicht zur Hauptarbeitszeit eingegeben werden.

7.3. Die Anwendung Ressourcenreservierung

In der Datenbank zur Ressourcenreservierung planen und reservieren Benutzer Räume und sonstige Ressourcen. Dabei kann es sich um Seminarbehelfe wie Beamer, Overheadprojektoren oder Tafeln handeln, manche Unternehmen verwalten damit aber auch ihren Fuhrpark. Benutzer können entweder den Raum oder die Ressource selbst auswählen und dann nach freien Zeiten suchen oder die Zeiten vorgeben und sich Räume oder Ressourcen vorschlagen lassen.

Die Datenbank zur Ressourcenreservierung enthält drei Dokumenttypen: Standortprofile, Ressourcen und Reservierungen. Das Standortprofil definiert, wo sich die Ressourcen befinden. Das Ressourcendokument selbst definiert Art und Name der Ressource und nach welchen Regeln sie reserviert werden darf.

Nachdem Sie mindestens ein Standortprofil und einen Raum oder eine Ressource erstellt haben, überprüft der **Rooms & Resources Manager** (RnRMgr) auf dieselbe Weise die freie Zeit wie der Schedule Manager für Benutzer.

7.3.1. Die Datenbank erstellen

Um einen Raum oder eine Ressource zu reservieren, kann der Benutzer entweder direkt in der Ressourcenreservierung eine Reservierung erstellen oder die Ressource auch über eine Besprechungseinladung reservieren.

Um eine Anwendung zur Ressourcenreservierung zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie **Datei > Anwendung > Neu...** oder drücken Sie [Strg]+[N].
2. Der Dialog **Neue Anwendung** wird angezeigt (siehe Abbildung 7.1).
3. Wählen Sie im Feld **Server** den Server, auf dem die Anwendung erstellt werden soll.
4. Geben Sie einen beliebigen Titel und Dateinamen ein.
5. Wählen Sie als Schablonenserver einen Server.
6. Aktivieren Sie das Kontrollkästchen **Weitere Schablonen anzeigen**, um die Schablone »Ressourcenreservierungen (11.0)« (resrc11.ntf) in der Liste vorzufinden.
7. Klicken Sie zum Erstellen der Anwendung auf **OK**.

Überprüfen Sie nach dem Erstellen die Zugriffskontrollliste der Datenbank:

- > Gewähren Sie den Benutzern mindestens Autorrechte mit dem Zusatzrecht, Dokumente zu löschen.
- > Sollen Benutzer Reservierungen direkt in der Anwendung Ressourcenreservierung erstellen dürfen, gewähren Sie ihnen Editorrechte.
- > Manager benötigen die Rolle [CreateResource], um Ressourcen erstellen zu dürfen.

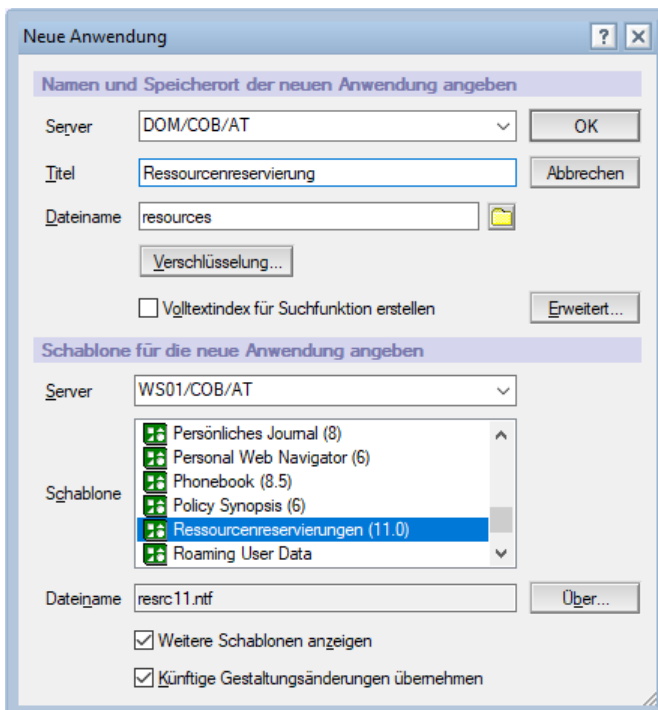


Abbildung 7.1: Neue Anwendung – Ressourcenreservierung

7.3.2. Ein Standortprofil erstellen

Erstellen Sie zuerst einen Standort. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie die Anwendung Ressourcenreservierung und wählen Sie die Ansicht **Reservierungen** > **Nach Datum**.
2. Klicken Sie auf die Schaltfläche **Neuer Standort**.

Sollten Sie die Schaltfläche nicht sehen, überprüfen Sie in der ACL, ob Sie über die Rolle [CreateResource] verfügen.

3. Geben Sie einen Namen ein, z. B. den Ort oder die Straße.
4. Stellen Sie gegebenenfalls den Domänennamen richtig.
5. Geben Sie an, ob an Reservierungen erinnert werden soll und wie viele Tage zuvor.
6. Speichern und schließen Sie das Dokument.

7.3.3. Eine Ressource erstellen

Zum Erstellen einer Ressource gehen Sie wie folgt vor:

1. Öffnen Sie die Anwendung Ressourcenreservierung und wählen Sie die Ansicht **Reservierungen** > **Nach Datum**.
2. Klicken Sie auf die Schaltfläche **Neue Ressource**.

Sehen Sie die Schaltfläche nicht, überprüfen Sie in der ACL, ob Sie über die Rolle [CreateResource] verfügen.

3. Wählen Sie als Ressourcentyp »Raum« oder »Andere«. (Einen Online-Besprechungsbereich können Sie nur anlegen, wenn Sie das Produkt HCL Sametime im Einsatz haben.)
4. (Optional) Geben Sie eine kurze Beschreibung der Ressource ein.
5. Wenn Sie einen Raum anlegen, geben Sie zusätzlich die Kapazität an.
6. Wenn Sie eine andere Ressource anlegen, geben Sie eine Kategorie an.
7. Geben Sie eine Internetadresse für die Ressource ein.
8. Weisen Sie der Ressource bei Bedarf Besitzerbeschränkungen zu.

»Keine« – Jeder kann die Ressource reservieren, nach dem Motto: Wer zuerst kommt, malt zuerst.

»Nur Besitzer« – Der Besitzer kann die Ressource direkt reservieren, alle anderen brauchen die Genehmigung des Besitzers. Sinnvoll für wertvolle Ressourcen, die man nicht leichtfertig hergeben möchte. Wenn Sie diese Option auswählen, müssen Sie einen oder auch mehrere Besitzer angeben.

»Bestimmte Personen« – Nur die in der Liste aufgeführten Personen können die Ressource reservieren.

»Automatische Verarbeitung« – Die in der Liste aufgeführten Personen können die Ressource direkt buchen, alle anderen benötigen die Bestätigung des Besitzers.

»Reservierungen deaktivieren« – Reservierungen sind vorübergehend nicht möglich.

9. Geben Sie im Bereich Verfügbarkeitseinstellungen die verfügbaren Uhrzeiten pro Tag ein oder aktivieren Sie »24 Stunden jeden Tag«.

10. Sie haben außerdem die Möglichkeit, das Reservieren der Ressource im Voraus zu beschränken, z. B. max. 90 Tage vorher.
11. Durch Klicken auf die Schaltfläche **Speichern und schließen** wird ein Auftrag an den Administrationsprozess gestellt, die neue Ressource ins Domino-Verzeichnis zu übertragen:

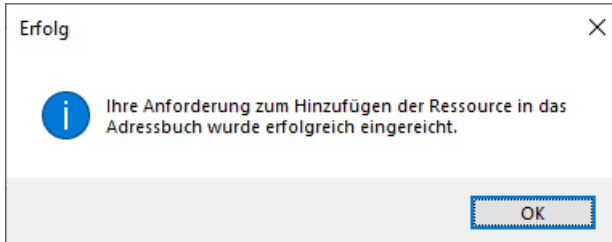


Abbildung 7.2: Neue Ressource eingereicht

12. Der Auftrag wird vom Administrationsserver des Domino-Verzeichnisses mit der Priorität »Sofort« verarbeitet. Sollten Sie die Ressource auf einem anderen Server eingereicht haben, sorgen Sie dafür, dass der Auftrag zum Administrationsserver repliziert wird.

Die Ressource kann erst reserviert werden, wenn sie in die Datenbank busytime.nsf aufgenommen wurde.

Um diesen Vorgang zu beschleunigen, verwenden Sie den folgenden Befehl:

```
tell rnmgr validate <Ressource/Standort>
```

7.3.4. Ändern und Löschen von Ressourcen

Nach dem Erstellen einer Ressource können Sie die folgenden Informationen direkt ändern: Verfügbarkeit, Beschreibung, Kapazität, Kommentare und die Besitzerfelder. Zum Ändern des Namens steht die Aktion **Ressource umbenennen** zur Verfügung (die Schaltfläche wird erst nach dem Umschalten in den Bearbeitungsmodus sichtbar).

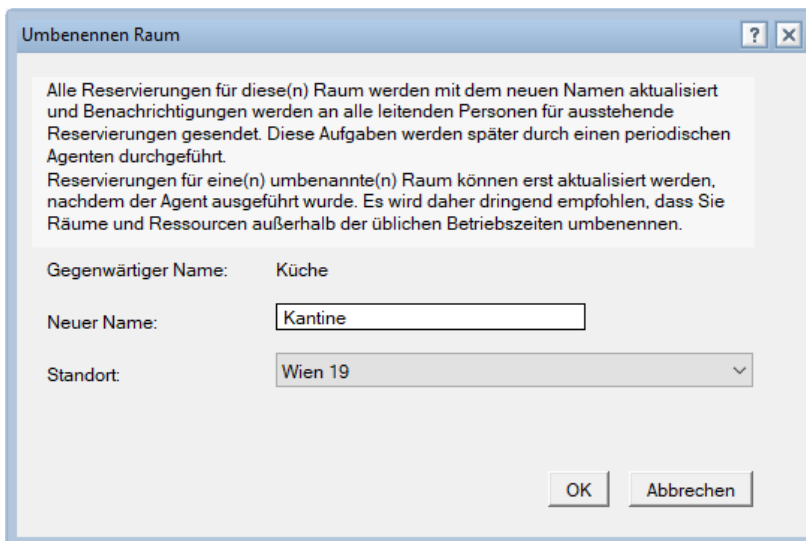


Abbildung 7.3: Ressource umbenennen

Beachten Sie, dass der Administrationsprozess die Änderungen ins Domino-Verzeichnis überträgt. Dazu wird in der Datenbank für Administrationsanforderungen (admin4.nsf) eine Anforderung

erstellt, die den Planungstyp »Intervall« zugeordnet hat. Die Vorgabe dafür ist einmal stündlich, wollen Sie nicht darauf warten, dann geben Sie folgenden Befehl ein:

```
tell adminp process interval
```

Beim Umbenennen wird zusätzlich der Agent »RenameReservations and SendNotice« aktiviert, welcher per Vorgabe alle 30 Minuten läuft und den Namen der Ressource in Reservierungen richtigstellt.

Löschen Sie eine Ressource aus der Anwendung Ressourcenreservierung, wird in der Anwendung Administrationsanforderungen (admin4.nsf) eine Anforderung zur Löschung aus dem Domino-Verzeichnis erstellt. Um die Löschung abzuschließen, müssen Sie die Anforderung genehmigen.

7.3.5. Die Agenten in der Ressourcenreservierung aktivieren

Die Datenbank Ressourcenreservierung enthält vier Agenten, die zur Gewährleistung des vollen Funktionsumfangs der Anwendung aktiviert werden müssen:

- > Autoreminder
- > Purge Documents (Auto)
- > RenameReservations and SendNotice
- > Update Blocker Documents

Öffnen Sie dazu die Datenbank im Admin- oder auch Notes-Client und wählen Sie im Menü **An-sicht > Agenten**. Die Liste der Agenten sollte im Domino-Designer geladen werden.

Wählen Sie der Reihe nach die oben aufgeführten Agenten aus und klicken Sie jedes Mal auf die Schaltfläche **Aktivieren**. Sie werden nach dem Server gefragt, auf dem der Agent ausgeführt werden soll. Wählen Sie den Server aus der Liste und klicken Sie auf OK:

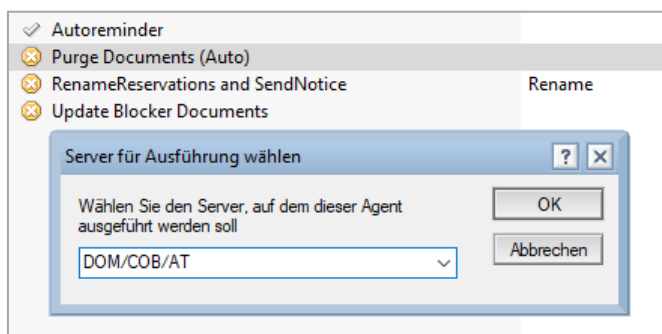


Abbildung 7.4: Server auswählen, auf dem der Agent laufen soll

7.3.6. Die Anwendung Ressourcenreservierung verschieben

Wenn Sie neue Server aufbauen oder auch alte Server auflassen, kann es passieren, dass Sie die Anwendung zur Ressourcenreservierung auf einen anderen Server verschieben müssen. Das klingt, als wäre das überhaupt kein Problem, aber jeder Raum, jede Ressource wurde nach dem Erstellen ins Domino-Verzeichnis kopiert und enthält dort in einem versteckten Feld den Namen des Herkunftsservers und der Herkunftsdatenbank. Diese Felder müssen beim Verschieben via Agenten aktualisiert werden. Am besten hat sich dafür die folgende Vorgangsweise erwiesen:

1. Erstellen Sie eine Replik der Ressourcenreservierung auf dem neuen Server.
2. Erstellen Sie eine Datenbankumleitung auf die neue Anwendung und löschen Sie dann das Original (oder verschieben Sie es auf Betriebssystemebene aus dem Domino-Datenverzeichnis).
3. Öffnen Sie die Zugriffskontrollliste der neuen Anwendung und setzen Sie den Administrationsserver auf den neuen Server. Ordnen Sie nötigenfalls neuen Administratoren Managerrechte zu.
4. Überprüfen Sie sicherheitshalber die Konsistenz der neuen Datenbank:

```
load fixup -j -f <Ressourcen.nsf>
```
5. Erstellen Sie im Domino-Verzeichnis einen einfachen Formelagenten zum Ändern der Raum-/Ressourcendokumente. Wenn die Anwendung am neuen Server gleich heißt, ist nur der Servername zu korrigieren, ansonsten Server- und Datenbankpfad.

```
FIELD MailServer := "CN=Server/OU=Unterorg/O=Org";
FIELD MailFile := <Pfad>;
```

Wenden Sie den Agenten auf alle Ressourcendokumente an, die geändert werden müssen. (Eine Anleitung zum Erstellen eines einfachen Formelagenten finden Sie in Kap. 11.3.3 Einen einfachen Formel-Agenten erstellen, ab Seite 315.)

6. Nach dem Aktualisieren der Felder sollten Sie vorsichtshalber die Ansichtsindizes neu erstellen. Geben Sie dazu auf dem neuen Server die folgenden Befehle ein:

```
load updall names.nsf -t "($rooms)" -r
load updall names.nsf -t "($resources)" -r
```
7. Öffnen Sie die neue Ressourcenreservierung im Domino Designer und wechseln Sie zu **Code > Agenten**. Überprüfen Sie der Reihe nach die in Abbildung 7.4 aufgeführten Agenten. Ist ein Agent deaktiviert, aktivieren Sie ihn und wählen Sie den neuen Server als Ausführungsort aus. Ist ein Agent bereits aktiviert, müssen Sie den Ausführungsserver händisch korrigieren. Öffnen Sie dazu den Agenten, klicken Sie in den **Eigenschaften > Allgemein** auf die Schaltfläche **Zeitplan...** und ändern Sie den Server im Feld **Ausführen auf**.

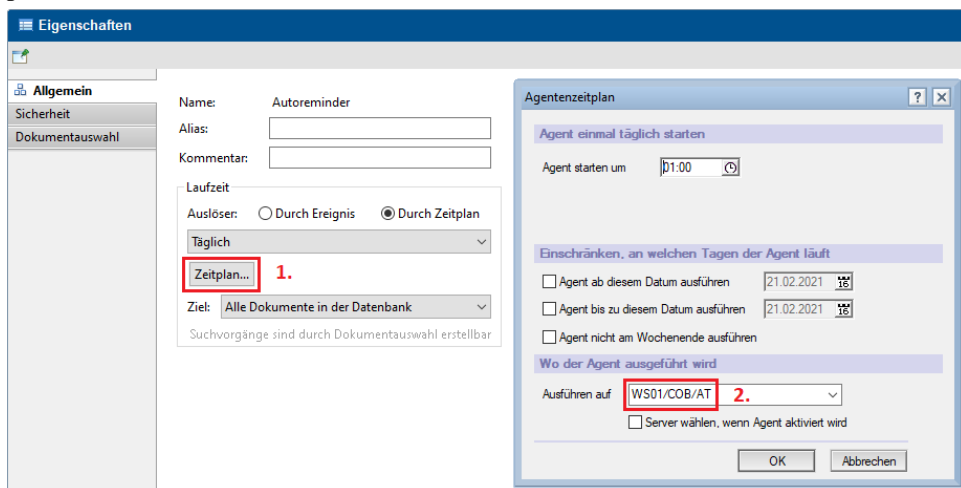


Abbildung 7.5: Server ändern, auf dem der Agent laufen soll

8. Beenden Sie die Servertasks Schedule Manager und Room & Resources Manager auf dem alten Server und löschen Sie die Planungsdatenbank busytime.nsf.
9. Starten Sie die beiden Tasks wieder. Die Planungsdatenbank wird neu erstellt.

7.3.7. Detaillierte Planungsinformationen extrahieren

Per Vorgabe werden nur Name und Uhrzeiten in die Planungsdatenbank busytime.nsf übertragen. Damit lässt sich aber eine Besprechung nur schwer planen, da nicht ersichtlich ist, wo sich die Kollegen befinden. Kann ich die Lücke von einer Stunde im Kalender meiner Chefin nutzen, um sie zur Abteilungsbesprechung einzuladen, oder ist sie gar nicht im Haus und benötigt eine unbestimmte Zeit für die Anreise? Glücklicherweise können Sie jedoch auch konfigurieren, dass mehr Kalenderdetails in die Planungsdatenbank eingetragen werden, darunter auch der Ort.

Das setzt allerdings voraus, dass auch der Benutzer sein Einverständnis zur Freigabe erweiterter Details gibt, was er im Posteingang über die Schaltfläche **Mehr > Vorgaben...** auf dem Register **Zugriff und Delegierung > Zugriff auf Ihren Zeitplan** tun kann. Sollten Sie den Auftrag dazu erhalten, können Sie dieses Einverständnis über die Mailrichtlinien auch erzwingen.

Um Kalendereinträge zu extrahieren, gehen Sie wie folgt vor:

1. Wählen Sie im Domino-Administrator das Register **Konfiguration** und dann **Server > Konfigurationen**.
2. Wenn es bereits ein Vorgabekonfigurationsdokument (mit dem Namen »* [Alle Server]«) gibt, bearbeiten Sie es, ansonsten erstellen Sie durch Klicken auf die Schaltfläche **Konfiguration hinzufügen** ein neues.
3. Aktivieren Sie auf dem Register **Allgemein** das Feld **Kalendereinträge extrahieren**. Damit wird die Liste der zu extrahierenden Kalendereinträge angezeigt.

Die Option **Kalendereinträge extrahieren** ist nur im Vorgabekonfigurationsdokument sichtbar.

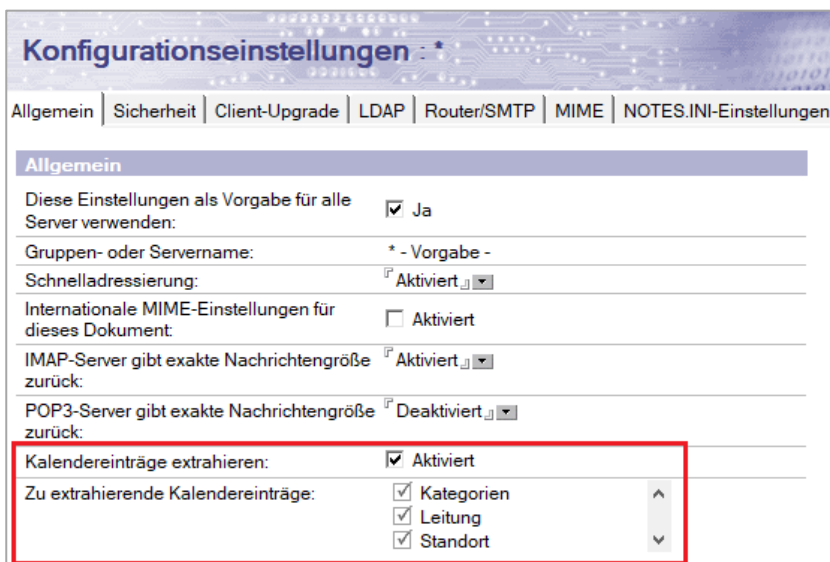


Abbildung 7.6: Die Option Kalendereinträge extrahieren im Vorgabekonfigurationsdokument

4. Wählen Sie die Felder, die extrahiert werden sollen:
 - Termtyp: Andere Benutzer können die Art des Eintrags sehen (Termin, Besprechung, ganztägige Veranstaltung).
 - Kategorien: Andere Benutzer können die vergebenen Kategorien sehen.
 - Leitung: Andere Benutzer sehen, wer die Leitung einer Besprechung innehat.

- Standort: Erlaubt es anderen Benutzern, den Standort einzusehen.
 Raum: Erlaubt es anderen Benutzern, den für eine Besprechung reservierten Raum einzusehen.

- Speichern und schließen Sie das Dokument.

7.4. Feiertage verwalten

Feiertagsdokumente erlauben es, Feiertage in Ihrem Unternehmen zentral zu verwalten. Im Domino-Verzeichnis sind bereits die Feiertage von 35 Ländern angelegt – die Bezeichnungen sind jedoch durchwegs auf Englisch.

Wählen Sie im Domino-Administrator das Register **Konfiguration** und dann **Verschiedenes > Feiertage**, um vorhandene Feiertage zu bearbeiten (z. B. auf Deutsch zu übersetzen), nicht benötigte Feiertage zu löschen sowie eigene, firmenspezifische Feiertage hinzufügen. Sie müssen neue Feiertage einer vorhandenen Gruppe zuordnen oder eine neue Gruppe erstellen. (Die Vorgabefeiertage sind nach Ländernamen gruppiert und entsprechen den Feiertagen in diesen Ländern.)

Benutzer können die Feiertage einer oder mehrerer Gruppen in Ihren persönlichen Kalender importieren und in weiterer Folge mit diesen abgleichen. Dies erfolgt im Kalender über die Aktionsschaltfläche **Mehr > Feiertage importieren...**

7.4.1. Die Feiertage aktualisieren

Wenn die Feiertage in Ihrem Domino-Verzeichnis abgelaufen sind, können Sie diese durch aktuellere Serien aus der Domino 11.0.1-Verzeichnisschablone (pubnames.ntf) ersetzen. (Dort sind die Feiertage bis zum Jahr 2027 angelegt.) Gehen Sie dazu wie folgt vor:

- Navigieren Sie im Domino-Administrator zum Register **Konfiguration** und dann zur Ansicht **Verschiedenes > Feiertage**.
- Wählen Sie im Menü **Aktionen** den Befehl **Feiertage aus Schablone importieren**. Beachten Sie, dass dazu die Schablone pubnames.ntf auf Ihrem Mailserver verwendet wird.

Achtung: Haben Sie die Feiertage auf Deutsch übersetzt, werden sie durch die Aktualisierung mit englischen Namen überschrieben!

8. Mail-Routing

- > 8.1 Die Mailkomponenten, Seite 201
- > 8.2 Notes-Mail, Seite 203
- > 8.3 Internet-Mail, Seite 208
- > 8.4 Weitere Maileinstellungen, Seite 219
- > 8.5 Mail-In-Datenbanken, Seite 222
- > 8.6 Sinnvolle Mailvorgaben setzen, Seite 223
- > 8.7 Beschränkungen beim Senden von Mails setzen, Seite 225
- > 8.8 Geplante Nachrichten versenden, Seite 227
- > 8.9 Auf Zustellungsfehler reagieren, Seite 230
- > 8.10 Auf unzustellbare Nachrichten reagieren, Seite 231
- > 8.11 Die Größen von Maildatenbanken beschränken, Seite 233
- > 8.12 Abwesenheitsnachrichten einrichten, Seite 236
- > 8.13 Einen Verzeichniskatalog erstellen, Seite 238

8.1. Die Mailkomponenten

HCL Domino bietet ein integriertes, serverbasiertes Mailsystem, über das Mails an andere Notes-Benutzer oder ins Internet geschickt werden können. Notes-Mails werden im Format Notes-Richtext (oder Compound Document, CD) über das NRPC-Protokoll weitergeleitet, Internet-Mails im Format MIME (Multipurpose Internet Mail Extensions) über das Protokoll SMTP. Welches Format bzw. welches Protokoll verwendet wird, entscheidet die Adressierung, Mailadressen nach dem Muster *.* (wobei der Punkt in der Domäne gemeint ist) werden als Internet-Mails weitergeleitet. Das Mailsystem besteht aus den folgenden Komponenten:

8.1.1. Mailer

Der Mailer läuft auf dem Notes-Client und sorgt für Adressauflösung, Namenserkennung (Type-Ahead) und Gruppenerweiterung. Er überprüft die eingegebene Mail-Adresse und schlägt bei Zweideutigkeit ähnliche Adressen vor. Der Mailer formatiert die Nachrichten entsprechend ihren Empfängern als CD oder MIME und sorgt – falls angefordert – für Verschlüsselung und Signierung. Der Mailer speichert ausgehende Nachrichten in der Mailbox (entweder lokal oder am Server).

8.1.2. Mailbox

Eine spezielle Notes-Datenbank mit dem Namen mail.box, die auf jedem Server, der Mails weiterleitet, vorhanden ist. In dieser Datenbank werden übertragungsbereite Mails so lange aufbewahrt, bis sie an ihre Empfänger weitergeleitet werden können.

Je nach Konfiguration können auf einem Domino-Server auch mehrere Mailboxen vorhanden sein, in diesem Fall heißen sie: mail1.box, mail2.box etc.

8.1.3. Router

Der Mail-Router (Router) läuft auf einem Mailserver. Er holt übertragungsbereite Mails aus der Mailbox und leitet sie entsprechend der angegebenen Mailadressen als Notes- oder Internet-Mails weiter.

8.1.3.1. Weiterleitung von Notes-Mail

Befindet sich die Maildatenbank des Empfängers auf demselben Domino-Server, steckt der Mail-Router die Mail direkt in die Maildatenbank und man spricht von **Zustellung** (Delivery). Befindet sich die Maildatenbank des Mailempfängers auf einem anderen Domino-Server, steckt der Mail-Router die Mail in die Mailbox des anderen Servers und man spricht von **Übertragung** (Transfer).

8.1.3.2. Weiterleitung von Internet-Mail

Handelt es sich um eine Internet-Mail, sendet sie der Router je nach Konfiguration entweder direkt an den Mailserver der Internet-Domäne oder an einen Relayhost im eigenen Unternehmen oder beim Provider. Eine direkte Verbindung zu anderen Internet-Domänen ist nur möglich, wenn der Domino-Server die IP-Adressen der SMTP-Server über die entsprechenden MX- (Mail Exchanger-) Einträge im DNS (Domain Name Service) auflösen kann.

8.1.4. SMTP-Server

Der SMTP-Server (auch als SMTP-Listener bezeichnet, weil er auf Port 25 auf Anfragen »horcht«) ist ein separater Task, der hereinkommende Mails überprüft und in die Mailbox steckt, wenn sie keiner Policy widersprechen.

8.1.5. Wo Mailadressen hinterlegt sind

Per Mail erreichbar sind Personen und **Mail-In-Datenbanken**. Bei Mail-In-Datenbanken handelt es sich in der Regel um Anwendungen, die Daten über das Mailsystem erhalten und diese via Programmcode weiterverarbeiten. Viele Administratoren verstehen darunter aber auch Gruppenpostfächer. (Zum Einrichten von Mail-In-Datenbanken lesen Sie Kap. 8.5 Mail-In-Datenbanken, ab Seite 222.)

Ebenfalls per Mail erreichbar sind Verteilergruppen (Gruppen vom Typ »Mehrere Zwecke« und »Nur Mail«), hinter denen jedoch keine eigenen Maildatenbanken stecken, sondern die, wie der Name bereits andeutet, Mails an die Gruppenmitglieder (Personen, Mail-In-Datenbanken oder weitere Gruppen) verteilen.

8.2. Notes-Mail

Um Notes-Mails zu versenden, bedarf es keinerlei Konfiguration – es muss nur der Mail-Router laufen, was per Vorgabe der Fall ist. (Natürlich ist immer ein gewisses Feintuning möglich – davon später mehr.) Sehen wir uns nun die Weiterleitung einer Mailnachricht genauer an.

8.2.1. Der Mailer

Der **Mailer** überprüft bei Notes-Mails innerhalb derselben Domäne, ob die eingegebene Mail-Adresse im Domino-Verzeichnis existiert und schlägt bei Zweideutigkeit ähnliche Adressen vor. Mails an nicht existente Adressen innerhalb derselben Domäne werden nicht versendet, Mailadressen aus anderen Notes-Domänen und Internet-Mails werden hingegen nicht geprüft und immer verschickt. Der Mailer löst abhängig vom Inhalt des (ausgeblendeten) Feldes \$ExpandGroups Gruppen auf (0 = keine Gruppen, 1 = nur lokale Gruppen, 2 = nur öffentliche Gruppen, 3 = alle Gruppen). Weiters trennt der Mailer die Nachrichten für Notes- und Internet-Empfänger und formatiert sie entsprechend als CD oder MIME. Der Mailer sorgt für Verschlüsselung und Signierung basierend auf den Nachrichteneinstellungen und Empfängerinformationen. (Er unterstützt Notes-Verschlüsselung via Public Key und S/MIME via X.509 Public Cert im Personendokument.) Letztendlich setzt der Mailer das Versanddatum (PostedDate) und legt die Mail je nach Art der Verbindung lokal oder am zuständigen Mailserver (= Homeserver) in der Mailbox ab.

8.2.2. Der Router

Der **Mail-Router** schlägt Mailadressen (egal ob Notes- oder SMTP-Adressen) in der versteckten Ansicht (\$Users) im Domino-Verzeichnis nach. Diese Ansicht enthält alle Namensfelder aus Personendokumenten (Vorname, Nachname, Kurzname und alle Zeilen aus dem Feld Benutzername) plus das Feld Internetadresse sowie alle Namensfelder plus das Feld Internetadresse aus Mail-In-Datenbanken und Gruppen. Ist die Zuordnung eindeutig (die nachgeschlagene Adresse kommt in der Ansicht nur einmal vor), schlägt er im aufgefundenen Dokument die Zustelladresse nach. Hier ein Beispiel für Mailserver und Maildatenbank eines Benutzers:

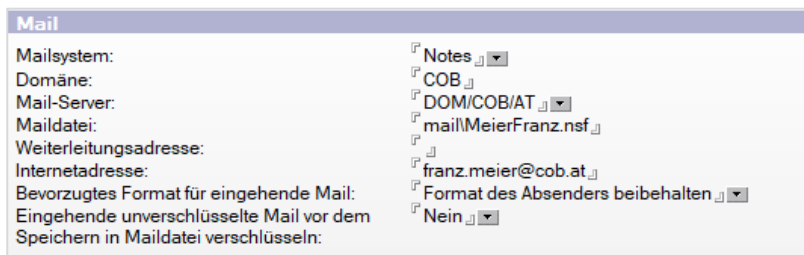


Abbildung 8.1: Die Mailfelder im Personendokument

Wie es weitergeht, hängt davon ab, auf welchem Server die Maildatenbank des Empfängers liegt. Liegt sie auf demselben Server wie die Datenbank des Absenders, kopiert der Mail-Router die Mail in die Datenbank und man spricht von **Zustellung** (Delivery). Handelt es sich um einen anderen Server, steckt der Mail-Router die Mail in die Mailbox des anderen Servers und man spricht von **Übertragung** (Transfer).

Notes Mail-Routing funktioniert also via Speichern und Weiterleiten von Server zu Server. Jeder Mail-Router berechnet den Routingpfad komplett neu, kooperiert also weder mit seinem Vorgänger noch mit seinem Nachfolger, da er aber auf denselben Informationen aufbaut, kommt er schluss-

endlich zu denselben Ergebnissen. Grundvoraussetzung für ein funktionierendes Notes-Mail-Routing ist also ein regelmäßiger Abgleich (Replizierung) aller Adressbücher.

Standardmäßig kontaktiert jeder Server direkt den Zielsever, egal wo er sich befindet und ob die Verbindung schnell oder langsam ist. Wollen Sie einen bestimmten Routingpfad vorgeben, müssen Sie zwei oder mehrere **Benannte Notes-Netzwerke** einrichten.

8.2.3. Benannte Notes-Netzwerke

Benannte Notes-Netzwerke (Notes Named Networks, NNN), manchmal auch als Benannte Domino Netzwerke (Domino Named Networks, DNN) benannt, sind Gruppen von Servern, die durch ein gemeinsames Netzwerk definiert sind. Bei diesem Netzwerkbegriff kann es sich um einen physischen Standort, ein gemeinsames Netzwerkprotokoll oder auch nur um einen Namen handeln.

Server und Clients *können* zum selben Notes-Netzwerk gehören, wenn sie:

- > dasselbe LAN-Protokoll benutzen
- > ständig miteinander verbunden sind

Server und Clients **müssen** unterschiedlichen Notes-Netzwerken angehören, wenn sie:

- > unterschiedliche LAN-Protokolle verwenden
- > an unterschiedliche physische LANs angeschlossen sind

Domino-Server können mehreren Notes-Netzwerken angehören. Wenn damit auch die Verwendung verschiedener Netzwerkprotokolle verbunden ist, nennt man sie **Multiprotokollserver**. Multiprotokollserver werden herangezogen, um die Mailweiterleitung oder Replikation über verschiedene Protokolle hinweg zu ermöglichen.

Ein Netzwerkname:

- > Alle Server »sehen« einander.
- > Die Mailweiterleitung funktioniert automatisch.

Mehrere Netzwerknamen:

- > Server unterschiedlicher Notes-Netzwerke »sehen« einander nicht.
- > Server können Mails an Server in einem anderen Domino-Netzwerk nicht direkt versenden.

Sehen wir uns nun die Notes-Mailweiterleitung im Detail an.

8.2.3.1. Mailweiterleitung innerhalb eines Notes-Netzwerks

1. Die Mailer-Software auf dem Client überprüft, ob es einen Empfänger namens Susanne Schmied im Domino-Verzeichnis überhaupt gibt. Wird der Empfänger gefunden, wird der eingegebene Name durch den Langnamen ersetzt, z. B.: Susanne Schmied/COB/AT.
2. Der Mailer legt die Mail in der Mailbox des zuständigen Mailservers ab.
3. Der Mail-Router konsultiert das Personendokument im Domino-Verzeichnis und sieht nach, auf welchem Mailserver sich Susanne Schmieds Maildatenbank befindet.
4. Liegt die Maildatenbank auf demselben Mailserver (man bezeichnet diesen Server dann als den **Homeserver** von Susanne Schmied) legt der Mail-Router die Mail dort ab (Zustellung –

Delivery). Dabei setzt er das Zustellungsdatum (DeliveredDate), arbeitet die Mailregeln ab und fügt die Mail (wenn sie keiner Mailregel widerspricht) zum Ordner Posteingang hinzu. Außerdem prüft er, ob eine Abwesenheitsnachricht an den Absender zu versenden ist.

5. Befindet sich die Maildatei auf einem anderen Server, legt der Mail-Router die Mail in der Mailbox des anderen Servers ab (Weiterleitung – Transfer), wo sich wiederum der lokale Mail-Router darum kümmert.

8.2.3.2. Mailweiterleitung zwischen Domino-Netzwerken

1. Der Mailer überprüft die Identität von Franz Meier.
2. Der Mailer legt die Mail in der Mailbox des Homeservers des Absenders ab.
3. Der Mail-Router konsultiert das Personendokument von Franz Meier im Domino-Verzeichnis und stellt den Namen des Mailservers fest. Aus dem Serverdokument erfährt der Mail-Router, dass der Mailserver von Franz Meier nicht zum selben Domino-Netzwerk gehört. Deshalb durchsucht er das Domino-Verzeichnis nach einem Verbindungsdokument, aus dem hervorgeht, welcher Server im selben Domino-Netzwerk eine Verbindung zum Netzwerk von Franz Meiers Homeserver aufbauen kann. Findet der Mail-Router einen solchen Server, legt er die Mail in der dortigen Mailbox ab.
4. Der Mail-Router des Verbindungsservers beratschlagt wiederum das Domino-Verzeichnis und baut je nach Vorgaben im Verbindungsdokument eine Verbindung zum Mailserver von Franz Meier auf. Nach geglückter Verbindung legt der Mail-Router die Mail in die Mailbox von Franz Meiers Mailserver ab.
5. Der Mail-Router auf Franz Meiers Mailserver stellt die Mail in die Maildatei zu.

8.2.3.3. Mailweiterleitung zwischen Domino-Netzwerken ermöglichen

Damit Ihr Domino-Server Mails an ein fremdes Domino-Netzwerk weiterleiten kann, muss er zuerst für beide Netzwerke konfiguriert werden. Anschließend müssen Sie Verbindungsdokumente zur Steuerung der Mailweiterleitung in beide Richtungen erstellen.

Als Beispiel sollen die beiden Domino-Netzwerke **TCPIP Network intern** und **TCPIP Network extern** (beide TCP/IP-Protokoll) herangezogen werden.

1. Bearbeiten Sie im Domino-Verzeichnis das gewünschte Serverdokument und wechseln Sie zum Register **Ports...** > **Notes Netzwerk-Ports**.

Port	Protokoll	Notes-Netzwerk	Netzadresse	Aktiviert
TCPIP	TCP	TCPIP Network intern	DOM	Aktiviert
TCPIPExt	TCP	TCPIP Network extern	www.cob.at	Aktiviert
			DOM	Deaktiviert
			DOM	Deaktiviert
			DOM	Deaktiviert
			DOM	Deaktiviert
			DOM	Deaktiviert
			DOM	Deaktiviert

Abbildung 8.2: Ein Serverdokument mit zwei aktivierten Anschlüssen

2. Fügen Sie den Anschlussnamen »TCPIPExt« sowie die Bezeichnung »TCPIP Network extern« für das neue Notes-Netzwerk hinzu.
3. Speichern Sie das Serverdokument.

Soll der Wechsel von einem Netzwerk zum anderen auch einen Protokollwechsel beinhalten, wählen Sie den gewünschten Server aus und dann **Werkzeuge > Server > Ports einrichten**:

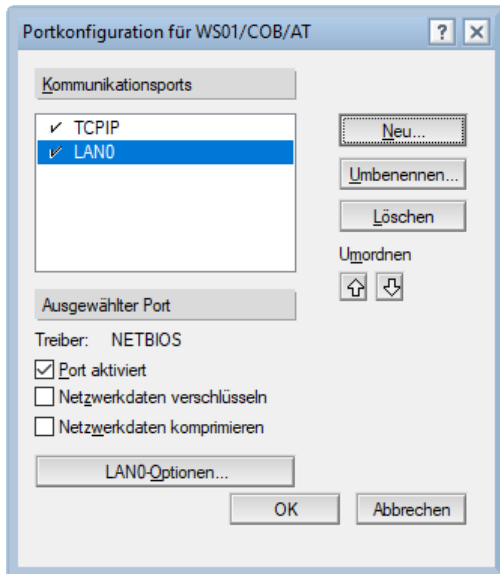


Abbildung 8.3: Ports (Anschlüsse) einrichten

8.2.3.4. Ein Verbindungsdokument erstellen

1. Öffnen Sie das Domino-Verzeichnis und wählen Sie die Ansicht **Konfiguration > Server > Verbindungen**.
2. Klicken Sie auf **Verbindung hinzufügen**.
3. Tragen Sie im Register **Allgemein** im Feld **Quellserver** den Namen des Servers ein, der die Verbindung zum anderen Netzwerk aufbaut, im Feld **Zielserver** den Namen des Servers im anderen Netzwerk. Sollte der Domino-Name des Zielservers nicht auflösbar sein, geben Sie im Feld **Optionale Netzwerkadresse** noch zusätzlich seinen Hostnamen oder seine IP-Adresse ein.
4. Wählen Sie den Namen des benutzten Anschlusses/Ports aus (in der Regel TCPIP).
5. Geben Sie die Domäne für den Quell- und Zielserver ein.



Abbildung 8.4: Verbindungsdokument, Register Allgemein

6. Wechseln Sie zum Register **Replizierung/Routing**.
7. Wenn Sie das Verbindungsdokument nur zum Zweck der Mailweiterleitung erstellen, deaktivieren Sie die Replizierungsfunktion.

Serververbindung: WS01/COB/AT zu DOM/COB/AT	
Allgemein Replizierung/Routing Zeitplan Kommentare Administration	
Replizierung	Routing
Replizierungsfunktion: <input type="checkbox"/> Deaktiviert <input type="checkbox"/>	Routing-Funktion: <input type="checkbox"/> Mail-Routing <input type="checkbox"/>
Zu replizierende Datenbanken: <input type="checkbox"/> Niedrig & Mittel & Hoch <input type="checkbox"/> Priorität	Sofortiges Routing, wenn: <input type="checkbox"/> 1 <input type="checkbox"/> Nachrichten warten
Replizierungstyp: <input type="checkbox"/> Pull Push <input type="checkbox"/>	Routing-Kosten: <input type="checkbox"/> 1 <input type="checkbox"/>
Pfade der zu replizierenden Dateien/Verzeichnisse: <input type="checkbox"/> (alle, falls nichts anderes angegeben)	Router-Typ: <input type="checkbox"/> Nur Push <input type="checkbox"/>
Pfade der NICHT zu replizierenden Dateien/Verzeichnisse: <input type="checkbox"/>	
Zeitlimit für Replizierung: <input type="checkbox"/> <input type="checkbox"/> Minuten	

Abbildung 8.5: Verbindungsdokument, Register Replizierung/Routing

Intern verwendet der Mail-Router sogenannte Routing Tables, die nicht nur Informationen zu Verbindungen, NNNs und Domänen aus dem Domino-Verzeichnis berücksichtigen, sondern auch Routing-Kosten; so wird bei zwei gleichen Verbindungen diejenige mit den geringeren Kosten gewählt.

Damit ist es möglich, alternative Verbindungen zu ein und demselben Ziel anzubieten, etwa eine schnellere Verbindung über eine Standleitung (Kosten: 2) und eine langsamere Wählverbindung (Kosten: 4). Fällt die Standleitung aus, wird nach zwei missglückten Verbindungsversuchen die Wählverbindung aktiviert.

Der Router setzt die Kosten einmal stündlich zurück; funktioniert die Standleitung wieder, kehrt er von selbst zur schnelleren Route zurück.

8. Wechseln Sie zum Register **Zeitplan** und legen Sie die Verbindungszeiten fest. Die Mailweiterleitung erfolgt sofort, wenn eine Nachricht wartet, aber nur innerhalb des angegebenen Zeitplans; wollen Sie, dass Mails den ganzen Tag sofort weitergeleitet werden, geben Sie »00:00 - 23:59« an (die Angabe »24:00« kann intern nicht in die 12-Stunden-Anzeige mit AM/PM umgewandelt werden). Das Intervall wird ignoriert, da jede wartende Nachricht ja sofort weitergeleitet wird. Vergessen Sie nicht, den Zeitplan zu aktivieren!

Serververbindung: WS01/COB/AT zu DOM/COB/AT	
Allgemein Replizierung/Routing Zeitplan Kommentare Administration	
Geplante Verbindung	
Zeitplan: <input type="checkbox"/> Aktiviert <input type="checkbox"/>	
Zu bestimmten Zeiten verbinden: <input type="checkbox"/> 00:00 - 23:59 <input type="checkbox"/> jeden Tag	
Wiederholungsintervall: <input type="checkbox"/> 30 <input type="checkbox"/> Minuten	
Wochentage: <input type="checkbox"/> So, Mo, Di, Mi, Do, Fr, Sa <input type="checkbox"/>	

Abbildung 8.6: Verbindungsdokument, Register Zeitplan

8.3. Internet-Mail

8.3.1. Das SMTP-Protokoll

SMTP steht für SIMPLE MAIL TRANSFER PROTOCOL und ist ein heillos veralteter Standard aus dem Jahr 1982. SMTP-Mail ist hauptsächlich ASCII-Text und besteht aus den folgenden Komponenten:

- > Envelope (RFC 821)
- > Header (RFC 822)
- > Body (Text oder MIME-Text)

8.3.1.1. SMTP Message-Envelope

Der sogenannte Envelope (wörtlich übersetzt: »Umschlag«) enthält praktisch nur Informationen, die zur Mailzustellung gebraucht werden, wie Absender und Empfänger.

Mail from: <user@domain.com> definiert den Absender.

Rcpt to: <user@domain.com> definiert den Empfänger.

8.3.1.2. SMTP Mail Header

Der Header enthält Information, die nicht zur Zustellung verwendet werden. Dabei handelt es sich um Felder wie Absender, SendTo, CopyTo, BlindCopyTo, Betreff (Subject) u. a. Es gibt Pflichtfelder, optionale Felder und spezifische Erweiterungen (sogenannte X-Felder). Dieser Teil der Nachricht wird in Notes-Felder (eigentlich: Notes-Items, also Felder, die nur im Dokument existieren, nicht aber in der Maske) übersetzt.

8.3.1.3. SMTP Mailtext (Body)

Der Body enthält den eigentlichen Mailtext, vergleichbar dem Body-Feld in Notes, jedoch als unformatierten Text, welcher meist MIME-codiert ist (MIME = Multipurpose Internet Mail Extensions).

MIME kann verschiedene Formate mit verschiedenen Codierungen enthalten, z. B. text/plain, text/html, text/calendar ... Es sind auch Anhänge möglich, die entweder »inline« (MIME-codiert als Text) oder referenziert (als getrennte Anhänge) mitgeschickt werden.

MIME unterstützt verschiedene Zeichensätze inclusive Unicode (UTF-8).

8.3.1.4. Domino Itemizer

MIME-Mails werden in Notes in sogenannten Items (das sind Felder, die es im Dokument gibt, aber nicht in der zugrunde liegenden Maske) gespeichert – ähnlich wie Notes-Mails.

Wenn die Mail von einem SMTP-Server versendet oder empfangen wird, wird sie entsprechend von einer Item-basierenden in eine textbasierende Form konvertiert und wieder zurück. Die Konvertierung hereinkommender Nachrichten wird dabei von einem sogenannten »Itemizer« erledigt, welcher genau weiß, welches Item er wie behandeln muss. Es gibt Standardfelder wie From, SendTo, Posted-Date und andere.

Diese Konvertierung kann vom Administrator in einem gewissen Ausmaß beeinflusst werden, so können Sie etwa Felder ausnehmen oder hinzufügen (siehe dazu auch Kap. Auf Spurensuche im MIME-Header, ab Seite 216).

Wollen Sie in ausgehenden MIME-Nachrichten immer alle Felder haben, können Sie in die Mailmaske (Memo) das Feld \$SMTPKeepNotesItems mit dem Wert »1« aufnehmen. Dadurch werden alle individuellen Felder in MIME in X-Tags übersetzt und zurück. (Dieses System wird z. B. bei Kalendereinladungen verwendet.)

8.3.1.5. TNEF und Winmail.dat

Erhalten Sie in E-Mails hin und wieder Dateien mit der Endung *.dat? (Meist heißen sie »winmail.dat«, aber auch andere Dateinamen wie »att00001.dat« sind möglich.) Dabei handelt es sich um TNEF-codierte Anhänge, die von Outlook verschickt wurden. Das Microsoft TNEF-Format entspricht keinem öffentlichen Standard und ist nicht RFC-konform – worauf sogar Microsoft hinweist. Siehe: <http://support.microsoft.com/kb/323483>

TNEF wurde schon vor langer Zeit offengelegt und ist seit Version 7.0.2 in Domino implementiert, standardmäßig aber deaktiviert. Um die TNEF-Konvertierung auf dem Domino-Server zu aktivieren, setzen Sie in der Datei notes.ini folgende Variable:

```
TNEFEnableConversion=1
```

Leider ändert Microsoft das TNEF-Format mit neueren Exchange-Versionen immer wieder, was dazu geführt hat, dass die .dat-Dateien nach Jahren plötzlich erneut auftauchen, weil Domino sie nicht mehr konvertieren kann.

8.3.2. Internet-Mailrouting aktivieren

Internet-Mailrouting ist per Vorgabe deaktiviert und muss erst aktiviert werden. Haben Sie beim Einrichten des Servers (siehe Seite 52) ein Häkchen im Feld **Internet Mail Clients** gesetzt, ist die Aktivierung bereits vom Setup-Assistenten vorgenommen worden.



Abbildung 8.7: Setup Internet Services – Internet Mail Clients

Haben Sie das Häkchen nicht gesetzt, müssen Sie die Aktivierung jetzt nachholen. Sie erfolgt im Konfigurationsdokument Ihres Mailservers, in dem Sie auch die weitere Mailkonfiguration vorfinden.

Gehen Sie zum Aktivieren von Internet-Mail wie folgt vor:

1. Öffnen Sie das Konfigurationsdokument Ihres Mailservers im Bearbeitungsmodus und navigieren Sie zum Register **Router/SMTP > Allgemein**.

- Wählen Sie im Feld **SMTP wird zum Senden von Nachrichten an Empfänger außerhalb der lokalen Internetdomäne verwendet** den Wert »Aktiviert«. Damit erlauben Sie das Senden von SMTP-Mails ins Internet.

Die lokale Internet-Domäne ist identisch mit der Notes-Domäne.

- Wählen Sie im Feld **SMTP innerhalb der lokalen Internetdomäne zulässig** den Eintrag »Nur MIME-Nachrichten«. Wählen Sie »Deaktiviert«, müssen Domino-Server, um Internet-Mails innerhalb der Notes-Umgebung weiterzuleiten, diese zuvor in Notes-Mails konvertieren, wodurch eventuell die Formatierung verloren geht (Newsletter!), was bei Anwendern nicht so gut ankommt. Wählen Sie »Alle Nachrichten«, wird jede interne Mail als Internet-Mail im MIME-Format verschickt, das heißt, Sie haben das Notes-Mailrouting deaktiviert.
- Wählen Sie im Feld **Server innerhalb der lokalen Notes-Domäne sind via SMTP über TCP/IP erreichbar** den Wert »Immer«.

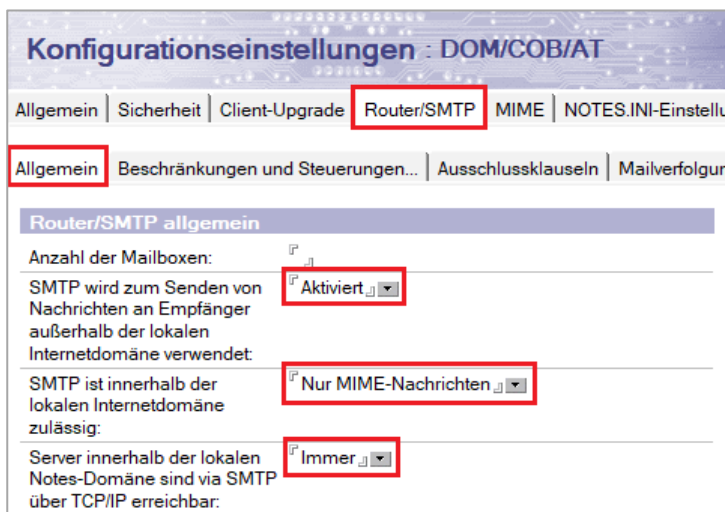


Abbildung 8.8: Konfigurationsdokument, SMTP-Mails aktivieren

- Speichern und schließen Sie das Konfigurationsdokument.

8.3.3. Den SMTP-Server starten

Überprüfen Sie als Nächstes, ob der SMTP-Server läuft. Ohne SMTP-Server können zwar Mails ins Internet geschickt, aber keine empfangen werden! Gehen Sie dabei wie folgt vor:

- Öffnen Sie das Domino-Verzeichnis und navigieren Sie zu **Konfigurationen > Server > Alle Serverdokumente**.
- Wählen Sie das Serverdokument Ihres Mailservers und öffnen Sie es im Bearbeitungsmodus.
- Wählen Sie im Register **Allgemein** im Feld **SMTP-Listener-Task** die Option »Aktiviert«:

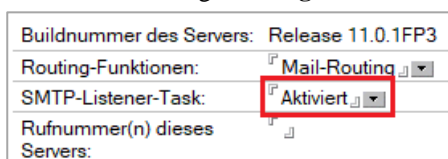


Abbildung 8.9: Serverdokument, SMTP-Listener-Task aktivieren

4. Speichern und schließen Sie das Serverdokument.
5. Wenn Sie den SMTP-Listener-Task zum ersten Mal aktiviert haben, müssen Sie ihn starten. Das geschieht, indem Sie auf der Serverkonsole einen der folgenden Befehle eingeben:
 - > `restart server` (startet den ganzen Server neu)
 - > `restart task router` (startet den Mail-Router neu)
 - > `load smtp` (startet nur den SMTP-Server)

Wenn der SMTP-Listener-Task im Serverdokument nicht aktiviert ist, können Sie ihn über den Befehl `load smtp` nicht starten.

Der Servertask SMTP kann nicht über ein Programmdokument oder über die `notes.ini`-Variable `ServerTasks` gestartet werden, sondern wird, wenn im Serverdokument konfiguriert, mit dem Mail-Router mitgestartet.

8.3.4. Internetdomänen zulassen

Wir haben soeben Internet-Mailrouting in beide Richtungen aufgesetzt, Anwender können nun Mails ins Internet schicken und aus dem Internet empfangen. Aber für welche Domänen soll der Domino-Server Mails entgegennehmen? Das dürfen natürlich nur die eigenen Domänen sein, denn würde der Server auch Mails an andere Domänen weiterleiten, wäre er ein offenes Relay, also ein Spammer!

Ich kann Sie jedoch beruhigen, der Server akzeptiert per Vorgabe nur Mails an eine Domäne, und zwar an jene, die Sie bei der Konfiguration im Feld **Vollständig qualifizierter Internet-Hostname** eingegeben haben. Steht dort etwa www.cob.at, dann lautet die einzige Domäne, für die der SMTP-Server Mails entgegennimmt `@cob.at`:

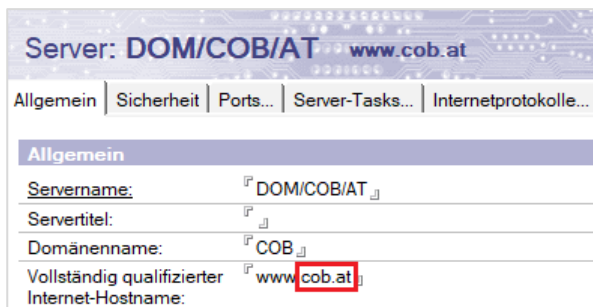


Abbildung 8.10: Serverdokument, Vollständig qualifizierter Internet-Hostname

Aber was tun Sie, wenn Sie eine andere oder gar mehrere Internet-Domänen haben wollen? – Sie erstellen ein Globales Domänenendokument!

8.3.4.1. Das Globale Domänenendokument

Im Globalen Domänenendokument definieren Sie:

1. Für welche Internet-Domänen der SMTP-Server Mails entgegennimmt (Mails an andere Domänen werden als Relay-Versuch gewertet)
2. Wie Internet-Mailadressen in Benutzernamen übersetzt werden

Um ein globales Domänenendokument zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Domino-Administrator die Ansicht **Konfiguration > Nachrichten > Domänen**.
2. Klicken Sie auf die Schaltfläche **Domäne hinzufügen**.
3. Wählen Sie als Typ »Globale Domäne« und vergeben Sie einen beliebigen Namen, z. B. »Internet«:

The screenshot shows the 'Domäne Internet' configuration window in the Domino Administrator. The 'Allgemein' tab is selected. The configuration includes:

- Domärentyp:** Globale Domäne (dropdown menu)
- Name der globalen Domäne:** Internet (text field)
- Funktion der globalen Domäne:** R5/R6/R7/R8-Internet-Domäne oder R4.x SMTP MTA (dropdown menu)
- Als Vorgabe für die globale Domäne verwenden (für alle Internetprotokolle außer HTTP):** Ja

Abbildung 8.11: Globales Domänenendokument, Register Allgemein

4. Klicken Sie im Feld **Als Vorgabe für die globale Domäne verwenden** auf »Ja«.
5. Wechseln Sie zum Register **Beschränkungen** und tragen Sie den Namen Ihrer Notes-Domäne ein:

The screenshot shows the 'Domäne Internet' configuration window in the Domino Administrator, with the 'Beschränkungen' tab selected. The configuration includes:

- R5/R6/R7 Domino-Domänen-Aliasnamen/R4.x SMTP MTA-Mitglieder:**
- Domino-Domänen und Aliasnamen:** COB (text field)
- Aliastrennzeichen:** = (text field)

Abbildung 8.12: Globales Domänenendokument, Register Beschränkungen

6. Wechseln Sie zum Register **Konvertierungen**. Geben Sie im Feld **Lokale primäre Internet-Domäne** den Namen der primären Internet-Domäne ein.

Die primäre Internet-Domäne wird verwendet, wenn im Personendokument keine Mailadresse eingetragen ist.

7. Geben Sie bei Bedarf im Feld **Alternative Aliasnamen für Internet-Domänen** alle weiteren Domänen ein, für die Ihr SMTP-Server Mails entgegennehmen soll.
8. Stellen Sie das Feld **Internetadresssuche** auf »Aktiviert«. Der SMTP-Server schlägt dann die Mailadresse im Personendokument, Feld **Internetadresse** nach.

Die Einstellungen zur Konvertierung der Internet-Mailadresse in den Namen werden jetzt nur noch verwendet, wenn das Feld **Internetadresse** im Personendokument leer ist.

9. Wählen Sie im Feld **Lokaler Anteil aufgebaut aus** »Allgemeiner Name«. Die Mailadresse wird dann aus dem Vor- und Nachnamen zusammengesetzt.

Wenn zwei Benutzer denselben Vor- und Nachnamen besitzen, kann diese Auswahl dazu führen, dass Mailadressen nicht eindeutig sind. Allerdings ist das zu ignorieren, da wir ja die

Internetadresssuche aktiviert haben und die Mailadressen aus den Personendokumenten verwendet werden.

10. Wählen Sie im Feld **Domino-Domäne(n) aufnehmen** den Eintrag »Keine«:

The screenshot shows the 'Domäne Internet' configuration window with the following settings:

- SMTP-Adresskonvertierung
- Lokale primäre Internetdomäne:
- Alternative Aliasnamen für Internetdomänen:
- Internetadresssuche:
- Falls deaktiviert oder wie folgt konvertieren: ohne Übereinstimmung
- Lokaler Anteil aufgebaut aus:
- Domino-Domäne(n) aufnehmen:
- Position der Domino-Domäne:
- Trennzeichen für Domino-Domänennamen:
- Adressbeispiel: JMD@acme.com

Abbildung 8.13: Globales Domänenendokument, Register Konvertierungen

8.3.5. Die Absenderadresse konfigurieren

Standardmäßig wird als Absenderadresse nur die Mailadresse angegeben, etwa:

franz.meier@cob.at

Es ist heute jedoch üblich, zusätzlich eine sogenannte Phrase, meist den vollständigen Namen, zur Anzeige mitzuschicken, und zwar nach dem Standard RFC822 (RFC821 inkludiert nur die E-Mailadresse):

"Franz Meier" <franz.meier@cob.at>

Die mitgesendete Phrase kann in Anführungszeichen gesetzt werden oder auch nicht, wichtig ist, dass die eigentliche E-Mail-Adresse in spitzen Klammern steht.

Ob Domino RFC821 oder RFC822 verwendet, konfigurieren Sie im Konfigurationsdokument, Register **MIME > Erweitert > Erweiterte Optionen für ausgehende Nachrichten**, im Feld **Behandlung von RFC822-Phrasen**. Vorgabe ist »Keine Phrase hinzufügen«.

Ich empfehle Ihnen unbedingt auf »Allgemeinen Namen als Phrase verwenden« umzustellen:

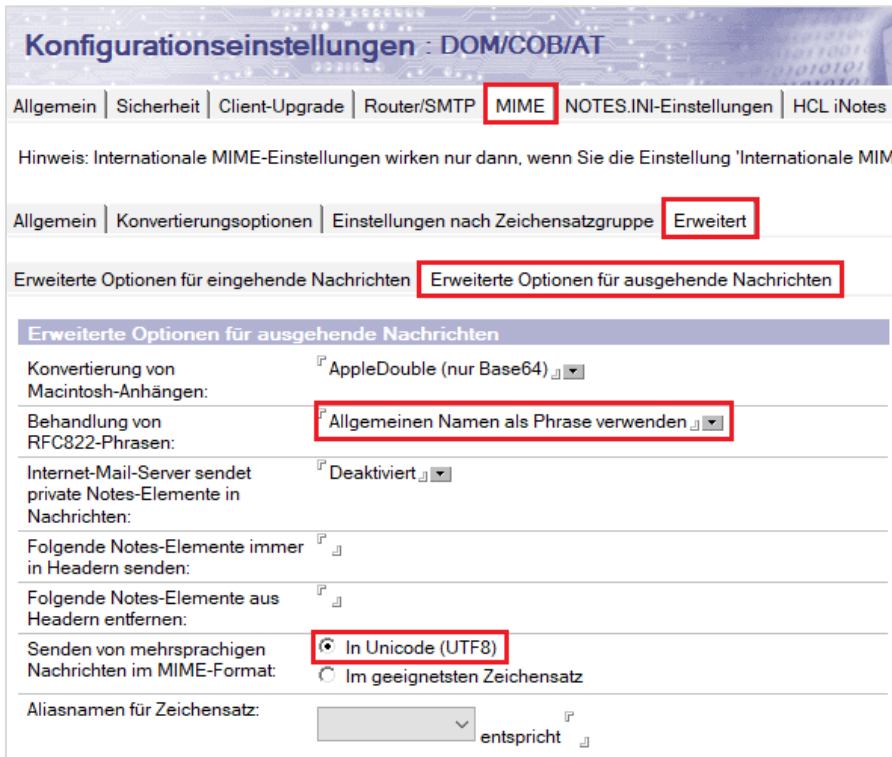


Abbildung 8.14: MIME-Konfiguration – Erweiterte Optionen für ausgehende Nachrichten

Im Posteingang der meisten Mail-Clients (auch in Notes) wird dann nur die mitgesendete Phrase angezeigt. Außerdem kann man in den meisten Clients (auch in Notes) einstellen, ob die Namensspalte nach dem Vornamen oder Nachnamen sortiert sein soll.

Tipp: Überprüfen Sie bei dieser Gelegenheit auch gleich, ob als Zeichensatz für das MIME-Format Unicode (UTF-8) eingestellt ist!

8.3.6. HTML-Mails ermöglichen

Per Vorgabe werden Notes-Mails als Textnachrichten ins Internet geschickt. Damit geht nicht nur die Formatierung verloren, sondern auch Ihre hübsch gestaltete Signatur, denn eingebettete Bilder werden dann als Anhänge mitgeschickt. Deshalb sollten Sie unbedingt die Konvertierung in HTML aktivieren, alles andere ist unprofessionell.

Damit auch Mail-Clients, die aus Sicherheitsgründen als Anzeigeeoption Text eingestellt haben, lesbare Mails empfangen, sollten Sie **mehrteilige Nachrichten** (Multi-Part Messages) generieren lassen.

Um mehrteilige Nachrichten zu versenden, navigieren Sie im Konfigurationsdokument zu **MIME > Konvertierungsoptionen > Ausgang** und wählen Sie im Feld **Nachrichteninhalt** die Option »von Notes in einfachen Text und HTML«.

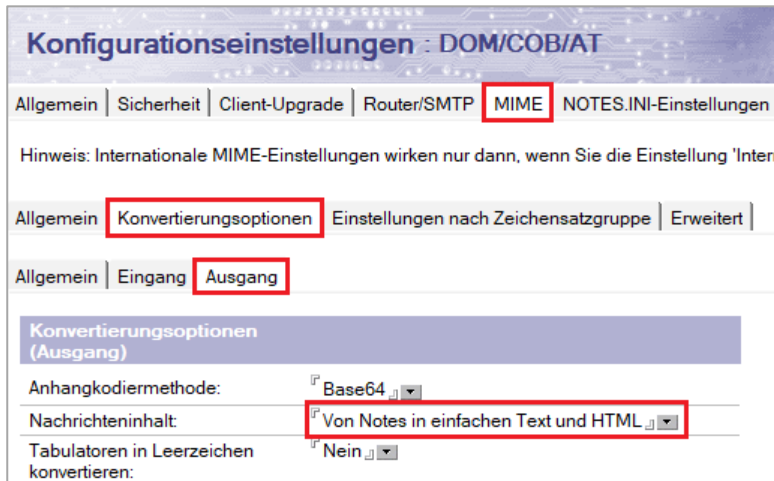


Abbildung 8.15: Konfiguration – Konvertierungsoptionen Mailausgang

8.3.7. Der SMTP-Server lässt grüßen

Wie sich Ihr SMTP-Server auf Anfragen auf dem Port 25 meldet, können Sie unter Windows mit dem Programm Telnet abfragen. Eröffnen Sie dazu einfach eine Eingabeaufforderung und geben Sie den folgenden Befehl ein:

```
telnet <Hostname> 25
```

Wenn Sie die Abfrage direkt am Server ausführen, können Sie natürlich auch mit den Platzhaltern localhost oder 127.0.0.1 arbeiten:

```
C:\>telenet localhost 25
Verbindungsaufbau zu localhost...
```

Die Ausgabe sieht dann wie folgt aus:

```
220 dom.cob.at ESMTP Service (HCL Domino Release 11.0.1) ready at Fri, 15 May
2020 19:54:10 +0200
```

Nach dem Motto: »Je mehr man preisgibt, desto angreifbarer wird man«, bevorzuge ich, im Internet so wenig wie möglich zu verraten. Daher ändere ich diese Meldung immer, was mit dem folgenden Eintrag in der Datei notes.ini möglich ist:

```
SMTPGreeting=Meldungstext
```

Dabei sollten Sie zwei Dinge beachten:

1. Am Anfang des Meldungstextes muss der Name des SMTP-Servers stehen. Wenn Ihr Server direkt erreichbar ist, dann derselbe, der auch im MX-Record aufscheint.
2. Der »Gruß« muss außerdem den Platzhalter »%s« enthalten, der durch das aktuelle Datum/die aktuelle Uhrzeit ersetzt wird, wenn die Verbindung hergestellt wird.

Am einfachsten geht das über einen Eintrag im Konfigurationsdokument, Register **NOTES.INI-Einstellungen**:

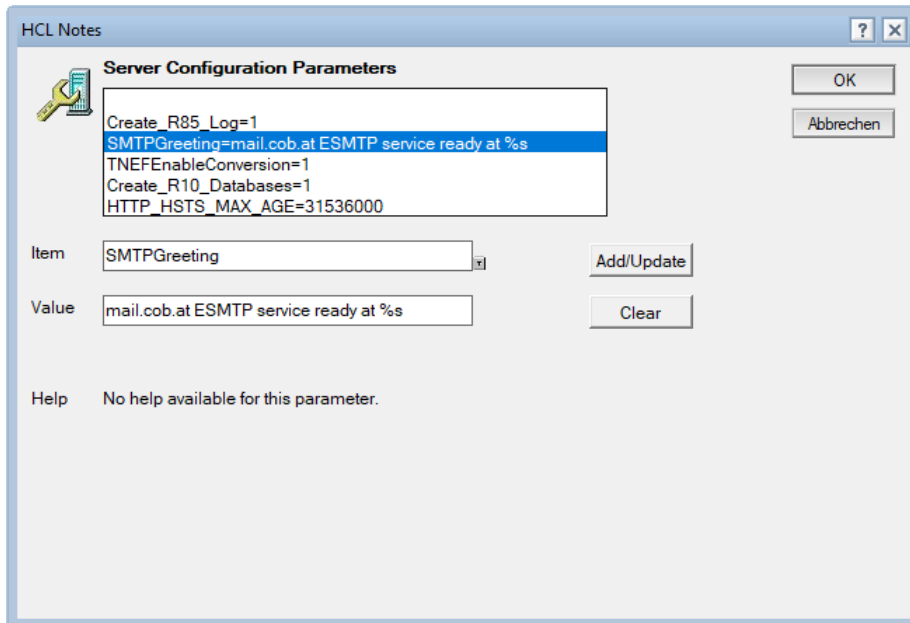


Abbildung 8.16: Konfigurationsdokument, Register NOTES.INI-Einstellungen – Parameter hinzufügen

8.3.8. Auf Spurensuche im MIME-Header

Beachten Sie, dass auch über Received-Header Produktinformationen offengelegt werden:

```
Received: from host.dom.at ([10.1.3.2])  
    by mail.cob.at (HCL Domino Release 11.0.1)  
    with ESMTP id 2020052207091241-582 ;  
    Fri, 22 May 2020 07:09:12 +0200
```

Wollen Sie Ihre Spuren komplett verwischen, müssen Sie in der Datei notes.ini den folgenden Eintrag setzen:

```
SMTPNoVersionInRcvdHdr=1
```

Aber das ist noch nicht alles: es gibt auch Client-Informationen im SMTP-Header, z. B.:

```
X-Mailer: HCL Notes Release 11.0.1|March 21, 2020  
Date: Wed, 20 May 2020 14:58:41 +0200  
X-MIMETrack: Serialize by Router on DOM/COB/AT(Release 11.0.1|March 21, 2020) at  
20.05.2020 14:58:42,  
    Serialize complete at 20.05.2020 14:58:42,  
    Itemize by SMTP Server on DOM/COB/AT(Release 11.0.1|March 21, 2020) at 20.05.2020  
14:58:44,  
    Serialize by NLNOTES.EXE on Christian Buchacher/COB/AT(Release 11.0.1|March 21,  
2020) at 23.05.2020 16:56:17
```

Diese können Sie aus dem Header entfernen, indem Sie die entsprechenden Notes-Items ausschließen. Die Einstellung dafür finden Sie im Konfigurationsdokument unter **MIME > Erweitert > Erweiterte Optionen für ausgehende Nachrichten**:

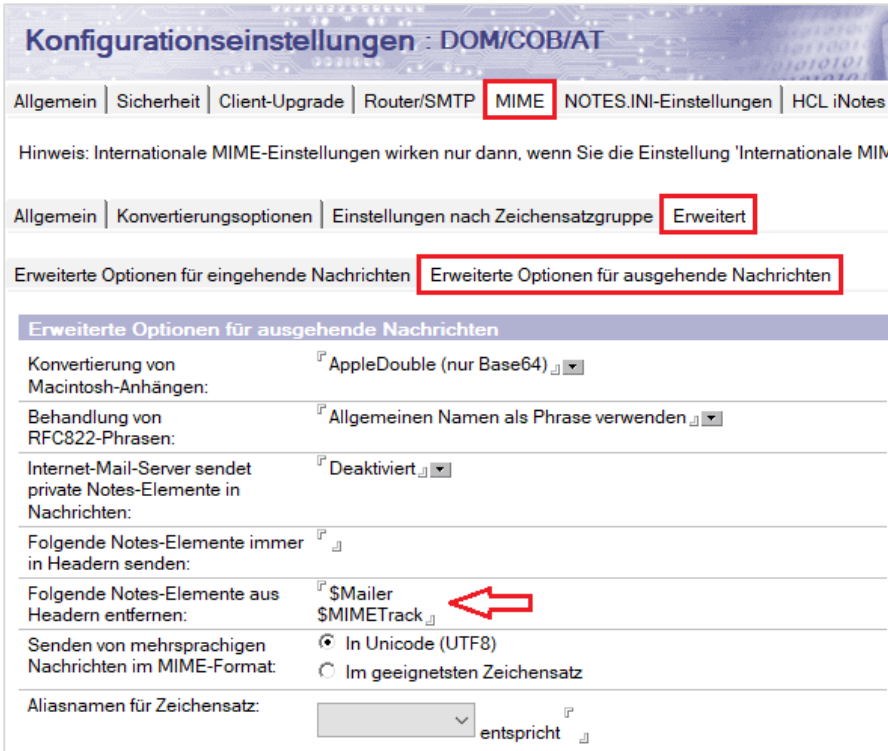


Abbildung 8.17: Konfiguration – Notes-Elemente aus Headern entfernen

Damit die Änderungen sofort greifen, geben Sie folgenden Befehl ein:

```
tell router update config
```

8.3.9. TLS für SMTP aktivieren

SMTP-Mails werden standardmäßig unverschlüsselt zwischen Servern ausgetauscht. Und da es sich um Textnachrichten handelt, können diese leicht mitgelesen werden. Die Mails selbst zu verschlüsseln wäre technisch zwar möglich (Standard S/MIME), jedoch aufwendig, da man mit allen Geschäftspartnern Geheimschlüssel austauschen müsste. Was man hingegen mit relativ wenig Aufwand und mit Boardmitteln einrichten kann, ist eine verschlüsselte Kommunikation zwischen den Mailservern. Dabei werden die Mails selbst nicht verschlüsselt, sondern nur verschlüsselt von einem Server zum nächsten übertragen (Sitzungsverschlüsselung).

Voraussetzung dazu ist der Erwerb eines TLS-Zertifikats. TLS-Zertifikate sind auch bei Webservern üblich und gewährleisten dort einen sicheren Zugriff auf eine Webseite. (Das Anfordern und Einspielen eines Zertifikats ist in Kap. 14.7 TLS-Zertifikate erstellen, ab Seite 394 beschrieben.)

Allerdings dürfen Sie nicht davon ausgehen, dass Ihre Kunden alle TLS unterstützen, weshalb Sie auf abgesicherte Verbindungen nicht unbedingt bestehen sollten – außer Sie haben ohnehin zu viel zu tun und wollen auf ein paar Mails verzichten ...

Die Verwendung von TLS kann für eingehende und für ausgehende Verbindungen getrennt konfiguriert werden. Die Einstellungen für eingehende Verbindungen finden Sie im Konfigurationsdokument, Register **Router/SMTP > Erweitert... > Befehle und Erweiterungen**.

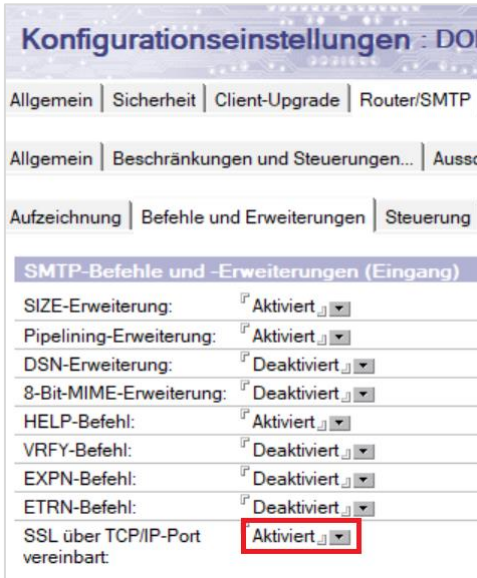


Abbildung 8.18: Konfigurationsdokument, Register **Befehle und Erweiterungen**

Wenn die Einstellung auf »Aktiviert« gestellt wird, versucht der Domino-Server, sich mit dem verbundenen Mailserver auf eine TLS-Verbindung zu einigen. Ist eine Verschlüsselung nicht möglich, wird unverschlüsselt übertragen. Wurde im Feld **SSL über TCP/IP-Port vereinbart** »Erforderlich« gewählt, wird die Verbindung in diesem Fall abgebrochen.

Für ausgehende Verbindungen werden die Einstellungen im Serverdokument unter **Ports... > Internet Ports... > Mail** vorgenommen. Wählen Sie hier in der Zeile **TCP/IP-Portstatus** für **SMTP-Ausgang** die Option »Vereinbartes SSL« Vergessen Sie nicht, den **TLS-Portstatus** auch zu aktivieren.



Abbildung 8.19: Einstellung »Vereinbartes SSL« im Serverdokument, Register Internet Ports

Leider erzwingt Domino TLS für ausgehende Verbindungen, auch wenn Sie hier »Vereinbartes SSL« auswählen. Dies können Sie korrigieren, indem Sie zur notes.ini des Servers den folgenden Parameter hinzufügen:

RouterFallbackNonTLS=1

(Danach sollten Sie den SMTP-Dienst neu starten.)

Die Einstellungen gelten auf dem Server dann natürlich für alle Verbindungen, das heißt, Sie können TLS nicht selektiv für einzelne Internet-Domänen ein- und ausschalten. Sie könnten allerdings einen extra Domino-Server aufbauen, der ausgehende TLS-Verbindungen erzwingt, und dann Mails an die gewünschten Internet-Domänen mithilfe von Domänen-Dokumenten (Typ: Fremde SMTP-Domäne) dorthin umleiten, was – zugegebenermaßen – eine etwas aufwendige Lösung darstellt.

8.4. Weitere Maileinstellungen

Die folgenden Einstellungen müssen nur bei Bedarf gesetzt, sollten aber alle kontrolliert werden.

8.4.1. Anzahl Mailboxen

Zwei Servertasks konkurrieren um eine Mailbox, der SMTP-Server und der Mail-Router. Wenn die Zugriffskonflikte dauerhaft mehr als 2 % betragen, sollten Sie Ihrem Server eine zweite Mailbox gönnen. Den Prozentsatz bestimmen Sie mithilfe der folgenden Statistiken:

$(\text{Mail.Mailbox.AccessConflicts} / \text{Mail.Mailbox.Accesses}) \times 100 > 2$

Kommen Sie zu dem Schluss, dass Ihr Server zwei Mailboxen benötigt, öffnen Sie das Konfigurationsdokument und geben Sie auf dem Register **Router/SMTP > Allgemein** im Feld **Anzahl der Mailboxen** die Ziffer »2« ein:



Abbildung 8.20: Konfiguration Anzahl Mailboxen

Wenn es zuvor häufig Zugriffskonflikte gab, erzeugt die zweite Mailbox einen enormen Performanceschub. Bei mehr als zwei Mailboxen wird der Nutzen geringer, mehr als vier Mailboxen machen auch in großen Umgebungen keinen Sinn.

Speichern und schließen Sie das Dokument und starten Sie den Server durch.

Beim Hochfahren erstellt der Mail-Router zwei neue Mailbox-Dateien mit den Namen mail1.box und mail2.box. Die alte Datei mail.box wird nicht mehr verwendet, kann aber noch nicht übertragene Mails enthalten. Daher sollten Sie die alte Mailbox einmalig öffnen und diese Mails in eine der beiden neuen Mailbox-Dateien kopieren.

8.4.2. Transaktionsprotokollierung für Mailboxen abschalten

Aus Performancegründen sollte Sie unbedingt die Transaktionsprotokollierung für Mailboxen abschalten! Dafür existiert eine zentrale INI-Variable:

MailboxDisableTXNLogging=1

Beachten Sie, dass erst nach dem Setzen dieser Variablen erzeugte Mailboxen keine Protokollierung mehr verwenden! Daher sollten Sie alle Mailboxen neu erstellen lassen.

8.4.3. Adresssuche

Nehmen wir an, Sie besitzen die Internet-Domänen cob.at und cobsoft.at. Ihr Mitarbeiter Franz Meier hat in seinem Personendokument die Adresse franz.meier@cob.at eingetragen. »franz.meier@cob.at« ist der vollständige Name (Fullname), alles vor dem At-Zeichen, also »franz.meier« der lokale Teil (Local Part).

Und jetzt nehmen wir an, der SMTP-Server erhält Mails an franz@cob.at, meier@cob.at oder auch franz.meier@cobsoft.at. Nimmt er sie entgegen und stellt sie Franz Meier zu?

Das hängt davon ab, was Sie im Konfigurationsdokument Ihres Mailservers, im Register **Router/SMTP > Allgemein** im Feld **Adresssuche** eingetragen haben.

8.4.3.1. »Vollst. Name dann lokaler Teil« (Vorgabe)

Der SMTP-Server nimmt alle Mails entgegen. Der Router findet zwar keine Person, die eine dieser Mailadressen eingetragen hat, die Mail wird aber trotzdem zugestellt, weil der Router bei der Adressierung automatisch auf den lokalen Teil herunterschaltet und »franz.meier« ebenso eindeutig ist. Dasselbe gilt auch für »meier« oder »franz« allein, wenn diese Namen eindeutig sind.

8.4.3.2. »Nur vollständiger Name«

Bei dieser Konfiguration nimmt der SMTP-Server die Mails nicht entgegen bzw. stellt sie der Router nicht zu, da obige Adressen in keinem Personendokument existieren. Nehmen Sie diese Einstellung vor, wenn Sie nicht wollen, dass Mails nur an Vor- bzw. Nachnamen geschickt werden bzw. Sie auch strikt zwischen Domänen trennen wollen.

8.4.4. Relay-Host

Wenn Sie nicht wollen, dass Ihr Domino-Server die Mailserver der Internet-Zieldomänen via DNS und MX-Record auflöst und direkt kontaktiert, sondern alle Internet-Mails an eine bestimmte Adresse (meist eine Firewall oder der Mailserver des Internet-Providers) schickt, tragen Sie im Feld **Relayhost für Nachrichten, die die lokale Internetdomäne verlassen** einen Hostnamen (oder auch eine IP-Adresse) ein.

Sie können auch zwei Relay-Hosts angeben, wobei zwei verschiedene Trennzeichen zur Verfügung stehen:

Verwenden Sie ein Komma, wenn beide Relay-Hosts abwechselnd (eigentlich in zufälliger Reihenfolge) verwendet werden sollen (Lastverteilung – Load Balancing):

Host1, Host2

Verwenden Sie ein Semikolon, wenn der zweite Host nur verwendet werden soll, wenn der erste nicht verfügbar ist (Ausfallsicherung – Failover):

Host1; Host2

Sollte der Relay-Host (etwa Ihres Internet-Providers) eine Authentifizierung erfordern, wählen Sie im Feld **Beim Senden von Nachrichten an den Relayhost Authentifizierung verwenden** »Aktiviert« und hinterlegen Sie Anmeldenamen und Kennwort:

Relaishost für Nachrichten, die die lokale Internetdomäne verlassen:	<input type="text" value="gateway1.cob.at; gateway2.cob.at"/>
Beim Senden von Nachrichten an den Relaishost	<input type="checkbox"/> Aktiviert
Authentifizierung verwenden:	Name: <input type="text" value="administrator"/> Kennwort: <input type="text" value="passwort"/>
Smart-Host der lokalen Internetdomäne:	<input type="text"/>
Smart-Host für alle Empfänger innerhalb der lokalen Internetdomäne:	<input type="checkbox"/> Deaktiviert
Zuordnung von Hostnamen:	<input type="checkbox"/> Dynamisch dann lokal

Abbildung 8.21: Konfiguration Relay-Hosts

In der deutschen Verzeichnisschablone wurde der falsche Name »Relaishost« verwendet.

8.4.5. Smart-Host

Ein Smart-Host ist eine spezielle Form eines Relay-Hosts, der Mails an Adressen innerhalb der Absenderdomäne entgegennimmt, die im Domino-Verzeichnis nicht existieren. Sie brauchen nur dann einen Smart-Host, wenn Ihr Domino-Verzeichnis nicht alle Empfänger Ihrer Domäne enthält.

8.4.6. Absenderadresse aus dem Personendokument erzwingen

Bei Internet-Mails wird als Absenderadresse standardmäßig das Feld **Internet-Mailadresse** aus der Arbeitsumgebung der Kontakte-Applikation verwendet (Feldname: ImailAddress). Normalerweise steht dort nicht nur dieselbe Adresse wie im Personendokument, der Notes-Client sorgt auch in regelmäßigen Abständen für einen Abgleich. Der Benutzer kann jedoch den Abgleich ausschalten, indem er in der Arbeitsumgebung im Bearbeitungsmodus den Befehl **Aktionen > Erweitert > Bearbeitungsflag setzen** aufruft und im angezeigten Dialog »Nein« wählt:

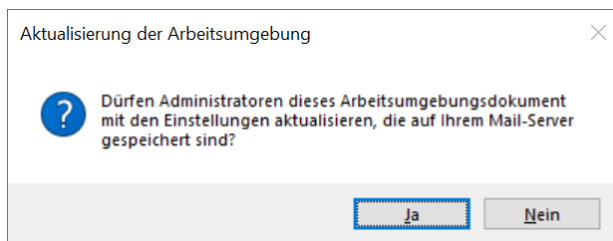


Abbildung 8.22: Arbeitsumgebung: Bestätigungsdialog Bearbeitungsflag setzen

Diese Vorgangsweise mag sinnvoll sein, wenn Benutzer verschiedene Absenderadressen benötigen. Dass hier jeder eine beliebige Adresse eintragen kann, führt aber auch rasch zu Problemen, vor allem wenn die Absenderdomäne geändert wurde. Um das serverweit zu verhindern, können Sie den folgenden Eintrag zur Datei notes.ini hinzufügen:

```
RouterTranslateSpecial=1
```

Wenn der Mail-Router diese Variable vorfindet, ersetzt er die Absenderadresse aus dem Feld INet-From durch die Internet-Mailadresse im Personendokument.

8.5. Mail-In-Datenbanken

Bei Mail-In-Datenbanken handelt es sich in der Regel um Anwendungen, die Daten über das Mail-System erhalten und diese via Programmcode weiterverarbeiten. (Dafür gibt es die Datenbankereignisse »Vor Eingang neuer Mail« und »Nach Eingang neuer Mail« zum automatischen Starten von Agenten, wenn Mails zugestellt werden.) Ich schreibe deshalb »in der Regel«, da viele Administratoren Mail-In-Datenbanken auch dazu verwenden, um generische Mailadressen wie Office, Verkauf, Service etc. abzubilden. Man könnte hier auch von Gruppenpostfächern sprechen – im Gegensatz zu Benutzerpostfächern. Der Vorteil von Mail-In-Datenbanken liegt vor allem darin, dass keine Lizenzkosten anfallen, so lange lizenzierte Benutzer (hinter denen ein Personendokument steckt) darauf zugreifen. So gesehen können Sie theoretisch nur eine einzige Benutzerlizenz kaufen (für den Administrator) und dann für alle benötigten E-Mail-Adressen Mail-In-Datenbanken einrichten.

Um im Domino-Verzeichnis eine Mail-In-Datenbank zu erstellen, müssen Sie mindestens Autor mit den folgenden Rechten sein:

- > Berechtigung »Dokumente erstellen«
- > Rolle »NetCreator«
- > Rolle »NetModifizier«

Zum Erstellen einer Mail-In-Datenbank gehen Sie wie folgt vor:

1. Starten Sie den Domino-Administrator und navigieren Sie zu **Personen und Gruppen > Mail-In-Datenbanken und Ressourcen**.
2. Klicken Sie auf die Schaltfläche **Mail-In-Datenbank hinzufügen**.
3. Geben Sie einen Namen für die Mail-In-Datenbank ein.

Wenn Sie den Namen später als Besitzer der Maildatenbank eintragen wollen, muss er hierarchisch angegeben werden, in unserem Beispiel `Verkauf/COB/AT`. Soll der Name nicht hinterlegt werden, etwa weil es sich um eine Anwendung handelt, die Mails verarbeitet, können Sie den Namen auch ohne Schrägstriche eingeben.

4. Optional: Geben Sie eine kurze Beschreibung ein.
5. Optional: Geben Sie eine Internetadresse ein. Wenn Sie das Feld leer lassen, wird der eingegebene Name kombiniert mit der Internet-Domäne als Internetadresse verwendet, in unserem Beispiel also `verkauf@cob.at`.

Geben Sie im Feld **Internetadresse** nur eine Adresse ein. Müssen Sie mehrere Adressen hinterlegen, verwenden Sie dazu das Feld **Mail-In-Name**.

6. Stellen Sie im Feld **Internet-Nachrichtenspeicherung** ein, in welchem Format Mails gespeichert werden sollen. Wenn zum Lesen der Mails ein Notes-Client verwendet wird, wählen Sie »Keine Vorgabe«, um zugestellte Mails in ihrem ursprünglichen Format zu belassen. Wenn dazu ein (z. B. via IMAP angebundener) externer Client verwendet wird, wählen Sie »MIME«, damit Notes-Mails bei der Zustellung in MIME konvertiert werden.
7. Stellen Sie im Feld **Eingehende Mail verschlüsseln** ein, ob der Router Mails beim Zustellen verschlüsseln soll. Normalerweise verwendet man in einer Mail-In-Datenbank keine Verschlüsselung, da der Inhalt ja für mehrere Personen verfügbar sein soll. Wollen Sie Mails bei der Zustellung dennoch verschlüsseln, müssen Sie auf dem Register **Administration** im Feld **Notes-zertifizierter öffentlicher Schlüssel** den öffentlichen Schlüssel eines Benutzers bereitstellen. Die verschlüsselten Mails können dann nur von diesem Benutzer gelesen werden.

Allgemein		Arbeitsumgebung	
Mail-In-Name:	Verkauf/COB/AT Verkauf	Domäne:	COB
Beschreibung:		Server:	DOM/COB/AT
Internetadresse:	sales@cob.at	Dateiname:	mailverkauf.nsf
Internetnachrichtenspeicherung:	Keine Vorgabe		
Eingehende Mail verschlüsseln:	Nein		

Abbildung 8.23: Konfiguration Mail-In-Datenbank

8.6. Sinnvolle Mailvorgaben setzen

Im Notes-Client und in den Maildatenbanken sind die meisten Vorgaben sinnvoll gesetzt. Dennoch zahlt es sich aus, diese einmal durchzugehen und – falls nötig – via Richtlinien abweichende Einstellungen zu setzen.

8.6.1. Papierkorb

Per Vorgabe werden gelöschte Mails bereits nach 48 Stunden aus dem Papierkorb des Benutzers entfernt und können danach nur noch über eine Rücksicherung wiederhergestellt werden. Das ist in der Praxis zu kurz, da eine irrtümlich gelöschte Mail nach einem Wochenende nicht mehr zurückgeholt werden kann, und sollte auf 72 oder sogar 120 Stunden hochgesetzt werden. Umgekehrt sollten Sie Benutzer daran hindern, eine allzu große Zahl zu hinterlegen (50.000 – mehr als 2.000 Tage – sind problemlos möglich!), weshalb ich empfehle, die Änderung dieser Einstellung zu verhindern.

Die dafür nötige Einstellung finden Sie in der Mailrichtlinie auf dem Register Allgemein im unteren Bereich:

Abbildung 8.24: Mailrichtlinie: Wartung des Posteingangs

8.6.2. Einheitliche Sortierung für Ordner und Ansichten

Notes merkt sich die Sortierfolge nur pro Ordner, es ist aber auch möglich, in den Mail-Vorgaben eine globale Einstellung für alle Ordner zu setzen:

Abbildung 8.25: Mail-Vorgaben – Papierkorb und Datumsspalten automatisch sortieren

Diese Einstellung kann via Desktoprichtlinie vorgegeben werden. Wählen Sie dazu das Register **Vorgaben > Mail**:

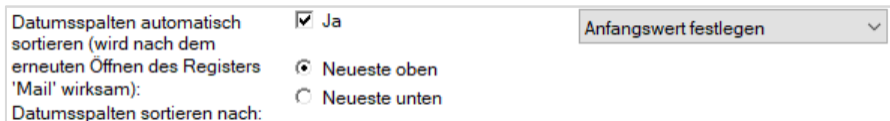


Abbildung 8.26: Globales Domänenendokument, Register Allgemein

8.6.3. Umgang mit Empfangsbestätigungen

An der Möglichkeit, Empfangsbestätigungen einzufordern, scheiden sich die Geister. Einerseits sind sie praktisch, weil der Absender damit feststellen kann, wann die von ihm versandte Mail gelesen wurde, andererseits setzen sie den Empfänger unter Druck, schnell auf eine Mail zu reagieren.

Da der Client die Bestätigung verschickt, wenn die Mail als gelesen markiert wird, stellen viele Anwender ein, dass im Vorschauenfenster geöffnete Mails nicht als gelesen gelten. Das gibt ihnen die Möglichkeit, eine Mail zu lesen, ohne dass der Absender davon erfährt.

Damit im Vorschauenfenster geöffnete Mails nicht als gelesen gelten, deaktivieren Sie in den Vorgaben des Notes-Clients, im Bereich **Notes-Client-Basiskonfiguration** in der Liste **Zusätzliche Optionen** das Feld **In Dokumentvorschau geöffnete Dokumente als gelesen markieren**.

Ihr Unternehmen muss jetzt eine Entscheidung treffen: Sollen Empfangsbestätigungen möglich sein oder nicht. Falls ja, erzwingen Sie, dass auch im Vorschauenfenster geöffnete Mails als gelesen markiert werden – überlassen Sie diese Entscheidung keinesfalls Ihren Benutzern. Die dafür nötige Einstellung finden Sie in der Desktoprichtlinie, im Register **Vorgaben > Verschiedenes**:



Abbildung 8.27: Desktoprichtlinie, Register Vorgaben > Verschiedenes

Oder falls nein, deaktivieren Sie Empfangsbestätigungen in der Mailrichtlinie, Register **Mail > Allgemein**:



Abbildung 8.28: Mailrichtlinie – Empfangsbestätigungen verbieten

Ein Abschalten der Empfangsbestätigung führt dazu, dass diese in den Mailoptionen deaktiviert werden:

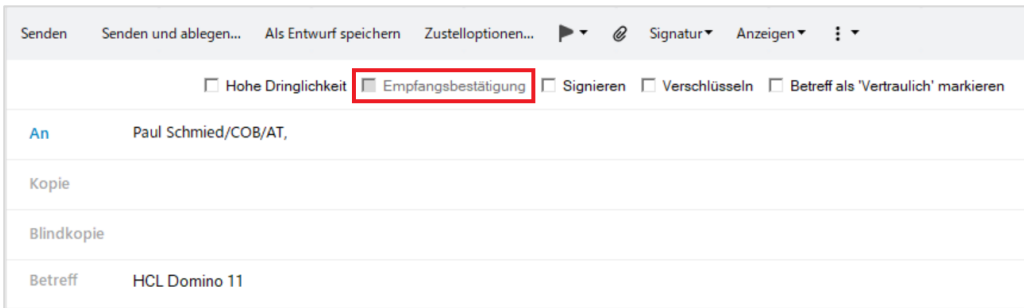


Abbildung 8.29: Mail bei deaktivierten Empfangsbestätigungen

In der folgenden Abbildung sehen Sie die Situation in den Zustelloptionen:

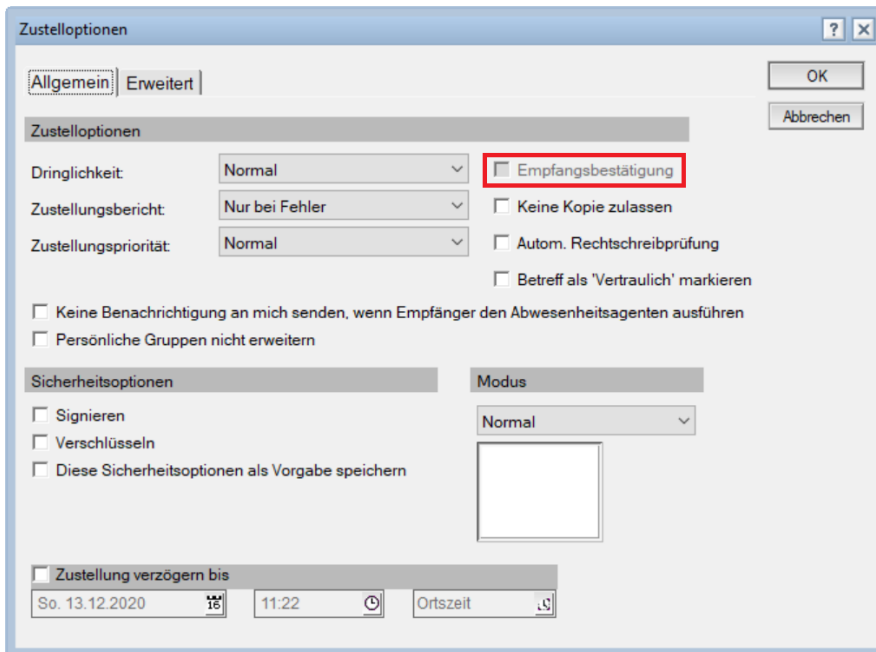


Abbildung 8.30: Zustelloptionen bei deaktivierten Empfangsbestätigungen

8.7. Beschränkungen beim Senden von Mails setzen

Sie können mehrere Beschränkungen für ausgehende Mails setzen. Größenüberschreitungen werden im Notes-Client beim Senden als Fehler oder Warnungen angezeigt. Warnungen können ignoriert werden (Link **Schließen**), beim Auftreten von Fehlern kann die Mail nicht verschickt werden. Folgende Beschränkungen sind möglich:

- > Maximale Dokumentgröße (Fehler)
- > Maximale Anzahl von Anhängen (Fehler)
- > Maximale Größe von Anhängen (Fehler)
- > Maximale Anzahl von Empfängern (Warnung)
- > Kein Betreff (Warnung)

> Schicken von Mails an externe Domänen (Warnung)

Für das Setzen von Beschränkungen für ausgehende Mails benötigen Sie eine Mailschablone der Version 10 (mail10.ntf) oder höher.

8.7.1. Vorgangsweise

1. Klicken Sie im Domino-Verzeichnis auf **Personen und Gruppen > Richtlinien > Einstellungen**.
2. Erstellen Sie eine neue Mail-Einstellung oder bearbeiten Sie eine vorhandene.
3. Setzen Sie im Register **Mail** bei **Grenzen für ausgehende festlegen** ein Häkchen und füllen Sie zumindest eines der folgenden Felder aus:

Grenzen für ausgehende festlegen:	<input checked="" type="checkbox"/> Ja
Maximale Dokumentgröße:	<input type="text" value="10000"/> KB
Maximale Anzahl von Anhängen:	<input type="text" value="4"/>
Maximale kombinierte Größe der Anhänge:	<input type="text" value="9000"/> KB
Maximale Anzahl einzelner Empfänger:	<input type="text" value="4"/>
Interne Domänen:	<input]<="" td="" type="text" value=""/>

Abbildung 8.31: Mailrichtlinie – Grenzen für ausgehende Mails festlegen

Die Erklärungen zu den einzelnen Einstellungen entnehmen Sie Tabelle 8.1.

4. Speichern und schließen Sie das Dokument.

Setzen Sie in der Mailrichtlinie keine Maximalgröße für ausgehende Mails, gilt die serverweite Einstellung im Konfigurationsdokument, Register **Router/SMTP > Beschränkungen und Steuerungen... > Beschränkungen** im Feld **Maximale Nachrichtengröße**. Steht hier die Ziffer 0, gibt es keine Größenbeschränkung für Mails.

Einstellung	Art	Beschreibung
Maximale Dokumentgröße	Fehler	Die maximale Dokumentgröße inklusive aller Anhänge
Maximale Anzahl von Anhängen	Fehler	Die maximale Anzahl von Anhängen
Maximale kombinierte Größe der Anhänge	Fehler	Maximale Größe aller Anhänge
Maximale Anzahl einzelner Empfänger	Warnung	Anzahl der Empfänger im Adressfeld (Ein Gruppenname wird als ein Eintrag gewertet.)
Interne Domänen	Warnung	Auflistung interner Internet-Domänen, bei allen anderen wird eine Warnung angezeigt

Tabelle 8.1: Grenzen für ausgehende Mails

Bei einer Warnung ist ein Verschicken nach Bestätigung möglich, bei einem Fehler kann die Mail hingegen nicht verschickt werden.

Wenn Sie zu einer der oben aufgezählten Grenzen auch noch die Eigenschaft **Warnung bei fehlendem Betreff in Nachrichten** setzen, erhält der Benutzer noch zusätzlich eine Warnung, wenn er die Mail ohne Betreff abschickt.

Die Änderungen in der Mail-Policy können mit dem folgenden Serverkonsolen-Befehl sofort an alle Benutzer ausgerollt werden:

```
tell adminp process mailpolicy
```

Das Überprüfen der Regeln erfolgt beim Senden der Mail. Eine Warnung wird angezeigt, wenn zumindest eine Beschränkung überschritten wird:

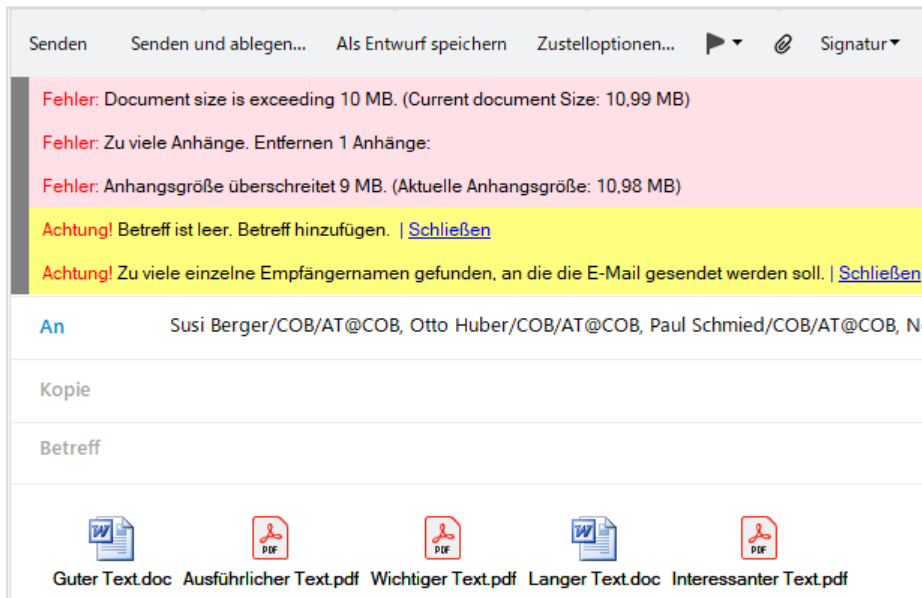


Abbildung 8.32: Mail mit mehreren überschrittenen Beschränkungen und Warnungen

Beachten Sie, dass diese Einstellungen von HCL iNotes (Webmail) nicht beachtet werden. Sie können jedoch in der Maileinstellung im Register **HCL iNotes > Konfiguration** die Maximalgröße von Anhängen beschränken.

8.8. Geplante Nachrichten versenden

In Notes ist es möglich, das Versenden einer Nachricht bis zu einer bestimmten Zeit zu verzögern. So kann ein Anwender die Nachricht bereits am Wochenende erstellen und an den Domino-Server senden, der sie dann zur eingestellten Zeit weiterleitet. **Geplante Nachrichten** (Scheduled Messages) werden bis zum Absenden in der mail.box des Homeservers des Absenders aufbewahrt.

Die Konfiguration von Geplanten Nachrichten ist in Domino auf zwei Ebenen implementiert: 1. serverweit im Konfigurationsdokument und 2. auf Richtlinienbasis. Die Möglichkeit, das Versenden von Nachrichten zu verzögern, ist auf einem neu installierten Domino-Server der Versionen 10 oder 11 per Vorgabe aktiviert. Haben Sie einen älteren Server aktualisiert, sollten Sie die Einstellungen überprüfen.

8.8.1. Geplante Nachrichten serverweit aktivieren

1. Öffnen Sie das Domino-Verzeichnis und navigieren Sie zu **Server > Konfigurationen**.
2. Öffnen Sie das Konfigurationsdokument Ihres Mailservers im Bearbeitungsmodus oder erstellen Sie ein neues.
3. Wählen Sie **Router/SMTP > Beschränkungen und Steuerungen > Übertragung**.
4. Wählen Sie im Feld **Benutzern erlauben, einen Zustellzeitpunkt für Nachrichten festzulegen** entweder »Aktiviert« oder »Deaktiviert«.
5. Speichern und schließen Sie das Dokument.
6. Geben Sie auf der Serverkonsole den folgenden Befehl ein:
`tell router update config`

Haben Sie das Versenden von Geplanten Nachrichten aktiviert, können Benutzer diese in den Zustelloptionen aktivieren:

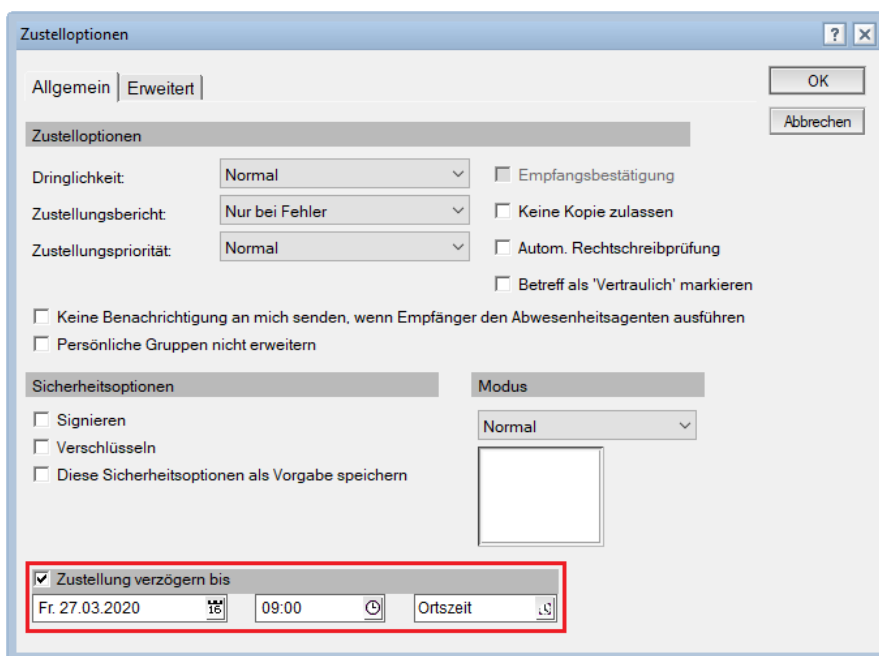


Abbildung 8.33: Zustelloptionen – Einstellungen verzögerte Zustellung

Ältere Domino-Versionen (vor 10) erkennen verzögerte Nachrichten nicht und versenden diese sofort. Außerdem muss das Domino-Verzeichnis auf Version 10 oder höher aktualisiert werden und die Maildatenbank auf der Mailschablone Version 10 (mail10.ntf) oder 11 (mail11.ntf) beruhen.

8.8.2. Geplante Nachrichten für bestimmte Benutzer aktivieren

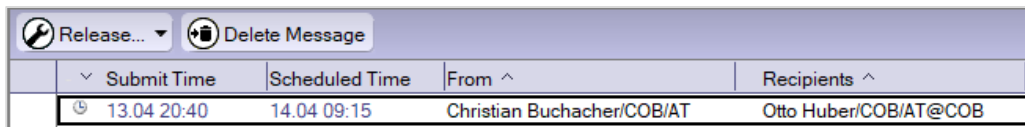
Mit der Einstellung im Konfigurationsdokument wird das Versenden von Geplanten Nachrichten serverweit für alle erlaubt oder verboten. Wollen Sie das Feature auf bestimmte Benutzergruppen einzuschränken, muss es serverweit erlaubt sein. Erstellen Sie sodann zwei Mailrichtlinien, eine, in der das Feature aktiviert, und eine zweite, in der es deaktiviert ist:

1. Öffnen Sie das Domino-Verzeichnis und navigieren Sie zu **Personen > Richtlinien > Einstellungen**.

2. Bearbeiten Sie eine existierende Maileinstellung und erstellen Sie mit der Schaltfläche **Einstellung hinzufügen...** > **Mail** eine neue.
3. Deaktivieren Sie im Register **Mail** > **Allgemein** im Bereich **Zustelloptionen** das Feld **Benutzern erlauben zu planen, wann Nachrichten zugestellt werden**, um das Feature zu verbieten.
4. Klicken Sie auf **Speichern und schließen**.
5. Erstellen Sie eine zweite Maileinstellung, in der Sie das Feature aktivieren.
6. Weisen Sie die Maileinstellung mit dem deaktivierten Feature einer Richtlinie zu, der alle Benutzer zugeordnet wurden.
7. Weisen Sie die Maileinstellung mit dem aktivierten Feature einer Richtlinie zu, der nur jene Benutzer zugeordnet wurden, die das Feature verwenden sollen.
8. Mailrichtlinien werden vom Administrationsprozess alle 12 Stunden ausgerollt. Wenn Sie nicht so lange warten wollen, geben Sie auf der Serverkonsole den folgenden Befehl ein:
`tell adminp process mailpolicy`
9. Nach Ausrollen der Mailrichtlinie sehen die Benutzer, die das Feature zugeordnet haben, im Dialog **Zustelloptionen** die Möglichkeit, die Zustellung zu verzögern (siehe Abbildung 8.33).

8.8.3. Zustellungszeit einer geplanten Nachricht ändern

Geplante Nachrichten (erkennlich am Uhrensymbol am linken Rand) warten in der Datei mail.box des Mailservers auf ihre Weiterleitung:



Submit Time	Scheduled Time	From	Recipients
🕒 13.04 20:40	14.04 09:15	Christian Buchacher/COB/AT	Otto Huber/COB/AT@COB

Abbildung 8.34: Mail mit verzögerter Zustellung in der Servermailbox

Um die geplante Zeit zu ändern, öffnen Sie die Nachricht und schalten Sie in den Bearbeitungsmodus um. Geben Sie im Feld **Scheduled Date** ein neues Datum bzw. eine neue Zeit ein und speichern Sie die Nachricht.

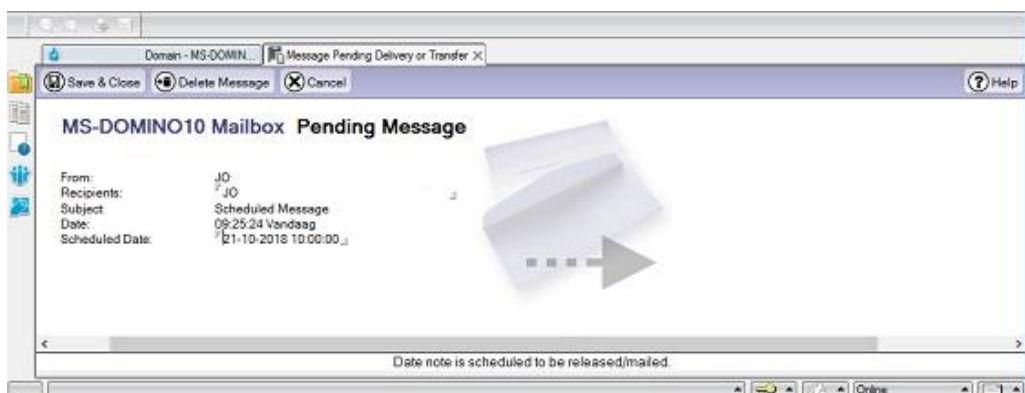


Abbildung 8.35: Aus der Mailbox geöffnetes Mail mit verzögerter Zustellung

Um die Nachricht zu löschen, klicken Sie auf **Delete Message**.

8.8.4. Überwachen geplanter Nachrichten

Die Statistiken für Geplante Nachrichten entnehmen Sie bitte Tabelle 8.2:

Statistik	Erklärung
Mail.WaitingForSchedule	Zeigt die Anzahl der auf Zustellung wartenden geplanten Nachrichten an
Mail.TotalScheduledReleased	Zeigt die Anzahl der versendeten geplanten Nachrichten seit dem letzten Serverstart an
Mail.WaitingNotScheduled	Zeigt die Anzahl der wartenden Nachrichten ausgenommen der geplanten Nachrichten an

Tabelle 8.2: Statistiken zu geplanten Nachrichten

Um eine Statistik aufzurufen, geben Sie auf der Serverkonsole folgenden Befehl ein:

```
show statistic <Statistik>
```

Mit den folgenden Befehlen erhalten Sie Informationen zum Status von Geplanten Nachrichten:

```
tell router list
```

```
tell router show
```

8.9. Auf Zustellungsfehler reagieren

Innerhalb der Notes-Domäne lässt die Mailer-Software ein Senden an unbekannte Empfänger nicht zu. Adressieren Sie jedoch an eine Internet-Domäne oder an eine fremde Notes-Domäne, verschickt der Mailer die Mail, ohne die Adresse zu prüfen. Existiert die Domäne nicht, wird dem Absender vom Mail-Router ein **Zustellungsfehlerbericht** (Non Delivery Report, NDR) zugestellt, der darüber informiert, warum die Nachricht nicht weitergeleitet werden konnte.

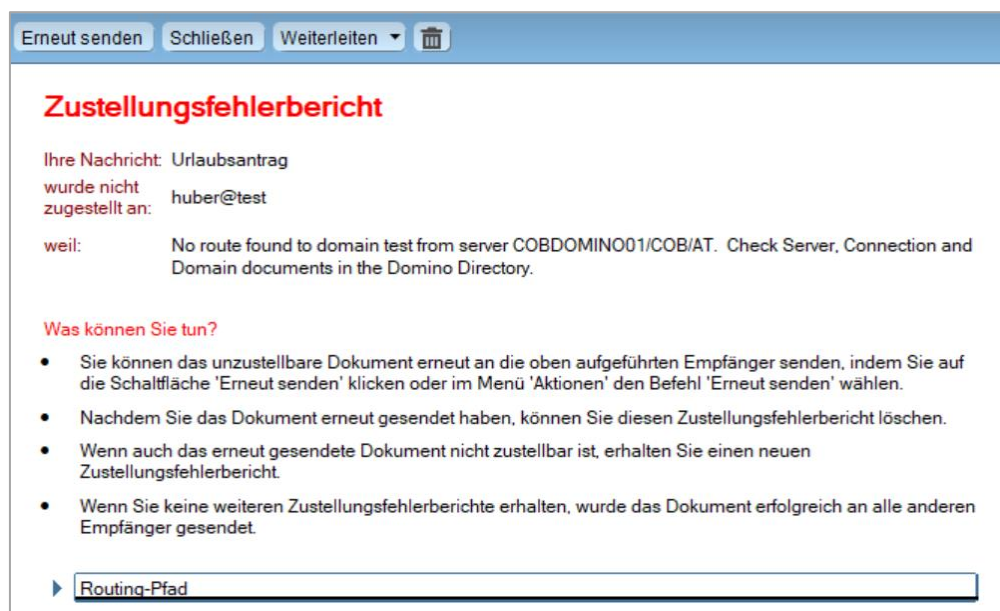


Abbildung 8.36: Zustellungsfehlerbericht

8.10. Auf unzustellbare Nachrichten reagieren

Eine unzustellbare Nachricht (Dead Message) entsteht, wenn der Router eine Mail weder an den vorgesehenen Empfänger senden noch an den Absender zurücksenden kann. Das kommt relativ häufig vor, da das Zurücksenden von Nachrichten an unbekannte Empfänger aufgrund von Richtlinienbeschränkungen oft nicht erlaubt ist. Andere Gründe für eine Unzustellbarkeit können sein, dass ein Personendokument fehlt, eine Person umbenannt wurde oder die Empfängermaildatenbank korrupt ist. Wurde eine Nachricht als unzustellbar (»Dead«) klassifiziert, wird keine Zustellung mehr versucht und sie bleibt in der Mailbox (mail.box) hängen.

8.10.1. Manuelle Verarbeitung nicht zustellbarer Mails

Für eine manuelle Verarbeitung stehen drei Optionen zur Verfügung:

1. Die Nachricht wurde aufgrund eines Fehlers nicht zugestellt und der Administrator kann den Fehler beheben. In diesem Fall kann die Mail in der Mailbox mit dem Befehl **Resend Selected Dead Message** erneut verschickt werden:

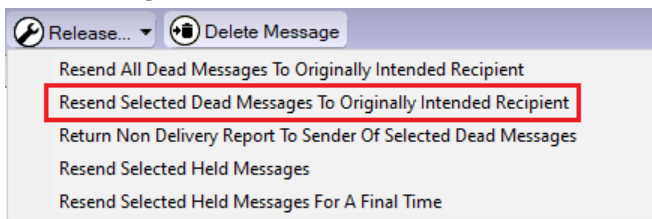


Abbildung 8.37: Mailbox – Gewählte unzustellbare Nachrichten erneut versenden

2. Die Mail ging an eine unbekannte Adresse, konnte aufgrund von Richtlinienbeschränkungen aber nicht als Zustellfehler (None Delivery Report – NDR) zurückgeschickt werden. In diesem Fall können Sie den Zustellfehler mit dem Befehl **Return Non Delivery Report** zurückschicken – Ihnen als Person ist das Relaying ja erlaubt.

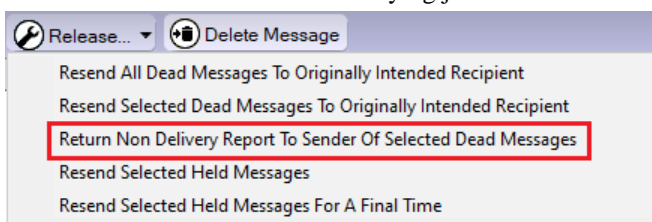


Abbildung 8.38: Mailbox – NDR für gewählte Nachrichten versenden

3. Sie können das Problem nicht beheben oder es handelt sich eindeutig um eine SPAM-Mail. In diesem Fall löschen Sie die Nachricht.

Das Vorhandensein von unzustellbaren Nachrichten kann auf der Serverkonsole über folgende Befehle abgefragt werden:

```
show server
show statistic mail (siehe Statistik mail.dead)
```

Alle Ereignisse, die die Mailweiterleitung betreffen, werden außerdem in der Protokolldatei (log.nsf) in der Ansicht **Mail-Weiterleitungsereignisse** angezeigt.

8.10.2. Automatische Verarbeitung nicht zustellbarer Mails

Wenn sich der Administrator nicht darum kümmert, sammeln sich die unzustellbaren Nachrichten in der Mailbox so lange an, bis sie von einem Administrator gelöscht werden. Alternativ kann konfiguriert werden, dass der Mail-Router nach Ablauf einer gewissen Zeit wieder eine Zustellung versucht und die Nachricht löscht, wenn dies erfolglos bleibt (Dead Mail Processing).

Wenn Sie die automatische Verarbeitung aktiviert haben und der Mail-Router in der mail.box auf eine nicht zustellbare Nachricht trifft, laufen die folgenden Schritte ab:

1. Wenn die erlaubte Anzahl von Zustellungsversuchen erreicht wurde, löscht der Mail-Router die nicht zustellbare Nachricht und die Verarbeitung ist damit beendet. Wenn der Administrator die Anzahl der erlaubten Zustellversuche auf 0 gesetzt hat, wird die Nachricht ohne weiteren Zustellversuch gelöscht.
2. Der Router versucht die Originalnachricht nochmals zuzustellen. Bei Erfolg endet die Verarbeitung.

Anmerkung: Dieser Schritt wird übersprungen, wenn der vorgesehene Empfänger von einer externen Domäne außerhalb Ihrer Firma stammt.
3. Der Router versucht eine Zustellfehlernachricht (Non-Delivery Report – NDR) an den Absender zu schicken. Bei Erfolg endet die Verarbeitung.
4. Der Router wartet die voreingestellte Wiederholungszeit ab und geht zu Schritt 1 zurück.

Um die Automatische Verarbeitung von nicht zustellbaren Mails zu konfigurieren:

1. Öffnen Sie das Domino-Verzeichnis.
2. Erweitern Sie **Konfiguration > Server > Konfigurationen**.
3. Wenn bereits ein Konfigurationsdokument existiert, öffnen Sie dieses und schalten Sie in den Bearbeitungsmodus um. Wenn es noch keines gibt, erstellen Sie ein neues und geben Sie im Feld **Gruppen- oder Servername** den Namen des Mailservers ein.
4. Navigieren Sie zum Register **Router/SMTP > Erweitert > Steuerung**.
5. Wählen Sie im Bereich **Unzustellbare E-Mails**, im Feld **Dead Mail automatisch verarbeiten** den Wert »Aktiviert«.
6. Geben Sie im Feld **Zulässige Zustellversuche für Dead Mail** die Anzahl der Zustellversuche ein, bevor die Mail gelöscht wird. (Vorgabe ist 12, Maximum ist 1000.) Der Router merkt sich die Anzahl erfolgter Zustellungsversuche auch über Router- und Serverneustarts hinaus. Wenn Sie 0 eingeben, wird keine erneute Zustellung versucht, sondern die Mail sofort gelöscht.
7. Geben Sie im Feld **Zeit zwischen Zustellversuchen für Dead Mail** die Zeit zwischen den Zustellversuchen in Minuten ein. Vorgabe ist 360 (6 Stunden), Minimum sind 15, Maximum sind 1.440 Minuten (24 Stunden).
8. Wenn Sie innerhalb ihres Unternehmens mehrere Internet-Domänen verwenden, geben Sie dies im Feld **Interne Internetdomänen** an, sonst lassen Sie das Feld leer. Ein Server versucht die Originalnachricht nochmals zu versenden, wenn der Zustellungsfehlerbericht aus einer internen Domäne kam. Zustellungsfehlerberichte von nicht aufgelisteten Domänen werden als extern angenommen und der Router versucht nur noch, den Zustellungsfehlerbericht erneut zuzustellen und nicht die Originalnachricht.

Unzustellbare E-Mails

Unzustellbare Mail zurückstellen: Deaktiviert

Dead Mail automatisch verarbeiten: Aktiviert

Zulässige Zustellversuche für Dead Mail:

Zeit zwischen Zustellversuchen für Dead Mail: Minuten

Interne Internetdomänen: cob.at
 cobsoft.at

Abbildung 8.39: Mailrichtlinien – Einstellungen für unzustellbare E-Mails

8.10.3. Verarbeitung von nicht zustellbaren Mails überwachen

Zum Überwachen der automatischen Verarbeitung von nicht zustellbaren Nachrichten stehen zwei Statistiken zur Verfügung.

Befehl	Beschreibung
Show Stat Mail.Dead.RetryCount	Anzahl der fehlgeschlagenen Zustellversuche seit dem Serverstart (Wenn das Versenden von Nachricht 1 einmal versucht wurde und das Versenden von Nachricht 2 dreimal, ist die Anzahl 4.
Show Stat Mail.Dead.DeletedCount	Anzahl der gelöschten Nachrichten seit dem Serverstart.

Tabelle 8.3: Statistiken zum Überwachen der Verarbeitung nicht zustellbarer Nachrichten

8.11. Die Größen von Maildatenbanken beschränken

Größenbeschränkungen (Database Quotas) können prinzipiell für alle Datenbanken gesetzt werden, sind in der Praxis jedoch nur für Maildatenbanken relevant. Die Größe von Maildatenbanken kann bereits beim Registrieren von Benutzern beschränkt werden (siehe Kap. 6.4 Notes-Benutzer anlegen, ab Seite 152). Zusätzlich zur Maximalgröße kann außerdem ein Schwellenwert angegeben werden, bei dessen Überschreitung der Benutzer eine Warnung erhält.

Im Notes-Standard-Client werden Größenbeschränkungen sehr anschaulich dargestellt:

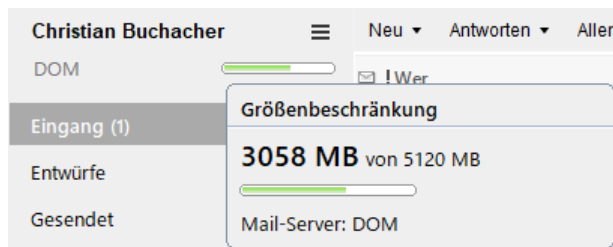


Abbildung 8.40: Anzeige von Größenbeschränkungen

8.11.1. Was passiert beim Überschreiten der Maximalgröße?

Wenn eine Datenbank die Maximalgröße überschritten hat, können keine Dokumente mehr gespeichert werden. Mails können entgegen der landläufigen Meinung auch weiterhin verschickt werden, zwar nicht über die Schaltfläche **Senden**, weil Notes per Vorgabe versucht, eine Kopie der gesendeten Mail zu speichern, aber durch Drücken der ESC-Taste und Auswahl der Option »Nur senden«.

Mails werden nach Überschreiten der Maximalgröße per Vorgabe auch weiterhin zugestellt, sodass der Anwender im Mailbereich eingeschränkt weiterarbeiten kann, etwa indem er Mails zusätzlich in Kopie an sich selbst schickt.

Was der Benutzer aber per sofort nicht mehr kann, ist Kalendereinträge oder Aufgaben erstellen bzw. auf Besprechungseinladungen zusagen.

8.11.2. Wann werden Größenbeschränkungen überprüft?

Löscht der Benutzer daraufhin mehrere Mails mit großen Anhängen (und leert auch den Papierkorb), kann er zunächst wieder Dokumente speichern, obwohl seine Maildatenbank nicht kleiner geworden ist, denn dazu müsste sie zuerst komprimiert werden. Das geht deshalb, weil die Größenbeschränkungen vom Domino-Server per Vorgabe nur überprüft werden, wenn die Datei zum Speichern eines Dokuments vergrößert werden müsste. Das Löschen der Mails hat jedoch Lücken (White Space) hinterlassen und so lange diese Lücken groß genug sind, um die neuen Dokumente darin aufzunehmen, kann der Benutzer wieder speichern.

Dieses Verhalten kann im Serverdokument, Register **Transaktionsprotokollierung**, im Feld **Größenbeschränkung erzwingen** angepasst werden:

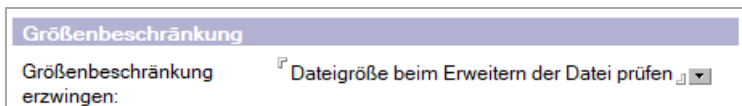


Abbildung 8.41: Einstellungen zu Größenbeschränkungen

Ich empfehle Ihnen, die Option »Belegten Speicherplatz in Datei beim Hinzufügen eines Dokuments prüfen«, weil Benutzer dann nach dem Löschen von Dokumenten sofort weiterarbeiten und Sie sich als Administrator mit dem Komprimieren der Datenbanken Zeit lassen können.

8.11.3. Mailzustellung bei Überschreiten der Maximalgröße

Wie bereits erwähnt, stellt der Mailrouter per Vorgabe Mails auch bei überschrittener Maximalgröße weiter zu. Wollen Sie das nicht, gehen Sie wie folgt vor:

1. Öffnen Sie das zuständige Konfigurationsdokument im Bearbeitungsmodus.
2. Navigieren Sie zum Register **Router/SMTP > Beschränkungen und Steuerungen... > Zustellung**.
3. Wählen Sie im Feld **Wenn Größenbeschränkung überschritten wurde** entweder die Option »Zustellfehlerbericht an Absender« oder »Zurückhalten und erneut versuchen«.

Im ersten Fall wird die Mail mit dem Hinweis an den Absender zurückgeschickt, dass sie nicht zugestellt werden konnte, weil die Empfängerdatenbank die erlaubte Größe überschritten hat.

Im zweiten Fall wird die Mail in der Mailbox solange mit dem Status »pending« (Zustellung ausstehend), zurückgehalten, bis eine Zustellung möglich ist. Dieses Verhalten kann auf eine

bestimmte Anzahl von Mails oder die Gesamtgröße aller zurückgehaltenen Mails limitiert werden. Ist das Limit erreicht, werden Zustellungsfehlerberichte an den Absender geschickt.

8.11.4. Größenbeschränkungen ändern/aufheben

Sie können Größenbeschränkungen jederzeit ändern oder auch ganz aufheben.

Gehen Sie dazu wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Dateien** und wählen Sie die Datenbank(en) aus, für die Sie die Änderung vornehmen wollen.
2. Wählen Sie in den Werkzeugen den Befehl **Datenbanken > Größenbeschränkungen...** oder klicken Sie mit der rechten Maustaste auf die Markierung und wählen Sie im Kontextmenü den Befehl **Größenbeschränkungen...**
3. Der Dialog **Größenbeschränkung festlegen** wird angezeigt:

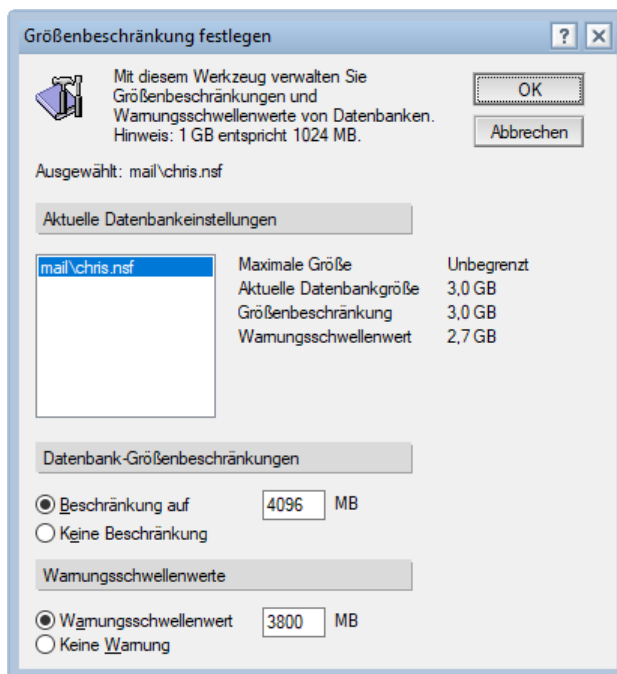


Abbildung 8.42 Der Dialog Größenbeschränkung festlegen

4. Geben Sie eine neue Beschränkung und optional einen Warnschwellenwert in MB ein (z. B. 4096 MB für genau 4 GB) oder wählen Sie die Option »Keine Beschränkung«, um die Beschränkung aufzuheben.
5. Klicken Sie auf **OK**.

Beachten Sie, dass Größenbeschränkungen nicht repliziert werden!

8.12. Abwesenheitsnachrichten einrichten

8.12.1. Übersicht

Abwesenheitsnachrichten (Out of Office, kurz OOO) informieren den Absender, dass ein Benutzer gerade nicht verfügbar, z. B. auf Urlaub ist. Abwesenheitsnachrichten können vom Benutzer selbst über den Notes-Client, via Webmail (iNotes-Web-Access) und sogar via Mobile Verse vom Handy aus aktiviert werden.

Technisch gesehen können Abwesenheitsnachrichten auf zwei Arten generiert werden:

1. Durch einen LotusScript-Agenten, der periodisch oder auch über das Ereignis »Nach Eingang neuer Mail« gestartet wird.
2. Durch den Mail-Router bei der Zustellung (als **Service** bezeichnet).

Die Vor- und Nachteile der beiden Methoden entnehmen Sie bitte Tabelle 8.4:

Service	Agent
Benachrichtigungen werden sofort ausgeschickt.	Benachrichtigungen werden periodisch alle 6 Stunden ausgeschickt (ohne großen Aufwand auf das Ereignis »Nach Eingang neuer Mail« umstellbar).
Unterstützt minimale Abwesenheit von einer Stunde.	Mindestabwesenheit von einem Tag (kann umprogrammiert werden)
Wird beim Erreichen des eingestellten Rückkehrdatums automatisch deaktiviert.	Muss vom Anwender deaktiviert werden.
Absender von automatisch generierten Nachrichten ist die Person aus dem Mailprofil.	Absender von automatisch generierten Nachrichten ist der Signierer des Agenten! Daher muss der Benutzer den Abwesenheitsagenten selbst aktivieren. Verfügt der Benutzer in seiner Maildatenbank über Entwicklerrechte, speichert und signiert er den Agenten direkt. Verfügt der Benutzer nur über Editorrechte, wird der Administrationsprozess damit beauftragt, den Agenten zu aktivieren (dieser trägt dann den Benutzer dann in das Feld Ausführen im Namen von ein).
Abwesenheit kann für den Benutzer auch von jemand anderem aktiviert werden.	Abwesenheit kann nur mit Tricks (via Designer-Client und dem Feld Ausführen im Namen von) von jemand anderen aktiviert werden.
Die Abwesenheitsverarbeitung erfolgt, nachdem die Mailregeln abgearbeitet wurden und nachdem ein Agent vom Typ »Vor Eingang neuer Mail« das Mail verarbeitet hat, jedoch vor der Verarbeitung des Mails durch einen Agenten vom Typ »Nach Eingang neuer Mail«. Das heißt, es wird keine Abwesenheitsnachricht geschickt, wenn die Mail zuvor durch eine Regel oder einen Agenten ausgeschieden wurde.	Die Abwesenheitsverarbeitung erfolgt, nachdem die Mailregeln abgearbeitet wurden abhängig von den Einstellungen im Agenten nach Zeitplan oder durch ein Ereignis.

Service	Agent
Nur beschränkt anpassbar (der Service greift auf die Felder in der Maske OutOfOfficeProfile zu).	Hochgradig anpassbar – in LotusScript programmiert. Sie können den Agenten etwa so umprogrammieren, dass er nur auf Absender antwortet, die in der Kundendatenbank stehen.
Unterstützt Failover	Unterstützt kein Failover (Im Agent ist Server fix eingestellt)

Tabelle 8.4: Vergleich Abwesenheits-Service und -agent

Zusammenfassend kann gesagt werden, dass der Service nicht nur flexibler, sondern auch weniger wartungsintensiv ist, da die Problematik der Ausführungsrechte wegfällt. Außerdem ist das Ausführen des Service effizienter als das Ausführen vieler Agenten in vielen Maildatenbanken. Ich würde nur dann an Agenten festhalten, wenn eine Umprogrammierung einen Mehrwert liefern.

8.12.2. Den Abwesenheitstyp konfigurieren

Der Service ist bereits seit Version 8 verfügbar, aber vielfach nicht aktiviert, da die Einstellungen im Domino-Verzeichnis bei einem Update nicht geändert werden.

Um den Abwesenheitstyp einzustellen, öffnen Sie das Konfigurationsdokument des Servers und navigieren Sie zum Register **Router/SMTP > Erweitert... > Steuerung**. Wählen Sie im Feld **Abwesenheitstyp** entweder »Service« oder »Agent«. Starten Sie nach der Umstellung den Domino-Server neu, ein Neustart des Routers reicht nicht aus!

8.12.3. Setzen von Rechten für Abwesenheitsagenten

Verwenden Sie Abwesenheitsagenten, müssen Sie auch noch dafür sorgen, dass die Ausführungsrechte am Server richtig konfiguriert sind.

Sind alle Benutzer in ihren Maildatenbanken Manager oder Entwickler, können sie den Agenten selbst signieren. In diesem Fall müssen Sie im Serverdokument, Register **Sicherheit**, rechts oben im Abschnitt **Einschränkungen der Programmierbarkeit** im Feld **Beschränkte LotusScript/Java-Agenten signieren oder ausführen** eingetragen sein.

Verfügen die Benutzer in ihren Maildatenbanken nur über Editorrechte (das ist die Regel) können sie den Agenten nicht selbst signieren. In diesem Fall wird beim Aktivieren eine Anforderung an den Administrationsprozess gestellt, der den Agenten dann für den Benutzer aktiviert (und damit signiert). Damit die Abwesenheitsnachricht trotzdem vom Benutzer kommt und nicht vom Server, wird der Benutzer vom Administrationsprozess im Agenten in das Feld **Ausführen im Namen von** eingetragen. Damit der Administrationsprozess das darf, muss der Server im Serverdokument, Register **Sicherheit**, rechts oben im Abschnitt **Einschränkungen der Programmierbarkeit** im Feld **Agenten signieren, die im Namen anderer ausgeführt werden** eingetragen sein.

Vergessen Sie nicht, den Server nach einer Änderung im Abschnitt **Einschränkungen der Programmierbarkeit** neu zu starten!

Welche Benutzer ihre Abwesenheitsnachrichten aktiviert haben, sehen Sie übrigens entweder im Domino-Administrator am Register **Dateien** oder durch Eingabe folgenden Serverkonsolenbefehls:
`tell router outofoffice`

8.13. Einen Verzeichniskatalog erstellen

Ein **Mobiler Verzeichniskatalog** (Condensed Directory Catalog) dient Notes-Clients zum Nachschlagen von Mailadressen, wenn sie nicht mit einem Domino-Server verbunden, also offline sind. Der Hauptvorteil besteht darin, dass in einer Datei mehrere Serververzeichnisse zusammenfasst werden können. Mobile Verzeichniskataloge enthalten außerdem nur jene Felder, die zur Adressauflösung benötigt werden und sind indiziert. Da sie keine Dokumente, sondern nur einen Index enthalten, brauchen sie wesentlich weniger Speicherplatz als die darin zusammengefassten Verzeichnisse zusammen.

Ein Mobiler Verzeichniskatalog wurde als Offline-Lösung konzipiert und ist serverseitig nicht vorgesehen. Wollen Sie auch auf dem Server mehrere Verzeichnisse zu einer Datei zusammenfassen, ist ein **Extended Directory Catalog** das Mittel der Wahl. Dieser verwendet nicht die Verzeichniskatalog-Schablone `dircat5.ntf`, sondern die Schablone des Domino-Verzeichnisses `pubnames.ntf` und enthält alle Dokumente und Ansichten, womit er auch zur Authentifizierung herangezogen werden kann.

Der Verzeichniskatalog wird von einem eigenen Task, dem **Verzeichniskatalogdienst** oder Directory Cataloger (Dircat), auf Deutsch manchmal auch als Verzeichniskatalogisator bezeichnet, befüllt und aktualisiert.

Der Verzeichniskatalog kann später über die Desktoprichtlinie auf mobile Clients ausgerollt werden, womit sämtliche Kontaktadressen auch im Offline-Modus zur Verfügung stehen. Als Nebeneffekt erfolgen eine schnelle automatische Vervollständigung und ein schneller Aufbau der Vorschlagsliste bei Eingabe einer E-Mail-Adresse, da die Namenssuche lokal erfolgt.

8.13.1. Einen Verzeichniskatalog erstellen

Um einen Verzeichniskatalog zu erstellen, gehen Sie wie folgt vor:

1. Legen Sie zuerst die Datenbank an. Wählen Sie dazu im Menü den Befehl **Datei > Anwendung > Neu...** oder drücken Sie `[Strg]+[N]`.
2. Wählen Sie als Speicherort den gewünschten Server aus.
3. Geben Sie einen beliebigen Titel ein, z. B. »Mailadressen«. Der Datenbanktitel scheint später im Dialog Adressauswahl als zusätzlicher Eintrag auf, weshalb Sie einen sprechenden Namen wählen sollten.
4. Vergeben Sie einen beliebigen Dateinamen, z. B. »dircat.nsf«.
5. Wählen Sie als Schablonenserver ebenfalls den Server und setzen Sie ein Häkchen bei »Weitere Schablonen anzeigen«.
6. Wählen Sie die Schablone »Verzeichniskatalog (11)« (`dircat5.ntf`) aus der Liste.
7. Klicken Sie auf **OK**, um die Datenbank zu erstellen.

8.13.2. Einen Verzeichniskatalog einrichten

Zum Definieren des Suchumfangs muss der Verzeichniskatalog konfiguriert werden. Gehen Sie dazu wie folgt vor:

1. Wechseln Sie im Verzeichniskatalog zur Ansicht **Konfiguration**.

Verzeichniskatalog
Kompaktes Verzeichnis

Speichern und schließen Abbrechen

VERZEICHNISKATALOG-KONFIGURATION

Allgemein | **Erweitert**

Aufzunehmende Verzeichnisse:

Aufzunehmende zusätzliche Felder:

 (Vollständiger Name und Listenname
 standardmäßig aufgenommen)

Sortierung: Eindeutiger Name
 Nachname
 Alternativer vollständiger Name

Soundex verwenden:

Doppelte Benutzernamen entfernen:

Gruppentypen:

Mail-In-Datenbanken aufnehmen

Aggregation auf diesen Server
 beschränken:

Verzeichniskatalogberichte senden an:

Kommentare:

Abbildung 8.43: Konfiguration des Mobilten Verzeichniskatalogs

2. Geben Sie im Feld **Aufzunehmende Verzeichnisse** an, welche Datenbanken indiziert werden sollen.
3. Für den gewünschten Suchumfang kann es nötig sein, weitere Felder zur Liste **Aufzunehmende zusätzliche Felder** hinzuzufügen.
 So werden etwa nur dann Mitglieder von Gruppen in den Verzeichniskatalog übernommen, wenn Sie zusätzlich das Feld »Members« in die Liste aufnehmen.
4. Geben Sie im Feld **Sortierung** an, wie Namen sortiert werden sollen. Ist eher eine Suche nach dem Nachnamen üblich als nach dem Vornamen, wählen Sie die Option »Nachname«.
5. Geben Sie an, ob Soundex-Varianten in den Index mit aufgenommen werden sollen (»Meier« findet auch »Maier«).
6. Wenn dieselben Benutzer in mehreren Verzeichnissen enthalten sind, wählen Sie im Feld **Doppelte Benutzernamen entfernen** die Option »Ja«.
7. Geben Sie an, welche Gruppentypen in den Index aufgenommen werden sollen. Wählen Sie entweder »Keine« oder »Mail und mehrere Zwecke«.
 Haben Sie einen Gruppentyp gewählt, muss das Feld »Members« in die Liste der zusätzlichen Felder aufgenommen werden.
8. Geben Sie an, ob Mail-In-Datenbanken indiziert werden sollen.

9. In einer Umgebung mit mehreren Servern sollte der Directory Cataloger nur auf einem Server aktiv sein, weil sonst Replikationskonflikte entstehen. Hinterlegen Sie entsprechend im Feld **Aggregation auf diesen Server beschränken** den Namen des Servers, auf dem der Directory Cataloger läuft.
10. Klicken Sie auf die Schaltfläche **Speichern und schließen**.

8.13.3. Befüllen des Verzeichniskatalogs

Um den Verzeichniskatalog zu befüllen, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Konfiguration** und wählen Sie die Ansicht **Verzeichnis > Verzeichniskatalogisator > Einstellungen**.
2. Geben Sie im Feld **Dateinamen von Verzeichniskatalogen** den Namen des Verzeichniskatalogs ein.
3. Aktivieren Sie den Zeitplan und geben Sie den gewünschten Zeitraum und das gewünschte Wiederholungsintervall ein.
4. Speichern und schließen Sie das Dokument.



Abbildung 8.44: Einstellungen des Verzeichniskatalogdienstes

5. Um den Verzeichniskatalog zum ersten Mal aufzubauen, kann der Task über den folgenden Befehl auch manuell gestartet werden:
6. `load dircat <Verzeichniskatalog.nsf>`

8.13.4. Verteilen des Verzeichniskatalogs an Notes-Clients

Sie können den Verzeichniskatalog via Desktoprichtlinie ausrollen. Gehen Sie dazu wie folgt vor:

1. Wählen Sie im Notes-Client das Symbol des Verzeichniskatalogs aus oder öffnen Sie den Verzeichniskatalog und gehen Sie im Menü auf **Bearbeiten > Kopieren als > Anwendungslink**.
2. Navigieren Sie dann im Domino-Administrator zum Register **Personen und Gruppen** und wählen Sie die Ansicht **Einstellungen**.
3. Erstellen Sie entweder über die Schaltfläche **Einstellungen hinzufügen... > Desktop** eine neue Desktoprichtlinie oder bearbeiten Sie ein vorhandenes Dokument.

4. Wechseln Sie in der Desktoprichtlinie zum Register **Anwendung** und fügen Sie den Anwendungs-Link aus der Zwischenablage in das Feld **Mobile Verzeichniskataloge** ein.



Abbildung 8.45: Ausrollen des Verzeichniskatalogs via Desktoprichtlinie

Ignorieren Sie den Hinweis: »Diese Einstellung ist ab Domino 8.5.1 veraltet...«

5. Speichern und schließen Sie das Dokument.

Bei der nächsten Anmeldung eines Benutzers wird automatisch eine lokale Replik des Verzeichniskatalogs angelegt.

Damit der lokale Verzeichniskatalog auch befüllt und regelmäßig aktualisiert wird, muss im Notes-Client zusätzlich eine Hintergrundreplikation eingerichtet werden.

9. Datenbanken verwalten

- > 9.1 Übersicht, Seite 243
- > 9.2 Datenbanken organisieren, Seite 244
- > 9.3 Neue Datenbanken erstellen, Seite 245
- > 9.4 Das Dateiformat, Seite 246
- > 9.5 Komprimieren von Datenbanken, Seite 252
- > 9.6 Das Database-Maintenance-Tool, Seite 256
- > 9.7 Datenbanken reparieren, Seite 260
- > 9.8 Ansichten verwalten, Seite 261
- > 9.9 Volltextindizes verwalten, Seite 266
- > 9.10 Die Servertasks Update und UpdAll, Seite 271
- > 9.11 Kompressionsverfahren anwenden, Seite 274
- > 9.12 Domino Attachment and Object Service, Seite 277
- > 9.13 Datenbanken verschieben, Seite 283
- > 9.14 Benutzeraktivitäten überwachen, Seite 287
- > 9.15 Dokumentlöschungen protokollieren, Seite 289
- > 9.16 Der Datenbankkatalog, Seite 290

9.1. Übersicht

In einer Notes-Datenbank wird alles (Daten, Einstellungen, die Zugriffskontrollliste, Gestaltungselemente u. a.) in Form von Dokumenten (sogenannten »Notes«) gespeichert. Jedes Dokument besitzt eine eindeutige ID. Datendokumente (Data Notes) enthalten zusätzlich Felder (Items) mit unterschiedlichen Datentypen (Text, Zahl oder Datum/Zeit). Zum Anzeigen und Ändern von Dateninhalten werden Masken (Forms) verwendet, die frei gestaltet werden können. In sogenannten Ansichten (Views) sowie in Ordnern (Folders) können Listen von Dokumenten aus dem Datenbestand gefiltert und tabellarisch angezeigt werden. Mittels selbst geschriebener Programme (Agenten) können Aktionen ereignis- oder zeitgesteuert ausgeführt werden. Sämtliche Inhalte einer Datenbank inklusive Dateianhänge lassen sich über die integrierte Volltextsuche durchsuchen. Dies gilt nicht nur für lokale Datenbanken auf einem Notes-Client, sondern auch für Datenbanken auf einem Domino-Server. Die Dateierweiterung *.nsf von Notes-Datenbanken steht für »Notes Storage Facility«, die Endung *.ntf der Schablonen für »Notes Template Facility« (manchmal liest man auch »Notes Template File«).

Eine Datenbank hat folgende Identifikationsmerkmale:

- > einen Dateinamen entsprechend dem zugrundeliegenden Dateisystem

- > einen Datenbanktitel (für den Anwender sichtbar)
- > eine Replik-ID, eine 16-stellige Zahl in hexadezimaler Schreibweise, die beim Erstellen der Datenbank zufällig generiert wird
- > einen Schablonennamen, falls es sich bei der Datenbank um eine Schablone oder um eine von einer Schablone abhängigen Anwendung handelt

Unterschiede zu anderen Datenbanksystemen: Notes-Datenbanken sind nicht relational, sondern folgen einem Dokumentmodell. Dokumente können (müssen aber nicht) eine hierarchische Beziehung zueinander haben (Hauptdokument – Antwort – Rückantwort). Relationen im RDBMS-Sinn können in Notes-Datenbanken hingegen nur programmatisch hergestellt werden. Felder können Mehrfachwerte enthalten, was einer Master-Detail-Tabelle in einem RDBMS entspricht.

Notes speichert nicht nur Daten, sondern auch das Design (Masken, Ansichten, Agenten etc.) in derselben Datei. Dort liegen sie ebenfalls in Form von Notes (Dokumenten) vor, die für den Benutzer nicht direkt einsehbar sind. Während das bei RDBMS für das Datenschema und die Ansichten üblich ist, speichert Notes auch Masken (Forms) und Ressourcen (CSS, JPG, Java etc.). Alle Designelemente sind signiert und erlauben so eine feingliedrige Ausführungskontrolle.

Notes-Dokumente sind nicht an Datenbanktabellen gebunden. Somit können Notes-Dokumente beliebige Felder enthalten. Eine Änderung am Masken- oder Ansichtslayout hat keine Auswirkung auf die gespeicherten Daten. Im Webdesign können Anwendungen auch ganz ohne Notes-Frontend entwickelt werden, das heißt in Notes geöffnete Masken zeigen nur HTML-Code etc.

Notes-Ansichten (Views) haben einen Index. (Views in RDBMS sind Abfragedefinitionen ohne Index, die zur Laufzeit ausgeführt werden.) Dies hat den Vorteil des schnellen Zugriffs und den Nachteil des Ressourcen- (Indexer) und Platzverbrauchs. Außerdem besteht die Einschränkung, dass der (bereits fertige) Index zur Laufzeit nicht verändert werden kann, d. h. ein Setzen von Filtern, die im Ansichtdesign nicht schon enthalten sind, ist nur beschränkt möglich.

Eine weitere Besonderheit ist die Unterstützung von Rich-Text als Feldtyp. Hier können formatierter Text, Dateianhänge oder eingebettete Objekte (Bilder, OLE-Objekte) gespeichert werden. Rich-Text-Felder zusammen mit dem Notes-Client erlauben ein besonders benutzerfreundliches »Hochladen« von nahezu beliebigen Daten auch über Ziehen und Ablegen (Drag and Drop).

9.2. Datenbanken organisieren

Sie können Datenbanken direkt im Domino-Datenverzeichnis speichern. Dies ist die Standardvorgehensweise. Sie können Datenbanken aber auch in Unterordnern des Domino-Datenverzeichnisses speichern, etwa um zusammengehörige Datenbanken zu gruppieren. Sie können mithilfe einer **Verzeichnis-ACL** (siehe Kap. 13.7 Verzeichnissicherheit, ab Seite 357) bereits auf Verzeichnisebene Zugriffsrechte zuordnen. Personen, die keinen Zugriff haben, sehen das Verzeichnis nicht.

Sie können einzelne Datenbanken außerhalb des Domino-Datenverzeichnisses speichern und mithilfe von **Datenbankverknüpfungen** (Datenbank-Links) darauf verweisen. Die Datenbank wird optisch so dargestellt, als befände sie sich innerhalb des Domino-Datenverzeichnisses. Datenbankverknüpfungen funktionieren auch beim Zugriff von einem Webbrowser. Zum Erstellen von Datenbankverknüpfungen lesen Sie Kap. 9.13.3 Auslagern von Datenbanken über Datenbank-Links, ab Seite 286.

Sie können ganze Ordner mit Notes-Datenbanken außerhalb des Domino-Datenverzeichnisses erstellen und mithilfe von **Verzeichnisverknüpfungen** (Verzeichnis-Links) darauf verweisen. Das Verzeichnis wird dann optisch wie ein Unterordner im Domino-Datenverzeichnis dargestellt. Sie können außerdem den Zugriff auf ausgelagerte Verzeichnisse beschränken. Zum Erstellen von Verzeichnisverknüpfungen lesen Sie Kap. 9.13.4 Auslagern von Verzeichnissen über Ordner-Links, ab Seite 286.

9.3. Neue Datenbanken erstellen

Sie können Datenbanken (Anwendungen) basierend auf einer der mitgelieferten Schablonen erstellen oder auch eine vorhandene Anwendung kopieren. Und letztendlich können Sie eine neue Anwendung auch selbst programmieren oder einen externen Dienstleister damit beauftragen.

9.3.1. Eine Anwendung basierend auf einer Schablone erstellen

Um eine Anwendung basierend auf einer Schablone zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Menü **Datei > Anwendung > Neu...** oder drücken Sie [Strg]+[N]. Der Dialog Neue Anwendung wird angezeigt:

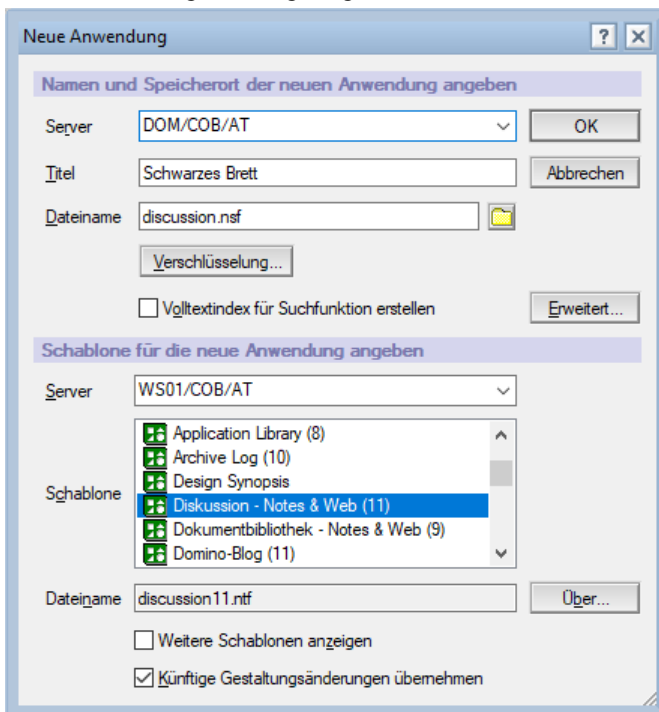


Abbildung 9.1: Dialog Neue Anwendung

2. Wählen Sie den Server, auf dem die neue Anwendung erstellt werden soll.
3. Vergeben Sie einen Anwendungstitel und einen Dateinamen.
Soll die Anwendung auch im Webbrowser genutzt werden, vergeben Sie einen URL-kompatiblen Namen (also ohne Umlaute und Leerzeichen).
4. Wählen Sie den Schablonenserver oder lokal, falls die Schablone vom Notes-Client kommt.

5. Wählen Sie die gewünschte Schablone aus der Liste.

Schablonen werden nach dem Titel sortiert angezeigt, was die Suche erschwert, weil sich die Titel je nach eingespieltem Sprachpaket voneinander unterscheiden.

Standardmäßig sehen Sie nur Schablonen, die einen Endanwenderbezug aufweisen. Wollen Sie alle Schablonen sehen, setzen Sie ein Häkchen bei **Weitere Schablonen anzeigen**.

6. Lassen Sie das Feld **Künftige Gestaltungsänderungen übernehmen** angehakt, wenn die neue Anwendung auch in Zukunft Design-Updates von der Schablone erhalten soll.

9.3.2. Eine Anwendung basierend auf einer Kopie erstellen

Bedenken Sie, dass eine auf Betriebssystemebene kopierte Datei immer dieselbe Replik-ID aufweist wie das Original. Daher sollten Sie zum Erstellen einer unabhängigen Kopie immer den Befehl **Datei > Anwendung > Neue Kopie...** verwenden:

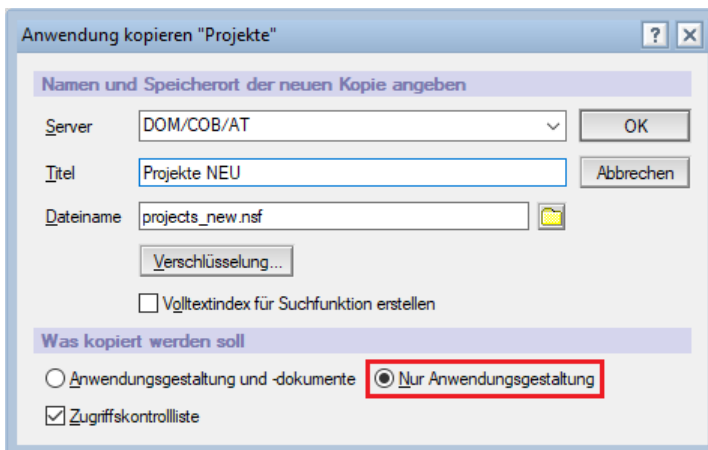


Abbildung 9.2: Dialog Anwendung kopieren

Soll nur die Gestaltung übernommen werden, nicht aber die enthaltenen Dokumente, aktivieren Sie im Bereich **Was kopiert werden soll** die Option »Nur Anwendungsgestaltung«:

9.4. Das Dateiformat

Das **Dateiformat** (ODS – On Disk Structure) bestimmt, auf welche Art und Weise der Domino-Server (oder der Notes-Client) Informationen auf den physischen Datenträger schreibt. Es hat keinen Einfluss auf die Interaktion zwischen Server und Client und wird auch nicht repliziert. Und das ODS hat auch nichts mit dem Design einer Datenbank zu tun.

Eine Übersicht über die Dateiformate der Domino-Versionen finden Sie in Tabelle 9.1:

Version	Format
Version 4	ODS 20
Version 5	ODS 41
Version 6	ODS 43
Version 8	ODS 48
Version 8.5	ODS 51

Version	Format
Version 9.0.1	ODS 52
Version 10	ODS 53

Tabelle 9.1: Vergleich Domino-Version und ODS

Welches Dateiformat eine Datenbank verwendet, können Sie im Admin-Client im Register **Dateien** in der Spalte **Dateiformat** oder auch in den Datenbankeigenschaften am **Inforegister** einsehen:

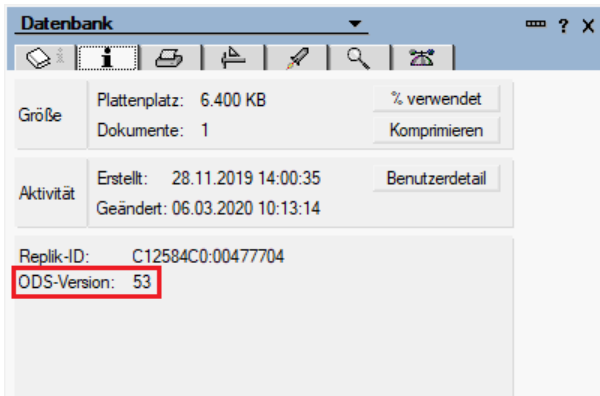


Abbildung 9.3: Datenbankeigenschaften – ODS-Version

Sie sollten immer das neueste ODS verwenden, welches neben neuen Konfigurationsmöglichkeiten auch eine bessere Performance und Wartbarkeit bietet. (Der Performanceunterschied zwischen ODS 43 und ODS 52 beträgt zwischen 20 und 40 %!)

Ein neu aufgesetzter Domino-Server der Versionen 10 oder 11 verwendet ODS 52, haben Sie jedoch eine ältere Domino-Version aktualisiert, können auch Datenbanken mit einem älteren ODS in Verwendung sein. So verwendet etwa Domino 9.0.1 aus Gründen der Rückwärtskompatibilität ODS 43.

9.4.1. Warum Sie ODS 53 aktivieren sollten

Datenbanken in ODS 53 können 256 GB groß sein (bei älterem ODS sind es nur 64 GB). Zusätzlich wurde die maximale Ordnergröße erhöht, d. h. es sind mehr Ordner möglich als vorher. Nach Aktualisierung auf ODS 53 gibt es Folgendes zu beachten:

- > Ein Notes 10-Client oder höher kann auf eine Datenbank auf einem Domino 10 oder 11-Server zugreifen, unabhängig wie groß sie ist. Ältere Notes-Clients können die Datenbank auf einem Domino 10 oder 11-Server jedoch nur öffnen, so lange sich Datenbank- und Ordnergrößen innerhalb ihrer Limits befinden.
- > Bis zu 64 GB der Datenbank können auf alle Domino-Server-Versionen oder Notes-Clients repliziert werden. Um mehr als 64 GB Daten zu replizieren, muss sich die Zielreplik jedoch zumindest auf einem Domino 10 Server oder Notes 10-Client befinden und ODS 53 aufweisen.
- > Ordner in der Datenbank innerhalb der Größenbeschränkung der älteren Version können in jede Zielreplik auf jeder Serverversion repliziert werden. Übertrifft die Ordnergröße jedoch die Beschränkungen der älteren Version, können Sie nur noch mit Repliken auf einem Domino 10-Server (oder höher) oder Notes 10-Client (oder höher) im Format ODS 53 replizieren.

9.4.2. Das Dateiformat am Server aktualisieren

Die Umwandlung in das neueste ODS erfolgt am Server in zwei Schritten:

1. den Server instruieren, dass er neue Datenbanken im neuesten Format erstellen soll
2. existierende Datenbanken komprimieren

9.4.2.1. Die notes.ini-Variable setzen

Damit der Server für neue Datenbanken ODS 53 verwendet, muss in der Datei notes.ini der folgende Eintrag gemacht werden:

```
Create_R10_Databases=1
```

Praxistipp: Verwenden Sie zum Setzen der Variable das Konfigurationsdokument, Register **NOTES.INI-Einstellungen**. Details dazu finden Sie im Kap. 5.2.2 Über das Konfigurationsdokument in die notes.ini schreiben, ab Seite 92.

Starten Sie nach dem Setzen der Variable den Server durch. Nach dem Hochfahren werden neue Datenbanken mit ODS 53 erstellt.

9.4.2.2. Datenbanken online konvertieren

Bereits existierende Datenbanken müssen nachträglich konvertiert werden. Dafür stehen zwei Tasks zur Verfügung:

1. Compact

Mit dem folgenden Befehl konvertieren Sie eine Datenbank in das neueste ODS:

```
load compact -C -# 4 -* -ODS
```

Schalter	Erklärung
-C	Bewirkt, dass die Datenbank »copy-style« (mittels Erstellung einer Kopie) komprimiert wird. Nur bei dieser Methode kann das ODS ausgetauscht werden.
-# 4	Bewirkt, dass vier Threads zum Komprimieren verwendet werden. Dieser Schalter ist nicht unbedingt nötig, beschleunigt aber die Komprimierung, wenn mehrere Prozessoren (bzw. Kerne) zur Verfügung stehen. Es können maximal 20 Threads verwendet werden.
-*	Bewirkt, dass auch Datenbanken mit einer anderen Endung als *.nsf komprimiert werden (also auch Schablonen und Mailboxen)
-ODS	Bewirkt, dass nur Datenbanken komprimiert werden, die noch nicht über das neueste ODS verfügen

Tabelle 9.2: Parameter für Compact zum Umwandeln in das neueste ODS

Datenbanken mit einem hart codierten älteren ODS können zuvor ein Upgrade brauchen:

```
load compact <Datenbank> -upgrade
```

Details zum Programm Compact finden Sie in Kap. 9.5.3 Die verschiedenen Komprimiermethoden, ab Seite 253.

2. DBMT

Das Database Maintenance Tool übernimmt mehrere Aufgaben, eine davon ist das Komprimieren von Datenbanken:

```
load dbmt -compactThreads 4 -ods
```

```
load dbmt -ct 4 -ods
```

Mit den obigen Befehlen weisen Sie DBMT an, alle Datenbanken, die noch nicht über das neueste ODS verfügen, mit 4 Threads gleichzeitig zu komprimieren.

Details zum Programm DBMT finden Sie in Kap. 9.6 Das Database-Maintenance-Tool, ab Seite 256.

Beide Programme, sowohl Compact mit dem Schalter -C als auch DBMT nehmen die Datenbanken beim Komprimieren offline, was nicht geht, so lange sie geöffnet sind. Einige Systemdatenbanken (names.nsf, log.nsf, busytime.nsf, events4.nsf, ddm.nsf und andere) sind immer geöffnet, während der Domino-Server läuft. Und selbst wenn Benutzer ihre Maildatenbanken schon vor Stunden geschlossen haben, können sich diese noch im Datenbankcache befinden. Daher empfehle ich folgende Strategie:

1. Komprimieren Sie so viele Datenbanken wie möglich online, um die Downtime möglichst gering zu halten.
2. Fahren Sie dann nachts oder am Wochenende den Domino-Server herunter und komprimieren Sie die fehlenden Datenbanken offline.

Tipp: Leeren Sie vor der Online-Komprimierung zuerst den Cache, indem Sie auf der Serverkonsole den folgenden Befehl eingeben:

```
dbcache flush
```

Starten Sie erst dann die Komprimierung mit Compact oder DBMT:

```
load compact -C -# 4 -* -ods bzw.: load dbmt -ct 4 -ods
```

Für geöffnete Datenbanken werden Fehlermeldungen angezeigt. Das können neben offenen Systemdatenbanken auch Maildatenbanken sein – bereits die Zustellung einer einzigen Mail sorgt dafür, dass die Datenbank wieder in den Cache aufgenommen wird.

```
* 06.03.2020 18:39:04 Compacting busytime.nsf (Local free time info), -C -*
✔ 06.03.2020 18:39:04 Error compacting busytime.nsf, -C -*: Database is currently in use by you or another user
```

Abbildung 9.4: Fehler beim Komprimieren – Datenbank bereits in Verwendung

Bei Bedarf können Sie auch mehrere Durchgänge starten – durch den Schalter -ODS werden ja nur jene Datenbanken komprimiert, die noch nicht über das neueste ODS 53 verfügen. Um den Komprimiervorgang in Portionen aufzuteilen, die sich in einer Nacht ausgehen, arbeiten Sie am besten mit Indirect-Dateien. Dabei handelt es sich um Textdateien mit der Endung *.ind, in der die zu komprimierenden Datenbankpfade untereinander aufgelistet sind. Eine Indirect-Datei erzeugen Sie halbwegs komfortabel im Domino-Administrator, indem Sie im Register Dateien die gewünschten Datenbanken markieren und dann in die Zwischenablage kopieren. Im Umweg über eine Tabellenkalkulation (z. B. Microsoft Excel) lässt sich die Liste der Pfade dann leicht extrahieren. Versehen Sie die Textdatei mit der Endung *.ind und legen Sie diese im Datenverzeichnis ab. Hier ein Beispiel:

```
load compact -C maildateien.ind
```

Den Erfolg sehen Sie im Admin-Client im Register **Dateien**, in der Spalte Dateiformat; hier können Sie auch nach der ODS-Version sortieren:

Titel	Dateiname	Physischer Pfad	Dateiformat
Monitoring Configuration	events4.nsf	D:\Domino\events4.nsf	R9 (52:0)
Domino-Domänenmonitor (11)	ddm.nsf	D:\Domino\ddm.nsf	R9 (52:0)
COB's Directory	names.nsf	D:\Domino\names.nsf	R9 (52:0)
WS01's Log	log.nsf	D:\Domino\log.nsf	R9 (52:0)
Local free time info	busytime.nsf	D:\Domino\busytime.nsf	R9 (52:0)
Java AgentRunner	agentrunner.nsf	D:\Domino\AgentRunner.nsf	R10 (53:0)
Homepage (11.0)	homepage.nsf	D:\Domino\homepage.nsf	R10 (53:0)
Reports for WS01/COB/AT	reports.nsf	D:\Domino\reports.nsf	R10 (53:0)
Administration Requests	admin4.nsf	D:\Domino\admin4.nsf	R10 (53:0)
Sample Web Agent - Reset User	pwdresetsample.nsf	D:\Domino\PwdResetSample.nsf	R10 (53:0)
Directory Assistance	da.nsf	D:\Domino\da.nsf	R10 (53:0)
cppfbws	cppfbws.ntf	D:\Domino\cppfbws.ntf	R10 (53:0)
CPP FreeBusy WebService	cppfbws.nsf	D:\Domino\cppfbws.nsf	R10 (53:0)
Server Certificate Admin	certsrv.nsf	D:\Domino\certsrv.nsf	R10 (53:0)
DPI (Domino Portal Integration)	dpicfg.nsf	D:\Domino\dpicfg.nsf	R10 (53:0)

Abbildung 9.5: Domino-Administrator, Register Dateien – Dateiformat

9.4.2.3. Datenbanken offline konvertieren

Fahren Sie nun den Server herunter und öffnen Sie eine Eingabeaufforderung (im Startmenü »cmd« eintippen). Führen Sie diese unbedingt als Administrator aus. Navigieren Sie zum Domino-Programmverzeichnis und geben Sie den folgenden Befehl ein:

```
C:\Program Files\HCL\Domino>ncompact.exe -C -* -ODS
```

Am Ende werden Sie informiert, wie viele Datenbanken tatsächlich komprimiert wurden.

Um zur letzten ODS-Version zurückzukehren (in diesem Fall ODS 52), verwenden Sie den Schalter -R:

```
load compact <Datenbank> -r
```

Sollten Sie das alte ODS 43 aus irgendeinem Grund weiterverwenden müssen, setzen Sie die folgende INI-Variablen:

```
CREATE_R6_DATABASES=1
```

9.4.3. Das Dateiformat am Client ändern

Um den Client anzuweisen, neue Datenbanken in ODS 53 zu erstellen, setzen Sie dieselbe notes.ini-Variablen wie am Server:

```
CREATE_R10_DATABASES=1
```

Durch Setzen der folgenden Variablen weisen Sie den Client zusätzlich an, alle lokalen Datenbanken beim nächsten Start ins neueste ODS umzuwandeln:

```
NSF_UpdateODS=1
```

Sie können die beiden Variablen auch via Desktopeinstellungen, Register **Benutzerdefinierte Einstellungen** > **Notes.ini** ausrollen, aber es geht noch einfacher:

Wählen Sie in den Desktopeinstellungen das Register **Mail** und dann den Abschnitt **Client-Einstellungen**. Aktivieren Sie dort die Einstellung **Alle lokalen NSF-Datenbanken auf die neueste ODS-Version aktualisieren**:

Client-Einstellungen		Wie diese Einstellung angewendet wird:
Dokumenteinstellungen automatisch abrufen:	<input type="checkbox"/> Deaktivieren ▾	<input checked="" type="checkbox"/> Wert nicht festlegen
Server kann neue Mail abfragen und, sofern solche vorhanden ist, eine Replizierung auslösen:	<input type="checkbox"/> Deaktivieren ▾	<input checked="" type="checkbox"/> Wert nicht festlegen
Automatisches Failover, wenn ein Server ausfällt:	<input type="checkbox"/> Deaktivieren ▾	<input checked="" type="checkbox"/> Wert nicht festlegen
Alle lokalen NSF-Datenbanken auf die neueste ODS-Version aktualisieren:	<input checked="" type="checkbox"/> Aktivieren ▾	<input type="checkbox"/> Wert nicht festlegen

Abbildung 9.6: Desktopeinstellungen, Register Mail: Abschnitt Client-Einstellungen

Achten Sie darauf, auch das Häkchen bei **Wert nicht festlegen** zu entfernen!

9.4.4. Das Dateiformat mit der Dateiendung steuern

Sie können das Dateiformat auch über die Dateiendung steuern. Erstellen Sie eine Kopie (**Datei > Anwendung > Neue Kopie...**) oder eine neue Replik (**Datei > Replizierung > Neue Replik...**). Geben Sie der neuen Datei die Endung *.ns10, wird diese automatisch mit ODS 53 erstellt:

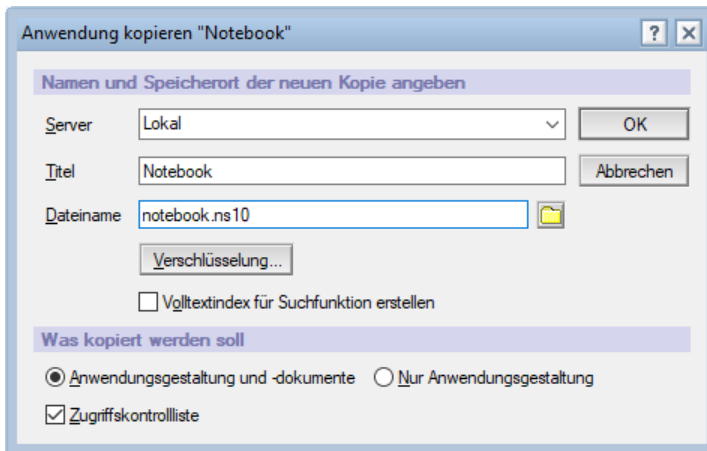


Abbildung 9.7: Dialog Anwendung Kopieren

Analog geht das auch mit anderen Dateieendungen:

Endung	Format
*.ns6	ODS 43
*.ns8	ODS 48
*.ns9	ODS 52

Tabelle 9.3: Dateieendungen und ODS

9.5. Komprimieren von Datenbanken

Durch Löschen von Dokumenten oder Anhängen entstehen in einer Datenbank laufend Lücken. Diese werden auf Deutsch etwas holprig als ungenutzter Speicherplatz, auf Englisch als »White Space« bezeichnet. Diese Lücken dürfen nicht mit der Fragmentierung im Dateisystem verwechselt werden, bei der die Datenbank in verschiedenen, weit voneinander entfernten Datenblöcken auf dem Datenträger gespeichert wird. Gegen die Fragmentierung im Dateisystem kann mit Bordmitteln wenig unternommen werden.

Ein bestimmter Prozentsatz von White Space wirkt sich günstig auf die Performance aus, zumindest wenn die Lücken groß genug sind, um neue Dokumente darin zu speichern, weil dann die Dateigröße nicht erweitert werden muss. Daher sollten Sie Datenbanken erst unter einer Verwendung von 90 % komprimieren.

9.5.1. Den belegten Platz eruieren

Um den belegten Platz innerhalb einer Datenbank zu ermitteln, öffnen Sie die Eigenschaften der Datenbank und wählen das Register **Info**. Klicken Sie dann auf die Schaltfläche **% verwendet**.

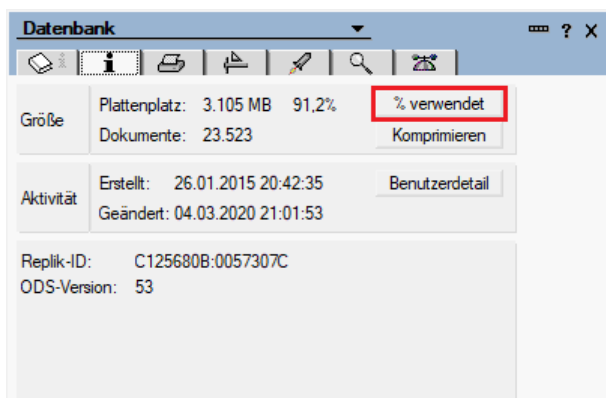


Abbildung 9.8: Das Register **Info** des Eigenschaftendialogs

9.5.2. Eine Komprimierung anfordern

Sie können die Datenbankkomprimierung an verschiedenen Stellen anfordern: In den Datenbankeigenschaften, über Serverkonsolenbefehle und im Domino-Administrator.

9.5.2.1. Über die Datenbankeigenschaften

Klicken Sie in den Datenbankeigenschaften im Register **Info** auf die Schaltfläche **Komprimieren**. Dazu benötigen Sie mindestens Entwicklerrechte. Lokale Datenbanken werden sofort komprimiert, am Server kann die Erledigung Ihrer Anfrage jedoch eine Weile dauern.

9.5.2.2. Über die Serverkonsole

Hier stehen zwei verschiedene Server-Tasks zur Verfügung, **Compact** (siehe Seite 253) und **DBMT** (siehe Seite 256):

```
load compact <Pfad> oder <Indirect-Datei> [Schalter]
```

```
load dbmt <Pfad> oder <Indirect-Datei> [Schalter]
```

9.5.2.3. Im Domino-Administrator, Register Dateien

Wählen Sie zuerst die zu komprimierende Datenbank aus und dann im Kontextmenü oder in den **Werkzeugen > Datenbank** den Befehl **Komprimieren...** Im angezeigten Dialog können verschiedene Methoden ausgewählt werden:

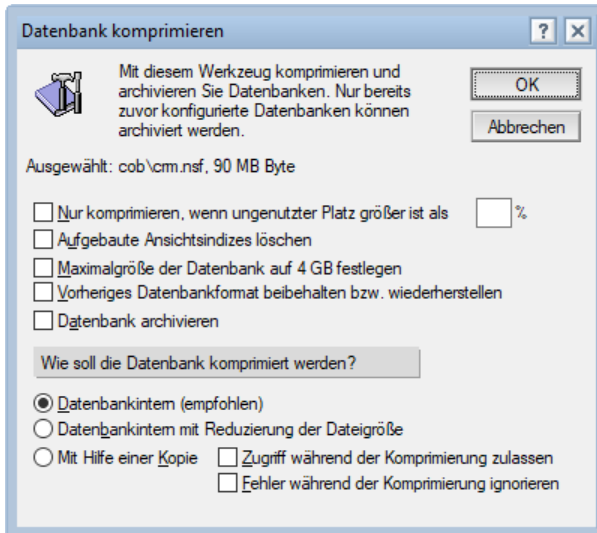


Abbildung 9.9: Dialog Datenbank komprimieren im Domino-Administrator

Im Admin-Client, Register Dateien, zeigt die Spalte **Zuletzt komprimiert** Datum und Uhrzeit der letzten Komprimierung an.

9.5.3. Die verschiedenen Komprimiermethoden

DBMD komprimiert immer »copy-style«, der Compactor kennt drei unterschiedliche Komprimiermethoden:

- > datenbankintern
- > mithilfe einer Kopie
- > mithilfe einer Replik

9.5.3.1. Datenbankinterne Komprimierung

Bei dieser Methode findet eine interne Reorganisation statt, das heißt, der White Space wird so lange hin- und hergeschaufelt, bis er in einem Stück am Dateiende steht. Mit dem Schalter -B wird dieser Bereich am Ende abgeschnitten und es kommt zu einer Größenreduktion, mit dem Schalter -b nicht. Bei der datenbankinternen Komprimierung muss die Datenbank nicht offline genommen werden.

9.5.3.2. Komprimierung mithilfe einer Kopie

Die Komprimierung mithilfe einer Kopie (»copy-style«) stellt die effektivste Methode dar. Dabei muss die Datenbank jedoch offline genommen werden, was nicht möglich ist, so lange Anwender (oder Servertasks) darauf zugreifen. Bei Maildatenbanken bedeutet bereits die Zustellung einer einzigen Mail, dass diese in den Cache gestellt wird, wodurch sie nicht offline genommen werden kann. Die Strategien, mit denen Sie Ihren Erfolg bei Online-Komprimierungen deutlich erhöhen, habe ich

bereits in Kap. 9.4.2.2 Datenbanken online konvertieren, auf Seite 248 dargelegt. Sie können zusätzlich noch Zeit sparen, indem Sie nur Datenbanken komprimieren, bei denen es etwas »zu holen« gibt, die also zumindest 10 % oder mehr ungenutzten Bereich enthalten. Verwenden Sie dazu den Schalter -S <%>:



Abbildung 9.10: Programmdokument – Einstellungen für das Programm Compact (Erklärung im Text)

Compact komprimiert in obigem Beispiel von Montag bis Freitag ab 21:00 Maildatenbanken durch Erstellen einer Kopie nur dann, wenn sie mindestens 15 % White Space enthalten.

Beachten Sie, dass zum Komprimieren kurzfristig doppelt so viel Platz benötigt wird, wie die Datenbank ursprünglich belegt hat.

Tip: Der Befehl `show schedule` zeigt auf der Serverkonsole alle zeitplangesteuerten Ereignisse an, inklusive der Ausführung von Programmdokumenten.

Übersicht über die Parameter für die verschiedenen Komprimiermethoden:

Parameter	Beschreibung
-C	Komprimieren durch Erstellen einer Kopie (»copy-style«)
-D	Wie -C, es werden aber auch noch die Ansichtsindizes neu erstellt
-B	Interne Reorganisation mit Größenreduktion
-b	Interne Reorganisation ohne Größenreduktion

Tabelle 9.4: Wichtige Parameter von Compact zum Komprimieren

Wenn es schnell gehen soll, verwenden Sie die folgenden Parameter:

Parameter	Erklärung
-S 10	Komprimiert nur Datenbanken mit mindestens 10 % »White Space« (Beachten Sie das Leerzeichen zwischen S und der Zahl!)
-w	Lässt die Systemdatenbanken (log.nsf, ddm.nsf) aus
-# 4	Startet mit mehreren Threads (max. 8) (Achten Sie auf das Leerzeichen zwischen der # und der Zahl!)
-W 7	Komprimiert nur Datenbanken, die seit 7 Tagen nicht komprimiert wurden
-X 10	Begrenzt die Komprimierung auf 10 Minuten pro Datenbank
Dateien.ind	Komprimiert nur die in der IND-Datei angegebenen Datenbanken

Tabelle 9.5: Parameter von Compact für ein Beschleunigen der Komprimierung

9.5.3.3. Komprimierung mithilfe einer Replik

Die Komprimierung mithilfe einer Replik besitzt folgende Eigenschaften:

- > Zugriff ist während des Komprimierens (des Replizierens) möglich
- > Optimieren des ID-Tables (Liste der vergebenen Unique-IDs)
- > Ersetzt nach dem Erstellen der Replik das Original – wenn nicht möglich, Abbruch.
- > Zusatzschalter -REN WAIT n wartet n Minuten auf Umbenennung
- > Zusatzschalter -RESTART ersetzt die Datenbank(en) erst nach einem Serverneustart
- > Zusatzschalter -IDS FULL n – nur ausführen, wenn ID Table zumindest n % voll ist

```
load compact mail\user.nsf -REPLICA
```

Oder:

```
load compact names.nsf -REPLICA -RESTART
```

Damit können erstmalig auch Systemdatenbanken regelmäßig komprimiert werden, z. B. via Programmdokument:



Abbildung 9.11: Programmdokument – Einstellungen für das Programm Compact (Erklärung im Text)

Tipp: Geben Sie eine Indirect-Datei an, um mehrere Systemdatenbanken gleichzeitig zu komprimieren, z. B.:

```
load compact systemdb.ind -REPLICA -RESTART
```

Unterschiede zwischen Komprimieren mithilfe einer Kopie und mithilfe einer Replik:

Komprimieren mithilfe einer Kopie	Komprimieren mithilfe einer Replik
temporäre Datei mit Endung *.tmp	temporäre Datei mit Endung *.repl
Notes ID-Table bleibt fragmentiert	Notes ID-Table wird neu erstellt (Lösung, wenn stark fragmentiert)
Zugriff nicht möglich	Zugriff möglich – außer in der Umbenennungsphase
Komprimierung löst nicht Fragmentierung auf dem Datenträger	nach Komprimierung ev. kleinere Fragmentierung

Tabelle 9.6: Vergleich Komprimieren mithilfe einer Kopie und mithilfe einer Replikation

9.5.4. Beschränkungen bei Feldgrößen

Leider machen alte Beschränkungen auch noch in Version 12 Administratoren und Entwicklern das Leben schwer. Ein Fehler, auf den fast jeder früher oder später einmal trifft ist folgender:

»Feld ist zu groß (32K), oder die Spalten- oder Auswahlformeln der Ansicht sind zu groß«

»Field is too large (32K) or View's column & selection formulas are too large«

In Notes dürfen Text-, Zahlen- und Zeit-Felder 64 K groß sein – aber nur, wenn sie nicht in Ansichten angezeigt werden. Felder, die in Ansichtsspalten angezeigt werden (sogen. »Summary-Fields«) dürfen bis ODS 52 nur 32 K groß sein – theoretisch, denn davon ist noch ein Verwaltungsoverhead abzuziehen. Normalerweise sind auch nur 32 K kein Problem, außer der Entwickler verwendet exzessiv die Eigenschaft »Feld enthält Mehrfachwerte«, dann kann das Limit schnell überschritten werden. .

Leider gibt es auch noch ein zweites Limit: Die Gesamtsumme alle Summary-Felder in einem Dokument darf nicht größer als 64 K sein. Der Fehler kann also schon auftreten, wenn mehrere Summary-Felder 15 K groß sind. Solche Dokumente können nicht mehr kopiert und nicht mehr gespeichert werden. Und schlimmer noch, wird eines der Summary-Felder in einer Ansichtsspalte verwendet, wird das Dokument in der Ansicht nicht mehr angezeigt!

Ab Domino und Notes Version 9.0.1 FP8 gibt es eine Erleichterung: Die 32 K-Grenze pro Feld gilt zwar weiterhin, aber die 64 K-Beschränkung für die Summe aller Summary-Felder pro Dokument kann auf 16 MB erhöht werden. Geben Sie dazu auf der Domino-Konsole einen der folgenden Befehle ein:

```
load compact <datenbank.nsf> -LargeSummary on
```

```
load compact <datenbank.nsf> -ls on
```

Mit der Einführung von ODS 53 unter Notes und Domino 10 wurde die erlaubte Größe eines einzelnen Summary-Fields auf 64 K erhöht.

9.6. Das Database-Maintenance-Tool

DBMT fasst die Fähigkeiten der Tasks UpdAll, Compact und Fixup in einem Programm zusammen. Es wurde vor allem für Maildatenbanken konzipiert, kann aber auch auf kundenspezifische Datenbanken angewendet werden. DBMT komprimiert standardmäßig keine Systemdatenbanken.

DBMT erledigt die folgenden Aufgaben:

- > führt Komprimierungen mithilfe einer Kopie aus
- > entfernt Löschinfos
- > entfernt Mails aus dem Papierkorb (Soft Deletion), wenn das Ablaufdatum erreicht wurde
- > aktualisiert Ansichten
- > reorganisiert Ordner
- > aktualisiert Volltextindizes
- > aktualisiert die Liste der ungelesenen Mails
- > sorgt dafür, dass kritische Ansichten für ein funktionierendes Failover vorhanden sind

DBMT erlaubt die Konfiguration von täglichen und wöchentlichen Operationen.

DBMT kann mit mehreren Threads ausgerufen werden, um die Operationen zu beschleunigen.

DBMT kann frei definierbare Wartungsfenster (Angabe von Anfang und Ende) nutzen. Ist die Zeit abgelaufen, stoppt die Komprimierung, setzt im nächsten Wartungsfenster aber bei derselben Datenbank fort.

In einer Cluster-Umgebung verwendet DBMT das Cluster-Directory (clbdir.nsf), um festzustellen, auf welchen Servern sich Repliken befinden, womit verhindert wird, dass alle Repliken zur selben Zeit komprimiert werden.

Über die Datei `dbmt_compact_filter.ind` können Datenbanken von der Komprimierung ausgeschlossen werden. (Diese Datei wird von DBMT selbst erstellt, wenn Datenbanken nicht komprimiert werden können, z. B. ODS 20 haben.)

Auf Datenbanken, die von DBMT gewartet werden, sollten Sie kein UpdAll mehr anwenden. Deaktivieren Sie daher den automatischen Start von UpdAll über die Variable `ServerTasksAt2` in der Datei `notes.ini`.

DBMT kennt die folgenden Parameter:

Parameter	Abk.	Beschreibung
<code>-blacklist</code>	<code>-bl</code>	Ermöglicht die Angabe einer IND-Datei mit Datenbanken, die nicht komprimiert werden sollen
<code>-compactThreads <n></code>	<code>-ct</code>	Anzahl Threads <n>, die für die Komprimierung verwendet werden. <n> kann Werte zwischen 1 und 100 einnehmen. Die Vorgabe ist 1. Ist 0 angegeben, wird keine Komprimierung ausgeführt.
<code>-updallThreads <n></code>	<code>-ut</code>	Anzahl Threads <n>, die für die Ansichtsaktualisierung verwendet werden. <n> kann Werte zwischen 1 und 100 einnehmen. Die Vorgabe ist 1 und 0 ist nicht zulässig.
<code>-ftiThreads <n></code>	<code>-ft</code>	Anzahl Threads <n>, die für die Volltextindexaktualisierung verwendet werden. Die Vorgabe ist 1 und 0 ist nicht zulässig.
<code>-ftiNdays <n></code>	<code>-fnd</code>	Bewirkt, dass Volltextindizes alle <n> Tage neu aufgebaut werden. Die Vorgabe ist, dass die Indizes nur neu aufgebaut werden, wenn sie beschädigt sind.
<code>-force <d></code>	<code>-f</code>	Gibt den Wochentag an, an dem Fixup für Datenbanken ausgeführt wird. Der Wertebereich von <d> ist 0 bis 7, wobei 1 Sonntag, 2 Montag usw. bedeutet, 0 hingegen jeder Tag.
<code>-compactNdays <n></code>	<code>-cnd</code>	Komprimiert nur Datenbanken, die seit <n> Tagen nicht komprimiert wurden. Diese Option bewirkt, dass alle <n> Tage versucht wird, alle Nicht-Systemdatenbanken zu komprimieren.
<code>-timeLimit <tl></code>	<code>-tl</code>	Neuer Name für Compact -x. Beschränkt die Komprimierungszeit auf <tl> Minuten (für alle Komprimierungen). Diese Option gilt nicht für UpdAll. Es wird angenommen, dass DBMT jeden Tag über ein Programmdokument ausgeführt wird. Sobald die Verarbeitung für alle Threads abgeschlossen ist, wird DBMT beendet.

Parameter	Abk.	Beschreibung
-range <s> <e>	-r	Nur zwischen <s> und <e> ausführen. Für diese Option wird angenommen, dass DBMT nur bei einem Serverstart über ein Programmdokument ausgeführt wird. DBMT ist inaktiv, bis <s> erreicht ist, und führt dann Komprimierungsvorgänge aus, bis <e> erreicht ist (oder alle Datenbanken verarbeitet wurden). Danach wartet das DBMT-Werkzeug wieder bis zur Startzeit. Der Zeitraum zwischen <s> und <e> muss mehr als 10 Minuten betragen. (Zeiten im 12-Stunden-Format mit AM/PM angeben (also z. B. 11:50PM))
-stoptime <e>	-st	Für diese Option wird angenommen, dass DBMT jeden Tag über ein Programmdokument gestartet wird. Der Wert <e> gibt an, zu welchem Zeitpunkt Komprimierungen abgeschlossen sein sollen. Sobald die Verarbeitung aller Threads abgeschlossen ist, wird DBMT beendet.
-noCompactLimit	-ncl	Erlaubt Compact so lange zu laufen, bis Komprimierung beendet ist.
-ods		Bewirkt, dass komprimierte Datenbanken in das aktuelle ODS konvertiert werden
-nounread		Keine Aktualisierung der Liste der ungelesenen Dokumente

Tabelle 9.7: Die wichtigsten Parameter des Programms DBMT

Standardmäßig unterbricht DBMT die Komprimierung bei der Zustellung eines Mails. Um das zu verhindern, setzen Sie in der Datei notes.ini die Variable MailFileDisableCompactAbort=1.

Achtung: Das kann zu längeren Zeiten ohne Mailzustellung führen. (Im Cluster können Sie die INI-Variable MailFileEnableDeliveryFailover=1 setzen, um die Mail auf einem anderen Server zuzustellen.)

9.6.1. DBMT und Systemdatenbanken

DBMT sieht die in der folgenden Liste aufgezählten Datenbanken als Systemdatenbanken an:

```
names.nsf
log.nsf
admin4.nsf
ddm.nsf
lndfr.nsf
events4.nsf
statrep.nsf
dbdirman.nsf
dircat.nsf
clubusy.nsf
domlog.nsf
clbdbir.nsf
busytime.nsf
catalog.nsf
daoscat.nsf
mtdata/mtstore.nsf
```

DBMT komprimiert keine Systemdatenbanken (führt aber UpdAll- und FTI-Operationen durch). Das bedeutet, Sie brauchen nach wie vor Compact, und zwar 1. für Systemdatenbanken (auch offline) und 2. für Datenbanken mit einem alten ODS (Schalter -upgrade).

9.6.2. Komprimieren

Die von DBMT angewandte Komprimierung erfolgt immer mithilfe einer Kopie («copy-style»).

Die Datei dbmt_compact_filter.ind listet jene Datenbanken auf, die DBMT auslöst. Diese Datei wird automatisch erstellt und gewartet. Es werden Datenbanken aufgenommen, die

- > zum Komprimieren länger brauchen würden, als es dem über den Parameter -range angegebenen Zeitraum entspricht
- > bei der Komprimierung das angegebene Zeitlimit überschritten haben
- > ein älteres ODS aufweisen als 41

Sie sollten die Datei dbmt_compact_filter.ind nicht händisch bearbeiten. Wenn Sie der Meinung sind, dass die Datei Datenbanken enthält, die dort nicht hineingehören, können Sie die Datei jedoch löschen und die betroffenen Datenbanken händisch komprimieren.

9.6.3. DBMT starten

DBMT kann auf drei Arten gestartet werden:

1. Über die Serverkonsole
2. Über ein Programmdokument
3. In der Windows-Befehlszeile (offline)

Aufgrund der vielen Parameter werden Sie DBMT wohl meist über Programmdokumente starten. Nachfolgend ein Beispiel für den Start mit Stoppzeit:

The screenshot shows a configuration window titled 'Programm: dbmt'. It has a tab 'Allgemein' selected under the 'Administration' section. The window is divided into two columns: 'Allgemein' and 'Zeitplan'.

Allgemein		Zeitplan	
Programmname:	dbmt	Aktiviert/deaktiviert:	Aktiviert
Befehlszeile:	mail -ct 4 -ut 4 -ft 4 -f 1 -st 6:00AM	Anfangszeiten:	21:00 jeden Tag
Läuft auf Server:	DOM/COB/AT	Wiederholungsintervall:	0 Minuten
Kommentare:		Wochentage:	So, Mo, Di, Mi, Do, Fr, Sa

Abbildung 9.12: Programmdokument – Einstellungen für das Programm DBMT (Erklärung im Text)

DBMT wird täglich um 21 Uhr mit 4 Threads gestartet und beendet sich selbst um 6 Uhr morgens. Am Sonntag wird Fixup ausgeführt.

Im zweiten Beispiel starten wir DBMT bereits beim Hochfahren mit dem Server. Damit es keine Kollisionen mit Benutzerzugriffen gibt, limitieren wir die Aktivität mit dem Parameter range auf 21:00 bis 06:00:

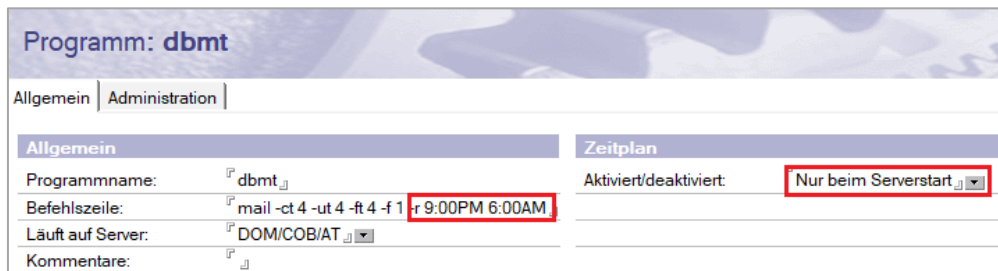


Abbildung 9.13: Programmdokument – Einstellungen für das Programm DBMT (Erklärung im Text)

DBMT bleibt immer aktiv, arbeitet aber nur im angegebenen Zeitraum (20 Uhr bis 6 Uhr morgens). Am Sonntag wird Fixup ausgeführt.

9.7. Datenbanken reparieren

Systemdatenbanken mit beschädigten Ansichten, Ordnern und/oder Dokumenten sind häufig Ursache für Serverabstürze. Datenbankschäden entstehen in erster Linie durch

- > Fehler auf Betriebssystemebene wie Hardware-Neustart, Systemabsturz, Stromausfall oder falsche Beendigungsprozeduren
- > Netzwerkprobleme bei Schreibzugriffen durch Clients
- > Fehlerhafte Datenbankzugriffe durch API-Programme

9.7.1. Das Programm Fixup

Das Programm **Fixup** sucht nach beschädigten Datenbanken und repariert sie. Prinzipiell prüft Notes bei jedem Öffnen einer Datenbank diese automatisch auf Beschädigungen und repariert sie gegebenenfalls. Wenn Fixup manuell ausgeführt wird, ist die Überprüfung exakter, da zusätzlich beschädigte Ansichten bzw. Ordner neu aufgebaut werden.

Fixup kann nicht mit offenen Datenbanken arbeiten. Ebenso kann eine Datenbank nicht geöffnet werden, wenn gerade Fixup darauf ausgeführt wird. Allerdings meldet Fixup der Logdatei alle offenen Datenbanken, beispielsweise log.nsf, mail.box oder names.nsf.

9.7.1.1. Fixup manuell starten

Geben Sie auf der Serverkonsole folgenden Befehl ein:

```
load fixup <Pfad> [Schalter]
```

Folgende Schalter stehen zur Verfügung:

Schalter	Erklärung
-F	Genaue Prüfung (full)
-L	Fehlerhafte Datenbanken werden in der Datei log.nsf aufgezeichnet.
-V	Es werden nur Dokumente (keine Ansichten) überprüft, wodurch Fixup schneller läuft.

Schalter	Erklärung
-I	Es werden nur Dokumente, die seit der letzten Überprüfung verändert wurden, beachtet.

Tabelle 9.8: Die wichtigsten Parameter für das Programm Fixup

9.7.1.2. Fixup über ein Programmdokument starten

Sie können Fixup natürlich auch über ein Programmdokument starten. Im folgenden Beispiel überprüft Fixup alle Datenbanken im Verzeichnis \mail:

Abbildung 9.14: Ein Programmdokument für den Start von Fixup mit dem Schalter -F (genaue Überprüfung) am Sonntag um vier Uhr

Fehlerhafte Dokumente werden von Fixup gelöscht, können aber beim Replizieren von anderen Servern wiederhergestellt werden, wenn sie dort fehlerfrei geblieben sind.

9.7.2. Fixup über DBMT ausführen

Die Syntax lautet:

```
load dbmt <Verzeichnis, Datenbank oder Indirect-Datei> -force <d>
```

<d> definiert den Wochentag, an dem Fixup ausgeführt wird. Der Wertebereich von <d> ist 0 bis 7, wobei 1 Sonntag bedeutet, 2 Montag usw. Bei Angabe von 0 wird Fixup jeden Tag ausgeführt. Analog zu Fixup kann auch DBMT entweder direkt auf der Serverkonsole oder über ein Programmdokument ausgeführt werden.

9.8. Ansichten verwalten

Notes-Ansichten (Notes Views) haben einen physischen Index – im Gegensatz zu Sichten (Views) in relationalen Datenbanken, die aus einer Abfragedefinitionen in SQL ohne Index bestehen. Bei Notes-Ansichten handelt es sich um ein internes Ablagesystem, das dazu verwendet wird, eine Liste aller Dokumente zu erstellen, die in einer Ansicht oder in einem Ordner angezeigt werden. Dies hat den Vorteil des schnellen Zugriffs und den Nachteil des Ressourcen- und Platzverbrauchs.

Ansichtsindizes werden innerhalb der Datenbank im NIF-Bereich (Notes Index Facility) gespeichert. Der Index kann auch ins Dateisystem ausgelagert werden – in Form von NDX-Dateien, siehe Kap. 9.8.5 auf Seite 265. Jede Ansicht besitzt ihren eigenen Index, die Regeln dafür legt der Entwickler fest. Per Vorgabe wird der Index erstellt, wenn die Ansicht zum ersten Mal verwendet wird und nach 45 Tagen Inaktivität wieder gelöscht.

Um den Status der Ansichtsindizes einzusehen, wechseln Sie im Admin-Client zum Register **Dateien** und wählen Sie die gewünschte Datenbank aus. Wählen Sie sodann in den Werkzeugen den Befehl **Datenbanken > Ansichten verwalten...**

Hier sehen Sie nicht nur, wie viel Speicherplatz alle Ansichtsindizes gemeinsam belegen, sondern auch die Größen der einzelnen Indizes mit ihren wichtigsten Einstellungen.

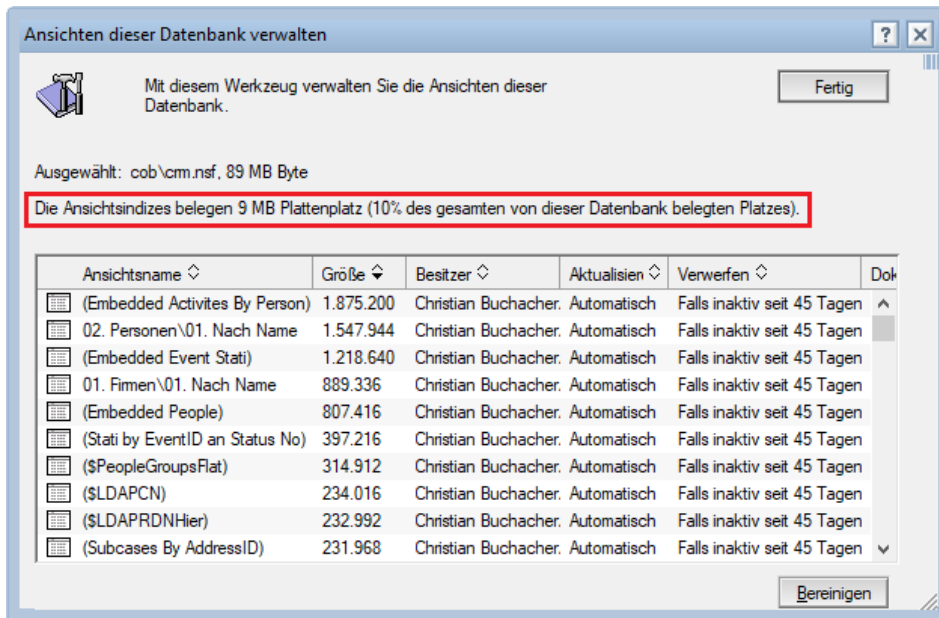


Abbildung 9.15: Dialog Ansichten verwalten

Um einen Index zu löschen, klicken Sie zuerst auf die Ansicht und dann auf **Bereinigen**. Der Index wird dann beim nächsten Zugriff eines Benutzers neu aufgebaut.

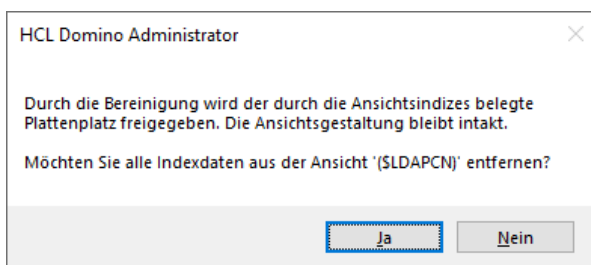


Abbildung 9.16: Warnung beim Bereinigen der Indexdaten

9.8.1. Nicht genutzte Ansichten finden

Das Werkzeug Ansichten verwalten eignet sich auch gut, um nicht genutzte Ansichten aufzuspüren. Stellen Sie sicher, dass in der Spalte **Aktualisieren** bei allen Ansichten »Automatisch, nach 1. Verwendung« steht. (Sollte das nicht der Fall sein, müssen Sie die Datenbank im Domino-Designer öffnen und für jede Ansicht diese Einstellung vornehmen.) Bereinigen Sie sodann alle Ansichten, die Indizes werden beim nächsten Zugriff neu erstellt. Überprüfen Sie nach mehreren Wochen, bei welchen Ansichten die Größe des Index immer noch 0 beträgt. Diese Ansichten wurden in der Zwischenzeit nicht verwendet.

Dieser Trick hilft Ihnen, nicht verwendete Ansichten aufzuspüren. Das heißt aber nicht, dass Sie diese Ansichten gleich löschen sollten, denn selten verwendete Ansichten können trotzdem wichtig sein, etwa für einen jährlichen Export.

9.8.2. Ansichtsindizes aktualisieren

Am Server kümmert sich der **Indexer** (Servertask Update) um die Aktualisierung von Ansichtsindizes. Zusätzlich steht mit UpdAll ein eigener Wartungstask zur Verfügung, mit dem der Administrator Ansichtsindizes aktualisieren oder auch neu aufbauen kann. (Mehr Details finden Sie in Kap. 9.10 Die Servertasks Update und UpdAll, ab Seite 271.)

Es kann auch passieren, dass Ansichtsindizes fehlerhaft werden, etwa alte Werte oder nicht alle Dokumente anzeigen oder auch die vom Entwickler hinzugefügten Spalten nicht aufscheinen. In diesem Fall muss der Index verworfen und neu aufgebaut werden. Das geht bei einzelnen Ansichten am schnellsten durch Drücken der Tasten UMSCHALT+F9. Ein Neuaufbau aller Ansichtsindizes in einer Datenbank kann durch die Tastenkombination [Strg]+[Umschalten]+[F9] erzwungen werden. Jedoch Achtung, das kann in größeren Datenbanken recht lang dauern, und der Client ist auch gesperrt, bis er mit dem Aktualisieren fertig ist. Besser (und schneller) ist die Eingabe des folgenden Serverkonsolenbefehls:

```
load updall <Datenbank> -r
```

9.8.3. Kritische Ansichten priorisieren

Per Vorgabe werden alle Ansichtsindizes nach einem planmäßigen Intervall aktualisiert. Um für kritische Ansichten eine raschere Aktualisierung zu erreichen, stehen zwei Methoden zur Verfügung:

1. Inline View Indexing
2. Ansichten mit hoher Nutzung (High Usage Views)

9.8.3.1. Inline View Indexing

Aktivieren Sie Inline View Indexing, um kritische Ansichten immer aktuell zu halten.

Inline View Indexing wurde mit Domino 9.0.1 FP9 eingeführt.

Es stehen zwei Methoden zur Aktivierung zur Verfügung:

- > Aktivierung über UpdAll
- > Aktivierung über die notes.ini-Variable `INLINE_VIEW_INDEX`

9.8.3.1.1. Aktivierung über UpdAll

Wenn Sie Inline View Indexing über den UpdAll-Task aktivieren, wird auch das \$Index-Designelement der Ansicht aktualisiert. Damit aktivieren Sie Inline View Indexing automatisch auch für alle Repliken dieser Datenbank. Wenn Sie mit UpdAll Inline View Indexing für eine Schablone aktivieren, wird dieses Feature automatisch an alle mit der Schablone erstellten Datenbanken weitergegeben.

Verwenden Sie den folgenden Befehl, um Inline View Indexing für eine einzelne Ansicht oder für alle Ansichten in einer Datenbank zu aktivieren:

Datenbanken verwalten: Ansichten verwalten

```
_load updall <Datenbank> -T "<Ansicht>" -inline on
```

```
_load updall <Datenbank> -inline on
```

9.8.3.1.2. Aktivierung mittels `INLINE_VIEW_INDEX`

Im Gegensatz zur Aktivierung via UpdAll führt das Setzen der `notes.ini`-Variable nicht zu einem Aktualisieren des \$Index-Designlements, weshalb die Änderung nicht weiterrepliziert wird. Am besten verwenden Sie zum Setzen der Variable das Konfigurationsdokument des Servers.

Beispiel:

```
INLINE_VIEW_INDEX=<Datenbank1>,<Datenbank2>,<Datenbank3>
```

Ein Serverneustart ist ausnahmsweise nicht nötig, Inline View Indexing wird beim nächsten Öffnen der Ansicht aktualisiert.

9.8.3.2. Ansichten mit hoher Nutzung (High Usage Views)

Die Ansichten mit hoher Nutzung werden nach Aktivierung dynamisch berechnet. Dabei überwacht Domino den Grad der Aktualisierungsaktivität für alle Ansichten und bewertet diese. Die zehn Ansichten mit der höchsten Bewertung werden als **Ansichten mit hoher Nutzung** (High Usage Views) betrachtet und mit extra Aktualisierungs-Threads auf dem neuesten Stand gehalten. Das ermöglicht ein schnelles Öffnen von stark genutzten Ansichten.

Welche Ansichten eine hohe Nutzung aufweisen, kann sich jederzeit ändern, wenn sich die Aktualisierungshäufigkeit der Ansicht ändert.

Diese Funktion ist standardmäßig deaktiviert. Zur Aktivierung schreiben Sie den folgenden Eintrag in die Datei `notes.ini`:

```
NIF_VIEW_USAGE_ENABLED=1
```

Nach dem Setzen dieser Variable muss der Server neu gestartet werden.

Über den Konsolenbefehl `show tasks` lassen sich Informationen zu Ansichten mit hoher Nutzung abrufen, z. B.:

```
View Indexer companies.nsf "CompanyAll" 10 sec. high usage read
```

Es steht dafür auch eine eigene Statistik zur Verfügung:

```
show statistic database.ViewUsage.*
```

9.8.4. Den temporären Ordner für Indexaktualisierungen ändern

Wenn Domino Ansichten aktualisiert – etwa, wenn Sie `updall -R` eingeben oder wenn ein Benutzer eine Ansicht öffnet, dessen Index bereinigt wurde – werden in dem in Windows vorkonfigurierten TEMP-Ordner (etwa `C:\TEMP`) temporäre Dateien zum Sortieren der Daten abgelegt. (Wenn kein TEMP-Ordner definiert ist, dann im Domino-Datenverzeichnis.) Nach dem Aktualisieren der Indizes löscht Domino die Dateien wieder.

Der dafür benötigte Platz im TEMP-Ordner kann beträchtlich sein (etwa zweimal die Größe der Daten in allen Dokumenten). Wenn Domino feststellt, dass zum Aktualisieren einer bestimmten Ansicht im temporären Ordner nicht genug Platz zur Verfügung steht, verwendet es eine langsamere

Methode, die nicht so viel Platz braucht. Das wird im Serverprotokoll (log.nsf) in der Ansicht Verschiedene Ereignisse protokolliert:

Warning: unable to use optimized view rebuild for view due to insufficient disk space at directory. Estimate may need n million bytes for this view. Using standard rebuild instead.

Bei Platzmangel wird empfohlen, den Ort für die temporären Dateien auf ein anderes Laufwerk zu verlegen. Damit gewährleisten Sie nicht nur, dass wieder genug Platz zur Verfügung steht, die Änderung kann sich durch die Lastverteilung auf verschiedene Laufwerke auch günstig auf die Performance auswirken.

Um den Ordner für temporäre Dateien zu ändern, nehmen Sie die folgende Zeile in die notes.ini des Servers auf:

```
View_Rebuild_Dir=<Pfad>
```

Wenn Sie für die Ansichtsaktualisierung wirklich keinen zusätzlichen Platz zur Verfügung stellen können und Sie obige Meldung in der Protokolldatei öfters sehen, können Sie die optimierte Ansichtsaktualisierung auch abschalten. Tragen Sie dazu die folgende Zeile in die notes.ini des Servers ein:

```
Disable_View_Rebuild_Opt=1
```

9.8.5. Verschieben der Ansichtsindizes ins Dateisystem (NIFNSF)

Die Funktion NIFNSF ist für große Datenbanken hilfreich und bietet die folgenden Vorteile:

- > Es entstehen kleinere Datenbankdateien.
- > Dadurch ergibt sich eine schnellere Sicherung und Wiederherstellung.
(In Maildatenbanken beträgt die Größe aller Ansichtsindizes rund 10 %. Wenn Sie auch den DAOS aktiviert haben, dann beträgt er von den übrigen Daten (ohne Anhängen) bereits rund 30 %.)
- > Wenn die Dateien auf einem anderen Laufwerk liegen, kann sich das auch positiv auf die Performance auswirken.

9.8.5.1. Vorgehensweise

Aktivieren Sie die Transaktionsprotokollierung im Serverdokument.

Fügen Sie die folgende Zeile zur notes.ini des Domino-Servers hinzu:

```
NIFNSFEnable=1
```

Die NDX-Dateien werden standardmäßig im Domino-Datenverzeichnis gespeichert. Um ein anderes Verzeichnis festzulegen, fügen Sie die folgende Zeile zur notes.ini des Servers hinzu:

```
NIFBasePath=<Pfad>
```

Dabei ist <Pfad> ein relativer Pfad zum Domino-Datenverzeichnis.

Starten Sie den Server neu.

9.8.5.2. Aktivieren von NISNSF für bestimmte Datenbanken

Im letzten Schritt haben wir NIFNSF serverweit aktiviert, jetzt müssen wir festlegen, für welche Datenbanken das Feature gelten soll. Um separate Ansichtsindizes für eine bestimmte Datenbank zu aktivieren, setzen Sie den folgenden Befehl auf dem Server ab:

```
load compact <Pfad> -c -nifnsf on
```

Um die Funktion NISNSF verwenden zu können, müssen Datenbanken ODS 51 oder höher verwenden.

9.8.5.3. Aktivieren von NISNSF für alle neuen Datenbanken

Um separate Ansichtsindizes für neu erstellte Datenbanken zu aktivieren, fügen Sie die folgende Zeile zur notes.ini des Servers hinzu:

```
CREATE_NIFNSF_DATABASES=1
```

Starten Sie den Server neu.

Um festzustellen, welche Datenbanken separate Ansichtsindizes verwenden, bzw. auch um die NDX-Dateigrößen einzusehen, geben Sie die folgenden Serverkonsolenbefehle ein:

```
show dir -nifnsf
```

```
show dir -nifnsfonly
```

9.8.5.4. Deaktivieren von NISNSF für bestimmte Datenbanken

Um separate Ansichtsindizes für eine Datenbank zu deaktivieren, führen Sie den folgenden Befehl auf dem Server aus:

```
load compact <Datenbank> -c -nifnsf off
```

9.9. Volltextindizes verwalten

Ein Volltextindex ist eine externe Struktur im Dateisystem, ein Unterverzeichnis mit dem Namen der Datenbank und der Endung *.ft, in dem sich die Indexdateien befinden. Volltextindizes werden nicht mitrepliziert, müssen also auf jedem Server extra erstellt werden, und auch Aktualisierungen werden nicht abgeglichen.

Eine eingeschränkte Volltextsuche ist auch ohne Index möglich. In diesem Fall werden direkt die Dokumente durchsucht, was bei großen Datenbanken lange dauert. Umgekehrt wird nach Erstellen des Index nur noch dieser durchsucht und nicht indizierte Dokumente fehlen im Suchergebnis.

Um das Suchergebnis möglichst akkurat zu halten, wird deshalb bei jeder Suche zunächst überprüft, ob der Index aktuell ist. Werden nicht indizierte Dokumente gefunden, werden diese bis zu einer Maximalzahl von 200 noch schnell indiziert, bevor die Suche ausgeführt wird. (Dieses Feature wird als **On Demand Full Text Indexing** bezeichnet.) Übrig gebliebene, nicht indizierte Dokumente werden in eine Warteschlange gestellt. Das passiert sowohl am Server als auch am Client, je nachdem, wo die Datenbank liegt.

Das ist ein tolles Feature, kann allerdings in großen lokalen Repliken, in denen es ja keine automatische Hintergrundindizierung gibt, beim Suchen zu Wartezeiten führen. Ähnliche Phänomene habe

ich auch in XPage-basierenden Webanwendungen beobachtet: Waren nicht indizierte Dokumente vorhanden, dauerte es bis zu einer Minute, bis das Suchergebnis angezeigt wurde. Wenn Ihnen dieses Feature lästig wird, können Sie es mit dem folgenden Eintrag in der notes.ini auch abschalten:

```
FT_SUPPRESS_AUTO_UPDATING=1
```

9.9.1. Einen Volltextindex erstellen

Ein Volltextindex kann entweder in den Datenbankeigenschaften oder im Admin-Client im Register **Dateien** erstellt werden – auf der Serverkonsole können Sie nur existierende Indizes aktualisieren.

9.9.1.1. Einen Volltextindex in den Dateieigenschaften erstellen

Um einen Volltextindex zu erstellen, öffnen Sie die Dateieigenschaften und wechseln Sie zum Register **Volltextindex** (Lupensymbol). Klicken Sie auf die Schaltfläche **Index erstellen...**

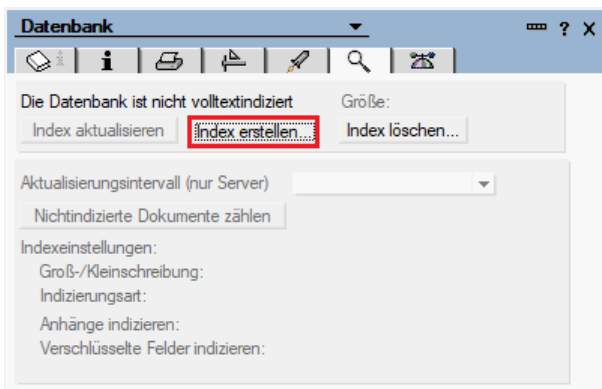


Abbildung 9.17: Datenbankeigenschaften – Volltextindex erstellen

Es wird der Dialog **Volltextindex erstellen** angezeigt:

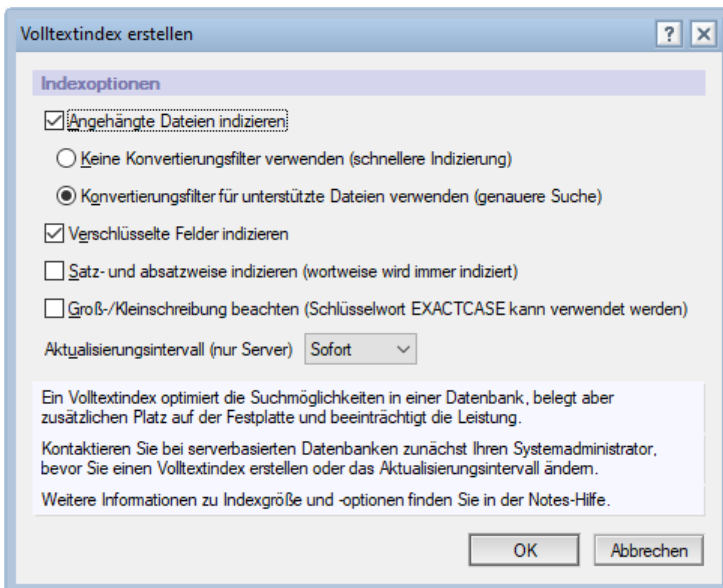


Abbildung 9.18: Dialog Volltextindex erstellen

Wenn Sie auch die Anhänge indiziert haben wollen, wählen Sie die Option »Konvertierungsfilter verwenden (genauere Suche)«.

Etwas aufwendiger wird die Sache, wenn Sie nur bestimmte Dateitypen indizieren wollen, etwa Word, Excel und PDF. In diesem Fall erstellen Sie zusätzlich die folgenden Einträge in der Datei notes.ini:

```
FT_USE_ATTACHMENT_WHITE_LIST=1
FT_INDEX_FILTER_ATTACHMENT_TYPES=*.docx,*.xlsx,*.pdf
FT_INDEX_FILTER_ATTACHMENT_TYPES_MAX_MB=5
```

Obige Einträge gelten serverweit, aber Sie können den Volltextindex auch für bestimmte Datenbanken konfigurieren. Nehmen wir an, eine Datenbank hat die Replik-ID C1257733:003B4D27, dann können Sie den folgenden Filter setzen:

```
FT_INDEX_FILTER_ATTACHMENT_TYPES_C1257733003B4D27=*.docx,*.pdf
```

9.9.1.2. Einen Volltextindex im Domino-Administrator erstellen

Navigieren Sie im Domino-Administrator zum Register **Dateien** und wählen Sie die Datenbanken, für die Sie einen Volltextindex erstellen wollen. Wählen Sie im Kontextmenü (rechte Maustaste) **Volltextindex...**:

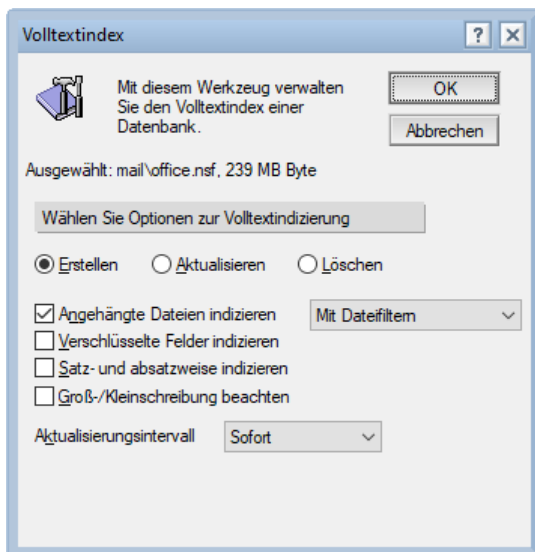


Abbildung 9.19: Dialog Volltextindex im Domino-Administrator

Wenn Sie auch die Anhänge indiziert haben wollen, wählen Sie die Option »Mit Dateifiltern«.

Seit Domino 10 ist **Apache Tika** (eine Java-basierende Open-Source-Komponente bestehend aus der Datei tika-server.jar) für die Anhangsindizierung zuständig. Sollten auf Ihrem Server Anhänge nicht indiziert werden, überprüfen Sie, ob ein Java-Tika-Prozess läuft. Ist das nicht der Fall, überprüfen Sie, ob die folgende Variable in der notes.ini gesetzt ist:

```
FT_INDEX_ATTACHMENTS=3
```

(Die Variable darf auch fehlen, aber wenn gesetzt, darf sie keinen anderen Wert als 3 haben!)

Tika verwendet den HTTP-Task und horcht auf Port 9998 auf Anfragen zur Textextraktion. Sollte dieser Anschluss bereits belegt sein, verwenden Sie die folgende `notes.ini`-Variable zum Ändern der Port-Nummer, z. B.:

```
TIKA_PORT=9997
```

9.9.2. Volltextindex aktualisieren

9.9.2.1. Manuelle Aktualisierung

Eine manuelle Indizierung ist nur lokal nötig, am Server werden Datenbanken im Hintergrund automatisch aktualisiert. Klicken Sie in den Datenbankeigenschaften auf die Schaltfläche **Index aktualisieren**, macht sich der Indexer (Update-Task) lokal sofort an die Arbeit. Am Server wird der Antrag zur Indizierung in eine Warteschlange gestellt und mit niedriger Priorität, d. h. nur bei geringer Serverauslastung, ausgeführt.

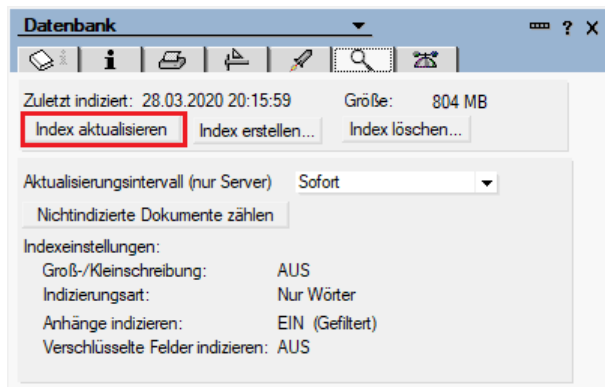


Abbildung 9.20: Datenbankeigenschaften – Volltextindex aktualisieren

Anders verhält es sich auf der Serverkonsole. Der Befehl `load updall <Pfad> -f` führt ein sofortiges Update aus.

Tipp: Anstatt den Index immer nur zu aktualisieren, empfehle ich, ihn zumindest einmal pro Monat über den Befehl `load updall <Pfad> -x` niederzureißen und neu aufzubauen.

9.9.2.2. Automatische Aktualisierung

Eine automatische Aktualisierung gibt es nur am Server. Je nach gewähltem Aktualisierungsintervall sind an der Indizierung mehrere Programme beteiligt:

Aktualisierung	Beschreibung
Täglich	Wird vom nächtlichen UpdAll ausgeführt. Vorgabe via <code>notes.ini</code> -Eintrag <code>ServerTasksAt2</code> , also um 2:00.
Nach Plan	Wird von einem Programmdokument, das UpdAll startet, ausgeführt. Der Vorteil besteht darin, dass im Gegensatz zur Methode »Täglich« mehrere Datenbanken zu verschiedenen Zeiten aktualisiert werden können.
Stündlich	Wird vom stündlich laufenden Task Chronos initialisiert. Wenn Update läuft, wird die Indizierung von diesem ausgeführt.

Aktualisierung	Beschreibung
Sofort	Wird von Update ausgeführt.

Tabelle 9.9: Aktualisierungsintervalle für Volltextindizes

Der Task **Chronos** wird von Domino automatisch gestartet und muss nicht zur Datei notes.ini hinzugefügt werden. Sie können den Task durch folgende Befehle auch per sofort ausführen:

```
load chronos daily
```

```
load chronos hourly
```

Sie können das automatische Starten von Chronos durch folgende notes.ini-Variable deaktivieren: Debug_Disable_Chronos=1

Tipp: Es empfiehlt sich, Aktualisierungen von Ansichts- und Volltextindizes in separaten Threads durchzuführen, was Sie mit dem folgenden Eintrag in der Datei notes.ini erzwingen können:

```
UPDATE_FULLTEXT_THREAD=1
```

9.9.3. Volltextindex löschen

Auch das Löschen von Volltextindizes ist in den Datenbankeigenschaften und im Admin-Client auf dem Register Dateien möglich (hier auch mit Mehrfachauswahl).

In den Datenbankeigenschaften klicken Sie einfach auf die Schaltfläche **Index löschen...**

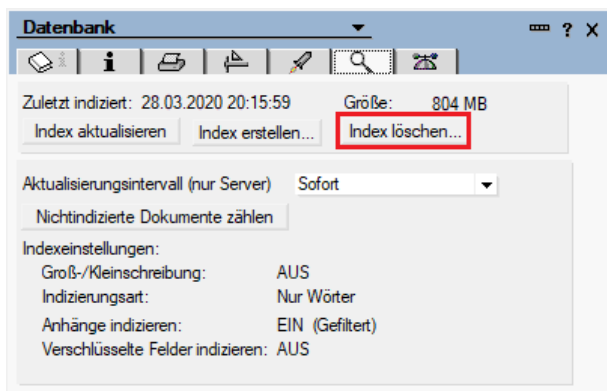


Abbildung 9.21: Datenbankeigenschaften – Volltextindex löschen

9.9.4. Volltextindex verschieben

Mit dem folgenden notes.ini-Parameter können Sie die Volltextindizes auf ein anderes Laufwerk bzw. auf eine andere Partition verschieben:

```
FTBasePath=<Pfad>
```

Das macht vor allem in größeren Umgebungen Sinn:

- > Der Volltextindex verursacht systembedingt eine hohe Fragmentierung der Datenträger.
- > In großen Umgebungen werden Datenbanken und deren Volltextindizes sehr groß und können so aufgeteilt werden.

- > Beim Backup muss der Volltextindex nicht berücksichtigt werden.
- > Performanceverbesserung durch Schreibzugriffe auf andere Laufwerke, dies entlastet damit die Schreibzugriffe der Domino-Datenpartition.

Gehen Sie zum Verlegen der Indexdateien wie folgt vor:

1. Tragen Sie im Konfigurationsdokument des Servers die folgende Variable ein:

```
FTBasePath=<Pfad>
```

2. Starten Sie den Server neu.

3. Starten Sie auf der Konsole das Programm UpdAll mit dem Parameter -f, um alle Volltextindizes neu aufzubauen:

```
load updall -f
```

Die bestehenden Indexdateien werden dabei gelöscht.

9.10. Die Servertasks Update und UpdAll

9.10.1. Der Servertask Update

Der Servertask Update wird auch **Indexer** genannt und bereits beim Hochfahren des Servers gestartet, das heißt, er ist aktiv, so lange der Server läuft. Zu den Aufgaben des Indexers gehört:

- > Das Aktualisieren von geänderten Ansichtsindizes
- > Das Aktualisieren von Volltextindizes mit den Aktualisierungsintervallen **Sofort** und **Stündlich**
- > Das Aufspüren von beschädigten Indizes und das Rekonstruieren derselben
- > Das Löschen von Ansichtsindizes, die seit 45 Tagen nicht benutzt wurden
- > Der Indexer kann nicht parametrisiert werden.

Die Update-Task startet einen zusätzlichen **Verzeichnis-Indexer**-Thread, der im Minutentakt exklusiv die Ansichtsindizes des Domino-Verzeichnisses aktualisiert. Dieser Thread erscheint in der Liste der Servertasks als Directory Indexer auf.

Tipp: Um die Leistung der Ansichtsindizierung zu verbessern, können Sie mehrere Update-Tasks gleichzeitig ausführen, wenn Ihr Server über eine angemessene CPU-Leistung verfügt. Fügen Sie hierzu entweder zur Variable `ServerTasks` in der Datei `notes.ini` einen zusätzlichen Eintrag `Update` hinzu oder erstellen Sie ein Programmdokument, um einen zweiten Update-Task zu starten. Wenn Sie mehrere Instanzen von Update ausführen wollen, können Sie auch die folgende Variable zur Datei `notes.ini` hinzufügen:

```
Updaters=[Anzahl Prozessoren], z. B. Updaters=4
```

Danach muss der Server neu gestartet werden.

9.10.2. Die Leistung von Update verbessern

Wenn Ihr Server trotz mehrerer Indexer eine zu hohe Aktualisierungsrate aufweist, können die Warteschlangen für die Aktualisierungen sehr groß werden. Und dann müssen Sie eine Vorgehensweise

entwickeln, um Ressourcen zu sparen. Im Folgenden finden Sie einige beispielhafte Methoden, die Sie in bestimmten Szenarien implementieren können.

Erstes Szenario – Die Warteschlangen sind in der Regel klein, es sei denn, es wird die Volltextindizierung einer großen Datenbank gestartet. In diesem Fall wartet die Ansichtsaktualisierung, bis der Volltextindex fertiggestellt ist. Um mehr Systemressourcen zur Verfügung zu haben, führen Sie Ansichtsaktualisierungen und Volltextaktualisierungen in separaten Threads durch. Fügen Sie dafür zur Datei notes.ini des Servers die folgende Zeile hinzu:

```
UPDATE_FULLTEXT_THREAD=1
```

Zweites Szenario – Die Warteschlangen wachsen allmählich an und werden schließlich zu groß, da der Update-Task nicht über genügend Systemressourcen verfügt. Um zusätzliche Ressourcen bereitzustellen, verkleinern Sie die Verzögerung zwischen jeder Aktualisierung. Standardmäßig beträgt die Verzögerung 5 Sekunden. Legen Sie mit der Variable UPDATE_IDLE_TIME (und FTUPDATE_IDLE_TIME, wenn zwei Threads verwendet werden) in der notes.ini-Datei des Servers eine kürzere Verzögerung fest. Mit der Variable UPDATE_IDLE_TIME_MS (und FTUPDATE_IDLE_TIME_MS bei Verwendung von zwei Threads) können Sie die Zeit auch in Millisekunden angeben.

Drittes Szenario – Anwendungen mit hohen Aktualisierungsraten benötigen häufig zu viele Systemressourcen, um die Warteschlangen klein zu halten. In diesem Fall sollten Sie einen leistungsfähigeren Server anschaffen! Bis es so weit ist, können Sie die Ansichtsaktualisierungen ganz ausschalten, sodass die Datenbanken nur noch beim Öffnen aktualisiert werden. Fügen Sie dazu zur Datei notes.ini die Variable UPDATE_DISABLE_VIEWS=1 hinzu. Alternativ können Sie auch die Anzahl der sofortigen Volltextaktualisierungen begrenzen. Ändern Sie dazu das Aktualisierungsintervall auf »Stündlich«, »Täglich« oder einen bestimmten Zeitplan.

9.10.3. Der Servertask UpdAll

Das Programm **UpdAll** wird standardmäßig via notes.ini über die Variable ServerTasksAt2 um 2:00 Uhr gestartet und beendet sich selbst, wenn es alle Aufgaben erledigt hat. Zu den Aufgaben gehören:

- > Das Aufspüren von fehlenden Indizes und das Erstellen derselben
- > Das Aufspüren von beschädigten Indizes und das Rekonstruieren derselben
- > Das Aktualisieren von Volltextindizes mit dem Aktualisierungsintervall **Täglich**
- > Das Entfernen von Lösinfos – mehr dazu in Kapitel Replikation, ab Seite 293

Sie können UpdAll auch manuell starten, entweder auf der Serverkonsole oder über ein Programmdokument. Dabei können Sie die Arbeitsweise des Programms durch Argumente ändern. Die Syntax des Befehls lautet:

```
load updall <Pfad> -[Schalter]
```

Bei <Pfad> kann es sich um eine Datenbank oder um ein Verzeichnis handeln.

Hier die wichtigsten Schalter:

Schalter	Erklärung
-c	Erstellt nicht verwendete Ansichtsindizes neu
-f	Aktualisiert Volltextindizes unabhängig von der eingestellten Frequenz
-v	Aktualisiert Ansichtsindizes

Schalter	Erklärung
-t <Ansicht>	Aktualisiert die Ansicht <Ansicht>
-r	Löscht Ansichtsindizes und erstellt sie neu
-x	Löscht Volltextindizes und erstellt sie neu

Tabelle 9.10: Die wichtigsten Parameter für das Programm UpdAll

Beispiel für den Start von UpdAll über ein Programmdokument:

Programm: updall

Allgemein Administration

Allgemein	Zeitplan
Programmname: <input type="text" value="updall"/>	Aktiviert/deaktiviert: <input type="text" value="Aktiviert"/>
Befehlszeile: <input type="text" value="names.nsf -r"/>	Anfangszeiten: <input type="text" value="23:00"/> jeden Tag
Läuft auf Server: <input type="text" value="DOM/COB/AT"/>	Wiederholungsintervall: <input type="text" value="0"/> Minuten
Kommentare: <input type="text" value=""/>	Wochentage: <input type="text" value="So"/>

Abbildung 9.22: Neuerstellen von Ansichtsindizes im Domino-Verzeichnis jeden Sonntag um 23:00 Uhr

Werden Ansichten aktualisiert – egal durch welchen Task – werden alle neuen Benutzersitzungen, die nach dem Start der Aktualisierung erstellt werden, ausgeschlossen. Daher empfehle ich, zumindest umfangreichere Ansichtsaktualisierungen erst spät nachts durchzuführen, wenn nur wenige Benutzer arbeiten.

Eigenschaft	Update	UpdAll
Läuft wann?	Kontinuierlich nach dem Serverstart	Einmalig um 2:00 Uhr (Vorgabe) und bei Bedarf
Behandelt alle Datenbanken?	Nein, nur geänderte	Ja
Aktualisiert Ansichtsindizes?	Ja	Ja
Aktualisiert Volltextindizes?	Ja, aber nur Volltextindizes mit den Aktualisierungsintervallen sofort und stündlich	Ja, aktualisiert alle Volltextindizes
Erkennt korrupte Ansichtsindizes und versucht, sie zu reparieren?	Ja	Ja
Erkennt korrupte Volltextindizes und versucht, sie zu reparieren?	Ja	Ja
Entfernt Löschinfos?	Nein	Ja
Verwirft ungenutzte Ansichtsindizes?	Ja (wenn 45 Tage nicht in Gebrauch bzw. wie vom Entwickler eingestellt)	Ja (wenn 45 Tage nicht in Gebrauch bzw. wie vom Entwickler eingestellt)
Ignoriert die Ansichtseigenschaft »Aktualisieren«?	Ja	Ja
Kann mit Optionen gestartet werden?	Nein	Ja

Tabelle 9.11: Vergleich zwischen Update und UpdAll

9.11. Kompressionsverfahren anwenden

Haben Sie viele große Datenbanken im Einsatz, belegen diese nicht nur mehr Platz, sondern erschweren auch die Datenbankwartung. Kleinere Datenbanken können schneller komprimiert und schneller gesichert werden. Domino bietet mehrere Lösungen an, um Datenbanken zu verkleinern und damit eine bessere Wartbarkeit zu erzielen:

- > Gestaltungskomprimierung
- > Zentralschablone
- > Komprimierung von Dokumentdaten
- > Anhangskomprimierung
- > Domino Attachment and Object Services (DAOS)

9.11.1. Gestaltungskomprimierung

Nach Aktivieren der **Gestaltungskomprimierung** (Design Compression) belegt die Gestaltung innerhalb der Datenbank um 55 bis 60 % weniger Platz. Um konkrete Zahlen zu nennen: Eine leere Maildatenbank der Version 11 mit unkomprimierter Gestaltung ist etwa 32 MB groß, davon belegt die Gestaltung rund 30 MB. Nach der Komprimierung des Designs ist die Datenbank nur noch 15 MB groß, d. h. um rund 17 MB kleiner. Das mag Ihnen nicht viel erscheinen, aber wenn Sie die Gestaltung aller Datenbanken auf Ihren Servern komprimieren, gewinnen Sie nicht nur Platz, sondern steigern auch die Wartbarkeit beträchtlich.

Anmerkung: Die Gestaltung der Maildatenbank ist in Version 11 per Vorgabe komprimiert, d. h. eine neu erstellte Maildatenbank ist 15 MB groß.

Aktivieren der Gestaltungskomprimierung via Datenbankeigenschaften

1. Wählen Sie die Datenbank aus und rufen Sie die Datenbankeigenschaften auf, etwa durch Drücken der Tastenkombination [Alt]+[Eingabe] oder durch den Menübefehl **Datei > Anwendung > Eigenschaften**.
2. Wählen Sie die Registerkarte **Erweitert**. (Propellerhut) und aktivieren Sie das Kontrollkästchen **Datenbankgestaltung komprimieren**.
3. Neu vom Entwickler hinzugefügte Designelemente werden danach sofort komprimiert gespeichert. Um auch bereits vorhandene Gestaltungselemente komprimiert zu speichern, müssen Sie die ganze Datenbank mithilfe einer Kopie komprimieren:
`load compact <Datenbank.nsf> -c`

Im Domino-Administrator können Sie die Gestaltungskomprimierung auch für eine Mehrfachauswahl aktivieren:

1. Navigieren Sie im Domino-Administrator zum Register **Dateien**.
2. Wählen Sie eine oder mehrere Datenbanken aus.
3. Wählen Sie in den Werkzeugen **Datenbank > Erweiterte Eigenschaften...** oder ziehen Sie die ausgewählte(n) Datenbank(en) in das Werkzeug Erweiterte Eigenschaften.
4. Aktivieren Sie beide Häkchen neben **Datenbankgestaltung komprimieren**.
5. Schließen Sie das Werkzeug Erweiterte Eigenschaften.
6. Komprimieren Sie die ausgewählten Datenbanken mithilfe einer Kopie.

Die Gestaltungskomprimierung über den Compact-Task aktivieren

Sie können die Gestaltungskomprimierung auch bei der Komprimierung einer Datenbank mithilfe einer Kopie durch den Zusatzschalter `-n` aktivieren:

```
load compact <Datenbank.nsf> -c -n
```

Um die Designelemente wieder zu dekomprimieren, führen Sie folgenden Befehl aus:

```
load compact <Datenbank.nsf> -c -N
```

Tipp: Aktivieren Sie mit folgendem Befehl die Gestaltungskomprimierung für alle Datenbanken auf Ihrem Server:

```
load compact -c -n
```

9.11.2. Zentralschablone

Bei Verwendung einer **Zentralschablone** (Single Copy Template, SCT) wird die Gestaltung aus der Datenbank gelöscht und durch einen Verweis auf die Schablone ersetzt. Entsprechend ist eine leere Maildatenbank, die eine Zentralschablone verwendet, nur noch etwa 2,5 MB groß!

Das Laden der Gestaltung aus der Schablone wirkt sich kaum auf die Performance aus, da Designelemente von Serverdatenbanken im lokalen Designcache (Datei `cache.ndk`) des Notes-Clients zwischengespeichert werden. (Mehr Details zum Designcache finden Sie in Kap. 18.2.3.3 Was Sie nach dem Ausrollen der Clients bedenken sollten, ab Seite 472.)

Beachten Sie vor der Einführung einer Zentralschablone folgende Regeln:

- > Bei der Zentralschablone handelt es sich um eine Serverlösung, erstellen Sie eine lokale Replik, wird die Gestaltung wieder in die Datenbank eingefügt.
- > Die Zentralschablone muss auf demselben Server liegen wie die abhängigen Datenbanken. Beachten Sie das beim Erstellen von Repliken auf anderen Servern.
- > Ändern Sie den Namen der Zentralschablone nicht, da Datenbanken, die auf die Schablone verweisen, sonst ihre Zuordnung verlieren.
- > Führen Sie größere Konvertierungen zu/von Zentralschablonen während Zeiten mit geringer Serveraktivität durch.
- > Zentralschablonen können nicht gelöscht werden. Löschen Sie die Datei gegebenenfalls auf Betriebssystemebene.

Um eine Zentralschablone zu erstellen, gehen Sie wie folgt vor:

1. Aktivieren Sie in den Datenbankeigenschaften der Schablone im Register **Design** das Kontrollkästchen **Zentralschablone** (siehe Abbildung 9.23).
2. Starten Sie den Design-Task (oder warten Sie, bis dieser nach Zeitplan ausgeführt wird), um die Gestaltung aus der Datenbank zu entfernen und durch einen Verweis auf die Zentralschablone zu ersetzen.

Beachten Sie, dass die Datenbanken dadurch zunächst nicht kleiner werden – dazu müssen sie erst komprimiert werden!

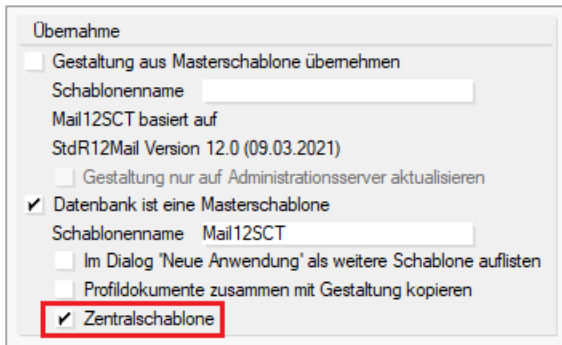


Abbildung 9.23: Datenbankeigenschaften, Register Gestaltung

9.11.3. Komprimieren von Dokumentdaten

Die **Dokumentdatenkomprimierung** (Document Body Compression) entspricht der Komprimierung von Rich-Text-Feldern, welche dadurch um bis zu 60 % weniger Platz beanspruchen.

Aktivieren der Dokumentdatenkomprimierung via Datenbankeigenschaften

1. Wählen Sie die Datenbank aus und rufen Sie die Datenbankeigenschaften auf, etwa durch Drücken der Tastenkombination [Alt]+[Eingabe] oder durch den Menübefehl **Datei > Anwendung > Eigenschaften**.
2. Wählen Sie die Registerkarte **Erweitert**. (Propellerhut) und aktivieren Sie das Kontrollkästchen **Dokumentdaten komprimieren**.
3. Neu erstellte Dokumente mit Rich-Text-Feldern werden danach beim Speichern sofort komprimiert. Um auch bereits vorhandene Dokumente komprimiert zu speichern, müssen Sie die ganze Datenbank mithilfe einer Kopie komprimieren:

```
load compact <Datenbank.nsf> -c
```

Im Domino-Administrator können Sie die Dokumentdatenkomprimierung auch für eine Mehrfachauswahl aktivieren:

1. Navigieren Sie im Domino-Administrator zum Register **Dateien**.
2. Wählen Sie eine oder mehrere Datenbanken aus.
3. Wählen Sie in den Werkzeugen **Datenbank > Erweiterte Eigenschaften...** oder ziehen Sie die ausgewählte(n) Datenbank(en) in das Werkzeug Erweiterte Eigenschaften.
4. Aktivieren Sie beide Häkchen neben **Dokumentdaten komprimieren**.
5. Schließen Sie das Werkzeug Erweiterte Eigenschaften.
6. Komprimieren Sie die ausgewählten Datenbanken mithilfe einer Kopie.

Die Komprimierung von Dokumentdaten über den Compact-Task aktivieren

Sie können die Komprimierung von Dokumentdaten auch bei der Komprimierung einer Datenbank mithilfe einer Kopie durch den Zusatzschalter -v aktivieren:

```
load compact <Datenbank.nsf> -c -v
```

Um die Komprimierung von Dokumentdaten wieder aufzuheben, verwenden Sie folgenden Befehl:

```
load compact <Datenbank.nsf> -c -V
```

9.11.4. Anhangskomprimierung

Anhänge werden in Dokumenten ohne Zutun des Benutzers komprimiert gespeichert. Bis Domino R5 kam dabei ausschließlich der Huffman-Algorithmus zum Einsatz, mit Version 6 wurde der LZ1-Algorithmus eingeführt, aber nicht automatisch aktiviert. Der LZ1-Algorithmus komprimiert nicht nur eine Spur besser (12–15 %), sondern ist auch viel schneller.

Stellen Sie daher sicher, dass alle Anhänge LZ1-komprimiert sind, bevor Sie den DAOS aktivieren, was in allen neu erstellten Datenbanken automatisch der Fall ist. Ältere Datenbanken, die mit Version 6 oder 7 erstellt wurden, können jedoch noch Anhänge enthalten, die mit dem alten Huffman-Algorithmus komprimiert sind, selbst wenn in den erweiterten Datenbankeigenschaften die Einstellung **LZ1-Komprimierung für Anhänge verwenden** gesetzt ist. Der folgende Befehl aktiviert nicht nur die LZ1-Komprimierung, er lädt auch alle Anhänge herunter und lädt sie LZ1-komprimiert neu hoch:

```
load compact <Datenbank> -C -ZU
```

9.12. Domino Attachment and Object Service

Nach Aktivierung des Domino Attachment and Object Services (DAOS) werden identische Dateianhänge auf demselben Server datenbankübergreifend nur noch einmalig gespeichert. Dieser Vorgang wird **Reduplizierung** oder **Anhangskonsolidierung** (Attachment Consolidation) genannt. Reduplizierung funktioniert mit allen Notes-Datenbanken, die Dateianhänge in Dokumenten speichern, ist aber besonders bei Maildatenbanken interessant.

Wenn die Anhangskonsolidierung für eine bestimmte Datenbank aktiviert ist und ein Benutzer einen Anhang speichert, enthält der im Dokument gespeicherte Text einen Verweis (auch als »Ticket« bezeichnet) auf den Anhang, der im **DAOS-Speicher** liegt. Im DAOS-Speicher selbst wird der Anhang als **NLO-Datei** (für Notes Large Object) abgelegt, welcher komprimiert und mit der Server-ID verschlüsselt vorliegt.

Ging die Nachricht, die den Anhang enthielt, an viele Benutzer, wird durch die Anhangskonsolidierung die Speicherplatznutzung erheblich reduziert. Die Einsparungen betragen durchschnittlich ein Viertel des verbrauchten Speicherplatzes, in einzelnen Fällen ist auch mehr möglich. 25 % Platzerparnis sind nicht zu verachten, ein noch größerer Vorteil liegt aber wohl in der besseren Wartbarkeit der Datenbanken. Denn wenn Datenbanken keine Anhänge mehr enthalten, brauchen sie nur noch 20 % (oder weniger) ihrer ursprünglichen Größe. (Das ist nicht mit 80 % Platzerparnis gleichzusetzen, da die Anhänge ja nur in den DAOS-Speicher verschoben wurden!) Und wenn Sie jetzt diese um 80 % kleinere Datenbank komprimieren, braucht das nur noch einen Bruchteil der Zeit, die es für die dieselbe Datenbank mit allen Anhängen gebraucht hätte. Somit geht die Komprimierung wesentlich rascher vonstatten.

Administratoren können eine Mindestgröße angeben, unter der Anhänge direkt im Dokument gespeichert werden, erst wenn die Mindestgröße überschritten wurde, wird der Anhang in den DAOS-Speicher ausgelagert.

Die Anhangskonsolidierung ist für Benutzer vollständig transparent. Wenn ein Empfänger ein Dokument öffnet, werden die Anhangssymbole gleich angezeigt, unabhängig davon, ob sich der Anhang direkt im Dokument befindet oder in den DAOS-Speicher ausgelagert wurde und nur noch ein Ticket enthält. Benutzer können in beiden Fällen völlig gleich agieren, Anhänge löschen, lokal speichern, ersetzen und ausführen. Wenn Benutzer einen Anhang löschen oder ersetzen oder neue Dokumente oder Nachrichten erstellen, die Kopien vorhandener Anhänge enthalten, passt der Server

die Verweise auf jeden Anhang im Repository nach Bedarf an und ermittelt anhand der Zuordnung, welche Anhänge auf dem Server identisch sind.

Wenn Sie den DAOS später wieder deaktivieren, bleiben alle Anhänge im DAOS-Speicher erhalten und werden beim Dokumentabruf auch von dort gelesen, können aber nicht mehr geändert werden. Neu erstellte Anhänge werden hingegen wieder direkt in den Dokumenten gespeichert. Sie können den Compactor auch anweisen, die ausgelagerten Dateien wieder in die Dokumente zurückzuführen.

9.12.1. Den DAOS zur Mailweiterleitung einrichten

Sie sollten auch die mail.box-Dateien auf allen an der Mailweiterleitung beteiligten Servern für den DAOS aktivieren. Dadurch werden Anhänge bereits beim Versenden im DAOS abgelegt – die Mails enthalten nur noch Verweise (Tickets). Das wirkt sich besonders bei der Übertragung von Mails mit Anhängen auf andere Server günstig auf die Performance aus.

9.12.2. Ein paar Worte zur Verschlüsselung

Werden Mails mit Anhängen an verschiedene Empfänger verschlüsselt verschickt, landet jeder Anhang einmal im DAOS-Speicher und es kommt zu keiner Platzersparnis. Das ist deshalb, weil aufgrund der verschiedenen Empfängerschlüssel jeder Anhang eine andere Byte-Länge hat. Überlegen Sie sich daher, die Verschlüsselung von Mails ganz zu unterbinden, um weniger Objekte im DAOS-Speicher zu haben. (Das Deaktivieren der Mailverschlüsselung ist in Kap. 12.5 Spezialfall Mailverschlüsselung, ab Seite 325 beschrieben.)

9.12.3. Ein paar Worte zur Anhangskomprimierung

Warum ist das für die DAOS-Aktivierung relevant? – Weil die Art der Komprimierung auf Datenbankebene eingestellt wird, was dazu führen kann, dass derselbe Anhang in einer Datenbank mit der Huffman-Kodierung komprimiert vorliegt und in einer anderen mit der LZ1-Kodierung, was unterschiedliche Byte-Summen und damit zwei Einträge im DAOS-Speicher ergibt. Stellen Sie daher sicher, dass alle Anhänge LZ1-komprimiert sind, bevor Sie den DAOS aktivieren. Dies erreichen Sie mit folgendem Befehl:

```
load compact <Datenbank> -C -ZU
```

9.12.4. Voraussetzungen für den DAOS

1. Bringen Sie alle Datenbanken auf das neueste ODS (ODS 51 oder höher).
2. Aktivieren Sie die Transaktionsprotokollierung auf dem Server.

9.12.5. Einen DAOS einrichten

Bevor Sie die Anhangskonsolidierung einrichten, müssen Sie entscheiden, wo die Dateien abgelegt werden sollen und ab welcher Größe – es macht aufgrund des Verwaltungsoverheads nämlich wenig Sinn, allzu kleine Anhänge in den DAOS zu verschieben.

Geben Sie keinen vollständigen Pfad an, wird der DAOS-Speicher relativ zum Datenverzeichnis erstellt. Domino erstellt automatisch Unterverzeichnisse, die mit 0001 beginnend durchnummeriert werden, erst darin werden die ausgelagerten Anhänge als NLO-Dateien abgelegt.

Um den DAOS auf Ihrem Server einzurichten und zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Domino-Administrator zum Register **Konfiguration** und erweitern Sie den Abschnitt **Server**.
2. Wählen Sie das gewünschte Serverdokument und klicken Sie auf **Server bearbeiten**.
3. Wechseln Sie zum Register **DAOS**.

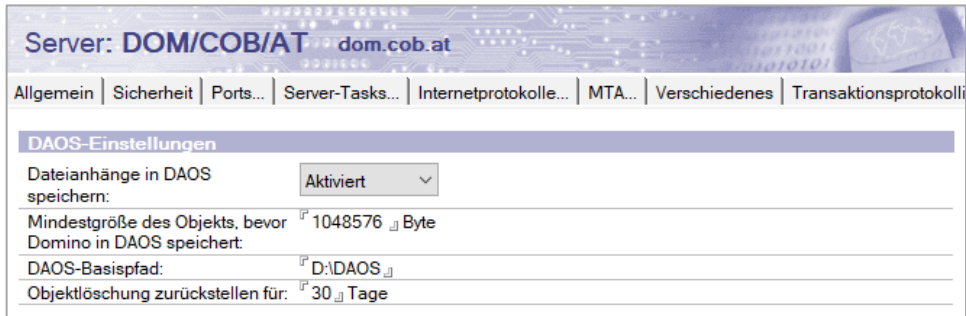


Abbildung 9.24: Das Register DAOS im Serverdokument

4. Wählen Sie im Feld **Dateianhänge in DAOS speichern** die Option »Aktiviert«.
5. Geben Sie im Feld **Mindestgröße des Objekts, bevor Domino in DAOS speichert**, die Mindestgröße in Bytes ein.
Bewährt haben sich Werte zwischen ein und zwei Megabyte. Bei kleineren Anhängen lohnt sich der Rechenaufwand kaum, weil dabei nur wenig Platz eingespart wird.
6. Geben Sie im Feld **DAOS-Basispfad** den Pfad zum vorgesehenen Verzeichnis ein. Das Verzeichnis sollte außerhalb des Domino-Datenverzeichnisses liegen, im Idealfall auf einem anderen Laufwerk.
7. Im Feld **Objektlöschung zurückstellen für n Tage** definieren Sie, wie lange ein Objekt im DAOS behalten wird, nachdem die letzte Referenz darauf gelöscht wurde. Geben Sie eine Zahl zwischen 0 und 9999 ein.
8. Speichern und schließen Sie das Dokument.
9. Starten Sie den Server neu, damit die neue Konfiguration wirksam wird.

Überlegen Sie nach dem Neustart, welche Datenbanken für den DAOS aktiviert werden sollen. Da dies mit einer Komprimierung verbunden ist, müssen die Datenbanken offline genommen werden können. Um eine Datenbank für den DAOS zu aktivieren, verwenden Sie den folgenden Befehl:

```
load compact <Datenbank oder Verzeichnis> -C -DAOS ON
```

Um die Aktivierung für den DAOS wieder aufzuheben und die Anhänge in die Dokumente zurückzuführen, verwenden Sie den Befehl:

```
load compact <Datenbank oder Verzeichnis> -C -DAOS OFF
```

Nach der Aktivierung des DAOS sehen Sie die wahre Größe der Datenbank nur noch im Domino-Administrator auf dem Register Dateien; dort gibt es zwei Spalten für die logische und physische Größe. Unter **logischer Größe** versteht man die Größe, die die Datei hätte, wenn alle Anhänge noch enthalten wären, und unter der **physischen Größe** die tatsächliche Größe der Datenbank im Dateisystem:





	Titel	Dateiname	Physischer Pfad	Dateiformat	Logische Größe	Physische Größe
	Maria Berger	maria.nsf	D:\Domino\mail\maria.nsf	R10 (53:0)	571.271.524	215.482.368
	Isodor Schmied	isidor.nsf	D:\Domino\mail\isidor.nsf	R10 (53:0)	56.360.960	56.360.960
	Susanne Meier	smeier.nsf	D:\Domino\mail\smeier.nsf	R10 (53:0)	15.466.496	15.466.496
	Otto Huber	otto.nsf	D:\Domino\mail\otto.nsf	R10 (53:0)	22.806.528	22.806.528

Abbildung 9.25: Logische und physische Größe

Falls Sie eine AntiVirus-Lösung am Server einsetzen, nehmen Sie unbedingt das Scannen von NLO-Dateien aus!

Der Befehl `show server` zeigt Ihnen, ob der DAOS derzeit auf dem Server aktiviert ist. Die folgenden drei Ausgaben sind möglich:

Not enabled (Nicht aktiviert)	Der DAOS ist derzeit auf diesem Server deaktiviert und wurde noch nicht aktiviert. Es existieren keine Dateianhänge im DAOS-Speicher und alle Anhänge sind in Dokumenten gespeichert.
Read only (Nur lesen)	Der DAOS ist derzeit auf diesem Server deaktiviert. Da der DAOS aber bereits aktiviert war, sind Dateianhänge im DAOS-Speicher vorhanden und werden beim Dokumentabruf gelesen. Neue Anhänge werden jedoch ausschließlich in Dokumenten gespeichert.
Enabled (Aktiviert)	Der DAOS ist derzeit auf diesem Server aktiviert. Alle Anhänge in für den DAOS aktivierten Datenbanken werden ausschließlich im DAOS-Repository gespeichert.

Tabelle 9.12: Status des DAOS-Managers

9.12.6. Der DAOS-Manager

Der Servertask **DAOS-Manager** (DAOSMgr) stellt Befehle zum Abfragen von Informationen und zur Wartung des DAOS-Speichers zur Verfügung. Er verwaltet außerdem den DAOS-Katalog (daoscat.nsf), der Informationen über NLO-Dateien zur schnelleren Abfrage bereitstellt.

Befehl	Ergebnis
<code>tell daosmgr quit</code>	Stoppt den DAOS-Manager-Prozess, räumt auf und beendet den Prozess
<code>tell daosmgr help</code>	Listet DAOS-Manager-Optionen auf
<code>tell daosmgr status</code>	Zeigt den DAOS-Status an
<code>tell daosmgr status <Datenbank></code>	Zeigt den DAOS-Status einer bestimmten Datenbank an
<code>tell daosmgr status catalog</code>	Zeigt den Status des DAOS-Katalogs an
<code>tell daosmgr dbsummary</code>	Zeigt den Status aller für den DAOS aktivierten Datenbanken an
<code>tell daosmgr databases</code>	Zeigt den Status aller für den DAOS aktivierten Datenbanken mit zusätzlichen Informationen an, z. B. die letzte Resynchronisierung einer Datenbank
<code>tell daosmgr listnlo <Datenbank.nsf></code>	Listet DAOS-Objekte (NLO-Dateien) im DAOS-Speicher auf. Damit kann ein Administrator die zur Sicherung nötigen Objekte identifizieren und an ein Sicherungsprogramm

Befehl	Ergebnis
	weitergeben bzw. bei einer Wiederherstellung die fehlenden Objekte identifizieren. Mit dem Parameter -o kann eine Ausgabedatei spezifiziert werden, mit ALL oder MISSING werden alle oder nur fehlende Objekte aufgelistet. Beispiel: tell daosmgr listnlo -o nlo.txt MISSING <Datenbank.nsf>
tell daosmgr prune <Tage>	Wird »0« angegeben, werden per sofort alle unreferenzierten Objekte aus DAOS gelöscht. Wird eine andere Zahl angegeben, werden alle unreferenzierten Objekte aus DAOS gelöscht, die älter sind die Zahl. Ohne dem Argument <Tage> wird die aktuelle Einstellung aus dem Serverdokument angezeigt.
tell daosmgr resync	Führt eine Synchronisierung der für den DAOS aktivierten Datenbanken mit dem DAOS-Katalog durch. Eine Resynchronisierung ist erforderlich, wenn die DAOS-Referenzzähler neu berechnet werden müssen, etwa bei einer Datenbankwiederherstellung oder bei der Löschung einer Datenbank über das Betriebssystem. Wenn eine Unstimmigkeit zwischen den Referenzzählern im DAOS-Katalog und der tatsächlichen Anzahl gefundener Objekte festgestellt wird, lässt der DAOS das Löschen (Pruning) von Anhangsobjekten nicht zu, bis er synchronisiert wird.
tell daosmgr resync force	Führt eine Resynchronisierung aus, unabhängig davon, ob der DAOS-Katalog einen synchronisierten Status besitzt.
tell daosmgr resync quick	Führt eine schnelle Resynchronisierung aus, ohne die Referenzzähler für NLO-Dateien zu aktualisieren. Der Katalog verbleibt dabei im RESYNCING-Zustand, ist aber funktionsfähig, Nach einer schnellen Resynchronisierung wird eine vollständige Resynchronisierung benötigt, damit der Prozess abgeschlossen und die Referenzzähler aktualisiert werden.

Tabelle 9.13: Die Befehle des DAOS-Managers

Achtung: Wenn Sie für gelöschte Objekte keine Sicherungskopie erstellt haben, können Sie diese bei der Rücksicherung einer Datenbank möglicherweise nicht wiederherstellen.

9.12.7. Den DAOS deaktivieren

Wollen Sie die DAOS-Aktivierung für einzelne Datenbanken aufheben und die Anhänge aus dem DAOS-Speicher in die Dokumente zurückführen, verwenden Sie den Befehl:

```
load compact <Datenbank oder Verzeichnis> -C -DAOS OFF
```

Dabei darf die Größe der resultierenden Datenbank 255 GB nicht überschreiten, d. h. bei sehr großen Datenbanken können Sie die DAOS-Aktivierung nicht aufheben, ohne zuvor Anhänge zu löschen.

Wollen Sie den DAOS auf dem Server komplett deaktivieren, öffnen Sie das Serverdokument, wechseln zum Register **DAOS** und wählen im Feld **Dateianhänge in DAOS speichern** die Option

»Deaktiviert«. Nach einem Neustart des Servers werden neue Anhänge wieder ausschließlich in Dokumenten (Mails) gespeichert. Dateianhänge, die bereits im DAOS-Speicher liegen, werden beim Dokumentabruf aber weiterhin gelesen. Der DAOS befindet sich jetzt im Nur-Lese-Modus (Read Only).

9.12.8. Den DAOS-Speicher verschieben

Wenn der zusätzliche Speicherplatz auf der aktuellen Festplatte begrenzt ist, können Sie das DAOS-Verzeichnis auf eine separate Festplatte mit mehr Speicherplatz verschieben. Analog können Sie ein aufgrund eines Hardwareproblems beschädigtes DAOS-Verzeichnis auf einem anderen Laufwerk neu erstellen und die fehlenden Dateien aus einer Sicherung an den neuen Speicherort kopieren. Gehen Sie dazu wie folgt vor:

1. Klicken Sie im Domino-Administrator auf das Register **Konfiguration** und erweitern Sie den Abschnitt **Server**.
2. Bearbeiten Sie das gewünschte Serverdokument und wechseln Sie zum Register **DAOS**.
3. Geben Sie im Feld **DAOS-Basispfad** das neue Verzeichnis an und speichern und schließen Sie das Serverdokument.
4. Beenden Sie den Domino-Server.
5. Erstellen Sie das im Serverdokument angegebene Verzeichnis und verschieben Sie die DAOS-Ordner mit den enthaltenen Dateien dorthin.
6. Aktualisieren Sie die Variable `DAOSBasePath` in der Datei `notes.ini` des Servers.
7. Suchen Sie in der Datei `daos.cfg` im Domino-Datenverzeichnis nach der Variable `PATH=` und ändern Sie diese auf den neuen Speicherort. Speichern und schließen Sie die Datei.
8. Starten Sie den Domino-Server.

9.12.9. DAOS-Tier 2-Speicher

Mit dem DAOS-Tier-2-Speicher können Sie einen S3-kompatiblen Speicherdienst verwenden, um ältere Anhangsobjekte zu speichern, auf die innerhalb einer bestimmten Anzahl von Tagen nicht zugegriffen wurde. Mit dieser Funktion können Sie die Datenmenge reduzieren, die auf Domino-Servern gespeichert ist, die DAOS verwenden. Es kann auch die Leistung von inkrementellen Datensicherungen verbessern.

Ein S3-kompatibler Speicherdienst verwendet die S3-API (Simple Storage Service) von Amazon Web Services (AWS). Die folgenden S3-kompatiblen Speicherdienste werden unterstützt:

- > AWS S3
- > IBM Cloud Object Storage
- > MinIO

Der DAOS-Tier 2-Speicher ist nur für Domino-Server verfügbar, die auf Windows- und Linux-Plattformen ausgeführt werden.

Zum Einrichten eines DAOS-Tier 2-Speichers wenden Sie sich an die Produktdokumentation des Herstellers unter: https://help.hcltechsw.com/domino/11.0.1/admin/admn_daos_t2.html

9.13. Datenbanken verschieben

9.13.1. Händisches Verschieben einzelner Dateien

Einzelne Datenbanken können Sie leicht händisch verschieben, indem Sie zuerst eine Replik auf einem anderen Domino-Server erstellen und anschließend die ursprüngliche Datei löschen.

Doch was passiert nach dem Verschieben mit den Client-Referenzen (Datenbanksymbole und Le-sezeichen), die auf die gelöschte Datenbank verweisen? – Diese führen dann ins Leere! Deshalb sollten Sie bei einem händischen Verschieben auch händisch dafür sorgen, dass die Client-Referenzen korrigiert werden. Das können Sie entweder vor dem Löschen über eine **Datenbankumleitung** bewerkstelligen oder beim Löschen direkt im Löschdialog.

9.13.1.1. Erstellen einer Datenbankumleitung

Um eine Datenbankumleitung zu erstellen, gehen Sie wie folgt vor:

1. Erstellen Sie die Replik auf dem neuen Server.
2. Markieren Sie im Domino-Administrator auf dem Register **Dateien** die ursprüngliche Datenbank und wählen in den Werkzeugen den Befehl **Datenbank > Umleitung erstellen...**
3. Der Dialog **Datenbankumleitung erstellen** wird angezeigt:

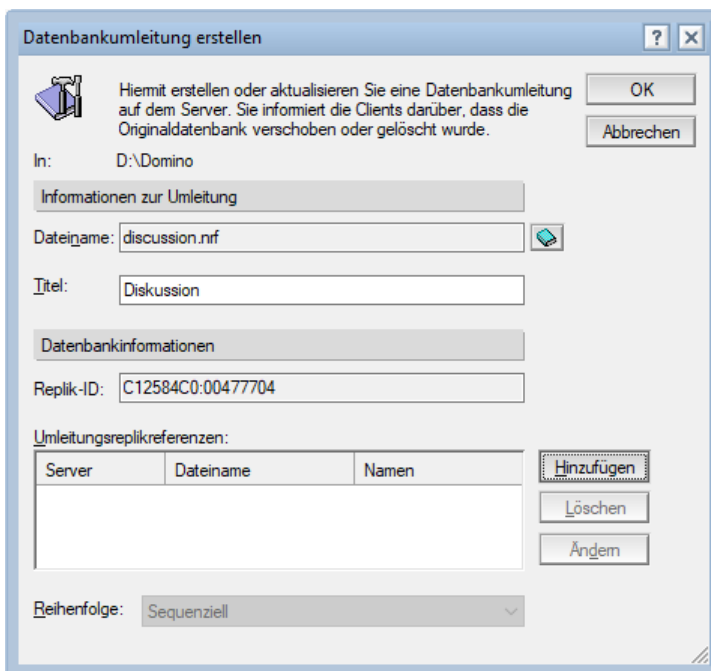


Abbildung 9.26: Dialog Datenbankumleitung erstellen

4. Klicken Sie auf **Hinzufügen** und wählen Sie die Replik auf dem anderen Server.
5. Der Dialog **Umleitungsreplikreferenz konfigurieren** wird angezeigt:

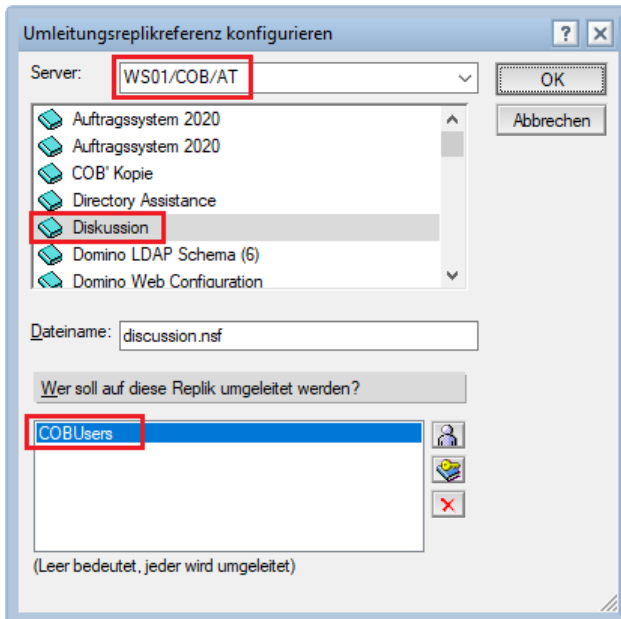


Abbildung 9.27: Dialog Umleitungsreplikreferenz konfigurieren

6. Geben Sie an, wer zur Replik auf dem anderen Server umgeleitet werden soll. Geben Sie niemanden an, werden alle umgeleitet.
7. Klicken Sie auf **OK**. Sie gelangen zum Dialog **Datenbankumleitung erstellen** zurück:

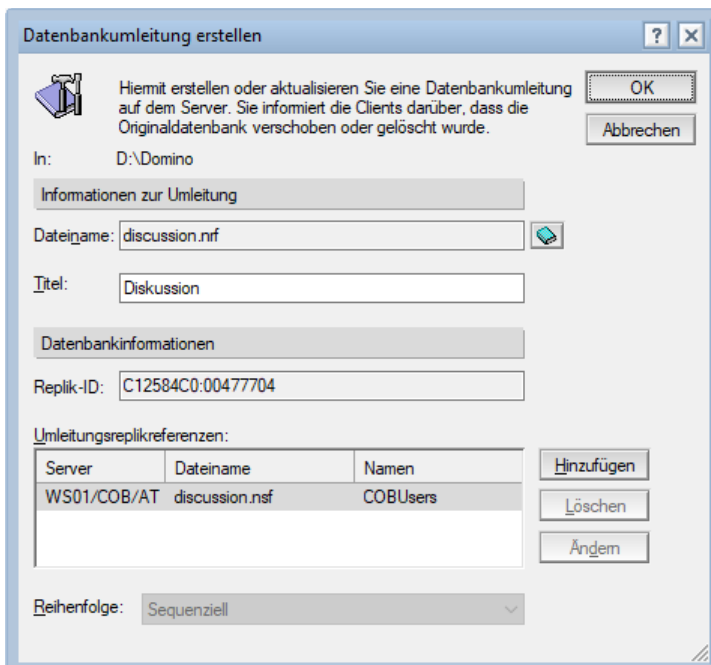


Abbildung 9.28: Dialog Datenbankumleitung erstellen nach Auswahl der Zieldatenbank

8. Klicken Sie auf **OK**.

9. Löschen Sie die ursprüngliche Datenbank. Die Umleitung funktioniert erst, wenn die ursprüngliche Datenbank nicht mehr vorhanden ist.

Die Informationen für die Umleitung holt Domino aus einer Datei mit demselben Dateinamen wie die gelöschte Datenbank, aber der Endung *.nrf (Notes Redirect File). Die NRF-Datei hat in unserem Beispiel folgenden Inhalt:

```
[NotesRedirectFile]
Order=Sequential
RepID=C12584C0:00477704
Title=Diskussion
Ref=CN=WS01/O=COB/C=AT!!discussion.nsf;COBUsers
```

9.13.1.2. Erstellen einer Datenbankumleitung über den Löschdialog

1. Erstellen Sie die Replik auf dem anderen Server.
2. Navigieren Sie im Domino-Administrator zum Register **Dateien** und markieren Sie die ursprüngliche Datenbank.
3. Wählen Sie in den Werkzeugen den Befehl **Datenbanken > Löschen...**
4. Setzen Sie im angezeigten Dialog ein Häkchen bei **Markierung erstellen, wodurch Clients ihre Referenzen auf diese Datenbank aktualisieren können**.
5. Aktivieren Sie außerdem die Option **Clients auf folgenden Server umleiten** und wählen Sie den Server aus, auf dem Sie die Replik erstellt haben.

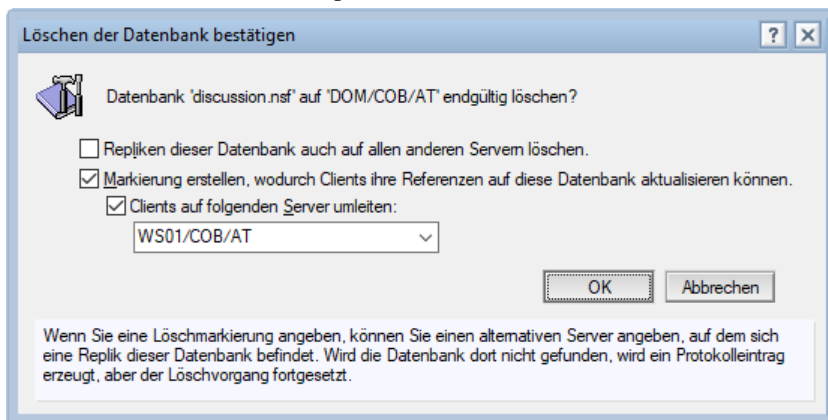


Abbildung 9.29: Dialog Löschen der Datenbank bestätigen

6. Klicken Sie auf **OK**.

Wollen Sie keine Umleitung erstellen, sondern nur eine Markierung hinterlassen, die den Benutzern mitteilt, dass die Datei gelöscht wurde, und die Client-Referenz anschließend entfernt, setzen Sie im angezeigten Dialog nur das Häkchen bei **Markierung erstellen, wodurch Clients ihre Referenzen auf diese Datenbank aktualisieren können** und klicken Sie auf **OK**.

Die automatisch generierte NRF-Datei hat nun folgenden Inhalt:

```
[NotesRedirectFile]
Type=Delete
```

9.13.2. Verschieben von Datenbanken über AdminP

Müssen Sie viele Datenbanken verschieben, beauftragen Sie besser den Administrationsprozess. Dieser ändert für Sie auf Wunsch auch die Dateinamen und erstellt Umleitungsmarkierungen zum Aktualisieren von Client-Referenzen. Navigieren Sie dazu im Domino-Administrator zum Register **Dateien** und markieren Sie die gewünschten Datenbanken der Reihe nach. Wählen Sie dann das Werkzeug **Datenbanken > Verschieben...**

Innerhalb desselben Servers können Sie das Werkzeug Verschieben (Move) auch dazu verwenden, um Datenbanken umzubenennen. Verschieben Sie Maildatenbanken, erkennt das Domino und wandelt die Anforderung in ein Verschieben des Benutzers um (siehe Kap. 6.9 Benutzer verschieben, ab Seite 171), womit auch die Mailfelder im Personendokument und in der lokalen Arbeitsumgebung korrigiert werden.

9.13.3. Auslagern von Datenbanken über Datenbank-Links

Geht es Ihnen darum, Platz zu schaffen, können Sie einzelne große Datenbanken auch auf ein anderes Laufwerk (also aus dem Domino-Datenverzeichnis heraus) verschieben. Dazu verwenden Sie einen **Datenbank-Link** (Datenbankverknüpfung).

Wählen Sie im Admin-Client im Register **Dateien** in den Werkzeugen den Befehl **> Ordner > Neuer Link**. Der Dialog **Neuen Link erstellen** wird angezeigt:

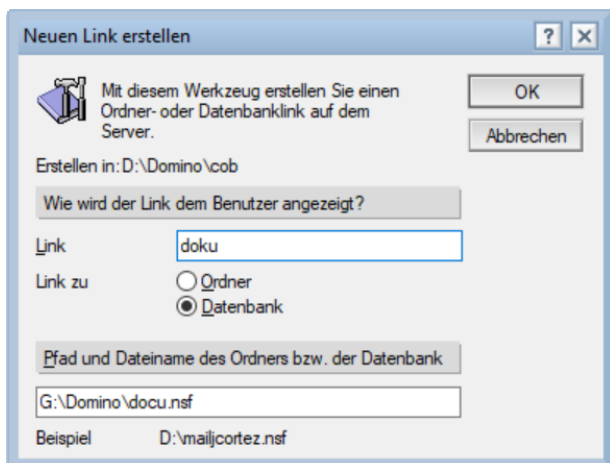


Abbildung 9.30: Dialog Neuen Link erstellen – Datenbank

Wählen Sie im Feld **Link zu** die Option »Datenbank« und geben Sie ein, welcher Dateiname angezeigt werden soll (die Endung *.nsf wird automatisch ergänzt). Geben Sie anschließend den kompletten Pfad zur Zieldatenbank ein. Da der Pfad beim Klicken auf **OK** überprüft wird, müssen Sie die Datenbank zuvor bereits an den Zielort kopiert haben.

9.13.4. Auslagern von Verzeichnissen über Ordner-Links

Wenn das Verschieben einzelner Datenbanken nicht ausreicht, können Sie auch ganze Ordner auslagern.

1. Markieren Sie dazu das Verzeichnis, in dem der neue Ordner eingeblendet werden soll.
2. Wählen Sie in den Werkzeugen den Befehl **Ordner > Neuer Link**.

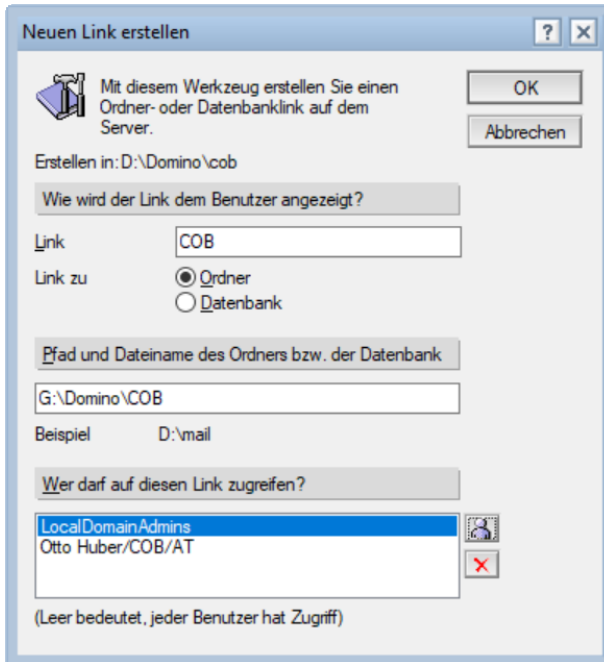


Abbildung 9.31: Dialog Neuen Link erstellen – Ordner

3. Wählen Sie im Feld **Link zu** die Option »Ordner«.
4. Geben Sie an, welcher Name für den neuen Ordner angezeigt werden soll, und verweisen Sie auf den Zielordner am anderen Laufwerk.
5. Geben Sie im Bereich **Wer darf auf diesen Link zugreifen?** an, wer den Ordner sehen darf. Wählen Sie niemanden aus, sehen alle den Ordner, wählen Sie Personen oder Gruppen aus, können ihn nur noch diese sehen.
6. Klicken Sie auf **OK**.

9.14. Benutzeraktivitäten überwachen

Sie sollten regelmäßig die Verwendung von Datenbanken überwachen, um rechtzeitig Leistungsprobleme aufzuspüren. Dazu steht das Werkzeug **Benutzeraktivität** zur Verfügung. Es zeigt jeden Datenbankbenutzer (Person oder Server) und wie viele Dokumente er während jeder Sitzung gelesen oder geschrieben hat.

Die Benutzeraktivität können Sie in den Datenbankeigenschaften oder in der Protokolldatei (log.nsf) einsehen.

Rufen Sie (etwa mit [Alt] + [Eingabe]) die Datenbankeigenschaften auf und klicken Sie auf dem Register **Info** auf die Schaltfläche **Benutzerdetail**:

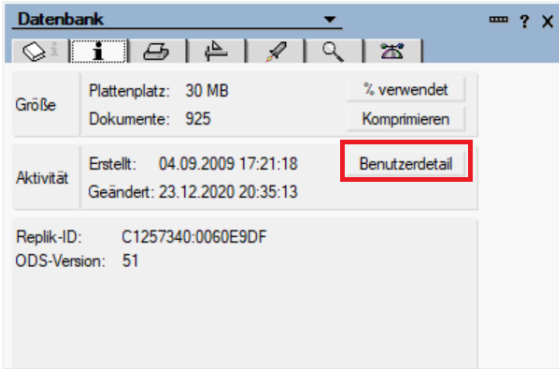


Abbildung 9.32: Datenbankeigenschaften – Benutzeraktivität aufrufen

Die Aktivitäten werden im Dialog **Benutzeraktivität** aufgelistet:

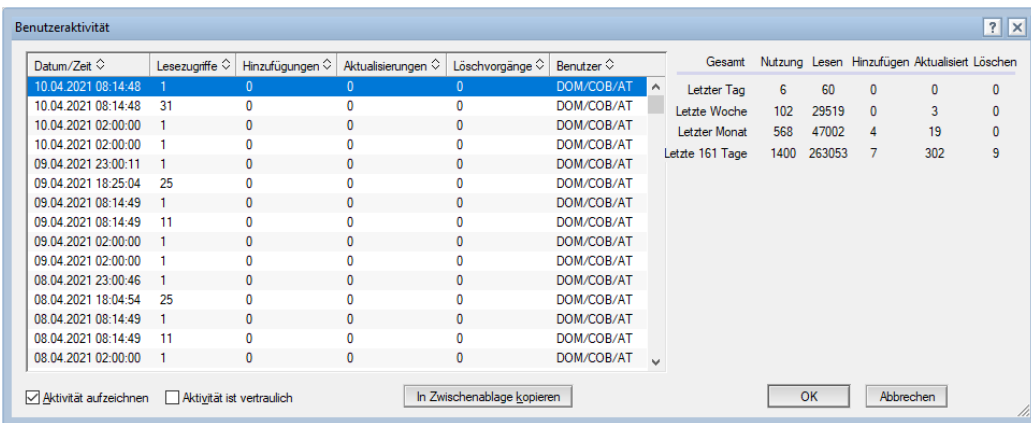


Abbildung 9.33: Der Dialog Benutzeraktivität

Wie in Abbildung 9.33 dargestellt, werden Datum und Uhrzeit, der Benutzer- oder Servername und die Aktivität selbst (Lesezugriffe, Hinzufügen, Aktualisierungen und Löschungen) aufgelistet.

In der Protokolldatei finden Sie Datenbankaktivitäten in den Ansichten **Benutzung** und **Datenbank**.

9.14.1.1. Die Aktivitätsaufzeichnung in Datenbanken steuern

Für das Aufzeichnen von Datenbankaktivitäten ist das Programm **Statistik Logging** (Statlog) zuständig. Per Vorgabe läuft der Task einmal täglich um 5 Uhr, beim ersten Start von Statlog wird die Aktivitätsaufzeichnung für alle Datenbanken aktiviert.

In dem in Abbildung 9.33 dargestellten Dialog können Sie durch Entfernen des Häkchens bei **Aktivität aufzeichnen** die Aufzeichnung zwar deaktivieren, diese wird beim nächsten Start von Statlog aber automatisch wieder aktiviert. Um Statlog anzuweisen, die Aufzeichnung nicht automatisch wieder zu aktivieren, fügen Sie zur Datei notes.ini die folgende Variable hinzu:

No_Force_Activity_Logging=1

Erst danach können Sie die automatische Aufzeichnung im Dialog Benutzeraktivität bleibend deaktivieren. (Die Protokollierung in die Datei log.nsf bleibt jedoch aufrecht.)

Bei aktivierter Aufzeichnung werden zur Datenbankgröße 64 K hinzugefügt.

Deaktivieren Sie die Aufzeichnung bei schlechter Datenbankperformance.

9.15. Dokumentlöschungen protokollieren

Das Löschen von Dokumenten kann ab Version 10 für ausgewählte Datenbanken auf dem Server protokolliert werden. Voraussetzung dafür ist allerdings das Einrichten eines Transaktionsprotokolls. Mit Löschprotokollen lässt sich zurückverfolgen, wer Dokumente gelöscht hat und wann, gelöschte Dokumente lassen sich jedoch nicht wiederherstellen. Das Löschprotokoll wird auf dem Server im Verzeichnis IBM_TECHNICAL_SUPPORT unter dem Namen delete.log angelegt.

Nach jedem Serverstart wird ein neues Löschprotokoll erstellt. Das alte Löschprotokoll wird in delete_<Servername>_yyyy_mm_dd@hh_mm_ss.log umbenannt; z. B. in:

delete_DOM_2020_03_24@10_28_45.log

Wenn ein Dokument aus einer Datenbank gelöscht wird, werden die folgenden Daten im CSV-kompatiblen Format ins Löschprotokoll geschrieben:

Daten pro Protokolleintrag	Erklärung
Datum und Zeit der Löschung	
Datenbankpfad	Relativ zum Datenverzeichnis
Replik-ID der Datenbank	
Prozess, der die Löschung ausgeführt hat	Zum Beispiel: nserver dbmt replica
Name des Servers oder der Person	
Art der Löschung	SOFT – Dokument ist im Papierkorb HARD – Dokument aus Datenbank gelöscht RESTORE – Dokument wurde aus dem Papierkorb wiederhergestellt
Klasse des Dokuments	Einer der folgenden HEX-Werte: 0001 (Dokument – NOTE_CLASS_DATA) 0002 (Dokument »Über die Datenbank« – NOTE_CLASS_INFO) 0004 (Maske – NOTE_CLASS_FORM)
UNID	Die Dokument-Unique-ID
Zusätzliche Felder	Bis zu vier zusätzliche Felder, um die Identifizierung des Dokuments zu erleichtern.

Tabelle 9.14: Aufbau des Löschprotokolls

9.15.1.1. Das Löschprotokoll aktivieren

Die Aktivierung erfolgt auf Datenbankebene. Um die Protokollierung für Dokumentlöschungen für eine bestimmte Datenbank zu protokollieren, geben Sie den folgenden Befehl ein:

```
load compact <Pfad> -dl on "<Feldliste>"
```

<Pfad> ist eine Datenbank oder ein Unterverzeichnis relativ zum Server-Datenverzeichnis.

<Feldliste> enthält eine durch Kommas getrennte Liste von max. vier Feldern, die zusätzlich ins Protokoll aufgenommen werden. Erlaubte Feldtypen sind: Text, Text_List, RFC822_Text oder Datum/Zeit. Beispiel:

```
lo compact projects.nsf -dl on "Subject,Categories"
```

Hier ein Beispiel für ein Löschprotokoll:

```
"20200402T170641,73+02","projects.nsf","C125853E:004E5EAE","nserver","CN=Christian  
Buchacher/O=COB/C=AT","HARD","0001",  
"61AA4F13:71AD95A7C1257579:006BBC5D","Subject","13","Collaboration","Categories","12",  
"Definitionen"
```

```
"20200402T170908,58+02","projects.nsf","C125853E:004E5EAE","nserver","CN=Christian  
Buchacher/O=COB/C=AT","HARD","0001",  
"81B6A49C:991E52F1C1257374:005D9857","Subject","11","TeamMailbox","Categories",  
"10","Schablonen"
```

9.15.1.2. Die Löschprotokollierung deaktivieren

Um die Löschprotokollierung aufzuheben, geben Sie auf der Serverkonsole folgenden Befehl ein:

```
load compact <Pfad> -dl off
```

<Pfad> ist eine Datenbank oder ein Unterverzeichnis relativ zum Server-Datenverzeichnis.

9.16. Der Datenbankkatalog

Beim Datenbankkatalog (catalog.nsf) handelt es sich um eine spezielle Notes-Datenbank, die ein Verzeichnis aller Datenbanken und ihrer Repliken innerhalb der Domäne enthält.

Der Datenbankkatalog wird vom **Catalog-Task** erstellt und aktualisiert. Standardmäßig erfolgt das jeden Morgen um 1:00 (Zeile ServerTasksAt1 in der Datei notes.ini).

Werden beispielsweise Datenbanken auf einen anderen Server verlagert, aktualisiert der Katalogdienst die Einträge für diese Datenbanken mit dem neuen Speicherort.

Sie können in den Datenbankeigenschaften festlegen, unter welchen Kategorien die Datenbank aufscheint, beziehungsweise das Anzeigen der Datenbank im Katalog auch ganz verhindern:

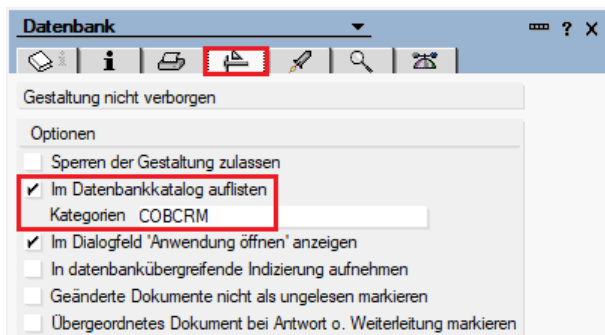


Abbildung 9.34: Datenbankeigenschaften, Register Gestaltung

9.16.1. Den Catalog-Task händisch starten

Geben Sie auf der Serverkonsole den folgenden Befehl ein:

```
load catalog
```

Der Katalog nimmt nur dann serverübergreifende Datenbankinformationen auf, wenn jeder Server eine Replik des Katalogs besitzt, auf die er Managerzugriff hat. Damit die Datenbank `catalog.nsf` automatisch replizieren kann, verwendet sie die Replik-ID des Domino-Verzeichnisses und tauscht eine Ziffer aus (07 statt 00 nach dem Doppelpunkt).

10. Replikation

- > 10.1 Übersicht, Seite 293
- > 10.2 Eine neue Replik erstellen, Seite 297
- > 10.3 Datenbanken replizieren, Seite 300
- > 10.4 Eine automatische Replizierung einrichten, Seite 301
- > 10.5 PIRC, Seite 303

10.1. Übersicht

Unter Replikation versteht man die Methode, Notes-Datenbanken miteinander abzugleichen. Die Datenbanken können dabei auf zwei Servern oder auch auf einem Client und einem Server liegen, einzig die Replikation zwischen zwei Notes-Clients ist nicht möglich. Der Abgleich umfasst (fast) alles, was innerhalb der Datenbank liegt, also geänderte, hinzugefügte oder gelöschte Dokumente, Änderungen in Ansichtsindizes, die Zugriffskontrollliste und die Gestaltung – nicht aber das Datenbankformat (ODS), Größenbeschränkungen und der Volltextindex.

Zwischen zwei Rechnern werden ausschließlich Datenbanken repliziert, die dieselbe Replik-ID aufweisen (Datenbanktitel und Dateiname spielen keine Rolle) – was es einem Domino-Administrator ermöglicht, die Datenbanken beliebig in Unterverzeichnisse zu verschieben, ohne die Replikationsfähigkeit dadurch zu beeinträchtigen. Pfadangaben sind also nur am Quellserver relevant, am Zielserver wird die Datenbank anhand der Replik-ID identifiziert.

Was genau repliziert wird, bestimmen einerseits die Repliziereinstellungen und andererseits die Rechte. Sind alle Rechte vorhanden, werden neue und geänderte Dokumente sowie Löschungen übertragen. In den Repliziereinstellungen kann auch der Abgleich nur eines Teils der Daten konfiguriert werden (Selektive Replikation).

Der Replikationsmechanismus erkennt Änderungen auf Feldebene und überträgt nur die geänderten Feldinhalte. Dadurch wird die zur Verfügung stehende Netzwerk-Übertragungskapazität effizient genutzt.

Kommen wir nun zu den einzelnen Komponenten der Replikation.

10.1.1. Replik-ID

Die Replik-ID (Replica ID) ist ein Code, der jede Replik kennzeichnet. Da es auf einem Server mehrere Datenbanken mit derselben Replik-ID geben kann (mit unterschiedlichen Dateinamen oder in unterschiedlichen Verzeichnissen) handelt es sich hierbei jedoch nicht um eine eindeutige Datenbankkennung. Beim Replizieren werden »gleiche« Datenbanken anhand dieser Replik-ID identifiziert, Datenbanken mit unterschiedlichen Replik-IDs können nicht miteinander replizieren.

Die Replik-ID kann über die Eigenschaften der Datenbank im Register **Info** eingesehen werden:

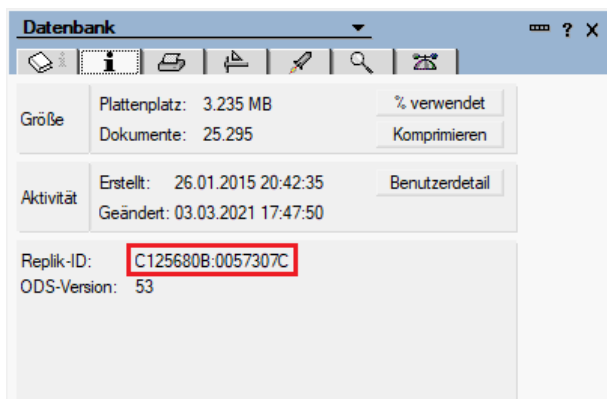


Abbildung 10.1: Datenbankeigenschaften, Register **Info**

10.1.2. Replik

Eine Kopie einer Datenbank mit derselben Replik-ID nennt man Replik (Replica). Repliken können miteinander replizieren. Eine neue Replik wird über den Befehl **Datei > Replizierung > Neue Replik...** erstellt. Natürlich erzeugt man auch eine Replik, wenn man eine Datenbank auf Betriebssystemebene kopiert.

10.1.3. Kopie

Kopien einer Datenbank mit unterschiedlichen Replik-IDs können nicht miteinander replizieren. Eine neue Kopie erzeugt man über den Befehl **Datei > Anwendung > Neue Kopie...**

10.1.4. Servertask Replikator

Der Servertask **Replikator** (Replica) führt die Replikation zwischen zwei Servern durch, nicht jedoch zwischen Client und Server. Er wird standardmäßig beim Hochfahren des Domino-Servers geladen. Dafür zuständig ist folgender Eintrag in der Datei notes.ini:

```
ServerTasks=<Andere Servertasks...>,Replica
```

Der Replikator ist ein sogenannter »Single-threaded-Task«, d. h. er kann gleichzeitig nur eine Replikations Sitzung zwischen zwei Servern ausführen. Wenn Sie Verbindungsdokumente erstellen, die einen Server für mehrere gleichzeitige oder überlappende Replikationen mit verschiedenen Zielseverern planen, kann der Replikator fünf weitere Anforderungen in eine Warteschlange stellen und verzögert abarbeiten, der sechste geht verloren. Richten Sie in diesem Fall besser mehrere Replikatoren ein, um Replikationssitzungen gleichzeitig durchzuführen und Replikationszyklen zu verkürzen. Sie können mehrere Replikatoren gleichzeitig laden, etwa durch folgenden Aufruf in der Datei notes.ini:

```
ServerTasks=<Andere Servertasks...>,Replica,Replica,Replica
```

Oder Sie bleiben in der Zeile ServerTasks bei einem einzigen Aufruf und setzen zusätzlich die Zeile:

```
Replicators=3
```

Es gibt keine hartcodierte Maximalanzahl von Replikatoren, die ein Server ausführen kann, da diese aber relativ viele Ressourcen (vor allem viel Arbeitsspeicher) verbrauchen, laden Sie nur so viele Replikatoren, wie Sie wirklich benötigen.

Die Variable Replicators funktioniert nur, wenn Sie den Task Replica über die Variable ServerTasks gestartet haben. Starten Sie, wie in Kap. 5.3.4.2 Starten aller Servertasks über Programmdokumente, ab Seite 98 vorgeschlagen, die Servertasks über Programmdokumente, müssen Sie für jeden zusätzliche Replikator ein weiteres Programmdokument erstellen.

10.1.5. Replizierkonflikte

Konflikte treten auf, wenn in unterschiedlichen Repliken in denselben Dokumenten dieselben Felder bearbeitet werden. Replizierkonflikte müssen manuell aufgelöst werden, leider gibt es im Notes-Client kein Tool, das Ihnen das abnimmt.

Das Auftreten von Konflikten kann jedoch stark reduziert werden, wenn man einige Regeln einhält!

10.1.5.1. Konfliktbehandlung auf Mischen einstellen

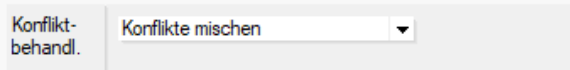


Abbildung 10.2: Konfliktbehandlung in den Maskeneigenschaften, Register **Info**

Wenn in den Maskeneigenschaften im Feld **Konfliktbehandl.** die Option »Konflikte Mischen« aktiviert ist, werden Änderungen in verschiedenen Feldern in ein Ergebnisdokument zusammenge-mischt. Wurden jedoch dieselben Felder bearbeitet, tritt ein Replizierkonflikt auf. Im Domino-Verzeichnis ist die Eigenschaft Mischen in den meisten Masken (wieso eigentlich nicht in allen?) per Vorgabe bereits aktiviert.

10.1.5.2. Nur Autorenrechte vergeben

Der Hauptgrund für Replizierkonflikte sind zu hohe Rechte! Die Benutzer sollten keinesfalls alle Editoren sein, sondern möglichst nur Autoren. (Voraussetzung für das Bearbeiten von Dokumenten für Autoren ist das Vorhandensein von Autorenfeldern – siehe Kap. 13.10.2 Autorenfelder, ab Seite 367.)

10.1.6. Repliziertypen

Eine Replikation ist immer ein Ein-Weg-Prozess. Bei einer Zwei-Weg-Replikation folgen zwei Ein-Weg-Replikationen dicht aufeinander bzw. überlappen einander.

- Pull Pull Der Quellserver holt sich aktiv die Daten vom Zielsever und schreibt sie in seine Replik. Wenn er damit fertig ist, gibt er die Kontrolle an den Zielsever ab, der sich dann die Daten auf dieselbe Weise holt. Es werden also nacheinander die Replika-toren beider Server aktiv.
- Pull Push Nur der Quellserver ist aktiv. Er holt zunächst die Änderungen vom Zielsever (Pull) und schiebt dann seine eigenen Änderungen auf den Zielsever (Push). Dabei schreibt er in die Datenbanken beider Server und der Replikator des Zielsevers bleibt inaktiv.

Nur Pull Nur der Quellserver ist aktiv und holt sich die Änderungen vom Zielserver.

Nur Push Nur der Quellserver ist aktiv und schiebt die Änderungen auf den Zielserver.

10.1.7. Die Server-zu-Server-Replikation

Eine Server-zu-Server-Replikation kann durch eine vorgegebene Zeitplanung oder durch den entsprechenden Befehl auf der Serverkonsole initiiert werden. Der Replikator arbeitet als Servertask, der Daten von einem anderen Server »ziehen« (pull) oder auf einen anderen Server »schieben« (push) kann. Bei der Server-zu-Server-Replikation vom Typ »Pull-Pull« werden die Replikatoren auf beiden Seiten aktiv.

10.1.8. Die Client-zu-Server-Replikation

Das Ergebnis einer Client-zu-Server-Replikation ist dasselbe wie bei einer Server-zu-Server-Replikation, der Replikator des Servers ist daran allerdings nicht beteiligt. Vielmehr zieht die Client-Software selbst die Änderungen vom Server und lädt anschließend lokale Änderungen zum Server hoch. Aus Sicht des Servers stellt sich die Client-zu-Server-Replikation wie ein Benutzerzugriff dar.

Da der Replikator-Task bei der Client-zu-Server-Replikation nicht aktiv wird, wird diese auch nicht in der Protokolldatei des Servers aufgezeichnet.

10.1.9. Replizierprotokoll

Replizieren zwei Datenbanken zum ersten Mal miteinander, wird ein genauer, dokumentweiser Vergleich durchgeführt. Nach erfolgreicher Replikation wird ein Eintrag im Replizierprotokoll (Replication History) erstellt und bei der nächsten Replikation nur noch repliziert, was nach diesem Datum-/Zeitstempel hinzugefügt, geändert oder gelöscht wurde. Diese Vorgangsweise verkürzt den Replikationsprozess, setzt jedoch voraus, dass die Zeiten auf allen Servern exakt übereinstimmen.

Soll wieder eine vollständige Replikation stattfinden, löschen Sie entweder das Replizierprotokoll oder geben Sie auf der Konsole (ab Domino 10) zusätzlich den Parameter -F an:

```
replicate <Server> <Pfad> -F
```

10.1.10. Löschinfos

Würden Dokumente beim Löschen ganz verschwinden, würden sie bei der nächsten Replikation zurückrepliziert werden. Damit das nicht passiert, sondern umgekehrt die Löschung weitergegeben wird, bleibt nach dem Löschen ein Dokumenttrumpf in der Datenbank übrig, die sogenannte **Löschinfo** (Deletion Stub). Löschinfos sammeln sich mit der Zeit in der Datenbank an und müssen regelmäßig entfernt werden. Diese Aufgabe erledigen Programme wie UpdAll (siehe Kap. 9.10.3, ab Seite 272) oder DBMT (siehe Kap. 9.6, ab Seite 256).

Wie lange Löschinfos aufgehoben werden, steuern Sie in den Replizieroptionen. Wählen Sie dazu den Befehl **Datei > Replizierung > Optionen für diese Anwendung...** und navigieren Sie zur Registerkarte **Platzsparer**:

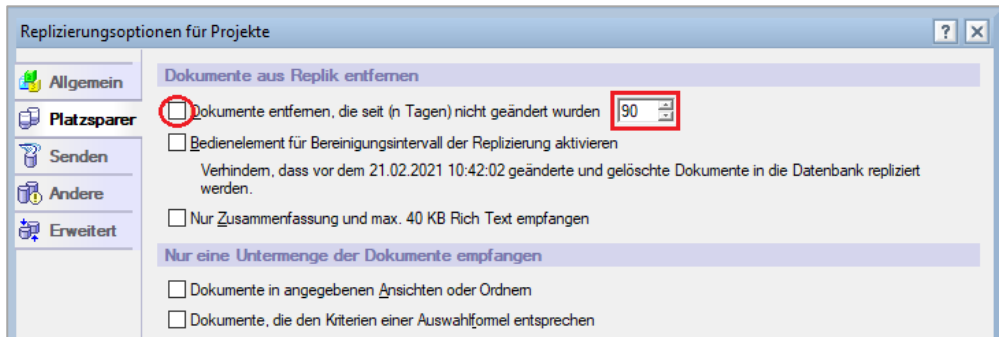


Abbildung 10.3: Replizieroptionen, Register Platzsparer

Standardmäßig werden Löschinfos entfernt, wenn sie älter als 90 Tage sind. Domino prüft nach einem Drittel der eingestellten Zeit, ob alte Löschinfos vorhanden sind. Standardmäßig erfolgt dies also alle 30 Tage. Sollen Löschinfos länger aufgehoben werden, erhöhen Sie die Zahl, z. B. auf 120. Geben Sie die Ziffer 0 ein, werden Löschinfos nicht mehr entfernt.

Achtung: Setzen Sie kein Häkchen, sonst werden Dokumente aus der Datenbank gelöscht, die seit der angegebenen Anzahl von Tagen nicht geändert wurden!

10.2. Eine neue Replik erstellen

Repliken werden bei einer Replikation nicht automatisch erstellt, sondern müssen vom Administrator zuvor händisch angelegt werden. Dazu stehen mehrere Methoden zur Verfügung:

1. im Notes-Client über das Menü **Datei > Replizierung** bzw. Kontextmenü **Replizierung**
2. im Domino-Administrator über das Werkzeug **Datenbank > Replik(en) erstellen**
3. auf der Serverkonsole über den Befehl `c1 copy`
4. auf Betriebssystemebene über das Kopieren einer Datei

10.2.1. Über das Menü

1. Fügen Sie die Datenbank, von der Sie eine Replik erstellen wollen, zuerst zu Ihrem Arbeitsbereich hinzu.
2. Markieren Sie das Datenbanksymbol und wählen Sie entweder **Datei > Replizierung > Neue Replik...** oder klicken Sie mit der rechten Maustaste auf das Datenbanksymbol und wählen Sie **Replizierung > Neue Replik...**
3. Wählen Sie den Server, auf dem die Replik erstellt werden soll oder den Eintrag »Lokal« für eine Replik in Ihrem Client-Datenverzeichnis.
4. Akzeptieren Sie denselben Dateinamen oder vergeben Sie einen anderen.
5. (Optional) Setzen Sie ein Häkchen für **Replik verschlüsseln mit Starker Verschlüsselung**, wenn die Replik verschlüsselt werden soll. Lokale Repliken auf Notebooks sollten immer verschlüsselt werden, auf Servern (hier erfolgt die Verschlüsselung mit der Server-ID) wird von einer Verschlüsselung in der Regel abgesehen.
6. (Optional) Volltextindizes können nicht aus den Quelldatenbanken repliziert werden; wählen Sie **Volltextindex für Suchfunktion erstellen**, wenn ein neuer Volltextindex erstellt werden soll.

Replikation: Eine neue Replik erstellen

7. (Optional) Wählen Sie **Zugriffskontrollliste kopieren**, wenn die Replik die Zugriffsliste der Quelldatenbank erhalten soll.

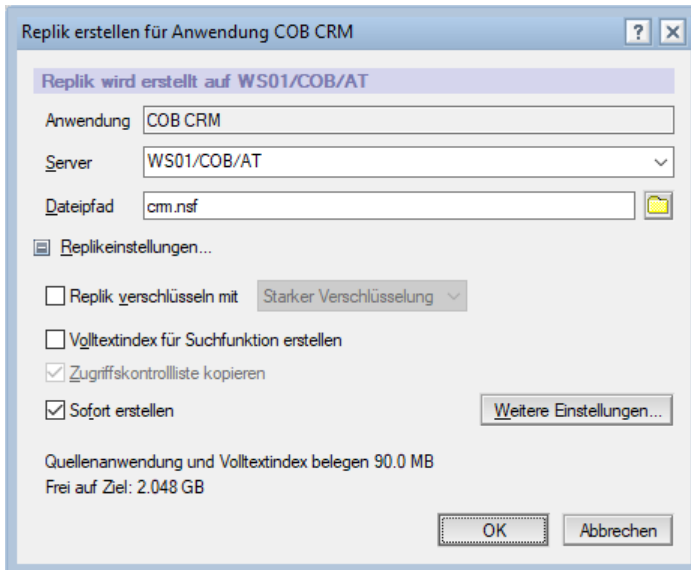


Abbildung 10.4: Der Dialog Neue Replik (**Datei > Replizierung > Neue Replik...**)

8. Setzen Sie ein Häkchen bei **Sofort erstellen** und klicken Sie auf **OK**.

Achtung: Auf Servern dürfen nur jene Benutzer neue Repliken erstellen, die im Serverdokument, Register **Sicherheit** im Feld **Neue Repliken erstellen** eingetragen sind.

10.2.2. Über das Werkzeug Replik(en) erstellen

1. Navigieren Sie im Domino-Administrator zum Register **Dateien** und wählen Sie die Datei, welche repliziert werden soll.
2. Wählen Sie in den Werkzeugen **Datenbank > Replik(en) erstellen...**
3. Der Dialog **Replik erstellen** wird angezeigt. Wählen Sie den Zielservers aus und klicken Sie auf die Schaltfläche **Hinzu(fügen)**.
4. Es ist auch eine Mehrfachauswahl möglich!
5. Klicken Sie bei Bedarf auf den Namen der Zieldatei, um den Dateinamen zu ändern.
6. Klicken Sie auf **OK**.

Der Administrationsprozess wird mit dem Erstellen der Replik(en) beauftragt. Beachten Sie, dass der Administrationsprozess nur sogenannte **Replikrümpfe** (Replication Stubs), also leere Datenbankhüllen mit den entsprechenden Replik-IDs, erstellt. Die Repliken werden bei der nächsten Replikation automatisch vervollständigt. (Die verschiedenen Möglichkeiten, eine Datenbank zu replizieren, beschreibe ich im Kap. 10.3 Datenbanken replizieren, ab Seite 300.)

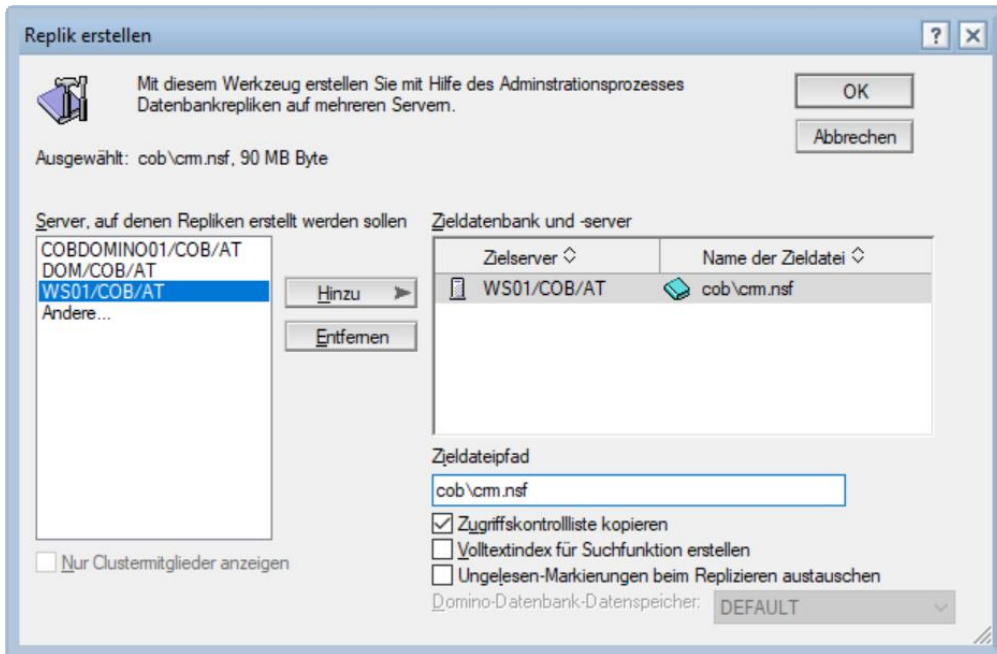


Abbildung 10.5: Replik erstellen

10.2.3. Über den Konsolenbefehl `cl copy`

Der Serverkonsolenbefehl `cl copy` (Cluster Copy) wurde zum Erstellen von Repliken in Clustern eingeführt, funktioniert aber auch ohne Cluster. Voraussetzung ist, dass Sie in der Datei `notes.ini` des Servers die folgende Variable setzen:

```
CLUSTER_ADMIN_ON=1
```

Wenn Sie die Variable über den Konsolenbefehl `set configuration` setzen, ist sie sofort gültig:

```
set configuration CLUSTER_ADMIN_ON=1
```

Sie können nun über das folgende Kommando eine Replik einer Datenbank von Server1 auf Server2 erstellen:

```
cl copy server1!!datenbank.nsf server2!!datenbank.nsf replica
```

Lassen Sie die Anweisung `replica` weg, erstellen Sie eine Kopie, in folgendem Beispiel auf demselben Server:

```
cl copy cob\datenbank.nsf test\datenbank.nsf
```

10.2.4. Lokale Repliken und Rechte

In einer lokalen Replik werden die Zugriffsrechte vom Notes-Client per Vorgabe nicht überprüft und jeder Benutzer ist de facto Manager. Bei der Replikation können allerdings nur Informationen hochgeladen werden, auf die der Benutzer auch am Server das Recht gehabt hätte.

Anders verhält es sich bei Datenbanken mit einer **Konsistenten Zugriffskontrollliste** (siehe auch Kap. 13.8.2 Konsistente , ab Seite 361), hier werden die Zugriffsrechte auch lokal vom Client überprüft. Beim Erstellen einer lokalen Replik werden (unabhängig davon, ob eine Konsistente ACL vorliegt oder nicht) Informationen zu Gruppenmitgliedschaften des aktuellen Benutzers in der Datenbank gespeichert. Für den Ersteller ergeben sich somit lokal dieselben Rechte wie auf dem Server. Wenn eine andere Person als der Ersteller (etwa nach einem Wechsel der ID), auf die lokale Replik zugreift, sind für diese Person keine Informationen zu Gruppenmitgliedschaften verfügbar und die ACL kann zur Überprüfung der Identität der Person nur noch Personeneinträge heranziehen.

10.3. Datenbanken replizieren

Die Replikierung läuft – im Gegensatz zur Mailweiterleitung – auch innerhalb eines Domino-Netzwerks nicht automatisch ab. Zu einer Replikation kommt es nur, wenn:

1. Sie die Replikation im Client händisch anfordern, z. B. über das (Kontext-) Menü oder via **Replikatorseite**.
2. Sie auf der Serverkonsole die Befehle `replicate`, `push` oder `pull` eingeben.
3. es der Zeitplan in einem Verbindungsdokument vorschreibt.

10.3.1. Replizieren über das Datenbanksymbol

Klicken Sie, wenn Sie gestapelte Repliksymbole verwenden, rechts oben auf den Pfeil und wählen Sie **Replizieren...** oder klicken Sie mit der rechten Maustaste auf das Datenbanksymbol und wählen Sie im Kontextmenü **Replikierung > Replizieren...**

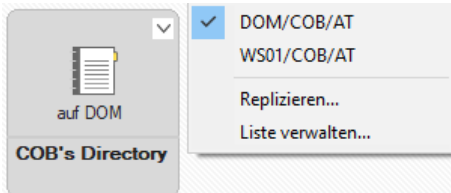


Abbildung 10.6: Gestapelte Repliksymbole im Arbeitsbereich

10.3.2. Replizieren auf der Serverkonsole

Geben Sie den folgenden Befehl auf der Serverkonsole ein:

```
replicate <Server oder Servergruppe> <Pfad>
```

Der Pfad ist optional, geben Sie keinen Pfad an, werden alle gemeinsamen Datenbanken repliziert.

Geben Sie zusätzlich den Parameter `-F` ein, wird eine vollständige Replikation ausgeführt (ab Domino 10):

```
replicate <Server oder Servergruppe> <Pfad> -F
```

Sollten Sie Änderungen nur in eine Richtung übertragen wollen, bietet sich der Befehl `push` an:

```
push <Server oder Servergruppe> <Pfad>
```

Während beim Replizieren im Client immer die Rechte des aktuell angemeldeten Benutzers herangezogen werden, erfolgt die Replikation auf der Konsole mit den Rechten des Servers.

10.4. Eine automatische Replizierung einrichten

10.4.1. Einen Replizierzeitplan erstellen

Das Aufstellen eines Zeitplans erfolgt durch Erstellen eines Verbindungsdokuments.

10.4.1.1. Vorabüberlegungen

Bevor Sie einen Zeitplan für eine Replikation aufstellen, sollten Sie überlegen:

- > welcher Server die Replikation durchführen soll
- > über welchen Anschluss die Replikation stattfindet
- > welche Datenbanken repliziert werden sollen
- > welche Art von Replikation herangezogen werden soll (Pull-Pull, Pull-Push etc.)
- > ob ein Zeitlimit für die Replikation vergeben werden soll

10.4.1.2. Ein Verbindungsdokument erstellen

1. Öffnen Sie das Domino-Verzeichnis und wählen Sie die **Ansicht Konfiguration > Verbindungen**.
2. Klicken Sie auf die Schaltfläche **Verbindung hinzufügen** oder wählen Sie im Menü **Erstellen > Server > Verbindung**.
3. Tragen Sie **Quellserver** und **Zielserver** ein. (Der Quellserver initiiert die Verbindung.) Sollte der Name des Zielservers nicht aufgelöst werden können, geben Sie zusätzlich eine Netzwerkadresse (einen Hostnamen oder eine IP-Adresse) ein.

Sie können als Zielserver auch eine Servergruppe angeben. In diesem Fall müssen alle Gruppenmitglieder über ihre Namen direkt aufgelöst werden können.

4. Geben Sie den benutzten Anschluss ein oder wählen Sie ihn aus der Liste (in unserem Beispiel TCPIP).

The screenshot shows the configuration window for a connection document. The title bar reads 'Serververbindung: DOM/COB/AT zu WEB/COB/AT'. Below the title bar are tabs for 'Allgemein', 'Replizierung/Routing', 'Zeitplan', 'Kommentare', and 'Administration'. The 'Allgemein' tab is selected and contains the following fields:

Verbindungstyp:	Lokales Netzwerk	Benutzungspriorität:	Normal
Quellserver:	DOM/COB/AT	Zielserver:	WEB/COB/AT
Quellendomäne:	COB	Zieldomäne:	COB
Benutzte Ports:	TCPIP	Optionale Netzwerkadresse:	

There is a 'Ports wählen...' button at the bottom left of the 'Allgemein' register.

Abbildung 10.7: Verbindungsdokument, Register Allgemein

5. Wechseln Sie zum Register **Replizierung/Routing** und deaktivieren Sie die Routing-Funktion.

Replikation: Eine automatische Replizierung einrichten

- (Optional) Passen Sie die **Replizierpriorität** an. Per Vorgabe haben alle Datenbanken eine mittlere Priorität. Wählen Sie z. B. »Hoch« aus, um nur noch Datenbanken hoher Priorität zu replizieren.
- Legen Sie den **Replizierungstyp** fest (normalerweise »Pull Push«, d. h. der initiiierende Server übernimmt beide Richtungen).

The screenshot shows a web-based configuration interface for a server connection. The title is 'Serververbindung: DOM/COB/AT zu WEB/COB/AT'. Below the title are several tabs: 'Allgemein', 'Replizierung/Routing', 'Zeitplan', 'Kommentare', and 'Administration'. The 'Replizierung/Routing' tab is active. It is divided into two sections: 'Replizierung' and 'Routing'.
In the 'Replizierung' section:
- 'Replizierungsfunktion:' is set to 'Aktiviert'.
- 'Zu replizierende Datenbanken:' is set to 'Niedrig & Mittel & Hoch' with a 'Priorität' label.
- 'Replizierungstyp:' is set to 'Pull Push'.
- 'Pfade der zu replizierenden Dateien/Verzeichnisse:' is set to 'names; admin4; catalog; certlog' (with a note 'falls nichts anderes angegeben').
- 'Pfade der NICHT zu replizierenden Dateien/Verzeichnisse:' is empty.
- 'Zeitlimit für Replizierung:' is set to 'Minuten'.
In the 'Routing' section:
- 'Routing-Funktion:' is set to '-Ohne-'.
The interface uses a light blue and white color scheme with standard web form elements like dropdown menus and text input fields.

Abbildung 10.8: Verbindungsdokument, Register Replizierung/Routing

- (Optional) Geben Sie die Namen der Datenbanken oder Verzeichnisse an, die repliziert werden sollen. Geben Sie nichts an, werden alle gemeinsamen Repliken repliziert, wovon ich eher abrate, da Sie damit viel Kontrolle abgeben.
- Bei Verbindungsdokumenten innerhalb desselben Benannten Dominonetzwerks: Deaktivieren Sie die Routing-Funktion.
- Wechseln Sie zum Register **Zeitplan** und definieren Sie die Verbindungszeiten. Geben Sie entweder einen Zeitraum an (etwa 08:00 - 22:00) oder einen oder mehrere Zeitpunkte; trennen Sie mehrere Uhrzeiten durch Semikolons (z. B. 09:00; 12:00; 15:00). Wenn Sie einen Zeitraum verwenden, geben Sie zusätzlich ein Intervall ein, etwa alle 60 Minuten.
- Geben Sie an, für welche Wochentage der Zeitplan gelten soll.

The screenshot shows the 'Zeitplan' register in the same configuration tool. The title is 'Serververbindung: DOM/COB/AT zu WEB/COB/AT'. The 'Zeitplan' tab is active. The section is titled 'Geplante Verbindung'.
- 'Zeitplan:' is set to 'Aktiviert'.
- 'Zu bestimmten Zeiten verbinden:' is set to '00:00 - 23:59' with the note 'jeden Tag'.
- 'Wiederholungsintervall:' is set to '10' with the unit 'Minuten'.
- 'Wochentage:' is set to 'So, Mo, Di, Mi, Do, Fr, Sa'.
The interface uses the same light blue and white color scheme as the previous screenshot.

Abbildung 10.9: Verbindungsdokument, Register Zeitplan

Tipp: Mit dem Befehl `show schedule` können Sie auf der Serverkonsole den Zeitpunkt der nächsten geplanten Replikation einsehen.

10.5. PIRC

Löschinfos werden je nach Einstellung (Vorgabe ist 30 Tage) in regelmäßigen Abständen aus Notes-Datenbanken entfernt. Wird danach eine ältere Replik der Datenbank zum Einsatz gebracht (z. B. durch ein länger ausgeschaltetes Notebook), werden Dokumente, die am Server bereits gelöscht waren, wiederhergestellt, weil die Löschinfos nicht mehr existieren und Notes nicht weiß, dass die Dokumente bereits gelöscht waren. Dies ist besonders beim Domino-Verzeichnis gefährlich, wo etwa Mitarbeiter, die das Unternehmen schon vor langer Zeit verlassen haben, plötzlich erneut aufstehen können.

Das **Purge Interval Replication Control (PIRC)**, auf Deutsch etwas holprig mit »Bedienelement für Bereinigungsintervall der Replizierung« übersetzt, ist eine Replikationseinstellung, die verhindern soll, dass alte Dokumente in eine Datenbank zurückkopiert werden, nachdem deren Löschrumpf bereinigt wurde.

PIRC können Sie an mehreren Stellen aktivieren:

1. In den Replizieroptionen einer Datenbank
2. Im Domino-Administrator, Register Dateien
3. Mit dem Compact-Task

10.5.1. Aktivieren von PIRC via Replizieroptionen

Um PIRC in den Replizieroptionen zu aktivieren, wählen Sie den Befehl **Datei > Replizierung > Optionen für die Anwendung... > Platzsparer**:

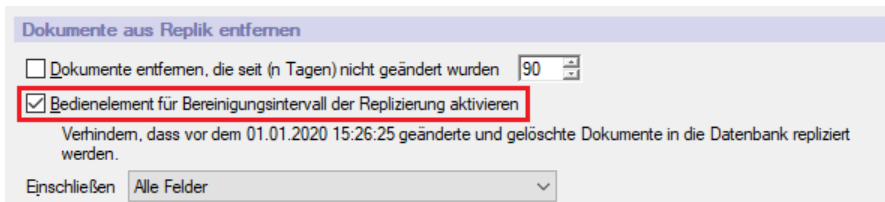


Abbildung 10.10: Replizieroptionen, Register **Platzsparer**

10.5.2. Aktivieren von PIRC via Domino-Administrator

Navigieren Sie im Domino-Administrator zum Register **Dateien** und markieren Sie dort die Datenbanken, für die Sie PIRC aktivieren möchten. Wählen Sie dann im Kontextmenü (rechte Maustaste) den Befehl **Erweiterte Eigenschaften...**

Setzen Sie im unteren Drittel des Dialogs zwei Häkchen für die Option »Bedienelement für Bereinigungsintervall der Replizierung« und klicken Sie auf **OK**.

10.5.3. Aktivieren von PIRC via Comapct-Task

Zusätzlich können Sie PIRC auch über einen Konsolenbefehl ein- und ausschalten:

```
load compact <Datenbank> -pirc on
load compact <Datenbank> -pirc off
```

Replikation: PIRC

Tipp: Um zu sehen, für welche Datenbanken PIRC bereits aktiviert wurde, geben Sie den folgenden Befehl ein:

```
show directory -pirconly
```


11. Anwendungsentwicklung

- > 11.1 Wozu dieses Kapitel?, Seite 305
- > 11.2 Anwendungsschablonen, Seite 305
- > 11.3 Agenten, Seite 312

11.1. Wozu dieses Kapitel?

Ein Kapitel Anwendungsentwicklung für Administratoren – wozu das?

Aus den folgenden Gründen:

1. Domino ist eine Werkzeugkiste. Alles lässt sich anpassen und das meist mit geringem Aufwand. Und diese Anpassungen sind manchmal auch nötig!
2. Jeder Administrator muss früher oder später einen Agenten schreiben, um Daten zu ändern. Und dieser Administrator sind Sie!
3. Domino ist eine Entwicklungsplattform. Auch wenn der Administrator nicht selbst programmiert, muss er in der Lage sein, die Voraussetzungen dafür zu schaffen. Und das kann er nur, wenn er versteht, was Entwickler brauchen!

11.2. Anwendungsschablonen

Mit Notes und Domino werden **Schablonen** (Templates) ausgeliefert, Dateien mit der Endung *.ntf (für Notes Template Facility), mit denen sich Anwendungen erstellen lassen. Die mitgelieferten NTF-Dateien erfüllen ganz unterschiedliche Zwecke, der Großteil ist hoch spezialisiert und dient zum Erstellen von Verwaltungsdatenbanken für diverse Servertasks. Diese NTF-Dateien werden auch als **Systemschablonen** bezeichnet und enthalten nicht immer ein ansprechendes User-Interface. Ein weiterer Teil liefert die Standardfunktionalität wie Mail und Kalender oder das Reservierungssystem. Und ein dritter Teil bietet die Möglichkeit, Anwendungen für Anwender zu erstellen, wie etwa ein Diskussionsforum oder einen TeamRoom, eine Anwendung zur Kommunikation von Projektteams. Diese Anwendungen bieten oft nicht nur im Notes-Client ein gefälliges Interface, sondern auch im Webbrowser.

Allen Schablonen gemeinsam ist, dass es sich um quelloffene Systeme handelt, die an die eigenen Bedürfnisse angepasst werden können, was bei Systemschablonen eher vorsichtig geschehen sollte. Dabei empfiehlt es sich, aus den eigenen Anpassungen neue Schablonen zu erstellen, da diese sonst beim nächsten Server-Update verloren gehen. Und letztendlich können Sie auf Basis einer mitgelieferten Schablone eine neue Anwendung designen und diese wieder als Schablone zur Verfügung stellen. So könnten Sie z. B. basierend auf dem mitgelieferten Diskussionsforum eine Wissens-

datenbank programmieren und das Ergebnis als neue Schablone zur Erstellung weiterer Wissensdatenbanken zur Verfügung stellen.

Schablonen dienen aber nicht nur dazu, neue Anwendungen zu erstellen, sie können auch nach der Erstellung mit den Anwendungen verbunden bleiben und im laufenden Betrieb immer wieder Gestaltungsänderungen an diese weitergeben. Wenn eine Schablone das ermöglicht, nennt man Sie **Masterschablone**. Dies ist etwa bei den Maildatenbanken der Fall, die alle mit der Schablone mail11.ntf verknüpft bleiben. Wollen Sie etwa eine zusätzliche Schaltfläche zum Einfügen einer Dateiverknüpfung in der Mailmaske haben, führen Sie (oder ein Entwickler) die Änderung in der Schablone durch und übertragen Sie diese dann auf alle verbundenen Maildatenbanken.

Mit dem Domino-Server werden nur englische Schablonen ausgeliefert. Wenn Sie zumindest ein Sprachpaket auf dem Server eingespielt haben, stehen manche Schablonen auch in einer anderen Sprache (Option Ersetzen) oder sogar in mehreren Sprachen (Option Hinzufügen) zur Verfügung. Für mehr Informationen zum Einspielen von Sprachpaketen lesen Sie Kap. 4.4 Sprachen installieren, ab Seite 41.

11.2.1. Eine Schablone erstellen

Das Erstellen einer Schablone erfolgt in zwei Schritten:

1. Erstellen der Datei mit der Endung *.ntf
2. Setzen der Eigenschaft »Datenbank ist eine Masterschablone«

11.2.1.1. Erstellen der Datei

Der einfachste Weg eine Schablone zu erstellen, besteht darin, eine vorhandene Anwendung (oder Schablone) zu kopieren. Tun Sie dies jedoch nicht auf Betriebssystemebene, da die Datei dann dieselbe Replik-ID aufweist, sondern verwenden Sie dazu den Befehl **Datei > Anwendung > Neue Kopie...**

Wählen Sie beim Kopieren einer Anwendung im Bereich **Was kopiert werden soll** die Option »Nur Anwendungsgestaltung«, damit die Dokumente nicht mitkopiert werden.

Steht keine Datenbank mit einem passenden Design zur Verfügung, können Sie alternativ mit dem Befehl **Datei > Anwendung > Neu...** auch eine leere Schablone erstellen. Wählen Sie in diesem Fall in der Liste der Schablonen den Eintrag »-leer-«.

Geben Sie in allen Fällen der neuen Datei die Endung *.ntf.

11.2.1.2. Setzen der Eigenschaft »Datenbank ist eine Masterschablone«

Rufen Sie nach dem Erstellen der neuen Datei die Datenbankeigenschaften auf und wechseln Sie zum Register **Gestaltung**. Aktivieren Sie die Option **Datenbank ist eine Masterschablone** und vergeben Sie einen Schablonennamen:

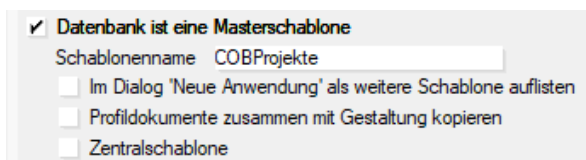


Abbildung 11.1: Datenbankeigenschaften, Register Gestaltung

Der Schablonenname muss systemweit eindeutig sein!

Um Masterschablonen auf dem Server erstellen zu können, müssen Sie im Serverdokument, Register **Sicherheit** direkt oder via Gruppe entweder im Feld **Administratoren** oder im Feld **Masterschablonen erstellen** eingetragen sein.

Ordnen Sie als letzten Schritt die nötigen Zugriffsrechte zu und übergeben Sie die Schablone an einen Entwickler.

Tipp: Setzen Sie in der Zugriffskontrollliste der Schablone Einträge in eckige Klammern, werden diese beim Erstellen von Anwendungen als Vorgaben übernommen (z. B.: [LocalDomainAdmins]).

11.2.2. Schablonen signieren

Bevor Sie die Änderungen in der Schablone an die abhängigen Datenbanken weitergeben, sollten Sie überprüfen, ob dem Signierer der Gestaltung vertraut wird. (Der Signierer ist jener Entwickler, der die Gestaltung zuletzt gespeichert hat.) Der Notes-Client vertraut nur Signaturen, die in der Ausführungskontrollliste (siehe Kap. 13.9, auf Seite 362) eingetragen sind und dort über ausreichende Rechte verfügen. Beim Ausführen von Code mit einer nicht vertrauenswürdigen Signatur oder einer Signatur mit zu geringen Rechten wird eine Sicherheitswarnung angezeigt – was Sie als Administrator unbedingt verhindern sollten!

Üblicherweise verwendet man als Signierer nicht den Namen des Entwicklers, da dieser das Unternehmen ja verlassen könnte, sondern einen generischen Namen wie z. B. »Admin« oder »Development« bzw. auch den Namen eines Servers.

Um eine Schablone zu signieren, gehen Sie wie folgt vor:

1. Starten Sie den Domino-Administrator.
2. Haben Sie zum Signieren eine bestimmte Notes-ID vorgesehen, wechseln Sie über den Menüpunkt **Datei > Sicherheit > ID wechseln...** zuerst zu dieser. (Ein Wechsel ist nicht erforderlich, wenn Sie die Schablone mit der Server-ID signieren wollen.)
3. Verbinden Sie sich mit dem Server, auf dem die Schablone liegt, und navigieren Sie zum Register **Dateien**.
4. Schalten Sie rechts oben im Feld **Anzeigen** auf »Schablonen« um.
5. Markieren Sie die gewünschte Schablone und wählen Sie im Kontextmenü (rechte Maustaste) den Befehl **Signieren...**
6. Der Dialog **Datenbank signieren** wird angezeigt (siehe Abbildung 11.2).
7. Wählen Sie im Bereich **Welche ID möchten Sie verwenden?** je nach Strategie entweder »ID des aktiven Benutzers« oder »ID des aktiven Servers«.
8. Wählen Sie im Bereich **Was möchten Sie signieren?** am besten die Option »Alle Gestaltungselemente«.
9. Klicken Sie auf **OK**.

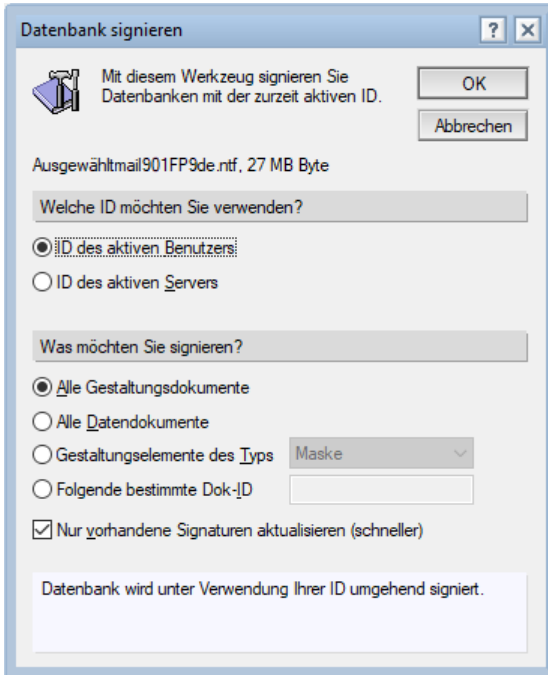


Abbildung 11.2: Der Dialog Datenbank signieren

11.2.3. Die Gestaltung von Anwendungen aktualisieren

Wird mit einer neueren Domino-Version eine neuere Version derselben Schablone ausgeliefert, muss die Gestaltung (Design) der abhängigen Datenbanken aktualisiert werden.

11.2.3.1. Einzelne Anwendungen aktualisieren

Gibt es nur eine oder wenige von einer Schablone abhängige Anwendungen, können Sie diese händisch aktualisieren. Wählen Sie dazu im Notes-Client oder Domino-Administrator zuerst die Anwendung aus und dann den Befehl **Datei > Anwendung > Gestaltung aktualisieren....** Wählen Sie dann den Server, auf dem die Schablone liegt, und klicken Sie auf **OK**:

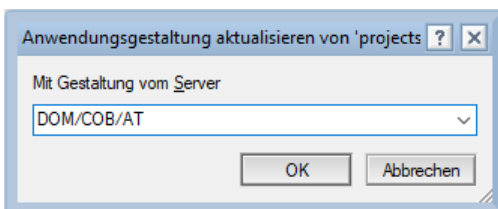


Abbildung 11.3: Anwendungsgestaltung aktualisieren, Server auswählen

Es wird eine Sicherheitswarnung angezeigt, die Sie ebenfalls bestätigen müssen.

Beachten Sie, dass zum Schutz von Änderungen die Aktualisierung von einzelnen Gestaltungselementen auch gesperrt sein kann. Um Gestaltungselemente zu schützen oder den Schutz aufzuheben, öffnen Sie die Datenbank im Domino-Designer und aktivieren Sie beim betroffenen Gestaltungselement die Eigenschaft »Durch Aktualisierung oder Ersetzung der Gestaltung nicht änderbar«:

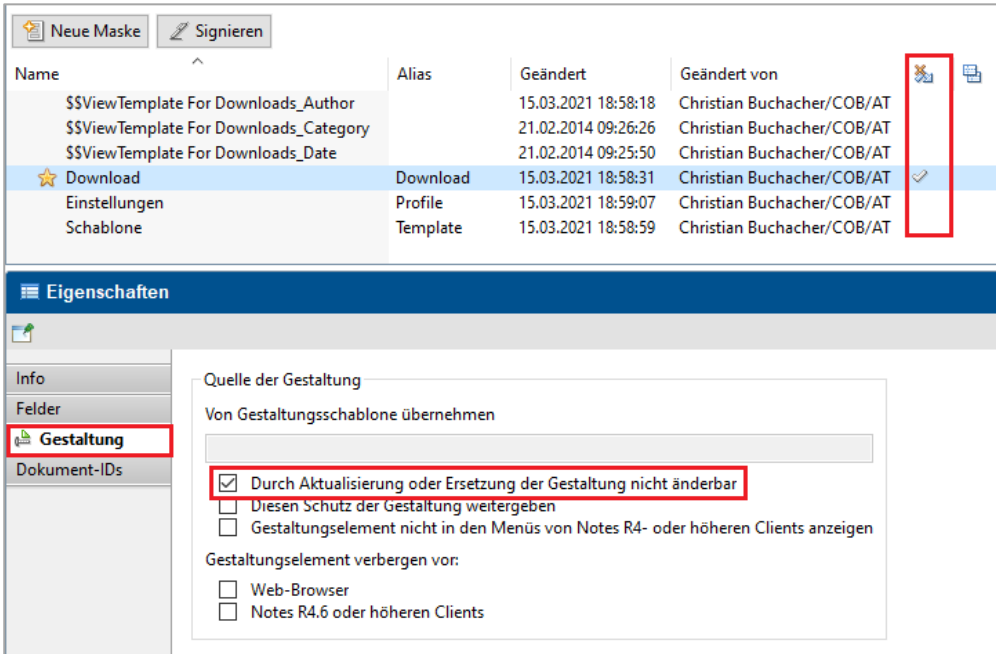


Abbildung 11.4: Eigenschaft »Durch Aktualisierung oder Ersetzung der Gestaltung nicht änderbar«

11.2.3.2. Der Servertask Design

Gibt es viele von der Schablone abhängige Datenbanken, kommt ein händisches Aktualisieren nicht mehr infrage. Das ist auch gar nicht notwendig, denn zum Aktualisieren der Gestaltung gibt es auf dem Domino-Server einen eigenen Task namens **Database Designer** (Design). Damit lassen sich alle Anwendungen in einem bestimmten Unterverzeichnis (z. B. mail\) oder auch im ganzen Datenverzeichnis auf einmal aktualisieren!

Der Designer wird per Vorgabe in der Datei notes.ini des Servers zusammen mit dem Catalog-Task täglich um ein Uhr morgens gestartet:

```
ServerTasksAt1=Catalog,Design
```

Wenn Sie regelmäßig Gestaltungsanpassungen durchführen, jedoch über keine getrennte Entwicklungsumgebung verfügen, rate ich Ihnen, den Design-Task nicht automatisch laufen zu lassen, sondern ihn nur bei Bedarf aufzurufen. Überlegen Sie daher, den Eintrag Design aus der Datei notes.ini zu entfernen, etwa durch den Befehl:

```
set configuration ServerTasksAt1=Catalog
```

Den Database Designer rufen Sie bei Bedarf mit den folgenden Befehlen auf:

```
load design -d <Verzeichnis>  
load design -f <Datenbank>  
load design -i <Indirect-Datei>
```

(Bei einer Indirect-Datei handelt es sich um eine Textdatei mit der Endung *.ind, in der die gewünschten Datenbanken aufgelistet sind. Mehr Informationen zum Erstellen von Indirect-Dateien finden Sie in Kap. 9.4.2.2 Datenbanken online konvertieren, ab Seite 248.)

11.2.4. Die Schablone wechseln

Bei Anwendungen, für die mit jeder neuen Domino-Version eine neue Schablone ausgeliefert wird (z. B. Mail) muss zuerst die Schablone gewechselt und dann die Gestaltung aktualisiert werden, z. B. von »StdR9Mail« (Datei mail9.ntf) auf »StdR11Mail« (Datei mail11.ntf). Den aktuellen Schablonennamen finden Sie in den Datenbankeigenschaften auf dem Register **Gestaltung**. In unserem Beispiel befindet sich die Maildatenbank noch auf Stand Version 9:

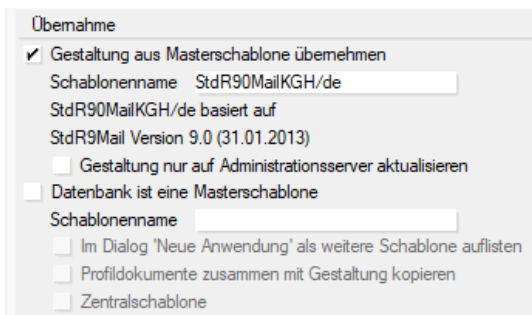


Abbildung 11.5: Datenbankeigenschaften, Register Gestaltung, Übernahme

Um die Schablone zu wechseln, markieren Sie die Anwendung und wählen Sie den Befehl **Datei > Anwendung > Schablone wechseln...** Es wird der folgende Dialog angezeigt:

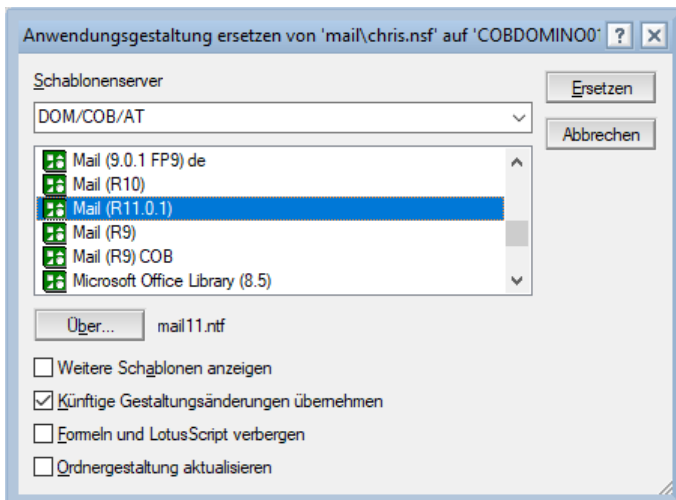


Abbildung 11.6: Datenbankeigenschaften, Bereich Übernahme

Wählen Sie den Server aus, auf dem die Schablone liegt und dann den Eintrag »Mail (R11.0.1)« mit dem Dateinamen »mail11.ntf« aus der Liste. Nach dem Klicken auf die Schaltfläche **Ersetzen** wird die Gestaltung aktualisiert.

Beim Wechseln der Mailschablone wird nur der Posteingang automatisch aktualisiert, alle anderen Ordner müssen mit dem Befehl **Aktionen > Ordner > Ordnergestaltung aktualisieren...** aktualisiert werden.

Zum Aktualisieren mehrerer Datenbanken steht unter Domino ein eigener Servertask zur Verfügung, welcher **Mail-Konvertierungs-Tool** (Mail Conversion Utility, Convert) genannt wird. Das Mail-Konvertierungs-Tool kann prinzipiell auf jede Art von Applikation angewendet werden, aber

wie der Name bereits verrät, liegt der Fokus auf Maildatenbanken. (Manche Parameter machen auch nur bei Maildaten einen Sinn.) Beachten Sie, dass das Mail-Konvertierungs-Tool nicht nur den neuen Schablonennamen einträgt, sondern auch gleich die Gestaltung aktualisiert; ein zusätzliches Starten des Design-Tasks ist somit nicht nötig. Weiteres können mit dem Zusatzparameter -u auch gleich die Ordner aktualisiert werden.

Die Syntax lautet:

```
load convert <Verzeichnis>\<Datenbank> <Schablonenname> <Schablone>
<Schablonenname> ist die Schablone, die ersetzt werden soll (z. B. »StdR9Mail«) und <Schablone>
der Dateiname der neuen Schablone (z. B. »mail11.ntf«). In allen Parametern kann auch mit Stell-
vertreterzeichen gearbeitet werden, z. B. »mail*.ntf« oder »StdR*Mail« oder überhaupt nur »*«.
```

Die wichtigsten Zusatzparameter entnehmen Sie bitte Tabelle 11.1:

Parameter	Beschreibung
-r	Aktiviert eine rekursive Suche. Mit diesem Zusatzparameter werden auch die Unterverzeichnisse des angegebenen Verzeichnisses durchsucht.
-f <Textdatei>	Aktualisiert die in der Textdatei angegebenen Maildatenbanken.
-l <Textdatei>	Generiert eine Liste von Maildateien, indem es die Dateinamen aus dem Domino-Verzeichnis ausliest, und schreibt sie in die angegebene Textdatei.
-g"<Sprache>"	Ersetzt die Sprache in der Datenbank durch die angegebene Sprache.
-u	Aktualisiert die Gestaltung Ordner basierend auf jener des Posteingangs (\$Inbox).

Tabelle 11.1: Zusatzparameter des Servertasks Convert

Nachfolgend zur besseren Anschaulichkeit ein paar Beispiele:

1. Aktualisieren aller Maildatenbanken im Verzeichnis mail\ inklusive aller Unterverzeichnisse auf die Schablone mail11.ntf:

```
load convert -r mail\*.nsf * mail11.ntf
```

2. Aktualisieren nur jener Maildatenbanken im Verzeichnis \mail, die den Schablonennamen StdR9Mail eingetragen haben, auf die Schablone mail11.ntf:

```
load convert mail\*.nsf StdR9Mail mail11.ntf
```

3. Aktualisieren aller Maildatenbanken in der Datei mailliste.txt auf die Schablone mail11.ntf:

```
load convert -f c:\temp\mailliste.txt * mail11.ntf
```

4. Haben Sie am Server das deutsche Sprachpaket hinzugefügt (d. h. die Schablone mail11.ntf enthält englische und deutsche Gestaltungselemente), können Sie das englische Schablonendesign mit dem folgenden Befehl in Deutsch konvertieren:

```
load convert -g"German" mail\*.nsf * mail11.ntf
```

11.3. Agenten

11.3.1. Was sind Agenten?

Agenten sind benutzerdefinierte Programme, die in der Regel im Domino-Designer programmiert werden. Dafür stehen gleich drei Programmiersprachen zur Verfügung:

- > Die Notes-Formelsprache (FS)
- > LotusScript (LS, ein Visual Basic-Dialekt)
- > Java

Agenten in LotusScript/Java sind sehr mächtig und können auf das Dateisystem und (via ODBC/JDBC) auch auf RDBM-Systeme zugreifen.

Agenten werden in einer Notes-Datenbank gespeichert und können in einem Client- oder in einem Serverkontext laufen. Ein klassischer Client-Kontext wäre der Start eines Agenten über eine Aktionsschaltfläche in einer Ansicht. In diesem Fall muss der ausführende Benutzer über die notwendigen Rechte verfügen, um die in der Ansicht ausgewählten Dokumente zu bearbeiten.

Werden Agenten durch einen Zeitplan oder durch ein Serverereignis aktiviert, laufen sie in einem Serverkontext und werden von einem speziellen Servertask namens **Agentenmanager** (Agent Manager, AMgr) ausgeführt. Diese Agenten laufen nicht mit den Rechten des Servers, sondern mit jenen des Signierers, also im Namen derjenigen Person, die den Agenten zuletzt gespeichert hat. Das ist meist ein Entwickler, der Domino-Administrator kann den Agenten aber auch mit einer anderen ID signieren, etwa wenn die Rechte des Entwicklers nicht ausreichen.

Serverseitig kommen weitere Restriktionen hinzu; hier wird nicht nur festgelegt, wer Agenten starten darf, sondern es wird auch noch zwischen beschränkten (restricted) und unbeschränkten (unrestricted) Funktionsaufrufen unterschieden. »Beschränkt« ist alles, was innerhalb einer Notes-Datenbank bleibt, »unbeschränkte« Aufrufe greifen auf Ressourcen außerhalb von Notes-Datenbanken zu, etwa auf das Dateisystem oder (via ODBC) auf RDBM-Systeme.

Wer was darf, steuern Sie im Serverdokument, im Register **Sicherheit > Einschränkungen der Programmierbarkeit**:

Einschränkungen der Programmierbarkeit	Wer kann -
Unbeschränkte Methoden und Operationen signieren oder ausführen:	<input type="checkbox"/> LocalDomainAdmins LocalDomainServers LocalDomainDevelopers ▾
Agenten signieren, die im Namen anderer ausgeführt werden:	<input type="checkbox"/> LocalDomainAdmins LocalDomainServers ▾
Agenten oder XPages signieren, die im Namen des Aufrufers ausgeführt werden:	<input type="checkbox"/> LocalDomainAdmins LocalDomainServers ▾
Beschränkte LotusScript/Java-Agenten signieren oder ausführen:	<input type="checkbox"/> */COB/AT ▾
Einfache und Formel-Agenten ausführen:	<input type="checkbox"/> */COB/AT ▾
Scriptbibliotheken signieren, die im Namen anderer ausgeführt werden:	<input type="checkbox"/> LocalDomainAdmins LocalDomainServers ▾
Die folgenden Einstellungen sind ab Domino 6 veraltet. Sie werden nur zwecks Kompatibilität mit früheren Versionen verwendet:	
Beschränktes Java/Javascript/COM ausführen:	<input type="checkbox"/> ▾
Unbeschränktes Java/Javascript/COM ausführen:	<input type="checkbox"/> ▾

Abbildung 11.7: Eigenschaften Agent, Sicherheitsstufen zur Laufzeit

Tip: Setzen Sie die folgende Variable in der Datei notes.ini, um nicht nur den Start von Hintergrundagenten auf der Serverkonsole (und dadurch in weiterer Folge auch im Protokoll) zu sehen, sondern auch mit welchen Rechten sie ausgeführt werden:

```
LOG_AGENTMANAGER=1
```

Dass ein Agent in seinem LotusScript- oder Java-Code unbeschränkte Funktionsaufrufe machen darf, müssen Sie (oder der Entwickler) in den Agenteneigenschaften explizit erlauben:

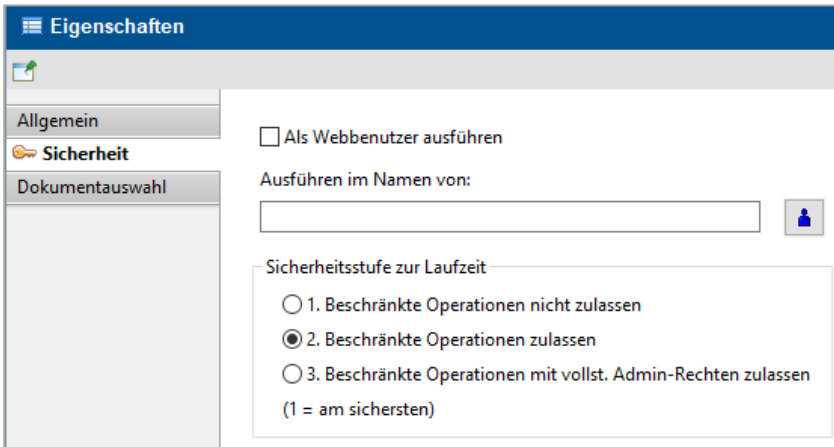


Abbildung 11.8: Eigenschaften Agent, Sicherheitsstufen zur Laufzeit

Leider gibt es hier ein ziemliches Durcheinander, was die Bezeichnungen anbelangt: Wenn Sie die Option »2. Beschränkte Operationen zulassen« auswählen, müssen Sie im Serverdokument im Feld **Unbeschränkte Methoden und Operationen signieren oder ausführen** eingetragen sein. Gemeint ist hier wohl eher: Methoden und Operationen ohne Beschränkungen signieren oder ausführen ...

Ein Agent, in dem beschränkte Operationen zugelassen sind, darf Mails verschicken, auf die Datei notes.ini (auch als »Umgebung« bzw. »Environment« bezeichnet) oder auf eine relationale Datenbank zugreifen, Daten in das Dateisystem exportieren und vieles anderes mehr.

Einen Sonderfall stellt der 3. Punkt dar: Wenn Sie als Administrator mit voller Berechtigung (siehe Kap. 5.6.7 Sonderfall Administratoren mit voller Berechtigung, ab Seite 110) einen Agenten schreiben und für diesen die 3. Option auswählen, können Sie damit auch Dokumente mit Leserfeldern bearbeiten, auf die Sie sonst keinen Zugriff hätten.

11.3.2. Der Agentenmanager

Agenten, die durch einen Zeitplan oder durch Serverereignisse (beim Hochfahren des Servers, bei der Mailzustellung, beim Ändern von Dokumenten u. a.) ausgelöst werden, werden wie gesagt vom **Agentenmanager** (Agent Manager, AMgr) ausgeführt. Beim Agentenmanager handelt es sich um einen sogenannten multi-threaded Task, er kann mehrere sogenannte **Executives** starten und pro Executive einen Agenten ausführen. Die Konfiguration hierzu finden Sie im Serverdokument, Register **Server-Tasks > Agentenmanager**. Sie können unterschiedliche Parameter für die Hauptarbeitszeit, in der der Server stärker belastet ist, und für den Rest des Tages (»Nacht-Parameter«) angeben. Achten Sie darauf, dass die maximale Ausführungszeit für LotusScript-/Java-Agenten per Vorgabe auf 10 (Tag) bzw. 15 Minuten (Nacht) beschränkt ist:

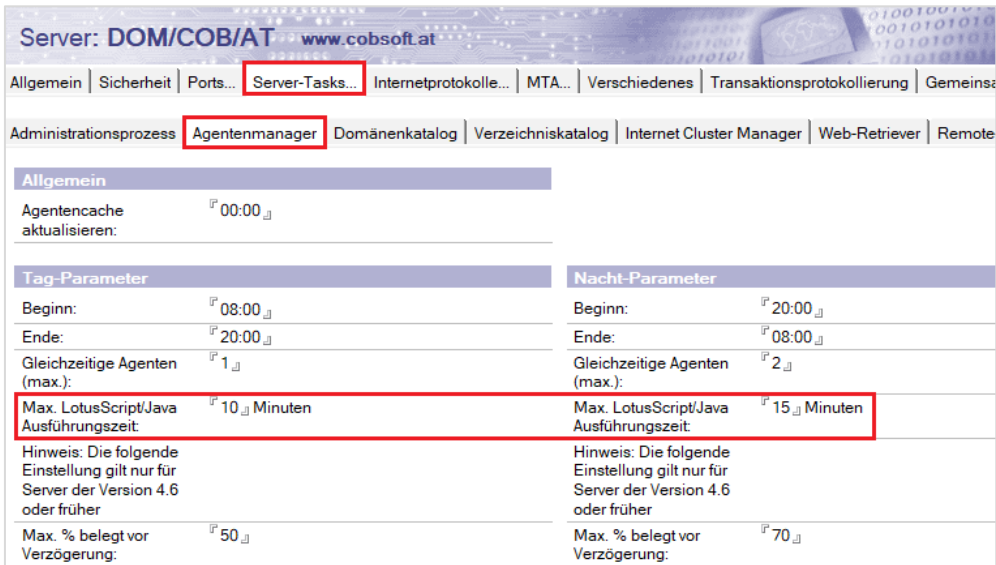


Abbildung 11.9: Serverdokument, Einstellungen für den Agentenmanager

Läuft ein Agent länger, als es die eingestellte maximale Ausführungszeit erlaubt, wird er einfach abgewürgt. Dabei handelt es sich um eine Selbstschutzfunktion des Servers, die verhindern soll, dass schlecht programmierte Agenten dem Server Ressourcen wegnehmen und ihn ev. sogar zum Absturz bringen. Überprüfen Sie daher regelmäßig, ob zeitplangesteuerte Agenten zu lange brauchen! Dies ist z. B. über DDM-Tests vom Typ Application Code/Long running agents möglich. (Mehr Informationen dazu finden Sie in Kap. 17.5.4 Probing, ab Seite 465.)

11.3.2.1. Konsolenbefehle

Zur Kommunikation mit dem Agentenmanager stehen mehrere Konsolenbefehle zur Verfügung. Eine Übersicht liefert Tabelle 11.2:

Befehl	Erklärung
<code>tell amgr cancel</code>	Bricht den gerade ausgeführten zeitplangesteuerten Agenten ab. Dieser Befehl bricht keine Agenten ab, die vom HTTP-Task oder dem Mail-Router ausgeführt werden. (Diese Agenten können nur über den entfernten Debugger abgebrochen werden.) Verwenden Sie den Befehl <code>tell amgr schedule</code> , um festzustellen, welche Agenten laufen.
<code>tell amgr debug</code>	Zeigt die aktuellen Debug-Einstellungen an und erlaubt das Setzen neuer Debug-Einstellungen. (Entspricht den Parametern der notes.ini-Variable <code>Debug_AMgr</code>).
<code>tell amgr pause</code>	Pausiert zeitplangesteuerte Agenten.
<code>tell amgr resume</code>	Setzt pausierte zeitplangesteuerte Agenten fort.
<code>tell amgr run <Agent></code>	Führt den angegebenen Agenten sofort aus. Verwenden Sie die Syntax: "Datenbank" 'Agent'

Befehl	Erklärung
	(doppelte Anführungszeichen für die Datenbank und einfache für den Agenten)
<code>tell amgr schedule</code>	Listet alle Agenten auf, deren Ausführung für den aktuellen Tag geplant ist. Dieser Befehl zeigt Namen des Agenten und der Datenbank, den Auslöser des Agenten und die Ausführungszeit an.
<code>tell amgr status</code>	Zeigt den Status des Agent Managers mit der Anzahl der sogenannten Executives, der Warteschlangen und der Einstellungen an.

Tabelle 11.2: Konsolenbefehle des Servertasks Agent Manager

Zusatzinformationen zum Befehl `tell amgr schedule`

Der Agent Manager verwendet drei verschiedene Warteschlangen: eine für ausführbare Agenten (E für Eligible), eine zweite für geplante Agenten (S für Scheduled) und eine dritte für ereignisgesteuerte Agenten, die darauf warten, dass das Ereignis eintritt (Wartet auf Ausführung V). Zeitplangesteuerte Agenten werden, wenn ihre Zeit gekommen ist, in die Warteschlange für ausführbare Agenten verschoben. Ereignisgesteuerte Agenten werden, wenn das Ereignis eintritt, analog zuerst in die Warteschlange der geplanten und dann ausführbaren Agenten verschoben.

Die Art der Warteschlange (E, S, V) wird in der ersten Spalte ausgegeben.

Die zweite Spalte zeigt das Ereignis, das den Agenten aktiviert: S, M, U. Der Buchstabe S (Schdule) steht für »nach Zeitplan«, M (Mail) für »Eingang neuer Mail« und U (Update) für »ein oder mehrere Dokumente erstellt oder aktualisiert«.

Hier eine Beispielausgabe:

```
E S 09:43 Heute      Sync documents      project.nsf
S S 16:36 Heute      DeleteExpired       files.nsf
V M                  ProcessMail         Urlaubsantraege.nsf
```

11.3.3. Einen einfachen Formel-Agenten erstellen

Sie sollten als Administrator in der Lage sein, per Agent ein Feld zu ändern. Die Notes-Formelsprache reicht dafür völlig. Zum Erstellen eines Agenten benötigen Sie einen Domino-Designer.

Nehmen wir an, Sie wollen den Domänennamen ändern. Der Domänenname steht im Domino-Verzeichnis in Server-, Personen-, Mail-In- und in Gruppendokumenten. Während Sie die wenigen Serverdokumente händisch korrigieren können, artet das Aktualisieren der Personendokumente rasch in Arbeit aus. Mit einem einfachen Formel-Agenten sind Sie hingegen in weniger als einer Minute fertig. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie das Domino-Verzeichnis und wählen Sie im Menü **Ansicht** den Befehl **Agenten**.
2. Das Domino-Verzeichnis wird im Designer geladen. Lassen Sie sich nicht dadurch irritieren, dass es bereits viele Agenten gibt, und klicken Sie auf die Schaltfläche **Neuer Agent**.
3. Der Dialog **Neuer Agent** wird angezeigt (siehe Abbildung 11.10).
4. Geben Sie einen Namen für Ihren Agenten ein, wählen Sie als Typ »Formel« und klicken Sie auf **OK**.

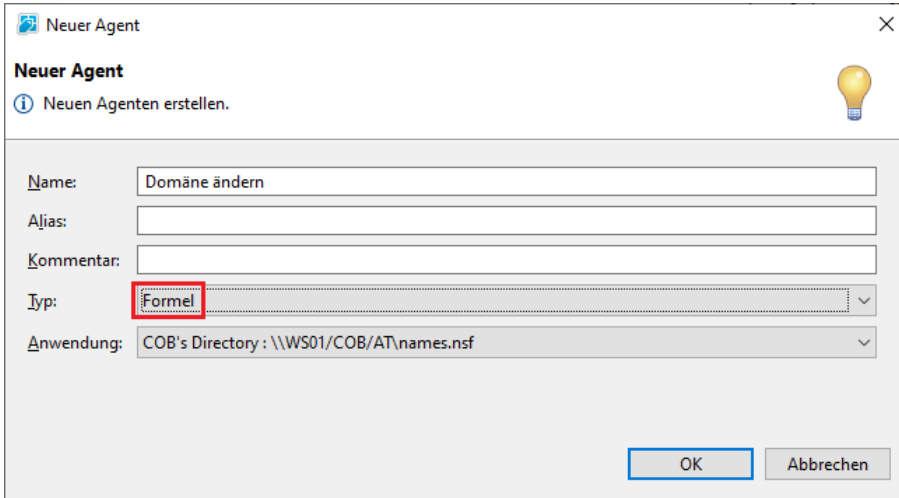


Abbildung 11.10: Dialog Neuer Agent

5. Tippen Sie jetzt den Code ein. Nehmen wir an, Ihre neue Domäne soll »VIE« heißen. Das Feld, das geändert werden soll, heißt **MailDomain**, daher lautet die Formel:

```
FIELD MailDomain := "VIE"
```

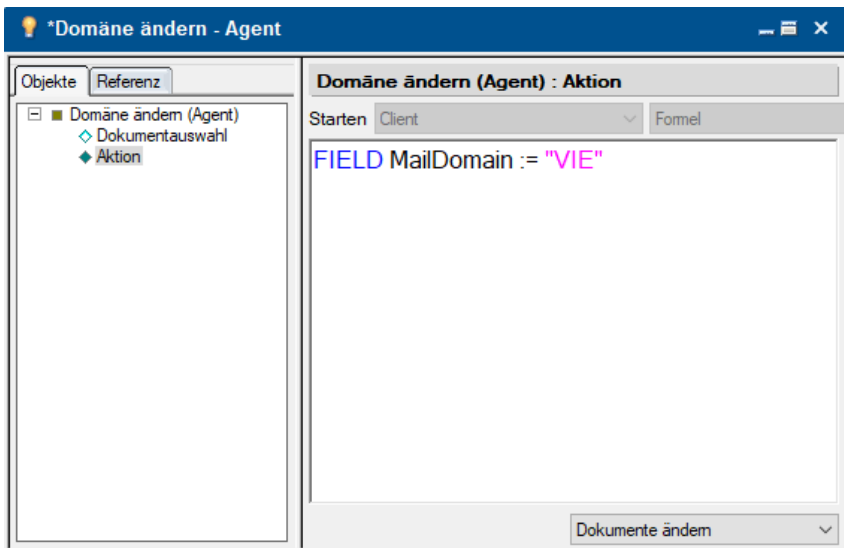


Abbildung 11.11: Der Aktionsbereich des Beispielagenten »Domäne ändern« mit dem Formelcode

Wollen Sie mehrere Felder aktualisieren, wiederholen Sie die Anweisung mit unterschiedlichen Feldnamen. Beachten Sie, dass Sie bei einem mehrzeiligen Code jede Zeile mit einem Semikolon (;) abschließen müssen! Also:

```
FIELD MailDomain := "VIE";  
FIELD MailFile := "mail\meier_franz.nsf";  
FIELD MailServer := "CN=DOM/O=COB/C=AT";
```

6. Klicken Sie mit der rechten Maustaste in den Hintergrund und wählen Sie im Kontextmenü **Eigenschaften: Agent**. Achten Sie darauf, dass im Bereich **Auslösen** »Auswahl im Menü Aktionen« und bei **Ziel** »Alle ausgewählten Dokumente« steht:

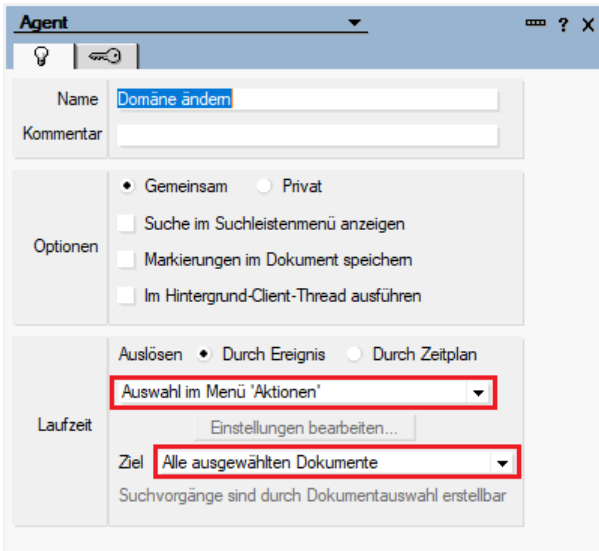
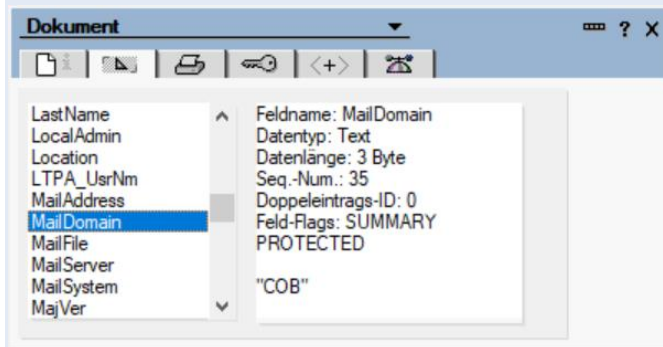


Abbildung 11.12: Eigenschaften Agent

7. Speichern und schließen Sie den Agenten.

Tipp: Wenn Sie einen Feldnamen nicht kennen, öffnen Sie die entsprechende Maske im Domino-Designer. Manchmal reicht dafür auch eine Durchsicht der Feldliste in den Dokumenteigenschaften:



Der neue Agent sollte jetzt im Menü **Aktionen** aufscheinen:

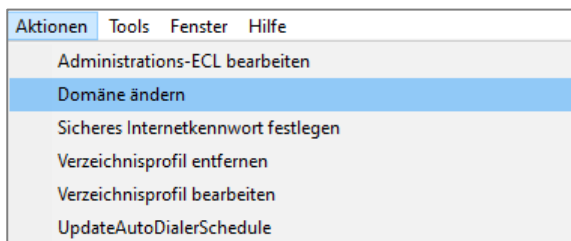


Abbildung 11.13: Der Beispielagent »Domäne ändern« im Menü Aktionen

Wechseln Sie nun in die Ansicht Personen und drücken Sie [Strg]+[A], um alle Dokumente zu markieren. Rufen Sie dann Ihren Agenten im Menü **Aktionen** auf.

Achtung: Erstellen Sie zuvor immer eine Sicherheitskopie der Datenbank! Testen Sie Ihren Code zuerst mit einem einzigen Dokument.

12. Verschlüsselung und Zertifikate

- > 12.1 Kurze Einführung in die Kryptografie, Seite 319
- > 12.2 Netzwerkverschlüsselung, Seite 321
- > 12.3 Datenbankverschlüsselung, Seite 323
- > 12.4 Dokumentverschlüsselung, Seite 325
- > 12.5 Spezialfall Mailverschlüsselung, Seite 325
- > 12.6 Feldverschlüsselung, Seite 327
- > 12.7 Signieren, Seite 328
- > 12.8 Verschlüsselung in ID-Dateien, Seite 328

12.1. Kurze Einführung in die Kryptografie

Als Administrator sollten Sie zumindest die Grundlagen der in Notes und Domino angewendeten Verschlüsselungsverfahren kennen.

12.1.1. Verschlüsselungsverfahren

12.1.1.1. Symmetrische Verschlüsselung

Bei diesem Verfahren erfolgen die Ver- und Entschlüsselung mit demselben Schlüssel. Der Algorithmus weist eine gute Performance auf, weshalb dieses Verfahren in der Regel angewendet wird, wenn es schnell gehen muss.

Ausschließlich die Schlüssellänge bestimmt die Sicherheit. – Je länger, desto sicherer! Gute Schlüssellängen sind 128 oder 256 Bit. In Notes können zwei verschiedene Verschlüsselungsalgorithmen verwendet werden: 128 Bit RC2 (rückwärtskompatibel bis Notes 6) und das bessere 128/256 Bit AES (Advanced Encryption Standard – seit Notes 8.0.1).

Der Symmetrische Schlüssel wird in Notes **Geheim Schlüssel** (Secret Encryption Keys) genannt. Der Vorteil besteht darin, dass der Schlüssel an mehrere Personen verteilt werden kann. Die Verwaltung ist jedoch aufwendig, es kann zwar jeder Notes-Benutzer einen neuen Geheim Schlüssel in seiner ID-Datei erstellen, aber nur Entwickler können ihn auf Felder anwenden. Diese müssen sich dann darum kümmern, dass alle beteiligten Personen den Schlüssel erhalten. Ein Verteilen ist per Mail oder via Export in eine Schlüsseldatei möglich. Problematisch wird die Sache, wenn ein Schlüssel ausgetauscht werden muss.

12.1.1.2. Asymmetrische Verschlüsselung

Bei diesem Verfahren existieren zwei Schlüssel, ein **Öffentlicher Schlüssel** (Public Key) zum Verschlüsseln und ein **Privater Schlüssel** (Private Key) zum Entschlüsseln. Der Öffentliche Schlüssel ist via Domino-Verzeichnis für jedermann zugänglich, der Private Schlüssel nur für den Besitzer der jeweiligen ID-Datei.

Als verwendeter Verschlüsselungsalgorithmus kommt RSA (nach **R**ivest – **S**hamir – **A**dleman, MIT 1977) zum Einsatz.

Der Hauptvorteil dieses Verfahrens liegt darin, dass sich niemand um die Schlüsselverteilung kümmern muss: Über die Kopie des Öffentlichen Schlüssels im Personendokument kann automatisch jeder etwas für andere verschlüsseln. Und das ist gleichzeitig auch das Problem, denn der weitergegebene Öffentliche Schlüssel bietet einen Ansatzpunkt zum Berechnen des mathematisch dazu passende Privaten Schlüssels, weshalb von vornherein mit sehr großen Schlüssellängen ab 1024 oder 2048 Bit gearbeitet wird.

Erschwert wird die Berechnung des Privaten Schlüssels durch Verwendung einer »Falltürfunktion«: In eine Richtung (Verschlüsselung) geht es einfach, aber man kann mit dem verschlüsselten Ergebnis (Chiffre) und dem Öffentlichen Schlüssel nur schwer auf die ursprüngliche Information zurückschließen.

Allgemein gilt: RSA-Verschlüsselung ist langsamer als symmetrisches Verfahren, aber bei ausreichender Schlüssellänge (> 1024 Bit) sicherer.

Anwendung asymmetrischer Verschlüsselung in Notes:

- > Verschlüsseln von Feldern
- > Verschlüsseln von Dokumenten bzw. Mails
- > Verschlüsseln von ganzen Datenbanken

12.1.2. Sicherheitsstandards

12.1.2.1. FIPS-140-2-Zertifizierung

FIPS (Federal Information Processing Standard) reguliert die Verwendung von kryptografischen Bibliotheken. Kryptografische Bibliotheken, aber nicht die Anwendung, die sie verwendet, können FIPS-140-2-zertifiziert sein. Alle von HCL Notes und Domino bereitgestellten Bibliotheken (OpenSSL 1.1.1a) auf der Plattform Windows sind FIPS-140-2-zertifiziert.

12.1.2.2. AES-Algorithmus

Der AES-Algorithmus (AES steht für Advanced Encryption Standard) steht für Notes und Domino unter der Plattform Windows für einige Verschlüsselungsmethoden zur Verfügung. AES ist nicht nur weit verbreitet, sondern auch FIPS 140-2-zertifiziert.

12.1.2.3. Secure-Hash-Algorithmus (SHA-2)

Der Secure-Hash-Algorithmus (SHA-2) ist Teil der FIPS-140-2-zertifizierten OpenSSL-Bibliothek und für die Compliance mit der behördlichen Vorschrift NIST 800-131 anerkannt. In Domino 11 steht SHA-2 zum Überprüfen von TLS-Zertifikatsignaturen und S/MIME-signierten Mails sowie

einigen Bereichen von Notes/Domino zur Verfügung, für die zuvor Kennwörter wie das Internetkennwort (HTTP) »gehasht« wurden.

Mit den Programmen **OpenSSL** und **KYRTool** können Sie bereits ab Domino 9.0.1 FP3 SHA-2-signierte Zertifikate erstellen. (Die Anleitung dazu finden Sie in Kap. 14.7 TLS-Zertifikate erstellen, ab Seite 394.)

12.1.2.4. Transport Layer Security (TLS)

Transport Layer Security (TLS) ist ein kryptografisches Protokoll, das auf der älteren Spezifikation Secure Sockets Layer (SSL) basiert.

12.1.3. Digitale Signatur

Asymmetrische Verfahren sind immer auch ein wenig symmetrisch: Man kann auch mit dem Privaten Schlüssel verschlüsseln! Das Ergebnis kann dann mit dem Öffentlichen Schlüssel entschlüsselt werden. Dieses Verfahren kommt bei der elektronischen Signatur zur Anwendung. Diese erfüllt zwei Aufgaben:

1. Sicherstellen, dass Informationen von der richtigen Person stammen
2. Sicherstellen, dass Informationen auf dem Weg nicht verändert wurden (Mails!)

Zum Signieren werden im Allgemeinen Hash-Funktionen verwendet, welche für einen Text eine Prüfsumme erzeugen, etwa eine fixe Zahl. Wird nur ein einziges Zeichen im Text verändert, ändert sich auch die Zahl, womit die Signatur zerstört ist.

12.2. Netzwerkverschlüsselung

Mit Netzwerkverschlüsselung ist die verschlüsselte Kommunikation zwischen zwei Domino-Servern oder zwischen einem Notes-Client und einem Domino-Server gemeint. Dabei kommt ausschließlich das NRPC-Protokoll zum Einsatz, die verschlüsselte Kommunikation über Internetprotokolle (wie HTTP) via TLS ist in Kap. 14.6.1 Transport Layer Security (TLS), ab Seite 388 beschrieben.

Bei der Netzwerkverschlüsselung kommen sowohl symmetrische als auch asymmetrische Verschlüsselungsverfahren zum Einsatz. Dies läuft so ab: Der Server generiert einen zufälligen symmetrischen Geheimschlüssel für die Sitzung und verschlüsselt ihn mit dem Öffentlichen Schlüssel der im Client aktiven Person. Der Geheimschlüssel wird dann an den Client geschickt, wo er mit dem Privaten Schlüssel aus der aktuell verwendeten ID-Datei entschlüsselt wird. Jetzt, wo Client und Server über denselben Schlüssel verfügen, findet die Kommunikation nur noch verschlüsselt statt. Das heißt, die eigentliche Netzwerkverschlüsselung läuft aus Performancegründen symmetrisch ab. Wird die Sitzung geschlossen, wird der Sitzungsschlüssel gelöscht. Für zukünftige Sitzungen wird jedes Mal ein neuer, unterschiedlicher Sitzungsschlüssel verhandelt.

Um eine verschlüsselte Kommunikation zu erzwingen, reicht es, die Netzwerkverschlüsselung auf dem Netzwerkport des Servers zu aktivieren, die Notes-Clients spielen automatisch mit.

Netzwerkverschlüsselung führt allgemein zu einer Performanceminderung und kann die Serverleistung beeinträchtigen, weshalb ich im LAN eher darauf verzichten würde; sie bietet sich jedoch an, wenn Notes-Clients über das Internet mit dem Domino-Server kommunizieren.

Besitzt der Server mehrere Anschlüsse, etwa einen für den Datenverkehr über das Internet und einen weiteren für den internen Datenverkehr, können Sie die Verschlüsselung auch selektiv nur für den Internetanschluss aktivieren und den internen Port unverschlüsselt lassen.

Um eine verschlüsselte NRPC-Kommunikation zu erzwingen, gehen Sie wie folgt vor:

1. Wählen Sie im Domino-Administrator den Server, dessen Netzwerkdaten Sie verschlüsseln möchten.
2. Navigieren Sie zum Register **Konfiguration**.
3. Wählen Sie im Werkzeugfenster den Eintrag **Server > Ports einrichten...**
4. Wählen Sie den Anschluss, über den die Daten verschlüsselt werden sollen, z. B. TCPIP.
5. Setzen Sie ein Häkchen bei **Netzwerkdaten verschlüsseln**:

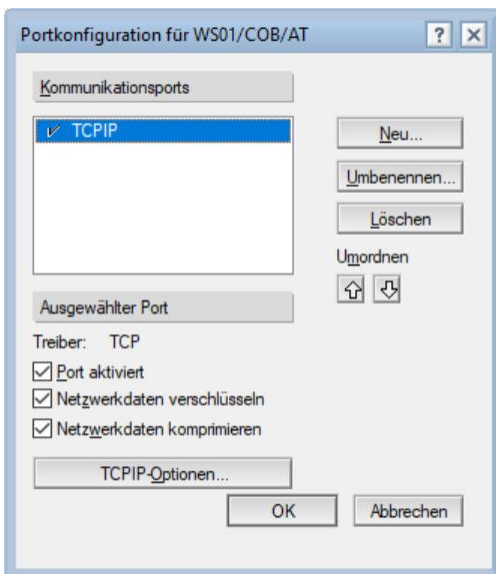


Abbildung 12.1: Dialog Portkonfiguration

6. Klicken Sie auf **OK**.

Die Änderungen wirken sich erst aus, wenn Sie den Anschluss neu starten. Dies ist durch ein Neustarten des Servers möglich oder über folgende Vorgangsweise:

1. Navigieren Sie im Domino-Administrator zum Register **Server** und wählen Sie die Ansicht **Status**.
2. Wählen Sie im Werkzeugfenster den Eintrag **Ports > Neustart...**

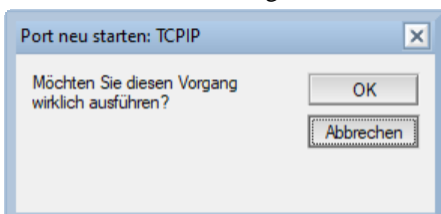


Abbildung 12.2: Dialog Port neu starten

3. Klicken Sie auf **OK**, um den Anschluss neu zu starten.

Die Netzwerkverschlüsselung können Sie auch schon bei der Erstkonfiguration des Servers aktivieren.

12.3. Datenbankverschlüsselung

Die Verschlüsselung kann lokal mit der Benutzer-ID oder am Server mit der Server-ID erfolgen.

12.3.1. Lokale Verschlüsselung

Das Verschlüsseln von lokalen Repliken auf tragbaren Computern wie Notebooks oder Tablets ist ein Muss – außer es ist bereits das Dateisystem verschlüsselt. Der Einsatz von Verschlüsselung auf einem Client bedeutet auch nicht viel Overhead – außer in einer Citrix-Umgebung, wo das Anlegen von lokalen Repliken ohnehin wenig Sinn macht.

Es wird zwar das RSA-Verfahren verwendet, die Verschlüsselung erfolgt jedoch nicht direkt mit dem Öffentlichen Schlüssel des Benutzers, sondern Notes generiert zuerst einen zufälligen Geheimschlüssel, verschlüsselt diesen mit dem Öffentlichen Schlüssel und hängt das Ergebnis an die Datenbank an. Danach ist ein Zugriff auf die verschlüsselte Datenbank nur noch möglich, wenn der Private Schlüssel des Benutzers den Geheimschlüssel dechiffrieren kann.

Achtung: Verwenden Sie bei verschlüsselten Datenbanken lokal immer mindestens ODS 52 – bis ODS 51 kann es beim Speichern zu korrupten Dokumenten kommen. Dieses Problem tritt nur bei Datenbanken mit starker Verschlüsselung auf, ist dort aber relativ häufig. (Der Fehler fällt meist nicht auf, weil kaputte Dokumente nach der Anwendung von Fixup regelmäßig aus der Serverreplik zurückrepliziert werden.)

Ab Version 11.0.1 stehen zwei Verschlüsselungsstärken zur Verfügung:

- > Starke Verschlüsselung
- > 128-Bit-AES

Verwenden Sie in älteren Notes-Versionen die Einstellung »Starke Verschlüsselung« und ab Version 11.0.1 stets »128-Bit-AES«:

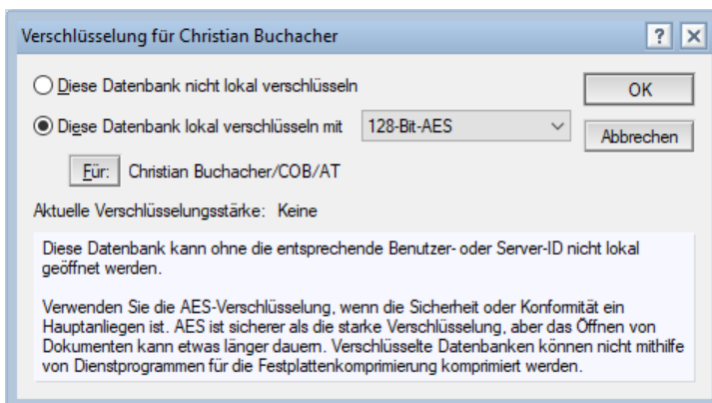


Abbildung 12.3: Dialog Datenbankverschlüsselung

Um die Verschlüsselung anzuwenden, muss die Datenbank nach der Umstellung »copy-style« komprimiert werden. (Dies erübrigt sich beim Erstellen einer lokalen Replik oder Kopie.) Ändern Sie die Verschlüsselungseinstellungen in den Datenbankeigenschaften im laufenden Betrieb, wird die Komprimierung automatisch gestartet.

Das Verschlüsseln lokaler Repliken und Kopien ist in Notes Vorgabe, kann im Erstellen-Dialog jedoch deaktiviert werden:

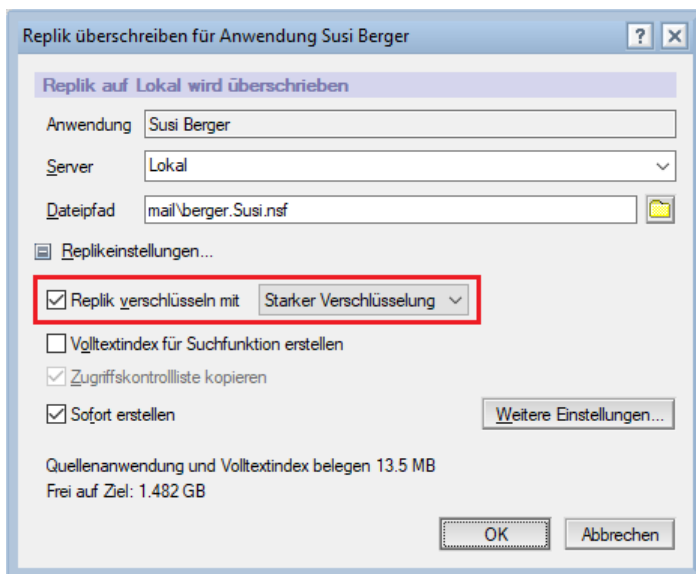


Abbildung 12.4: Dialog Replik erstellen

Die Vorgabe kann im Sicherheitsdialog (**Datei > Sicherheit > Benutzersicherheit > Notes-Daten**) abgeschaltet werden.

Umgekehrt können Sie mithilfe der folgenden notes.ini-Variable die lokale Verschlüsselung auf Clients erzwingen:

```
LOCAL_DB_ENCRYPT_ENABLE=1
```

Mithilfe der folgenden notes.ini-Variable kann zusätzlich die Stärke der Verschlüsselung vorgegeben werden:

```
LOCAL_DB_ENCRYPT_DEFAULT=3
```

(0 = keine Verschlüsselung, 1 = Einfache Verschlüsselung, 2 = Mittlere Verschlüsselung, 3 = Starke Verschlüsselung)

Ältere Clients verwendeten als Vorgabe eine mittlere Verschlüsselung. Mit der folgenden notes.ini-Variable können Sie den Verschlüsselungsgrad bei der nächsten »copy-style«-Komprimierung von mittel auf stark hochsetzen:

```
COMPACT_UPGRADE_MEDIUM_ENCRYPTION_TO_STRONG=1
```

12.3.2. Verschlüsselung am Server

Die Verschlüsselung von Datenbanken auf dem Domino-Server ist eher unüblich. Hier darf zur Verschlüsselung keine Benutzer-ID, sondern einzig die Server-ID herangezogen werden, weil der Server die Datenbank sonst nicht mehr lesen kann. Wenn der Server, auf dem Domino läuft, gleichzeitig

als Dateiserver fungiert, erhöht die Verschlüsselung die Sicherheit, da direkt aus dem Domino-Datenverzeichnis herauskopierte Datenbanken nicht gelesen werden können. Es kompliziert jedoch Ihr Leben als Administrator, da die Datenbanken auch im Backup verschlüsselt sind und Sie immer die Server-ID brauchen, um darauf zugreifen zu können.

Bedenken Sie, dass Verschlüsselung immer auch Overhead erzeugt und Performance kostet. Anbei ein (schon etwas älterer) Vergleich zur CPU-Nutzung durchgeführt von der IBM. Gemessen wurde auf einem Windows Server 2008 R2, 64-Bit mit 4.000 Usern und dem Mail9-Template:

Verschlüsselung	CPU-Last
Nicht verschlüsselt	35 %
Mittlere Verschlüsselung	39 %
Starke Verschlüsselung	48 %

Tabelle 12.1: CPU-Last bei Anwendung verschiedener Verschlüsselungsverfahren

Resümee: Viele verschlüsselte Datenbanken sorgen auf einem Domino-Server zumindest für eine zusätzliche Prozessorlast! Bedenken Sie dies bei Performanceproblemen.

Der notes.ini-Eintrag `SHOW_ENCRYPTED_DATABASES` zeigt verschlüsselte Datenbanken auf der Konsole an. Mögliche Schalter sind:

- 1 = Einfache Verschlüsselung anzeigen
- 2 = Mittlere Verschlüsselung anzeigen
- 4 = Starke Verschlüsselung anzeigen

12.4. Dokumentverschlüsselung

Ein Verschlüsseln von Dokumenten gibt es de facto nicht, es können nur Felder verschlüsselt werden. Oft ist mit Dokumentverschlüsselung das Verschlüsseln des Rich-Text-Feldes gemeint. Felder können sowohl über einen oder mehrere Öffentliche Schlüssel (symmetrisch) als auch über einen oder mehrere Geheimschlüssel (asymmetrisch) verschlüsselt werden.

12.5. Spezialfall Mailverschlüsselung

Notes-Mails sind auch nur Dokumente, aber weil hier einige Spezialregeln gelten, widme ich ihnen ein eigenes Unterkapitel. Notes-Mails können beim Senden oder beim Empfangen (= bei der Zustellung durch den Mail-Router) verschlüsselt werden, in beiden Fällen mit dem Öffentlichen Schlüssel des Empfängers. Die Betonung liegt hier wirklich auf **Notes**-Mails, denn die Verschlüsselung von SMTP-Mails folgt komplett anderen Regeln.

12.5.1. Mails beim Senden verschlüsseln

Per Vorgabe bestimmt der Anwender in den Zustelloptionen, ob eine Notes-Mail verschlüsselt versendet wird. Sie als Administrator können die Verschlüsselung von Notes-Mails via Policy erzwingen oder verbieten. Gehen Sie dazu in den Desktopeinstellungen zum Register **Vorgaben > Mail** und aktivieren Sie wie in Abbildung 12.5 dargestellt die Einstellung **Gesendete Mail verschlüsseln**

mit »Anfangswert festlegen« (dann wirkt sie als Vorschlag, der vom Anwender abgeschaltet werden kann) oder »Wert festlegen und Änderungen verhindern« (dann ist es eine verpflichtende Vorgabe).

12.5.2. Behalten einer verschlüsselten Kopie

Wollen Sie, dass Kopien von gesendeten Mails in der Ansicht Gesendet ebenfalls (mit dem Schlüssel des Absenders) verschlüsselt werden, setzen Sie in den Desktopeinstellungen, Register **Vorgaben > Mail** wie in Abbildung 12.5 dargestellt die Einstellung **Gespeicherte Mail verschlüsseln** mit der Option »Anfangswert festlegen« oder »Wert festlegen und Änderungen verhindern«. Hier ein Beispiel für einen nicht verpflichtenden Vorschlag:



Abbildung 12.5: Desktopeinstellungen, Register Mail – Mailverschlüsselung aktivieren

Und hier ein Beispiel für eine verpflichtende Vorgabe – in diesem Fall wird die Mailverschlüsselung dauerhaft deaktiviert:



Abbildung 12.6: Desktopeinstellungen, Register Mail – Mailverschlüsselung verbieten

12.5.3. Mails beim Zustellen verschlüsseln

Unverschlüsselte Mails können bei der Zustellung vom Mail-Router mit dem Schlüssel des Empfängers verschlüsselt werden. Konfigurieren können Sie dies entweder als globale Vorgabe im Konfigurationsdokument des Servers oder als individuelle Einstellung im Personendokument.

Um alle Mails bei der Zustellung zu verschlüsseln, aktivieren Sie im Konfigurationsdokument des Mailserver im Register **Router/SMTP > Beschränkungen und Steuerungen... > Zustellung** die Einstellung **Alle zugestellten Mails verschlüsseln**:

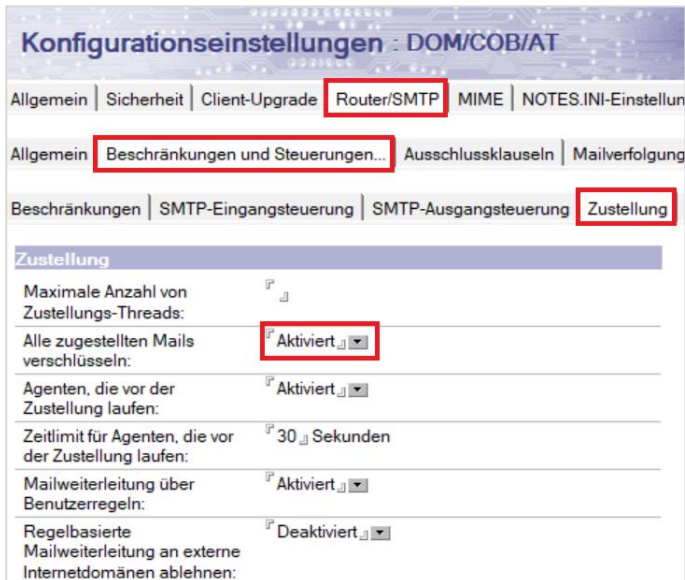


Abbildung 12.7: Konfigurationsdokument, Verschlüsseln zugestellter Mails

Um nur die Mails an bestimmte Personen bei der Zustellung zu verschlüsseln, setzen Sie im Personendokument die Einstellung **Eingehende unverschlüsselte Mail vor dem Speichern in Maildatei verschlüsseln** auf »Ja«:

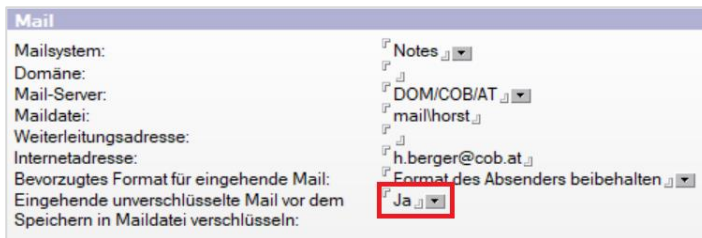


Abbildung 12.8: Personendokument, Bereich Mail

12.6. Feldverschlüsselung

Felder können sowohl über einen oder mehrere Öffentliche Schlüssel (asymmetrisch) als auch über einen oder mehrere Geheimschlüssel (symmetrisch) verschlüsselt werden.

Der Feldinhalt steht dann nur noch für Benutzer zur Verfügung, die über einen passenden Schlüssel verfügen.

Achtung: Verschlüsselte Felder können nicht in Ansichtspalten angezeigt werden.

Der Vorteil der Anwendung symmetrischer Verfahren besteht darin, dass der Schlüssel an mehrere Personen verteilt werden kann. Die Verwaltung symmetrischer Schlüssel ist jedoch aufwendig: Jeder Notes-Benutzer kann einen neuen Geheimschlüssel in seiner ID-Datei erstellen, aber nur Entwickler können ihn auf Felder anwenden. Diese müssen sich dann darum kümmern, dass alle beteiligten Personen den Schlüssel erhalten. Ein Verteilen ist per Mail oder via Export in eine Schlüsseldatei möglich. Problematisch wird die Sache dann, wenn ein Schlüssel ausgetauscht werden muss.

12.7. Signieren

12.7.1. Signieren von Mails

Der Absender verschlüsselt den Hash-Wert des Textes mit seinem Privaten Schlüssel aus der ID-Datei. Der Empfänger entschlüsselt den Hash-Wert mit dem öffentlichen Schlüssel des Absenders aus dem Domino-Verzeichnis und vergleicht das Ergebnis mit dem selbst berechneten Hash-Wert.

12.7.2. Signieren von Dokumentänderungen

In Workflow-Anwendungen sollte jeder Schritt signiert werden, was durch das Verwenden von signierten Abschnitten ermöglicht wird. So muss etwa das Genehmigungsfeld in einem eigenen Abschnitt liegen, welchen der Genehmiger durch einfaches Speichern des Dokuments signiert.

12.8. Verschlüsselung in ID-Dateien

Eine Notes-ID ist eine Binärdatei, die einen Benutzer oder Server bzw. einen Zertifizierer (inklusive ID-Vault) eindeutig identifiziert. Sie enthält die folgenden Informationen:

Komponente	Erklärung
Name	Der vollständige Name des Benutzers, Servers oder Zertifizierers
ID-Typ	»Hierarchischer Benutzer oder Server« bzw. »Hierarchischer Zertifizierer« (auch für Vault-IDs)
Ablaufdatum	Das Ablaufdatum der ID-Datei
Zulassungen	Die von einer Zulassungsstelle ausgestellte Zulassung. Einer Server- oder Benutzer-ID können eine oder mehrere Zulassungen zugewiesen sein.
Öffentlicher Schlüssel	Dient zum Überprüfen und Verschlüsseln von Datenbanken, Dokumenten (Mailnachrichten) und Feldern. Notes speichert eine Kopie des öffentlichen Schlüssels jedes Benutzers im Domino-Verzeichnis.
Persönlicher Schlüssel	Dient zum Entschlüsseln von Datenbanken, Dokumenten (Mailnachrichten) und Feldern.
(Optional) ein oder mehrere Geheimschlüssel	Der Geheimschlüssel dient zum Verschlüsseln oder Entschlüsseln von Feldern. Diese Schlüssel werden gezielt an andere Benutzer verteilt, um sicherzustellen, dass nur sie bestimmte verschlüsselte Felder lesen können.
Kennwort	Das Kennwort ist in der Notes-ID nicht direkt enthalten, sondern der ganze Inhalt der ID wird mit dem Hashwert des Kennworts verschlüsselt, d. h. Sie geben das Kennwort ein, um den Inhalt der Notes-ID entschlüsseln zu können.

Tabelle 12.2: Die einzelnen Komponenten der ID-Datei

Informationen über die eigene ID-Datei können Sie im Notes-Client über den Befehl **Datei > Sicherheit > Benutzersicherheit...** abrufen.

Andere ID-Dateien können Sie mithilfe des Domino-Administrators abfragen – sofern Sie ihr Kennwort wissen. Navigieren Sie dazu zum Register **Konfiguration** und wählen Sie: **Zertifizierung > ID-Eigenschaften**.

12.8.1. Interne Verschlüsselung

Der Inhalt der ID-Datei wird durch einen vom Hash-Wert des Kennworts abgeleiteten Schlüssel symmetrisch verschlüsselt. Standardmäßig ist der Verschlüsselungsgrad von der Länge des verwendeten RSA-Schlüssels abhängig – siehe Einstellung »Stärke auf Länge des RSA-Schlüssels basieren«. Bei RSA-Schlüssellängen größer oder gleich 1024 Bit wird 128 Bit RC2 verwendet. Unter 1024 Bit wird die ID-Datei mit einem 64-Bit langen Schlüssel verschlüsselt. Die Einstellungen für die interne Verschlüsselung können Sie beim Registrieren eines Benutzers über die Schaltfläche **Kennwortoptionen** festlegen:

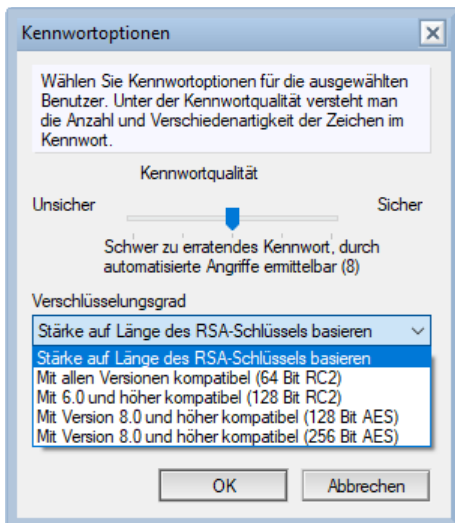


Abbildung 12.9: Der Dialog Kennwortoptionen mit aufgeklappter Liste der Verschlüsselungsgrade

Danach kann der Benutzer bei jeder Kennwortänderung selbst auswählen, welcher Verschlüsselungsgrad zur Anwendung kommen soll. Die Entscheidung sollten Sie allerdings nicht Ihren Anwendern überlassen, sondern den gewünschten Verschlüsselungsgrad via Sicherheitsrichtlinie selbst festlegen. Ich würde nur noch 256 Bit AES verwenden – dieser Standard wurde bereits mit Version 8.0.1 eingeführt.

Um die interne Verschlüsselung der ID-Dateien zu erhöhen, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Personen und Gruppen** und wählen Sie die Ansicht **Einstellungen**.
2. Erstellen Sie entweder über die Schaltfläche **Einstellungen hinzufügen... > Sicherheit** eine neue Sicherheitseinstellung oder bearbeiten Sie eine vorhandene.
3. Wählen Sie das Register **Kennwortverwaltung > Kennwortverwaltung - Allgemein** und dann den Abschnitt **Verschlüsselungseinstellungen der ID-Datei**.
4. Wählen Sie im Feld **Vorgeschriebener Verschlüsselungsstandard** den Wert »Mit Release 8 und höher kompatibel (256 Bit AES)«:



Abbildung 12.10: Sicherheitseinstellungen, Register Kennwortverwaltung

5. Speichern und schließen Sie das Dokument.

Sollten Sie eine neue Sicherheitseinstellung erstellt haben, vergessen Sie nicht, diese auch einer Richtlinie zuzuordnen, da die Konfigurationsänderung sonst nicht greift!

Der Verschlüsselungsgrad 256-Bit-AES wird beim nächsten Serverzugriff des Notes-Clients in die ID-Datei übertragen. Wie in Abbildung 12.11 ersichtlich, kann der Anwender danach den Verschlüsselungsgrad bei einer Kennwortänderung nicht mehr ändern:

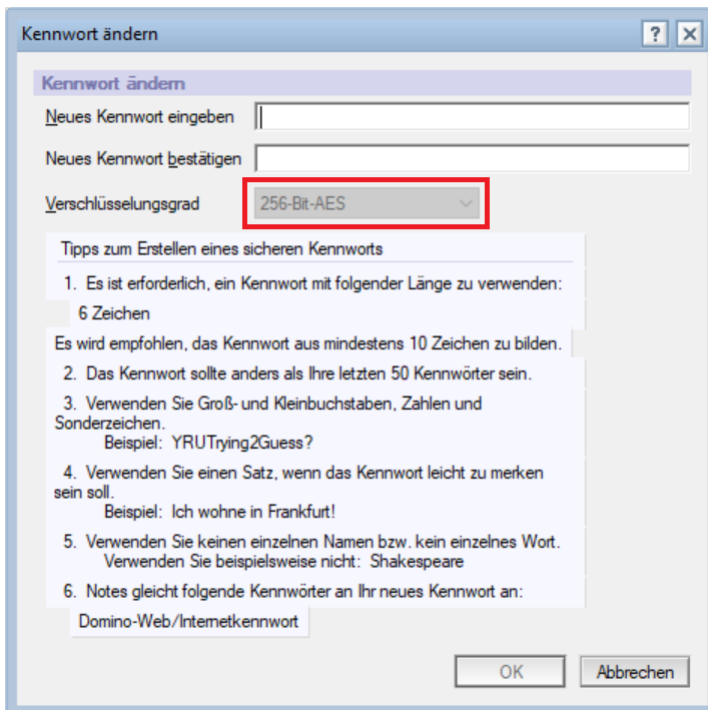


Abbildung 12.11: Der Dialog Kennwort ändern

Achtung: Ältere Clients (vor Version 8.0.1) können eine ID-Datei mit einem Verschlüsselungsgrad von 256-Bit nicht mehr lesen!

Die verfügbaren Verschlüsselungsgrade sind abhängig von der Domino-Version. Eine Aufstellung finden Sie in Tabelle 12.3:

Ab Version	Lesen Bit	Schreiben Bit
5	64, 40	64
6	128, 64, 40	64
7	128, 64, 40	128, 64
8.0.1	256, 128, 64, 40	256 AES, 128 AES, 128 RC2, 64 RC2

Tabelle 12.3: Verschlüsselungsgrad von ID-Dateien abhängig von der Notes-Version

Welcher Verschlüsselungsgrad aktuell verwendet wird, sehen Sie in den ID-Eigenschaften:

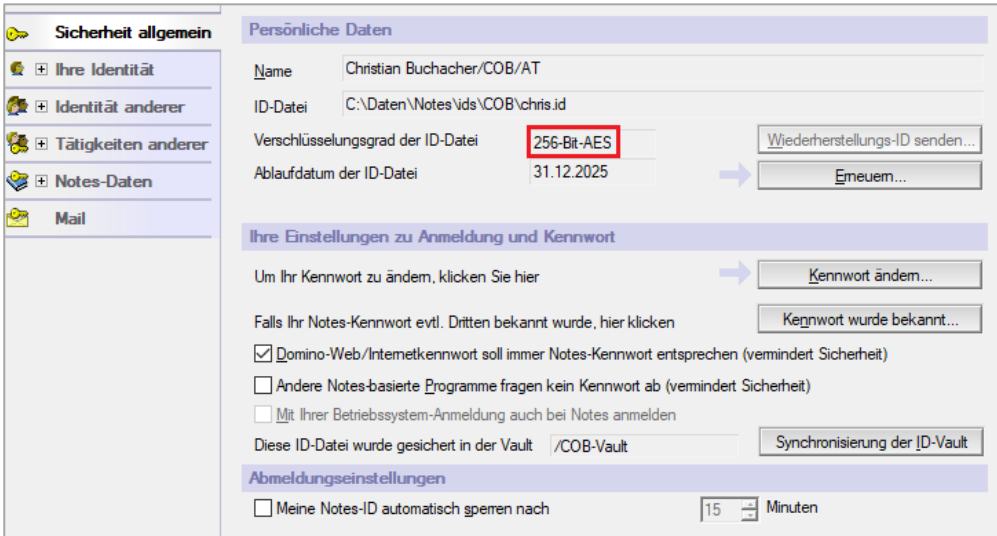


Abbildung 12.12: Der Dialog Benutzersicherheit

Beachten Sie, dass eine Erhöhung des Verschlüsselungsgrads ohne Kennwortänderung nicht möglich ist. Um einen höheren Verschlüsselungsgrad auszurollen, müssen Sie daher das Kennwort ablaufen lassen, sodass der Benutzer gezwungen ist, ein neues zu vergeben. Lesen Sie dazu Kap. 13.3.4 Kennwort überprüfen oder ablaufen lassen, ab Seite 344.

Ab Version 8.0.1 kann AES auch zur Mail- und Dokument-Verschlüsselung sowie bei SSL verwendet werden.

- > Benutzer müssen dazu mindestens einen 1024-Bit langen RSA-Schlüssel besitzen!
- > Dieses Feature kann über die Sicherheitsrichtlinie aktiviert werden: »FIPS-140-2-Algorithmen für Notes-Verschlüsselung verwenden (erfordert Server und Client der Version 8.0.x oder höher)« (Register Schlüssel und Zertifikate)
- > In einer gemischten Umgebung kann die Eigenschaft auch pro User gesetzt werden: Register **Personen und Gruppen, Werkzeuge > Verschlüsselungsfunktionen:**

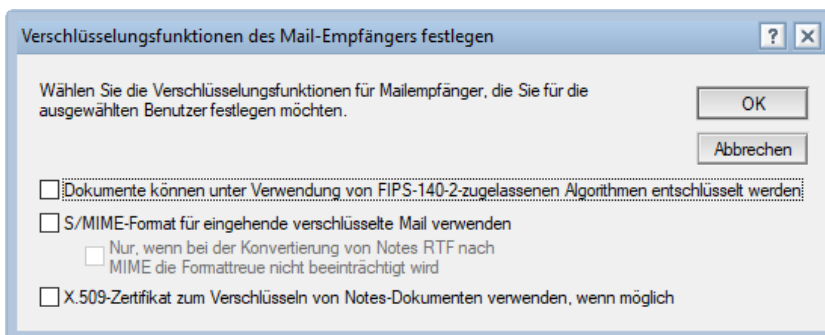


Abbildung 12.13: Der Dialog Verschlüsselungsfunktionen

12.8.2. RSA-Verschlüsselung

Auch RSA-Schlüssellängen sind von der Notes-Version abhängig:

- > 512/630 (R5)
- > 630/1024 (R6/6.5)
- > 630/1024/2048 (R7)
- > 630/1024/2048/4096/8192 (ab R8)

Beachten Sie, dass Domino ab Version 8 alle angegebenen Schlüssellängen zwar lesen aber nicht schreiben kann. (Dabei handelt es sich um eine Vorbereitung auf zukünftige Versionen.)

Domino 8 und höher kann:

- > 2048 Bit RSA-Schlüssel für Benutzer und Server lesen **und schreiben**
- > 4096 Bit RSA-Schlüssel für Benutzer und Server lesen
- > 4096 Bit RSA-Schlüssel für Zertifizierer lesen **und schreiben**
- > 8192 Bit RSA-Schlüssel für Zertifizierer lesen

Die in einer ID-Datei verwendete RSA-Schlüsselstärke können Sie ebenfalls über die ID-Eigenschaften einsehen. Navigieren Sie dazu im Domino-Administrator zum Register **Konfiguration** und wählen in den Werkzeugen den Befehl **Zertifizierung > ID-Eigenschaften**. Wählen Sie die zu prüfende ID-Datei aus und geben Sie bei Bedarf das Kennwort ein. Wechseln Sie im Dialog ID-Eigenschaften zum Bereich **Ihre Identität > Ihre Zertifikate** und wählen Sie ein Zertifikat aus der Liste. Hier ein Beispiel für eine Zertifizierer-ID:

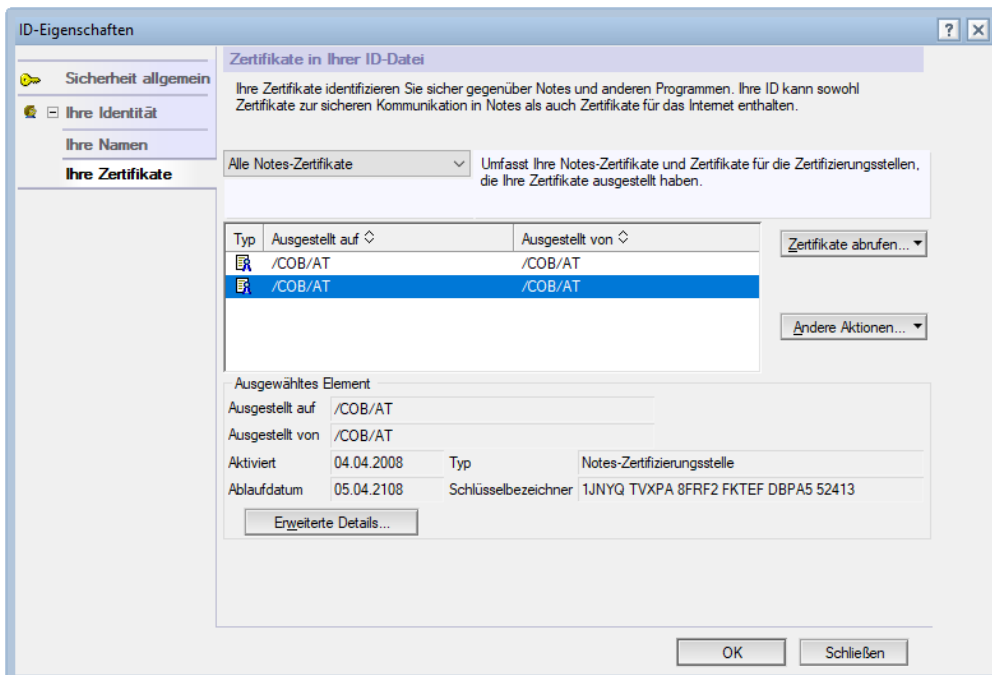


Abbildung 12.14: Der Dialog ID-Eigenschaften, Bereich Ihre Identität > Ihre Zertifikate

Klicken Sie dann auf die Schaltfläche **Erweiterte Details...**

Im Feld **Schlüsselstärke** sehen Sie die aktuell verwendete RSA-Schlüssellänge:

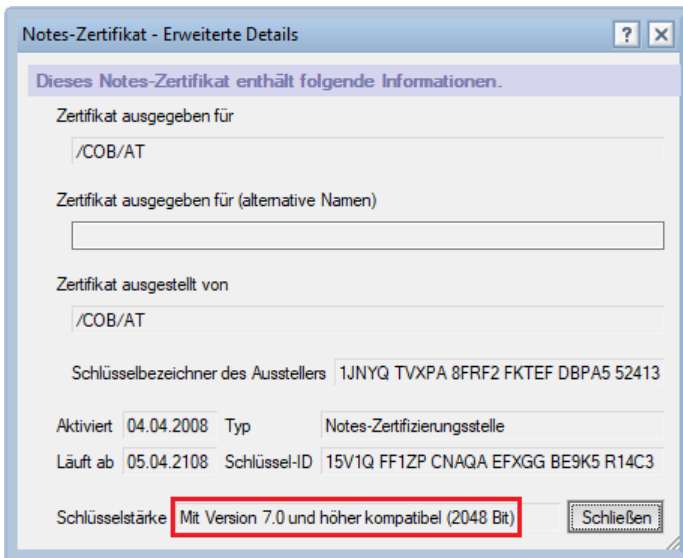


Abbildung 12.15: ID-Eigenschaften – Ihre Zertifikate, erweiterte Details

13. Das Domino-Sicherheitsmodell

- > 13.1 Übersicht über die einzelnen Sicherheitsebenen, Seite 335
- > 13.2 Serversicherheit, Seite 336
- > 13.3 ID-Sicherheit, Seite 342
- > 13.4 Gemeinsame Notes-Anmeldung, Seite 350
- > 13.5 Nachruf: Einmalige Notes-Anmeldung, Seite 352
- > 13.6 Das Internetkennwort, Seite 353
- > 13.7 Verzeichnissicherheit, Seite 357
- > 13.8 Datenbanksicherheit, Seite 358
- > 13.9 Ausführungskontrolllisten, Seite 362
- > 13.10 Gestaltungssicherheit, Seite 366

13.1. Übersicht über die einzelnen Sicherheitsebenen

In der Dokumentation des Herstellers HCL finden sich die folgenden Sicherheitsebenen:

1. Physische Sicherheit
2. Betriebssystemsicherheit
3. Netzwerksicherheit
4. Serversicherheit
5. ID-Sicherheit
6. Verzeichnissicherheit
7. Datenbanksicherheit
8. Gestaltungssicherheit
9. Dokumentsicherheit
10. Feldverschlüsselung

Die ersten drei Sicherheitsebenen liegen außerhalb des Rahmens dieses Buches. Darum muss sich Ihr Unternehmen bereits gekümmert haben, bevor Sie den ersten Domino-Server einrichten. Ich möchte zum Vermeiden der größten Fehler jedoch ein paar Punkte ansprechen.

Zur **physischen Absicherung** Ihrer Server gehört natürlich der Schutz vor Diebstahl oder mutwilliger Zerstörung der Hardware, aber auch vor Umwelteinflüssen wie Nässe oder Überhitzung.

Zur **Betriebssystemsicherheit** gehört vor allem, den direkten Zugriff (also unter Umgehung des Domino-Servers) auf das Dateisystem zu verhindern. Gelingt es, eine Datenbank direkt zu öffnen,

können Sicherheitsfeatures wie Zugriffskontrolllisten umgangen werden. Datenbanken im Cache können zwar nicht direkt geöffnet werden, da sie vom Domino-Server gesperrt sind, aber sie können etwa im laufenden Betrieb wegekopiert werden. Erlangt ein Angreifer über Tools wie Remote Desktop oder TeamViewer Zugriff auf den Server, kann er auch Prozesse beenden und dann Programme oder Datenbanken löschen.

Damit kommen wir zur **Netzwerksicherheit**, die durch Router, Firewalls und Proxy-Server gewährleistet wird. Netzwerkverbindungen erlauben für bestimmte Benutzer über bestimmte Protokolle (wie NRPC, HTTP, LDAP, IMAP u. a.) Zugriff auf bestimmte Ziele. Dabei handelt es sich um ein besonders komplexes Thema, das den Rahmen dieses Buches mehr als sprengen würde. Hüten Sie sich vor Netzwerkfreigaben, verwenden Sie den Windows-Server, der Ihren Domino-Server hostet, keinesfalls auch als Dateiserver.

13.2. Serversicherheit

Damit sind wir endlich in medias res, also beim Domino-Server angelangt! Welche Regeln hier gelten, hängt vom verwendeten Protokoll ab. Betrachten wir zunächst den Zugriff via NRPC, also über eine normale Notes-Verbindung: Um Zugriff auf den Server zu erlangen, muss der Benutzer mit diesem **authentifizieren** können.

13.2.1. Authentifizierung

Bei der **Authentifizierung** handelt es sich vereinfacht ausgedrückt um einen Schlüsselvergleich. Die Authentifizierung setzt das NRPC-Protokoll voraus und findet daher nur zwischen Notes-Client und Domino-Server bzw. zwischen zwei Domino-Servern statt. Es werden zwei Prüfungen vorgenommen:

- > 1. Validierung des Öffentlichen Schlüssels mithilfe des Zertifikats
- > 2. Gegenseitige Authentifizierung via Challenge-Response-Verfahren:
 - Der Server erzeugt eine Zufallszahl, verschlüsselt sie mit dem Öffentlichen Schlüssel des Benutzers und überträgt das Ergebnis.
 - Der Benutzer entschlüsselt die Zahl und überträgt sie verschlüsselt mit dem Öffentlichen Schlüssel des Servers zurück.
 - Der Server entschlüsselt das Ergebnis und vergleicht es mit der ursprünglichen Zahl.
 - Dann wird ein umgekehrter zweiter Durchgang vorgenommen.

Wer kann miteinander authentifizieren?

1. Benutzer und Server derselben Organisation (Regel des »gemeinsamen Vorfahrens« auf Zertifikatebene)
2. Benutzer und Server aus anderen Domino-Organisationen, für die ein Gegenzertifikat ausgestellt wurde

Über das NRPC-Protokoll ist auch ein anonymer Zugriff möglich, per Vorgabe aber deaktiviert. Er kann bei Bedarf aktiviert werden, etwa um Benutzern oder Servern aus anderen Organisationen Zugriff auf bestimmte Ressourcen zu gewähren, ohne ein Gegenzertifikat austauschen zu müssen. (Die Aktivierung erfolgt im Serverdokument, Register Sicherheit.)

13.2.2. Querzulassung

Um Benutzern oder Servern aus anderen Organisationen Zugriff auf Ihr Notes-Umfeld zu gewähren bzw. auch, um digitale Signaturen von Benutzern aus anderen Organisationen verifizieren zu können, muss eine Querzulassung (Cross Certificate) ausgetauscht werden. Dieser Vorgang wird auch **Erstellen eines Gegenzertifikats** bzw. **Gegenzertifizieren** genannt. Notwendig wird dies, wenn Notes-Mails oder Notes-Datenbanken zwischen zwei Organisationen ausgetauscht oder mehrere Organisationen in ein Domino-Verzeichnis aufgenommen werden sollen.

Auf welcher Ebene in der Hierarchie Sie das Gegenzertifikat austauschen, entscheidet, worauf die Gegenseite Zugriff erhält. Lässt Ihr eigener Unternehmenszertifizierer etwa den fremden Unternehmenszertifizierer zu, erhalten die Benutzer und Server der fremden Organisation Zugriff auf alle Ihre Server und im Gegenzug Ihre Benutzer und Server Zugriff auf alle fremden Server. Diese Ebene wählen Sie, wenn mehrere Organisationen sich ein Domino-Verzeichnis teilen. Wählen Sie auf beiden Seiten eine Server-ID, erhalten nur die beiden Server aufeinander Zugriff. Diese Ebene ist die beste Wahl, wenn nur Mails ausgetauscht oder einzelne Anwendungen repliziert werden sollen. Alle weiteren Kombinationen entnehmen Sie der folgenden Tabelle:

	Zertifizierer /HAL	Server HP01/HAL
Zertifizierer /COB/AT	Alle Benutzer und Server von /HAL dürfen auf alle Server von /COB/AT zugreifen und umgekehrt.	Der Server HP01/HAL darf auf alle Server von /COB/AT zugreifen. Alle Benutzer und Server von /COB/AT dürfen auf den einen Server HP01/HAL zugreifen.
Server DOM/COB/AT	Alle Benutzer und Server von /HAL dürfen nur auf Server DOM/COB/AT zugreifen. Server DOM/COB/AT darf auf alle Server von /HAL zugreifen.	Der Server HP01/HAL darf auf Server DOM/COB/AT zugreifen und umgekehrt.

Tabelle 13.1: Kombinationsmöglichkeiten bei der Querzulassung

Wurden die beteiligten Server von einer Unterorganisation (OU) zertifiziert, gibt es noch mehr Kombinationsmöglichkeiten.

Mit »zugreifen« ist gemeint, dass beide Seiten miteinander authentifizieren können. Ein tatsächlicher Zugriff auf den fremden Server ist nur möglich, wenn es auch die Serverzugriffskontrollliste erlaubt. Ein Zugriff auf eine fremde Ressource ist nur möglich, wenn es die Datenbankzugriffskontrollliste erlaubt.

Das Erstellen eines Gegenzertifikats kann auf mehrere Arten erfolgen:

- > auf Anfrage (On Demand)
- > per Datei

13.2.2.1. Ein Gegenzertifikat »auf Anfrage« erstellen

Voraussetzung ist, dass Sie zum Server der fremden Organisation eine Verbindung via NRPC (Port 1352) aufbauen können.

Zum Erstellen eines Gegenzertifikats »auf Anfrage« (on Demand), gehen Sie wie folgt vor:

1. Rufen Sie im Notes-Client den Öffnen-Dialog auf (z. B. durch Drücken der Tasten [Strg]+[O]) und tippen Sie den Netzwerknamen ein, unter dem der fremde Domino-Server erreichbar ist (Hostnamen oder IP-Adresse).
2. Notes zeigt Ihnen an, dass es für die fremde Organisation (in unserem Beispiel /HAL) kein Gegenzertifikat gibt:

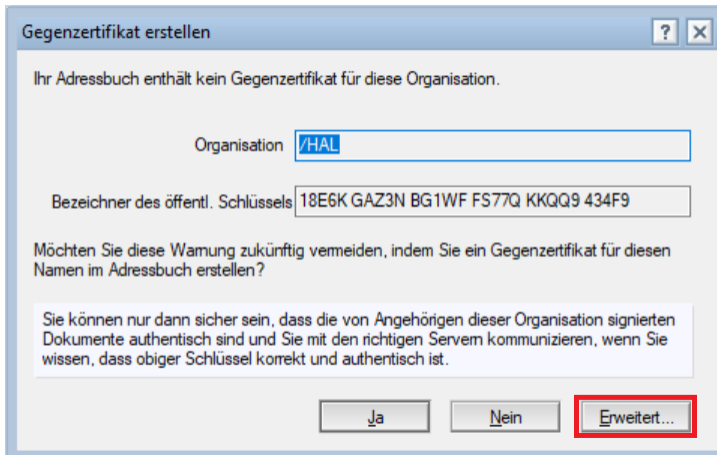


Abbildung 13.1: Der Dialog Gegenzertifikat erstellen

Sollten Sie diesen Dialog nicht erhalten, überprüfen Sie, ob es in Ihrer Kontakte-Anwendung bereits ein Gegenzertifikat gibt. Wählen Sie dazu im Navigator auf der linken Seite **Erweitert** und dann die Ansicht **Zertifikate**. Sollte das Gegenzertifikat innerhalb der Kategorie **Notes-Gegenzertifikate** vorhanden sein, löschen Sie es.

3. Klicken Sie auf die Schaltfläche **Erweitert...**
4. Wählen Sie Ihren Server und die ID-Datei, mit der Sie das Gegenzertifikat austauschen wollen, in unserem Beispiel die beiden Zertifizierer von /COB/AT und /HAL:

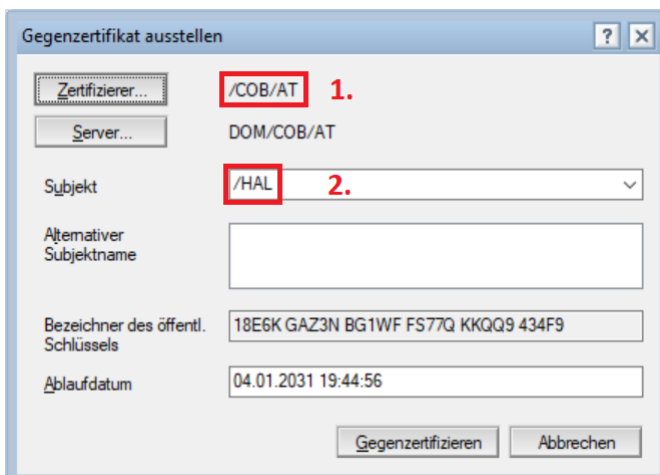


Abbildung 13.2: Der Dialog Gegenzertifikat ausstellen

5. Klicken Sie auf **Gegenzertifizieren**.
Danach wird nochmals eine Warnung angezeigt. Hat Sie die andere Seite bereits zugelassen, klicken Sie auf die Schaltfläche **Auf Server zugreifen**, ansonsten klicken Sie auf **Abbrechen**:

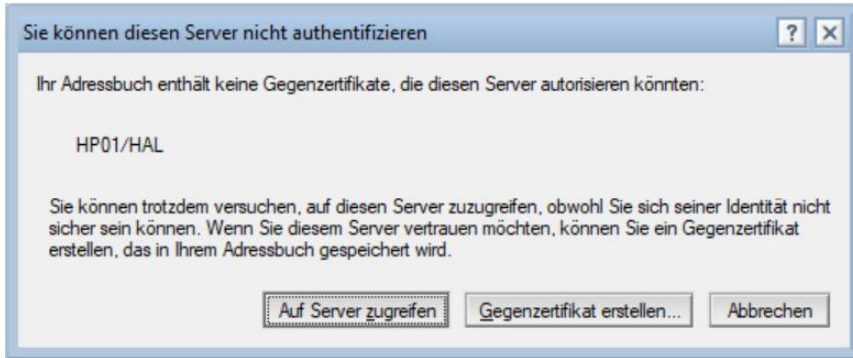


Abbildung 13.3: Warnung Authentifizierung nicht möglich

6. Klicken Sie auf **Abbrechen**.

Damit ein beidseitiger Zugriff möglich ist, etwa zum Austauschen von Notes-Mails, muss auch die Gegenseite ein Gegenzertifikat ausstellen.

Das Ergebnis dieser Operation ist ein Gegenzertifikat im Domino-Verzeichnis. Sie finden es im Admin-Client im Register **Konfiguration** in der Ansicht **Sicherheit > Zertifikate > Zertifikate** unter der Kategorie **Notes-Gegenzertifikate**:



Abbildung 13.4: Gegenzertifikatsdokument im Domino-Verzeichnis

Und das Praktische an dieser Lösung: Wollen Sie irgendwann nicht mehr mit der fremden Organisation zusammenarbeiten, löschen Sie das Gegenzertifikat aus dem Domino-Verzeichnis, um ihr den Zugriff zu entziehen!

13.2.2.2. Ein Gegenzertifikat via Datei erstellen

Wenn der Zugriff auf den Server der fremden Organisation (noch) nicht möglich ist, können Sie auch eine ID-Datei gegenzertifizieren. Dabei kann es sich um eine Server-ID oder um eine Zertifizierer-ID handeln. Erhalten Sie die ID-Datei wirklich von einem fremden Unternehmen, handelt es sich wahrscheinlich um eine sogenannte **Sichere Kopie** (Save Copy), die nur das Ausstellen eines Gegenzertifikats erlaubt. (Eine sichere Kopie erzeugen Sie in den ID-Eigenschaften, Register **Ihre**

Identität > Ihre Zertifikate über die Schaltfläche **Andere Aktionen... > Notes ID exportieren (Sichere Kopie)...**

Zum Gegenzertifizieren einer ID-Datei navigieren Sie im Domino-Administrator zum Register **Konfiguration** und wählen das Werkzeug **Zertifizierung > Gegenzertifizieren...**

Wählen Sie im ersten Schritt den Zertifizierer, mit dem die Datei gegenzertifiziert werden soll, sowie den Server, in dessen Domino-Verzeichnis das Gegenzertifikat gespeichert werden soll.

Wählen Sie dann die ID-Datei aus und klicken Sie auf die Schaltfläche **Gegenzertifizieren**.

13.2.3. Den Serverzugriff steuern

Die erste Voraussetzung für den Zugriff auf den Server, eine erfolgreiche Authentifizierung, hätten wir damit geschafft. Aber es ist nicht gesagt, dass jeder, der mit dem Server authentifizieren kann, auch Zugriff erhalten soll. Und so ist es auch nicht, es gilt noch eine zweite Hürde zu bewältigen: die Serverzugriffskontrollliste!

Unter **Serverzugriffskontrollliste** (Server Access Control List) versteht man den Abschnitt **Auf Server zugreifen** im Serverdokument, Register **Sicherheit**.

13.2.3.1. Das Feld Serverzugriff

Ist dieses Feld leer, dürfen alle Benutzer und Server auf diesen Server zugreifen, die mit ihm authentifizieren konnten. Ist das Feld beschickt, dürfen nur noch die angegebenen Benutzer oder Server zugreifen.

Aktivieren Sie das Feld **In allen vertrauenswürdigen Verzeichnissen aufgeführte Benutzer**, werden ID-Dateien ohne Personendokument in einem vertrauenswürdigen Domino-Verzeichnis vom Serverzugriff ausgeschlossen.

Haben Sie diese Option aktiviert, müssen Sie die Server zusätzlich ins Feld **Serverzugriff** aufnehmen, da Server ja nicht über ein Personendokument verfügen, z. B. über die Gruppe »LocalDomainServers«.

Verwenden Sie in diesem Feld nur Server, Gruppen oder Verweise auf die Hierarchie (z. B. »*/COB/AT«).

13.2.3.2. Das Feld Kein Serverzugriff

Dieses Feld verweigert eingetragenen Benutzern und Servern den Zugriff, selbst wenn sie korrekt mit dem Server authentifizieren können. Mit dieser Option können Sie aus Ihrem Unternehmen ausgeschiedenen Personen den Zugriff verwehren.

Verwenden Sie in diesem Feld ausschließlich Gruppen vom Typ »Nur Negativliste«.

13.2.3.3. Weitere Felder

Ist das Feld **Datenbanken und Schablonen erstellen** leer, dürfen alle zugelassenen Benutzer und Server neue Datenbanken auf diesem Server erstellen. Ist das Feld beschickt, dürfen nur noch die angegebenen Benutzer und Server sowie die Administratoren Datenbanken erstellen.

Ist das Feld **Neue Repliken erstellen** leer, dürfen nur Administratoren Repliken auf diesem Server erstellen. Ist das Feld beschriftet, dürfen nur die angegebenen Benutzer und Server sowie die Administratoren Repliken erstellen.

Das Feld **Masterschablonen erstellen** steuert, wer aus Schablonen Masterschablonen machen darf. Mehr über Masterschablonen erfahren Sie in Kap. 11.2.1 Eine Schablone erstellen, ab Seite 306.

Der Bereich **Auf Server zugreifen** könnte etwa so konfiguriert werden:

Auf Server zugreifen	Wer kann -
Serverzugriff:	<input type="checkbox"/> In allen vertrauenswürdigen Verzeichnissen aufgeführte Benutzer und [IP] [] [v]
Kein Serverzugriff:	[IP] NoAccess [] [v]
Datenbanken und Schablonen erstellen:	[IP] LocalDomainAdmins LocalDomainDevelopers LocalDomainServers [] [v]
Neue Repliken erstellen:	[IP] LocalDomainAdmins LocalDomainServers [] [v]
Masterschablonen erstellen:	[IP] LocalDomainAdmins LocalDomainDevelopers [] [v]
Verwendung von Monitoren zulässig für:	[IP] [] [v]
Verwendung von Monitoren nicht zulässig für:	[IP] [] [v]
Vertrauenswürdige Server:	[IP] [] [v]

Abbildung 13.5: Die Serverzugriffskontrollliste im Serverdokument, Register Sicherheit

13.2.4. Abgänger ausschließen

Wenn jemand die Firma verlässt, können Sie nicht verhindern, dass er seine ID-Datei mitnimmt. Und die ID bleibt gültig, bis sie abläuft, was per Vorgabe zwei Jahre dauert. Wenn davon auch nur eine hypothetische Gefahr ausgeht (schließlich muss der Angreifer erst einmal ins Netzwerk kommen, bevor er Notes starten kann), sollten Sie den Zugriff für Abgänger immer sperren.

Hierfür bieten sich zwei Strategien an.

13.2.4.1. Durch Löschen des Personendokuments

Aktivieren Sie dazu im Serverdokument, Register **Sicherheit** im Bereich **Auf Server zugreifen** die Option **In allen vertrauenswürdigen Verzeichnissen aufgeführte Benutzer**

Mit dieser Einstellung können Personen ohne Personendokument per sofort nicht mehr zugreifen. Das ist zwar praktisch, andererseits geht damit die Verbindung zwischen E-Mail-Adresse und Maildatenbank verloren. Sie können die E-Mail-Adresse des gelöschten Benutzers jedoch als Synonym bei jemand anderem eintragen.

Achtung: Mit dieser Einstellung verlieren die Server den Zugriff und müssen im Feld **Serverzugriff** extra angegeben werden!

Auf Server zugreifen	Wer kann -
Serverzugriff:	<input checked="" type="checkbox"/> In allen vertrauenswürdigen Verzeichnissen aufgeführte Benutzer und <input type="checkbox"/> DOM/COB/AT <input type="checkbox"/> WS01/COB/AT
Kein Serverzugriff:	<input type="checkbox"/>

Abbildung 13.6: Option In allen vertrauenswürdigen Verzeichnissen aufgeführte Benutzer

13.2.4.2. Durch Aufnahme in eine Sperrgruppe

Erstellen Sie eine Gruppe vom Typ »Nur Negativliste« und vergeben Sie einen beliebigen Namen, z. B. »NoAccess«. Die Gruppe braucht vorerst keine Mitglieder zu haben.

Gruppe für Negativliste : NoAccess		
Allgemein	Kommentare	Administration
Allgemein		
Gruppenname:	<input type="text" value="NoAccess"/>	
Gruppentyp:	<input type="text" value="Nur Negativliste"/>	
Kategorie:	<input type="text"/>	
Beschreibung:	<input type="text"/>	
Maildomäne:	<input type="text"/>	
Internetadresse:	<input type="text"/>	
Methode zum automatischen Füllen:	<input type="text" value="Keine"/>	
Mitglieder:	<input type="text"/>	

Abbildung 13.7: Gruppe vom Typ »Nur Negativliste« zum Aussperren von Benutzern

Tragen Sie die Gruppe im Serverdokument, Register **Sicherheit**, im Bereich **Auf Server zugreifen** in das Feld **Kein Serverzugriff** ein.

Speichern und schließen Sie das Serverdokument und starten Sie den Server neu.

Wenn ein Mitarbeiter die Firma verlassen hat, nehmen Sie ihn in die Gruppe auf, und er wird sofort gesperrt. Diese Methode hat den Vorteil, dass das Personendokument zunächst intakt bleibt, und Mails so lange weiter zugestellt werden, bis Sie auch das Personendokument löschen.

13.3. ID-Sicherheit

In dieser Ebene wird manchmal zwischen **Client-Sicherheit** und **ID-Sicherheit** unterschieden. Unter Client-Sicherheit versteht man alle Schutzmechanismen, die einen unberechtigten Benutzer daran hindern, einen fremden Notes-Client zu starten. Dazu gehört etwa das Hochsetzen der Wartezeit nach mehrmaliger Falscheingabe des Kennworts. Wird die ID-Datei selbst angegriffen, etwa durch Tools wie »Lotus Notes Key«, geht es um die Themen Kennwort und interne Verschlüsselung.

13.3.1. Allgemeines zu Kennwörtern

Bei der klassischen Konfiguration muss sich jeder Benutzer mit zwei Kennwörtern auseinandersetzen: dem Notes-ID-Kennwort und dem Internetkennwort. Diese können auch synchronisiert werden, sodass sich der Benutzer nur noch ein Kennwort merken muss. Ab Domino 11 kann das

Internetkennwort auch aus dem ID-Vault ausgelesen werden, d. h. es ist dann identisch mit dem Notes-ID-Kennwort. Es gibt jedoch auch den umgekehrten Fall, bei dem das Kennwort aus der ID-Datei gelöscht und diese mit Windows-Mitteln (Microsoft DPAPI-Schnittstelle – siehe Kap. 13.4 Gemeinsame Notes-Anmeldung, ab Seite 350) verschlüsselt wird. Und letztendlich kann auch ganz auf Notes-eigene Kennwörter verzichtet und die Authentifizierung auf das Active Directory verlagert werden (SAML-Authentifizierung – in diesem Buch nicht behandelt.)

13.3.2. Kennwortlänge und Komplexität

Die nachfolgenden Betrachtungen sollen Ihnen ein Gefühl für Kennwortsicherheit vermitteln. Wichtig sind hier weniger die genauen Zahlen, sondern vielmehr die Verhältnisse zueinander:

- > 6 Zeichen nur Kleinbuchstaben: **308.915.776 Möglichkeiten**
 - Eine handelsübliche Core 2 Quad Q6600 CPU, die auf 3 GHz getaktet ist, (ergibt 45.423.600 Tastenanschläge pro Sekunde) errechnet das Kennwort in **6,8 Sekunden**
- > 6 Zeichen, Klein- und Großbuchstaben und Zahlen: **56.800.235.584 Kombinationen**
 - Um das Passwort zu knacken rechnet dieselbe Quad-CPU jetzt rund **21 Minuten**
- > 7 Zeichen, Klein- und Großbuchstaben und Zahlen
 - Die Quad-CPU rechnet jetzt fast **22 Stunden**
- > 8 Zeichen, Klein- und Großbuchstaben und Zahlen
 - Die Quad-CPU rechnet jetzt schon rund **2 Monate**
- > 10 Zeichen, Klein- und Großbuchstaben und Zahlen
 - Für die Berechnung bräuchte die Quad-CPU nun rund **600 Jahre!**
- > Würden im Kennwort zusätzlich noch Sonderzeichen verwendet, würde sich die Berechnungsdauer jeweils um ein Vielfaches verlängern!

Durch eine hohe Kennwortkomplexität wird also die Sicherheit erhöht. Aber wie können Sie komplexe Kennwörter bei Ihren Benutzern durchsetzen? Dafür bieten sich mehrere Methoden an.

13.3.3. Kennwortqualität

Bereits bei der Registrierung eines Benutzers lässt sich über die Schaltfläche **Kennwortoptionen...** eine sogenannte **Kennwortqualität** festlegen (siehe Abbildung 13.8).

Die Kennwortqualität ist nicht identisch mit der Kennwortlänge! Nachfolgend zur Veranschaulichung die Regeln für Kennwortqualität 8:

Es können 6 bis 10 Zeichen verwendet werden.

- > Bei 6 Zeichen Länge müssen 3 der 4 möglichen Zeichenarten verwendet werden.
- > Bei 8 Zeichen Länge müssen 2 der 4 möglichen Zeichenarten verwendet werden.
- > Bei 10 Zeichen Länge muss nur noch eine der 4 Zeichenarten verwendet werden.

Die möglichen Zeichenarten sind: Kleinbuchstaben, Großbuchstaben, Zahlen, Sonderzeichen.

Achtung: Die oben dargestellten Regeln für die Kennwortqualität sind nicht völlig kompatibel zu den Regeln in den Windows Gruppen-Policies. Je nach Einstellungen können sich daher Probleme bei der Synchronisierung mit dem Windows-Passwort ergeben!

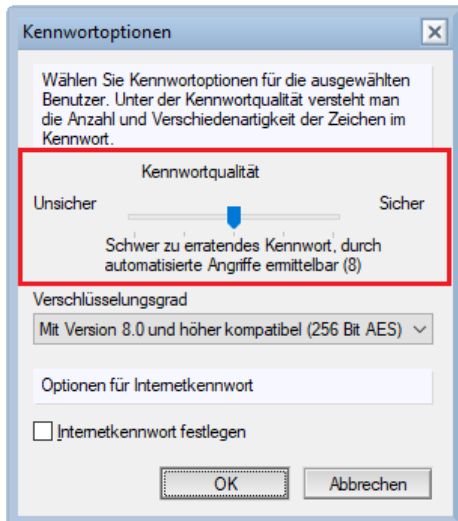


Abbildung 13.8: Dialog Kennwortoptionen

Testfrage: Welche Kennwortqualität müssen Sie einstellen, um das Kennwort »notes« zu ermöglichen?

(Antwort: Kennwortqualität 3)

Das Setzen einer Mindestkennwortqualität für den Zugriff auf den Domino-Server ist in der Sicherheitsrichtlinie, Register **Kennwortverwaltung** > **Kennwortverwaltung Allgemein** im Abschnitt **Einstellungen für Kennwortqualität** möglich:



Abbildung 13.9: Sicherheitsrichtlinie, Einstellungen für Kennwortqualität

Stellen Sie hier auf eine höhere Qualität um, gilt diese leider erst bei der nächsten Kennwortänderung. Das heißt, wenn Sie Ihre Benutzer zum Verwenden einer Mindestkennwortqualität zwingen wollen, müssen Sie das Kennwort auch noch ablaufen lassen!

13.3.4. Kennwort überprüfen oder ablaufen lassen

Per Vorgabe interessiert sich der Domino-Server nicht für ID-Datei-Kennwörter, Sie können ihn jedoch anweisen, das aktuelle Kennwort in einem Feld im Personendokument abzulegen, den sogenannten **Kennwortdigest**.

Erst damit können Benutzer:

- > dazu gezwungen werden, Kennwörter nach Ablauf einer gewissen Zeit zu ändern
- > daran gehindert werden, bereits verwendete Kennwörter zu wiederholen
- > daran gehindert werden, eine gekaperte ID-Datei mit einem kompromittierten Kennwort weiterzuverwenden

Um das Speichern des aktuellen Kennworts im Personendokument zu aktivieren, sind zwei Schritte nötig:

1. Sie weisen den Server an, Kennwörter zu überprüfen.
2. Sie legen fest, für welche Benutzer Kennwörter überprüft werden sollen.

13.3.4.1. Den Server anweisen Kennwörter zu überprüfen

Öffnen Sie das Serverdokument und navigieren Sie zum Register Sicherheit.

Setzen Sie im Abschnitt **Sicherheitseinstellungen** das Feld **Kennwörter von Notes-IDs überprüfen** auf »Aktiviert«:

Sicherheitseinstellungen	
Öffentliche Schlüssel vergleichen:	<input type="checkbox"/> Ja <input checked="" type="checkbox"/> Nein
Nichtübereinstimmungen von Öffentlichen Schlüsseln protokollieren:	<input type="checkbox"/> Ja <input checked="" type="checkbox"/> Nein
Anonyme Notes Verbindungen zulassen:	<input type="radio"/> Ja <input checked="" type="radio"/> Nein
Kennwörter von Notes-IDs überprüfen:	<input checked="" type="radio"/> Aktiviert <input type="radio"/> Deaktiviert

Abbildung 13.10: Serverdokument, Sicherheitseinstellungen

Danach sollten Sie den Server neu starten.

Diese Einstellung muss auf allen Servern, die die Überprüfung vornehmen sollen, aktiviert werden!

13.3.4.2. Festlegen, für welche Benutzer die Kennwortüberprüfung gilt

Sie könnten die Kennwortüberprüfung entweder im Personendokument der betroffenen Benutzer oder via Sicherheitsrichtlinie aktivieren.

Ein Aktivieren für einzelne Benutzer (mit Mehrfachauswahl) ist im Domino-Administrator, im Register **Personen und Gruppen** über den Befehl **Aktionen > Kennwortfelder festlegen** möglich.

Um die Kennwortüberprüfung via Sicherheitsrichtlinie zu aktivieren, setzen Sie im Register **Kennwortverwaltung > Kennwortverwaltung Allgemein** im Abschnitt **Kennwortverwaltungsoptionen** das Feld **Kennwort überprüfen anhand der Notes-ID-Datei** auf »Ja«.

Kennwortverwaltungsoptionen	
Benutzerdefinierte Kennwortrichtlinie für Notes-Clients verwenden:	<input type="checkbox"/> Ja <input checked="" type="checkbox"/> Nein
Kennwort überprüfen anhand der Notes-ID-Datei:	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein
Benutzer dürfen das Internetkennwort über HTTP ändern:	<input type="checkbox"/> Ja <input checked="" type="checkbox"/> Nein
Internetkennwort bei Änderung des Notes-Client-Kennworts aktualisieren:	<input type="checkbox"/> Ja <input checked="" type="checkbox"/> Nein
Andere Notes-basierte Programme fragen kein Kennwort ab (vermindert Sicherheit):	<input type="checkbox"/> Ja <input checked="" type="checkbox"/> Nein
Einmalige Anmeldung von Windows für Standard-Notes-Client aktivieren:	<input type="checkbox"/> Ja <input checked="" type="checkbox"/> Nein

Abbildung 13.11: Sicherheitsrichtlinie, Einstellungen für Kennwortqualität

In beiden Fällen wird bei der nächsten Benutzeranmeldung eine Anforderung an den Administrationsprozess gestellt, die Kennwort-Hashes einzutragen. Ausgeführt wird die Anforderung am Administrationsserver des Domino-Verzeichnisses, sorgen Sie also dafür, dass alle Server ihre Datenbank für Administrationsanforderungen mit diesem replizieren.

Beachten Sie, dass Benutzer mit ID-Dateien auf anderen Clients, die unterschiedliche Kennwörter verwenden, danach nicht mehr zugreifen können. Sollte es damit Probleme geben, leeren Sie das Feld mit dem Kennwortdigest, und ein Zugriff sollte wieder klappen:

Kennwortverwaltung	
Kennwort überprüfen:	<input type="checkbox"/> Kennwort nicht überprüfen ▾
Intervall für Kennwortänderung:	<input type="text" value="0"/> ▾
Nachfrist:	<input type="text" value="0"/> ▾
Letzte Änderung am:	09.03.2021 12:41:54 GMT
Digest des Kennworts:	<input type="text" value="EBDAECC4922617418D0A5BDAB8F4BD6F"/> ▾
Letzte Änderung am: (Internetkennwort)	30.09.2018 12:48:49 CEDT
Benutzer muss das Internetkennwort bei der nächsten Anmeldung ändern:	<input type="checkbox"/> Ja

Abbildung 13.12: Personendokument, Kennwortdigest

13.3.4.3. Kennwörter ablaufen lassen

Auch das Ablaufen von Kennwörtern kann im Personendokument oder in der Sicherheitsrichtlinie konfiguriert werden. Da die Sicherheitsrichtlinie wesentlich mehr Möglichkeiten bietet, würde ich die Konfiguration unbedingt dort vornehmen.

Geben Sie im Feld **Ablauf des Kennworts erzwingen** an, wo das Kennwort ablaufen soll. Eine mögliche Strategie wäre, es nur in Notes ablaufen zu lassen, wenn 1. das Internetkennwort im ID-Vault überprüft wird (d. h. es gibt kein eigenes Internetkennwort, siehe Kap. 13.6.1 auf Seite 353) oder 2. das Internetkennwort mit dem Notes-ID-Kennwort synchronisiert wird.

Kennwortablaufseinstellungen	
Ablauf des Kennworts erzwingen	<input type="text" value="Nur Notes"/> ▾
Intervall für Kennwortänderung	<input type="text" value="365"/> Tage
Nachfrist zulassen	<input type="text" value="0"/> Tage
Kennwortprotokoll (nur Notes)	<input type="text" value="10"/> Kennwörter
Warnfrist	<input type="text" value="30"/> Tage
Benutzerdefinierte Warnnachricht	<input type="text"/> ▾

Abbildung 13.13: Sicherheitsrichtlinie, Einstellungen für das Ablaufen des Kennworts

Geben Sie im Feld **Intervall für Kennwortänderung** an, nach wie vielen Tagen das Kennwort abläuft.

Im Feld **Warnfrist** steuern Sie, ab wann eine Warnung angezeigt wird: »Ihr Kennwort läuft in *n* Tagen ab. Bitte ändern Sie Ihr Kennwort.«

Geben Sie im Feld **Nachfrist zulassen** eine Zahl größer 0 ein, ist auch eine Anmeldung nach dem Ablauf des Kennworts noch zulässig. Die Warnung lautet dann entsprechend: »Ihr Kennwort ist vor *n* Tagen abgelaufen. Bitte ändern Sie Ihr Kennwort.«

Die Kombination aus Warnfrist und Nachfrist sollte länger sein, als ein Urlaub dauern kann, da der Anwender sonst keine Warnung erhält.

Über das Feld **Kennwortprotokoll (nur Notes)** steuern Sie, ab wann ein Kennwort wiederholt werden darf. Steht hier 10, darf das 11. Kennwort wieder dem 1. entsprechen.

Ist das Kennwort einmal abgelaufen, ist ein Zugriff erst wieder möglich, nachdem es geändert wurde.

13.3.5. Benutzerdefinierte Kennwortrichtlinie

Die sogenannte **benutzerdefinierte Kennwortrichtlinie** (Custom Password Policy) ist leistungsfähiger und flexibler als die Verwendung einer Kennwortqualität:

- > Es können wesentlich mehr Regeln aufgestellt werden, z. B., dass das Kennwort nach dem ersten Start geändert werden muss.
- > Sie gilt »sofort«, d. h. die neuen Regeln werden beim nächsten Zugriff auf den Server in die ID-Datei kopiert und gelten dann beim nachfolgenden Client-Neustart.
- > Ist das Notes-ID-Kennwort nicht ausreichend komplex, ist kein Serverzugriff mehr möglich und der Benutzer wird aufgefordert, ein komplexeres Kennwort einzugeben. Es ist also nicht nötig, das Kennwort auch noch ablaufen zu lassen, was Sie aber natürlich zusätzlich konfigurieren können, denn auch komplexe Kennwörter sollten einmal geändert werden.
- > Benutzerdefinierte Kennwortrichtlinien sind im Gegensatz zur Kennwortqualität kompatibel zu Windows-Gruppenrichtlinien.

Die Aktivierung der benutzerdefinierten Kennwortrichtlinie erfolgt in der Sicherheitsrichtlinie, Register **Kennwortverwaltung**. Setzen Sie das Feld **Benutzerdefinierte Kennwortrichtlinie für Notes-Clients verwenden** auf »Ja«, wird ein zusätzliches Register eingeblendet:

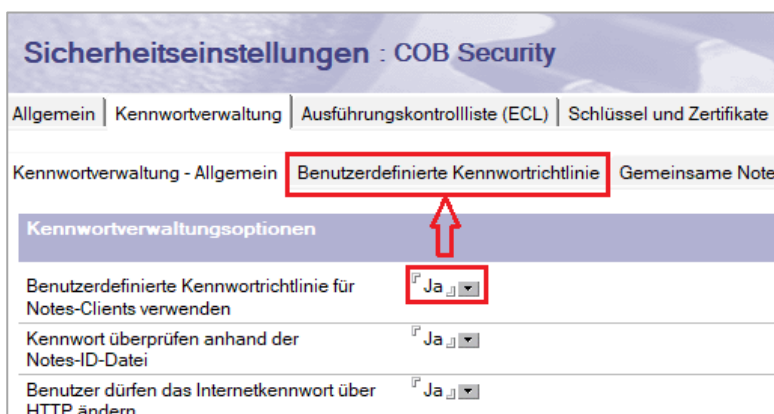


Abbildung 13.14: Sicherheitsrichtlinie, Aktivieren der benutzerdefinierten Kennwortrichtlinie

Die folgenden Zusatzregeln sind möglich:

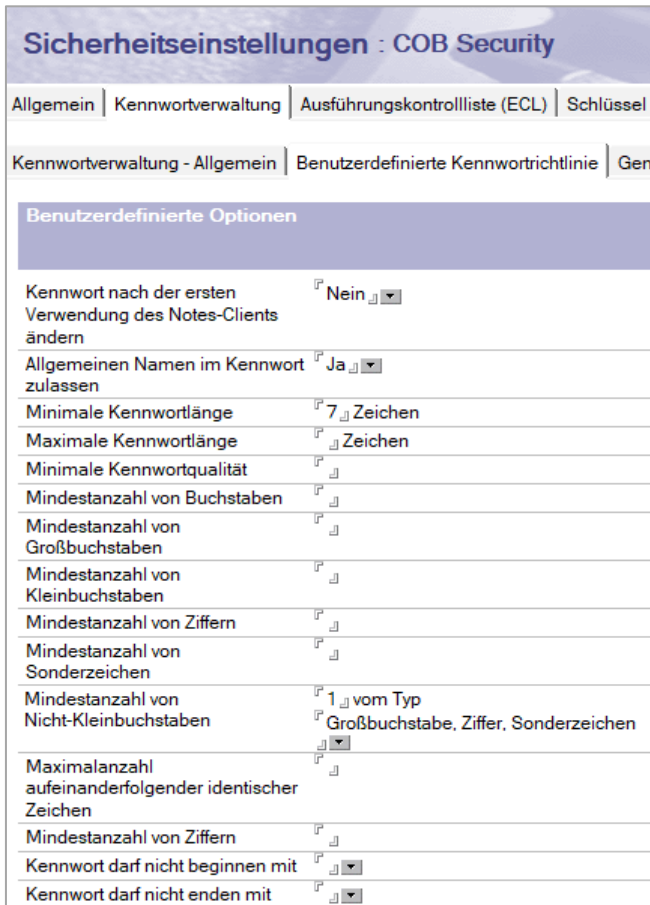


Abbildung 13.15: Sicherheitsrichtlinie, Beispiel für eine benutzerdefinierte Kennwortrichtlinie (Erklärung im Text)

Die Vorteile der benutzerdefinierten Kennwortrichtlinie sind:

- > Der Anwender kann gezwungen werden, das Kennwort bei der ersten Anmeldung zu ändern.
- > Sie können die Verwendung von Namenskomponenten im Kennwort verbieten (kein »otto123«, wenn der Benutzer Otto Huber heißt).
- > Sie können alternativ auf Großbuchstaben, Zahlen & Sonderzeichen bestehen.
- > Sie können verbieten, dass Kennwörter mit Zahlen enden: »001«, »002« etc.

Achtung: Kaum vorhandene Prüfungen im Dokument lassen Widersprüche zu! Das führt im schlimmsten Fall dazu, dass sich die Anwender nicht mehr anmelden können!

Hier ein Beispiel für eine (ziemlich moderate) Kennwortvorgabe:

- > mindestens 7 Zeichen
- > Das Kennwort muss mindestens einen Großbuchstaben oder eine Ziffer oder ein Sonderzeichen enthalten

Wenn das Kennwort in der ID-Datei nicht komplex genug ist, wird dem Benutzer bei der nächsten Anmeldung die folgende, leider nicht sehr aussagekräftige Meldung präsentiert:



Abbildung 13.16: Meldung bei nicht ausreichend komplexem Kennwort

Nach Klicken auf **OK** wird der Benutzer aufgefordert, ein neues Kennwort einzugeben.

Leider werden im Dialog **Kennwort ändern** (siehe Abbildung 13.17) die Regeln aus der Benutzerdefinierten Kennwortrichtlinie vollständig aufgelistet, also auch jene Felder, in denen Sie gar nichts konfiguriert haben (»Nicht zutreffend«), was für Anwender ziemlich verwirrend ist! Alles in allem handelt es sich also um ein tolles Feature mit einer ziemlich schlechten Benutzerführung!

Ich rate Ihnen daher unbedingt, die Anwender entsprechend vorzubereiten: Senden Sie zumindest eine Mail mit einer Anleitung (mit Screenshots!), bevor Sie das Feature ausrollen. Und egal wie viel Mühe Sie sich damit auch geben, rechnen Sie damit, dass in den ersten Tagen nach Scharfschalten trotzdem viele entsetzte Anwender bei Ihrer Hotline anrufen! Planen Sie das also entsprechend ein.

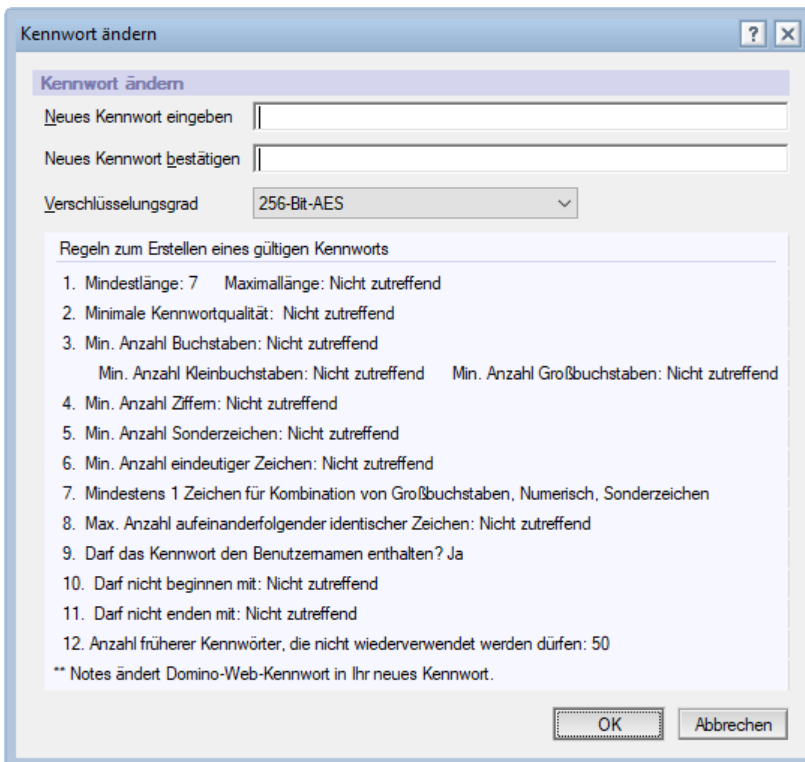


Abbildung 13.17: Dialog Kennwort ändern nach Aktivierung der benutzerdefinierten Kennwortrichtlinie

13.4. Gemeinsame Notes-Anmeldung

Bei der Gemeinsamen Notes-Anmeldung (Notes Shared Login – NSL) wird ein komplett anderer Ansatz gewählt:

- > Das Kennwort wird aus der ID-Datei gelöscht.
- > Die ID-Datei wird mittels Microsoft DPAPI-Schnittstelle (Data Protection API – für alle Windows-Versionen seit 2000 verfügbar) verschlüsselt.
- > Die Verschlüsselung ist pro Computer einzigartig.
- > Die Notes-Kennwortaufforderung wird unterdrückt,

Daraus ergeben sich die folgenden Eigenschaften:

- > Anwender müssen sich nur noch das Windows-Kennwort merken.
- > Eine Kennwortänderung unter Windows hat keinen Einfluss auf die Notes-Anmeldung.
- > Es sind keine Kennwortzurücksetzungen mehr nötig (außer der PC wird neu aufgesetzt oder die ID-Datei geht verloren).
- > Alle Funktionen der ID-Datei bleiben unverändert:
 - Der Client authentifiziert auch weiterhin mit dem Domino-Server via Zertifikat aus der ID-Datei.
 - Die ID-Datei enthält auch weiterhin alle Internet-Zertifikate.
 - Die ID-Datei enthält auch weiterhin Geheimschlüssel.
- > Es werden die Windows-Anmeldeinformationen verwendet, um die ID-Datei zu sperren/entsperren.
- > Funktioniert auch mit dem ID-Vault – die ID-Datei wird mit dem ursprünglichen Kennwort im Vault gespeichert.
 - Der ID-Vault sollte zuerst aktiviert werden, damit er alle ID-Dateien enthält. Verschlüsselte ID-Dateien können nicht in den Vault hochgeladen werden!
 - Erst dann können Sie NSL via Richtlinien aktivieren.

Was passiert, wenn NSL auf einem Client aktiviert wird:

1. Benutzer meldet sich in Windows an.
2. Notes stellt beim Start fest, dass via Richtlinie NSL aktiviert wurde.
3. Notes generiert einen langen, komplexen Geheimtext.
4. Notes ruft die Microsoft DPAPI-Schnittstelle auf, um den Geheimtext basierend auf der aktuellen Benutzeridentität und Maschine zu verschlüsseln.
5. Notes speichert den verschlüsselten Geheimtext im Benutzerprofil der Client-Maschine.
6. Notes verschlüsselt die ID-Datei mit einem vom Geheimtext abgeleiteten Schlüssel.

Was passiert, wenn ein für NSL aktivierter Client gestartet wird:

1. Der Benutzer meldet sich in Windows an.
2. Der Benutzer startet den Notes-Client.
3. Aufgrund der ID-Datei ergibt sich, dass NSL aktiv ist.

4. Notes holt den verschlüsselten Geheimtext aus dem Windows-Profil des Computers und ruft Microsoft DPAPI auf, um ihn zu entschlüsseln.
5. Notes verwendet den entschlüsselten Geheimtext, um die ID-Datei zu entschlüsseln.
6. Notes startet ohne Kennworteingabe!

13.4.1. Einrichten der Gemeinsamen Notes-Anmeldung

Die Konfiguration erfolgt in der Sicherheitseinstellung.

Wechseln Sie zum Register **Gemeinsame Notes-Anmeldung** und wählen Sie im Feld **Gemeinsame Notes-Anmeldung mit dem Betriebssystem aktivieren** die Option »Ja«.

Wählen Sie in der Spalte **Wie diese Einstellung angewendet wird:** »Wert nach jeder Änderung festlegen«.

Wählen Sie im Feld **Benutzer darf Änderungen vornehmen?** die Option »Ja«, kann der Benutzer später im Sicherheitsdialog die Gemeinsame Notes-Anmeldung abschalten.

Optional: Konfigurieren Sie, ob Benachrichtigungen angezeigt werden sollen. Wählen Sie im Feld **Benachrichtigungsart bei Aktivierung** bzw. **Benachrichtigungsart bei Deaktivierung** den Wert »Benutzerdefiniertes Nachrichtendialogfeld«, können Sie den Text selbst definieren.

The screenshot shows the 'Sicherheitseinstellungen : COB Security' interface. The 'Gemeinsame Notes-Anmeldung' tab is active. Under 'Gemeinsame Notes-Anmeldung', the 'Gemeinsame Notes-Anmeldung mit dem Betriebssystem aktivieren:' dropdown is set to 'Ja'. The 'Wie diese Einstellung angewendet wird:' dropdown is set to 'Wert nach jeder Änderung festlegen'. Below this, the 'Benutzer dürfen Änderungen vornehmen?' section has 'Nein' selected. The 'Aktivierungsbenachrichtigung' section has 'Keine Benachrichtigung' selected. The 'Deaktivierungsbenachrichtigung' section also has 'Keine Benachrichtigung' selected.

Abbildung 13.18: Konfiguration der Gemeinsamen Notes-Anmeldung in den Sicherheitseinstellungen

Achtung: Die Gemeinsame Notes-Anmeldung kann nicht auf Notes-Clients aktiviert werden, auf denen die Einmalige Notes-Anmeldung (Notes Single Sign-On) installiert ist.

13.4.2. Einschränkungen

- > Da es sich um einen Microsoft-Standard handelt, funktioniert NSL nur mit Notes für Windows.

- > Die Verschlüsselung der ID-Datei ist auf jeder Client-Maschine anders!
 - Daher kann die ID-Datei nicht in iNotes/Verse importiert werden!
 - Daher sind Windows-Roaming-Profiles mit dem Anmelden von verschiedenen Clients nicht möglich.
- > Die Synchronisation mit dem Internetkennwort kann bei aktiviertem NSL nicht verwendet werden – die ID enthält ja kein Kennwort mehr!
- > DPAPI ist angreifbar, so lange eine Sitzung besteht!
- > ID-Datei darf bei Notes-Roaming nicht mehr ins Persönliche Adressbuch hochgeladen werden! (Sie verwenden ohnehin besser einen ID-Vault ...)
- > Keine Unterstützung für Smart Cards

13.5. Nachruf: Einmalige Notes-Anmeldung

Die Einmalige Notes-Anmeldung (Notes Single Logon) sollten Sie aus verschiedenen Gründen nicht mehr verwenden, daher schreibe ich hier der Vollständigkeit halber nur noch einen kurzen Nachruf. Die Eigenschaften der Einmaligen Notes-Anmeldung sind:

- > Starten von Notes ohne Kennworteingabe
- > Verwenden eines Netzwerk-Providers und eines Windows-Dienstes, um das eingegebene Windows-Kennwort zu erfassen
 - Voraussetzung dafür ist Verwendung desselben Kennworts in Windows und in der Notes-ID
- > Aktivieren/Deaktivieren vom Benutzer über den Sicherheitsdialog möglich.

Das klingt an sich nicht schlecht, es gibt aber jede Menge Einschränkungen:

- > Sicherheitsrichtlinien von Windows und Notes lassen die Definition unterschiedlicher Regeln zu:
 - Mit der Kennwortqualität kann nicht gearbeitet werden.
 - Mit einer Benutzerdefinierten Kennwortrichtlinie geht es, wenn man die richtigen Regeln aufstellt.
- > Synchronisation erfolgt nur, wenn das Kennwort vom Benutzer lokal geändert wird.
- > Verwendung eines ID-Vaults wird von der HCL nicht unterstützt!
- > Gilt als unsicher und leicht angreifbar!

Da bei der Einmaligen Notes-Anmeldung ein Dienst installiert wird, der das Windows-Kennwort ausspäht, handelt es sich um eine optionale Installationskomponente, die per Vorgabe gar nicht mehr aktiviert ist. Sollten Sie diese dennoch installieren, kann die Gemeinsame Notes-Anmeldung (siehe Kap. 13.4 Gemeinsame Notes-Anmeldung, ab Seite 350) auf diesem Client nicht mehr aktiviert werden.

13.5.1. Was nützen die ganzen Schlösser, wenn sie keiner absperrt?

Am Ende nochmals eine Zusammenfassung der wichtigsten Regeln:

- > Geben Sie ausreichend komplexe Kennwörter vor! (Sicherheitsrichtlinie)

- > Setzen Sie die interne Verschlüsselung hoch! (Sicherheitsrichtlinie)
- > Lassen Sie die Kennwörter ablaufen – zumindest einmal pro Jahr. (Sicherheitsrichtlinie)
- > Steigen Sie auf eine Benutzerdefinierte Kennwortrichtlinie um (Sicherheitsrichtlinie)
- > Speichern Sie ID-Dateien mit Startkennwörtern NIE im Domino-Verzeichnis.
- > Nennen Sie Server-IDs nicht »server.id« und legen Sie sie nicht im Datenverzeichnis ab. (Datei kann mit ein paar Zeilen LotusScript-Code aus dem Verzeichnis gefischt werden!)
- > Richten Sie einen ID-Vault ein!

13.6. Das Internetkennwort

Seit Domino 11 kann das Internetkennwort an zwei verschiedenen Stellen gespeichert werden: im Personendokument oder im ID-Vault. Hier ein Vergleich zwischen den beiden Möglichkeiten:

Personendokument	ID-Vault
Internetkennwort wird als Hash im Feld HTTPPassword gespeichert, aber nicht verschlüsselt	Das Internetkennwort entspricht dem Kennwort der User-ID, welche mit dem Öffentlichen Schlüssel des Servers verschlüsselt wurde
Synchronisation zwischen Notes- und Internetkennwort oder zwei unterschiedliche Kennwörter	Keine Synchronisation zwischen Notes- und Internetkennwort nötig; Notes- und Internetkennwort sind immer gleich
Für Notes-Benutzer mit User-ID und Webbenutzer ohne User-ID	Nur für Notes-Benutzer mit User-ID

Tabelle 13.2: Unterschiede je nach Speicherort des Internetkennworts

13.6.1. Den Speicherort des Internetkennworts konfigurieren

Welche Methode verwendet wird, steuern Sie im Konfigurationsdokument, Register **Sicherheit**:

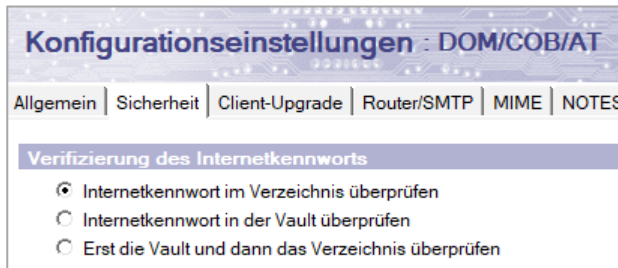


Abbildung 13.19: Optionen zum Verifizieren des Internetkennworts im Serverkonfigurationsdokument

Sie können nur dann alle Optionen verwenden, wenn Sie einen ID-Vault eingerichtet haben!

Option	Beschreibung
Internetkennwort im Verzeichnis überprüfen	Es wird das Kennwort aus dem Personendokument zur Authentifizierung von Webbenutzern verwendet.
Internetkennwort im Vault überprüfen	Es wird das Kennwort aus der User-ID im Vault zur Authentifizierung von Webbenutzern verwendet. Webbenutzer müssen

Option	Beschreibung
	mit Notes-ID registriert worden sein und die ID muss sich im Vault befinden.
Erst die Vault und dann das Verzeichnis überprüfen	Es wird zuerst versucht, das Kennwort aus der User-ID im Vault zur Authentifizierung zu verwenden. Wenn im Vault keine User-ID existiert, wird das Internetkennwort im Personendokument zur Authentifizierung verwendet. Verwenden Sie diese Option, wenn nicht alle Webbenutzer über Notes-IDs verfügen oder sich nicht alle IDs im Vault befinden.

Tabelle 13.3: Optionen bei der Verifizierung des Internetkennworts

13.6.2. »Sichere« und »sicherere« Internetkennwörter

Speichern Sie das Internetkennwort im Personendokument, wird es im Feld HTTPPassword als Hash-Wert (proprietär verändert) abgelegt. Domino kennt drei Hash-Algorithmen, die unterschiedlich sicher sind. In älteren Domino-Versionen (vor 6) kam ausschließlich Version 1 (SEC_pwddigest_V1) zur Anwendung, bei der für Kennwörter ein 34 Zeichen langer, hexadezimaler Schlüssel im Format (A-F, 0-9) generiert wurde. Problem bei der Sache: Der erzeugte Buchstabensalat sah für ein bestimmtes Kennwort immer gleich aus. Hier zum Beispiel der Hashwert für »lotusnotes«:

(DE9CA9CD7BD212362B6D312A33E10FB2)

Mit Domino 7 wurde Version 2 (SEC_pwddigest_V2) eingeführt, welche erlaubt, »sicherere« Kennwörter zu erzeugen. Hier werden 22 Zeichen lange Passwort-Hashes mit einer Zufallszahl (einem 5-Byte langen Variant, der auch als »Salt« bezeichnet wird) berechnet, wodurch zwei Hashes desselben Passworts unterschiedlich aussehen. Hier ein Beispiel für einen »gesalzenen« Hash:

(GWbtayIKtF3BwkePOdcE)

Mit Domino 8.0.1 wurde Version 3 (SEC_pwddigest_V3) und damit der aktuelle Hash-Algorithmus eingeführt. Der Salt ist der gleiche, aber die Hashes sind mit 51 Zeichen Länge noch sicherer. Hier ein Beispiel:

(HDaLvuuZ11+fiWhP1O2BIJ0mC30mC3KmC30mCc325x8tFGZE)

Natürlich sollten Sie nur noch Version 3 verwenden, diese ist aber nicht Vorgabe! Überprüfen Sie daher sofort die Einstellung im Verzeichnisprofil. Wählen Sie dazu in einer beliebigen Ansicht im Domino-Verzeichnis stehend den Befehl **Aktionen > Verzeichnisprofil bearbeiten**. Wählen Sie dann im Feld **Sicherere Internet-Kennwörter verwenden** die Option: »Ja - Kennwortüberprüfung ist kompatibel mit Notes/Domino Version 8.01 oder höher«, um nur noch Hashes der Version 3 zu erzeugen:



Abbildung 13.20: Verzeichnisprofil: Sichereres Internetkennwort verwenden

Nach dem Ändern der Einstellung werden die Hashes in den Personendokumenten auf die neuere Version aktualisiert, aber nur, wenn jedes Personendokument zumindest einmalig bearbeitet und gespeichert wird.

Es gibt jedoch auch ein Werkzeug, mit dem Sie bereits bestehende Personendokumente nachträglich auf sicherere Kennwörter aktualisieren können: Markieren Sie die gewünschten Personen (oder alle durch Drücken der Tasten [Strg]+[A]) und wählen Sie im Menü **Aktionen** den Befehl **Sicheres Internetkennwort festlegen**:

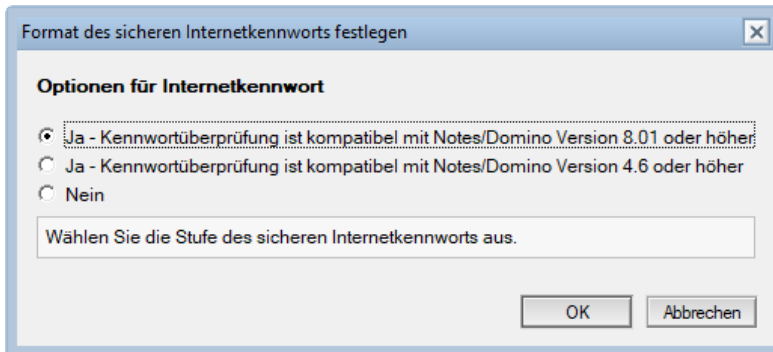


Abbildung 13.21: Optionen für die Sicherheit des Internetkennworts

Alternativ können Sie das Feld **\$SecurePassword** auch mithilfe eines einfachen Formel-Agenten beschicken. Die Formel dafür lautet:

```
FIELD $SecurePassword := "2"
```

Achtung: Wählen Sie in obigem Dialog »Nein«, werden »ungesalzene« Hashwerte gespeichert. Somit sehen die Hashes derselben Kennwörter immer gleich aus und können leicht angegriffen werden. Manchmal reicht dazu eine Google-Suche aus!

13.6.3. Sperren des Internetkennworts erzwingen

Mit dem Feature **Internetsperre** (Internet Password Lockout) können Sie Browseranwender nach mehrfacher Falscheingabe ihres Kennworts aussperren.

- > Erschwert Wörterbuch-Attacken auf Internetkonten
- > Das funktioniert derzeit nur für den Web-Zugriff (Protokolle HTTP/HTTPS), andere Protokolle werden nicht unterstützt!
- > Funktioniert bei Single-Sign-On (SSO) nur, wenn der SSO-Schlüssel von Domino stammt
- > Kann durch DSAPI-Filter deaktiviert werden, da diese die Authentifizierung umgehen
- > Achtung: Kann bei DoS-Attacken rasch zum Aussperren aller Benutzer führen!

Um die Internetsperre zu aktivieren, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zu **Konfiguration > Server > Konfigurationen**.
2. Öffnen Sie das Konfigurationsdokument Ihres Webservers im Bearbeitungsmodus und navigieren Sie zum Register **Sicherheit**.
3. Setzen Sie das Feld **Sperre des Internetkennworts erzwingen** auf »Ja«.
4. Geben Sie im Feld **Protokolleinstellungen** an, ob nur Sperren oder auch Fehlversuche protokolliert werden sollen.
5. Über das Feld **Vorgegebene maximale Anzahl der Versuche** limitieren Sie die Anzahl der Versuche – bei Angabe von »5« wird der Anwender nach der 5. Falscheingabe gesperrt.

6. Im Feld **Vorgegebenes Ablaufdatum der Sperre** legen Sie fest, wie lange der Benutzer gesperrt bleibt (in Minuten, Stunden oder Tage). Bei Eingabe von 0 muss die Sperre vom Administrator manuell aufgehoben werden.

Um das Sperren aller Benutzer durch DoS-Attacken zu verhindern, empfiehlt es sich, die Dauer der Sperre auf wenige Minuten zu setzen.

7. Über das Feld **Intervall für die vorgegebene maximale Anzahl der Versuche** steuern Sie, in welchem Zeitraum die Falschangaben gezählt werden.

1 Tag: Falscheingaben werden täglich neu gezählt.

0 Tage: Falscheingaben werden ewig gemerkt.

Internetsperre	
Sperre des Internetkennworts erzwingen:	<input type="checkbox"/> Ja <input checked="" type="checkbox"/> Nein
	<input checked="" type="checkbox"/> Sperren
Protokolleinstellungen:	<input checked="" type="checkbox"/> Fehlschläge
Vorgegebene maximale Anzahl der Versuche:	<input type="text" value="5"/>
Vorgegebenes Ablaufdatum der Sperre:	<input type="text" value="15"/> <input type="text" value="Minuten"/>
Intervall für die vorgegebene maximale Anzahl der Versuche:	<input type="text" value="1"/> <input type="text" value="Tage"/>

Abbildung 13.22: Konfigurationsdokument, Einrichten der Internetsperre

Ein Feintuning für unterschiedliche Benutzergruppen ist weiters in der Sicherheitsrichtlinie möglich:

Sperreinstellungen für Internetkennwörter	
Sperreinstellungen für Internetkennwörter des Servers überschreiben?	<input checked="" type="checkbox"/> Ja
Maximale Anzahl der erlaubten Kennwortversuche	<input type="text" value="3"/>
Ablaufzeit der Sperre	<input type="text" value="10"/> <input type="text" value="Minuten"/>
Intervall für die maximale Anzahl der Versuche	<input type="text" value="0"/> <input type="text" value="Minuten"/>

Abbildung 13.23: Sicherheitseinstellungen – Einrichten der Internetsperre

Nach dem Aktivieren des Sperrens wird die Datenbank »Internet Lockouts« (inetlockout.nsf) im Datenverzeichnis des Servers erstellt.

Diese Datenbank bietet die folgenden Möglichkeiten:

- > zeigt den aktuellen Status an (Falscheingaben und Sperren)
- > erlaubt durch Entfernen eines Benutzers aus der Datenbank die Sperre aufzuheben:

Internet Lockouts		Mark for Delete/Unlock	Delete Marked Items				
	Server Name	User Name	Locked Out	Failed Attempts	First Failure Time	Last Failure Time	
<input checked="" type="checkbox"/> Locked Out Users <input type="checkbox"/> Login Failures	DOM/COB/AT						
	Admin/COB/AT	Yes	3	20.10.2018 20:32:54	24.05.2020 16:11:57		

Abbildung 13.24: Datenbank Internet Lockouts (inetlockout.nsf)

Damit die Sperren serverübergreifend funktionieren, muss die Datenbank inetlockout.nsf zwischen allen Webservern repliziert werden!

Stellen Sie eine passende Login-Maske bereit, in der auf die Sperre hingewiesen wird!

13.6.4. Passwort-Synchronisierung

Speichern Sie das Internetkennwort im Personendokument, können Sie in der Sicherheitsrichtlinie eine Synchronisierung mit dem Notes-ID-Kennwort konfigurieren. Ändert der Benutzer sein Notes-ID-Kennwort, wird eine Anforderung an den Administrationsprozess gestellt, das neue Kennwort ins Personendokument zu übertragen. Das ist für die Benutzer zwar praktisch, weil sie sich nur noch ein Kennwort merken müssen, setzt aber die Sicherheit herab, da das Internetkennwort leichter angreifbar ist. Wenn Sie zusätzlich das Feature Internetsperre konfigurieren (siehe Kap. 13.6.3 Sperren des Internetkennworts erzwingen, auf Seite 355), ist auch das Internetkennwort weniger leicht angreifbar und das Einrichten einer Kennwortsynchronisierung vertretbar.

13.7. Verzeichnissicherheit

Sie haben die Möglichkeit, mithilfe einer **Verzeichniszugriffskontrollliste** (Verzeichnis-ACL, Directory ACL) bereits auf Verzeichnisebene Zugriffsrechte zu vergeben. Benutzer, die keinen Zugriff auf ein Verzeichnis haben, sehen dieses erst gar nicht. Innerhalb des Verzeichnisses gelten die Zugriffskontrolllisten der einzelnen Datenbanken.

Um Rechte für ein Unterverzeichnis zu vergeben, navigieren Sie im Domino-Administrator zum Register **Dateien** und klicken mit der rechten Maustaste auf das gewünschte Verzeichnis. Wählen Sie im Kontextmenü den Befehl **Verzeichnis-ACL verwalten...** Der Dialog Verzeichnis-ACL verwalten wird angezeigt:

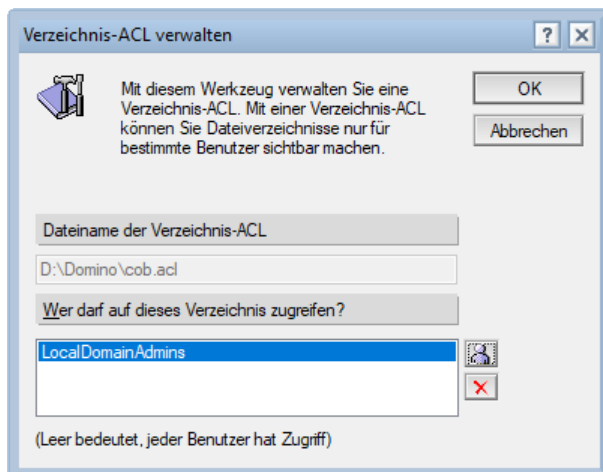


Abbildung 13.25: Der Dialog Verzeichnis-ACL verwalten

Klicken Sie auf die Schaltfläche mit dem Männchen, um Benutzer oder Gruppen hinzuzufügen. Klicken Sie auf die Schaltfläche mit dem X, um Einträge aus der Liste zu entfernen. Bestätigen Sie am Ende durch Klicken auf **OK**, wird eine Textdatei mit dem Namen des Verzeichnisses und der Endung *.acl erstellt. Ein Schloss neben dem Ordnersymbol zeigt an, dass der Zugriff beschränkt

wurde. Die Verzeichnis-ACL zieht in allen nachträglich initiierten Benutzersitzungen sofort, ein Durchstarten des Servers ist nicht nötig.

Um den Zugriff zu bearbeiten, wählen Sie das Verzeichnis erneut aus und dann im Kontextmenü (rechte Maustaste) wieder den Befehl **Verzeichnis-ACL verwalten...**

Analog können Sie auch direkt die Textdatei mit der Endung *.acl im Datenverzeichnis bearbeiten.

Wollen Sie die Verzeichnis-ACL ganz löschen, klicken Sie mit der rechten Maustaste auf das Ordnersymbol und wählen Sie im Kontextmenü den Befehl **Ordner löschen...** oder löschen Sie die Textdatei mit der Endung *.acl im Dateisystem.

13.8. Datenbanksicherheit

Unter Datenbanksicherheit versteht man in erster Linie die Zugriffskontrollliste (Access Control List – ACL) der Datenbank. In dieser können Sie verschiedene Arten von Einträgen haben:

Eintrag	Erklärung
-Default-	alle, die in der ACL nicht aufgelistet sind
Anonymous	Anonyme (= nicht authentifizierte Benutzer)
Person	eine beliebige Person aus dem Domino-Verzeichnis, z. B.: Otto Huber/COB/AT
Gruppe	eine beliebige Gruppe aus dem Domino-Verzeichnis, z. B.: Local-DomainAdmins
Verweis auf die Hierarchie	ein Verweis auf eine hierarchische Namenskomponente, etwa eine Organisationseinheit oder die ganze Organisation, z. B.: */Verkauf/COB/AT

Tabelle 13.4: Arten von Einträgen in der ACL

Die verschiedenen Zugriffsrechte entnehmen Sie bitte Tabelle 13.5.

Recht	Erklärung
Manager	Darf zusätzlich zu den Entwicklerrechten auch die Zugriffskontrollliste ändern.
Entwickler	Darf zusätzlich zu den Editorrechten auch die Gestaltung der Anwendung ändern.
Editor	Darf Dokumente immer erstellen und immer bearbeiten.
Autor	Darf Dokumente, Eigenschaften und die ACL lesen. Darf mit dem Zusatzrecht »Dokumente erstellen« neue Dokumente erstellen. Darf selbst oder von anderen erstellte Dokumente bearbeiten, wenn er in einem Autorenfeld steht. Darf mit dem Zusatzrecht »Dokumente löschen« Dokumente löschen, wenn er in einem Autorenfeld steht.
Leser	Darf Dokumente, Eigenschaften und die ACL lesen, jedoch keinerlei Änderungen vornehmen.

Recht	Erklärung
Einlieferer	Darf die Datenbank öffnen und Dokumente erstellen, jedoch die Ansichten nicht nutzen. Für einen Einlieferer ist die Datenbank immer leer.
Kein Zugriff	Darf die Datenbank nicht öffnen und auch keinerlei Eigenschaften sehen.

Tabelle 13.5: Die verschiedenen Zugriffsrechte

Beachten Sie folgende Regeln:

- > Die ACL wird per Vorgabe nur vom Server überprüft!
 - außer: Die Eigenschaft »Konsistente ACL erzwingen« ist gesetzt
- > Öffentliche Gruppen funktionieren ohne Serververbindung nicht!
- > Der Internetzugriff kann vollkommen deaktiviert werden (Maximalen Internetzugriff auf »Kein Zugriff« setzen).
- > Das Kopieren und Replizieren von Datenbanken kann verhindert werden.
- > Schablonen: Sie können mit Einträgen in eckigen Klammern Vorgaben setzen, z. B.:
[LocalDomainAdmins]

13.8.1. Benutzerrollen

Rollen ähneln Gruppen, sind jedoch spezifisch für die Datenbank, in der sie erstellt werden. Rollen werden dazu verwendet, um den Zugriff auf Gestaltungselemente oder Funktionen einzuschränken. Wenn Sie beispielsweise möchten, dass alle Autoren in einer Datenbank Diskussionsbeiträge erstellen dürfen, aber kein Datenbankprofil, können Sie eine Rolle mit dem Namen »Configuration« anlegen und diese zu den Maskeneigenschaften hinzufügen.

Wechseln Sie dazu in der Zugriffskontrollliste zum Register **Rollen** und klicken Sie auf die Schaltfläche **Hinzufügen...**

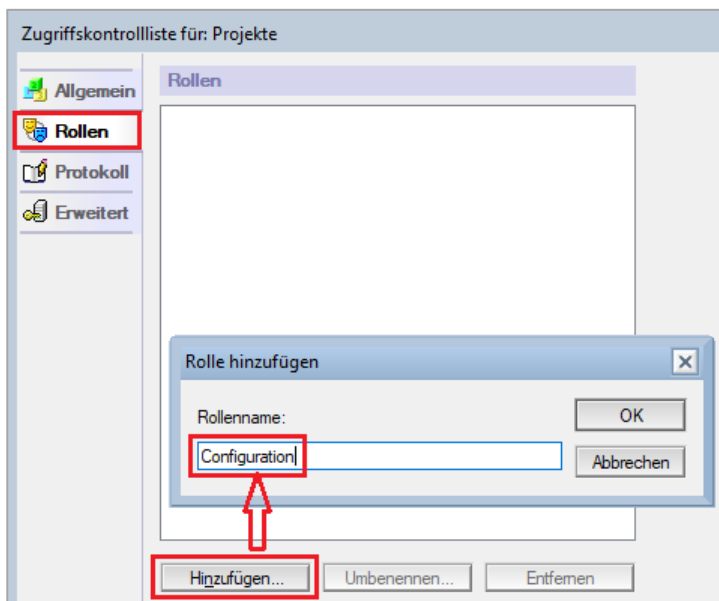


Abbildung 13.26: Zugriffskontrollliste, Rollen hinzufügen

Rollenamen werden in Klammern angezeigt, z. B. [Vertrieb]. Nach dem Erstellen können Sie die Rolle einer Person oder einer Gruppe zuweisen, indem Sie die Rolle im Listenfeld **Rollen** auswählen.

Das Zuweisen der Rolle allein bewirkt gar nichts. Sie (oder ein Entwickler) müssen die Rolle auch in den Eigenschaften eines Designelements oder in einer Funktion verwenden. In unserem Beispiel mit dem Datenbankprofil wären das die Maskeneigenschaften:

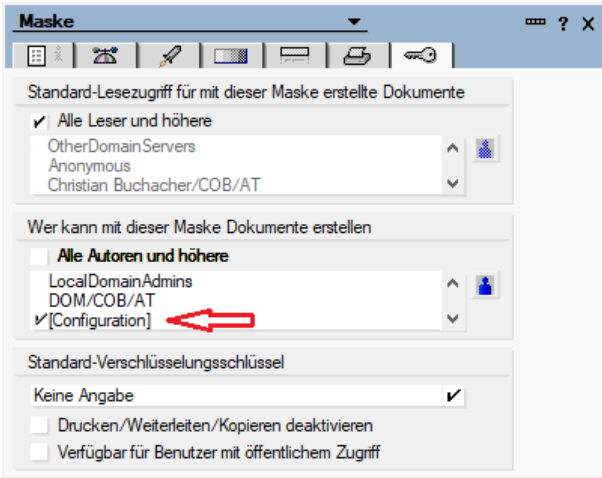


Abbildung 13.27: Maskeneigenschaften, Eigenschaft »Wer kann mit dieser Maske Dokumente erstellen«

Entnehmen Sie die Gestaltungselemente und Funktionen, auf die der Entwickler den Zugriff mithilfe von Rollen beschränken kann, Tabelle 13.6:

Um einzuschränken, wer kann...	...verwendet der Entwickler Rollen in...
bestimmte Dokumente bearbeiten	Autorenfeldern
einen bestimmten Bereich eines Dokuments bearbeiten	Abschnitten
bestimmte Dokumente lesen	Leserfeldern/Maskeneigenschaften
Dokumente in einer bestimmten Ansicht sehen	Ansichtseigenschaften
Dokumente in einem bestimmten Ordner sehen	Ordnerseigenschaften
Dokumente lesen, die mit einer bestimmten Maske erstellt wurden	Maskeneigenschaften
Dokumente mit einer bestimmten Maske erstellen	Maskeneigenschaften
Designelemente (Felder, Tabellen, Aktions-schaltflächen etc.) innerhalb eines Dokuments ein-/ausblenden	Formelsprache (@UserRoles)

Tabelle 13.6: Verwendung von Rollen in Designelementen

Achtung: Rollen werden vom Client lokal nur überprüft, wenn eine konsistente ACL eingestellt ist!

13.8.1.1. Spezialfall Domino-Verzeichnis

Während die Benutzerrollen in Eigenentwicklungen immer erklärungsbedürftig sind, sind jene im Domino-Verzeichnis klar definiert:

Rolle	Erklärung
GroupCreator	kann Gruppen erstellen
GroupModifier	darf alle Gruppendokumente bearbeiten
NetCreator	kann alle Dokumente außer Gruppen, Personen, Server und Richtlinien erstellen
NetModifier	kann alle Dokumente außer Gruppen, Personen, Server und Richtlinien bearbeiten
PolicyCreator	kann Richtlinie und Richtlinieneinstellungen erstellen
PolicyModifier	kann alle Richtliniendokumente bearbeiten
PolicyReader	kann Richtliniendokumente sehen, aber nicht bearbeiten
ServerCreator	kann Server erstellen
ServerModifier	kann alle Serverdokumente bearbeiten
UserCreator	kann Personen erstellen / registrieren
UserModifier	kann alle Personendokumente bearbeiten

Tabelle 13.7: Die Benutzerrollen im Domino-Verzeichnis

13.8.2. Konsistente Zugriffskontrollliste

Mit einer **konsistenten Zugriffskontrollliste** (Consistent Access Control List, Consistent ACL) können Sie eine identische ACL über alle Repliken einer Datenbank erzwingen.

Erstellt ein Benutzer eine lokale Replik von einer Datenbank mit einer Konsistenten ACL, werden die Zugriffsrechte des Benutzers lokal so berechnet wie am Server.

Mit einer Konsistenten ACL funktionieren auch Benutzerrollen in lokalen Datenbanken. Beachten Sie jedoch, dass außer für den Ersteller der Replik lokal keine Informationen zu Gruppenmitgliedschaften verfügbar sind, weshalb zur Überprüfung der Identität anderer Personen als dem Ersteller nur Personeneinträge herangezogen werden können. Sollte im Client ein Identitätswechsel vorgesehen sein, sorgen Sie daher dafür, dass jeder Benutzer als Person in der ACL steht und auch alle benötigten Benutzerrollen zugewiesen hat. Arbeiten Sie in diesem Fall nicht wie sonst üblich mit Gruppen.

Wenn ein Benutzer die ACL einer lokalen Replik ändert, wenn eine Konsistente Zugriffssteuerungsliste aktiviert ist, wird die Replikation der Datenbank beendet. Das Protokoll (log.nsf) zeichnet eine Nachricht auf, die angibt, dass die Replikation nicht fortgesetzt werden konnte, da das Programm keine einheitliche ACL für Repliken verwalten konnte.

Setzen Sie zum Aktivieren einer konsistenten Zugriffskontrollliste am Register **Erweitert** ein Häkchen bei: **Konsistente ACL über alle Repliken dieser Datenbank erzwingen**:

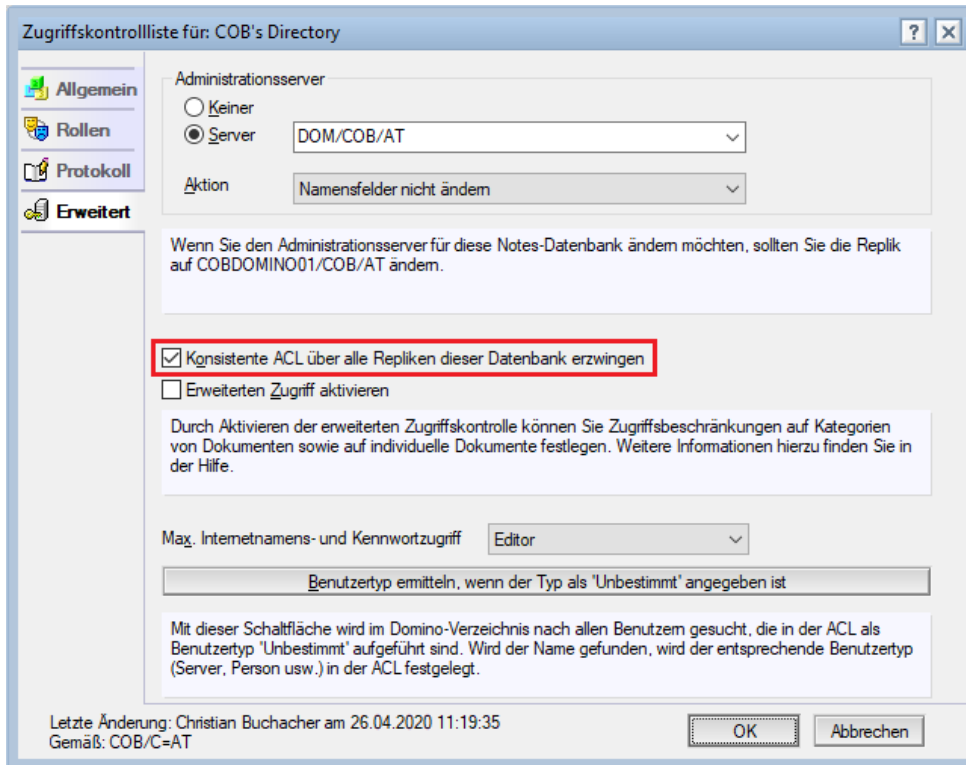


Abbildung 13.28: Zugriffskontrollliste, Register Erweitert

Setzen Sie diese Einstellung unbedingt auf einem Server, der über Managerzugriff verfügt, da er sonst die ACL nicht auf andere Serverrepliken übertragen kann.

13.9. Ausführungskontrolllisten

Ausführungskontrolllisten (Execution Control Lists – ECL) überprüfen die Ausführung von sogenanntem »Active Content«. Dazu gehört alles, was im Notes-Client-Kontext abläuft wie Formeln, Scripts, Agenten, Designelemente in Datenbanken & Schablonen, Dokumente mit gespeicherten Masken, Aktionen, Schaltflächen oder Hotspots.

Das Ausführen von Windows-Programmen (etwa durch Doppelklicken einer angehängten EXE-Datei) wird von der ECL hingegen nicht erfasst, da diese Programme in einem Betriebssystemkontext laufen und nicht in einem Notes-Kontext. (Das Speichern des Dateianhangs im Dateisystem hingegen schon.)

Achtung: Beim Zugriff via Notes-API greift die ECL nicht!

In der ECL selbst steht natürlich nicht der Name eines Programms, sondern der sogenannte Unterzeichner (Signierer), also diejenige Person, die den Active Content zuletzt gespeichert hat. Zusätzlich gibt es noch die Einträge »-Default« und »-Keine Signatur-«:

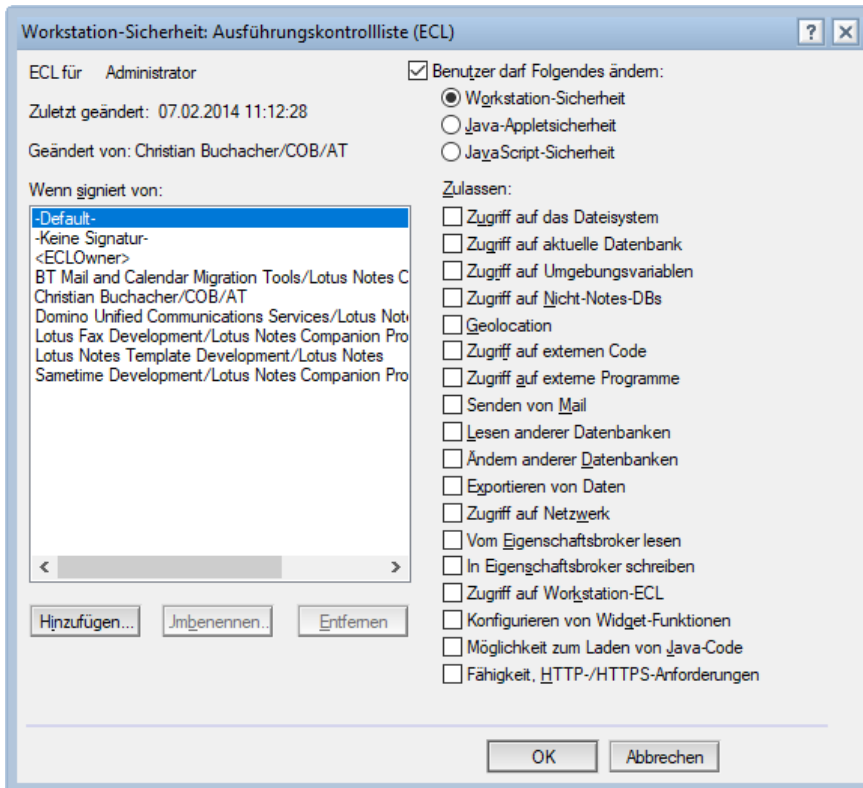


Abbildung 13.29: Die Administrations-ECL im Domino-Verzeichnis nach dem Bearbeiten

Wobei »-Default-« für Active Content steht, der eine Signatur enthält, die von Domino überprüft wurde, jedoch keinem Eintrag in der ECL entspricht.

»-Keine Signatur-« steht wiederum für Active Content, der eine ungültige oder beschädigte Signatur enthält, gar nicht signiert ist oder dessen Signatur von einer Identität oder Organisation stammt, die von Domino nicht überprüft werden kann.

Wenn vom Active Content versucht wird, eine Aktion auszuführen, die für die betreffende Signatur nicht erlaubt ist (oder die Signatur nicht in der ECL enthalten ist), wird eine Sicherheitswarnung (Execution Security Alert – ESA) generiert.

Der Benutzer hat dann die Möglichkeit:

- > dem Code nicht zu vertrauen (Aktion NICHT ausführen)
- > dem Code einmalig zu vertrauen (Aktion nur dieses eine Mal ausführen)
- > dem Code mehrmals (ohne erneute Bestätigung) in der aktuellen Arbeitssitzung zu vertrauen (Aktion nur in dieser Notes-Sitzung ausführen...)
- > dem Code in Zukunft zu vertrauen (Aktion ausführen und dem Unterzeichner dieser Aktion vertrauen)

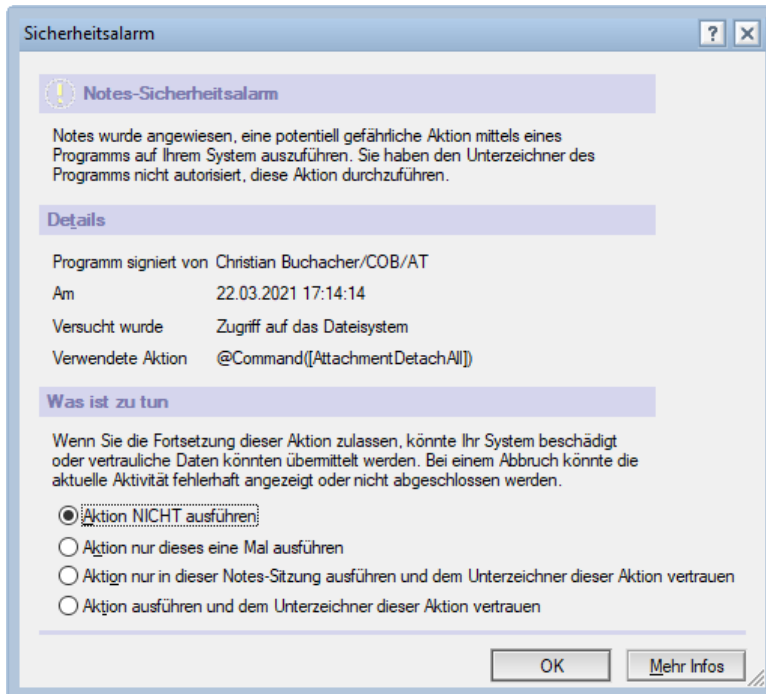


Abbildung 13.30: Sicherheitswarnung (Execution Security Alert – ESA)

13.9.1. Die Vorgabe-ECL bearbeiten

Beim Aufsetzen des ersten Servers wird eine hartcodierte Vorgabe-ECL erstellt. Diese Vorgabe-ECL enthält unter anderem die Signatur »Lotus Notes Template Development/Lotus Notes«, mit welcher alle mitgelieferten Schablonen signiert sind. Bei der Konfiguration eines Notes-Clients wird die Vorgabe-ECL aus dem Domino-Verzeichnis in die lokale Kontakte-Anwendung kopiert und die aktuelle Notes-ID mit allen Rechten hinzugefügt.

Die Vorgabe-ECL kann vom Administrator bearbeitet werden und wird dann im Domino-Verzeichnis als **Administrations-ECL** gespeichert. Zum Bearbeiten der Vorgabe-ECL öffnen Sie entweder das Domino-Verzeichnis und wählen den Menüpunkt **Aktionen > Administrations-ECL bearbeiten** oder Sie erstellen eine Sicherheitsrichtlinie und klicken im Register **Ausführungskontrollliste (ECL)** auf die Schaltfläche **Bearbeiten**.

13.9.2. Änderungen in der Administrations-ECL ausrollen

Haben Sie die Administrations-ECL angepasst, müssen Sie sich darum kümmern, dass die Änderungen an alle Notes-Clients ausgerollt werden. Zum Abgleich einer Workstation-ECL (das ist die lokale ECL des Notes-Clients) mit der Administrations-ECL im Domino-Verzeichnis stehen drei Möglichkeiten zur Verfügung:

- > die Funktion @RefreshECL
- > die Schaltfläche **Alles Aktualisieren** im Dialog **Benutzersicherheit > Tätigkeiten anderer > Workstation**
- > die Zuordnung von Sicherheitsrichtlinien

Sie können etwa eine Notes-Mail mit einer Schaltfläche versenden, hinter der die Funktion @RefreshECL steckt, was aber nicht zuverlässig ist, da Sie nicht wissen, ob die Benutzer draufklicken. Entsprechend sollten Sie zum Aktualisieren der ECLs die Sicherheitsrichtlinie verwenden.

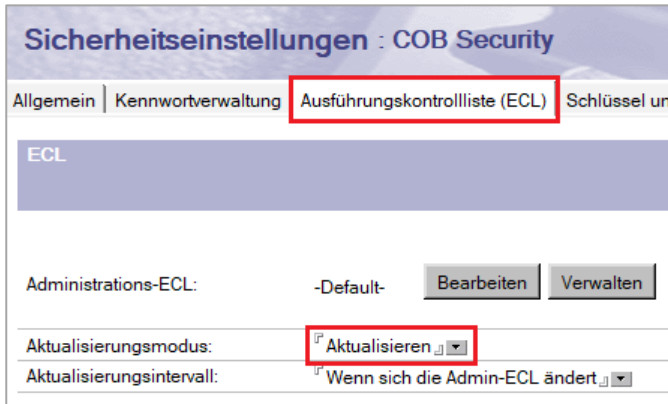


Abbildung 13.31: Sicherheitsrichtlinie, Register Ausführungskontrollliste (ECL)

Wählen Sie den **Aktualisierungsmodus** »Aktualisieren«, werden die fehlenden Einträge aus der Administrations-ECL zu den lokalen Workstation-ECLs hinzugefügt. Wählen Sie hin gegen »Ersetzen«, werden die lokalen Workstation-ECLs durch die Administrations-ECL ersetzt.

13.9.3. Mehrere Administrations-ECLs erstellen

In der Sicherheitsrichtlinie können Sie auch mehrere ECLs für unterschiedliche Benutzergruppen verwalten. Klicken Sie dazu auf die Schaltfläche **Verwalten**, tippen Sie den Namen der neuen ECL im Feld **Neue Admin-ECL erstellen** ein und bestätigen Sie mit **OK**. Der neue Name wird zwar sofort im Feld **Administrations-ECL** angezeigt, die ECL jedoch erst erstellt, wenn Sie danach einmalig auf **Bearbeiten** und **OK** klicken.

Über die Schaltfläche **Verwalten** können Sie Administrations-ECLs auch löschen:

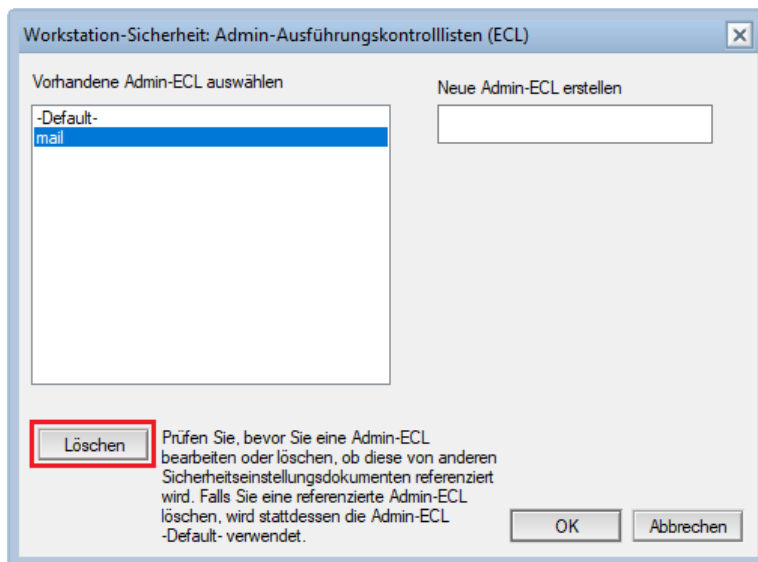


Abbildung 13.32: Admin-ECL verwalten

13.9.4. ECL-Empfehlungen

- > Die ECL sollte so eingestellt sein, dass vertrauenswürdige Programme alles dürfen und nicht vertrauenswürdige nichts.
- > Signieren Sie vertrauenswürdige Programme entweder mit einer Server-ID oder mit einem extra dafür erstellten Benutzer, z. B.: »Development/COB/AT«
- > Wird eine Server-ID zum Signieren verwendet, müssen alle anderen Server diesem Server vertrauen (Im Serverdokument als vertrauenswürdiger Server eintragen!)
- > NIE mit Verweisen auf die Organisation (z. B. */COB/AT) arbeiten! – Sonst wird dem Code jedes Benutzers vertraut!
- > Ein unsignierter Code sollte keine Rechte erhalten, ebenso wenig der mit einer unbekanntem Signatur versehene Code (Vorgabe).
- > Entziehen Sie Benutzern das Recht, die eigene ECL anzupassen!
- > Über den Platzhalter »<ECLOwner>« können Sie in der Administrations-ECL Vorgaben für Benutzer setzen. (><ECLOwner>« wird beim Aktualisieren der ECL durch den aktuellen Benutzernamen ersetzt.)

13.10. Gestaltungssicherheit

Diese Sicherheitsebene steuert den Zugriff auf Daten in Anwendungen und wird in der Regel von Entwicklern implementiert. Sie soll der Vollständigkeit halber hier nur gestreift werden. Zur Gestaltungssicherheit gehören die folgenden Bereiche:

- > Maskenzugriffslisten (\$Readers)
- > Lesezugriffslisten für Ansichten
- > Maskenformeln
- > Leserfelder
- > Autorenfelder
- > Öffentlicher Zugriff
- > Feldverschlüsselung

13.10.1. Leserfelder

Leserfelder (Reader Fields) steuern den Zugriff auf Dokumente. Sie sind sehr mächtig, denn sie übersteuern die Zugriffskontrollliste, d. h. auch Manager sehen Dokumente nicht, wenn sie in keinem Leserfeld aufscheinen. Leserfelder sind jedoch auch sehr ressourcenintensiv, da der Server für jeden Benutzer in allen Ansichten berechnen muss, was dieser sehen darf.

Beachten Sie, dass Leserfelder nur vom Server überprüft werden – außer Sie haben eine konsistente ACL eingestellt, dann erfolgt die Überprüfung auch lokal.

Beachten Sie bei Verwenden von Leserfeldern die folgenden Regeln:

- > Leserfelder können Personen und Gruppen enthalten sowie Benutzerrollen (in eckigen Klammern). Es kann außerdem mit Platzhalterzeichen gearbeitet werden, z. B. */COB/AT.
- > Ist nur ein Leserfeld vorhanden und dieses ist leer, haben alle Zugriff.
- > Gibt es mehrere Leserfelder, reicht es, in einem zu stehen.

- > Sind Leser und Autorenfelder vorhanden, reicht es auch, in einem Autorenfeld zu stehen.
- > Auch die Server müssen in Leserfeldern angegeben werden, sonst ist keine Replikation möglich.

Spezialfall Administratoren mit vollem Zugriff

Administratoren mit vollem Zugriff sehen immer alle Dokumente in einer Datenbank, auch wenn der Zugriff durch Leserfelder eingeschränkt wurde. Ähnliches gilt auch für Agenten, die von Administratoren mit vollem Zugriff erstellt werden. (Hier ist allerdings in den Eigenschaften des Agenten auch noch die Sicherheit auf »3. Beschränkte Operationen mit vollst. Admin-Rechten zulassen« hochzusetzen.) Somit können Administratoren mit vollem Zugriff Leserfelder in Datenbanken manipulieren.

13.10.2. Autorenfelder

Autorenfelder (Author Fields) dienen als Erweiterung für das Zugriffsrecht Autor. Ein Autor darf Dokumente erstellen, wenn er über das Zugriffsrecht »Dokumente erstellen« verfügt. Er darf einmal erstellte Dokumente jedoch nicht bearbeiten, wenn er nicht zusätzlich mit seinem Namen, einer Gruppenzugehörigkeit oder einer Rolle in einem Autorenfeld steht. Dass Autorenfelder auch berechnet sein können, macht sie vor allem im Workflow interessant.

Editoren und höher können Dokumente immer bearbeiten, auch wenn sie nicht in einem Autorenfeld stehen.

13.10.3. Öffentlicher Zugriff

Der sogenannte **öffentliche Zugriff** (Public Access) erlaubt es, in Notes oder auch im Web Zugriff auf einzelne Dokumente (bzw. Masken) und Ansichten zu gewähren. Dies funktioniert auch für Benutzer, die auf die Zieldatenbank keinen Zugriff haben. Beim Öffnen werden nur jene Dokumente und Ansichten angezeigt, die für den öffentlichen Zugriff freigegeben wurden, alle anderen Dokumente und Ansichten bleiben ausgeblendet. Der Hauptanwendungsfall für den öffentlichen Zugriff ist die Notes-Kalenderfreigabe.

Der öffentliche Zugriff kann nur im Domino-Designer aktiviert werden:

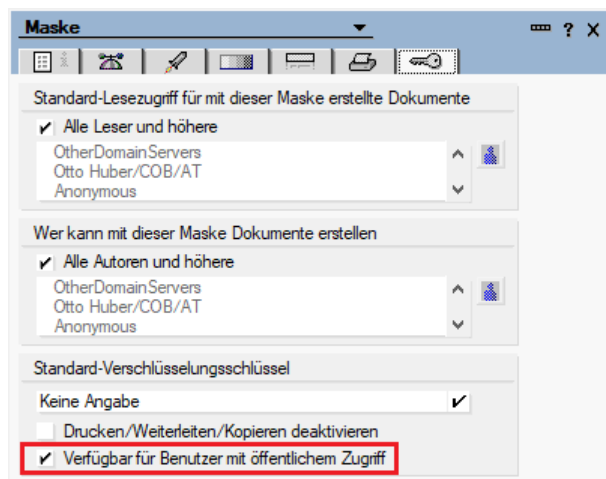


Abbildung 13.33: Öffentlichen Zugriff aktivieren

13.10.4. Feldverschlüsselung

13.10.4.1. Einen Geheimschlüssel erstellen

Der Vorteil von Geheimschlüsseln liegt sicherlich in der einfachen Verteilung. Sie – oder ein Entwickler – erstellen den Schlüssel in Ihrer ID-Datei. Anschließend verteilen Sie den Schlüssel per Mail oder als kennwortgeschützte Schlüsseldatei (*.key) an alle beteiligten Benutzer.

Um einen Geheimschlüssel zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Menü **Datei > Sicherheit > Benutzersicherheit**.
2. Wechseln Sie zum Register **Notes-Daten** und dann **Dokumente**.
3. Klicken Sie auf die Schaltfläche **Neuer Geheimschlüssel...**

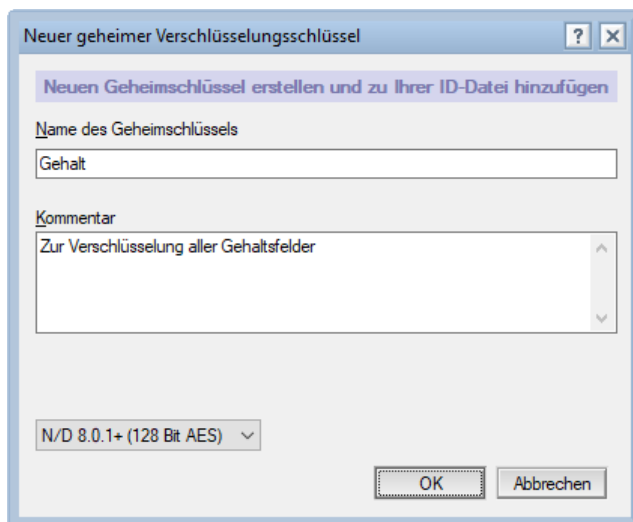


Abbildung 13.34: Dialog Neuer geheimer Verschlüsselungsschlüssel

4. Geben Sie einen Namen für den neuen Schlüssel ein.
5. (Optional) Verfassen Sie einen Kommentar, etwa um die Verwendung des Schlüssels zu erklären.
6. (Optional) Wählen Sie den Verschlüsselungsalgorithmus aus, z. B. N/D 8.0.1+ (128 Bit AES).
7. Klicken Sie auf **OK**.

13.10.4.2. Verschlüsselung in der Maske konfigurieren

Die Feldverschlüsselung muss von Ihnen oder einem Entwickler im Domino-Designer aktiviert werden. Gehen Sie dazu in der Maske zu dem zu verschlüsselnden Feld und wählen Sie in den Sicherheitsoptionen (**Feldeigenschaften**, Register **Erweitert**) den Wert »Verschlüsselung für dieses Feld aktivieren«:

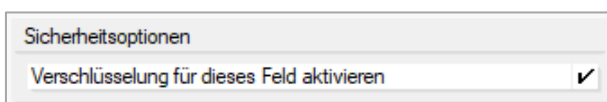


Abbildung 13.35: Feldeigenschaften, Sicherheitsoptionen

Sie können die Verschlüsselung für mehrere Felder einer Maske aktivieren. Das Feld kann einen beliebigen Datentyp besitzen. Wenn die Feldverschlüsselung aktiviert ist, werden die Feldbegrenzungen im Notes-Client rot dargestellt.

Welcher Schlüssel zur Anwendung kommt, steuern Sie in den **Maskeneigenschaften**, Register **Sicherheit**, im Feld **Standard-Verschlüsselungsschlüssel**.

Alternativ können Sie auch ein Feld mit dem reservierten Namen »SecretEncryptionKeys« hinzufügen, das den Namen des anzuwendenden Schlüssels berechnet.

Über ein Feld mit dem reservierten Namen »PublicEncryptionKeys« können Sie hingegen die Verschlüsselung mit Öffentlichen Schlüsseln erzwingen. Das Feld »PublicEncryptionKeys« muss die Namen der Benutzer berechnen, mit deren Öffentlichen Schlüsseln die Felder verschlüsselt werden sollen.

13.10.4.3. Verschlüsselung aus einem Dokument entfernen

Entwickler können die Verschlüsselung in der Maske für bestimmte oder alle Felder aufheben bzw. auch den Schlüssel ändern. Danach müssen die Dokumente von jemandem bearbeitet werden (z. B. über einen Agenten), der den passenden Schlüssel enthält. Nach dem Speichern sind die Felder nicht mehr verschlüsselt.

Beachten Sie bei der Planung der Anwendung, dass verschlüsselte Felder in Ansichten nicht angezeigt werden!

14. Der Webserver

- > 14.1 Fähigkeiten des Domino-Webservers, Seite 371
- > 14.2 Einrichten eines Domino-Webservers, Seite 372
- > 14.3 Benutzeranmeldung im Web, Seite 376
- > 14.4 Webserver-Konfiguration, Seite 380
- > 14.5 Ein Webserverprotokoll einrichten, Seite 383
- > 14.6 Einen sicheren Webserver aufbauen, Seite 387
- > 14.7 TLS-Zertifikate erstellen, Seite 394
- > 14.8 Der Domino-Webadministrator, Seite 409
- > 14.9 Einen Credential Store einrichten, Seite 410
- > 14.10 Webmail einrichten, Seite 411
- > 14.11 Auf HCL Verse umstellen, Seite 413

14.1. Fähigkeiten des Domino-Webservers

HCL Domino bietet einen integrierten Webserver, der Informationen sowohl aus statischen HTML-Seiten im Dateisystem als auch aus Notes-Datenbanken zur Verfügung stellen kann.

Wenn ein Webbrowser Informationen aus einer Notes-Datenbank anfordert, übersetzt Domino diese in HTML. Wenn ein Webbrowser eine statische HTML-Datei anfordert, liest Domino diese direkt aus dem Dateisystem. Der Domino-Webserver verwendet (wie alle anderen Webserver) das Standard-HTTP-Protokoll (Port 80 bzw. 443), um Informationen an Webbrowser zu senden.

Informationen in Notes-Datenbanken zu speichern ist wesentlich flexibler, als diese in statischen HTML-Seiten abzulegen, da sie dort nicht nur leichter bearbeitet, sondern auch (via Replikation) mit anderen Servern abgeglichen werden können.

Jede Notes-Datenbank ist von sich aus bereits eingeschränkt webfähig. Bevor Sie eine Datenbank erstellen, sollten Sie sich informieren, ob Webbrowser-Benutzer oder Notes-Benutzer (oder beide) darauf zugreifen werden. Manche Schablonen (Diskussion und TeamRoom) enthalten bereits ein mächtiges, auf XPages basierendes Webinterface.

14.1.1. Domino Webserver-Features im Detail

- > Unterstützung für statische HTML-Seiten im Dateisystem und Notes-Datenbanken.
- > Sicherheit der Anwendungen unter Verwendung der Standard-Domino-Sicherheit, wie etwa Zugriffskontrolllisten, kombiniert mit Internet-Sicherheit wie Authentifizierung über Name- und Kennwort.

- > Unterstützung für URL-Erweiterungen, die Domino-Funktionalität an Webbrowser weitergeben – etwa um ein Dokument zu speichern oder einen Agenten zu starten.
- > Automatische Übersetzung von Domino-Features in HTML-Code. So werden etwa Hot-Spots in HTML-Anchor-Tags (<A>) übersetzt.
- > Durchgangs-HTML (Pass-through HTML) ermöglicht die Verwendung von nativem HTML-Code in Domino-Designelementen wie Masken, Seiten und den Hilfedokumenten »Über diese Anwendung« und »Benutzen dieser Anwendung«. Damit können Domino-Features mit Webelementen (inklusive JavaScript) verbunden werden, die sonst nur in HTML möglich sind.
- > Unterstützung für JavaScript, eingebettet in Durchgangs-HTML oder auch direkt im Notes-Dokument.
- > Unterstützung für CGI-Programme, die via Durchgangs-HTML auf Seiten aufgerufen werden können. Unterstützte CGI-Programme sind: EXE-, CMD- und BAT-Dateien sowie Scripts programmiert in Perl, Python und PHP.
- > Das Domino Webserver Application Interface (DSAPI) unterstützt alle Phasen des Request-Handlings, inklusive dem Mapping und Transformieren von URLs, der Authentifizierung von Benutzern, der Verarbeitung von Anfragen und der Protokollierung.
- > Unterstützung für multiple Websites mit separaten DNS-Namen auf einem einzelnen Server.
- > Beim Einsatz von TLS (Transport Layer Security) und Internetzertifikaten ist nur eine IP-Adresse notwendig (Server Name Indication, SNI).
- > Unterstützung für das Feld Subject Alternative Name (SAN) in X.509-Zertifikaten.
- > URL-Weiterleitungen und Umleitungen zu Verzeichnissen oder anderen Ressourcen.
- > Unterstützung für Last-Modified-HTTP-Response-Header in Domino-URLs, was Webbrowsern oder Proxy-Servern erlaubt, Domino-Seiten zu cachen.
- > Unterstützung für Server-Cluster mit Ausfallsicherheit und Lastverteilung.

14.2. Einrichten eines Domino-Webservers

14.2.1. Bevor Sie einen Webserver einrichten

- > Muss der Domino-Server natürlich installiert worden sein und laufen.
- > Müssen Sie sich mit den Themen Serversicherheit und TCP/IP-Konzepte (DNS-Hostnamen und IP-Adressierung) vertraut gemacht haben.
- > Um Benutzern zu erlauben, innerhalb des lokalen Netzwerkes (im Intranet) auf Ihren Domino-Webserver zuzugreifen, müssen Sie den voll qualifizierten Servernamen im DNS-Server Ihrer Organisation registriert haben.
- > Um Benutzern zu erlauben, sich über das Internet mit Ihrem Domino-Server zu verbinden, müssen Sie:
 - über eine öffentliche IP-Adresse verfügen.
 - bei einem Internet Service Provider (ISP) eine Internet-Domäne registriert haben, um den Webserver über einen Hostnamen (www.IhreFirma.de) ansprechen zu können.
 - bei einer vertrauenswürdigen Zertifizierungsstelle (CA) ein Internetzertifikat angefordert und eingespielt haben, um Ihren Anwendern einen sicheren Zugriff auf den Webserver zu ermöglichen.

- > Sollte es nicht schon der Fall sein, müssen Sie gegebenenfalls Ihre Firewall für die Protokolle HTTP und HTTPS öffnen.

14.2.2. Den Webserver starten

Der Webserver ist identisch mit dem HTTP-Task. Überprüfen Sie über den folgenden Befehl, ob dieser bereits läuft:

```
show tasks only
```

```
HTTP Server      Listen for connect requests on TCP Port:80, 443
```

Wenn der HTTP-Server nicht läuft, starten Sie ihn mit dem Befehl:

```
load http
```

Sie sollten in weiterer Folge dafür sorgen, dass der Task automatisch startet, wenn der Domino-Server hochfährt, entweder über die Variable ServerTasks in der notes.ini oder über ein Programm-dokument:

Programm: HTTP	
Allgemein Administration	
Allgemein	Zeitplan
Programmname: <input type="text" value="HTTP"/>	Aktiviert/deaktiviert: <input type="text" value="Nur beim Serverstart"/>
Befehlszeile: <input type="text"/>	
Läuft auf Server: <input type="text" value="DOM/COB/AT"/>	
Kommentare: <input type="text"/>	

Abbildung 14.1: Programmdokument zum automatischen Start des HTTP-Servers

14.2.3. Eine Webseite einrichten

Ist der HTTP-Task aktiv, können Sie in der Adresszeile des Webbrowsers entweder den Hostnamen oder die IP-Adresse des Domino-Servers eingeben.

Was dann angezeigt wird, steuern Sie im Serverdokument, Register **Internetprotokolle** > **HTML** im Abschnitt **Zuordnung**:

Zuordnung	
Home-URL:	<input type="text" value="/homepage.nsf?Open"/>
HTML-Verzeichnis:	<input type="text" value="domino/html"/>
Symbolverzeichnis:	<input type="text" value="domino/icons"/>
Symbol-URL-Pfad:	<input type="text" value="/icons"/>
CGI-Verzeichnis:	<input type="text" value="domino/cgi-bin"/>
CGI-URL-Pfad:	<input type="text" value="/cgi-bin"/>

Abbildung 14.2: Vorgabepfade des Domino-Webserver

Standardmäßig wird die Datenbank homepage.nsf als Startseite angezeigt:

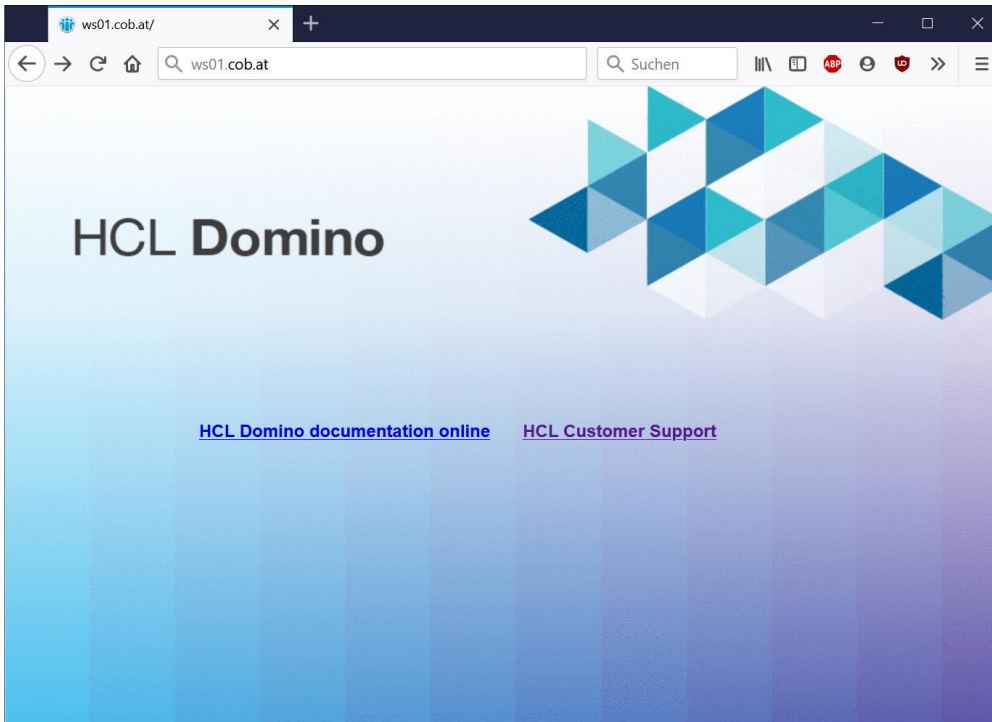


Abbildung 14.3: Vorgabestartseite des Domino-HTTP-Servers

Wollen Sie eine andere Startseite haben, müssen Sie nur den Verweis im Feld **Home-URL** austauschen. Sie können dort auf eine Notes-Datenbank oder auf eine statische HTML-Seite verweisen. Danach müssen Sie den HTTP-Task neu starten:

```
tell http restart
```

In Abbildung 14.2 sehen Sie, dass Sie HTML-Seiten im Unterverzeichnis `domino\html` platzieren müssen, um direkt darauf zugreifen zu können:

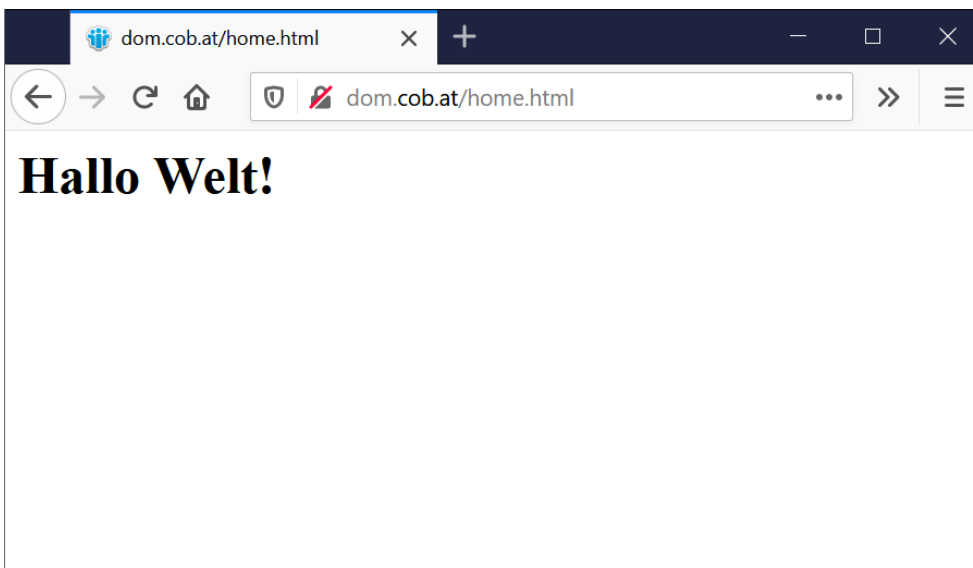


Abbildung 14.4: Statische HTML-Seite home.html im Unterverzeichnis `domino\html`

14.2.4. Mehrere Websites einrichten

Wenn Sie den Webserver nur dazu verwenden wollen, um Ihre Website zu hosten, kommen Sie mit der Konfiguration im Serverdokument aus. Brauchen Sie jedoch mehrere Websites oder wollen Sie Ihren Anwendern Webmail oder gar die Anbindung mobiler Clients ermöglichen, sollten Sie auf die Verwendung von Internet-Site-Dokumenten umstellen. Ich würde sogar bei der Verwendung einer einzigen Website auf Internet-Site-Dokumente umstellen, da dies wesentlich mehr Möglichkeiten bietet.

Um Internet-Site-Dokumente einzurichten, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Administration** > **Server**.
2. Öffnen Sie das gewünschte Serverdokument und aktivieren Sie die Einstellung **Internet-Konfigurationen aus Server-Internet-Site-Dokumenten laden**.
3. Speichern und schließen Sie das Serverdokument.
4. Navigieren Sie nun zur Ansicht **Web** > **Internet-Sites** und klicken Sie auf die Schaltfläche **Internet-Site hinzufügen... > Web**.

Site-Informationen	
Beschreibender Name dieser Site:	IP cobsoft.at
Organisation:	IP COB
Diese Website bearbeitet Anforderungen, die keiner anderen Website zugeordnet werden können:	<input type="radio"/> Ja <input checked="" type="radio"/> Nein Hinweis: Nur bei einer einzigen Website sollte diese Option auf 'Ja' gesetzt werden
Hostnamen und Adressen, die dieser Site zugeordnet werden:	IP www.cobsoft.at 212.186.208.67
Domino-Server, die diese Website hosten:	IP DOM/COB/AT

Abbildung 14.5: Internet-Site-Dokument, Register Allgemein am Beispiel von www.cobsoft.at

5. Geben Sie einen beschreibenden Namen für die Internet-Site ein, z. B. den Namen der Website.
6. Geben Sie den Namen der Organisation ein.
7. Geben Sie an, ob es sich um die Vorgabe-Website handelt. Wählen Sie »Ja«, wird diese Adresse verwendet, wenn der in der Anfrage verwendete Hostname oder die IP-Adresse keiner anderen Website zugeordnet werden kann. Wählen Sie »Nein«, wenn Sie stattdessen den Hostnamen und/oder die IP-Adresse angeben wollen.
8. Wählen Sie im Feld **Domino-Server, die diese Website hosten** die Server aus, die auf die Anfrage reagieren sollen. Sie können auch einen Stern (*) eingeben, wenn die Website alle Server betrifft.
9. Wechseln Sie zum Register **Konfiguration**, um die Startseite festzulegen. Im Beispiel in Abbildung 14.6 wird auf eine statische HTML-Seite verwiesen.
10. Speichern und schließen Sie das Dokument.
11. Starten Sie den HTTP-Server neu.

Achtung: Haben Sie auf Internet-Site-Dokumente umgestellt, müssen Sie auch für alle anderen IP-Protokolle Site-Dokumente konfigurieren, etwa für IMAP, SMTP oder LDAP.



Abbildung 14.6: Internet-Site-Dokument, Register Konfiguration mit statischer Home-URL

14.3. Benutzeranmeldung im Web

14.3.1. Anonyme Benutzer

Benutzer, die sich nicht angemeldet haben, gelten als **anonym**. Und sie sind nicht nur anonym, sie heißen auch so: Über den Platzhalter »Anonymous« können Sie ihnen in den Zugriffskontrolllisten Rechte zuweisen. Steht der Eintrag »Anonymous« nicht in der ACL, fallen anonyme Benutzer automatisch unter »-Default-«.

Anonyme Benutzer können auf statische HTML-Seiten zugreifen bzw. auf Datenbanken, in deren Zugriffskontrolllisten der Eintrag »Anonymous« (bzw. »-Default-«, wenn »Anonymous« fehlt) mit dem Recht Leser oder höher enthalten ist. (Es gibt auch noch den Spezialfall »Öffentliche Dokumente lesen« – siehe auch Kap. 13.10.3 Öffentlicher Zugriff, ab Seite 367.)

Greift ein anonym Benutzer auf eine Ressource zu, auf die er kein Recht hat, wird er aufgefordert, den Namen und das Kennwort eines Benutzers einzugeben, der das Recht dazu hat. In anderen Worten: Er muss sich authentifizieren.

14.3.2. Arten der Authentifizierung

Der Webserver kennt drei Arten der Authentifizierung:

- > Standardauthentifizierung (Basic Authentication)
- > Sitzungsauthentifizierung (Session Authentication)
- > Zertifikatbasierte Authentifizierung

14.3.2.1. Standardauthentifizierung (Basic Authentication)

Beim Zugriff auf eine Ressource, auf die ein anonym Benutzer kein Recht hat, wird eine 401-Meldung an den Webbrowser geschickt, der darauf den Anmeldedialog anzeigt. Diese Meldung beinhaltet einen sogen. **Realm** (Bereich). Dabei handelt es sich um den Pfad, für den der Benutzer

authentifiziert werden muss. Der Benutzer gilt als authentifiziert, wenn Name und Internetkennwort mit den Angaben in einem Personendokument bzw. im ID-Vault übereinstimmen.

Bei der Standardauthentifizierung werden bei jeder Anfrage Benutzername und Kennwort codiert im Paket-Header mitgeschickt. Die dazu verwendete Base64-Codierung erhöht nicht die Sicherheit, sondern nur die Kompatibilität: Jedes Zeichen wird in ein druckbares ASCII-Zeichen umgewandelt, damit die Daten auch von Gateways, die nur ASCII-Code verarbeiten können, transportiert werden. Eine Base64-codierte Zeichenfolge kann jederzeit in Normaltext zurückverwandelt werden. (Das Auslesen der Daten aus dem Header nennt man »Sniffen«.)

14.3.2.2. Sitzungsauthentifizierung (Session Authentication)

Dieser Authentifizierungstyp wird auch maskenbezogene Authentifizierung genannt, da eine Anmeldemaske angezeigt wird. Greift ein Benutzer auf eine Ressource zu, auf die er keinen Zugriff hat, wird eine 200 OK HTTP-Meldung zum Browser zurückgeschickt. Anstatt die gewählte Ressource anzuzeigen, wird die vordefinierte Anmeldemaske angezeigt. Diese sieht, wenn man keine hübschere Maske bereitgestellt hat, so aus:

Serveranmeldung

Geben Sie bitte Ihren Benutzernamen und Ihr Kennwort ein.

Benutzername:

Kennwort:

Abbildung 14.7: Vorgabeanmeldemaske nach Aktivieren der Sitzungsauthentifizierung

Der Benutzer gibt seinen Anmeldenamen und sein Anmeldekennwort ein und sendet die Maske ab. Waren die Anmeldeinformationen richtig, wird ein Cookie erstellt, welches dann für alle weiteren Anfragen des Benutzers zur Authentifizierung verwendet wird.

Der Server behält eine Liste aller aktiven Benutzersitzungen im Speicher. Wenn längere Zeit (einstellbar, Vorgabe ist 30 Min.) keine Aktivitäten erfolgt sind, werden die Sitzungsinformationen gelöscht und der Benutzer muss sich erneut anmelden.

Achtung: Benutzername und Kennwort werden bei dieser Methode zwar nur bei der Anmeldung, dafür aber im Klartext (also auch nicht Base64-codiert) über das Netzwerk übertragen! Entsprechend sollte die Sitzungsauthentifizierung immer mit TLS verschlüsselt sein.

Bei der sitzungsbasierten Authentifizierung wird zwischen der Option »Für jeden Server getrennt« (Single Server) und »Serverübergreifend« (SSO) unterschieden.

Authentifizierung pro Server

Konfigurieren Sie eine getrennte Authentifizierung, gelten die Cookies für jeden Server einzeln. Klicken Benutzer auf einen Link, der zur Anwendung auf einem anderen Server führt, müssen sie sich erneut anmelden.

Serverübergreifende Authentifizierung

Bei der Konfiguration von SSO (Single Sign On) gelten die Cookies serverübergreifend, d. h. Benutzer müssen sich nicht erneut anmelden, wenn Sie einem Link zu einem anderen Server folgen. Die Verwendung von SSO erfordert zusätzlich das Einrichten einer **Web-SSO-Konfiguration**.

Um eine Web-SSO-Konfiguration zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie zur Ansicht **Web > Internet-Sites** und klicken Sie auf die Schaltfläche **Web-SSO-Konfiguration erstellen**.
2. Geben Sie einen Namen ein (Vorgabe ist »LtpaToken«).
3. Geben Sie den Namen der Organisation ein (muss mit der Organisation im Internet-Site-Dokument übereinstimmen).
4. Geben Sie die DNS-Domäne ein, für die der Schlüssel (Token) generiert werden soll, z. B. .cob.at (mit führendem Punkt!). Die Server mit SSO-Aktivierung müssen alle der angegebenen DNS-Domäne angehören, z. B. www.cob.at, mail.cob.at etc.

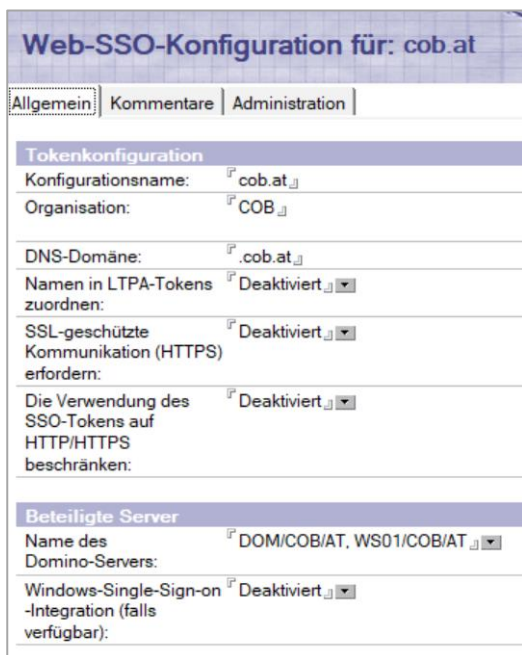


Abbildung 14.8: Web-SSO-Konfiguration

5. Wählen Sie die beteiligten Server aus.
6. Klicken Sie auf **Schlüssel... > Domino SSO-Schlüssel erstellen**. Es wird der folgende Dialog angezeigt:

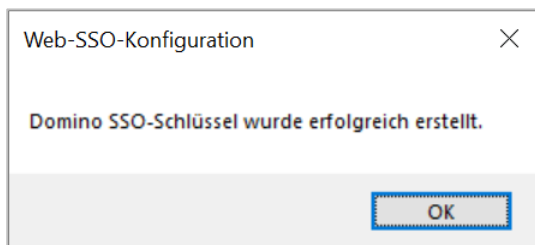


Abbildung 14.9: Domino SSO-Schlüssel erfolgreich erstellt

7. Setzen Sie gegebenenfalls ein Zeitlimit für die Sitzung.
8. Speichern und schließen Sie das Dokument.
9. Öffnen Sie nun das Website-Dokument und wechseln Sie zum Register Domino-Webserver. Wählen Sie im Feld **Sitzungsauthentifizierung** »Serverübergreifend (SSO)« und im Feld **Web-SSO-Konfiguration** den Namen der erstellten Konfiguration, in unserem Beispiel »cob.at«:



Abbildung 14.10: SSO-Konfiguration im Website-Dokument

Sie können auch einen von WebSphere generierten LTPA-Schlüssel importieren, um SSO zwischen HCL Domino und HCL Connections einzurichten.

14.3.2.3. Authentifizierung über Client-Zertifikate

Der Client (Webbrowser) weist sich bei dieser Art der Authentifizierung gegenüber dem Domino-Server über ein Internetzertifikat aus. Die Eingabe eines Namens oder Kennworts wird beim Zugriff unterdrückt, weil der Benutzer bereits über das Zertifikat authentifiziert ist. Die zertifikatbasierte Authentifizierung wird in diesem Buch nicht behandelt.

14.3.3. Welche Anmeldenamen sind erlaubt?

Per Vorgabe akzeptiert der Webserver zur Authentifizierung nur Namensvarianten aus dem Feld Benutzername (User name). Das bedeutet, dass der Benutzer seinen vollständigen Namen angeben muss – außer Sie stellen ihm einen kürzeren Anmeldenamen als Alias in diesem Feld zur Verfügung. Sollen alle Namensfelder zur Anmeldung erlaubt sein (immer unter der Voraussetzung, dass sie eindeutig sind), müssen Sie im Serverdokument, im Register **Sicherheit**, im Feld **Internet-Authentifizierung** auf »Mehr Namensvariationen mit geringerer Sicherheit« umstellen:

Abbildung 14.11: Serverdokument, Register **Sicherheit** – **Internetzugriff**

Der Server verwendet dann zum Nachschlagen des Anmeldenamens die versteckte Ansicht (\$Users), die alle Namenskomponenten enthält. Sie können sogar eine eigene Ansicht definieren, in der nur bestimmte Benutzer aufscheinen, und den Webserver über den folgenden Eintrag in der Datei notes.ini dazu veranlassen, diese zum Überprüfen der Anmeldedaten zu verwenden:

```
NABWebLookupView=<Ansicht>
```

14.3.4. Benutzer ohne Zugriff auch für HTTP sperren

Benutzer, die Ihr Unternehmen verlassen haben, werden üblicherweise ins Feld **Kein Serverzugriff** aufgenommen (bzw. in die Gruppe, die dort steht). Das funktioniert standardmäßig jedoch nur für das NRPC-Protokoll (also für den Zugriff über einen Notes-Client), beim Webzugriff wird die Serverzugriffsliste per Vorgabe ignoriert!

Wenn Sie wollten, dass gesperrte Benutzer auch über das HTTP-Protokoll ausgeschlossen werden, müssen Sie im Register **Ports... > Internet-Ports... > Web** das Feld **Einstellungen zum Serverzugriff erzwingen** auf »Ja« setzen:

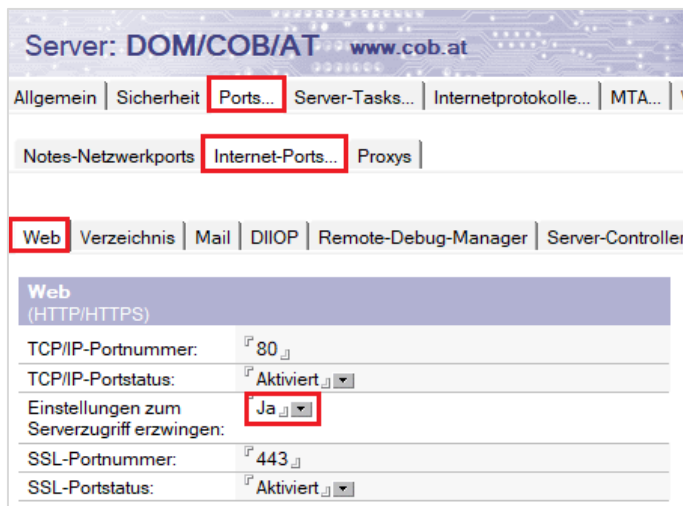


Abbildung 14.12: Serverdokument, Register Ports... > Internet-Ports... > Web

Jetzt fehlt nur noch eine vernünftige Anmeldemaske. Um diese zu erhalten, müssen Sie zuerst eine Datenbank erstellen. Wie Sie das genau machen, erkläre ich im nächsten Kapitel.

14.4. Webserver-Konfiguration

Mithilfe der Webserver-Konfiguration (Datenbank domcfg.nsf – die Anwendung ist nur auf Englisch verfügbar) können Sie ohne viel Aufwand vordefinierte Masken zum Anmelden und zur Ausgabe diverser Fehlermeldungen bereitstellen. Über diese Datenbank können Sie auch (die entsprechenden Entwicklerkenntnisse vorausgesetzt) eigene Masken erstellen und einbinden.

Um die Datenbank Webserver-Konfiguration zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in Domino-Administrator den Menüpunkt **Datei > Anwendung > Neu...** (oder drücken Sie die Tasten [Strg]+[N]).
2. Geben Sie im Feld **Server** den Namen des Domino-Webservers an, auf dem Sie die Datenbank erstellen möchten.
3. Setzen Sie das Häkchen für **Weitere Schablonen anzeigen** und wählen Sie in der Liste die Schablone »Domino Web Server Configuration 11« (domcfg5.ntf) aus.
4. Geben Sie einen beliebigen Titel ein, aber nennen Sie die Datenbank unbedingt »domcfg.nsf«:

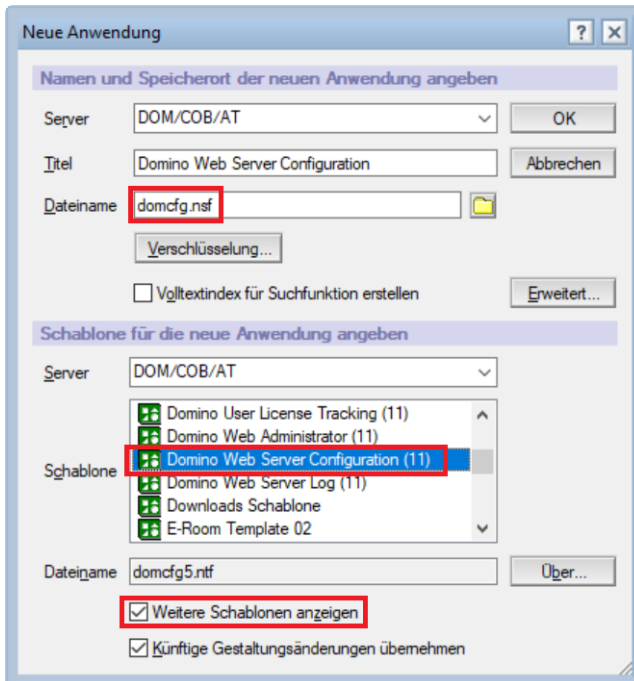


Abbildung 14.13: Datenbank Domino Web Server Configuration (domcfg.nsf) erstellen

5. Klicken Sie auf **OK**.
6. Stellen Sie sicher, dass der Eintrag »Anonymous« mit Leserzugriff in der ACL steht.

14.4.1. Eine Anmeldemaske bereitstellen

Um eine Anmeldemaske aus der Datenbank domcfg.nsf bereitzustellen, gehen Sie wie folgt vor:

1. Öffnen Sie die soeben erstellte Datenbank und klicken Sie in der Ansicht **Sign In Form Mappings** auf die Schaltfläche **Add Mapping**:

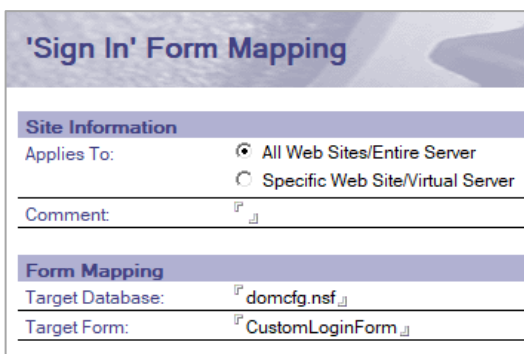


Abbildung 14.14: Sign In Form Mapping

2. Wenn Sie wollen, dass die Anmeldemaske für alle Websites gilt, wählen Sie im Feld **Applies To** »All Web Sites/Entire Server«, ansonsten wählen Sie »Specific Web Site/Virtual Server« und geben den Namen der Website im Feld **Web Site/Virtual Server** ein.
3. Geben Sie im Feld **Target Database** den Namen der Datenbank ein, in der die Anmeldemaske gespeichert ist (Vorgabe ist domcfg.nsf).

4. Geben Sie im Feld **Target Form** den Namen (oder den Alias) der Anmeldemaske ein. Der Name der vordefinierten Maske mit dem Schlüssel lautet »CustomLoginForm«.

Eine etwas moderner anmutende Anmeldemaske finden Sie in der Datenbank »HCL iNotes Redirect« (Schablone iwaredir.ntf) unter dem Namen »DWALoginForm«.

5. Speichern und schließen Sie das Dokument.

Die neue Anmeldemaske sollte sofort bereitstehen:



Abbildung 14.15: Vorgabe-Anmeldemaske aus der Datenbank domcfg.nsf

Sie können die Maske `$$LoginUserForm` im Domino-Designer anpassen, z. B. auf Deutsch übersetzen und Ihr Firmenlogo hinzufügen. Sie können aber auch eine komplett neue Anmeldemaske erstellen und dann im Mapping auf diese verweisen.

14.4.2. Eine Maske zur Kennwortänderung bereitstellen

Die Webserver-Konfiguration enthält auch eine Vorgabemaske zur Kennwortänderung. Die Maske wird automatisch angezeigt, wenn das Kennwort abgelaufen ist.

Um die Maske zu aktivieren, klicken Sie in der Ansicht **Change Password Form Mappings** auf die Schaltfläche **Add Mapping**.

Analog zur Anmeldemaske können Sie auch diese Maske (`$$ChangePasswordForm`) an Ihre Bedürfnisse anpassen, also etwa auf Deutsch übersetzen.

14.4.3. Fehlermeldungen des Webservers anpassen

Weiters können Sie in der Datenbank domcfg.nsf vom Web-Server generierte Fehlermeldungen oder Antworten auf benutzerdefinierte Masken umleiten.

Sie können die Nachrichten für folgende Fälle anpassen:

- > Der Benutzer konnte sich beim Server nicht authentifizieren.
- > Der Benutzer ist nicht berechtigt, auf eine bestimmte Datenbank zuzugreifen, die Teil der Website auf dem Server ist.

- > Der Benutzer gibt dem Server den Befehl, ein Dokument in einer Datenbank zu löschen, und der Server schließt die Ausführung des Befehls erfolgreich ab.
- > Das Internetkennwort eines Benutzers ist abgelaufen.
- > Der Benutzer versucht, das Internetkennwort zu ändern. Diese Operation ist jedoch nicht zulässig.
- > Der Benutzer ändert das Internetkennwort und die Änderung wird eingereicht und angenommen.
- > Ferner können Sie eine allgemeine Nachricht für alle anderen Fehlertypen oder Antworten angeben, die auf dem Web-Server auftreten.

Die vordefinierten Fehlermeldungen werden nur angezeigt, wenn der Fehler beim Zugriff auf NSF-Dateien auftritt, nicht aber bei HTML-Dateien.

Datenbankentwickler können auch benutzerdefinierte Fehlermeldungen für einzelne Datenbanken erstellen, die nur dann generiert werden, wenn der Fehler beim Zugriff auf diese Datenbank auftritt.

14.5. Ein Webserverprotokoll einrichten

Sie können zwei verschiedene Arten von Protokollierungen aktivieren:

1. Die Protokollierung in der Notes-Datenbank `domlog.nsf`
2. Die Protokollierung in Textdateien

14.5.1. Protokollierung in einer Notes-Datenbank

Das Domino-Webserverprotokoll `domlog.nsf` ist hübsch gemacht, aber nur für kleinere Umgebungen mit wenigen Anforderungen geeignet. Bei stärker ausgelasteten Webservern ist zu bedenken, dass das Protokollieren in der Notes-Datenbank wesentlich langsamer ist als das Protokollieren in Textdateien.

Im Domino-Webserverprotokoll werden alle Aktivitäten des Domino-Webserver und Informationen zu den einzelnen HTTP-Anforderungen aufgezeichnet:

- > Datum und Uhrzeit der Anforderung
- > IP-Adresse des Benutzers (oder die DNS-Adresse, wenn im Serverdokument **DNS-Suche** aktiviert ist)
- > Benutzername (wenn der Benutzer einen Namen und ein Kennwort für den Zugriff auf den Server angegeben hat)
- > Statuscode, den der Server an den Browser zurückgibt, um anzugeben, ob die Anforderung erfolgreich generiert wurde
- > Umfang (in Byte) der vom Server an den Browser gesendeten Informationen
- > Art der Daten, auf die ein Benutzer zugreift, z. B. `text/html` oder `image/gif`
- > Vom Server an den Browser gesendete HTTP-Anforderung
- > Für den Zugriff auf den Server benutzter Browser-Typ

Der Webserver: Ein Webserverprotokoll einrichten

- > Interne und CGI-Programmfehler (Common Gateway Interface)
- > URL, die der Benutzer besucht hat, um Zugriff auf eine Seite dieser Site zu erhalten
- > IP-Adresse des Servers oder DNS-Name
- > Zeitdauer in Millisekunden, die für die Verarbeitung der Anforderung erforderlich war
- > Vom Browser gesendete Cookies
- > Übersetzte URL (vollständiger Pfad zu der tatsächlichen Serverressource, wenn verfügbar)

Um die Notes-Datenbank domlog.nsf als Webserverprotokoll zu aktivieren, setzen Sie im Serverdokument, Register **Internetprotokolle...** > **HTTP** im Bereich **Protokollierung aktivieren für** das Feld **Domlog.nsf** auf »Aktiviert«:



Protokollierung aktivieren für:	
Protokolldateien:	Deaktiviert ▾
Domlog.nsf:	Aktiviert ▾

Abbildung 14.16: Serverdokument, Register Internetprotokolle... > HTTP, Bereich Protokollierung aktivieren

14.5.1.1. Informationen aus dem Protokoll ausschließen

In der Datenbank werden nicht nur Seitenaufrufe protokolliert, sondern auch jeder einzelne Bild- oder CSS-Aufruf, also Informationen, die Sie in der Regel nicht interessieren. Dazu kommen die Zugriffe der eigenen Mitarbeiter auf Webmail und Traveler, die Sie auch nur begrenzt interessieren dürften. Wenn Sie diese Informationen nicht sehen wollen, schließen Sie sie vom Protokoll aus.

Geben Sie dazu im Bereich **Vom Protokoll ausschließen** alles an, was nicht aufscheinen soll. In Tabelle 14.1 finden Sie eine Aufstellung der verschiedenen Optionen:

Feld	Eingabe
URLs	Geben Sie auszuschließende URL-Pfade ein – z. B. »*.gif« oder »/mail/*«
Verfahren	Geben Sie HTTP-Verfahren ein – z. B. »POST« oder »DELETE«
MIME-Typen	Geben Sie die auszuschließenden MIME-Typen an – z. B. »image/gif« (für .GIF-Bilder) oder »text/css« (für CSS-Dateien)
Benutzer-Agenten	Geben Sie Zeichenfolgen ein, die Teil von Benutzer-Agent-Zeichenfolgen (Browser-Namen) sind, um Anforderungen eines bestimmten Benutzer-Agenten auszuschließen. Geben Sie z. B. zum Ausschließen des Microsoft Internet Explorer »MSIE*« ein.
Ausgabecodes	Geben Sie auszuschließende HTTP-Antwort-Codes ein – z. B. »300«
Hosts und Domänen	Geben Sie auszuschließende DNS-Namen oder IP-Adressen für Browser-Clients ein – z. B. »136.142.*« oder »*.org«. Um DNS-Namen ausschließen zu können, müssen Sie zunächst im Serverdokument auf dem Register Internet-protokolle > HTTP die Einstellung DNS-Suche aktivieren. Andernfalls können Sie nur IP-Adressen eingeben. Das Aktivieren dieser Einstellung wirkt sich auf die Leistung aus.

Tabelle 14.1: Optionen zum Ausschließen von Einträgen im Webserver-Protokoll

Hier ein Beispiel von meinem eigenen Webserver:

Vom Protokoll ausschließen	
URLs:	<input type="checkbox"/> /traveler* <input type="checkbox"/> /mail/* <input type="checkbox"/> /iNotes/* <input type="checkbox"/> /redir.nsf
Verfahren:	<input type="checkbox"/>
MIME-Typen:	<input type="checkbox"/> image/gif <input type="checkbox"/> image/jpeg <input type="checkbox"/> image/png <input type="checkbox"/> text/css
Benutzer-Agenten:	<input type="checkbox"/>
Rückkehrcodes:	<input type="checkbox"/>
Hosts und Domänen:	<input type="checkbox"/>

Abbildung 14.17: Serverdokument, Register Internetprotokolle... > HTTP (Erklärung im Text)

In obigem Beispiel werden die folgenden Einträge ausgeschlossen:

- > Bildaufrufe
- > CSS-Aufrufe
- > Webmail-Zugriffe (unter der Voraussetzung, dass Maildateien im Verzeichnis (Mail stehen)
- > Zugriffe auf HCL iNotes Redirect (in meinem Fall redir.nsf)
- > Traveler-Zugriffe (die in den Protokollen des Traveler-Servers besser sichtbar sind)

14.5.2. Protokollierung in Textdateien

Die Protokollierung in Textdateien geht schneller und empfiehlt sich für stärker ausgelastete Webserver. Dafür ist die Auswertung der Protokolle nicht so komfortabel wie in der Notes-Datenbank domlog.nsf. Sie können die Protokollierung in einer einzigen Datei oder – je nach Funktion – auch in mehreren Dateien konfigurieren. Die meisten Protokollanalyseprogramme von Fremdanbietern benötigen eine einzige Textdatei.

14.5.2.1. So aktivieren Sie die Protokollierung in Textdateien

Um die Protokollierung in Textdateien zu aktivieren, setzen Sie im Serverdokument, Register **Internetprotokolle... > HTTP** im Bereich **Protokollierung aktivieren für** das Feld **Protokolldateien** auf »Aktiviert«. Standardmäßig speichert Domino die Protokolldateien im Datenverzeichnis, Sie können im Feld **Verzeichnis für Protokolldateien** aber auch ein anderes Verzeichnis angeben. Außerdem können Sie die Namen der Protokolldateien für die einzelnen Bereiche vorgeben:

Feld	Eingabe
Verzeichnis für Protokolldateien	Das Verzeichnis zum Speichern der Protokolldateien. Bleibt das Feld leer, speichert Domino die Protokolldateien im Datenverzeichnis.
Zugriffsprotokoll	Das Präfix für die Zugriffsprotokolldatei. Die Vorgabe lautet »access«. Geben Sie keine Dateierweiterung ein.
Agentenprotokoll	Das Präfix für die Agentenprotokolldatei. Die Vorgabe lautet »agent«. Wenn Sie sich für das Format »Erweitert allgemein« entscheiden, benötigen Sie kein Agentenprotokoll; die entsprechenden Informationen sind dann im Zugriffsprotokoll enthalten.
Referrer-Protokoll	Das Präfix für die Referenzprotokolldatei. Die Vorgabe lautet »referer«.

Feld	Eingabe
	Wenn Sie sich für das Format »Erweitert allgemein« entscheiden, benötigen Sie kein Referenzprotokoll; die entsprechenden Informationen sind im Zugriffsprotokoll enthalten.
CGI-Fehlerprotokoll	Das Präfix für das CGI-Fehlerprotokoll. Die Vorgabe lautet »cgi-error«. Das CGI-Fehlerprotokoll wird nur dann erstellt, wenn das CGI-Script Informationen in »stderr« protokolliert. Das Format der CGI-Protokollinformationen ist abhängig vom CGI-Script. Das Zugriffsprotokollformat hat keinerlei Auswirkung auf das CGI-Fehlerprotokoll.

Tabelle 14.2: Die verschiedenen Protokolldateien des Webservers

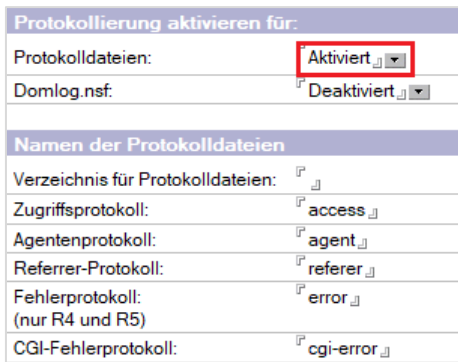


Abbildung 14.18: Serverdokument, Reg. Internetprotokolle... > HTTP – Protokolldateien aktivieren

Während der Webserver läuft, erstellt er neue Protokolldateien, abhängig von den Einstellungen für die Zeit bis zum Löschen der Protokolldatei. Wenn der Webserver nicht läuft, erstellt er Protokolldateien nach Bedarf, sobald der Webserver gestartet wird.

Geben Sie im Bereich **Protokolldatei-Einstellungen** Werte in die folgenden Felder ein:

Feld	Eingabe
Zugriffsprotokollformat	Wählen Sie einen der folgenden Werte aus: »Allgemein« – Informationen werden in drei separaten Protokolldateien aufgezeichnet. »Erweitert allgemein« – Informationen werden in einer Datei aufgezeichnet.
Zeitformat	Wählen Sie ein Format für die Aufzeichnung der Uhrzeit: »Ortszeit« (Vorgabe) verwendet die Zeitzone des Servers. »GMT« verwendet die westeuropäische Zeit.
Protokolldatei löschen	Geben Sie an, wie häufig eine neue Protokolldatei erstellt wird: » Täglich « (Vorgabe) für jeden Tag; die Protokollierung startet dabei um Mitternacht. Es wird der folgende Dateiname verwendet: <i>Dateinamenpräfix</i> TTMMJJJ.log, z. B. »access19052021.log« für den 19. Mai 2021. » Wöchentlich « für jede Woche; die Protokollierung startet dabei am Sonntag um Mitternacht. Es wird der folgende Dateiname verwendet: <i>Dateinamenpräfix</i> __WWJJJ.log, z. B. »access__210221.log« für die Woche vom 21. Februar 2021.

Feld	Eingabe
	<p>»Monatlich« für jeden Monat; die Protokollierung startet dabei am ersten Tag des Monats um Mitternacht. Es wird der folgende Dateiname verwendet: <i>Dateinamenpräfix-MMJJJJ.log</i>, z. B. »access-052021.log« für Mai 2021.</p> <p>»Nie« für keine zeitliche Begrenzung. Dabei wird der folgende Dateiname verwendet: <i>Dateinamenpräfix.log</i>, z. B. »access.log«.</p>
Maximale Länge eines Protokolleintrags	Die für einen Eintrag in der Zugriffsprotokolldatei maximal zulässige Länge. Wenn der Eintrag die angegebene Länge überschreitet, wird er nicht in die Datei geschrieben. Der Vorgabewert ist 10 KB.
Maximale Größe des Zugriffsprotokolls	Die für die Zugriffsprotokolldatei maximal zulässige Größe. Wenn diese Grenze erreicht ist, werden keine weiteren Einträge in die Datei geschrieben. Der Wert »0« (Vorgabe) bedeutet, dass die Datei in ihrer Größe nicht beschränkt ist.

Tabelle 14.3: Protokolldatei-Einstellungen des Webservers

Das könnte etwa so aussehen:

Protokolldatei-Einstellungen	
Zugriffsprotokollformat:	<input type="checkbox"/> Erweitert allgemein ▾
Zeitformat:	<input type="checkbox"/> Ortszeit ▾
Protokolldatei löschen:	<input type="checkbox"/> Wöchentlich ▾
Maximale Länge eines Protokolleintrags:	<input type="checkbox"/> 10 ▾ KB
Maximale Größe des Zugriffsprotokolls:	<input type="checkbox"/> 0 ▾ MB

Abbildung 14.19: Serverdokument, Reg. Internetprotokolle... > HTTP – Protokolldatei-Einstellungen

14.6. Einen sicheren Webserver aufbauen

Um vom Webbrowser eine sichere Verbindung zu Ihrem Domino-Server aufbauen zu können, müssen Sie vom Internetprotokoll HTTP auf **HTTPS** (Hypertext Transfer Protocol Secure) umstellen. HTTPS bietet eine Sitzungsverschlüsselung zur abhörsicheren Datenübertragung. Ohne diese Verschlüsselung würden die Daten im Klartext über das Internet (oder auch Intranet) übertragen werden.

Die Verschlüsselung der Daten erfolgt mittels SSL/TLS. Unter Verwendung des SSL-Handshake-Protokolls findet zunächst eine geschützte Identifikation und Authentifizierung der Kommunikationspartner statt. Anschließend wird ein gemeinsamer symmetrischer Sitzungsschlüssel ausgetauscht. Dieser wird dann zur Verschlüsselung der übertragenen Daten verwendet. Der Standardport für HTTPS-Verbindungen ist 443.

Um HTTPS aktivieren zu können, brauchen Sie ein **Zertifikat** von einer **Zertifizierungsstelle** (Certificate Authority – CA). Dabei kann Ihre eigene Organisation als Zertifizierungsstelle auftreten oder ein kommerzieller Anbieter. Wenn Sie Ihre Zertifikate selbst zertifizieren, kostet Sie das zwar nichts, es vertraut Ihnen aber auch niemand. Das ist in den meisten Fällen kein Problem, solange Sie die Zertifikate ausschließlich für Ihre eigenen Mitarbeiter verwenden. (Achtung: Manche Clients unterstützen vielleicht in Zukunft keine selbstsignierten Zertifikate.)

Der Webserver: Einen sicheren Webserver aufbauen

Neben den Serverzertifikaten können nach X.509.3 auch signierte Client-Zertifikate erstellt werden. Das ermöglicht eine Authentifizierung der Clients gegenüber dem Server nur über das Zertifikat (ohne Angabe von Namen und Kennwort), wird jedoch selten eingesetzt.

14.6.1. Transport Layer Security (TLS)

Transport Layer Security (TLS, englisch für »Transportschichtsicherheit«) ist immer noch besser bekannt unter der alten Bezeichnung **Secure Sockets Layer** (SSL). HTTPS und damit SSL 1.0 wurde von Netscape entwickelt und 1994 mit dem eigenen Browser veröffentlicht. Die letzte Version, SSL 3.0 (auch als SSLv3 bezeichnet), wurde 1996 veröffentlicht und wies eine Sicherheitslücke auf, die als POODLE-Attacke (Padding Oracle On Downgraded Legacy Encryption) bekannt ist. Es handelt sich dabei um eine sogen. MITM-Attacke (für »Man-in-the-middle«), von der alle Webbrowser betroffen sind. Danach wurde das Protokoll unter dem Namen TLS weiterentwickelt und standardisiert. TLS 1.0 (entspricht SSL 3.1) stammt aus dem Jahr 1999, TLS 1.2 aus dem Jahr 2008. Die Unterstützung der aktuellen Version 1.3 wird für Domino 12.0.1 erwartet. (Erscheint noch 2021.)

Die wichtigen Browser (Firefox, Chrome, Edge und Safari) unterstützen die in die Jahre gekommenen Protokolle TLS 1.0 und 1.1 seit März 2020 nicht mehr, weshalb sie auf dem Domino-Server deaktiviert werden sollten.

Der Domino-Webserver unterstützt TLS 1.2:

- > für Inbound und Outbound
- > für alle IP-Protokolle (HTTP, SMTP, LDAP, POP3, IMAP & DIIOP)
- > für alle Plattformen inklusive IBM iSeries mit System_SSL
- > für SSL/TLS Session Resumption
- > Inklusive Client-Zertifikat-basierter Authentifizierung
- > Support für TLS_FALLBACK_SCSV (Signaling Cipher Suite Value), um Webbrowser, die ein Fallback unterstützen, vor Downgrade-Attacken zu schützen

Wenn die Gegenseite kein TLS 1.2 unterstützt, kann via »Negotiation« auf SSLv3 zurückgeschaltet werden, wobei eine Protokoll-Negotiation nicht gleichzusetzen ist mit einem Protokoll-Fallback.

14.6.2. Die eigene Webseite überprüfen

Testen Sie die Sicherheit Ihres Webserver bei Qualys SSL Labs:

<https://www.ssllabs.com/ssltest/>

Achtung: Wenn Sie nicht wollen, dass Ihr Testergebnis auf der Webseite von Qualys SSL Labs auftaucht, setzen Sie ein Häkchen bei: »Do not show the results on the boards«.

Hier ein Beispiel für einen unsicheren Webserver (Domino 9.0.1 ohne Fix Pack mit selbstzertifizierendem Zertifikat) mit der schlechten Note F:

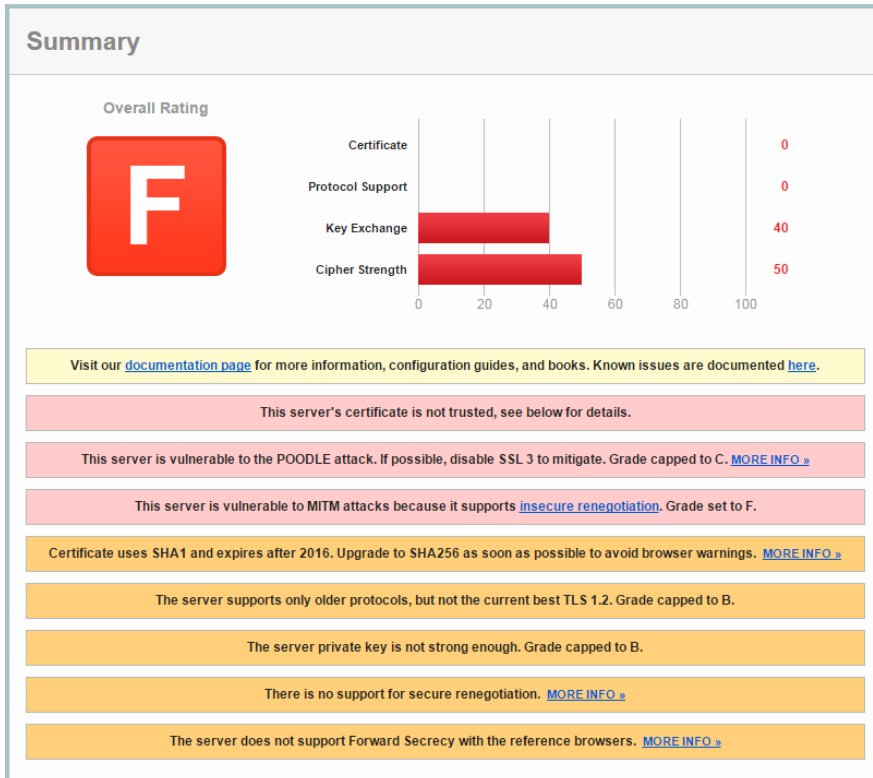


Abbildung 14.20: Testergebnis von Qualys SSL Labs mit der Note F (Erklärung im Text)

Warum wird der Server so schlecht eingestuft? Ganz einfach, weil:

- > dem Serverzertifikat nicht vertraut wird
- > der Server durch Verwendung von SSL für POODLE-Attacken verwundbar ist
- > der Server für MITM-Attacken verwundbar ist
- > die alte kryptografische Bibliothek SHA-1 zur Verschlüsselung verwendet wird
- > der Server nur alte Protokolle (alles vor TLS 1.2) unterstützt
- > das private Schlüssel des Servers eine schwache Verschlüsselung verwendet (weniger als 256 Bit)
- > keine Forward Secrecy verwendet wird (siehe auch Kap. 14.6.2.1 Kleiner Einschub: Was sind Ciphers?, ab Seite 390)

Nachfolgend zum Vergleich ein vertrauenswürdiges (=käuflich erworbenes Zertifikat) und Domino 9.0.1 mit FP2, welches TLS 1.0-Unterstützung bringt. Damit kann man bestenfalls Note B erreichen, weil:

- > TLS 1.2 nicht unterstützt wird
- > als unsicher eingestufte RC4-Ciphers verwendet werden (siehe auch Kap. 14.6.2.1 Kleiner Einschub: Was sind Ciphers?, ab Seite 390)

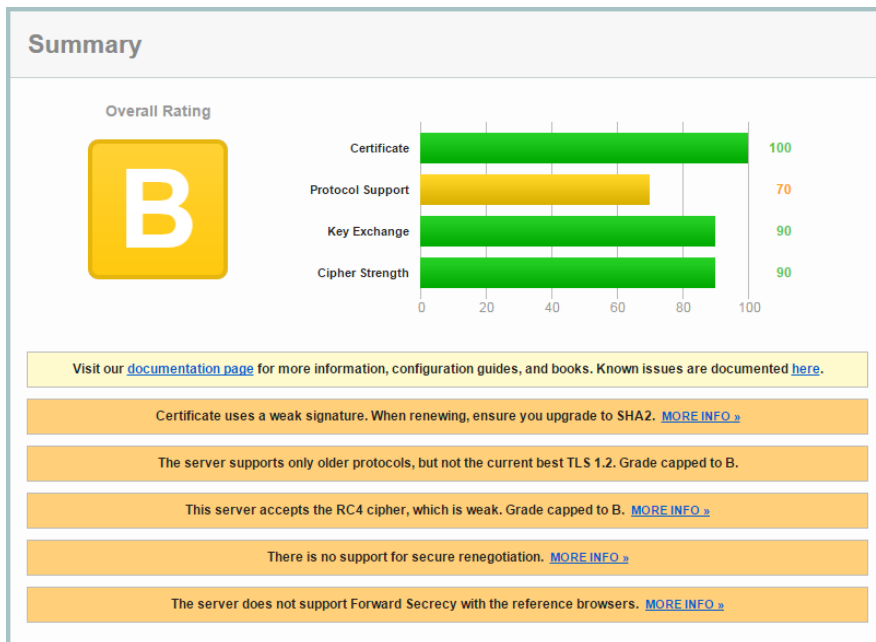


Abbildung 14.21: Testergebnis von Qualys SSL Labs mit der Note B (Erklärung im Text)

14.6.2.1. Kleiner Einschub: Was sind Ciphers?

Ciphers (oder Cipher Suites) könnte man als Verschlüsselungscodes übersetzen. Als Teil des TLS-Protokolls legen Sie fest, welche Algorithmen zum Verschlüsseln einer gesicherten Datenverbindung zur Anwendung kommen. Als besonders sicher gelten Ciphers, die **Forward Secrecy** (auf Deutsch oft als »Folgenlosigkeit« bezeichnet) unterstützen. Forward Secrecy bedeutet, dass der zwischen den Kommunikationspartnern ausgetauschte Schlüssel nach der Beendigung der Sitzung nicht rekonstruiert werden kann. Da ständig neue Schwachstellen entdeckt werden, gilt eine bestimmte Cipher oftmals von einem Tag auf den anderen als unsicher. Aber kein Grund zur Sorge: Auf dem Domino-Server kann die Verwendung jeder einzelnen Cipher ein- oder ausgeschaltet werden!

14.6.2.2. Schwache Verschlüsselungscodes (Ciphers) deaktivieren

Die gute Nachricht: Bei einer Neuinstallation von Domino 10 oder 11 gelten die Ciphers als ausreichend sicher konfiguriert. Die schlechte Nachricht: Wenn Sie eine ältere Domino-Version aktualisiert haben, werden als schwach geltende Ciphers übernommen. (Immerhin wird beim Starten des HTTP-Servers auf der Serverkonsole eine Warnung angezeigt – was die meisten wohl übersehen.) In jedem Fall sollten Sie die aktiven Ciphers einmal überprüfen:

1. Öffnen Sie das Domino-Verzeichnis
2. Wenn Sie mehrere Webseiten betreiben (im Serverdokument also die Einstellung **Internet-Konfigurationen aus Server-Internet-Site-Dokumenten laden** gesetzt haben), navigieren Sie zur Ansicht **Web > Internet-Sites** und öffnen das Dokument der betroffenen Internet-Site. Wechseln Sie dort zum Register Sicherheit in den Abschnitt **SSL-Sicherheit**.

Wenn es nicht der Fall ist, bleiben Sie im Serverdokument und navigieren Sie zum Register **Ports... > Internet-Ports...** und dort in den Abschnitt **SSL-Einstellungen**.

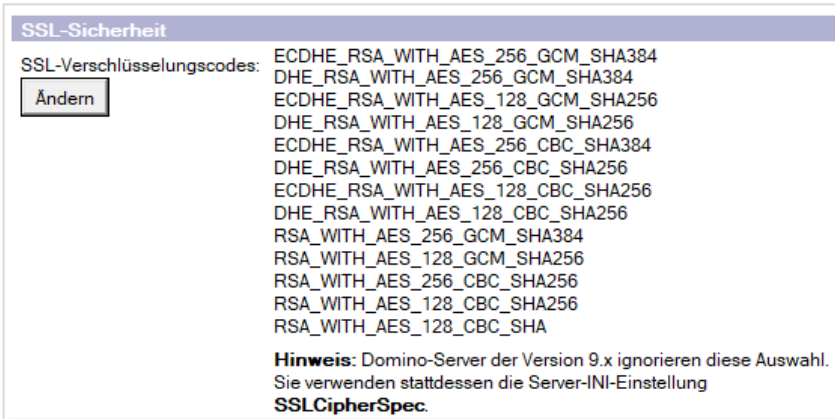


Abbildung 14.22: SSL-Verschlüsselungscodes

3. Schalten Sie in den Bearbeitungsmodus um und klicken Sie auf die Schaltfläche **Ändern**.
4. Ein Dialog mit allen SSL-Verschlüsselungscodes (Ciphers) wird angezeigt:

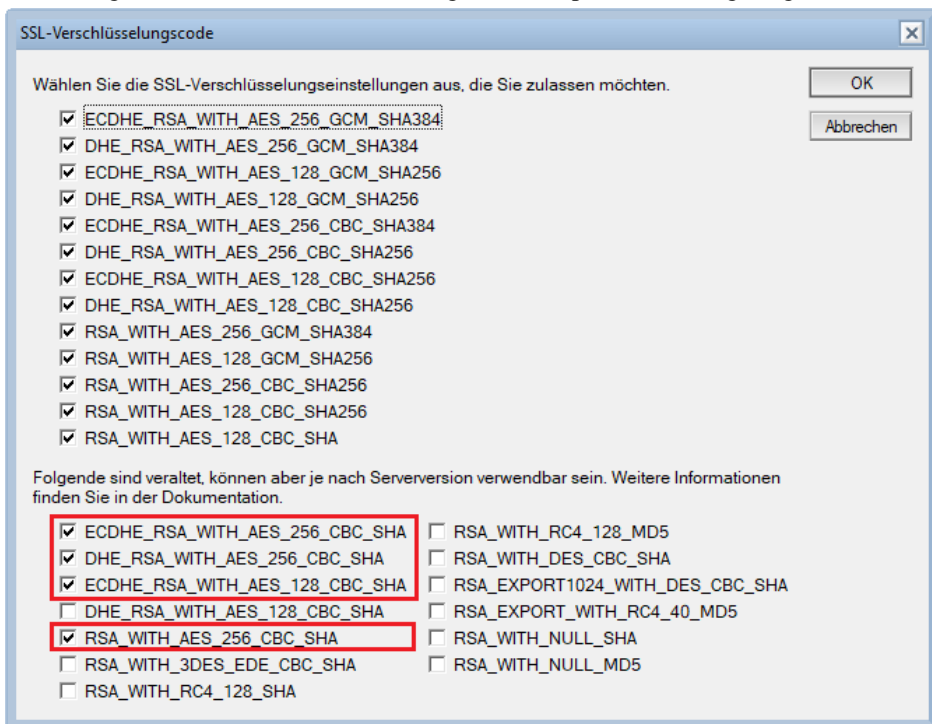


Abbildung 14.23: Dialog SSL-Verschlüsselungscodes bearbeiten

5. Wählen Sie alle veralteten Verschlüsselungscodes im unteren Bereich ab und klicken Sie auf **OK**.

Die umrahmt dargestellten, veralteten Ciphers müssen bei Ihnen nicht aktiviert sein – es kommt darauf an, was zuvor aktiviert war.

6. Speichern und schließen Sie das Serverdokument bzw. das Internet-Site-Dokument.
7. Geben Sie auf der Serverkonsole den folgenden Befehl ein:

```
tell http refresh
```

Der Webserver: Einen sicheren Webserver aufbauen

Sollten Sie aus irgendeinem Grund doch einmal eine schwache Cipher aktivieren müssen, vergessen Sie nicht, in der notes.ini auch den Eintrag USE_WEAK_SSL_CIPHERS=1 vorzunehmen.

Danach sollte beim Test von Qualys SSL Labs erstmals die Note A möglich sein:

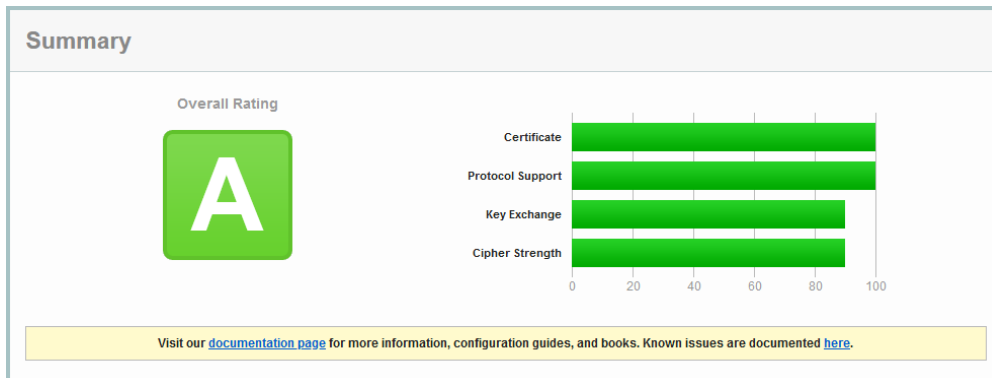


Abbildung 14.24: Testergebnis von Qualys SSL Labs mit der Note A (Erklärung im Text)

14.6.2.3. Schwache Verschlüsselungscodes (Ciphers) ausschließen

Sehen wir uns das Testergebnis im Detail an, stellen wir im Abschnitt Cipher Suites fest, dass bis auf die ersten vier Einträge in der Liste (die Codes sind nach ihrer Stärke absteigend sortiert), alle als schwach gelten. Es bietet sich also an, alle bis auf die ersten vier zu deaktivieren:

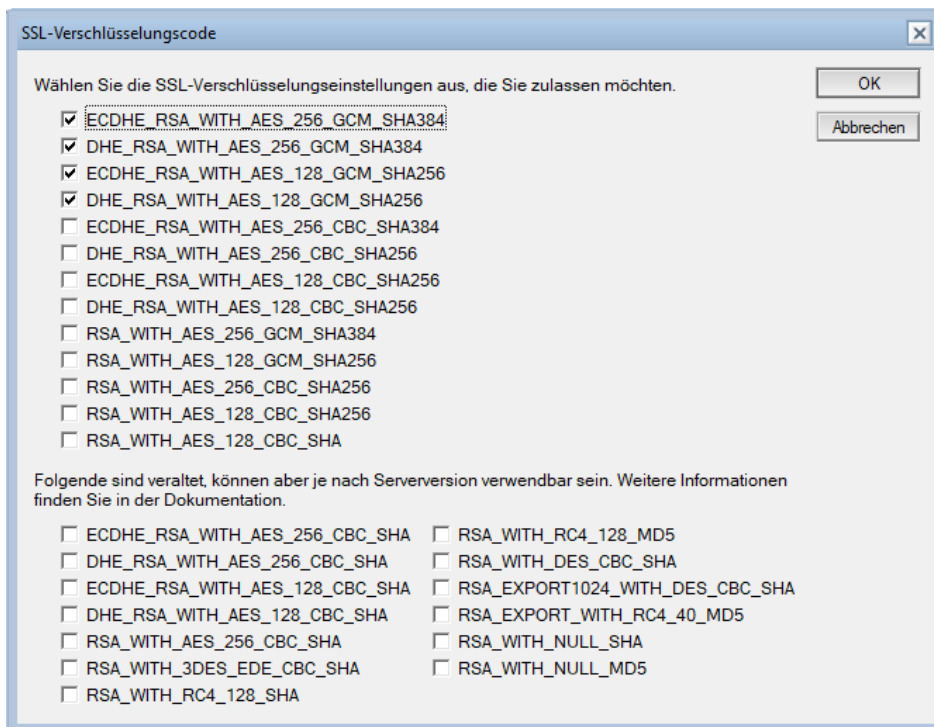


Abbildung 14.25: Dialog SSL-Verschlüsselungscodes bearbeiten

Achtung: Moderne Browser sowie der Verse-Client auf Ihrem Mobiltelefon sollten danach normal weiterfunktionieren. Bedenken Sie jedoch, dass Sie damit womöglich ältere Clients, die in Ihrem Unternehmen noch in Verwendung sind, ausschließen!

14.6.3. Was Sie nach einem Upgrade überprüfen sollten

Wie schon erwähnt, gilt bereits Domino 10 als ausreichend sicher konfiguriert, wenn es auf einer nackten Maschine neu installiert wurde. Haben Sie jedoch eine ältere Domino-Version mit Domino 10 oder 11 aktualisiert, sollten Sie danach ein paar Dinge überprüfen:

- > Stellen Sie sicher, dass SSL 3.0 deaktiviert ist und deaktivieren Sie es gegebenenfalls.
Dies erfolgt durch Hinzufügen der folgenden Zeile zur Datei notes.ini:
DISABLE_SSLV3=1
- > Stellen Sie sicher, dass TLS 1.0 deaktiviert ist und deaktivieren Sie es gegebenenfalls.
Dies erfolgt durch Hinzufügen der folgenden Zeile zur Datei notes.ini:
SSL_DISABLE_TLS_10=1

14.6.4. HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) ist ein Sicherheitsmechanismus für HTTPS-Verbindungen, der sowohl vor der Aushebelung der Verbindungsverschlüsselung durch eine Downgrade-Attacke als auch vor Session-Hijacking schützen soll. Mit HSTS kann ein Server dem Browser des Anwenders mitteilen, für eine definierte Zeit (max-age) ausschließlich verschlüsselte Verbindungen für diese Domain zu nutzen. Dieses Verhalten kann auf dem Domino-Server durch Hinzufügen der folgenden Zeile zur Datei notes.ini aktiviert werden:

```
HTTP_HSTS_MAX_AGE=31536000
```

Für die Aktivierung von HSTS werden Sie von Qualys SSL Labs mit der Note A+ belohnt:

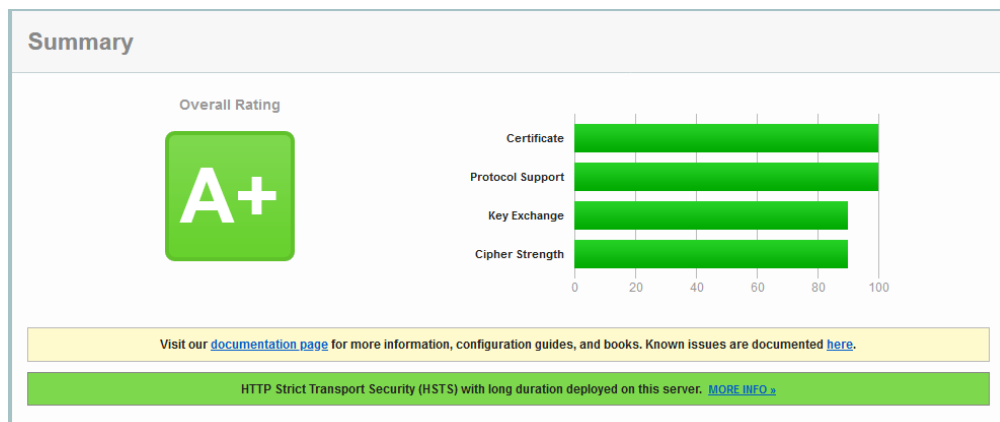


Abbildung 14.26: Testergebnis von Qualys SSL Labs mit der Note A+ (Erklärung im Text)

Das Speichern von HSTS-Informationen durch den Client lässt sich auch für ein Tracking von Benutzern ausnutzen. Besonders kritisch wurde diskutiert, dass Google Chrome die HSTS-Informationen in den für den Datenschutz ausgelegten Inkognito-Modus übernimmt. Trotz dieses Datenschutzrisikos wird durch HSTS die Kommunikation auf der Browserseite sicherer, da Daten

nicht unverschlüsselt übertragen werden. Auch kann eine zwingend erforderliche SSL/TLS-Verbindung helfen, einen MITM-Angriff leichter zu erkennen – wenn es diesen auch nicht ausschließen kann. Ob Sie HSTS einsetzen, bleibt Ihre Entscheidung.

14.6.5. Server Name Indication – SNI

Vor Domino 11.0.1 war für jedes Zertifikat eine eigene IP-Adresse nötig, ab Version 11.0.1 können sich mehrere Zertifikate eine IP-Adresse teilen. Diese Fähigkeit nennt man Server Name Indication (SNI) .

Ohne SNI fordert der Client, der die TLS-Verbindung aufbaut, vom Server sofort ein digitales Zertifikat an. Mit SNI übermittelt der Client dem Server zuerst den gewünschten Host, erst dann wird ein verschlüsselter Kanal aufgebaut. SNI ist eine Erweiterung von TLS, die es dem Client erlaubt, gewisse Information (in diesem Fall den Hostnamen) unverschlüsselt zu übertragen. Dies ermöglicht den Einsatz sogenannter Wildcard-Zertifikate wie z. B. *.cob.at.

Die Unterstützung von SNI steht nicht automatisch zur Verfügung, Sie müssen dazu zuerst die notes.ini-Variable ENABLE_SNI=1 setzen und den HTTP-Task durchstarten.

14.7. TLS-Zertifikate erstellen

14.7.1. Die einzelnen Komponenten

Zertifikate werden unter Domino in einer proprietären **Schlüsselringdatei** mit der Endung *.kyr (für »Keyring«) aufbewahrt. Um beim Erstellen von Zertifikaten die volle SHA-2-Unterstützung zu erhalten, müssen zwei Werkzeuge verwendet werden:

- > OpenSSL
- > KYRTool

OpenSSL wird benötigt:

1. zum Erstellen des privaten Serverschlüssels
2. zum Erstellen der **Zertifikatsanforderung** (Certificate Signing Request – CSR) an die **Zertifizierungsstelle** (Certificate Authority – CA)
3. (optional) zum Konvertieren von Zertifikaten in andere Formate
4. (optional) zum Überprüfen der Schlüssel und Zertifikate

OpenSSL Light für Windows kann unter der folgenden URL heruntergeladen werden:

<https://slproweb.com/products/Win32OpenSSL.html>

OpenSSL kann sowohl auf dem Server als auch auf dem Client installiert werden, je nachdem, wo Sie die Zertifikate erstellen. Laden Sie für den Server die 64-Bit-, für den Client die 32-Bit-Version herunter.

KYRTool wird benötigt:

1. (optional) zum Verifizieren der Eingabedateien
2. zum Erstellen einer neuen Domino-Schlüsselringdatei
3. zum Importieren des privaten Schlüssels, der von der Zertifizierungsstelle signierten Zertifikatsanforderung und der Zertifikatskette in den Schlüsselring
4. (optional) zum Verifizieren des Schlüsselrings

Das Programm kyrtool.exe benötigt zum Ausführen die Datei nnotens.dll, die 64-Bit-Version jene des Domino-Servers und die 32-Bit-Version jene des Domino-Administrators. Die 64-Bit-Version von kyrtool.exe wird bei der Server-Installation automatisch mitinstalliert, die 32-Bit-Version können Sie vom HCL-Support herunterladen:

https://support.hcltech.com/csm?id=kb_article&sysparm_article=KB0073172

14.7.2. Ein Zertifikat bei einer offiziellen CA anfordern

14.7.2.1. Einen privaten Serverschlüssel erstellen

Erstellen Sie einen Ordner zum Speichern der Zertifikate, z. B. D:\certs.

Wechseln Sie dann in den Ordner C:\OpenSSL\bin und führen Sie den Befehl zum Generieren eines privaten 4096-Bit-Schlüssels aus:

```
openssl genrsa -out D:\certs\server.key 4096
```

14.7.2.2. Eine Zertifikatsanforderung (CSR) erstellen

Um einen CSR zu erstellen, geben Sie den folgenden Befehl ein:

```
openssl req -new -sha256 -key D:\certs\server.key -out D:\certs\server.csr
```

Daraufhin werden Sie aufgefordert, Ihre Daten einzugeben:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

(Optional) Geben Sie zuerst den zweistelligen Code Ihres Landes an, z. B. AT oder DE:

```
Country Name (2 letter code) [AU]:AT
```

(Optional) Geben Sie Ihr Bundesland an:

```
State or Province Name (full name) [Some-State]:Vienna
```

(Optional) Geben Sie Ihren Ort an:

```
Locality Name (eg, city) []:Vienna
```

Der Webserver: TLS-Zertifikate erstellen

Geben Sie den Namen Ihres Unternehmens an. Damit die CA Ihre Identität überprüfen kann, sollte der Name so eingegeben werden, wie er im Handels- (oder sonstigem) Register steht:

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:COB Consulting
```

(Optional) Geben Sie eine Organisationseinheit, etwa eine Abteilung ein:

```
Organizational Unit Name (eg, section) []:IT
```

Geben Sie den Namen des Webservers ein, für den das Zertifikat ausgestellt werden soll, z. B. www.cob.at. Wenn Sie ein Wildcard-Zertifikat – also ein Zertifikat für Ihre ganze Domäne – beantragen, geben Sie anstelle des Hostnamens einen Stern (*) ein, z. B. *.cob.at:

```
Common Name (e.g. server FQDN or YOUR name) []:www.cob.at
```

(Optional) Geben Sie eine E-Mail-Adresse an:

```
Email Address []:office@cob.at
```

Extra Attribute sind immer optional:

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Senden Sie die Zertifikatsanforderung (CSR) server.csr anschließend an die Zertifizierungsstelle (CA). Das erfolgt häufig durch Einfügen des Inhalts der CSR-Datei in ein Feld auf der Webseite Ihres Anbieters.

Die Zertifizierungsstelle prüft Ihre Identität und sendet Ihnen das von ihr signierte Serverzertifikat certificate.crt zurück. Sollte die Endung nicht *.crt lauten, lassen Sie sich nicht beirren, auch *.pem, *.cer oder *.key sind völlig in Ordnung. Öffnen Sie im Zweifelsfall die erhaltene Datei in einem Editor; das Zertifikat sollte mit der Zeile:

```
-----BEGIN CERTIFICATE-----
```

... beginnen und mit der Zeile:

```
-----END CERTIFICATE-----
```

... enden.

14.7.2.3. (Optional) Binäre Dateiformate konvertieren

Nicht direkt verwenden können Sie binäre Formate wie *.der, *.p7b oder *.p12. Sollte Ihre Zertifizierungsstelle nichts anderes anbieten, können Sie diese Formate jedoch mit OpenSSL in eine lesbare Form umwandeln. Um etwa ein Zertifikat im Format *.p7b ins Format *.crt zu konvertieren, führen Sie den folgenden Befehl aus:

```
openssl pkcs7 -print_certs -in cert.p7b -out cert.crt
```

Ein Spezialfall sind Dateien mit der Endung *.pfx: Sie enthalten bereits die ganze Zertifikatskette, also nicht nur den privaten Schlüssel und das signierte Serverzertifikat, sondern auch alle Zwischen- und Stammzertifikate. (Dieses Format wird vor allem bei Wildcard-Zertifikaten gerne verwendet.)

Um eine PFX-Datei verwenden zu können, müssen Sie diese zuerst in eine für das KYRTool lesbare Form umwandeln. Verwenden Sie dazu den Befehl:

```
openssl pkcs12 -in certs.pfx -out certs.crt -nodes -chain
```

(Sie werden gegebenenfalls dazu aufgefordert, ein Kennwort einzugeben.)

Nach dem Konvertieren können Sie gerne den Inhalt überprüfen: Wenn die Datei 1.) den privaten Schlüssel, 2.) das signierte Serverzertifikat, 3.) ein Zwischenzertifikat und 4.) ein Stammzertifikat enthält, müssen Sie die folgenden Abschnitte vorfinden:

1.)

```
-----BEGIN RSA PRIVATE KEY-----
```

```
...
```

```
-----END RSA PRIVATE KEY-----
```

(Die Zeichenfolge »RSA« kann auch fehlen.)

2.)

```
-----BEGIN CERTIFICATE-----
```

```
...
```

```
-----END CERTIFICATE
```

3.)

```
-----BEGIN CERTIFICATE-----
```

```
...
```

```
-----END CERTIFICATE-----
```

4.)

```
-----BEGIN CERTIFICATE-----
```

```
...
```

```
-----END CERTIFICATE-----
```

Statt der drei Punkte innerhalb der einzelnen Abschnitte sehen Sie natürlich einen längeren Buchstabensalat ...

Sollte zwischen den einzelnen Abschnitten noch zusätzlicher Text stehen (z. B. sogenannte »Bag Attributes«), löschen Sie ihn heraus.

14.7.2.4. (Optional) Zertifikate überprüfen

Was tun Sie, wenn Sie die Art des Zertifikats (Server-, Zwischen- oder Stammzertifikat) am Dateinamen nicht erkennen können? – Sie schauen hinein! Aber nicht, indem Sie die Datei im Editor öffnen – hier sehen Sie immer nur Buchstabensalat –, sondern durch Eingabe des Befehls:

```
openssl x509 -in certificate.crt -text -noout
```

Das Serverzertifikat erkennen Sie am Servernamen in der Zeile Subject.

Stammzertifikate sind immer selbstsignierend, bei ihnen steht im Feld Subject dasselbe wie im Feld Issuer (Aussteller).

Bei Zwischenzertifikaten steht im Feld Subject ein anderer Name als im Feld Issuer. Der Name in Subject sollte dem Namen im Feld Issuer im Serverzertifikat entsprechen und der Name in Issuer sollte identisch sein mit dem Namen im Feld Subject des Stammzertifikats.

Haben Sie alle Komponenten eindeutig identifiziert, müssen Sie entscheiden, ob Sie vor dem Import in den Schlüsselring den privaten Schlüssel und die Zertifikate zu einer Datei zusammenfassen (weniger Aufwand) oder die einzelnen Dateien nacheinander importieren. (Außer Sie haben gerade eine PFX-Datei konvertiert, dann sind der private Schlüssel und alle Zertifikate ja bereits zu einer Datei zusammengefasst.)

14.7.2.5. (Optional) Schlüssel und Zertifikate zusammenfassen

Zum Zusammenfassen des privaten Schlüssels und aller Zertifikate zu einer Datei öffnen Sie eine Windows-Eingabeaufforderung und wechseln in das von Ihnen erstellte Verzeichnis, z. B.: D:\certs. Setzen Sie dort den folgenden Befehl ab:

```
type server.key certificate.crt intermediate.crt root.crt >server.txt
```

Achtung: Die Reihenfolge in der Zertifikatskette muss unbedingt eingehalten werden: 1. privater Schlüssel, 2. signiertes Serverzertifikat, 3. Zwischenzertifikat (Intermediate-Zertifikat) und 4. Stammzertifikat (Root-Zertifikat).

14.7.2.6. Die Schlüsselringdatei erstellen

Je nachdem, ob Sie die 32- oder 64-Bit-Version verwenden, starten Sie kyrtool.exe aus dem Client- oder aus dem Server-Programmverzeichnis. Öffnen Sie eine Eingabeaufforderung und navigieren Sie in das richtige Verzeichnis. Setzen Sie dort den folgenden Befehl ab:

```
kyrtool create -k D:\certs\server.kyr -p <Passwort>
```

(Verwenden Sie anstelle von <Passwort> Ihr eigenes Kennwort.)

KYRTool generiert zwei Dateien, die eigentliche Schlüsselringdatei server.kyr und die Datei server.sth, die das von Ihnen angegebene Kennwort in versteckter (»stashed«) Form enthält. Das Kennwort benötigen Sie, um die Schlüsselringdatei zu entsperren und Änderungen vorzunehmen (was eher selten vorkommt).

14.7.2.7. Importieren von Schlüssel und Zertifikaten in den Schlüsselring

Hier gibt es zwei Vorgangsweisen: A) Sie haben zuvor alle Textdateien zu einer einzigen zusammengeführt und importieren diese nun mit einem Befehl in den Schlüsselring, oder B) Sie importieren die Dateien nacheinander. Welche Vorgangsweise Sie wählen, hängt unter anderem davon ab, in welchem Format Sie Schlüssel und Zertifikate erhalten haben. Der Import einer einzigen Textdatei ist mit weniger Aufwand verbunden.

A) Import einer Datei in den Schlüsselring

Bevor Sie die Datei importieren, sollten Sie nochmals überprüfen, ob die Zertifikatskette passt und nichts fehlt:

```
kyrtool verify D:\certs\server.txt
```

Die Antwort sollte so aussehen:

```
Successfully read 4096 bit RSA private key
INFO: Successfully read 3 certificates
INFO: Private key matches leaf certificate
INFO: IssuerName of cert 0 matches the SubjectName of cert 1
INFO: IssuerName of cert 1 matches the SubjectName of cert 2
INFO: Final certificate in chain is self-signed
```

Sollte die Reihenfolge nicht passen, etwa weil Sie Stamm- und Zwischenzertifikat vertauscht haben, erhalten Sie folgende Fehlermeldungen:

```
Successfully read 4096 bit RSA private key
INFO: Successfully read 3 certificates
INFO: Private key matches leaf certificate
ERROR: IssuerName of cert 0 does NOT match the SubjectName of cert 1
ERROR: IssuerName of cert 1 does NOT match the SubjectName of cert 2
WARNING: Final certificate in chain is not self-signed
```

Haben Sie alle Dateien zu einer zusammengeführt (oder eine PFX-Datei konvertiert), können Sie diese nun mit einem einzigen Befehl in den Schlüsselring importieren:

```
kyrtool import all -k D:\certs\server.kyr -i D:\certs\server.txt
```

Stammzertifikate (Root Certificates) müssen als vertrauenswürdige Zertifikate im Domino-Verzeichnis gespeichert sein. Ob das der Fall ist, können Sie in der Ansicht **Sicherheit > Zertifikate > Internetzertifizierer** überprüfen. Sollte das Stammzertifikat Ihres Anbieters dort fehlen, kann es über **Aktionen > Internetzertifikate importieren** auch nachträglich hinzugefügt werden. Zwischenzertifikate (Intermediate Certificates) müssen nicht im Domino-Verzeichnis gespeichert sein. Sie vermitteln zwischen dem Stammzertifikat der verwendeten CA und dem Serverzertifikat.

B) Import mehrerer Dateien in den Schlüsselring

Liegen die Dateien einzeln vor, gehen Sie wie folgt vor:

1. Schritt: Import des privaten Schlüssels:

```
kyrtool import keys -k D:\certs\server.kyr -I D:\certs\server.key
```

2. Schritt: Import des signierten Serverzertifikats:

```
kyrtool import certs -k D:\certs\server.kyr -I D:\certs\certificate.crt
```

3. Schritt: Import des Zwischenzertifikats:

```
kyrtool import roots -k D:\certs\server.kyr -i D:\certs\intermediate.crt
```

4. Schritt: Import des Stammzertifikats:

```
kyrtool import roots -k D:\certs\server.kyr -i D:\certs\root.crt
```

14.7.3. Das TLS-Zertifikat einspielen und aktivieren

Kopieren Sie die beiden Dateien server.kyr und server.sth ins Domino-Datenverzeichnis.

Überprüfen Sie, ob der SSL-Portstatus im Serverdokument, Register **Ports...** > **Internet-Ports...** > **Web** aktiviert ist und aktivieren Sie ihn gegebenenfalls:

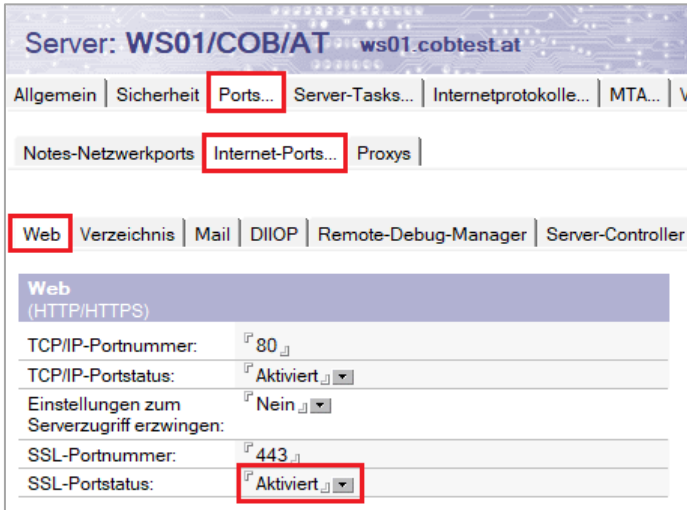


Abbildung 14.27: Serverdokument, SSL-Portstatus aktivieren

Bleiben Sie je nach Konfiguration entweder im Serverdokument oder öffnen Sie das Website-Dokument und hinterlegen Sie im Register **Sicherheit** den Namen der Schlüsselringdatei (z. B. »server.kyr«):

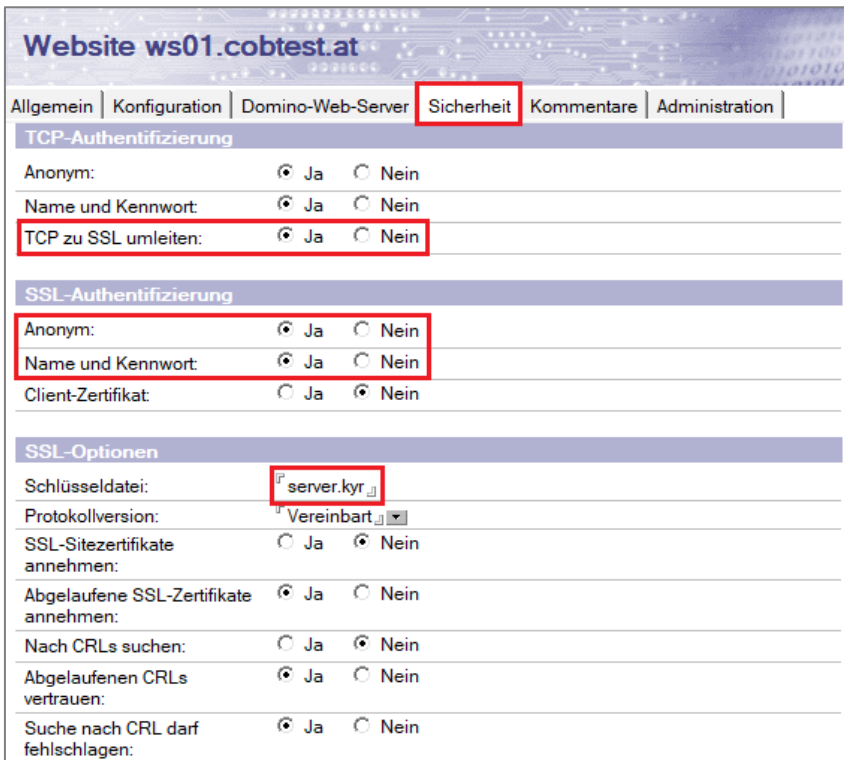


Abbildung 14.28: Website-Dokument, Register Sicherheit

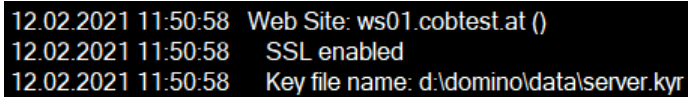
Aktivieren Sie im Bereich **SSL-Authentifizierung** das Feld **Anonym**. Soll auch eine Anmeldung erlaubt sein (z. B. für Webmail), aktivieren Sie auch **Name und Kennwort**. Alternativ können Sie auch die Umleitung von TCP zu SSL erzwingen.

Starten Sie nach dem Speichern des Dokuments den Webserver neu:

```
restart task http
```

Nach dem Neustart können Sie überprüfen, ob der Webserver das Zertifikat geladen hat:

```
tell http show security
```



```
12.02.2021 11:50:58 Web Site: ws01.cobtest.at ()
12.02.2021 11:50:58 SSL enabled
12.02.2021 11:50:58 Key file name: d:\domino\data\server.kyr
```

Abbildung 14.29: Ausgabe des Befehls `tell http show security`

Wenn dem Domino-Server ein Reverse Proxy (z. B. HCL SafeLinX) vorgeschaltet ist, müssen Sie auch dort ein Zertifikat einspielen. Wie das zu geschehen hat und in welchem Format, entnehmen Sie bitte der Dokumentation des Herstellers. Der Reverse-Proxy kann auch so konfiguriert werden, dass er nach außen via SSL/TLS kommuniziert, nach innen aber ohne Verschlüsselung. In diesem Fall können Sie auf dem Domino-Server gegebenenfalls auch ganz auf ein Zertifikat verzichten.

14.7.4. TLS-Zertifikate mit Let's Encrypt erstellen

14.7.4.1. Vorstellung der Zertifizierungsstelle Let's Encrypt

Zertifikate kosten je nach Anbieter von rund zwanzig bis hin zu einigen hundert Euro für Wildcard-Zertifikate und werden meist nur für ein Jahr ausgestellt. Danach müssen die Zertifikate verlängert, also neu ausgestellt und neu bezahlt werden. Dafür existiert kein Automatismus, Zertifikate müssen händisch beantragt, verlängert und eingespielt werden. Einige Anbieter haben zwar Schnittstellen oder APIs entwickelt, die aber bei jedem anders funktionieren und meist auch extra zu bezahlen sind. Daher hat sich 2014 eine Gruppe von Unternehmen und Instituten mit dem Ziel zusammengefunden, verschlüsselte Verbindungen im Web zu normieren. Primäres Ziel dabei ist es, den Aufwand für die Einrichtung und Pflege von TLS-Zertifikaten deutlich zu senken. Let's Encrypt war geboren, mit folgenden Eigenschaften:

- > ist kostenfrei nutzbar
- > automatisierte Zertifikatsausstellung und -verlängerung
- > ist sicher – erfüllt alle Anforderungen an eine sichere CA
- > ist transparent – Stichwort Sperren von Zertifikaten
- > ist offen – der Prozess zur Zertifikatsgenerierung und -bereitstellung basiert auf einem offenen Standard
- > ist kooperativ – offene Stiftung
- > ist ideal für das aktuelle Cloud- & Micro-Service-Zeitalter

14.7.4.2. Wie funktioniert Let's Encrypt?

Let's Encrypt verwendet zur Validierung und auch späteren Zertifikatsausstellung und Bereitstellung das offene ACME-Protokoll (für Automatic Certificate Management Environment).

ACME macht es möglich, alle Schritte zur Zertifikatsausstellung zu automatisieren, inkl. der Validierung. Hierfür wird auf dem Webserver ein ACME-kompatibler Management-Client eingesetzt. ACME sieht zwei Schritte vor:

1. Der Client muss der CA beweisen, dass er für die Domäne des Webserverns berechtigt ist, Zertifikate auszustellen. Das wird Domänenvalidierung (Domain Validation) genannt.
2. Dann erst kann er für diese Domäne Zertifikate anfordern, verlängern oder sperren.

Die einzige Beschränkung besteht darin, dass Zertifikate nach 90 Tagen ablaufen. Aber Sie können Sie so oft erneuern, wie Sie wollen.

Klassische CAs verlangen einen Handelsregisterauszug, schicken Mails an definierte Mailadressen, um die Domänenvalidierung durchzuführen. Let's Encrypt bietet dafür zwei Wege an:

- > HTTP-Challenge: Auf dem Webserver wird eine Datei an eine bestimmte Stelle gelegt.
- > DNS Challenge: Ein spezieller DNS-Eintrag wird unter example.com angelegt.

Let's Encrypt muss bei der HTTP-Challenge die gewünschte Datei aus dem Internet über Port 80 bzw. 443 abrufen können. Wird ein benutzerdefinierter Port verwendet oder das System ist nicht aus dem Internet erreichbar, kann die Methode HTTP-Challenge nicht verwendet werden. In diesem Fall hilft die DNS-Challenge.

14.7.4.3. Let's Encrypt 4 Domino (LE4D)

Was macht LE4D (wie Englisch »lead« ausgesprochen):

- > erstellt Benutzer- und Domänenschlüssel
- > erstellt und speichert Let's Encrypt Challenge auf dem Server
- > erstellt und sendet die Zertifikatsanforderung (CSR) an Let's Encrypt
- > lädt das Zertifikat herunter
- > lädt die Zertifikatskette herunter
- > erstellt den Schlüsselring mit dem KYRTool
- > importiert die Zertifikatskette in den Schlüsselring und erstellt ein Backup der erzeugten Dateien
- > startet den HTTP-Task neu
- > verlängert das Zertifikat, falls notwendig

LE4D kann hier kostenfrei angefordert werden:

<https://www.midpoints.de/de-solutions-LE4D>

Achtung: LE4D benötigt Java 8, welches erst ab Domino 9.0.1 FP8 verfügbar ist!

Das Installationspaket beinhaltet:

- > midpoints Let's Encrypt 4 Domino-Schablone (NTF-Datei)
- > Die Schablone beinhaltet das Notes-UI, eine XPage und einen Agenten
- > einen First-Step-Guide.
- > Bis auf das KYRTool (das mit Domino ausgeliefert und sich bereits im Server-Programmverzeichnis befinden sollte) werden keine weiteren Tools benötigt.

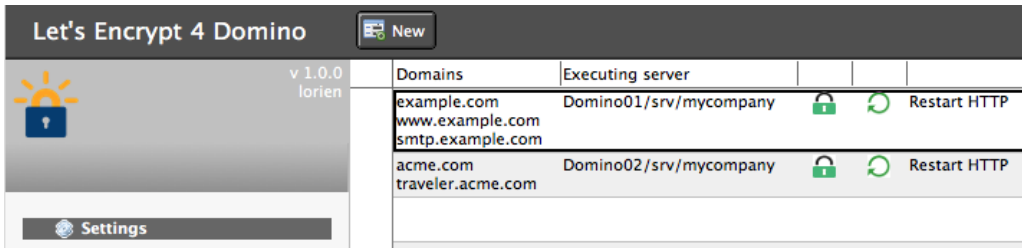


Abbildung 14.30: Let's Encrypt 4 Domino

14.7.4.4. LE4D – Erste Schritte

1. Signieren Sie zuerst die LE4D-Schablone
2. Erstellen Sie basierend auf der LE4D-Schablone eine neue Datenbank
3. Passen Sie bei Bedarf die ACL an
4. Öffnen Sie die LE4D-Datenbank und erstellen Sie neues Setting-Dokument.
5. Führen Sie den Agenten aus:

```
tell amgr run "midpoints/le4d.nsf" 'letsencrypt'
```

Weiterführende Informationen über Let's Encrypt finden Sie hier:

<https://letsencrypt.org/docs/>

14.7.5. Eigene Zertifikate erstellen

Warum überhaupt noch eigene Zertifikate erstellen, wenn Zertifikate mit LE4D gratis sind? Weil man auch firmenintern (im Intranet) abgesicherte Verbindungen benötigt, LE4D aber eine Verbindung nach außen, ins Internet aufbauen muss! Und wenn es nur darum geht, eine abgesicherte Verbindung für die eigenen Mitarbeiter zum eigenen Webserver zu etablieren, ist die Bestätigung durch einen vertrauenswürdigen Dritten auch nicht notwendig. Selbst erstellte Zertifikate sind nämlich nicht weniger sicher als die einer anerkannten Zulassungsstelle, die Clients vertrauen Ihnen nur nicht. Die meisten Clients kann man aber dazu überreden, auch den eigenen Zertifikaten zu vertrauen, etwa, indem man das Zertifikat in den Windows-Zertifikatsspeicher importiert. Daher kann der Einsatz von selbst kreierte Zertifikaten durchaus Sinn machen – und sei es nur als temporäre Lösung, bis das bei der CA bestellte Zertifikat eintrifft. Und da selbst erstellte Zertifikate auch noch beliebig lang gültig bleiben, ist so manche temporäre Lösung auch nach vielen Jahren noch im Einsatz ...

Dennoch würde ich nicht allzu sehr auf eigene Zertifikate setzen, denn die Regeln für Internetprotokolle werden immer strenger und bereits nach dem nächsten Update könnte ein wichtiger Client plötzlich nicht mehr funktionieren!

14.7.5.1. Vorbereitung

OpenSSL (light) muss zuvor installiert worden sein, in unserem Beispiel in C:\OpenSSL.

Der Notes-Client muss Version 9.0.1 FP4 oder höher sein. Das Tool kyrtool.exe muss sich im Programmverzeichnis des verwendeten Domino-Administrators befinden.

Erstellen Sie ein temporäres Verzeichnis für die generierten Dateien, in unserem Beispiel D:\certs.

Der Webserver: TLS-Zertifikate erstellen

Öffnen Sie eine Windows-Kommandozeile und wechseln Sie in C:\OpenSSL\bin.

Öffnen Sie ein zweite Kommandozeile und wechseln Sie in das Programmverzeichnis des Domino-Administrators, z. B. in C:\Program Files (x86)\HCL\Notes.

14.7.5.2. Generieren des Stammzertifikats (Root)

1. Schritt: Erstellen Sie das Stammzertifikats (Root) für Ihr Unternehmen. Dazu generieren Sie zuerst den privaten Schlüssel:

```
openssl genrsa -des3 -out D:\certs\root.key 4096
```

(Am Ende müssen Sie ein Kennwort eingeben.)

2. Schritt: Damit erstellen Sie ein zehn Jahre gültiges SHA-2-Zertifikat:

```
openssl req -new -sha256 -x509 -days 3650 -key D:\certs\root.key -out  
D:\certs\root.crt
```

Geben Sie zuerst das Kennwort ein und dann die von Ihnen gewünschten Informationen (zumindest den Namen des Unternehmens).

14.7.5.3. Generieren des Serverzertifikats

1. Schritt: Generieren Sie mit dem folgenden Befehl einen RSA-4096-Schlüssel und speichern Sie ihn als server.key:

```
openssl genrsa -out D:\certs\server.key 4096
```

2. Schritt: Generieren Sie eine Zertifikatsanforderung (CSR) und speichern Sie diese in der Datei server.csr:

```
openssl req -new -sha256 -key D:\certs\server.key -out D:\certs\server.csr
```

Sie werden aufgefordert, die Daten für das Zertifikat einzugeben, z. B.:

```
Country Name (2 letter code) [AU]:AT  
State or Province Name (full name) [Some-State]:Vienna  
Locality Name (eg, city) []:Vienna  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:COB Consulting  
Organizational Unit Name (eg, section) []:IT  
Common Name (e.g. server FQDN or YOUR name) []:ws01.cob.at  
Email Address []:office@cob.at
```

3. Schritt: Signieren Sie den CSR mit Ihrem Root-Zertifikat:

```
openssl x509 -req -sha256 -days 1825 -in D:\certs\server.csr -CA  
D:\certs\root.crt -CAkey D:\certs\root.key -set_serial 01 -out  
D:\certs\server.crt
```

4. Schritt: Kopieren Sie die Inhalte der Datei server.key und server.pem in eine neu erstellte Textdatei, z. B. in D:\certs\server.txt:

```
D:\certs>type server.key server.crt root.crt >server.txt
```

14.7.5.4. Erstellen der Schlüsselringdatei

1. Schritt: Generieren Sie eine leere Schlüsselringdatei:

```
kyrtool ="C:\Program Files (x86)\HCL\Notes\notes.ini" create -k
D:\certs\server.kyr -p password
```

(Verwenden Sie statt »password« Ihr eigenes Kennwort.)

2. Schritt (optional): Verifizieren Sie den Inhalt der Textdatei:

```
kyrtool ="C:\Program Files (x86)\HCL\Notes\notes.ini" verify
D:\certs\server.txt
```

Die Ausgabe sollte in etwa so aussehen:

```
KyrTool v1.1

Successfully read 4096 bit RSA private key
INFO: Successfully read 2 certificates
INFO: Private key matches leaf certificate
INFO: IssuerName of cert 0 matches the SubjectName of cert 1
INFO: Final certificate in chain is self-signed
```

3. Schritt: Importieren Sie die Datei server.txt in den Schlüsselring:

```
kyrtool ="C:\Program Files (x86)\HCL\Notes\notes.ini" import all -k
D:\certs\server.kyr -i D:\certs\server.txt
```

```
Using keyring path 'D:\cert\server.kyr'
Successfully read 4096 bit RSA private key
SECIssUpdateKeyringPrivateKey succeeded
SECIssUpdateKeyringLeafCert succeeded
```

4. Schritt (optional): Verifizieren Sie den Inhalt des Schlüsselrings:

```
kyrtool ="C:\Program Files (x86)\HCL\Notes\notes.ini" show certs -k
D:\certs\server.kyr
```

14.7.5.5. Das Zertifikat einspielen

Kopieren Sie die Dateien server.kyr und server.sth aus dem Verzeichnis D:\certs in das Datenverzeichnis des Domino-Servers. Aktivieren Sie das Zertifikat wie in Kap. 14.7.3, ab Seite 399 beschrieben.

Überlegen Sie, welche Webbrowser zum Einsatz kommen sollen und wie Sie bewerkstelligen, dass diese dem neuen Zertifikat vertrauen. Die Vertrauensstellung ist bei Webbrowsern relativ leicht zu erreichen: Sie brauchen das Zertifikat nur in den jeweils verwendeten Zertifikatsspeicher zu importieren.

Explorer, Edge und Chrome

Konvertieren Sie das Zertifikat zuerst in das unter Windows verbreitete PFX- bzw. PKCS #12-Format:

```
openssl pkcs12 -in D:\certs\root.crt -export -nokeys -out D:\certs\root.pfx
```

Unter Windows nutzen Internet Explorer, Edge und Chrome den Zertifikatsspeicher des Betriebssystems. Doppelklicken Sie einfach das konvertierte Stammzertifikat (root.pfx), um es dort in den Bereich vertrauenswürdige Stammzertifizierungsstellen zu importieren. Fertig.

(Sie können das importierte Zertifikat mit der Anwendung certmgr.msc begutachten und auch wieder löschen.)

14.7.5.5.1. Firefox

Firefox verwendet seinen eigenen Zertifikatsspeicher. Gehen Sie zu den **Einstellungen** und dann zu **Datenschutz & Sicherheit**. Klicken Sie auf **Zertifikate anzeigen...** und dann auf **Importieren...** (Firefox will das Zertifikat wieder im CRT- oder PEM-Format haben.) Fertig!

14.7.6. Zertifikate für mehrere Hostnamen erstellen

Es ist auch möglich, ein Zertifikat für mehrere Hostnamen aus verschiedenen Domänen zu erstellen, z. B. für www.cob.at, www.cobsoft.at und www.cobtest.at. Solche Zertifikate enthalten ein spezielles Feld **Subject Alternative Name** (SAN), das die zusätzlichen Hostnamen auflistet. **SAN-Zertifikate** sind mit Zertifikaten von offiziellen Zertifizierungsstellen (inklusive Let's Encrypt) genauso kompatibel wie mit selbst signierten Zertifikaten, funktionieren unter Domino aber erst ab Version 11.0.1.

Das Erstellen von Zertifikaten über eine offizielle Zertifizierungsstelle ist in Kap. 14.7.2, ab Seite 395 beschrieben, das Erstellen von eigenen Zertifikaten in Kap. 14.7.5, ab Seite 403. Nachfolgend gehe ich nur noch auf die Unterschiede beim Erstellen ein.

Bei meinen Beispielen gehe ich wieder davon aus, dass Sie alle Dateien im Verzeichnis D:\certs speichern.

Der erste Schritt, das Erstellen des privaten Serverschlüssels server.key bleibt gleich.

Um mehrere Hostnamen und/oder IP-Adressen ins Zertifikat hineinzubekommen, müssen Sie die Zertifikatsanforderung (CSR) durch zusätzliche Felder erweitern. Das geht entweder durch Hinzufügen der zusätzlichen Felder über den Parameter -addtext "Feldname = Inhalt" oder über das Laden einer Konfigurationsdatei über den Parameter -config datei.txt.

Hier ein Beispiel für eine erweiterte Befehlszeile:

```
openssl req -new -subj "/C=AT/CN=www.cob.at" -addext "subjectAltName =  
DNS:www.cobsoft.at" -addext "certificatePolicies = 1.2.3.4" -newkey rsa:2048 -  
keyout key.pem -out req.pem
```

Ich persönlich bevorzuge eine Konfigurationsdatei. Diese könnte so aussehen:

```
[req]  
distinguished_name = req_dis  
req_extensions = req_ext  
prompt = no
```

```
[req_dis]
C = AT
ST = Vienna
L = Vienna
O = COB Consulting
OU = IT
CN = www.cob.at
[req_ext]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = www.cob.at
DNS.2 = www.cobsoft.at
DNS.3 = www.cobtest.at
DNS.4 = ws01.cobtest.at
```

Legen Sie mit dem Editor eine leere Textdatei an, in unserem Beispiel D:\certs\config.txt. Erstellen Sie die einzelnen Abschnitte genau wie im Beispiel angegeben, ersetzen Sie aber natürlich alle Angaben zum Unternehmen und den Hostnamen durch Ihre eigenen.

Sie können anstatt der DNS-Namen oder auch zusätzlich zu den DNS-Namen auch IP-Adressen angeben:

```
IP.1 = 10.10.1.11
IP.2 = 10.10.1.12
IP.3 = 10.10.1.13
```

Durch die Zeile »prompt = no« werden Sie beim Erstellen des CSR nicht mehr nach den einzelnen Parametern gefragt.

Achtung: Da einige Clients bei SAN-Zertifikaten das Feld Common Name (CN) nicht mehr berücksichtigen, sollten Sie alle Hostnamen im Feld Subject Alternative Name auflisten!

Speichern und Schließen Sie die Konfigurationsdatei und erstellen Sie die Zertifikatsanforderung mit dem folgenden Befehl:

```
openssl req -new -sha256 -key D:\certs\server.key -out D:\certs\server.csr -
config D:\certs\config.txt
```

Überprüfen Sie, ob die Zertifikatsanforderung das Feld Subject Alternative Name enthält:

```
openssl req -noout -text -in D:\certs\server.csr
```

Wenn alles geklappt hat, müssten Sie den Bereich »Requested Extensions« vorfinden:

```
Requested Extensions:
  X509v3 Key Usage:
    Key Encipherment, Data Encipherment
  X509v3 Extended Key Usage:
```

Der Webserver: TLS-Zertifikate erstellen

```
    TLS Web Server Authentication
X509v3 Subject Alternative Name:
    DNS:www.cob.at, DNS:www.cobsoft.at, DNS:www.cobtest.at, DNS:ws01.cobtest.at
Signature Algorithm: sha256WithRSAEncryption
```

Leiten Sie nun die Zertifikatsanforderung (CSR) entweder an Ihre Zertifizierungsstelle (CA) weiter oder signieren Sie die Zertifikatsanforderung mit dem in Kap. 14.7.5 erstellten Stammzertifikat. Der Befehl dazu lautet bei SAN-Zertifikaten etwas anders:

```
openssl x509 -req -sha256 -days 3650 -in D:\certs\server.csr -CA
D:\certs\root.crt -CAkey D:\certs\root.key -set_serial 01 -out
D:\certs\server.crt -extensions req_ext -extfile D:\certs\config.txt
```

Die weitere Vorgangsweise ist gleich wie in Kap. 14.7.5 angegeben: Kopieren Sie den privaten Serverschlüssel, das signierte Serverzertifikat und das Stammzertifikat in eine Textdatei und importieren Sie diese mit dem Programm KYRTool in eine neu erstellte Schlüsselringdatei.

Installieren Sie den Schlüsselring wie in Kap. 14.7.3 auf Seite 399 angegeben.

Ergreifen Sie je nach verwendetem Client die notwendigen Maßnahmen, um dem Zertifikat zu vertrauen. So zeigt der Webbrowser Google Chrom nach Import des Stammzertifikats in den Windows-Zertifikatsspeicher nach dem Zugriff auf den Domino-Server beim Klicken auf das Schlosssymbol eine sichere Verbindung an:

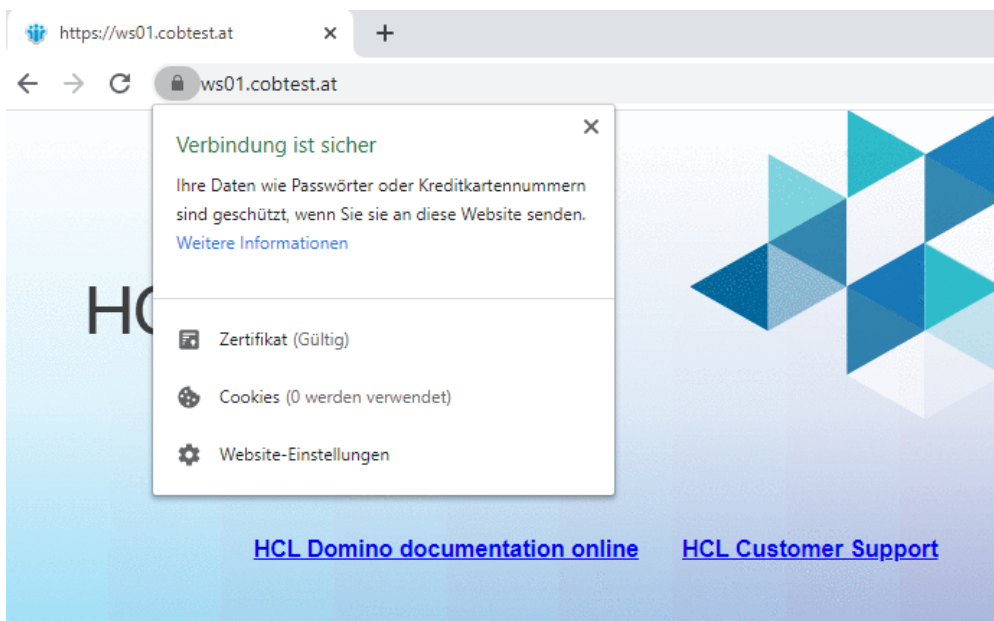


Abbildung 14.31: Google Chrome – Anzeigen einer sicheren Verbindung nach Import des Zertifikats in den Windows-Zertifikatsspeicher

Klicken Sie auf **Zertifikat**, werden die Eigenschaften des Zertifikats angezeigt. Wechseln Sie zum Register **Details** und wählen Sie das Feld **Alternativer Antragstellername** aus, sehen Sie, dass alle Hostnamen enthalten sind (siehe Abbildung 14.32).

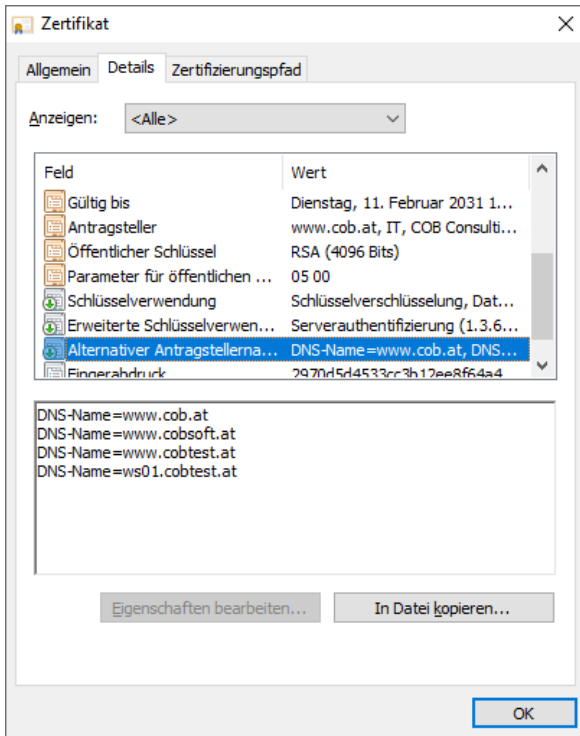


Abbildung 14.32: Eigenschaften des Zertifikats, Feld Alternativer Antragstellername (SAN)

14.8. Der Domino-Webadministrator

Über den Domino-Webadministrator kann man die meisten Admin-Aufgaben von einem Browser aus erledigen. Hinter diesem Feature steckt die Datenbank `webadmin.nsf`, die sich direkt im Datenverzeichnis befindet. Starten Sie den Webadministrator über die folgende URL: <https://IhrServer-name/webadmin.nsf>

Auf den ersten Blick sieht der Webadministrator fast genauso aus wie der Domino-Administrator. Man kann hier auch alles tun, was man im Client tun kann, nur der Domino-Server-Monitor und das Zeichnen von Diagrammen sind nicht verfügbar. Darüber hinaus bietet der Webadministrator einige Features, die im Domino-Administrator nicht gehen, wie etwa das direkte Bearbeiten der Datei `notes.ini` des Servers über einen integrierten Texteditor.

14.8.1. Einrichten des Webadministrators

Die Datenbank `webadmin.nsf` wird beim ersten Start des Domino-Webserver basierend auf der Schablone `webadmin.ntf` automatisch erstellt. Damit alle Features verwendet werden können, müssen neben dem HTTP-Task auch der Administrationsprozess (AdminP) und zum Registrieren von Benutzern und Servern der Task Certificate Authority (CA) laufen.

Per Vorgabe erhält die Gruppe `LocalDomainAdmins` Zugriff auf alle Bereiche. Sollten Sie einen Bereich beschränken wollen, können Sie die entsprechende Rolle in der ACL der Datenbank `webadmin.nsf` deaktivieren:

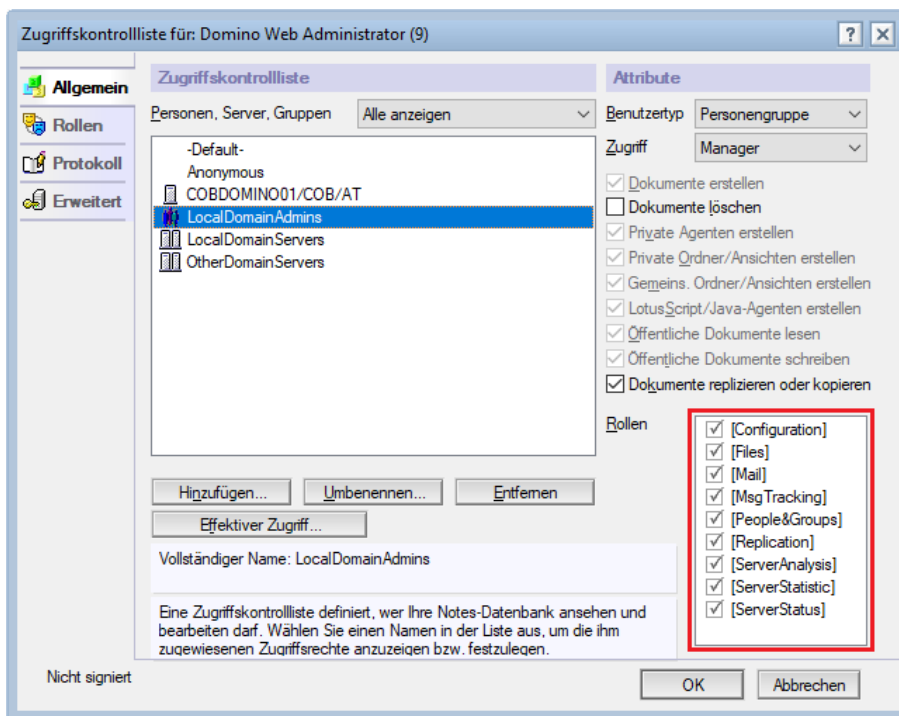


Abbildung 14.33: Domino-Webadministrator – Rollen in der ACL

Derzeit wird nur der Webbrowser Firefox unterstützt. Für das Ausführen der Live-Konsole muss das Java-Plugin 1.4 oder höher installiert und aktiviert sein, was in neueren Firefox-Versionen nicht mehr möglich ist.

14.9. Einen Credential Store einrichten

Bereits beim ersten Hochfahren Ihres Domino-Servers sehen Sie auf der Serverkonsole die Meldung: »Credential Store Configuration not enabled, less secure mode«. Was ist damit gemeint?

Bei einem Credential Store handelt es sich um eine Notes-Datenbank mit dem Dateinamen credstore.nsf, in der Anmeldeinformationen zur Authentifizierung und Verschlüsselungsschlüssel gespeichert werden. Damit können Notes-Benutzer Domino-Anwendungen Zugriff auf Webseiten gewähren, die das OAuth-Protokoll (Open Authorization) verwenden, wodurch zusätzliche Kennworteingaben vermieden werden. Anwendungsfälle umfassen HCL Verse, einige Komponenten des Domino AppDev-Packs oder die DAOS-Tier 2-Funktion zum Verbinden zu einem Remotespeicherdienst.

Der Credential Store wird über den Konsolenbefehl `keymgmt` aus der Schablone `websecuritystore.ntf` erstellt. (Verwenden Sie die Schablone nicht, um selbst einen Credential Store zu erstellen, sondern verwenden Sie dafür immer nur den vorgesehenen Befehl!)

14.9.1. Einen Credential Store auf einem einzelnen Server einrichten

Verwenden Sie den folgenden Konsolenbefehl, um einen Verschlüsselungsschlüssel (Named Encryption Key, NEK) zur Server-ID hinzuzufügen:

```
keymgmt create nek credstorekey
```

Der Schlüssel »credstorekey« wird von Domino später verwendet, um Anmeldedaten (Credentials) zu verschlüsseln, die im Credential Store gespeichert werden.

Nach Eingabe des Befehls sollten Sie auf der Serverkonsole eine ähnliche Meldung sehen wie diese:

```
17.04.2021 17:04:15,81 [024C:0008-3848] NEK > NEK credstorekey -
Fingerprint 44A5 624A 65CD 1771 F274 4779 C7AB 2FE0 9671 BB30
NEK credstorekey created successfully
```

Geben Sie nun den Befehl ein, um die Anwendung credstore.nsf zu erstellen und mit dem generierten Schlüssel zu verschlüsseln:

```
keymgmt create credstore credstorekey
```

Die Datenbank wird im Domino-Datenverzeichnis unter dem folgenden Pfad abgelegt: \\IBM_CredStore\credstore.nsf.

14.9.2. Einen Credential Store in einem Cluster einrichten

Wenn der Mailserver Teil eines Clusters ist, führen Sie die folgenden Schritte aus, um den Credential Store auf jedem Server zu installieren:

Geben Sie auf der Serverkonsole des Servers, auf dem Sie die Datei credstore.nsf erstellt haben, den folgenden Befehl ein, um den Geheimschlüssel zu exportieren:

```
KEYMGMT export nek credstore <Schlüsselname>.key <Kennwort>
```

Kopieren Sie die Schlüsseldatei ins Datenverzeichnis jedes Clustermitglieds.

Geben Sie dann auf der Konsole jedes Domino-Servers den folgenden Befehl ein, um den Schlüssel zu importieren:

```
KEYMGMT import nek <Schlüsselname>.key <Kennwort>
```

Sie sollten die folgende Antwort erhalten:

```
NEK credstore - Fingerprint XXXX XXXX XXXX XXXX XXXX XXXX NEK credstore
imported successfully
```

Erstellen Sie eine Replik der Datenbank credstore.nsf auf allen Cluster-Mitgliedern.

14.10. Webmail einrichten

Der Webmailzugang heißt bei Domino **iNotes Web Access**. Sie als Administrator müssen Domino-seitig nichts tun, wenn der HTTP-Task läuft, steht auch das Webmail zur Verfügung. Die Benutzer können via Browser über die folgenden URL auf ihr Webmail zugreifen:

<https://IhrServername/mail/IhreMaildatei.nsf>

Da Sie davon ausgehen müssen, dass die wenigsten Anwender den Namen ihrer Maildatei kennen, sollten Sie die Prozedur deutlich vereinfachen:

Der Webserver: Webmail einrichten

1. Erstellen Sie die Anwendung »iNotes Redirect« zum automatischen Umleiten der Benutzer zu ihrem Webmail nach der Anmeldung.
2. Binden Sie die Anwendung iNotes Redirect auf eine kurze, sprechende URL, z. B. www.cob.at/webmail oder auf einen sprechenden Hostnamen, z. B. webmail.cob.at.
3. Stellen Sie eine ansprechende Anmeldemaske zur Verfügung

14.10.1. iNotes Redirect einrichten

Mit iNotes Redirect müssen Benutzer den Pfad zu ihrer Maildatei nicht wissen, sondern nur die Start-URL des Servers kennen. iNotes Redirect benutzt Domino-Authentifizierungsmethoden, um den Browser basierend auf dem Benutzernamen zur Maildatei umzuleiten.

Über die Anwendung iNotes Redirect können Sie auch eine TLS-Verbindung erzwingen, entweder für die ganze Sitzung oder nur zur Authentifizierung, nach der der Benutzer zu einer normalen HTTP-Verbindung zurückkehrt. Sie können in der Anwendung auch die Portnummer ändern, sollten Sie etwas anderes als 443 brauchen.

Die Schablone für iNotes Redirect heißt `iwaredir.ntf` und befindet sich im Domino-Datenverzeichnis.

Gehen Sie wie folgt vor, um iNotes Redirect einzurichten:

1. Erstellen Sie basierend auf der Schablone `iwaredir.ntf` eine neue Datenbank. Verwenden Sie einen beliebigen, aber URL-kompatiblen Namen (keine Leer- und Sonderzeichen, keine Umlaute).
2. Wählen Sie als Sprache Englisch oder Deutsch.
3. Öffnen Sie die neu erstellte Anwendung im Notes-Client.
4. Klicken Sie auf die Schaltfläche **Setup** und folgen Sie den Angaben.

14.10.2. Eine Websiteregeln erstellen

Um es den Anwendern zu ermöglichen, eine kurze, sprechende URL wie »mail« oder »webmail« zu verwenden, müssen Sie eine Websiteregeln mit einer URL-Umleitung (URL Redirection) erstellen. Gehen Sie dazu wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Konfiguration > Web**.
2. Öffnen Sie die Webseite, für die Sie die URL-Umleitung erstellen wollen.
3. Klicken Sie auf die Schaltfläche **Website** und wählen Sie den Befehl **Regel erstellen**.
4. Geben Sie eine Beschreibung für die Regel ein.
5. Wählen Sie als **Typ der Regel** »Umleitung«.
6. Geben Sie im Feld **Muster der eingehenden URL** an, was die Anwender eingeben, z. B. »/webmail«.
7. Geben Sie im Feld **An diese URL umleiten** den Pfad zur iNotes Redirect-Datenbank an, z. B. »/redir.nsf«.

Websiteregeln	
Allgemein Kommentare Administration	
Allgemein	
Beschreibung:	Webmail
Typ der Regel:	Umleitung
Muster der eingehenden URL:	/webmail
An diese URL umleiten:	/redir.nsf
301 Redirect senden:	<input checked="" type="checkbox"/> Ja

Abbildung 14.34: Websiteregeln

8. Starten Sie den HTTP-Task neu:
`tell http restart`

14.11. Auf HCL Verse umstellen

14.11.1. Was ist HCL Verse?

HCL Verse ist ein webbasierender E-Mail-Client, der zahlreiche Innovationen wie soziale Analyse- und fortgeschrittene Suchfunktionen beinhaltet. (Einige Features stehen nur mit HCL Connections zur Verfügung.) Gedacht ist Verse nicht nur für den Zugriff aus dem Internet, sondern auch als alternative Desktoplösung im lokalen Netzwerk.

Zum Einrichten von Verse müssen Sie einige Schritte auf einem Domino-Server ausführen, um die Nutzung von Mail- und Kalenderfunktionen vorzubereiten. Offline-Funktionalität ist standardmäßig verfügbar und erfordert keine spezielle Konfiguration.

Benutzerfotos können aus dem Domino-Verzeichnis, aus HCL Connections oder über den Gravatar-Dienst eingebunden werden. Die Fotos können direkt im Verse-Client hochgeladen werden.

Um eine Vorschau für Dateianhänge zu erhalten, können Sie Verse für die Zusammenarbeit mit HCL Docs konfigurieren. Dies ermöglicht es Verse-Anwendern, Anhänge im Format PDF, Microsoft Office und OpenOffice anzuzeigen, ohne diese herunterladen zu müssen.

14.11.2. Voraussetzungen

Verse wird unabhängig von Domino gewartet und die Versionen wechseln sehr rasch. Die Voraussetzungen für die zum Zeitpunkt der Veröffentlichung dieses Buchs aktuelle Version 2.1.0 lauten:

- > Domino 9.0.1 FP 10 oder höher auf Microsoft Windows 2008 und 2012 64-bit
- > Domino 10.0.x oder höher auf Microsoft Windows 2012 und 2016 64-bit
- > Domino 11.0.x auf Microsoft Windows 2012, 2016 und 2019 64-bit

Um eine Vorschau von Anhängen wie Tabellenkalkulationen, Dokumente oder Präsentationen anzuzeigen, muss HCL Docs 2.0 CR2 iFix003 integriert werden.

Auf dem Desktop funktioniert Verse mit den folgenden Webbrowsern:

- > Mozilla Firefox (aktuelle Version)
- > Google Chrome (aktuelle Version)
- > Apple Safari 10, 11
- > Microsoft Edge (aktuelle Version)

Auf Mobilgeräten muss Chrome (Android) oder Safari (iOS) verwendet werden.

14.11.3. Installation von Verse

1. Stellen Sie sicher, dass Sie den HTTP-Server-Task ausführen und iNotes konfiguriert haben. Zur Konfiguration von iNotes lesen Sie Kap. 14.10 Webmail einrichten, ab Seite 411.
2. Stellen Sie sicher, dass der Webserver UTF-8 für die Ausgabe verwendet. Diese Einstellung finden Sie je nach Konfiguration entweder im **Serverdokument**, Register **Internetprotokolle > Domino-Web-Engine** oder, wenn Sie Internet-Site-Dokumente verwenden, im Website-Dokument im Register **Domino-Web-Engine**.
3. Erstellen Sie, wenn noch nicht vorhanden, Volltext-Indizes für alle Maildateien. Informationen zum Erstellen von Volltextindizes finden Sie in Kap. 9.9 Volltextindizes verwalten, ab Seite 266.
4. Fügen Sie zur Datei notes.ini auf Ihrem Domino-Web-Server die folgenden Einstellungen hinzu:

```
HTTPJVMMMaxHeapSize=2048M
```

```
HTTPJVMMMaxHeapSizeSet=1
```

Sollten die Einstellungen bereits vorhanden sein, stellen Sie sicher, dass sie die angegebenen Werte enthalten.

5. Aktivieren Sie TLS auf dem Domino-Server. Verse erfordert HTTPS und ein gültiges Zertifikat. Eine Anleitung zum Anfordern und Einspielen von SHA-2-Zertifikaten eines Drittanbieters unter Verwendung von OpenSSL und KYRTool finden Sie in Kap. 14.7 TLS-Zertifikate erstellen, ab Seite 394.

Anmerkung: Wenn Sie einen Proxy-Server vor dem Domino-Server verwenden, muss der Proxy-Server HTTPS unterstützen und über das gültige Zertifikat verfügen.

6. Stellen Sie sicher, dass der SSL-Portstatus aktiviert ist. Weitere Informationen dazu finden Sie im Kap. 14.6 Einen sicheren Webserver aufbauen, ab Seite 387.
7. Wenn das noch nicht geschehen ist, konfigurieren Sie einen ID-Vault auf dem Domino-Server und sorgen Sie dafür, dass sich ID-Dateien von allen Verse-Benutzern im Vault befinden. Ein ID-Vault ist erforderlich, damit Benutzer signierte oder verschlüsselte Nachrichten lesen und senden können. Informationen zum ID-Vault und zum Zuordnen von Anwendern zu einem ID-Vault finden Sie in Kap. 6.2.1 Einen ID-Vault einrichten, ab Seite 138.
8. Setzen Sie in der **Sicherheitsrichtlinie**, Register **ID-Vault** das Feld **Notes-basierte Programme dürfen die Notes-ID-Vault verwenden** auf »Ja«.
9. Achten Sie darauf, dass in den Personendokumenten der Benutzer gültige Internetadressen eingetragen sind.
10. Extrahieren Sie die Dateien aus dem Verse-Paket. Das Paket enthält folgende Dateien:
HCL_Verse_On_Premises.zip, iwaredir.ntf und readme.zip

11. Stoppen Sie den Domino-Webserver über den Befehl:
`tell http quit`
12. Wenn eine Vorgängerversion von Verse installiert ist, löschen Sie die vorhandenen .jar-Dateien aus einem der folgenden Verzeichnisse, je nachdem, wo das Produkt installiert wurde:
 <Domino-Programmverzeichnis>\osgi\shared\eclipse\plugins
 oder:
 <Domino-Datenverzeichnis>\domino\workspace\applications\eclipse\plugins
 Verwenden Sie die Platzhaltersyntax "*-1.0.*-0.0-*.jar", core-1.0.*.*.jar und servlet-1.0.*.*.jar, um sicherzustellen, dass nur die Jar-Dateien von Verse gelöscht werden.
13. Extrahieren Sie den Inhalt der Datei HCL_Verse_On_Premises.zip in das folgende Verzeichnis:
 <Domino-Datenverzeichnis>\domino\workspace\applications
 Anmerkung: Extrahieren Sie die Dateien mit intakter Verzeichnisstruktur. Nach der Extraktion sollten sich die JAR-Dateien von Verse im folgenden Verzeichnis befinden:
 <Domino-Datenverzeichnis>\domino\workspace\applications\eclipse\plugins
14. Kopieren Sie die mit dem Verse-Paket mitgelieferte Schablone iwaredir.ntf ins Domino-Datenverzeichnis.
 Wenn keine Redirect-Datenbank vorhanden ist, erstellen Sie mithilfe der Schablone iwaredir.ntf eine neue. Andernfalls ersetzen Sie das Design der vorhandenen Redirect-Datenbank durch das der neuen Schablone. Wählen Sie dazu den Menübefehl **Datei > Anwendung > Schablone wechseln**.
 Das Verse-Paket enthält Übersetzungen der Redirect-Schablone für Englisch, Chinesisch (China), Chinesisch (Taiwan), Französisch, Deutsch, Italienisch, Japanisch, Koreanisch, Portugiesisch (Brasilien) und Spanisch. Achten Sie darauf, die deutsche Schablone zu verwenden.
15. Öffnen Sie nun die Redirect-Datenbank im Notes-Client und wählen Sie die Seite UI-Setup aus, um Benutzern die Anmeldung bei Verse zu ermöglichen:
 Wenn Sie Domino zur Authentifizierung verwenden, gehen Sie wie folgt vor:
 A. Persönliche Optionen aktivieren? **Nein**
 B. Anmeldeoptionen aktivieren? **Ja**
 C. HCL-Verse aktivieren? **Ja**
16. Wenn es auf dem Server noch keinen Credential Store gibt, richten Sie einen ein.
17. Legen Sie die Ausgangs-URL Ihres Servers entweder auf /verse oder /iwaredir.nsf?open fest.
18. Um Ihre Konfiguration zu testen, melden Sie sich einmalig mit einem berechtigten Benutzer unter der folgenden URL an:
<https://IhrDominoServer/verse>.

Für den Betrieb von Verse muss die Maildatenbank die zusätzlichen Ansichten (\$VerseLookup) und (\$VerseTrashLookup) enthalten. Diese sind ab Version 9.0.1 FP9 bereits in der Mailschablone enthalten. Sollten Sie Maildatenbanken mit einem älteren Design verwenden, können Sie die Ansichten aus der bis zu Version 1.0.8 im Verse-Paket enthaltenen Schablone VOPDesign.nsf in die Mailschablone kopieren. Beruhen Ihre Maildatenbanken auf einer Schablone 9.0.1 FP9 oder höher, ist nichts weiter zu unternehmen.

14.11.4. Verse als eigenständige Anwendung ausführen

Ab Version 2.0 können Sie HCL Verse als eigenständige Browseranwendung mit progressiver Webanwendungstechnologie (PWA) installieren. Als PWA wird Verse in einem eigenen Fenster ausgeführt und nicht als Registerseite in Ihrem Browser. Starten und stoppen Sie Verse wie jede andere installierte Browseranwendung. Dieses Feature wird derzeit nur von den folgenden Browsern unterstützt:

- > Chrome unter Microsoft Windows, Mac OS und Android
- > Microsoft Edge (80+) unter Microsoft Windows
- > Apple Safari unter iOS

Um Verse als eigenständige Anwendung zu installieren, gehen Sie wie folgt vor:

1. Melden Sie sich über die vordefinierte URL bei Verse an.
2. Der Browser zeigt an, dass die Installation einer Anwendung verfügbar ist. Zum Beispiel wird auf Chrome, das unter Windows läuft, ein +-Symbol in der Browserleiste angezeigt, auf das Sie klicken können, um die Verse-Anwendung zu installieren:



Abbildung 14.35: Plusymbol in der URL-Leiste von Chrome

3. Klicken Sie im angezeigten Dialog auf **Installieren**:

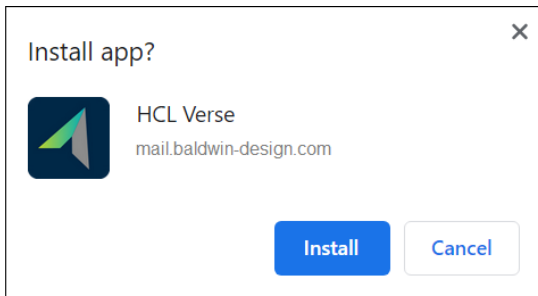


Abbildung 14.36: Sicherheitsdialog Verse-PWA installieren

15. Mobile Endgeräte

- > 15.1 Übersicht, Seite 417
- > 15.2 Installation des Traveler-Servers, Seite 418
- > 15.3 Den Traveler starten und beenden, Seite 423
- > 15.4 Traveler-Benutzer hinzufügen, Seite 424
- > 15.5 Traveler-Benutzer löschen, Seite 425
- > 15.6 Geräte verwalten, Seite 425
- > 15.7 Das Traveler-Protokoll, Seite 431
- > 15.8 Die Derby-Datenbank, Seite 432

15.1. Übersicht

Mit dem HCL Traveler können Ihre Anwender E-Mails, Kontakte, Termine und Aufgaben mit einer Vielzahl von Smartphones und Tablets synchronisieren. Die Software glänzt durch eine schlanke Architektur und lässt sich einfach installieren, warten und nutzen. Sie unterstützt Passworrichtlinien, Transportverschlüsselung (TLS/SSL) und Fernlöschung. Für die am weitesten verbreiteten mobilen Betriebssysteme iOS & Android existieren native Apps (Verse), die aus dem jeweiligen App-Store heruntergeladen werden können. Andere mobile Endgeräte und Microsoft Outlook ab Version 2013 können über das Protokoll Exchange ActiveSync (EAS) angebunden werden. Und das Beste daran: Der Traveler ist für lizenzierte Notes-Benutzer kostenlos!

Der Traveler ist kein eigener Server, sondern wird als Software-Komponente auf einem Domino-Server ausgeführt, wobei Traveler 11.0.2 auf Domino 9.0.1 (ab FP5), 10.0.x und 11.0.x läuft.

Beachten Sie, dass Sie nach einer Aktualisierung des Domino-Servers auch die Traveler-Installation erneut ausführen müssen, um sicherzustellen, dass die richtigen Binärdateien installiert sind. Wenn Sie beispielsweise Traveler 11.0.2 unter Domino 10.0.1 ausführen und ein Upgrade auf Domino 11.0.1 durchführen, führen Sie das Installationsprogramm für Traveler 11.0.2 erneut aus.

Der Traveler-Server muss nicht identisch mit dem Mailserver sein und auch nicht über lokale Repliken der Maildatenbanken verfügen, er muss jedoch Zugriff auf die Maildatenbanken am Mailserver haben. Dafür werden auch ältere Mailserver bis zurück zu Version 7 unterstützt.

Die Übertragung der Daten von und zu den mobilen Endgeräten erfolgt über das Protokoll HTTPS (Port 443) und muss über TLS 1.2 verschlüsselt sein. Da Geräte mit Android vor Version 4.1 kein TLS 1.2 unterstützen, können sie somit nicht verwendet werden.

Damit die Anbindung über HTTPS funktioniert, müssen Sie ein Serverzertifikat anschaffen. Dieses muss den folgenden Regeln entsprechen:

- > Das Zertifikat darf nicht abgelaufen oder ungültig sein.

- > Das Zertifikat muss entweder von einer anerkannten Zertifizierungsstelle (CA) stammen, dessen Root-Zertifikat die Endgeräte vertrauen, oder, wenn Sie Ihr eigenes Zertifikat verwenden wollen, müssen Sie es zuvor selbst auf den Geräten installiert haben. (Laut Hersteller-Website funktionieren selbst erstellte Zertifikate für Verse auf iOS nicht, ich konnte nach dem Import des Zertifikats aber problemlos damit arbeiten.)
- > Der Common Name (CN) bei einem einzelnen Zertifikat oder einer der »Alternative Names« bei einem SAN-Zertifikat (siehe dazu Kap. 14.7.6 Zertifikate für mehrere Hostnamen erstellen, ab Seite 406) muss mit dem Hostnamen des Servers übereinstimmen.
- > Wildcard-Zertifikate sind ebenfalls erlaubt, die Domäne aus der Wildcard muss mit der Domäne des Servers übereinstimmen.
- > Das Serverzertifikat muss mit einer der folgenden Schlüsselarten signiert sein:
 - RSA-Schlüssel mit einer Länge von zumindest 2048 Bit
 - Elliptic-Curve Cryptography (ECC/ECDSA) Schlüssel mit einer Größe von mindestens 256 Bit
- > Der verwendete Secure Hash-Algorithmus muss SHA-2 mit einer Mindestlänge von 256 (SHA-256) oder größer sein.
- > Die ausgehandelte Chiffre-Suite für die TLS-Verbindung muss Forward Secrecy unterstützen (ist bei Domino 11 automatisch der Fall).

Da der Traveler-Server die Push-Messaging-Dienste von Google und Apple nutzt, um Benutzer über neue E-Mails zu informieren, muss er eine direkte Internetverbindung aufbauen können. Vorsicht daher mit Proxys. Lesen Sie dazu auch:

https://help.hcltechsw.com/traveler/11.0.0/google_messaging.html

15.2. Installation des Traveler-Servers

15.2.1. Vorgaben

Der Traveler-Server muss im Serverdokument jedes Mailserver als vertrauenswürdiger Server eingetragen werden.

Der Domino-Server, der den Traveler hostet, muss weiters Manager-Zugriff mit Löschrechten auf alle Maildatenbanken haben. Das ist leicht erledigt, indem Sie den Traveler-Server in die Gruppe LocalDomainServers aufnehmen.

Laden Sie die Software herunter und entpacken Sie die ZIP-Datei in einen Ordner. (Der Traveler heißt auf FlexNet: Traveler_11.0.1_Win_ML.zip – wobei ML für Multi Language steht).

15.2.2. Vorgangsweise

Um den HCL Traveler zu installieren, gehen Sie wie folgt vor:

1. Beenden Sie den Domino-Server.
2. Führen Sie die Installationsdatei (üblicherweise TravelerSetup.exe) als Administrator aus. InstallAnywhere wird geladen.
3. Wählen Sie die Installations Sprache aus und klicken Sie auf **OK**:

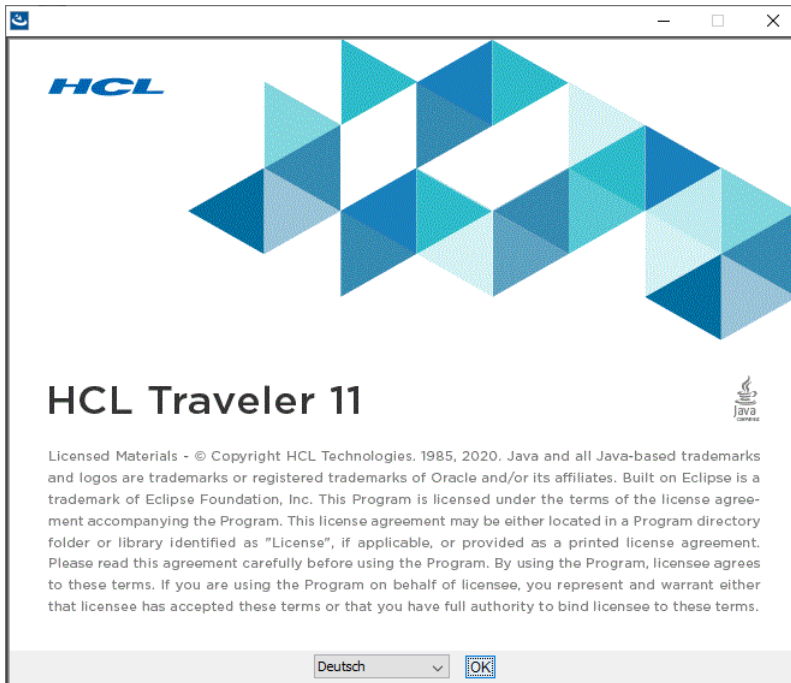


Abbildung 15.1: Traveler-Installation, Startbildschirm

Der Willkommensbildschirm wird angezeigt:

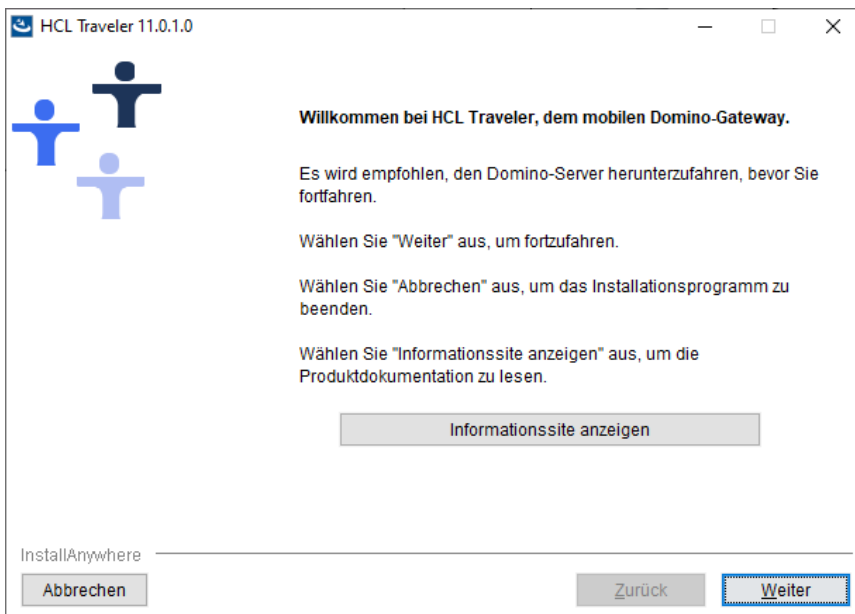


Abbildung 15.2: Traveler-Installation, Willkommenseite

4. Klicken Sie auf **Weiter**.

Der Lizenzvertrag wird angezeigt:

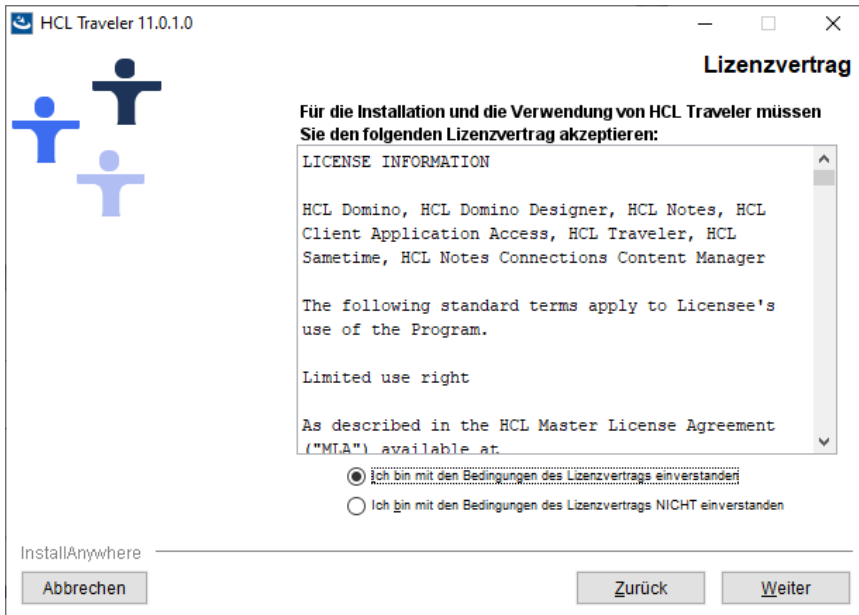


Abbildung 15.3: Traveler-Installation, Lizenzvertrag

5. Wählen Sie »Ich bin mit den Bedingungen des Lizenzvertrags einverstanden« und klicken Sie auf **Weiter**.
6. Bestätigen Sie Programm- und Datenverzeichnis des Domino-Servers und klicken Sie auf **Weiter**. (Die angezeigten Pfade werden aus der Windows-Registrierdatenbank ausgelesen.)

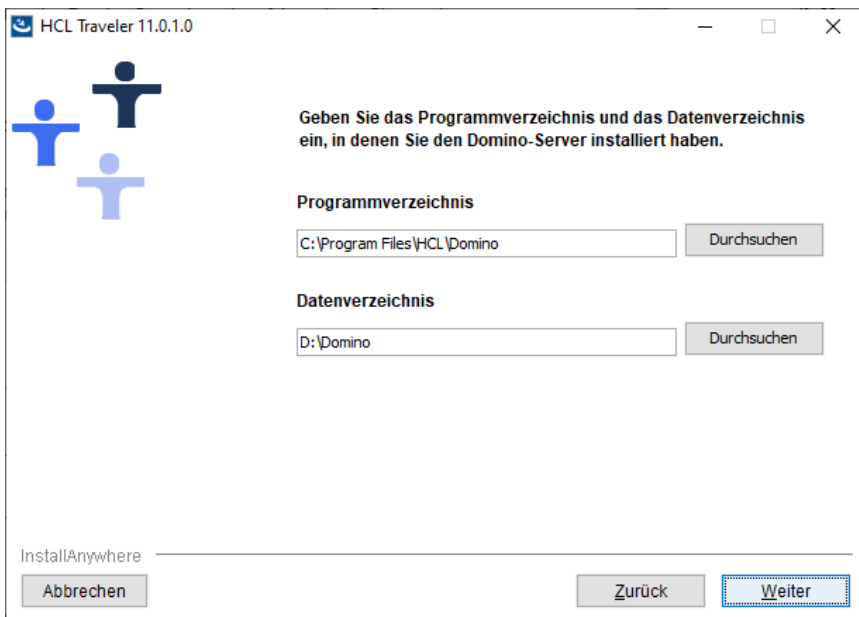


Abbildung 15.4: Traveler-Installation, Auswahl von Programm- und Datenverzeichnis

7. Geben Sie an, ob die Benutzer-Homepage des Traveler als Standard-Website konfiguriert werden soll. Wählen Sie diese Option nur, wenn es noch keine andere Homepage gibt.

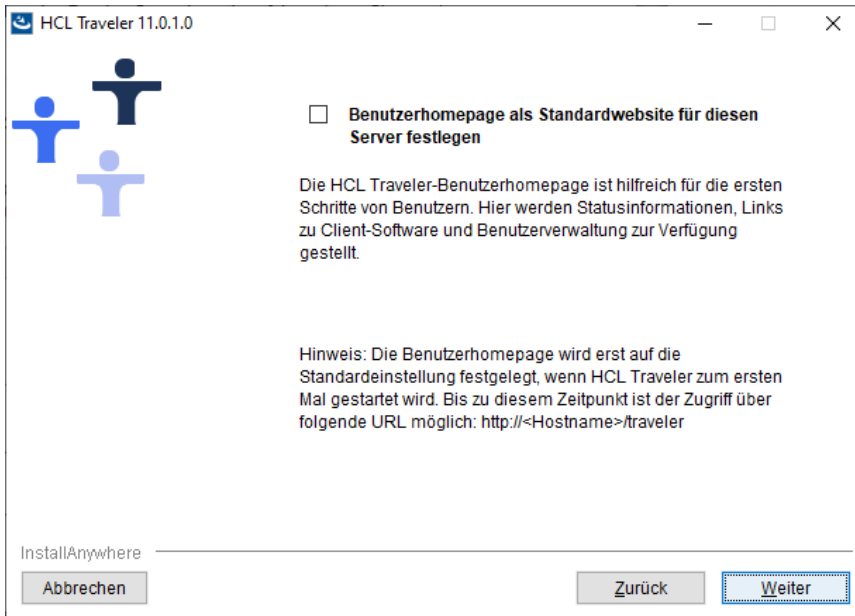


Abbildung 15.5: Traveler-Installation, Option Benutzerhomepage als Standardwebseite festlegen

8. Geben Sie an, wie sich Clients mit dem Server verbinden, und klicken Sie auf **Weiter**.

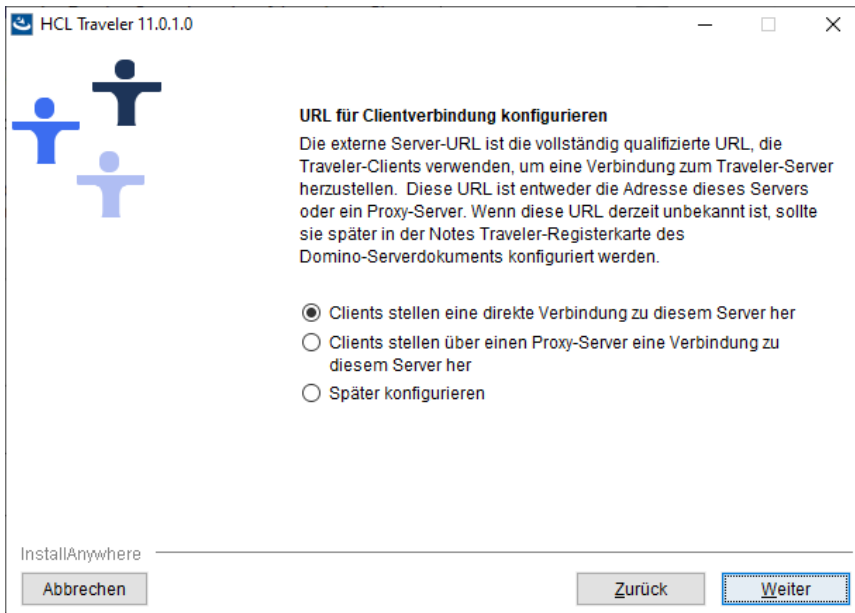


Abbildung 15.6: Traveler-Installation, Optionen für Client-Verbindung konfigurieren

9. Geben Sie die externe Server-URL an. Das ist jene Adresse, mit der sich die Endgeräte mit dem Traveler-Server verbinden:

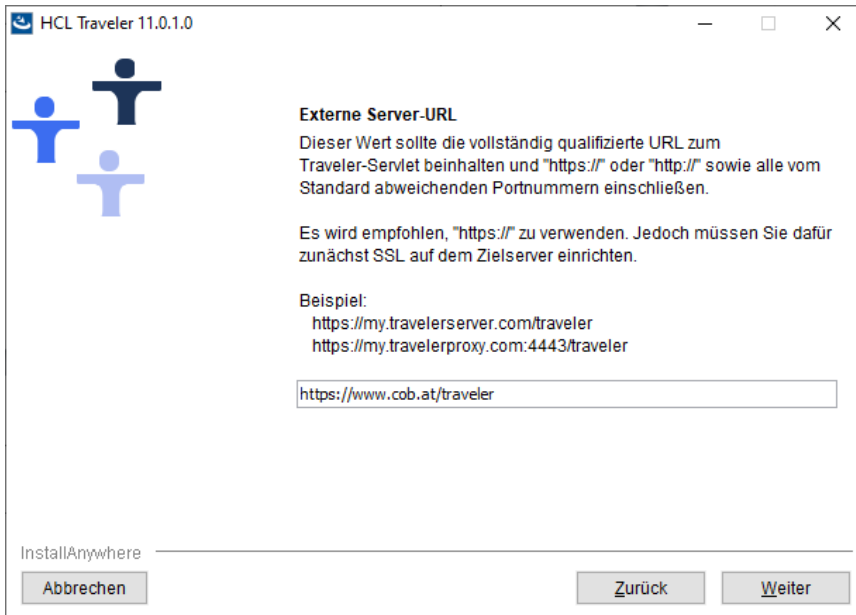


Abbildung 15.7: Traveler-Installation, Externe Server-URL festlegen

10. Klicken Sie auf **Weiter**.

Eine Zusammenfassung wird angezeigt. Sollten Sie etwas Falsches ausgewählt haben, können Sie über die Schaltfläche **Zurück** zurücknavigieren und Ihre Auswahl ändern.

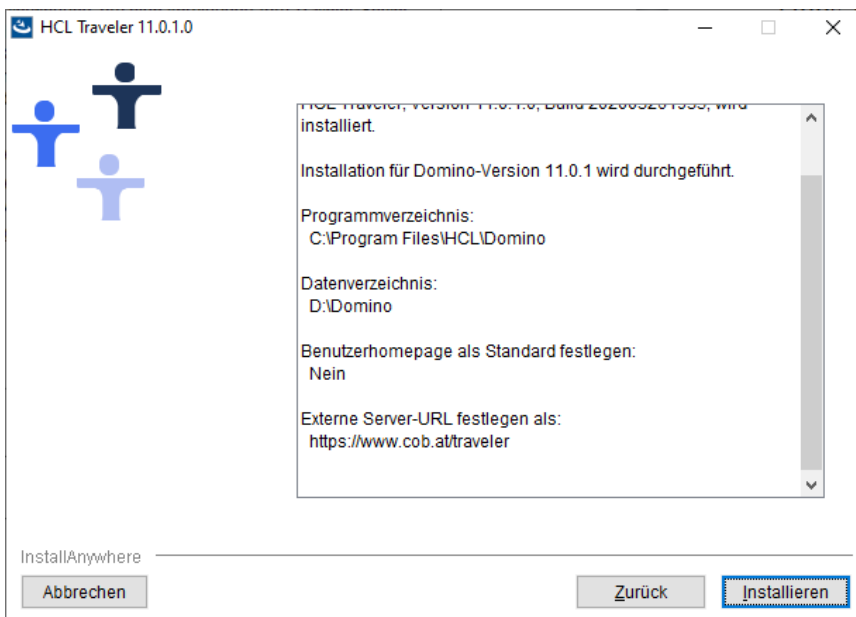


Abbildung 15.8: Traveler-Installation, Zusammenfassung

11. Klicken Sie auf **Installieren**.



Abbildung 15.9: Traveler-Installation, Installationsfortschritt

Am Ende der Installation wird eine Erfolgsmeldung angezeigt:

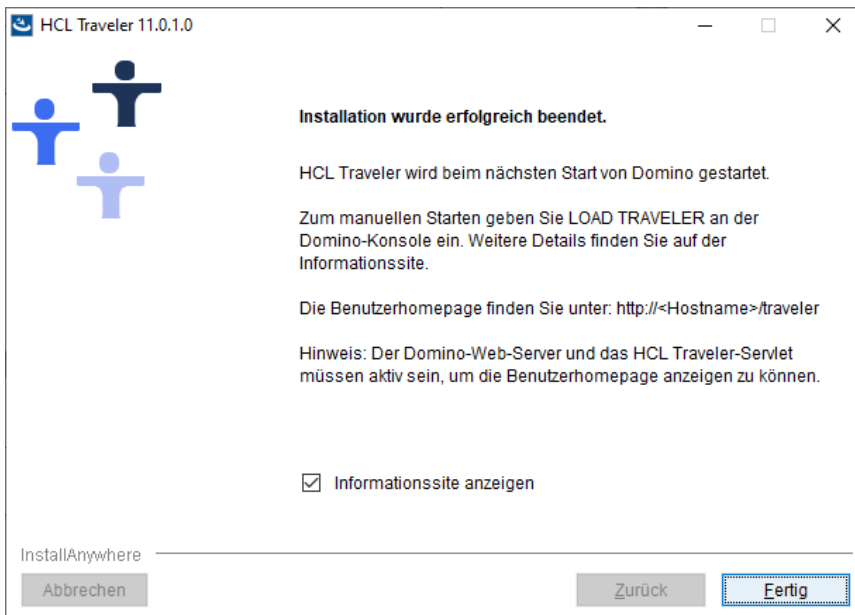


Abbildung 15.10: Traveler-Installation, Erfolgsmeldung

12. Klicken Sie auf **Fertig**.

15.3. Den Traveler starten und beenden

Der Traveler-Task benötigt zusätzlich den HTTP-Task, da mobile Endgeräte über das Protokoll HTTPS mit dem Server kommunizieren. Bei der Installation verweigert sich der Traveler in der Zeile

ServerTasks in der notes.ini, entfernt jedoch den Eintrag für den HTTP-Server. Dafür wird der folgende Eintrag hinzugefügt:

```
NTS_AUTOSTART_HTTP=true
```

Der Traveler-Server verwaltet also ab jetzt den Start des Webservers.

Wenn Sie den Domino-Server herunterfahren, erhalten alle Prozesse gleichzeitig den Befehl zu stoppen. Wenn jedoch der HTTP-Server und der Traveler gleichzeitig herunterfahren, kann das bei vielen offenen Anfragen von Endgeräten zu einem Hängenbleiben des HTTP-Tasks führen. Daher sollten Sie wann immer möglich vor dem Herunterfahren des ganzen Domino-Servers zuerst den Traveler stoppen. Verwenden Sie dazu den Befehl:

```
tell traveler shutdown
```

Nach Eingabe dieses Befehls, akzeptiert der Traveler keine neuen Anfragen mehr, arbeitet die laufenden ab und fährt erst nach deren erfolgreicher Beendigung herunter.

Wenn Sie zur Datei notes.ini den folgenden Eintrag hinzufügen, kümmert sich der Traveler auch darum, dass auch der HTTP-Task korrekt heruntergefahren wird:

```
NTS_AUTOSTOP_HTTP=true
```

15.4. Traveler-Benutzer hinzufügen

Benutzer können den Traveler verwenden, wenn sie die folgenden Voraussetzungen erfüllen:

- > Das Personendokument muss im Domino-Verzeichnis (names.nsf) des Traveler-Servers existieren.
- > Der Benutzer muss ein Internetkennwort eingetragen haben.
- > Der Benutzer muss über eine Internet-Mailadresse verfügen.
- > Die Felder **Serverzugriff** und **Kein Serverzugriff** im **Register Notes Traveler** des Serverdokuments sind entweder leer (dann dürfen alle Benutzer den Traveler nutzen) – in diesem Fall wird im Lesemodus »Alle Benutzer können auf diesen Server zugreifen« angezeigt:



Abbildung 15.11: Serverdokument, Register **Notes Traveler**

- > Oder der Benutzer ist über seinen Namen (nicht empfohlen) oder über eine Gruppe im Feld **Serverzugriff** eingetragen und fehlt im Feld **Kein Serverzugriff**.

Abbildung 15.12: Serverdokument, Register **Notes Traveler**

- > Damit Anwender auf ihren Endgeräten alle Informationen zur Verfügung haben, müssen sie ihre Kontakte in ihre Maildatenbank hochgeladen haben.

15.5. Traveler-Benutzer löschen

Löschen Sie nicht einfach nur den Benutzer aus LotusTraveler.nsf, denn der Traveler-Task verwaltet die Masterdaten in einer relationalen Derby-Datenbank im Verzeichnis \traveler\ntsdb. (Details finden Sie im Kap. 15.8 Die Derby-Datenbank auf Seite 432.) Es ist ganz im Gegenteil sogar so, dass ein gelöschter Benutzereintrag bei der nächsten Änderung in LotusTraveler.nsf wieder auftaucht. Wollen Sie einen Benutzer korrekt löschen, so ist dies derzeit nur über einen Konsolenbefehl möglich:

```
tell traveler delete * <Benutzername>
```

Haben Sie den Benutzer bereits aus dem Domino-Verzeichnis gelöscht, müssen Sie seinen Namen vollständig (kanonisch) angeben, z. B.:

```
tell traveler delete * CN=Otto Huber/O=COB/C=AT
```

Ein allfälliges entferntes Löschen für den Benutzer oder ein Gerät muss zuvor rückgängig gemacht werden. (Siehe dazu Kap. 15.6.5 Ein Remote Wipe zurücknehmen auf Seite 430.)

Auf älteren Traveler-Versionen (vor 9.0.1.10) ist auch noch die Eingabe des folgenden Befehls nötig:

```
tell traveler security delete * <Benutzer>
```

15.6. Geräte verwalten

15.6.1. Den Geräten Vorgaben zuweisen

Es gibt drei Arten, mobilen Geräten Einstellungen zuzuordnen:

1. Über die Vorgabe-Geräteinstellungen in der Traveler-Datenbank (LotusTraveler.nsf).

- Über die hartcodierten Vorgaben des Traveler-Servers (gelten für alle von den Vorgabe-Geräteeinstellungen ausgeschlossenen Benutzer). Die hart codierten Einstellungen sind identisch mit den anfänglichen Vorgabe-Geräteeinstellungen.
- Über Traveler-Richtlinien im Domino-Verzeichnis.

15.6.1.1. Verwenden der Vorgabe-Geräteeinstellungen

Mithilfe der Traveler-Datenbank (LotusTraveler.nsf) können Sie Vorgabe-Geräteeinstellungen für die Erstregistrierung Ihrer mobilen Geräte festlegen. Idealerweise legen Sie die gewünschten Einstellungen fest, bevor Sie mobile Geräte ausrollen.

Um die Vorgabe-Geräteeinstellung zu bearbeiten, gehen Sie wie folgt vor:

- Öffnen Sie die HCL Traveler-Administration (LotusTraveler.nsf). Die Anwendung gibt es nur auf Englisch.
- Gehen Sie zur Ansicht **Device Settings**.
- Klicken Sie auf die Schaltfläche **Edit Settings**.
- Navigieren Sie zum Register **Preferences**.
- Wechseln Sie zu den entsprechenden Unterregistern, um Einstellungen zu ändern.
- Navigieren Sie bei Bedarf zum Register **Assignment**, um Benutzer hinzuzufügen oder auszuschließen. Lassen Sie das Feld **Include Users** leer, gelten die Einstellungen für alle Benutzer. Nehmen Sie Benutzer über ihre Namen (nicht empfohlen) oder über Gruppen in das Feld auf, gelten die Einstellungen nur noch für diese.
- Nehmen Sie Benutzer über ihre Namen (nicht empfohlen) oder über Gruppen in das Feld **Exclude Users** auf, gelten die Änderungen in den Einstellungen für diese nicht.

Die Hauptaufgabe der Felder Include/Exclude besteht darin, es Administratoren zu ermöglichen, bestimmte Benutzer von Änderungen auszuschließen. Für ausgeschlossene Benutzer gelten nämlich die hartcodierten Vorgaben des Traveler-Servers, die den Anfangswerten der Vorgabe-Geräteeinstellungen entsprechen.

- Klicken Sie auf die Schaltfläche **Save and Close**.

Die Einstellungen in den Registern »Sync«, »Filter«, und »Device« werden nur bei der Erstregistrierung auf die Geräte übertragen. Sollten Sie danach Änderungen vornehmen, gelten diese nur für neue Geräte. Ausnahme sind die Sicherheitseinstellungen (alle im Register »Security«), welche immer übertragen werden.

Wollen Sie Vorgaben nachträglich ändern, müssen Sie zusätzlich die Option »Lock Value on Device« aktivieren. Wenn diese Option gesetzt ist, werden die Änderungen auf den Registern »Sync«, »Filter«, und »Device« wieder an alle Geräte geschickt, wo sie von den Benutzern nicht übersteuert werden können. Sollen Änderungen nur für bestimmte Benutzer oder Benutzergruppen gelten, erstellen Sie eine Traveler-Richtlinie.

15.6.1.2. Verwenden der Traveler-Richtlinie

Der Vorteil von Richtliniendokumenten besteht darin, dass Sie unterschiedlichen Benutzergruppen unterschiedliche Einstellungen zuordnen können.

Damit Sie auch die neuesten Einstellungen nutzen können, sorgen Sie dafür, immer die aktuellste Domino-Verzeichnisschablone einzusetzen!

Bevor Sie beginnen, stellen Sie sicher, dass Sie im Domino-Verzeichnis über die folgenden Rechte verfügen:

Editorzugriff so wie die Rollen [PolicyCreator] und/oder [PolicyModifier]

Um eine Traveler-Richtlinie zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Personen und Gruppen** und wählen Sie die Ansicht **Einstellungen**.
2. Klicken Sie auf **Einstellungen hinzufügen... > Notes Traveler**.
3. Vergeben Sie im Register **Allgemein** einen Namen und (optional) eine Beschreibung für die Richtlinie.
4. Wechseln Sie zu **Vorgaben > Synchronisieren** und wählen Sie zumindest einen Eintrag aus der Liste (E-Mail, Kalender, Kontakte, Aufgaben, Journal) sowie Optionen für Auto-Sync. Vergessen Sie nicht, für jede Einstellung in der Spalte **Wie diese Einstellung angewendet wird** zumindest »Anfangswert festlegen« auszuwählen.

Die Einstellungen gelten nicht für via Exchange ActiveSync angebundene iOS-Clients.

5. Wechseln Sie zum Register **Vorgaben > Filtereinstellungen** und setzen Sie die gewünschten Filter.

Die Einstellungen gelten nicht für via Exchange ActiveSync angebundene iOS-Clients.

6. Wechseln Sie zum Register **Vorgaben > Geräteeinstellungen** und wählen Sie die gewünschten Einstellungen aus.
7. Wechseln Sie zum Register **Vorgaben > Sicherheitseinstellungen** und dann zu den Unterregistern der von Ihnen verwendeten Geräte. Wählen Sie die gewünschten Einstellungen aus.
8. Wechseln Sie zum Register **Vorgaben > Gerätezugriff** und geben Sie an, ob für die Konfiguration von neuen Geräten eine Genehmigung notwendig sein soll. Sie können hier auch die Anzahl der Geräte pro Person limitieren.
9. Speichern und schließen Sie das Dokument.
10. Weisen Sie die Richtlinieneinstellung einer Richtlinie zu. Für mehr Informationen zum Thema Richtlinien lesen Sie Kap. 6.1 auf Seite 123.

Eine neu erstellte oder aktualisierte Traveler-Richtlinie wird vom Administrationsprozess alle sechs Stunden auf die Maildatenbanken übertragen. Wollen Sie die Änderungen per sofort übertragen, geben Sie auf der Serverkonsole des Mailservers den folgenden Befehl ein:

```
tell adminp process traveler
```

15.6.2. Wie Vorgaben gesetzt werden

Wenn sich ein mobiles Gerät zum ersten Mal am Traveler-Server registriert, entsprechen die Geräteeinstellungen der vom Administrator festgelegten Richtlinie. Wenn für einen Benutzer keine Richtlinie existiert, werden die Vorgabe-Einstellungen aus der Traveler-Datenbank (LotusTraveler.nsf) verwendet. Wenn für einen Benutzer eine Traveler-Richtlinie existiert, haben die Einstellungen aus der Richtlinie gegenüber den Vorgaben aus der Traveler-Datenbank Vorrang. Ausgenommen sind Einstellungen, die in der Richtlinie fehlen, etwa, weil ein älteres Verzeichnisdesign zur Anwendung kam oder die Option »Wert nicht festlegen« ausgewählt wurde.

Nach Abschluss der Registrierung werden die mobilen Geräteeinstellungen als verstecktes Geräteprofil in der Maildatenbank des Benutzers gespeichert. Wenn der Benutzer später ein neues Gerät registriert, dann kommen die Gerätevorgaben von der aktuellen Richtlinie aus der Maildatenbank des Benutzers.

15.6.3. Geräte löschen oder zurücksetzen

Verwenden Sie auch zum Löschen oder Zurücksetzen von Geräten ausschließlich Konsolenbefehle. Die Syntax zum Löschen eines Geräts lautet:

```
tell traveler delete <Gerät> <Benutzer>
```

Die Syntax zum Zurücksetzen eines Geräts lautet:

```
tell traveler reset <Gerät> <Benutzer>
```

Gelöschte Geräte werden nach dem Löschen in der Ansicht »Devices« nicht mehr angezeigt, in der Ansicht »Device Security« jedoch noch bis zu 30 Tage. Die Sicherheitsdaten für gelöschte Geräte werden für 30 Tage aufgehoben, damit:

- > eine Liste der gelöschten Geräte über die Traveler Web Administration Console oder das Traveler Administration REST API abgefragt werden kann,
- > genügend Zeit für das Beenden von Sicherheitsaktionen bleibt.

Diese Frist kann über die notes.ini-Variable NTS_ADMIN_CLEANUP_TIMEOUT auch verkürzt und sogar auf 0 gesetzt werden; bei 0 werden die Daten nach dem Löschen sofort entfernt. Ansonsten gilt: Die Daten werden erst entfernt, wenn innerhalb der gesetzten Frist keinerlei neue Geräteaktivität erfolgt.

15.6.4. Entferntes Löschen

Wenn ein Mobiltelefon verloren geht oder gar gestohlen wird, können sowohl der Besitzer als auch der Administrator ein **entferntes Löschen** (Remote Wipe) aller sensiblen Daten auf dem Gerät anfordern. Sie können die Traveler-Anwendung und ihre Daten vom Gerät löschen und, abhängig vom Gerät, dieses sogar auf die Werkseinstellungen zurücksetzen.

15.6.4.1. Allgemeine Überlegungen zum entfernten Löschen

Der Löschbefehl wird ausgeführt, wenn sich das Gerät das nächste Mal verbindet. Wenn sich das Gerät nicht mehr verbindet, aber eine SMS-Adresse verfügbar ist, wird das Endgerät via SMS aufgefordert, sich am Server anzumelden, oder, wenn auch das nicht möglich ist, den Löschbefehl direkt zu akzeptieren. Nach dem Löschen ist das Gerät gesperrt und kann sich auch nach einem erneuten Installieren der Verse-App nicht mehr verbinden.

Achtung: Nehmen Sie den Benutzer nicht in eine Gruppe ohne Zugriff auf, bevor Sie das Gerät zurückgesetzt haben, da sich das Gerät zum entfernten Löschen einmalig mit dem Server verbinden muss.

15.6.4.2. Besonderheiten verschiedener Endgeräte

Was Remote Wipe im Einzelnen bewirkt, hängt vom Endgerät, seinem Betriebssystem und einer möglicherweise auf dem Gerät installierten MDM-Software (Mobile Device Management) ab.

Auf Android-Geräten wird das entfernte Löschen nur unterstützt, wenn der Geräteadministrator aktiv ist. Das ist nur der Fall, wenn Einstellungen vorgenommen wurden, die das benötigen, so wie »Gerätekenntwort erforderlich«, »Kamera verbieten (nur OS 4+)«, oder »Geräte verbieten, die keine Sicherheitsmaßnahmen unterstützen«.

Auf Apple-Geräten wird nur das Entfernen der Traveler-Anwendung und ihrer Daten unterstützt, nicht aber das Zurücksetzen via SMS.

BlackBerry 10-Geräte unterstützen das entfernte Löschen nur, wenn sie direkt an einen Traveler angebunden sind und nicht von einem BlackBerry Enterprise Service verwaltet werden.

Via Exchange ActiveSync angebundene Geräte unterstützen ein entferntes Löschen, das Gerät muss sich jedoch verbinden, damit es durchgeführt wird. Dabei werden alle Traveler-Daten wie Kalender- und Kontaktinformationen genauso gelöscht wie Mailordner samt Inhalt. Der Benutzerzugriff wird dabei nicht beschränkt, aber wenn das Gerät zu synchronisieren versucht, wird die Verbindung verweigert.

15.6.4.3. Entferntes Löschen durch den Administrator

1. Öffnen Sie die Traveler Administrationsdatenbank (LotusTraveler.nsf – nur auf Englisch verfügbar).
2. Navigieren Sie zur Ansicht **Device Security**.
3. Wählen Sie das Gerät aus.
4. Klicken Sie auf die Schaltfläche **Wipe Device** und wählen Sie eine der Optionen:
 - **Hard Reset Device** – setzt das Gerät auf seine Werkseinstellungen zurück und entfernt die Traveler-Anwendung und alle PIM und Maildaten.
 - **HCL Traveler Application and Data** – entfernt die Traveler-Anwendung und alle PIM und Maildaten.
 - **Storage Card** – Diese Option entfernt alle Daten, die auf einer Speicherkarte auf dem Gerät gespeichert wurden.

Die Administrationsdatenbank verfügt über ein ansprechendes, auf XPages basierendes Interface, über welches die meisten Aktionen auch im Webbrowser ausgeführt werden können. Sie erreichen die Datenbank unter der Adresse:

<https://IhrServer.de/lotustraveler.nsf>

15.6.4.4. Entferntes Löschen durch den Besitzer

Der Besitzer des Geräts kann das entfernte Löschen über die Traveler Homepage anfordern.

Dazu muss sich dieser auf der Traveler Homepage (www.IhrServer.de/traveler) anmelden und auf den Link **Befehle ausführen** klicken.

Auf der darauf angezeigten Seite muss der Besitzer im Bereich **Befehle für das Gerät** die Option **Löschen** anklicken:

Traveler

Benutzerbefehle für Christian Buchacher/COB/AT

[Benutzer](#)
Zeigt alle Informationen zu einem Benutzer und den Geräten des Benutzers an

[Auszug](#)
Schreibt die Informationen für einen Benutzer in eine Datei auf dem Server

Befehle für das Gerät

Gerät samsung SM-N960F mit der Geräte-ID Android_a5bb80f65d86db66

[Löschen](#)
Traveler-Daten für das Gerät löschen

[Zurücksetzen](#)
Zurücksetzen der Synchronisation für das Gerät erzwingen

[Synchronisation stoppen](#)
Stoppt jede aktive Synchronisation für das Gerät

Abbildung 15.13: Traveler-Webseite mit Benutzerbefehlen

15.6.5. Ein Remote Wipe zurücknehmen

Wenn ein vermeintlich verloren gegangenes Gerät wiedergefunden wird, wollen Sie die Sperre des Geräts wahrscheinlich aufheben.

15.6.5.1. Über die Datenbank Traveler-Administration

Öffnen Sie die Datenbank Traveler-Administration (LotusTraveler.nsf) und wählen Sie die Ansicht **Device Security**.

Wählen Sie das Gerät, für das Sie die Sperre aufheben wollen.

Wählen Sie den Befehl **Undo Wipe/Allow Access**.

15.6.5.2. Über die Serverkonsole

Zum Entsperren des Geräts auf der Serverkonsole benötigen Sie entweder die sogenannte Device-ID oder Sie geben einen Stern (*) an, um die Sperre für alle dem Benutzer zugeordneten Geräte aufzuheben:

```
tell traveler security flagsRemove all <Gerät> <Benutzer>
```

Tipp: Wenn Sie die Geräte-ID nicht wissen, können Sie diese über folgenden Befehl in Erfahrung bringen:

```
tell traveler show <Benutzer>
```

z. B.: `tell traveler show "Franz Meier/COB/AT"`

15.7. Das Traveler-Protokoll

Der HCL Traveler verwendet ein eigenes Protokoll im Verzeichnis:

```
\IBM_TECHNICAL_SUPPORT\traveler\logs
```

Darin befinden sich vier Textdateien mit Namen im Format NTS*_YYMMDD_HHMMSS.log, wobei YYMMDD_HHMMSS für das Erstellungsdatum steht:

- > NTSErrors enthält alle Fehler, die am HCL Traveler aufgetreten sind, mit der Protokollierungsstufe SEVERE.
- > NTSAudit enthält Systemänderungen wie Konfigurationsänderungen (im Serverdokument, der Datei notes.ini etc.) sowie Statusänderungen. Alle Einträge entsprechen der Protokollierungsstufe USAGE.
- > NTSUsage enthält alle Informationen aus NTSAudit, plus einen Eintrag pro Transaktion pro Gerät. Diese Informationen erlauben es dem Administrator, genau zu sehen, wer wann und wie lange synchronisiert hat und ob dabei Fehler aufgetreten sind.
- > NTSActivity enthält alle Informationen aus NTSErrors, NTSAudit, NTSUsage, plus alle übrigen protokollierten Angaben. Die Datei NTSActivity enthält also das vollständige Protokoll.

Sie können die Traveler-Protokolldateien nicht via Domino-Administrator einsehen, sondern benötigen direkten Zugriff auf das Dateisystem des Traveler-Servers und einen Texteditor.

Wie genau die Protokollierung erfolgt, kann eingestellt werden, der Traveler kennt die Protokollierungsstufen SEVERE, WARNING, INFO, FINE, FINER und FINEST. Mit der Einstellung SEVERE werden nur Fehler protokolliert, mit FINEST so ziemlich alles. Die Vorgabe-Protokollierungsstufe ist INFO, was üblicherweise einen guten Kompromiss zwischen der Menge an protokollierten Informationen und der Größe der Protokolldateien darstellt. HCL Traveler kennt außerdem die benutzerdefinierte Stufe USAGE.

Zum Einstellen der Stufe setzen Sie auf der Serverkonsole den folgenden Befehl ab:

```
tell traveler log level <Stufe>
```

Wenn die maximale Protokollgröße erreicht ist, wird die aktuelle Datei gezippt und eine neue erstellt. Zusätzlich gibt es für jeden Dateisatz eine Obergrenze, was die Anzahl als auch Alter der Dateien betrifft. Wenn entweder die Anzahl oder das maximale Alter erreicht ist, wird die älteste Datei gelöscht. Wenn Sie alle Ereignisse z. B. 30 Tage zurückverfolgen wollen, können Sie etwa die Einstellung für die Anzahl sehr hoch setzen und das maximale Alter auf 30 Tage.

Wenn ein Benutzer in der Stufe FINEST protokolliert wird, erstellt der Traveler außerdem eine XML-Repräsentation aller HTTP-Nachrichten, die zu und von den betroffenen Geräten geschickt werden. Diese kann im Verzeichnis \IBM_TECHNICAL_SUPPORT\traveler\logs\xml gefunden werden und verwendet ein ähnliches Rotationssystem wie die NTS*.log-Dateien. Aufgrund der großen Datenmengen wird die extra Protokollierung mit FINEST spätestens nach 14 Tagen wieder aufgehoben. (Diese Frist kann durch die notes.ini-Einstellung NTS_LOG_USER_EXPIRATION verändert werden.)

Die Protokollstufe kann auch nur für einen einzelnen Benutzer hochgesetzt werden:

```
tell traveler log adduser <Stufe> <Benutzer>
```

Wenn ein Benutzer in der Stufe FINEST protokolliert wird, erstellt der Traveler außerdem eine XML-Repräsentation aller HTTP-Nachrichten, die zu und von den betroffenen Geräten geschickt werden. Diese kann im Verzeichnis `\IBM_TECHNICAL_SUPPORT\traveler\logs\xml` gefunden werden und verwendet ein ähnliches Rotationssystem wie die `NTS*.log`-Dateien.

Aufgrund der großen Datenmengen wird die extra Protokollierung mit FINEST spätestens nach 14 Tagen wieder aufgehoben. Diese Frist kann durch folgende `notes.ini`-Einstellung verändert werden:

`NTS_LOG_USER_EXPIRATION`

Wenn es Probleme mit einem bestimmten Benutzer gibt, können Sie z. B. die folgenden Befehle absetzen:

```
tell traveler log adduser finest "Franz Meier/COB/AT"  
tell http debug thread on  
tell traveler log fields *
```

Und um das Protokoll einzusammeln und an den HCL Customer-Support zu schicken:

```
tell traveler dump <Benutzer>  
tell traveler systemdump  
tell traveler log collect
```

Der letzte Befehl erstellt eine Zip-Datei. Der Name der Datei wird auf der Konsole angegeben.

Und mit dem folgenden Befehl ist der ganze Spuk wieder vorbei:

```
tell traveler log removeuser <Benutzer>  
tell http debug thread off
```

15.8. Die Derby-Datenbank

Der Traveler verwendet eine relationale Datenbank, um Informationen über Geräte, Sicherheit (Sperrungen!) und Konfigurationen sowie Meta-Daten für die Synchronisierung zu speichern. Per Vorgabe wird dazu eine Derby-Datenbank verwendet, die im Domino-Datenverzeichnis unter `\traveler\ntsdb` liegt. Veranschlagen Sie hierfür bei ein paar hundert Benutzern 3 bis 4 GB Speicherplatz.

Es gibt auch die Möglichkeit, eine HA- (High Availability) Variante des Travelers zu installieren, bei der die Derby-Datenbank gegen ein leistungsfähigeres RDBMS ausgetauscht wird. Unterstützt werden zurzeit IBM DB2, Microsoft SQL-Server und MySQL. Die HA-Variante des Travelers wird in diesem Buch nicht behandelt.

Die Derby-Datenbank ist nicht sehr wartungsintensiv, eine regelmäßige Defragmentierung (mind. einmal pro Monat) sollte ausreichen, um eine gute Performance aufrechtzuerhalten. Sie können die Datenbankgröße selbst überwachen und bei Bedarf manuell defragmentieren oder automatisch nach einem Zeitplan defragmentieren.

15.8.1. Die Datenbank manuell defragmentieren

Die Datenbank im Verzeichnis \traveler\ntsdB wächst im laufenden Betrieb je nach Aktivität mehr oder weniger stark, was sich irgendwann negativ auf die Performance auswirkt. Deshalb sollten Sie die Datenbank von Zeit zu Zeit defragmentieren – in der Regel zwischen einmal pro Monat und einmal alle 2 bis 3 Monate.

Die Defragmentierung kann nur beim Start wie unten beschrieben ausgeführt werden. Zusätzlich wird eine automatische Defragmentierung bei jedem Upgrade auf eine neuere Version durchgeführt.

Achtung: Löschen Sie niemals den Ordner traveler\ntsdB. Die Datenbank wird zwar beim nächsten Start neu erstellt, jedoch gehen alle Sicherheitsinformationen (Gerätesperren nach einem entfernten Löschen etc.) verloren und alle Anwender werden zu einer Neusynchronisation ihrer Geräte gezwungen.

Um eine manuelle Defragmentierung auszuführen, gehen Sie wie folgt vor:

1. Beenden Sie die Tasks Traveler und HTTP auf Ihrem Domino-Server:

```
tell traveler quit
```

```
tell http quit
```
2. Starten Sie nach dem Herunterfahren den Traveler mit dem Parameter -defrag:

```
load traveler -defrag
```
3. Der Traveler führt die Defragmentierung aus und startet dann ganz normal.
4. Wenn der Traveler nicht dafür konfiguriert wurde, den HTTP-Task automatisch zu starten (siehe Kap. 15.3, ab Seite 423), starten Sie ihn manuell mit dem Befehl:

```
load http
```

Achtung: Die Defragmentierung kann je nach Größe der Datenbank 30 Minuten oder länger dauern!

15.8.2. Die Datenbank nach Zeitplan defragmentieren

Um eine Defragmentierung nach Zeitplan auszuführen, gehen Sie wie folgt vor:

Verwenden Sie den Befehl `DBMaint set interval`, um ein Intervall zu setzen. Geben Sie etwa für eine Defragmentierung alle 30 Tage auf der Serverkonsole folgenden Befehl ein:

```
tell traveler dbmaint set interval 30
```

Verwenden Sie den Befehl `DBMaint set auto`, um eine automatische Defragmentierung zu aktivieren:

```
tell traveler dbmaint set auto
```

Um eine sofortige Defragmentierung zu erzwingen, geben Sie folgenden Befehl ein:

```
tell traveler dbmaint run
```

Das setzt die Variable `NTS_DEFrag_ONCE=1` und die Derby-Datenbank wird beim nächsten Neustart des Travelers defragmentiert.

16. Domino-Cluster

- > 16.1 Was ist ein Cluster?, Seite 435
- > 16.2 Einen Cluster einrichten, Seite 437
- > 16.3 Lastverteilung einrichten, Seite 442
- > 16.4 Symmetrische Cluster, Seite 445

16.1. Was ist ein Cluster?

Ein Domino-Cluster besteht aus einer Gruppe von zwei oder mehreren Servern, die bestimmte Datenbankrepliken in hoher Frequenz miteinander abgleichen. Der Abgleich geschieht mithilfe der **Cluster-Replikation**, die ereignisgesteuert funktioniert: Wird auf einem Server ein Dokument hinzugefügt, geändert oder gelöscht, wird dieses (im Idealfall) in Sekundenbruchteilen zu den anderen Cluster-Mitgliedern (auch als Knoten bezeichnet) übertragen, sodass die Informationen in den einzelnen Repliken stets identisch sind. Versucht ein Benutzer, auf eine Ressource auf einem ausgefallenen Server zuzugreifen, wird er automatisch auf ein anderes Cluster-Mitglied umgeleitet (**Ausfallsicherheit**). Zusätzlich kann auch eine **Lastverteilung** (Load Balancing) eingerichtet werden, bei der die **Umleitung** (Failover) auch bei starker Auslastung erfolgt. Dies funktioniert allerdings nur für Notes-Clients, andere Clients (z. B. Webbrowser) bleiben außen vor.

Bei einem Domino-Cluster handelt es sich um eine proprietäre Domino-Lösung, die nichts mit einem Windows-Cluster zu tun hat. In einem Domino-Cluster können verschiedene Versionen von Domino-Servern (z. B. 9, 10 und 11) auf verschiedenen Plattformen (z. B. Windows und Linux) miteinander verbunden werden. Achten Sie jedoch auf die Serverlizenz: Cluster sind nur bei Domino Enterprise und Utility Servern möglich, nicht aber bei Messaging Servern.

Nachfolgend die Eigenschaften im Detail:

Hohe Verfügbarkeit

24 / 7 / 365 ist heute die Devise. Service Level Agreements mit einer Verfügbarkeit von 99+ % sind keine Seltenheit. Diese wahnwitzigen Werte können nur noch mithilfe von Clustern erreicht werden: Der Prozess des Umleitens (Failover) zu einem anderen Server im Cluster bei Nichtverfügbarkeit gewährleistet einen kontinuierlichen Datenzugriff. Dies beinhaltet auch das Failover von Durchgangsservern zu anderen Mitgliedern des Clusters. Das Failover ermöglicht es Ihnen auch, Server während der Arbeitszeit zu Wartungsarbeiten herunterzufahren, ohne dass die Benutzer es bemerken.

Lastverteilung

Wenn Benutzer versuchen, auf Datenbanken stark frequentierter Server zuzugreifen, werden die Anforderungen an weniger frequentierte Cluster-Server umgeleitet, sodass die Belastung

gleichmäßig im Cluster verteilt wird. Die Lastverteilung kann basierend auf der Auslastung oder der Benutzeranzahl konfiguriert werden.

Skalierbarkeit

Wenn die Anzahl der Benutzer zunimmt, können Sie Server zum Cluster hinzufügen, um eine hohe Serverleistung aufrechtzuerhalten. Sie können zudem Benutzer auf andere Server im Cluster verschieben, um eine gleichmäßige Verteilung und somit Belastung der einzelnen Server aufrechtzuerhalten.

Datensicherheit

Da Sie von jeder unternehmenskritischen Datenbank über mehrere Repliken auf mehreren Cluster-Servern verfügen, können Sie verlorene oder korrupte Daten leichter wiederherstellen. Sie können außerdem einen Server im Cluster als »Backup-Server« einrichten, auch über ein WAN, sodass Sie über einen aktuellen Datenbestand an einem anderen geografischen Standort verfügen. Dazu können Sie Benutzern den Zugriff auf diesen Server auch verweigern.

Cluster-Typen

Bei **Active-Active-Clustern** sind alle Knoten aktiv: Die gewählte Kachel entscheidet, auf welchem Server der Anwender arbeitet. Active-Active-Cluster sind die erste Wahl für Applikationsserver.

Bei **Active-Passive-Clustern** ist nur ein Server aktiv, der andere übernimmt nur bei einem Ausfall. Diese Lösung ist typisch für einen Mail-Cluster.

Cluster-Replikation

Innerhalb des Clusters wird eine **Streaming-Cluster-Replikation (SCR)** verwendet, welche weniger Overhead und eine geringere Latenz aufweist als die klassische (zeitplangesteuerte) Replizierung. SCR ist eine Push-Replikationsmethode, die Änderungen auf dem lokalen Server erfasst und sie auf andere Repliken innerhalb des Clusters überträgt. SCR findet aus Performancegründen im Hauptspeicher statt.

Einmal pro Minute speichert SCR seinen aktuellen Status in der Datei `scrstate.dat` im Datenverzeichnis. Wenn der Server heruntergefahren und neu gestartet wird, liest SCR die Datei `scrstate.dat`, um den Status vor dem Neustart zu ermitteln:

```
19.04.2021 10:02:25 RestoreSCRState: Starting SCR restore at 19.04.2021 10:02:25
19.04.2021 10:02:25 RestoreSCRState: Finished SCR restore at 19.04.2021 10:02:25
19.04.2021 10:02:25 RestoreSCRState: Input Lines = 5, Destinations Restored = 2
```

Ähnlich wird verfahren, wenn ein entfernter Server nicht mehr verfügbar ist. Wenn SCR feststellt, dass ein Cluster-Mitglied fehlt, speichert es die Änderungen, die für diesen Server bestimmt sind, bis zu 20 Minuten in der SCR-Warteschlange.

Wenn der andere Cluster-Server startet, findet ein Abgleich statt:

```
19.04.2021 10:01:54 ClientSCRDestHandler: Starting wait for server CN=WS01/O=COB/C=AT to
restart at 19.04.2021 10:01:54
19.04.2021 10:01:54 ClientSCRDestHandler: Connection re-established to server
CN=WS01/O=COB/C=AT at 19.04.2021 10:01:54
```

Klassische (zeitplangesteuerte) Replikation

Zusätzlich zur Cluster-Replikation sollten Sie immer auch eine zeitplangesteuerte Replikation konfigurieren. Und zwar aus den folgenden Gründen:

- > Wenn ein Server ausfällt, können Änderungen verloren gehen, da die Cluster-Replikation ja ausschließlich im Speicher erfolgt ist. Dabei kommt es zu keinem Datenverlust, da die anderen Server ja über alle Informationen verfügen, aber zu einer Inkonsistenz, die erst durch eine Standard-Replikation korrigiert wird.
- > Damit Datenbanken, für die Sie die Cluster-Replikation deaktiviert haben, repliziert werden.
- > Damit Datenbanken basierend auf selektiven Replikationsformeln repliziert werden.
- > Damit Repliken auf demselben Server repliziert werden. Der Cluster-Replikator überträgt Änderungen auf Repliken auf anderen Servern aber nicht auf denselben Server.
- > Zum Vervollständigen von Replikrumpfen

Wenn auf einem Server mehrere Repliken vorhanden sind, verwendet der Cluster-Manager das Failover nach Pfad, um die Replik auszuwählen, die ein Benutzer während des Failovers öffnen soll. Wenn Sie mehrere Repliken auf einem Server ablegen, stellen Sie daher sicher, dass alle Repliken im Cluster mit demselben Pfad dieselben selektiven Replikationsformeln verwenden. Andernfalls enthält die Replik, auf die Benutzer ein Failover durchführen, möglicherweise andere Daten als erwartet.

16.2. Einen Cluster einrichten

Das Einrichten eines Clusters ist einfach, da der Großteil der Konfiguration im Hintergrund vom Administrationsprozess erledigt wird. Auch das Hinzufügen von Servern zu einem bestehenden Cluster (oder Entfernen von Servern aus demselben) ist ohne großen Aufwand möglich. Nach dem Erstellen müssen Sie angeben, welche Datenbanken abgeglichen (repliziert) werden. (Sollten nicht alle Cluster-Mitglieder über Repliken der gewünschten Datenbanken verfügen, müssen Sie diese zuerst erstellen.) Der letzte Schritt ist die Optimierung des Clusters, bei der Sie zahlreiche Tools unterstützen.

16.2.1. Voraussetzungen

Überprüfen Sie vor dem Einrichten des Clusters folgende Voraussetzungen:

- > Alle Cluster-Mitglieder sind Server vom Lizenztyp Enterprise oder Utility.
- > Alle Cluster-Mitglieder befinden sich innerhalb derselben Domino-Domäne (keine Replikierung über Verbindungsdokumente).
- > Alle Cluster-Mitglieder befinden sich innerhalb desselben Benannten Domino-Netzwerks. (Für mehr Informationen lesen Sie Kap. 3.4.2 Benannte Notes-Netzwerke, ab Seite 30.)
- > Alle Clustermitglieder stammen vom selben Zertifizierer ab.

Bedenken Sie, dass Sie zwar verschiedene Domino-Versionen mischen können, einige Funktionen (z. B. Symmetrische Cluster) aber erst ab Domino 10 zur Verfügung stehen.

Achten Sie weiters darauf, dass für die Cluster-Replizierung mehr Speicher und eine höhere Prozessorleistung erforderlich sind. Sind Ihre Server nicht mit GB-Netzwerkkarten ausgestattet, überlegen Sie die Anschaffung einer schnelleren oder auch einer zusätzlichen Netzwerkkarte.

16.2.2. Vorgangsweise

1. Wechseln Sie im Domino-Administrator zum Register **Konfiguration**.
2. Erweitern Sie im Navigationsbereich die Kategorie **Server** und wählen Sie die Ansicht **Alle Serverdokumente**.
3. Wählen Sie die Server aus, die Sie zum neuen Cluster hinzufügen möchten.
4. Klicken Sie auf die Schaltfläche **Zum Cluster hinzufügen**.

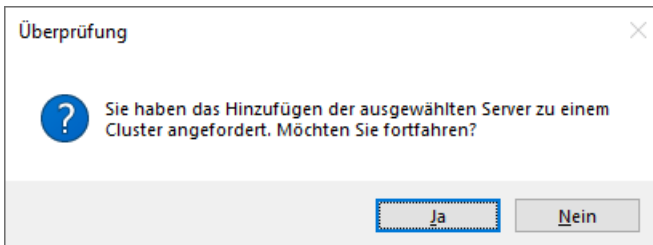


Abbildung 16.1: Bestätigung Hinzufügen zu einem Cluster

5. Wählen Sie im Dialogfeld Clustername die Option »*Neuen Cluster erstellen« und klicken Sie auf **OK**.

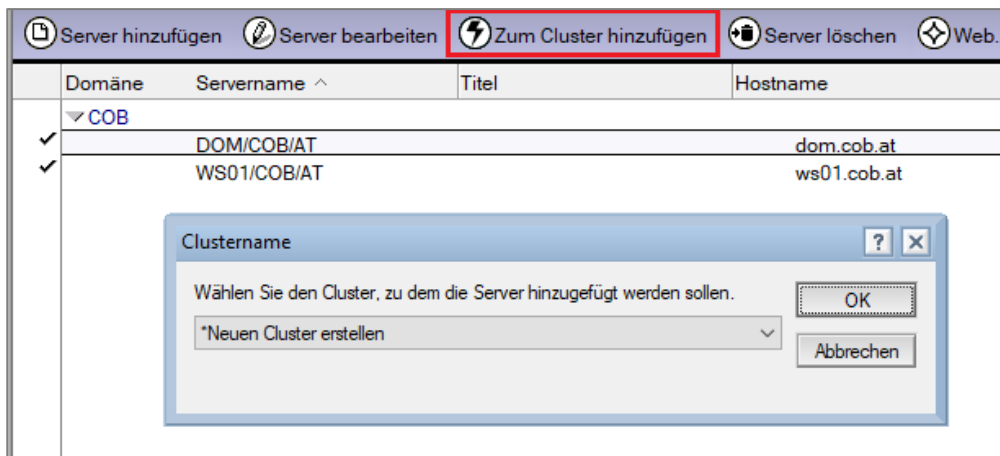


Abbildung 16.2: Zum Cluster hinzufügen

6. Geben Sie jetzt den Namen für den neuen Cluster ein und klicken Sie auf **OK**:

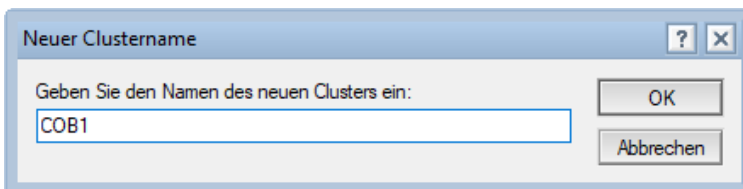


Abbildung 16.3: Dialog Neuer Cluster-Name

7. Wählen Sie »Ja«, um die Server sofort zum Cluster hinzuzufügen, oder »Nein«, um eine Anforderung an den Administrationsprozess zu erstellen, der die Server dann im Hintergrund zum Cluster hinzufügt:

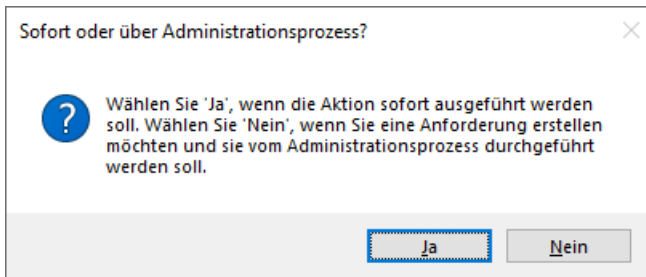


Abbildung 16.4: Abfrage sofortige Cluster-Erstellung

8. Sie erhalten eine Erfolgsmeldung:

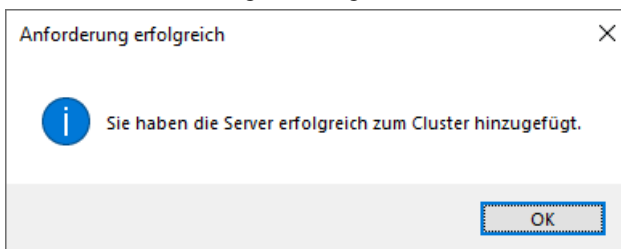


Abbildung 16.5: Erfolgsmeldung Cluster-Erstellung

9. (Optional) Wenn Sie in Schritt 7 »Nein« ausgewählt und die Server nicht auf dem Administrationsserver des Domino-Verzeichnisses hinzugefügt haben, erzwingen Sie eine Replikation zwischen dem von Ihnen verwendeten Server und dem Administrationsserver, damit dieser die angeforderten Änderungen sofort erhält.
10. (Optional) Wenn Sie in Schritt 7 »Nein« ausgewählt haben, erzwingen Sie die Replikation zwischen dem Administrationsserver und den Clusterservern, damit die Clusterserver alle Änderungen sofort erhalten.
11. (Optional) Wenn Sie in Schritt 7 »Ja« gewählt haben, werden die Cluster-Informationen sofort zum Domino-Verzeichnis auf dem Server hinzugefügt, auf dem Sie den Cluster erstellt haben. Wenn dieser Server nicht Teil des neuen Clusters ist, replizieren Sie die Änderungen auf einen der Server, die Sie dem Cluster hinzugefügt haben.

Nach dem Einrichten setzt der Cluster-Manager die notes.ini-Variable `Server_Cluster_on=1` und startet die Servertasks **Cluster-Replikator** (clrepl) und **Cluster Database Directory Manager** (clbdbdir) auf allen Knoten. Solange der Cluster aktiv ist, starten diese Tasks automatisch und müssen nicht zur Datei notes.ini hinzugefügt werden.

Es wird jedoch nur ein Cluster-Replikator pro Server gestartet, was für einen Cluster aus zwei Knoten optimal ist. Besteht Ihr Cluster aus mehr als zwei Servern, sollten Sie nach der Formel $n = \text{Anzahl Cluster-Server} - 1$ zusätzliche Instanzen des Cluster-Replikators starten. Dies geschieht über den folgenden Eintrag in der Datei notes.ini:

```
cluster_replicators=n
```

Der Cluster Database Directory Manager erstellt ein Cluster-Verzeichnis (Cluster Directory, clbdbdir.nsf) und aktiviert die Cluster-Replikation für alle vorgefundenen Datenbanken.

Außerdem wird die Zeitplanungsdatenbank busytime.nsf in clubusy.nsf konvertiert.

16.2.3. Überprüfen, ob der Cluster korrekt eingerichtet ist

Erweitern Sie im Domino-Administrator im Register Konfiguration die Kategorie Cluster. Sie sollten den Namen des Clusters gefolgt von den Namen der einzelnen Cluster-Server sehen:

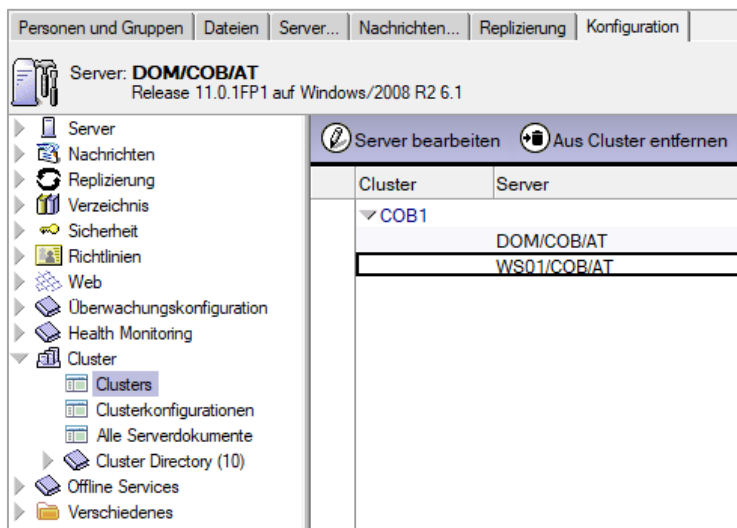


Abbildung 16.6: Der frisch erstellte Beispiel-Cluster COB1

Überprüfen Sie, ob eine Datenbank mit dem Title »Cluster Directory« auf jedem Cluster-Server vorhanden ist.

Geben Sie auf der Serverkonsole den folgenden Befehl ein:

```
>show cluster
```

Cluster information:

Cluster name: COB1, Server name: WS01/COB/AT

Server cluster probe timeout: 1 minute(s)

Server cluster probe count: 98

Server cluster default port: *

Server cluster auxiliary ports:

Server availability threshold: 0

Server availability index: 100 (state: AVAILABLE)

Server availability default minimum transaction time: 3000

Cluster members (2):

Server: WS01/COB/AT, availability index: 100

Server: DOM/COB/AT, availability index: 100

16.2.4. Einen eignen Cluster-Port einrichten

Sie sollten für die Cluster-Replizierung eine eigene IP-Adresse verwenden. Die Verwendung einer zusätzlichen Netzwerkkarte ist bei Vorhandensein einer Gigabit-Verbindung hingegen kein Muss.

Tragen Sie zunächst in der Datei notes.ini des Servers (oder im Konfigurationsdokument) den Standard-Notes-Port ein:

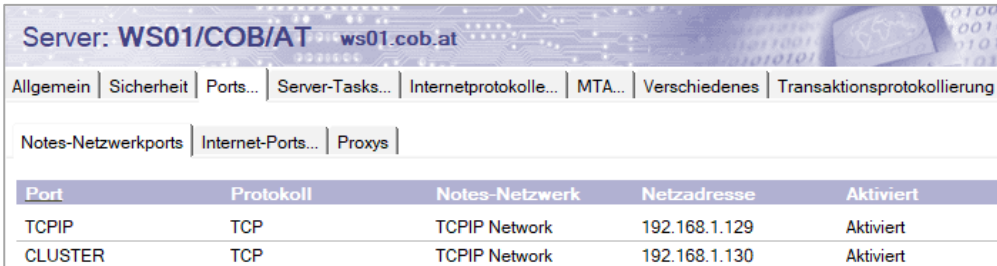
```
TCPIP_TcpIPAddress=0,192.168.1.129:1352
```

Tragen Sie dann den zusätzlichen Cluster-Port in die Datei notes.ini ein:

```
CLUSTER_TcpIPAddress=0, 192.168.1.130:1352
```

```
Server_Cluster_Default_Port=CLUSTER
```

Tragen Sie den zusätzlichen Port im Serverdokument ein:



Port	Protokoll	Notes-Netzwerk	Netzadresse	Aktiviert
TCPIP	TCP	TCPIP Network	192.168.1.129	Aktiviert
CLUSTER	TCP	TCPIP Network	192.168.1.130	Aktiviert

Abbildung 16.7: Serverdokument, Register Ports...

16.2.5. Das Cluster-Verzeichnis

Das Cluster-Verzeichnis (Cluster Directory, cldbdir.nsf – nur auf Englisch verfügbar) enthält Informationen über alle Datenbanken im Cluster und wird bei Serverausfällen dazu verwendet, um Repliken für Umleitungen (Failovers) zu finden.

Das Cluster-Verzeichnis wird durch den Task **Cluster Database Directory Manager** (cldbdir) gepflegt. Dieser nimmt nach dem Einrichten des Clusters jede Datenbank in das Verzeichnis auf und aktiviert die Cluster-Replizierung. Wollen Sie einzelne Datenbanken aus der Cluster-Replizierung ausnehmen, können Sie diese hier markieren und den Befehl **Tools > Disable Cluster Replication on Selected Databases** aufrufen:

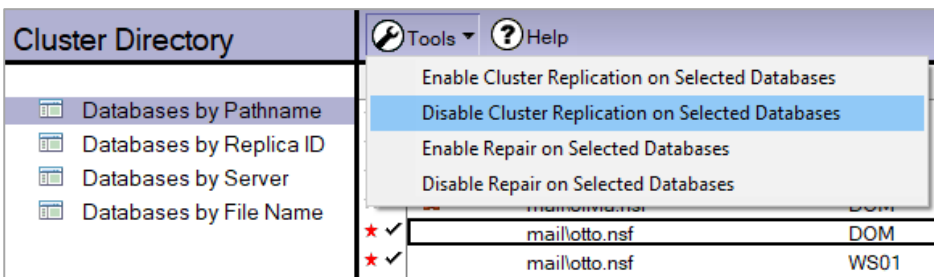


Abbildung 16.8: Cluster-Verzeichnis

Ich empfehle sogar, den Spieß umzudrehen und die Cluster-Replizierung zunächst für alle Datenbanken zu deaktivieren und dann nur für jene Datenbanken wieder einzuschalten, für die eine Umleitung erfolgen soll.

Überprüfen Sie, ob Datenbanken fehlen und die Cluster-Server in den ACLs der Datenbanken über ausreichende Rechte verfügen. Die beste Strategie ist hier, eine konsistente Zugriffskontrollliste über alle Repliken zu erzwingen. Ein Werkzeug, das Sie dabei unterstützt, ist die Cluster-Analyse.

Verbinden Sie sich dazu im Domino-Administrator mit einem beliebigen Cluster-Server und wählen Sie auf dem Register **Server** > **Analyse** das Werkzeug **Analyse** > **Cluster...**

Wählen Sie im angezeigten Dialog die Option »Datenbanken«:

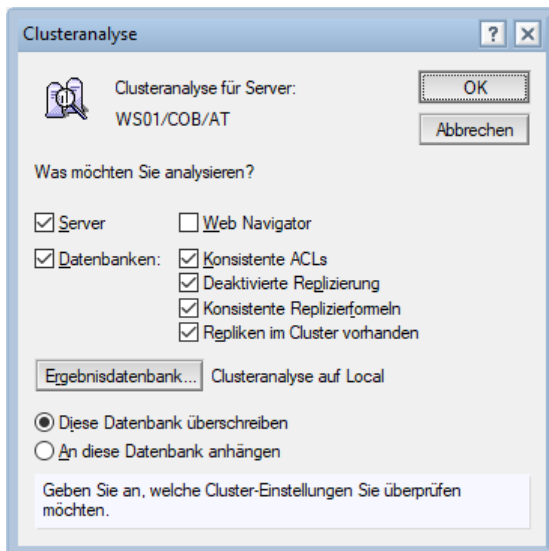


Abbildung 16.9: Der Dialog Clusteranalyse

16.3. Lastverteilung einrichten

Ziel einer Lastverteilung ist es, die Arbeitslast im Cluster so zu verteilen, dass kein Server überlastet wird. Dafür gibt es zwei Möglichkeiten: 1. die Angabe eines Verfügbarkeitschwellenwertes und 2. die Angabe einer Maximalzahl von Benutzern.

Setzen Sie ein Limit für die Auslastung eines Servers, markiert der Cluster-Manager, sowie der Verfügbarkeitschwellenwert erreicht ist, den Server als »belegt« (busy). Wenn ein Server ausgelastet ist, werden Anforderungen zum Öffnen von Datenbanken an andere Server gesendet, die Repliken der angeforderten Datenbanken enthalten.

Geben Sie stattdessen eine maximale Anzahl von Benutzern an, werden Benutzer, die auf den Server zugreifen möchten, beim Erreichen des Limits auf einen anderen Server umgeleitet.

Dazu sucht der Cluster-Manager im Cluster-Verzeichnis nach einer Replik der angeforderten Datenbank. Anschließend wird die Verfügbarkeit der Server überprüft, die eine Replik enthalten, und der Benutzer auf den am besten verfügbaren Server umgeleitet. Wenn kein anderer Cluster-Server eine Replik enthält oder wenn alle Cluster-Server ausgelastet sind, wird die ursprüngliche Datenbank geöffnet, obwohl der Server ausgelastet ist.

16.3.1. Lastverteilung über die Maximalzahl von Benutzern

Setzen Sie in der Datei notes.ini des Servers (oder im Konfigurationsdokument) die Variable:

```
Server_MaxUsers=n
```

Wobei n die Anzahl der Benutzer ist, ab der der Server in den Status »belegt« (busy) wechselt und neue Anfragen an einen anderen Server weiterleitet.

Sie können die Variable `Server_MaxUsers` mit jedem Domino-Server verwenden. Allerdings leiten beim Überschreiten der erlaubten Anzahl nur Server in einem Cluster Anforderungen an andere Server um. Server, die sich nicht in einem Cluster befinden, lehnen den Zugriff ab.

16.3.2. Lastverteilung über einen Verfügbarkeitsschwellenwert

Setzen Sie in der Datei `notes.ini` des Servers (oder im Konfigurationsdokument) die Variable:

```
Server_Availability_Threshold=n
```

Wobei *n* der Schwellenwert ist, ab dem der Server in den Status »belegt« wechselt und neue Anfragen an einen anderen Server weiterleitet.

Der **Server Availability Threshold** (SAT) basiert auf dem **Server Availability Index** (SAI), einem Wert zwischen 0 und 100. Ein SAI von 100 bedeutet, dass die Ressourcen des Servers zu 100 % verfügbar sind, ein SAI von 0, dass der Server komplett ausgelastet ist und keine Anfragen mehr entgegennehmen kann.

Bedenken Sie, dass der SAI immer nur eine Momentaufnahme zeigt, d. h. ein Wert von 70 zu Spitzenbelastungszeiten stellt üblicherweise kein Problem dar. Daher würde ich den SAT auf einen Wert zwischen 72 und 80 einstellen.

16.3.3. Wie die Client-Umleitung funktioniert

Im Datenverzeichnis des Notes-Clients befindet sich die Datei `cluster.ncf`, welche Informationen über Cluster-Server bereitstellt. Hier ein Beispiel:

```
Time=18.04.2021 19:52:08 (C12586BB:00622881)
COB1
CN=DOM/O=COB/C=AT
CN=WS01/O=COB/C=AT
```

Die Datei `cluster.ncf` wird bei jedem Zugriff auf einen der Cluster-Server automatisch aktualisiert.

Wenn ein Client die Verbindung zu einem Server verliert, wird der Anwender per Vorgabe gefragt, ob sich der Notes-Client mit einem anderen Server verbinden soll. Sie können aber auch einstellen, dass sich der Client automatisch und ohne Rückfrage verbindet. Dies bewerkstelligen Sie am besten in der Desktoprichtlinie, Register Mail, im Bereich **Client-Einstellungen**:

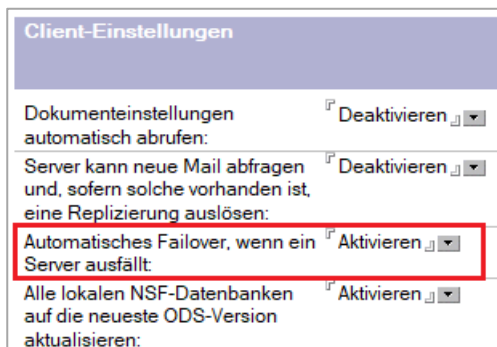


Abbildung 16.10: Desktoprichtlinie, Client-Einstellungen

Vergessen Sie nicht, auch das Häkchen aus dem Feld **Wert nicht festlegen** zu entfernen!

16.3.4. Zugriff auf einen Cluster-Server beschränken

Ein weiterer Vorteil des Clusters besteht darin, dass man einen Server aus Wartungsgründen jederzeit offline nehmen kann. Um Benutzer am Zugriff auf einen Server zu hindern, setzen Sie in der Datei notes.ini des Servers eine der folgenden Variablen:

Server_Restricted=1

- > Es können keine neuen Benutzersitzungen eröffnet werden.
- > Existierende Benutzersitzungen bleiben erhalten (und können von Ihnen durch den Befehl drop all beendet werden).
- > Administratoren können sich weiterhin mit dem gesperrten Server verbinden.
- > Der beschränkte Server kann Replikationen mit anderen Servern initiieren, akzeptiert aber keine Anfragen von anderen Servern.
- > Der beschränkte Server kann Mails an andere Server weiterleiten, akzeptiert aber keine Mails von anderen Servern.
- > Nach Neustart des Servers ist die Beschränkung aufgehoben.

Server_Restricted=2

- > Weist alle Eigenschaften der Variable Server_Restricted=1 auf.
- > Der Serverzugriff ist dauerhaft beschränkt und wird auch durch einen Neustart nicht aufgehoben.

Server_Restricted=3

- > Weist alle Eigenschaften der Variable Server_Restricted=1 auf.
- > Blockt alle Replikationen, die nicht von einer Administrator-ID kommen.
- > Nach Neustart des Servers ist die Beschränkung aufgehoben.

Server_Restricted=4

- > Weist alle Eigenschaften der Variable Server_Restricted=3 auf.
- > Der Serverzugriff ist dauerhaft beschränkt.

16.3.5. Mail-Routing im Cluster konfigurieren

Wenn der Router versucht, eine Mail zuzustellen und der Mailserver des Empfängers ist nicht verfügbar, übermittelt der Router die Mail an einen anderen Cluster-Server, der eine Replik der Maildatenbank des Empfängers enthält. Somit empfängt der Empfänger weiterhin E-Mails.

Standardmäßig wird das Mail-Routing nur für den letzten Hop der Übermittlungsrouten ausgeführt. Das heißt, es wird ein Failover für den Hop zum Mailserver des Benutzers durchgeführt, wenn sich der Mailserver des Benutzers in einem Cluster befindet. Sie können das Mail-Routing so konfigurieren, dass es bei jedem Hop auf der Übermittlungsrouten ein Failover durchführt, oder Sie können das Failover für das Mail-Routing vollständig deaktivieren.

Wenn Sie das Mail-Routing so konfigurieren, dass bei jedem Hop ein Failover durchgeführt wird und ein Server entlang der Route nicht verfügbar ist, sich jedoch in einem Cluster befindet, wird das Mail-Routing auf einen Cluster-Server übertragen, und dieser Server leitet die Nachricht weiter. Das Aktivieren des Mail-Routing-Failovers für jeden Hop ist besonders hilfreich, wenn Sie einen Hub-Server zum Weiterleiten von E-Mails verwenden. Wenn dieser Hub-Server nicht verfügbar ist, sich

jedoch in einem Cluster befindet, übermittelt der Router die E-Mails an einen anderen Hub-Server im Cluster. Dieser Hub-Server sendet die Nachricht weiterhin an sein Ziel.

Um ein sofortiges Failover für das Mail-Routing zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Domino-Administrator zum Register Konfiguration.
2. Erweitern Sie die Kategorie **Server** und wählen Sie die Ansicht **Konfigurationen**.
3. Wählen Sie das gewünschte Konfigurationsdokument und klicken Sie auf **Konfiguration bearbeiten**.
4. Navigieren Sie zum Register **Router/SMTP > Erweitert... > Steuerung**.
5. Wählen Sie im Feld Cluster-Failover die Option »Für alle Übertragungen in dieser Domäne aktiviert«.
6. Speichern und schließen Sie das Konfigurationsdokument.

16.4. Symmetrische Cluster

Ein symmetrischer Cluster stellt sicher, dass Notes-Datenbanken auf allen Servern in einem Cluster identisch bleiben. Ein Reparaturdienst repariert fehlende oder beschädigte Datenbanken, indem er sie durch gute Repliken von anderen Servern des Clusters ersetzt.

16.4.1. Erkennung und Reparatur fehlender Datenbanken

Der Servertask AutoRepair wird in einem symmetrischen Cluster auf jedem Server ausgeführt. AutoRepair durchsucht bestimmte Ordner auf dem Server nach fehlenden Datenbanken. AutoRepair bezieht sich auf das Cluster-Datenbankverzeichnis (clbdbir.nsf), um zu bestimmen, welche Datenbanken die überwachten Ordner enthalten sollen. Wenn AutoRepair fehlende Datenbanken erkennt und repariert, repariert es auch alle NLO-Dateien im DAOS, auf die von den Datenbanken verwiesen wird.

Verwenden Sie das Cluster-Konfigurationsdokument, um die folgenden Aspekte von AutoRepair zu konfigurieren:

- > Ob AutoRepair fehlende Datenbanken nur protokolliert oder ob der Reparaturdienst den Ersatz fehlender Datenbanken auslöst.
- > Die zu scannenden Ordner. Ordner müssen sich unter dem Serverdatenverzeichnis befinden.
- > Die Häufigkeit, mit der AutoRepair nach fehlenden Datenbanken sucht.

16.4.2. Erkennung und Reparatur defekter Datenbanken

Um beschädigte Datenbanken zu erkennen und zu reparieren, wählen Sie in einem Cluster-Konfigurationsdokument die Option »Beschädigte Dateien korrigieren«. Wenn diese Option ausgewählt ist und ein Domino-Server eine beschädigte Datenbank in einem überwachten Ordner erkennt, wird Fixup ausgeführt, um zu versuchen, die Datenbank zu reparieren. Wenn die Korrektur nicht erfolgreich ist, wird die beschädigte Datenbank isoliert und der Reparaturdienst stellt eine gute Version von einem Spender-Cluster-Mitglied wieder her. Die isolierten Datenbanken werden nach einer einstellbaren Anzahl von Tagen gelöscht.

Um fehlende oder beschädigte Datenbanken zu ersetzen, geht der Reparaturdienst wie folgt vor:

- > Er kopiert einen Snapshot der Datenbank von einem Spenderserver, der über eine intakte Version verfügt.
- > Er aktualisiert alle Ordnerreferenzen.
- > Er setzt das Replizierprotokoll zurück.
- > Er erstellt einen neuen Volltextindex.
- > Er durchsucht die Datenbank, um festzustellen, ob alle verwendeten DAOS-Objekte vorhanden sind. Fehlende Objekte werden hinzugefügt.

16.4.3. Bedingungen für einen symmetrischen Cluster

Bevor Sie einen symmetrischen Cluster konfigurieren, überprüfen Sie die folgenden Voraussetzungen:

Jeder Server im Cluster muss Domino 10 oder höher sein, sowie ein Verzeichnis-Design basierend auf der Schablone von Version 10 oder höher besitzen.

Planen Sie genügend Speicherplatz ein! Bei aktivierter Ordnersymmetrie sollten außerdem alle Server im Cluster über annähernd gleich viel Speicher verfügen.

Wenn Sie den Domino Attachment and Object Service (DAOS) verwenden, muss dieser auf allen Cluster-Mitgliedern gleich konfiguriert sein. Zusätzlich muss der DAOS-Catalog zwischen allen Cluster-Servern synchronisiert werden.

Überwachte Datenbankrepliken müssen auf allen Cluster-Servern denselben Pfad aufweisen.

Folgende Datenbanken können nicht repariert werden:

- > Datenbanken mit einem niedrigeren ODS als 52
- > verschlüsselte Datenbanken
- > Datenbanken, für die die Zugriffsrechte nicht ausreichen (in der Datenbank-ACL oder Ordner-ACL)
- > Datenbanken, für die die Cluster-Replikation nicht aktiviert wurde
- > Datenbanken, die über keine Repliken auf den anderen Cluster-Servern verfügen
- > Verzeichnis- oder Datenbank-Links

16.4.4. Einen symmetrischen Cluster aufsetzen

Fügen Sie zur Datei notes.ini jedes Servers im Cluster die folgende Variable hinzu:

```
D10_ENABLE_REPAIR=1
```

Starten Sie den Servertask AutoRepair und fügen Sie ihn entweder zur Variable ServerTasks in der Datei notes.ini jedes Cluster-Servers hinzu oder erstellen Sie ein Programmdokument vom Typ »Nur beim Serverstart«.

Jede Replik, die Sie überwachen, muss auf allen Servern im Cluster denselben Dateipfad aufweisen. Das überprüfen Sie im am besten im Cluster-Verzeichnis (clbdbir.nsf) in der Ansicht **Databases by Replica ID**.

Um eine Cluster-Konfiguration zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Konfiguration** und erweitern Sie die Kategorie **Cluster**.
2. Wählen Sie die Ansicht **Cluster-Konfigurationen** und klicken Sie auf die Schaltfläche **Cluster-Konfiguration hinzufügen**.
3. Wählen Sie im Register **Allgemein** den Cluster aus:

Abbildung 16.11: Cluster-Konfiguration, Register Allgemein

4. Wechseln Sie zum Register **Symmetrie**:

Abbildung 16.12: Cluster-Konfiguration, Register Symmetrie

5. Geben Sie das Ausmaß der Symmetrie an. Soll die Symmetrie für alle Ordner gewahrt werden, wählen Sie im Feld **Symmetrie wahren** die Option »Alle Ordner«. Um die Symmetrie nur für bestimmte Ordner zu wahren, wählen Sie hingegen die Option »Angegebene Ordner« und geben die Ordner an.
6. Wählen Sie eine Option für die automatische Reparatur aus.

Um den Reparaturdienst zu veranlassen, beschädigte oder fehlende Dateien in den gewählten Ordnern zu ersetzen, wählen Sie im Feld **Automatische Reparatur** die Option »Fehlende Dateien korrigieren«.

Um fehlende Dateien nur im Protokoll aufzulisten, ohne sie zu reparieren, wählen Sie stattdessen »Fehlende oder beschädigte Dateien im Protokoll auflisten«.

Um die Automatische Reparatur zu deaktivieren, wählen Sie »Deaktiviert«.

7. Geben Sie im Feld **Scan-Intervall** an, wie oft fehlende oder beschädigte Dateien repariert werden sollen. Die Vorgabe ist 15 Minuten.
8. Wählen Sie im Feld **Beschädigte Dateien** die Option »Beschädigte Dateien korrigieren« oder deaktivieren Sie die Funktion.
Wenn die Korrektur nicht erfolgreich ist, isoliert der Server die beschädigte Datenbank, indem er die Dateierweiterung in *.pd_bad_<Zeitstempel> ändert. Der Reparaturdienst stellt sofort eine gute Version von einem Spender-Cluster-Mitglied wieder her. Der Servertask Repair Cleanup löscht die isolierten Datenbankversionen nach der im Feld **Beschädigte Dateien entfernen nach** angegebenen Anzahl von Tagen. Die Vorgabe ist 28 Tage.
9. Haben Sie das Entfernen von beschädigten Daten aktiviert, starten Sie den Servertask Repair Cleanup (RprCleanup) auf Basis eines Zeitplans, entweder über die Datei notes.ini oder über ein Programmdokument.
10. Speichern und schließen Sie das Dokument.

16.4.5. Den Reparaturdienst tunen

Verwenden Sie das Register **Tuning** in der Cluster-Konfiguration, um das Verhalten des Reparaturdienstes anzupassen.

Cluster-Konfiguration: COB1		
Allgemein Symmetrie Tuning Administration		
Anzahl von Reparatur-Threads:	<input type="text" value="4"/>	
Spender-Verfügbarkeit überprüfen:	<input type="text" value="5"/>	Minuten
Fehlgeschlagene Reparaturen wiederholen nach:	<input type="text" value="5"/>	Minuten
Maximale Anzahl von Wiederholungen:	<input type="text" value="3"/>	
Reparaturleistung:	<input type="text" value="5"/> (1=langsamstes, 5=schnellstes)	
Protokollierungsstufe für Reparatur:	<input type="text" value="Normal"/>	

Abbildung 16.13: Cluster-Konfiguration, Register Tuning

Das Feld **Anzahl von Reparatur-Threads** steuert, wie viele Threads der Reparaturdienst verwenden soll. Geben Sie einen Wert von 1 bis 20 ein. Die Vorgabe ist 4.

Das Feld **Spender-Verfügbarkeit überprüfen** steuert wie häufig der Reparaturdienst die Verfügbarkeit von Spenderservern überprüfen soll. Geben Sie einen Wert von 1 bis 15 Minuten ein. Die Vorgabe ist 5 Minuten.

Das Feld **Fehlgeschlagene Reparaturen wiederholen nach** steuert, wann eine fehlgeschlagene Reparatur wiederholt werden soll. Geben Sie einen Wert zwischen 1 und 15 Minuten an. Die Vorgabe ist 5 Minuten.

Das Feld **Maximale Anzahl von Wiederholungen** steuert, wie oft sich der Reparaturdienst mit dem Spenderserver verbinden kann, um eine Datei zu ersetzen. Wenn das Limit erreicht ist, wird die Datei als nicht reparierbar protokolliert. Sie können maximal 5 Versuche konfigurieren.

Das Feld **Reparaturleistung** steuert, wie viele Ressourcen für den Reparaturdienst reserviert werden sollen.

Das Feld **Protokollierungsstufe für Reparatur** steuert das Ausmaß der Protokollierung.

16.4.6. Der Befehl Repair

Zusätzlich stehen die folgenden Befehle zur Verfügung, um manuell einschreiten zu können:

Befehl	Beschreibung
<code>tell repair list servers</code>	Listet die möglichen Spenderserver auf, von denen der aktuelle Server Dateien erhalten kann.
<code>tell repair list files</code>	Listet alle Datenbanken auf, die sich auf dem aktuellen Server befinden sollten. Es wird für jede Datenbank angegeben, ob sie vorhanden ist (present) oder fehlt (missing).
<code>tell repair list missing</code>	Listet alle fehlenden Datenbanken auf. Listet auch jene Dateien auf, die sich aufgrund eines abweichenden Dateinamens disqualifiziert haben.
<code>tell repair <Datei> <Server></code>	Beauftragt den Reparaturdienst, die angegebene Datenbank zu reparieren.
<code>tell repair all</code>	Durchsucht alle überwachten Ordner nach fehlenden Dateien und der mit ihnen verbundenen DAOS-Objekten.
<code>tell repair disable <Datenbank></code>	Schließt die angegebene Datenbank von der Suche nach fehlenden Dateien aus, z. B. weil sie via Backup eingespielt wurde.
<code>tell repair enable <Datenbank></code>	Inkludiert die angegebene Datenbank wieder in die Suche nach fehlenden Dateien.
<code>tell repair show config</code>	Zeigt die Cluster-Konfiguration an.

Tabelle 16.1: Die Parameter des Befehls Repair

17. Serverüberwachung

- > 17.1 Übersicht, Seite 451
- > 17.2 Das Domino-Serverprotokoll, Seite 451
- > 17.3 Statistiken, Seite 453
- > 17.4 Server-Ereignisse, Seite 458
- > 17.5 Domino-Domänenüberwachung, Seite 462

17.1. Übersicht

Die Server sind aufgesetzt und konfiguriert. Zeit sich zurückzulehnen und sich auszuruhen? Ja, das sollten Sie tun, Sie haben es sich verdient! Aber Ihre Arbeit ist noch nicht zu Ende. Sie müssen regelmäßig nachsehen, wie es den Servern geht. »Proaktive Administration« lautet die Devise, was so viel heißt, wie nicht darauf zu warten, bis etwas passiert, sondern zu versuchen, Engpässe und Probleme im Vorhinein zu erkennen und zu verhindern.

Der Domino-Server stellt zur Überwachung zahlreiche Werkzeuge zur Verfügung. Nicht alle sind wirklich brauchbar, einige heillos überaltert, aber wenn man sich überall die Rosinen herauspickt, geht das meiste. Wichtige Quellen zum Einschätzen der Servergesundheit sind:

- > das Serverprotokoll (log.nsf)
- > die Serverstatistiken (statrep.nsf)
- > die Ereignisüberwachung (events4.nsf)
- > die Domino-Domänenüberwachung (Domino Domain Monitoring – DDM, ddm.nsf)
- > das Client-Monitoring (Echtzeitüberwachung)

17.2. Das Domino-Serverprotokoll

Der Domino-Server verwendet zur Protokollierung die Notes-Datenbank log.nsf. Das Serverprotokoll kann per Vorgabe von allen Mitgliedern der Gruppe LocalDomainAdmins über den Notes-Client oder über den Domino-Administrator eingesehen werden.

Um die Protokolldatei im Domino-Administrator zu öffnen, navigieren Sie zum Register **Server...**
> **Analyse** und wählen Sie den Eintrag **<Servername>'s Log**.

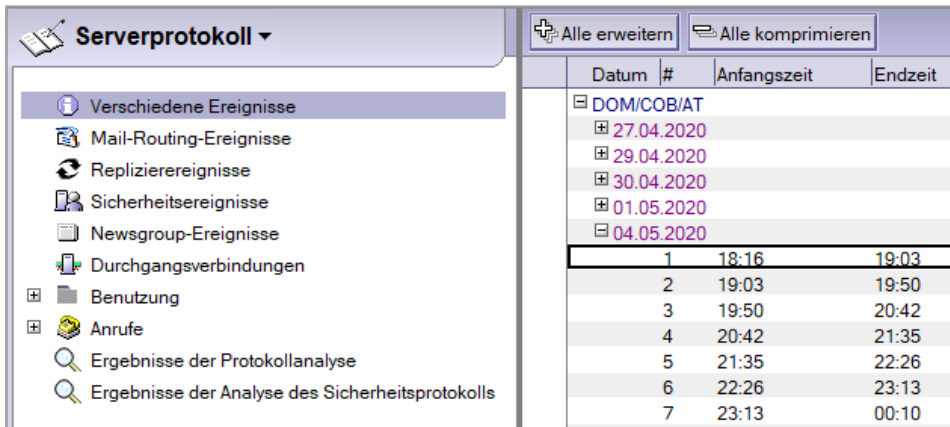


Abbildung 17.1: Das Serverprotokoll, Ansicht Verschiedene Ereignisse

Wichtig sind die folgenden Ansichten:

Ansicht	Beschreibung
Mail-Routing-Ereignisse	Hier wird alles protokolliert, was mit dem Mailsystem zu tun hat, etwa die Zustellung und Weitergabe von Mails, bzw. auch, wenn Fehler auftreten.
Repliziereignisse	Hier werden die Replikationen zwischen den Servern protokolliert.
Sicherheitereignisse	Hier wird alles protokolliert, was mit dem ID-Vault zu tun hat, etwa wenn eine ID-Datei nicht heruntergeladen werden konnte.
Verschiedene Ereignisse	Hier wird alles protokolliert, was auf der Serverkonsole ausgegeben bzw. in diese eingegeben wurde (Abfragen der Administratoren).

Tabelle 17.1: Die wichtigsten Ansichten im Serverprotokoll

Um das Protokoll zu durchsuchen, blenden Sie über den Menüpunkt **Ansicht > In dieser Ansicht suchen** die Suchleiste ein.

Achtung: Sie sollten keinen Volltextindex für die Protokolldatei erstellen. Wenn die Suche aufgrund der Größe zu lange dauert, können Sie auf die Protokollanalyse zurückgreifen (**Werkzeuge > Analyse > Protokoll...**)

17.2.1. Steuern, wie lange Protokolleinträge aufgehoben werden

Standardmäßig werden Protokolleinträge nach 7 Tagen gelöscht. Gesteuert wird dies durch die notes.ini-Variable LOG. Die Vorgabe lautet:

```
Log=log.nsf, 1, 0, 7, 30000
```

Damit werden maximal 30 K große Logeinträge für 7 Tage in der Datei log.nsf aufgehoben. Wenn Sie einen längeren Zeitraum überwachen wollen, ersetzen Sie den Wert 7 durch eine höhere Zahl, etwa durch 30 für einen Monat, z. B. über den Befehl:

```
set configuration Log=log.nsf, 1, 0, 30, 30000
```

Achtung: Behalten Sie nach dieser Änderung die Größe der Protokolldatei im Auge!

Tip: Sie können über die Datenbankeinstellungen eine Archivierung vornehmen. Erstellen Sie sodann ein Programmdokument zum Archivieren älterer Einträge (compact log.nsf -a).

17.2.2. Protokollfilter

Eine andere Möglichkeit, den Zeitraum zu verlängern und das Protokoll trotzdem klein zu halten, besteht darin, Protokollfilter (Log Filter) zu setzen. So könnten Sie etwa konfigurieren, dass Ereignisse mit niedrigen Dringlichkeitsstufen (Severities) gar nicht erst in der Protokolldatei aufgezeichnet werden.

Um Log Filter zu setzen:

1. Starten Sie den Domino-Administrator und navigieren Sie zu **Konfiguration > Überwachungskonfiguration > Log Filters**.
2. Klicken Sie auf **New Event Filter**.
3. Wählen Sie auf der Seite **Basics** den Namen des Servers, für den Sie den Filter setzen wollen.
4. Wechseln Sie zur Seite **Database** und setzen Sie Filter auf Ereignistypen und Severities.
5. Optional: Setzen Sie auch Filter für die Ausgabe auf der Serverkonsole.

17.3. Statistiken

Der Server erstellt eine große Zahl von Echtzeitstatistiken. Diese können auf der Serverkonsole über den folgenden Befehl abgefragt werden:

```
show statistic <Bereich>
```

Als Bereich kann man eine Kategorie angeben, etwa »Mail« oder »Server«, aber auch spezifischer werden. Nachfolgend einige Beispiele:

```
show statistic server
```

```
show statistic server.sessions.*
```

```
show statistic mail.del*
```

Beim Abfragen von Unterbereichen muss ein Stern (*) angegeben werden.

In der Datenbank für Überwachungskonfiguration (»Monitoring Configuration«, events4.nsf) sind (Stand Version 11.0.1) 1.194 Statistiken mit Erklärungen und Schwellenwerten aufgeführt. Leider haben es die Statistiken für die mit Domino 10 oder 11 neu eingeführten Features bisher noch nicht in diese Datenbank geschafft. Zu beachten ist auch, dass bei der Installation von Zusatzprodukten (z. B. dem Notes Traveler) weitere Statistiken hinzukommen, die ebenfalls nicht in der Datenbank stehen.

Echtzeitstatistiken sind immer Momentaufnahmen und oft nicht aussagekräftig. Nehmen wir z. B. die Statistik: Server.Users: In diesem Augenblick sind 357 Benutzer mit dem Server verbunden. Was sagt uns das? Dass gerade 357 Benutzer verbunden sind – mehr nicht. Es wäre interessanter zu erfahren, wie sich die Benutzerzahl im Laufe des Tages verändert und ob es dabei zu Engpässen kommt! Und das geht auch, Sie müssen den Server nur anweisen, die Statistiken zu sammeln. Dafür

existiert ein eigener Task, der sogenannte **Statistic Collector** (Collect), der die Statistiken periodisch in die Datenbank »Monitoring Results« (statrep.nsf) schreibt.

Es gibt zwei Arten, das Sammeln von Statistiken aufzusetzen. Sie können entweder einen Statistic Collector auf jedem Server starten, der dann nur die eigenen Statistiken sammelt, oder einen Sammler festlegen, der die Statistiken von allen Servern der Domäne in die Datenbank »Monitoring Results« schreibt.

Aber der Statistic Collector kann mehr: Er sammelt nicht nur Statistiken, er überprüft auch in der Datenbank »Monitoring Configuration« (events4.nsf) hinterlegte Schwellenwerte und gibt Warnungen aus, wenn diese überschritten werden. Diese Warnungen werden auf der Serverkonsole ausgegeben und in der Datenbank »Monitoring Results« gespeichert.

17.3.1. Das Sammeln von Statistiken konfigurieren

Um das Sammeln von Statistiken und das Überprüfen von Schwellenwerten zu konfigurieren, gehen Sie wie folgt vor:

1. Starten Sie den Domino-Administrator und verbinden Sie sich mit dem Server, der die Statistiken sammeln soll.
2. Navigieren Sie zu **Konfiguration > Überwachungskonfiguration > Server Statistic Collection**.
3. Überprüfen Sie zuerst, ob bereits ein Dokument für Ihren Server existiert. Sollte es fehlen, erstellen Sie durch Klicken auf die Schaltfläche **New Statistic Collection** ein neues, ansonsten bearbeiten Sie das vorhandene Dokument.

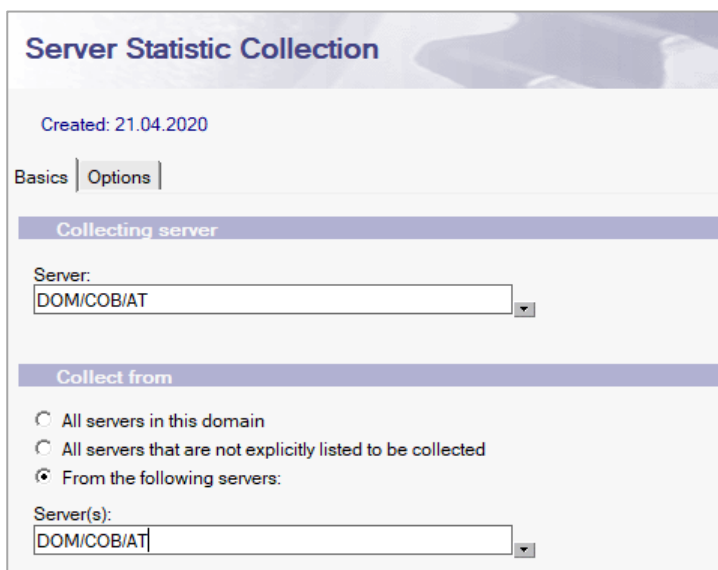


Abbildung 17.2: Server Statistic Collection, Register Basics

4. Akzeptieren Sie im Bereich **Collecting server** die Vorgabe oder wählen Sie einen anderen Server aus.
5. Wählen Sie im Bereich **Collect from** eine der folgenden Optionen:
Soll der Server die Statistiken von allen Servern in der Domäne sammeln, wählen Sie »All servers in the domain«.

Soll der Server nur seine eigenen Statistiken sammeln, wählen Sie »From the following servers« und wählen denselben Server nochmals aus.

Soll der Server Statistiken von bestimmten Servern sammeln, wählen Sie »From the following servers« und wählen die gewünschten Server aus.

- Wechseln Sie zum Register **Options** und setzen Sie ein Häkchen im Feld **Log statistics to a database**. Der Name der Datenbank sollte statrep.nsf lauten.

Server Statistic Collection

Created: 21.04.2020

Basics | **Options**

Log statistics to a database

Database to receive reports (file name):

Collection report interval: minutes

Collection alarm interval: minutes

Statistic Filters:

- Adminp
- Agent
- Calender
- Comm
- DAOS
- Database
- DECS
- Disk
- FT
- HTTP
- ICM

Abbildung 17.3: Server Statistic Collection, Register Options

- Geben Sie einen **Collection report interval** ein. Je kürzer der Zeitraum, desto genauer wird später Ihre Auswertung. Ich empfehle zumindest 60 Minuten, damit Sie die Statistiken im Verlauf des Tages mindestens stündlich auswerten können. Das Sammeln von Statistiken ist nicht sehr ressourcenintensiv, auch 30 Minuten wären vertretbar.
- Den **Collection alarm interval** würde ich auf 30 oder 60 Minuten setzen, denn auf das Überschreiten von Schwellenwerten muss man im Bedarfsfall schnell reagieren.
- Sie müssen im Feld **Statistic Filters** nichts auswählen. Ganz im Gegenteil, die Liste dient zum Einschränken: Was Sie hier auswählen, wird NICHT gesammelt. Normalerweise wählt man nichts aus, sammelt also alles. (Wenn bestimmte Tasks nicht laufen, z. B. DECS, gibt es dazu ohnehin keine Statistiken.)
- Speichern und schließen Sie das Dokument.
- Starten Sie den Task Statistic Collector:

```
load collect
```

Der Task erstellt beim ersten Start die Datenbank »Monitoring Results« (nur auf Englisch verfügbar) mit dem Dateinamen statrep.nsf.

Sorgen Sie dafür, dass der Statistic Collector beim Hochfahren des Servers automatisch startet – entweder über ein Programmdokument (siehe Kap. 5.3.4 Programme über Programmdokumente

starten, ab Seite 97) oder über die Variable ServerTasks in der Datei notes.ini (siehe Kap. 5.3.3 Programme über die Datei notes.ini starten, ab Seite 96).

Um den Statistic Collector anzuweisen, per sofort Statistiken für alle konfigurierten Server zu sammeln, geben Sie den folgenden Befehl ein:

```
tell collector collect
```

17.3.2. Historische Statistiken abfragen

Wenn der Collector die Statistiken lange genug gesammelt hat, können Sie daraus im Domino-Administrator Diagramme erstellen. »Lange genug« bezieht sich in dem Fall auf den Zeitraum, den Sie betrachten wollen; ist für Sie etwa eine Arbeitswoche interessant, müssen Sie die Statistiken eine Arbeitswoche gesammelt haben.

Um historische Statistiken abzufragen, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Server > Leistung** und wählen Sie die Ansicht **Statistikdiagramme > Historische Statistiken**.
2. Klicken Sie auf das grüne Plus und wählen Sie im Dialog **Statistik hinzufügen** den Server aus.
3. Klappen Sie in der Liste der Statistiken den gewünschten Bereich auf und wählen Sie die Statistik aus, z. B. Server > Users.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

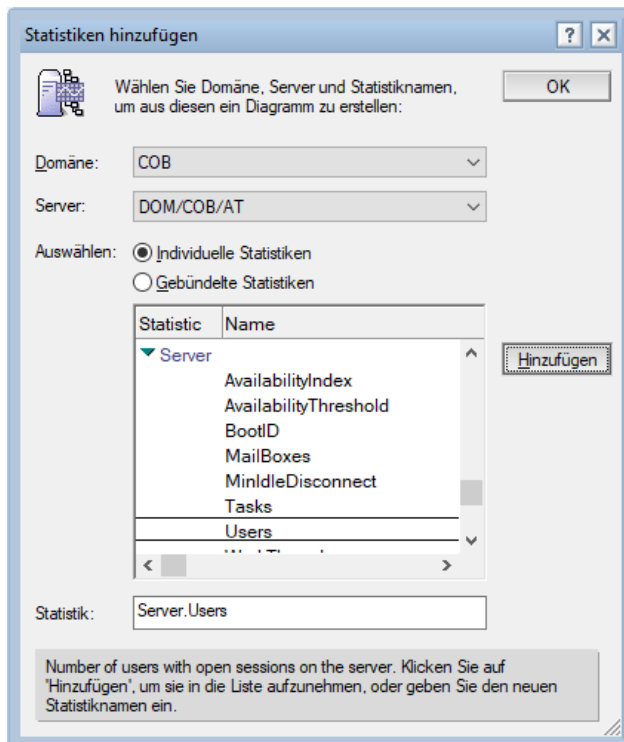


Abbildung 17.4: Dialog Statistiken hinzufügen

5. Wählen Sie weitere Statistiken aus und klicken Sie jedes Mal auf die Schaltfläche **Hinzufügen**.
6. Wenn Sie alle gewünschten Statistiken ausgewählt haben, klicken Sie auf **OK**.

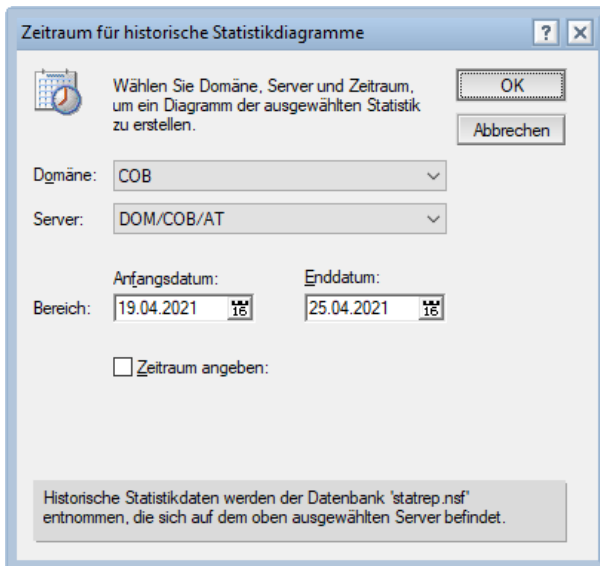
7. Klicken Sie nun auf die Schaltfläche **Bereich...**

Abbildung 17.5: Dialog Zeitraum für historische Statistikdiagramme

8. Wählen Sie erneut den Server aus und geben Sie den gewünschten Bereich an.
9. (Optional) Möchten Sie die Statistiken auf einen bestimmten Zeitraum reduzieren, z. B. auf die Arbeitszeiten, setzen Sie ein Häkchen im Feld **Zeitraum angeben** und wählen Sie die Uhrzeiten aus.
10. Klicken Sie auf **OK**. Die Statistiken werden sofort in der Datenbank für Statistik Monitoring (statrep.nsf) abgefragt.

Sollten für den ausgewählten Zeitraum keine der gewählten Statistiken verfügbar sein, wird folgende Meldung angezeigt:

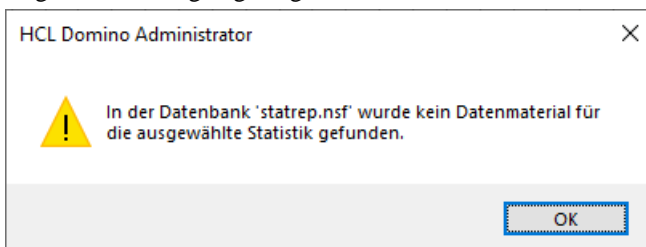


Abbildung 17.6: Historische Statistiken abfragen – keine Daten gefunden

17.3.3. Veröffentlichen von Statistiken bei externen Diensten

Der Vollständigkeit halber möchte ich hier erwähnen, dass Sie Domino seit Version 10 auch anweisen können, Statistiken bei webbasierten Überwachungsdiensten von Drittanbietern zu veröffentlichen. Damit können Sie die Statistiken mehrerer Domino-Server quasi in Echtzeit (die Übertragung erfolgt einmal pro Minute) von einem Dashboard aus visuell überwachen. Die Dienste müssen zu diesem Zweck Zeitreihendaten über HTTP-POST-Anforderungen akzeptieren.

Leicht zu konfigurieren war das nur für den Anbieter New Relic – man musste dazu nach der Registrierung auf der Website nur den Lizenzschlüssel in die Datei notes.ini eintragen. Die

Veröffentlichung von Domino Statistiken auf New Relic ist jedoch ab dem 16. Juni 2021 nicht mehr möglich, da ab diesem Datum keine Plugins mehr unterstützt werden.

Die Veröffentlichung von Statistiken bei anderen Überwachungsdiensten (HCL nennt nur Hosted Graphite) wird auch über den 16. Juni hinaus funktionieren, die Konfiguration ist jedoch wesentlich aufwendiger. Weiterführende Informationen finden Sie in der englischen Produktdokumentation des Herstellers unter:

https://help.hcltechsw.com/domino/11.0.1/admin/stats_publish_other_external.html

17.4. Server-Ereignisse

Der Servertask **Ereignismonitor** (Event) überwacht permanent alle auf dem Server auftretenden Ereignisse (Events), wird aber nur aktiv, wenn für ein Ereignis oder einen Ereignistyp ein Ereignishandler konfiguriert wurde.

Der Task Ereignismonitor wird beim Hochfahren des Servers automatisch gestartet, obwohl das nirgends explizit angegeben ist.

17.4.1. Ereignishandler

Ereignishandler (Event Handler) werden in der Datenbank »Monitoring Configuration« (nur auf Englisch verfügbar – events4.nsf) erstellt. Mit einem Ereignishandler können Sie Domino anweisen, eine Aktion auszuführen, wenn ein bestimmtes Ereignis eintritt. Die in Ereignishandlern möglichen Aktionen werden als **Benachrichtigungsmethoden** (Notification Methods) bezeichnet und sind in Tabelle 17.2 zusammengefasst:

Methoden	Erklärung
Broadcast	Eine Meldung anzeigen
Run an agent	Einen Agenten starten
Send Java Controller Command	Einen Befehl an den Java-Controller senden
Mail	Eine Mail senden
Log to Event Viewer	Eine Meldung an die Windows-Ereignisanzeige senden
Pager	An ein Pager-Gateway senden
Run Programm	Ein Programm starten
Relay to other server	Per Mail an einen anderen Server senden
Sound	Eine Melodie abspielen
Forward event to Tivoli Enterprise Console	An die Tivoli-Enterprise-Konsole senden
SNMP Trap	Einen SNMP-Trap generieren
Log to Unix system Log	In das UNIX-Systemprotokoll schreiben

Tabelle 17.2: Die verschiedenen Benachrichtigungsmethoden

Bei den Ereignissen, denen Sie Ereignishandler zuordnen können, kann es sich um ein **eingebautes Ereignis** (Built-in Event) handeln, dem jeweils ein Typ und eine Dringlichkeitsstufe (Severity) zugeordnet sind, oder auch um eine beliebige auf der Serverkonsole ausgegebene Meldung, von der Sie nur den Text kennen.

Eine dritte Möglichkeit der Zuordnung besteht in der Auswahl sogenannter **Ereignisgeneratoren**, die spezifische Aktionen erlauben. Sie sind in Kap. 17.4.3 Ereignisgeneratoren, ab Seite 461, genauer beschrieben.

In der Datenbank »Monitoring Configuration« sind 7.525 eingebaute Ereignisse gespeichert. (Die Anzahl hat sich seit einigen Versionen nicht verändert...) Um die Liste einzusehen, navigieren Sie im Admin-Client zum Register **Konfiguration** > **Überwachungskonfiguration** > **Names & Messages (Advanced)** und öffnen eine der Event-Messages-Ansichten.

17.4.2. Einen Eventhandler für eine bestimmte Meldung einrichten

Nehmen wir an, Sie wollen wissen, wann jemand die Administration mit voller Berechtigung (siehe Kap. 5.6.7, auf Seite 109) angefordert hat. Dafür gibt es kein eingebautes Ereignis, sondern nur eine Meldung auf der Serverkonsole:

»xy was granted full administrator access«

Um einen Ereignishandler für diese Meldung zu generieren, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Konfiguration** > **Überwachungskonfiguration**.
2. Klicken Sie in der Ansicht **Event Handlers** > **All** auf die Schaltfläche **New Event Handler**.
3. Wählen Sie im Bereich **Server(s) to monitor** die Option »Notify of the event on any server in the domain« und als **Notification trigger** die Option »Any event that matches a criteria«:



Abbildung 17.7: Eventhandler, Register Basics

4. Wechseln Sie zum Register **Event**.

The screenshot shows the 'Event Handler' configuration page with the 'Criteria to match' section. The page title is 'Event Handler' and it was created on '04.04.2020'. There are three tabs: 'Basics', 'Event', and 'Action'. The 'Criteria to match' section has three main options, each with a radio button and a sub-option:

- Events can be any type:
 - Events must be this type:
- Events can be any severity:
 - Events must be one of these severities:
- Events can have any message
 - Events must have this text in the event message:
 - was granted full administrator access

Abbildung 17.8: Eventhandler, Register Event

5. Wählen Sie die Optionen »Events can be any type«, »Events can be any severity« und »Events must have this text in the event message«.
6. Geben Sie den folgenden Text ein: »was granted full administrator access«.
7. Wechseln Sie zum Register **Action**.

The screenshot shows the 'Event Handler' configuration page with the 'Notification' and 'Enablement' sections. The page title is 'Event Handler' and it was created on '04.04.2020'. There are three tabs: 'Basics', 'Event', and 'Action'. The 'Notification' section has two fields:

- Method: Mail
- Mailing address: Christian Buchacher/COB/AT

The 'Enablement' section has three options, each with a radio button:

- Enable this notification
- Disable this notification
- Enabled only during these times:

Abbildung 17.9: Event-Handler, Register Action

8. Wählen Sie die Notification Method »Mail« und geben Sie die gewünschte Adresse ein:
9. Speichern und schließen Sie das Dokument. Es ist nicht nötig, den Server durchzustarten, der Event-Task findet den neuen Handler von selbst.

Und so sieht die Mail aus:

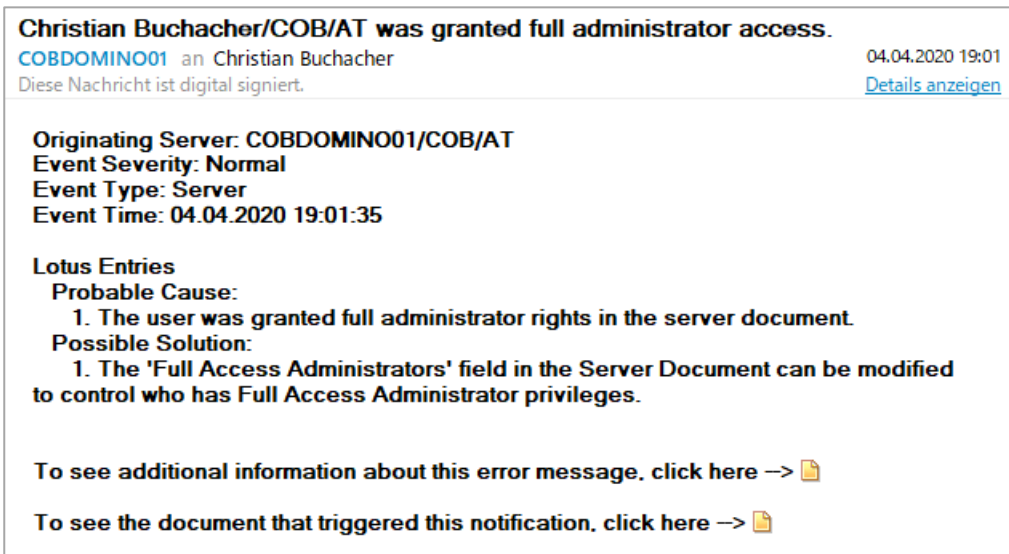


Abbildung 17.10: Mail des Event-Tasks

17.4.3. Ereignisgeneratoren

Ereignisgeneratoren (Event Generators) überwachen je nach Typ ganz unterschiedliche Ereignisse wie Änderungen in der ACL einer Datenbank, die Verfügbarkeit eines Servertasks oder TCP-Servers oder auch das Überschreiten von Schwellenwerten in Statistiken. Wird ein Ereignis generiert, wird es an den Ereignismonitor (Event) übergeben, der überprüft, ob ein zugeordneter Ereignishandler existiert. Wenn kein Ereignishandler definiert ist, führt der Ereignismonitor keine Aktion aus. Wenn ein Ereignishandler definiert ist, führt der Ereignismonitor die Anweisungen im Ereignishandler aus.

In der Ansicht **Event Generators** in der Datenbank »Monitoring Configuration« (events4.nsf) sind einige Beispiele für Ereignisgeneratoren aufgeführt. Erstellen Sie neue Ereignisgeneratoren und die jeweils dazu passenden Ereignishandler, um für Sie relevante Ereignisse zu überwachen.

Die folgende Tabelle listet die verfügbaren Ereignisgeneratoren auf:

Ereignisgenerator	Beschreibung
Database event generator	Überwacht die folgenden Bereiche in einer Datenbank: <ul style="list-style-type: none"> – Benutzeraktivität – Ausmaß des ungenutzten Bereichs – Häufigkeit und Erfolg der Replikation – Änderungen in der Zugriffskontrollliste
Domino server event generator	Überprüft die Konnektivität und den Portstatus der angegebenen Domino-Server.
Mail routing event generator	Sendet über den Task ISpy Nachrichten an eine bestimmte Mailadresse und sammelt Statistiken über die Dauer der Zustellung in Sekunden.

Ereignisgenerator	Beschreibung
Statistic event generator	Überwacht das Überschreiten von Schwellenwerten für spezifische Statistiken. Dafür muss im Dokument Server Statistic Collection ein Collection alarm interval definiert worden sein.
Task status event generator	Überwacht den Status von Domino-Servertasks.
TCP server event generator	Prüft über den Task ISpy die Verfügbarkeit der angegebenen Internet-Ports und generiert Statistiken zur Dauer in Millisekunden.

Tabelle 17.3: Die verschiedenen Ereignisgeneratoren

Beim Erstellen von Server- und Mail-Routing-Ereignisgeneratoren, müssen Sie zusätzlich den ISpy-Task starten. Geben Sie dazu auf der Serverkonsole den folgenden Befehl ein:

```
load runjava ISpy
```

Geben Sie zum Beenden des Tasks ISpy den folgenden Befehl ein:

```
tell runjava unload ISpy
```

Achten Sie auf die Schreibweise, in Java wird zwischen Groß- und Kleinschreibung unterschieden!

Wenn Sie den ISpy-Task bleibend einbinden wollen, fügen Sie den Eintrag runjava ISpy zur Variable ServerTasks= in der Datei notes.ini des Servers hinzu oder erstellen Sie ein Programmdokument.

Um einen neuen Ereignisgenerator zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie im Domino-Administrator zum Register **Konfiguration > Überwachungskonfiguration > Event Generator** und öffnen Sie anschließend die entsprechende Ansicht, z. B. **Database** für Datenbank-Ereignisgeneratoren.
2. Klicken Sie auf die Schaltfläche **New <Generatortyp>**, um einen neuen Ereignisgenerator zu erstellen.
3. Füllen Sie den Ereignisgenerator aus, wie nach Typ unterschiedlich angegeben.
4. Wechseln Sie zum Register **Other** und klicken Sie auf die Schaltfläche **Create a new event handler for this event**, um den dazu passenden Eventhandler zu erstellen. Der optisch ansprechende Event Handler Wizard macht es Ihnen leicht, dem Ereignis eine Benachrichtigungsmethode zuzuordnen.
5. Speichern und schließen Sie das Dokument.

17.5. Domino-Domänenüberwachung

Zusätzliche Möglichkeiten bietet die **Domino-Domänenüberwachung** (Domino Domain Monitoring – DDM, ddm.nsf), welche mit Version 7 eingeführt und mit Version 8 überarbeitet wurde. Die Basis dafür liefert ebenfalls der Ereignismonitor, die Ereignisse werden jedoch besser aufbereitet dargestellt. Dazu kommt die Möglichkeit, ein Probing in Bereichen zu konfigurieren, die über Ereignisgeneratoren nicht möglich sind. Dafür kennt DDM nur das Protokollieren in der Datenbank ddm.nsf, andere Benachrichtigungsmethoden wie das Versenden von Mails u. a. sind nicht möglich.

Die Domino-Domänenüberwachung bietet die folgenden Funktionen:

- > Bietet neben der Fehlermeldung auch zusätzliche Informationen zum Ort des Auftretens wie Server, Datenbank oder Benutzer – nur bei erweiterten (enhanced) Ereignissen.
- > Erkennt wiederholt auftretende Ereignisse und stellt sie nur einmal dar.
- > Ordnet Ereignissen eine Dringlichkeit (Severity) zu.
- > Erlaubt es, Ereignisse Personen zuzuweisen.
- > Ordnet Ereignissen einen Status zu und erlaubt das Abschließen und Ausblenden erledigter Probleme.
- > Geschlossene Ereignisse werden vom Server wieder geöffnet, wenn sie nicht gelöst sind.
- > Erlaubt das Ausblenden nicht relevanter oder unlösbarer Probleme.
- > Unterstützt die Problemerkennung durch Vorschlagen möglicher Ursachen und liefert (je nach Beschickung der Datenbank) sogar mögliche Lösungen.
- > Bietet Schaltflächen (»Corrective Actions«) mit Links zu Datenbanken, dem Wechseln zu bestimmten Bereichen im Domino-Administrator oder dem Absetzen von Konsolenbefehlen, um erkannte Probleme schneller beheben zu können.
- > Erlaubt es, eigene Korrekturschaltflächen mit LotusScript-Code zu erstellen.
- > Fasst auf Wunsch die Ereignisse mehrerer Server zusammen (Erfassungshierarchie).
- > Bietet aktive Überwachungsfunktionen mit mehr als 50 vorkonfigurierten Proben mit flexibel konfigurierbaren Zeitplänen, Inhalten und Zielen.

17.5.1. Erweiterte und einfache Ereignisse

Ein Erfassungsserver sammelt zwei Klassen von Ereignissen, einfache (simple) und erweiterte (enhanced) Ereignisse. **Erweiterte Ereignisse** liefern neben der eigentlichen Meldung auch noch Zusatzinformationen wie am Ereignis beteiligte Server, Datenbanken, Agenten oder Benutzer. **Einfache Ereignisse** liefern nur eine Meldung, den Meldeserver und die Dringlichkeit. Bei den meisten auftretenden Ereignissen handelt es sich um einfache Ereignisse.

Welche Ereignisse tatsächlich gesammelt werden, können Sie steuern. Gehen Sie dazu im Domino-Administrator zum Register **Konfiguration** und wählen Sie die Ansicht **Überwachungskonfiguration > DDM Filters**: Per Vorgabe werden nur einfache Ereignisse der Dringlichkeiten Schwerer Fehler (Fatal) und Fehlschlag (Error) sowie alle erweiterten Ereignisse gesammelt. Sie können aber auch Filter auf erweiterte Ereignisse setzen.

17.5.2. Problembearbeitung

Das DDM könnte man fast schon als Ticketsystem bezeichnen: Sie können Probleme anderen Administratoren zuweisen und gelöste Probleme abschließen und damit aus den meisten Ansichten ausblenden. Aber eben leider nur fast, denn es gibt keine Möglichkeit, andere über eine Zuordnung (z. B. per Mail) zu informieren, die Zusammenarbeit im DDM setzt einen proaktiven Zugang voraus: Jeder muss selbst nachsehen, ob etwas zu tun ist! Aber habe ich nicht gesagt, Domino ist eine Werkzeugkiste? Wenn Sie wollen, dass die Anwendung E-Mails verschickt, dann programmieren Sie es doch!

Wenn Sie mit dem DDM noch nicht vertraut sind, empfehle ich Ihnen, die Ansicht **Nach Dringlichkeit** und das Abarbeiten der Ereignisse von oben nach unten, d. h. Sie kümmern sich um die dringenden Ereignisse zuerst.

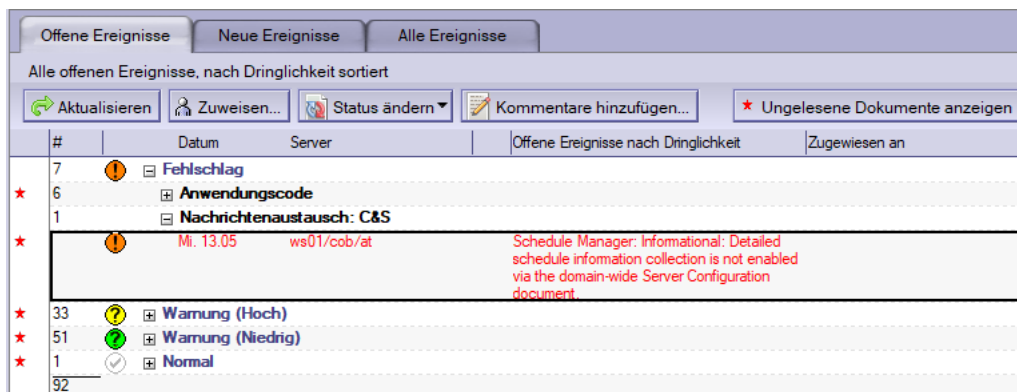


Abbildung 17.11: DDM, Ansicht nach Dringlichkeit

Administratoren mit der Rolle [Assign Events] können über die Schaltfläche **Zuweisen...** Ereignisse anderen Benutzern zuweisen. In der Ansicht **Nach Zuordnung** auf der linken Seite können Sie sehen, wer welche Ereignisse zu bearbeitet hat, in der Ansicht **Meine Ereignisse** sehen Sie die Ihnen zugewiesenen Ereignisse.

Administratoren mit der Rolle [Change State] können offene Ereignisse über die Schaltfläche **Status ändern > Ereignisse schließen...** aus allen Ansichten der Registerkarte **Offene Ereignisse** ausblenden. Das geht sowohl mit einer Mehrfachauswahl auf Ansichtsebene als auch im Ereignis selbst. Geschlossene Ereignisse werden nur mehr auf der Registerkarte **Alle Ereignisse** angezeigt.

Sollte ein von Ihnen geschlossenes Ereignis erneut auftreten, setzt es der Server automatisch auf den Status offen zurück. Mit dem Befehl **Status ändern > Ereignisse permanent schließen...** können Sie Einträge bleibend ausblenden. Sie werden vom Server zwar weiter beobachtet, aber nicht mehr geöffnet, selbst wenn das Problem weiter besteht. Sollten Sie ein Ereignis irrtümlich geschlossen haben, können Sie es in den Ansichten des Registers **Alle Ereignisse** wieder öffnen.

Über die Schaltfläche **Kommentar hinzufügen...** lassen sich ergänzende Kommentare eintragen, etwa um die Problemlösung zu hinterlegen oder auch nur um zu dokumentieren, was bisher unternommen wurde. Wenn Sie alles genau dokumentieren, wird die DDM-Datenbank damit zu einer Art »Knowledge Base« mit gespeicherten Erfahrungen zur Fehlerbehebung.

Im Rahmen einer proaktiven Administration sollten Sie das DDM ein- bis zweimal pro Woche kontrollieren und zumindest die Ereignisse mit hohen Dringlichkeiten abarbeiten. Ziel wäre, die Ansicht Offene Ereignisse so gut wie es geht auszuräumen. Ist das DDM bereits lange in Betrieb, können sich aber schon sehr viele Einträge (50.000 und mehr sind keine Seltenheit) angesammelt haben, die Sie dann mit einem vertretbaren Aufwand nicht mehr abarbeiten können. Da davon auszugehen ist, dass viele Probleme gar nicht mehr aktuell sind, rate ich Ihnen in diesem Fall zu einer radikalen Vorgangsweise: Markieren Sie alle Ereignisse ([Strg]+[A]) und wählen Sie **Status ändern > Ereignisse schließen...** Nach wie vor bestehende Probleme werden vom Server wieder geöffnet, alle anderen sind Sie los...

In eine ähnliche Kerbe schlägt die Möglichkeit, sogenannte »Automatic Report Closing Probes« zu konfigurieren. Damit werden ausgesuchte Ereignisse, die bereits eine vorkonfigurierte Anzahl von Tagen offen sind, automatisch geschlossen. Lesen Sie dazu Kap. 17.5.4 Probing auf Seite 465.

Damit Sie bei Ihren wöchentlichen Kontrollen nicht jeden Server einzeln prüfen müssen, empfehle ich Ihnen außerdem, alle Ereignisse in einer Datenbank zusammenzufassen.

17.5.3. Erfassungshierarchie

Zum Sammeln und Protokollieren von Informationen über mehrere Server hinweg verwendet DDM eine **Erfassungshierarchie**, die definiert, welche Server Ereignisse von welchen Servern sammeln. Die Erfassungshierarchie können Sie in der Datenbank Überwachungskonfiguration (events4.nsf) bearbeiten. Das geht nicht im Domino-Administrator, sondern nur durch direktes Öffnen der Datenbank events4.nsf. Wechseln Sie dort zur Ansicht **Server Collection Hierarchy** und klicken Sie auf die Schaltfläche **New Server Collection Hierarchy**. Geben Sie an, ob ein Server die Ereignisse aller Server in der Domäne sammeln soll oder ob Sie eine Hierarchie aufbauen wollen:

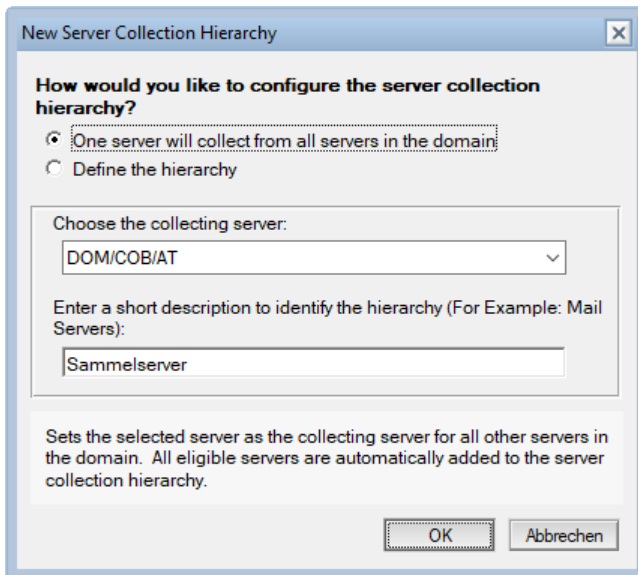


Abbildung 17.12: Dialog New Server Collection Hierarchy

Haben Sie nur wenige Server an einem Standort im Einsatz, gibt es hier nicht viel zu planen, Sie werden sich in diesem Fall für einen Sammelsever entscheiden. Die Konfiguration einer Hierarchie ist erst bei mehreren Standorten sinnvoll.

17.5.4. Probing

Das DDM sammelt nicht nur Probleme und unterstützt Sie bei der Problemerkennung, es bietet auch die Möglichkeit, konfigurierbare periodische Tests (Proben) zu fahren. Diese Tests überprüfen die Verfügbarkeit von Servertasks, messen die Dauer einer Mailzustellung oder eines Agentenlaufs und vieles andere mehr. Die Tests werden nach einem Zeitplan oder nach Bedarf ausgeführt und die Ergebnisse in der Datenbank ddm.nsf gespeichert. Es gibt (Stand Version 11.0.1) 58 vordefinierte Tests, die Sie aktivieren können, und zusätzlich noch die Möglichkeit, eigene Tests zu erstellen.

Die Aktivierung erfolgt wieder in der Datenbank Überwachungskonfiguration (events4.nsf). Wechseln Sie dazu im Domino-Administrator zum Register **Konfiguration** und wählen Sie die Ansicht **DDM Probes > By Type**. Alle Tests sind per Vorgabe deaktiviert und müssen manuell aktiviert werden. Wählen Sie dazu die gewünschten Tests aus und klicken Sie auf die Schaltfläche **Enable Probes**.

Die meisten Tests sind für »All Servers in the domain« vorkonfiguriert, bei einzelnen Tests wie z. B. der Security Best Practices Probe müssen Sie zusätzlich angeben, auf welchem Server sie laufen sollen, weshalb sie auf Ansichtsebene nicht aktiviert werden können.

18. Anwender-Clients

- > 18.1 Übersicht, Seite 467
- > 18.2 HCL Notes, Seite 467
- > 18.3 HCL Nomad: Notes auf iPad, iPhone und Co., Seite 473
- > 18.4 POP- und IMAP-Clients, Seite 474
- > 18.5 Microsoft Outlook über HTMO anbinden, Seite 487

18.1. Übersicht

Administratoren (und häufig auch Support-Mitarbeiter) benötigen natürlich einen Domino-Administrator, Entwickler einen Domino-Designer. Für Endanwender existieren gleich mehrere spezialisierte Clients: Für die Plattformen Windows und Mac HCL Notes, auf dem iPad oder auf Android-Tablets HCL Nomad. Brauchen Sie nur eine Mailanbindung (ohne Kalender), bieten sich auch POP3- oder IMAP-Clients an. Einen Spezialfall stellt Microsoft Outlook 2013 und höher dar – es kann zusätzlich über den Traveler und ActiveSync angebunden werden. Damit können Outlook-Anwender nicht nur auf Mails, sondern auch auf Kalender und Kontakte zugreifen. Wollen Sie auf das Ausrollen von Clients verzichten, können Ihre Anwender auch komfortabel mit dem Webbrowser mit Mail, Kalender und Kontakten arbeiten (iNotes Web Access oder Verse) sowie damit auf weboptimierte Anwendungen zugreifen. In weiterer Folge zeige ich Ihnen, wie Sie den Domino-Server konfigurieren müssen, um diese Clients anzubinden.

18.2. HCL Notes

Der Notes-Client läuft auf Windows 7, 8 und 10, aber erst Version 11.01 FP4 ist für Windows 11 zertifiziert.

18.2.1. Basic- und Standard-Client

Der Notes **Basic-Client** wurde in C++ entwickelt und steht für Windows und Mac OS zur Verfügung. Er ist schnell und kommt mit wenigen Ressourcen aus, eignet sich somit gut für schlecht ausgestattete PCs, bietet jedoch nicht den vollen Funktionsumfang.

Der Notes **Standard-Client** basiert auf der Entwicklungsumgebung **Eclipse** und steht für Windows, Mac OS und – allerdings nur in Version 9 – für Linux zur Verfügung. Er bietet als einziger alle Funktionen, benötigt jedoch wesentlich mehr Ressourcen.

Beide Clients können sowohl Mail als auch Notes-Anwendungen ausführen und bieten mittels OLE-Automation (auch programmatisch) die Möglichkeit mit anderen Desktopanwendungen (Microsoft Office!) zu interagieren.

Der Standard-Client lädt den Posteingang als gefällige Eclipse-Applikation, die nicht nur modern wirkt, sondern auch mehr Funktionen bietet, der Basic-Client im klassischen, ziemlich »altbacken« anmutenden Notes-Design.

Auch beim **Domino-Administrator** handelt es sich technisch um einen Basic-Client, was erklärt, warum Sie beim Öffnen einer Maildatenbank im Register Dateien ebenfalls das klassische Notes-Design sehen.

Den **Domino-Designer** gibt es wiederum nur als Standard-Client. Beide, sowohl der Administrator als auch der Designer-Client laufen nur unter Windows.

In jedem Standard-Client steckt auch ein Basic-Client, den man auch allein starten kann. Dies kann hilfreich sein, wenn der Standard-Client aus irgendeinem Grund Probleme bereitet.

Geben Sie über den Dialog **Ausführen** den Befehl `notes.exe -sa` (für »stand alone«) oder `notes.exe -basic` ein:

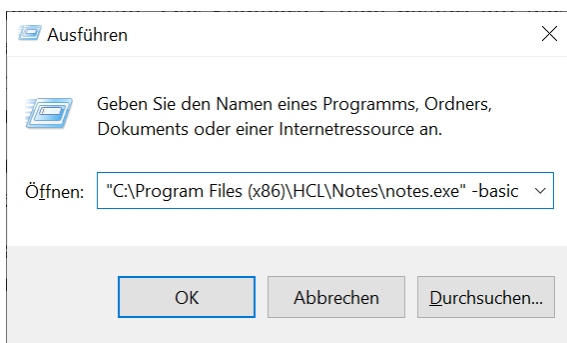


Abbildung 18.1: Notes als Basic-Client starten

18.2.2. Die verschiedenen Client-Pakete

HCL Notes können Sie von FlexNet in drei verschiedenen Paketen herunterladen:

- > als »Client-Only«-Paket für Endanwender in der Basic-Version
- > als »Client-Only«-Paket für Endanwender in der Standard-Version
- > als »All-Clients«-Paket für Administratoren und/oder Entwickler

Die Dateinamen für das »Client-Only«-Paket lauten in FlexNet je nach Version und Sprache:

Notes_1101_Win_German.exe

Notes_1101_Win_English.exe

Die Datei für den Basic-Client heißt analog:

Notes_1101_Basic_Win_German.exe

Das »All-Clients«-Paket heißt je nach Version und Sprache:

Notes_Designer_Admin_11.0_Win_English.exe

Notes_Designer_Admin_11.0.1_Win_German.exe

Die Installation des Domino-Administrators aus dem »All-Clients«-Paket haben wir bereits in Kap. 4.8 auf Seite 64 besprochen. Jetzt wollen wir einen Endanwender-Client installieren, brauchen also nur den Notes-Client. Nehmen Sie dazu das »All-Clients«-Paket und wählen als Installationsoption den Notes-Client oder das »Client-Only«-Paket?

Vorsicht, zwischen den beiden Paketen gibt es einen bedeutenden Unterschied: Nur der Notes-Client aus dem »Client-Only«-Paket beherrscht die **Mehrbenutzerinstallation** (Multi-User Installation) unter Windows, d. h. die Installation der benutzerspezifischen Daten ins Windows-Profil des Benutzers. Das ist wichtig, wenn sich mehrere Benutzer auf ein und demselben PC oder auch auf verschiedenen PCs anmelden und dort ihre eigenen Daten vorfinden sollen. Der Notes-Client aus dem »All-Clients«-Paket beherrscht hingegen nur eine lokale Installation, d. h. das bei der Installation angegebene Datenverzeichnis ist für alle Benutzer gleich.

18.2.3. Notes-Clients ausrollen

18.2.3.1. Überlegungen vor der Installation

Gehen wir davon aus, Sie wollen einen Notes-Standard-Client mit dem »Client-Only«-Paket installieren. Egal, was Sie für Angaben vorfinden, unter Windows 10 brauchen Sie, wenn Sie neben Notes auch noch flüssig mit anderen Anwendungen (etwa einem Webbrowser und einem Office-Paket) arbeiten wollen, mindestens 8 GB Hauptspeicher.

Der Notes-Standard-Client besteht aus etwa 27.000 Dateien in etwa 2.200 Unterverzeichnissen (davon etwa 9.000 Dateien weitestgehend undokumentiert!), wovon er beim Start gleich einmal ein paar Hundert lädt. Der Flaschenhals ist hier die Festplattenperformance, die Investition in eine Solid-State-Disk (SSD) lohnt sich also.

Früher (als es noch keine Mehrbenutzerinstallation gab) war es weit verbreitet, das Datenverzeichnis auf einem Netzwerklaufwerk (z. B. auf N:\Notes) abzulegen, wovon ich aus Performancegründen abrate. Und wenn es denn unbedingt sein muss, verlegen Sie wenigstens die Datei cache.ndk, in der Gestaltungselemente von Server-Datenbanken zwischengespeichert werden, nach lokal. Dafür gibt es eine eigene notes.ini-Variablen:

```
CACHE=<Pfad>
```

18.2.3.2. Durchführen einer Mehrbenutzerinstallation

Die Mehrbenutzerinstallation erfolgt in zwei Schritten:

1. Installation des Notes-Clients als Administrator
2. Anpassen der Installation zur automatischen Client-Konfiguration

1. Administratorinstallation

Melden Sie sich auf dem Computer als Administrator an und führen Sie die Installationsdatei des »Client-Only«-Pakets aus.

Wählen Sie auf der Dialogseite **Installationspfad** die Option »Jeden, der diesen Computer verwendet (alle Benutzer)«:

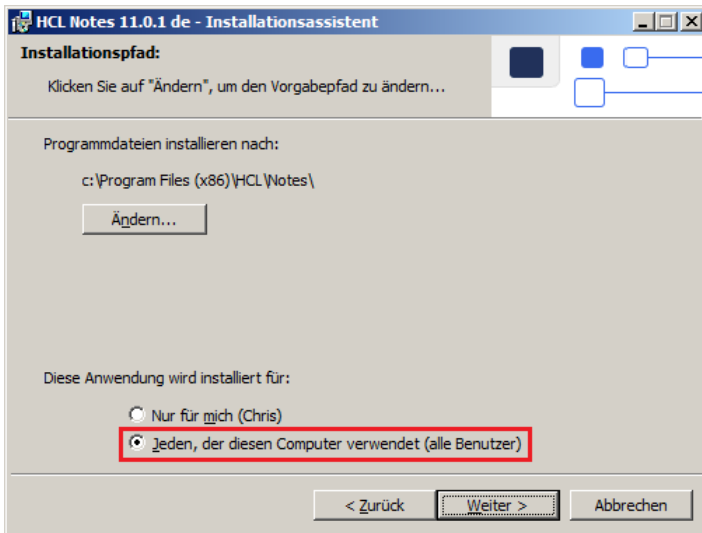


Abbildung 18.2: Installation Notes-Client – Installationspfad

Die Auswahl »Nur für mich (<Benutzer>« führt zu einer Einzelbenutzerinstallation bei der Sie das Datenverzeichnis auswählen können.

Bei der Mehrbenutzerinstallation werden die Dateien in die folgenden Verzeichnisse kopiert:

Verzeichnis	Beschreibung
C:\Program Files (x86)\HCL\Notes	Programmverzeichnis
C:\ProgramData\HCL\Notes\Data\notes.ini	Vorlage-notes.ini (wird bei der Konfiguration ins Datenverzeichnis kopiert.)
C:\ProgramData\HCL\Notes\Data\Common	Alle Dateien aus diesem Verzeichnis (bei Bedarf anlegen!) werden bei der Konfiguration durch den Endanwender ins Datenverzeichnis kopiert.
C:\ProgramData\HCL\Notes\Data\Shared	Gemeinsames Verzeichnis für Ressourcen und Schablonen
C:\Users\<User>\AppData\Local\HCL\Notes\Data	Datenverzeichnis

Tabelle 18.1: Verzeichnispfade bei einer Gemeinsamen Installation

Praxistipp: Sie können im Windows Explorer mit Variablen auf Verzeichnisse zugreifen. Einige Variablen sind in Tabelle 18.2 aufgelistet.

Verzeichnis	Variable
C:\ProgramData\	%programdata%
C:\Users\<User>\AppData\Local\	%localappdata%

Tabelle 18.2: Variablen zum Zugriff auf Verzeichnisse

2. Anpassen der Installation zur automatischen Client-Konfiguration

Mit wenigen Anpassungen können Sie die Konfiguration beim ersten Client-Start vollständig automatisieren. Der Endanwender muss in diesem Fall weder wissen, welchen Namen er einzugeben hat, noch wie sein Mailserver heißt, sondern nur noch das Kennwort kennen.

Anpassen der Vorgabe-notes.ini

Die Vorgabe-notes.ini liegt im Verzeichnis: C:\ProgramData\HCL\Notes\Data

Sie enthält nur wenige Zeilen:

```
[Notes]
KitType=1
SharedDataDirectory=C:\ProgramData\HCL\Notes\Data\Shared
UserInterface=de
InstallType=6
InstallMode=1
NotesProgram=C:\Program Files (x86)\HCL\Notes\
```

Öffnen Sie die Datei in einem Editor und fügen Sie die folgende Zeile hinzu:

```
ConfigFile=C:\ProgramData\HCL\Notes\Data\setup.txt
```

Wenn Sie den Eintrag am Ende angefügt haben, vergessen Sie nicht, danach noch eine Leerzeile hinzuzufügen,

Speichern und schließen Sie die Datei.

Erstellen einer Konfigurationsdatei

Erstellen Sie mit dem Editor im Verzeichnis C:\ProgramData\HCL\Notes\Data die Datei setup.txt. Fügen Sie die folgenden Einträge ein:

```
UserName=<Eindeutiger Name des Benutzers>
Domino.Name=<Name des Domino-Servers>
Domino.Address=<Hostname des Servers oder IP-Adresse>
Domino.Server=1
Additional.Services=-1
```

Sie können auch noch zahlreiche andere Vorgaben setzen. Eine Übersicht über mögliche Variablen liefert Anhang C.

Richtig interessant wird die Sache erst, wenn Sie Windows-Umgebungsvariablen verwenden. (Achtung: Diese müssen beim Anmelden in Windows auch gesetzt werden!)

In der Datei notes.ini:

```
ConfigFile=%ALLUSERSPROFILE%\ApplicationData\HCL\Notes\Data\setup.txt
```

```
ConfigFile=%HOMEDRIVE%\%HOMEPATH%\Desktop\config.txt
```

In der Konfigurationsdatei:

```
UserName=%USERNAME%
```

Diese Variable %USERNAME% macht nur Sinn, wenn der Windows-Anmeldename einem eindeutigen Namen im Domino-Verzeichnis entspricht; das kann der Benutzername oder Kurzname sein, aber auch Vor- oder Nachname, wenn diese eindeutig sind.

Unter der Voraussetzung, dass Sie einen ID-Vault eingeführt haben (siehe Kap. 6.2.1 Einen ID-Vault einrichten, ab Seite 138) und sich die ID-Datei des Benutzers darin befindet, sollte der Benutzer beim ersten Notes-Client-Start nur noch nach dem Kennwort gefragt werden.

18.2.3.3. Was Sie nach dem Ausrollen der Clients bedenken sollten

Für eine besonders tolle Performance ist der Notes-Standard-Client nicht berühmt – und der besondere Trick, der den Client schnell starten lässt, existiert auch nicht. Dennoch gibt es einiges, das Sie beachten sollten:

Wechseln Sie auf das neueste Dateiformat (ODS)

Verwenden Sie auch im Notes-Client unbedingt das neueste Dateiformat ODS 53! Das Dateiformat wird am Client nicht automatisch aktualisiert, auch nicht, wenn Sie es am Server einsetzen. Es gibt jedoch die Möglichkeit, ODS 53 sehr komfortabel über die Desktoprichtlinie auszurollen. Setzen Sie im Register **Mail** ganz unten die Eigenschaft **Alle lokalen NSF-Datenbanken auf die neueste ODS-Version aktualisieren**:

Client-Einstellungen	Wie diese Einstellung angewendet wird:
Dokumenteinstellungen automatisch abrufen:	<input checked="" type="checkbox"/> Wert nicht festlegen
Server kann neue Mail abfragen und, sofern solche vorhanden ist, eine Replizierung auslösen:	<input checked="" type="checkbox"/> Wert nicht festlegen
Automatisches Failover, wenn ein Server ausfällt:	<input checked="" type="checkbox"/> Wert nicht festlegen
Alle lokalen NSF-Datenbanken auf die neueste ODS-Version aktualisieren:	<input type="checkbox"/> Wert nicht festlegen

Abbildung 18.3: Desktopeinstellungen – Client-Einstellungen

Vergessen Sie auch nicht, das Häkchen bei **Wert nicht festlegen** zu entfernen!

Schalten Sie den Virenschanner ab

Etwa 55 % der Dateien im Notes-Datenverzeichnis ändern sich täglich! Sollten Sie daher einen Virenschanner im Einsatz haben, nehmen Sie das ganze Datenverzeichnis oder zumindest die folgenden Dateitypen vom Scannen aus:

- *.ns*
- *.ndk
- *.xml
- *.properties
- *.jar

Vergrößern Sie den lokalen Designcache

Der lokale Designcache cache.ndk fungiert als Zwischenspeicher für Gestaltungselemente von Serverdatenbanken (die Wichtigste ist die Maildatenbank!), also Masken, Teilmasken, Ansichten, LotusScript-Code etc., was die Übertragung von Informationen zwischen Server und Client dramatisch verringert. Das Design einer Serveranwendung wird beim ersten Zugriff in der Datei cache.ndk gespeichert und dann von dort abgerufen. Das reduziert den Traffic zwischen Server und Client um bis zu 4.000 % – dieser wäre ohne die Verwendung des Caches also vierzig Mal höher!

Die maximale Größe der Datei cache.ndk ist per Vorgabe 30 MB. Dabei wird nach dem FIFO-Prinzip (first in – first out) gearbeitet, d. h. wenn kein Platz mehr vorhanden ist, werden die ältesten Designelemente gelöscht, um Platz für neue zu schaffen. Arbeiten Sie und Ihre Anwender mit vielen Serveranwendungen, empfiehlt es sich, den Wert zu erhöhen, z. B. auf 100 MB.

Das geht auch über das Setzen von notes.ini-Variablen, welche Sie über die Desktoprichtlinie ausrollen können. Beachten Sie, dass Sie zwei Variablen setzen müssen:

```
UserSetCacheQuota=1
UserCacheQuotaSize=kilobytes
```

Mögliche Werte sind z. B. 102400 für 100 MB oder 153600 für 150 MB.

Das lokale Zwischenspeichern des Designs kann auch Probleme verursachen. So können Masken oder Ansichten ein altes Design aufweisen. Davon abgeleitet können beim Öffnen einer Datenbank Fehler angezeigt werden. Beenden Sie in diesem Fall den Notes-Client und löschen Sie die Datei cache.ndk, sie wird beim nächsten Start neu erstellt und der Cache neu aufgebaut.

18.3. HCL Nomad: Notes auf iPad, iPhone und Co.

Der unter iOS und Android laufende **HCL Nomad** entspricht technisch weitestgehend einem Notes-Basic-Client und kann als solcher auch Mail und Applikationen ausführen. Dadurch wird nahezu jede Domino-Anwendung ohne Anpassungen auf dem mobilen Gerät lauffähig.

Die Features des HCL Nomad-Clients im Detail:

- > HCL Nomad ermöglicht es, direkt auf Domino-Anwendungen auf dem Server zuzugreifen, inklusive E-Mail, Kalender und Kontakte.
- > Anwendungen funktionieren ohne Anpassungen auf dem mobilen Gerät, einschließlich LotusScript.
- > LotusScript wurde um mobile Klassen erweitert; so lässt sich beispielsweise mit der GPS-Funktionalität des Geräts der aktuelle Standort bestimmen.
- > Auch andere Funktionalitäten mobiler Geräte lassen sich nutzen. So können Sie etwa auf die Kamera und die damit erstellten Fotos auf Ihrem Gerät zugreifen.
- > Informationen werden lokal verschlüsselt.
- > HCL Nomad enthält ausgewählte Funktionen des Panagenda MarvelClients, die eine leichtere Konfiguration des Clients ermöglichen.

Der Nomad-Client wird unabhängig vom Domino-Server weiterentwickelt – laden Sie die aktuelle Version einfach aus dem entsprechenden App-Store.

Damit Sie mit HCL Nomad auf einen Domino-Server zugreifen können, ist serverseitig keinerlei Konfiguration nötig. Um alle Funktionen in Nomad nutzen zu können, muss der Domino-Server jedoch mindestens Version 9.0.1 oder höher sein.

18.4. POP- und IMAP-Clients

Mit den Postfachprotokollen POP3 und IMAP4 können Sie fast jeden externen Mail-Client dazu überreden, mit Ihrem Domino-Server zusammenzuarbeiten. Allerdings ist die Zusammenarbeit begrenzt: Postfachprotokolle dienen nur dazu, Mails abzufragen, Kalender, Aufgaben und Kontakte bleiben außen vor. Immerhin können Sie ein Nachschlagen von Mail-Adressen über eine zusätzliche LDAP-Anbindung ermöglichen. Wenn für eine bestimmte Anwendergruppe ein Notes-Client nicht infrage kommt, sollten Sie sich überlegen, ob Webmail (iNotes oder Verse) nicht die bessere Lösung bietet.

18.4.1. Vergleich zwischen POP3 und IMAP4

Eigenschaft	POP3	IMAP4
Ports	110/995	143/993
Datenbankkonvertierung nötig	Nein	Ja
Konfiguration nötig	Nein	Ja
Öffentliche Ordner	Nein	Ja
Offlinefähig	Ja	Client-abhängig
E-Mails gespeichert am	Client (Kopie am Server)	Server (Kopie am Client)

Tabelle 18.3: Vergleich zwischen POP3 und IMAP4

Beide Tasks können über ein Programmdokument vom Typ »Nur beim Serverstart« bleibend eingebunden werden. Ein manueller Start ist über folgende Befehle möglich:

```
load pop3
```

```
load imap
```

Die Protokolle POP3 und IMAP4 holen nur Mails ab, damit externe Clients auch Mails senden können, müssen Sie zusätzlich SMTP zur Verfügung stellen.

18.4.2. POP3

Standardmäßig werden Mails via POP3 (Post Office Protokoll Version 3) vom Server heruntergeladen, sodass die Maildatenbank am Server anschließend leer ist. Die meisten Clients erlauben es jedoch, Kopien der Mails am Server zu belassen und diese erst zu löschen, wenn sie auch lokal gelöscht wurden.

Die Authentifizierung via POP3 erfolgt über Benutzername und Internetkennwort, ein anonymer Zugriff ist nicht möglich.

Haben Sie im Serverdokument die Einstellung **Internet-Konfigurationen aus Server-Internet-Site-Dokumenten laden** auf »Aktiviert« gesetzt, müssen Sie, um eine Anmeldung via POP3 zu ermöglichen, zusätzlich ein POP3-Site-Dokument erstellen.

Um ein POP3-Site-Dokument zu erstellen:

1. Wechseln Sie im Domino-Administrator zum Register **Konfiguration** und wählen Sie **Web > Internet-Sites**. Klicken Sie auf die Schaltfläche **Internet-Site hinzufügen... > POP3**.
2. Geben Sie einen Namen und eine Organisation ein.

3. Wenn der Site Hostnamen oder IP-Adressen zugeordnet sind, führen Sie diese im Feld **Hostnamen und Adressen, die dieser Seite zugeordnet werden** der Reihe nach auf. (Drücken Sie [Eingabe] für einen neuen Eintrag.)
4. Geben Sie im Feld **Domino-Server, die diese Website hosten** an, welcher Server zuständig ist. Sie können auch mehrere Server oder einen * für alle Server eingeben.

The screenshot shows the 'POP3-Site' configuration page in the 'Allgemein' register. The 'Site-Informationen' section contains the following fields:

- Beschreibender Name dieser Site: DOM POP3
- Organisation: COB
- Hostnamen und Adressen, die dieser Site zugeordnet werden: 192.168.1.100
- Domino-Server, die diese Website hosten: DOM/COB/AT

Abbildung 18.4: POP3-Site, Register Allgemein

5. Achten Sie darauf, dass im Register Sicherheit im Bereich **TCP-Authentifizierung** im Feld **Name und Kennwort** »Ja« ausgewählt ist (Vorgabe):

The screenshot shows the 'POP3-Site POP3 DOM' configuration page in the 'Sicherheit' register. The 'TCP-Authentifizierung' section has the 'Name und Kennwort' field set to 'Ja'. The 'SSL-Authentifizierung' section has the 'Name und Kennwort' field set to 'Nein' and the 'Client-Zertifikat' field set to 'Nein'.

Abbildung 18.5: POP3-Site, Register Sicherheit

6. Wiederholen Sie den Schritt im Abschnitt **SSL-Authentifizierung**, wenn Sie POP3 mit TLS absichern wollen. (Mehr zum Thema TLS finden Sie im Kap. 14.6.1 Transport Layer Security (TLS), ab Seite 388.)
7. Speichern und schließen Sie das Dokument.

18.4.3. IMAP

Bei IMAP4 (Internet Message Access Protocol Version 4) verbleiben die Mails standardmäßig auf dem Server. Das hat den Vorteil, dass Sie bei Benutzung mehrerer Clients immer den gleichen Datenbestand sehen. Auch das Durchsuchen von Mails erfolgt serverseitig. Verfügen Sie über keine Netzwerkverbindung zu Ihrem Mailserver, ist in der Regel auch kein Zugriff auf Ihre Mails möglich. Einige Clients können jedoch auch lokale Kopien der Mails anlegen, auf die sie im Offline-Modus zurückgreifen können. Bei wiederhergestellter Netzwerkverbindung werden die Daten dann mit dem Mailserver abgeglichen (synchronisiert).

IMAP erlaubt auch den Zugriff auf Maildatenbanken anderer Benutzer sowie auf gemeinsam genutzte Maildatenbanken, die **Öffentliche Ordner** genannt werden.

Die Authentifizierung erfolgt über Benutzername und Internetkennwort, ein anonymer Zugriff ist nicht möglich.

Im Gegensatz zu POP3 muss die Maildatenbank für die Verwendung von IMAP zusätzlich vorbereitet werden. Dies geschieht über folgenden Serverkonsolenbefehl:

```
load convert mail\datenbank.nsf -e
```

Achtung: Ohne Konvertierung ist der Zugriff auf eine Maildatei via IMAP nicht möglich!

Um öffentliche Ordner nutzen zu können, müssen Sie für den IMAP-Zugriff ein Internet-Site-Dokument erstellen. Dazu muss im Serverdokument, Register **Allgemein**, die Einstellung **Internet-Konfigurationen aus Server-Internet-Site-Dokumenten laden** aktiviert sein.

Um ein IMAP-Site-Dokument zu erstellen:

1. Wechseln Sie im Domino-Administrator zum Register **Konfiguration** und wählen Sie **Web > Internet-Sites**. Klicken Sie auf die Schaltfläche **Internet-Site hinzufügen... > IMAP**.
2. Geben Sie einen Namen und eine Organisation ein.
3. Wenn der Site Hostnamen oder IP-Adressen zugeordnet sind, führen Sie diese im Feld **Hostnamen und Adressen, die dieser Seite zugeordnet werden** der Reihe nach auf. Drücken Sie [Eingabe] für einen neuen Eintrag.
4. Geben Sie im Feld **Domino-Server, die diese Website hosten** an, welcher Server zuständig ist. Sie können auch mehrere Server oder einen * für alle Server eingeben.

Site-Informationen	
Beschreibender Name dieser Site:	IMAP DOM
Organisation:	COB
Hostnamen und Adressen, die dieser Site zugeordnet werden:	212.186.208.69
Domino-Server, die diese Website hosten:	DOM/COB/AT

Abbildung 18.6: IMAP-Site

5. Sie müssen die Authentifizierung über Namen und Kennwort erlauben. Wechseln Sie dazu zum Register **Sicherheit** und wählen Sie im Feld **Name und Kennwort** »Ja« aus:

TCP-Authentifizierung	
Name und Kennwort:	<input checked="" type="radio"/> Ja <input type="radio"/> Nein

SSL-Authentifizierung	
Name und Kennwort:	<input checked="" type="radio"/> Ja <input type="radio"/> Nein
Client-Zertifikat:	<input type="radio"/> Ja <input checked="" type="radio"/> Nein

Abbildung 18.7: IMAP-Site, Register Sicherheit

6. Wiederholen Sie den Schritt im Abschnitt **SSL-Authentifizierung**, wenn Sie IMAP mit TLS absichern wollen. Mehr zum Thema TLS finden Sie im Kap. 14.6.1 Transport Layer Security (TLS), ab Seite 388.
7. Speichern und schließen Sie das Dokument.

18.4.4. Benutzer für POP3 oder IMAP4 anlegen

POP- oder IMAP-Benutzer können normal registriert werden – dann besitzen Sie auch eine Notes-ID, die von den beiden Internetprotokollen aber natürlich nicht verwendet wird. Wenn Sie das Personendokument händisch erstellen, beachten Sie folgende Regeln:

- > Wählen Sie im Feld **Mailsystem** »POP oder IMAP«, damit man sieht, worum es sich handelt.
- > Vergeben Sie ein Internetkennwort. Dieses Kennwort verwenden Sie später zur Authentifizierung via POP3 oder IMAP4 (und gegebenenfalls auch via SMTP).
- > Tragen Sie eine eindeutige zulässige Internetadresse ein.
- > Stellen Sie im Feld **Bevorzugtes Format für eingehende Mail** »MIME« ein, da externe Clients das Notes-Richtext-Format nicht lesen können.
- > Belassen Sie die Option **Eingehende unverschlüsselte Mail vor dem Speichern in Maildatei verschlüsseln** unbedingt auf »Nein«, weil POP3 und IMAP4 keine verschlüsselten Notes-Mails verarbeiten können.

Haben Sie das Personendokument händisch angelegt, müssen Sie auch die Maildatei händisch erstellen. Vergessen Sie dabei nicht, den Benutzer in der ACL als Editor mit dem Zusatzrecht, Dokumente zu löschen, einzutragen. Und vergessen Sie bei Verwendung von IMAP nicht, die Maildatei zu konvertieren.

18.4.5. SMTP für POP3- oder IMAP-Clients erlauben

Problematischer ist die SMTP-Anbindung. SMTP verwendet in Domino per Vorgabe einen anonymen Zugriff, externe Benutzer können sich also nicht identifizieren. Und ohne Authentifizierung gibt es kein Relaying, also kein Senden von E-Mails ins Internet. Sie haben nun zwei Möglichkeiten:

1. Sie schalten in Domino die Authentifizierung für SMTP über Namen und Kennwort ein.
2. Sie erstellen eine Ausnahme für eine IP-Adresse oder einen IP-Adressbereich.

18.4.5.1. Die Authentifizierung für SMTP erlauben

Navigieren Sie im Domino-Administrator zu **Konfiguration > Web > Internet-Sites** und öffnen Sie das Dokument für die SMTP-Eingangs-Site. Setzen Sie im Register **Sicherheit** im Bereich TCP-Authentifizierung das Feld **Name und Kennwort** auf »Ja«.



Abbildung 18.8: SMTP-Eingangs-Site

18.4.5.2. Eine Ausnahme zulassen

Wechseln Sie im Konfigurationsdokument des Servers zum Register **Router/SMTP > Beschränkungen und Steuerungen... SMTP-Eingangsteuerung** und tragen Sie jene IP-Adressen in eckigen Klammern ein, für die ein Relaying auch ohne Authentifizierung erlaubt sein soll:

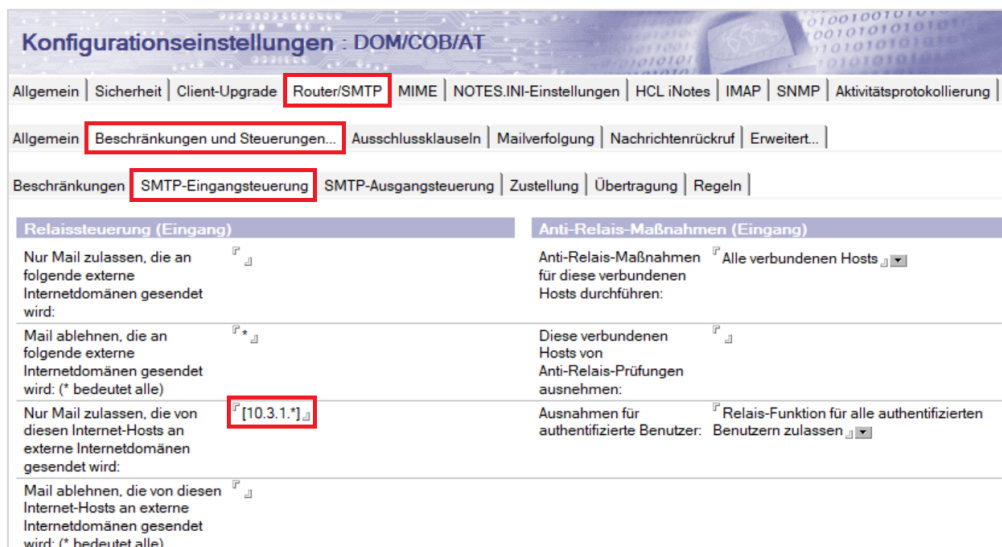


Abbildung 18.9: SMTP-Eingangsteuerung – IP-Adressen ausnehmen

Sie können mit dem Stern (*) als Platzhalterzeichen auch IP-Bereiche definieren. Um weitere IP-Adressen oder -Bereiche einzugeben, drücken Sie die Eingabetaste.

Ich empfehle, aus Sicherheitsgründen nur private (im Internet nicht geroutete) Adressbereiche (z. B. IP-Adressen, die mit 10.*, 192.168.* oder 169.254.* beginnen) zuzulassen. In diesem Fall müssen sich externe Anwender zuerst via VPN ins lokale Netzwerk einwählen, um eine private IP-Adresse zu erhalten, was die Sicherheit zusätzlich erhöht.

18.4.6. Beispiel: IMAP-Konfiguration für Microsoft Outlook 2019

18.4.6.1. Voraussetzungen

- > Am Domino-Server müssen die Tasks IMAP und SMTP laufen.
- > SMTP muss eine Authentifizierung über Namen und Kennwort erlauben.
- > Sie müssen ein Personendokument mit dem Verweis zu einer Maildatenbank angelegt haben. Im Personendokument müssen eine gültige E-Mail-Adresse und ein Internetkennwort angegeben sein.
- > Die Maildatenbank muss für IMAP konvertiert worden sein.

18.4.6.2. Vorgangsweise

Starten Sie Microsoft Outlook und geben Sie die gewünschte E-Mail-Adresse ein. Aktivieren Sie die Option **Ich möchte mein Konto manuell einrichten** und klicken Sie auf **Verbinden**:

Outlook

E-Mail-Adresse
p.schmied@cob.at

Erweiterte Optionen ^

Ich möchte mein Konto manuell einrichten

Verbinden

Abbildung 18.10: Konfiguration Outlook – Schritt 1

Wählen Sie im nächsten Schritt die Option **IMAP**. Der Dialog IMAP-Kontoeinstellungen wird angezeigt:

IMAP-Kontoeinstellungen
p.schmied@cob.at (Nicht Sie?)

Eingehende E-Mail
Server: DOM Port: 143
Verschlüsselungsmethode: Keinen

Anmeldung mithilfe der gesicherten Kennwortauthentifizierung (SPA) erforderlich

Ausgehende E-Mail
Server: DOM Port: 25
Verschlüsselungsmethode: Keinen

Anmeldung mithilfe der gesicherten Kennwortauthentifizierung (SPA) erforderlich

Zurück Weiter

Abbildung 18.11: Konfiguration Outlook – Schritt 2

Geben Sie die Servernamen ein. In meinem Beispiel reichte die Angabe des Hostnamens, in der Praxis müssen Servernamen meist voll qualifiziert (also Hostname + Domäne, z. B.: »dom.cob.at«) angegeben werden.

Geben Sie die zu verwendeten Ports ein. Für **eingehende E-Mails** wird IMAP (Port 143) verwendet und für **ausgehende E-Mails** SMTP (Port 25).

Sollten Sie TLS verwenden, wählen Sie in der Liste **Verschlüsselungsmethode** »SSL/TLS« aus.

Klicken Sie auf **Weiter**.

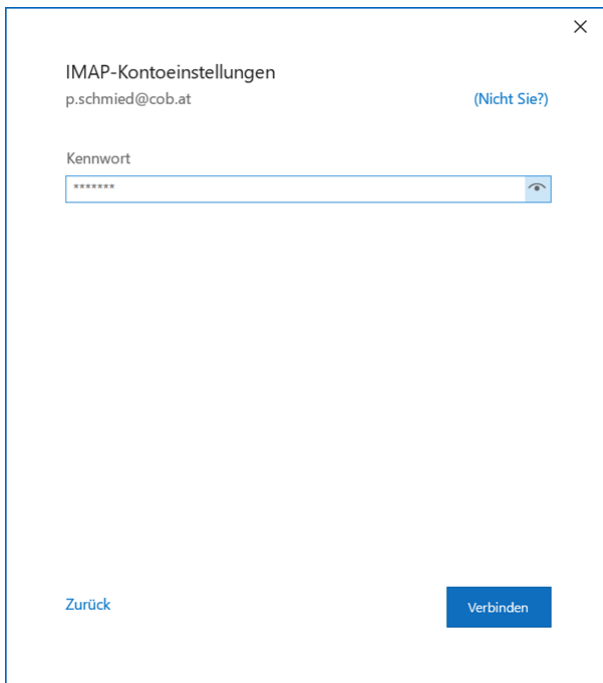


Abbildung 18.12: Konfiguration Outlook – Schritt 3

Hinterlegen Sie das Kennwort und klicken Sie auf **Verbinden**.

Sehen Sie die folgende Meldung, hat die Anbindung geklappt:

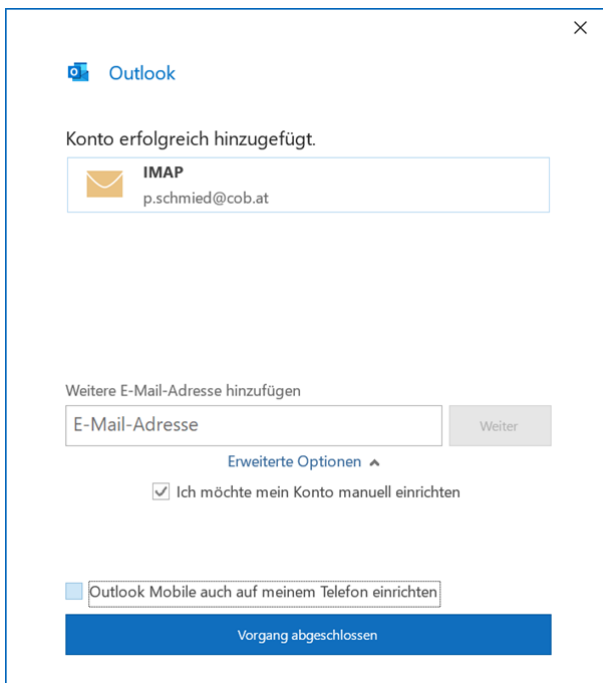


Abbildung 18.13: Konfiguration Outlook – Schritt 4

Sehen Sie hingegen die Meldung »Da hat etwas nicht geklappt«, ist möglicherweise die SMTP-Authentifizierung am Domino-Server nicht erlaubt. Outlook geht nämlich fix davon aus, dass eine Authentifizierung für den Postausgangsserver (SMTP) nötig ist, und da der Assistent nicht anbietet, sie abzuschalten, müssen Sie diese (zumindest kurzfristig) zulassen, sonst können Sie die Einrichtung nicht abschließen.

Klicken Sie nach dem Zulassen der SMTP-Authentifizierung im Assistenten auf **Wiederholen**.

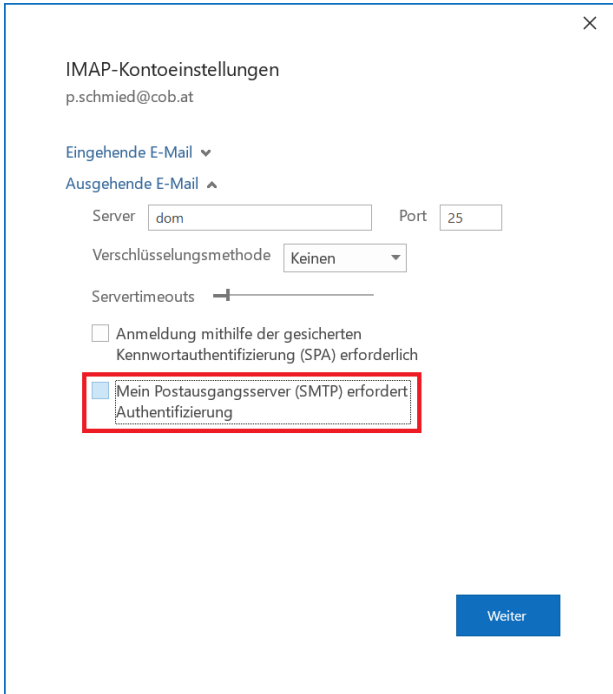


Abbildung 18.14: Konfiguration Outlook – Authentifizierung abschalten

Sollten Sie die Authentifizierung für SMTP später in Outlook abschalten wollen, gehen Sie auf **Datei > Informationen > Kontoinformationen** und klicken Sie auf **Kontoeinstellungen > Servereinstellungen**.

Erweitern Sie den Bereich **Ausgehende E-Mail** und entfernen Sie das Häkchen bei **Mein Postausgangsserver (SMTP) erfordert Authentifizierung**.

Das Aktivieren der SMTP-Authentifizierung ist in Kap. 18.4.5 SMTP für POP3- oder IMAP-Clients erlauben, ab Seite 477, beschrieben.

18.4.6.3. Den Zugriff auf Ordner konfigurieren

Standardmäßig zeigt Outlook nur den Posteingang und den Papierkorb an. Wollen Sie auch auf andere Ordner zugreifen können, müssen Sie diese zuerst abonnieren. Klicken Sie dazu in Outlook mit der rechten Maustaste auf den Posteingang und wählen Sie den Befehl **IMAP-Ordner...**

Wählen Sie im angezeigten Dialog alle gewünschten Ordner aus (in unserem Beispiel den Ordner »Kunden«) und klicken Sie auf die Schaltfläche **Abonnieren**:

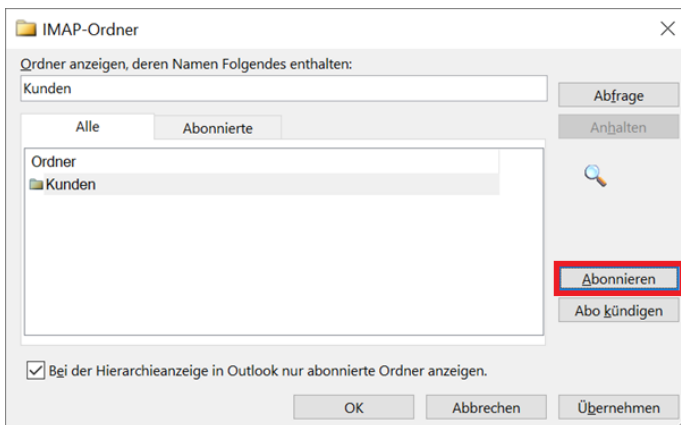


Abbildung 18.15: Konfiguration Outlook – Ordner abonnieren

Nach Klicken auf **Übernehmen** oder **OK** werden die Ordner angezeigt:

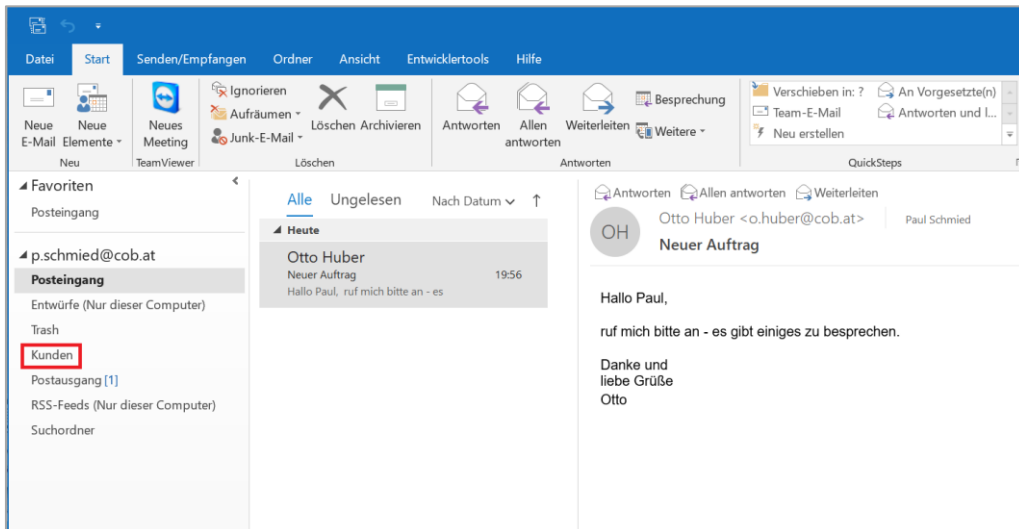


Abbildung 18.16: Outlook mit abonniertem Ordner

18.4.7. Öffentliche Ordner einbinden

Um Datenbanken als öffentliche Ordner zu verwenden, müssen folgende Bedingungen erfüllt sein:

- > Die Datenbank muss auf der Mailschablone (mail11.ntf, mail10.ntf oder mail9.ntf) basieren, andere Anwendungen werden nicht unterstützt.
- > Die Datenbank muss über den Befehl `load convert -e` für IMAP aktiviert worden sein.
- > Autorisierte Benutzer müssen in der ACL namentlich oder via Gruppenzuordnung aufgeführt sein. Ansonsten sehen Sie zwar öffentliche Ordner, aber keine Inhalte. Ein vollwertiges Arbeiten ist erst ab dem Editor-Recht möglich.

Damit eine Datenbank als öffentlicher Ordner im IMAP-Client angezeigt wird, muss im IMAP-Site-Dokument im Feld **Datenbanklinks für öffentliche Ordner** ein Verweis in Form eines Anwendungslinks eingefügt werden:



Abbildung 18.17: IMAP-Site mit Datenbanklink für öffentliche Ordner

Im Feld **Präfix für öffentliche Ordner** geben Sie an, unter welcher Rubrik die Datenbank im IMAP-Client dargestellt werden soll. Unterhalb dieser Rubrik werden zuerst der Datenbanktitel, dann die einzelnen Ordner angezeigt, z. B.: Öffentliche Ordner > Projekte > Domino Admin-Buch

18.4.7.1. Öffentliche Ordner anderer Benutzer

Öffnen Sie das Konfigurationsdokument des Servers und navigieren Sie zum Register **IMAP > Öffentliche Ordner und Ordner anderer Benutzer**:



Abbildung 18.18: Konfigurationsdokument, Register IMAP > Öffentliche Ordner und Ordner anderer Benutzer

Unterstützung öffentlicher Ordner und Ordner anderer Benutzer: Ist die Option aktiviert, werden auch die Ordner anderer Benutzer, auf die ein Anwender Zugriff hat, angezeigt.

Alle öffentlichen Ordner und Ordner anderer Benutzer aufnehmen, wenn eine Ordnerliste angefordert wird: Ist diese Option aktiviert, sehen Clients immer alle öffentlichen Ordner. Ist sie deaktiviert, sehen nur Clients, die die NAMESPACE-Erweiterung unterstützen, öffentliche Ordner.

18.4.7.2. Verwenden von öffentlichen Ordnern am Beispiel von Outlook

Legen Sie eine neue Maildatenbank an – in unserem Beispiel mail\projekte.nsf. Vergeben Sie einen passenden Datenbanktitel (dieser wird später als Präfix angezeigt!), z. B. »Projekte«.

Erstellen Sie mit dem Befehl **Bearbeiten > Kopieren als > Anwendungslink** einen Anwendungslink von der Maildatenbank »Projekte«. Öffnen Sie das IMAP-Site-Dokument und navigieren Sie zum Register **Öffentliche Ordner**. Fügen Sie den Anwendungslink durch Drücken von [Strg]+[V] aus der Zwischenablage in das Feld **Datenbanklinks für öffentliche Ordner** ein:



Abbildung 18.19: IMAP-Site mit Link zur Datenbank Projekte

Fügen Sie die gewünschten Benutzer als Editoren zur Zugriffskontrollliste hinzu.

Aktivieren Sie den IMAP-Zugriff auf die Datenbank über folgenden Befehl:

```
load convert mail\projekte.nsf -e
```

Legen Sie nun die Ordner an, die gemeinsam genutzt werden sollen:

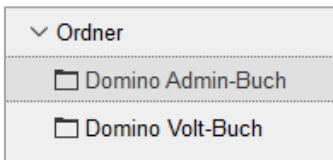


Abbildung 18.20: Datenbank »Projekte« mit Ordnern

Beim nächsten Zugriff von Outlook sollten die zusätzlichen Ordner bei Aufruf des Befehls **IMAP-Ordner...** unter dem angegebenen Präfix in der Liste aufscheinen:

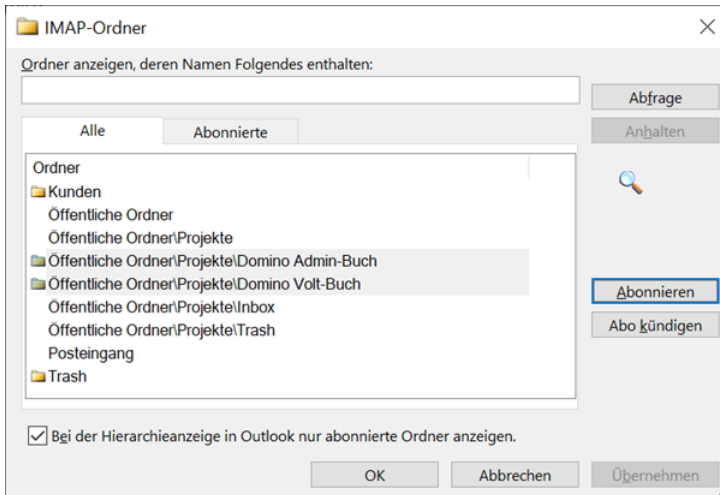


Abbildung 18.21: Konfiguration Outlook – öffentliche Ordner abonnieren

Wählen Sie die Ordner aus und klicken Sie auf **Abonnieren**. Die Ordner sollten nun sichtbar sein:

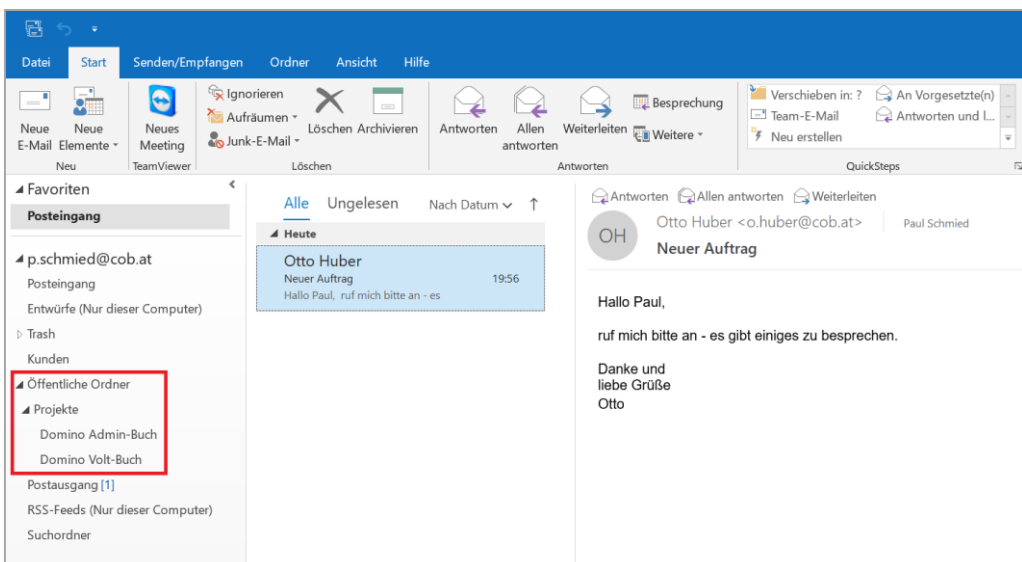


Abbildung 18.22: Outlook mit eingebundenen öffentlichen Ordnern

Beachten Sie, dass ein IMAP-Client nur auf Informationen zugreifen kann, die sich auf demselben Server befinden, auf dem auch der IMAP-Server-Dienst ausgeführt wird.

18.4.8. Auch IMAP verrät die Identität Ihres Servers

Wie sich Ihr IMAP-Server auf Anfragen auf dem Port 143 meldet, können Sie unter Windows mit dem Programm Telnet überprüfen. Eröffnen Sie dazu einfach eine Eingabeaufforderung und geben Sie folgenden Befehl ein:

```
C:\>telnet localhost 143
```

Sie erhalten die folgende Meldung zurück:

```
OK Domino IMAP4 Server Release 11.0.1FP2 ready Sat, 31 Oct 2020 18:36:30 +0100
```

Wenn es Sie stört, dass der IMAP-Server bei der Anmeldung seine Identität preisgibt, können Sie das im Konfigurationsdokument Register **IMAP > Erweitert** abstellen:

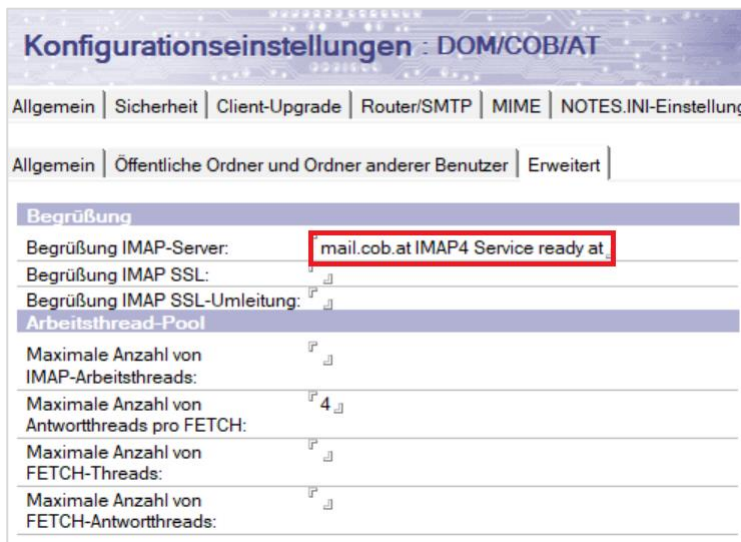


Abbildung 18.23: Konfigurationsdokument, Register IMAP > Erweitert

Hier brauchen Sie keinen Platzhalter für Datum und Uhrzeit, diese werden automatisch ergänzt:

```
OK mail.cob.at IMAP4 Service ready at Sat, 31 Oct 2020 22:38:53 +0100
```

18.4.9. Konfiguration von LDAP am Beispiel von Outlook 2019

Um Outlook zu ermöglichen, E-Mail-Adressen abzufragen, müssen wir noch den Verzeichnisdienst (LDAP) des Domino-Servers bemühen. Sorgen Sie dafür, dass der LDAP-Task auf Ihrem Domino-Server läuft und unter der Portnummer 389 (bzw. 636 bei Verwendung von TLS) antwortet.

Gehen Sie zum Einrichten von LDAP in Outlook auf **Datei > Informationen > Kontoinformationen** und klicken Sie auf die Schaltfläche **Kontoeinstellungen**. Wählen Sie im Drop-Down-Menü den ersten Befehl **Kontoeinstellungen...** und navigieren Sie im angezeigten Dialog zum Register **Adressbücher**. Klicken Sie auf die Schaltfläche **Neu...**

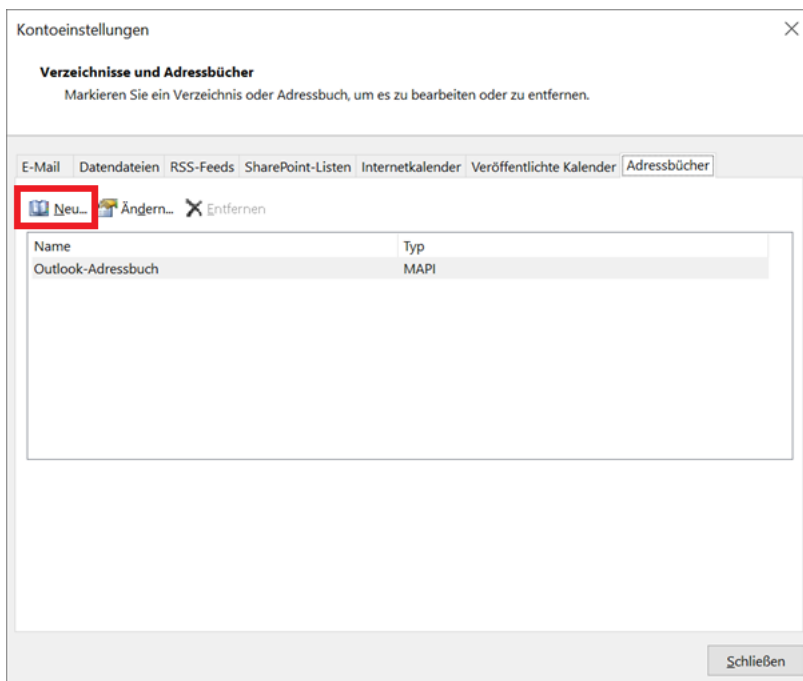


Abbildung 18.24: Konfiguration Outlook – Authentifizierung abschalten

Wählen Sie **Internetverzeichnisdienst (LDAP)** und klicken Sie auf die Schaltfläche **Weiter >**:

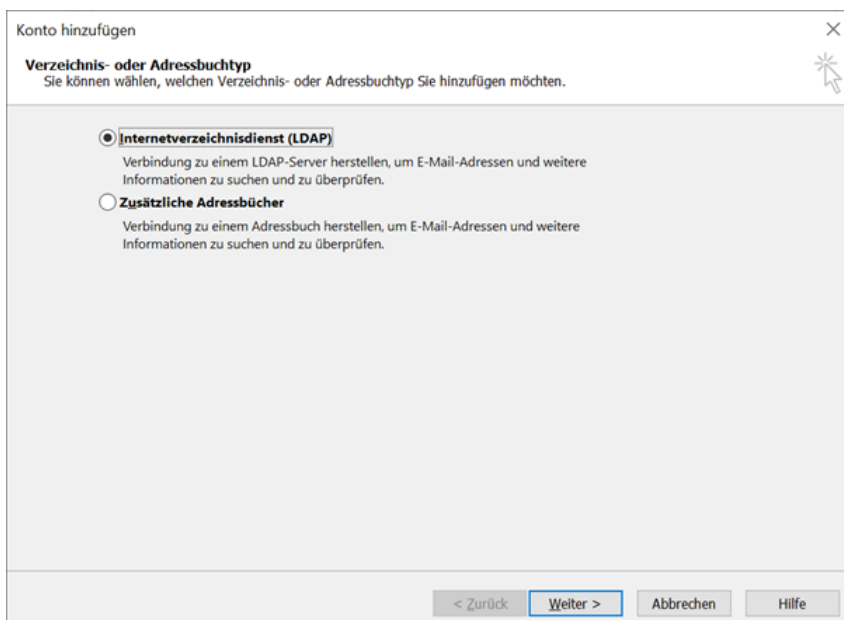


Abbildung 18.25: Konfiguration Outlook – Authentifizierung abschalten

Geben Sie den Namen Ihres Servers ein. Gegebenenfalls müssen Sie den Namen voll qualifiziert (also plus Domäne, z. B.: »dom.cob.at«) eingeben. Erfordert Ihr Verzeichnisdienst eine Authentifizierung, aktivieren Sie das Feld **Server erfordert Anmeldung** und tragen Sie Benutzername und Kennwort ein:

Konto hinzufügen

Einstellungen für den Verzeichnisdienst (LDAP)
Geben Sie die Einstellungen ein, die für den Zugriff auf Informationen eines Verzeichnisdiensts erforderlich sind.

Serverinformationen
Geben Sie den Namen des Verzeichnisseservers ein, den Sie von Ihrem Internetdienstanbieter oder Systemadministrator erhalten haben.
Servername:

Anmeldeinformationen
 Server erfordert Anmeldung
Benutzername:
Kennwort:
 Gesicherte Kennwortauthentifizierung (SPA) erforderlich
[Weitere Einstellungen...](#)

< Zurück [Weiter >](#) Abbrechen Hilfe

Abbildung 18.26: Konfiguration Outlook – Authentifizierung abschalten

Wenn Sie eine verschlüsselte Verbindung via TLS aufbauen wollen, klicken Sie auf **Weitere Einstellungen...** und aktivieren Sie die Option **Secure Sockets Layer verwenden**. Klicken Sie auf **Weiter >** und **Fertig stellen**. Danach ist das Nachschlagen von E-Mail-Adressen möglich:

Namen auswählen: dom

Suchen: Nur Name Mehr Spalten **Adressbuch**
christian dom - Weitere Adressbücher [Erweiterte Suche](#)

Name	E-Mail-Adresse	E-Mail-Typ	Telefon geschäftlich	Büro
Christian Buchacher/COB/AT	cb@cob.at	SMTP	+4313289525	

Christian Buchacher/COB/AT

Abbildung 18.27: Konfiguration Outlook – Authentifizierung abschalten

18.5. Microsoft Outlook über HTMO anbinden

Microsoft Outlook 2013/2016/2019 spricht das Protokoll EAS (Exchange ActiveSync) und kann sich daher wie ein mobiles Gerät mit einem normalen HCL Traveler-Server verbinden und Mails und Kalender abgleichen. Ein normal konfigurierter Traveler-Server ist aber nicht dafür ausgelegt,

mehr als eine Handvoll Outlook-Clients zu bedienen, weshalb Sie auf HTMO zurückgreifen sollten. Bei HTMO (HCL Traveler for Microsoft Outlook) handelt es sich einerseits um einen speziell konfigurierten Traveler-Server und andererseits um einen lokal zu installierenden Ad-In-Client, der innerhalb von Outlook Zugriff auf Spezialfunktionen gewährt. Dazu gehört die Möglichkeit, Abwesenheitsmeldungen zu konfigurieren, verschlüsselte Mails zu lesen, Räume zu suchen und zu reservieren, das Notes-ID-Kennwort zu ändern, Delegierungen zu erstellen und einiges mehr.

Outlook verwendet lokal eine OST-Datei, serverseitig werden die Daten in einer Maildatenbank (*.nsf) gespeichert. Der Ad-In-Client verwendet zum Zugriff auf einige Funktionen REST-Services.

HTMO läuft in der aktuellen Version 3.0.2 nur auf 64-Bit Domino mit einem 64-Bit Traveler auf 64-Bit Windows. Es ist bis auf Weiteres auch kein anderes Betriebssystem angekündigt. Unterstützt werden Domino 10.x mit Traveler 10.x oder höher.

Achtung: Nach der Konfiguration des Traveler-Servers als HTMO steht dieser exklusiv für Outlook-Clients zur Verfügung und kann keine mobilen Geräte mehr bedienen. Sollten Sie also auch mobile Geräte anbinden wollen, brauchen Sie einen zweiten Traveler-Server!

18.5.1. Eigenschaften im Detail

18.5.1.1. Mail

- > Erstellen, Bearbeiten, Löschen, Senden und Empfangen von Mail
- > Suchen, Filtern und Kategorisieren von Mails
- > Erstellen und Verschieben von Ordnern
- > Unterstützung von Type-Ahead und Letzte Kontakte
- > Unterstützung für bis zu 50 GB große Maildatenbanken
- > Verschlüsseln und Signieren von Nachrichten, wenn mit dem Server verbunden
- > Abwesenheitsmeldungen senden
- > Unterstützung für das Abschneiden von Nachrichten, die älter als 30 Tage sind (vom Administrator einstellbar). Doppelklicken auf eine abgeschnittene Nachricht lädt diese vollständig.

18.5.1.2. Kalender

- > Erstellen, Aktualisieren, Löschen von Terminen
- > Erstellen, Akzeptieren, Absagen von Einladungen
- > Finden und Reservieren von verfügbaren Räumen
- > Einsehen der Verfügbarkeit von Personen, Räumen und Ressourcen
- > Anzeige von Rich-Text-Inhalten wie Abschnitte und Tabellen
- > Keine Unterstützung von Anhängen und eingebetteten Bildern in Kalendereinträgen

18.5.1.3. Kontakte

- > Erstellen, Aktualisieren und Löschen von Kontakten.

18.5.1.4. Andere Eigenschaften

- > Freigabe der eigenen Maildatenbank für andere Benutzer
- > Einsicht in Größenbeschränkungen

18.5.2. Konfiguration des Traveler-Servers für Outlook

Nach der Installation des Traveler-Servers (Details zur Installation finden Sie in Kap. 15.2, ab Seite 418) muss dieser für die exklusive Verwendung mit Outlook wie folgt konfiguriert werden:

1. Fügen Sie zur notes.ini des Traveler-Servers die folgende Variable hinzu:

```
NTS_OUTLOOK_ONLY=true
```

Nach einem Neustart wird im Serverdokument statt des Registers Traveler das Register **Microsoft Outlook** angezeigt. Hier können Sie unter anderem die URLs für »Freebusy« und Kennwortmanagement hinterlegen, die vom Outlook-Add-In verwendet werden.

2. Fügen Sie zur notes.ini des Traveler-Servers die folgende Einstellung hinzu:

```
NTS_SMIME_SUPPORT=true
```

Damit aktivieren Sie das Signieren und Verschlüsseln über X.509-Zertifikate.

3. Um die Konfiguration in Grenzen zu halten, werden per Vorgabe alle Abfragen gegen den Mailserver des Benutzers ausgeführt. Sollten Sie (etwa aus Performancegründen) lokale Repliken auf dem HTMO-Server verwenden und es sich dabei nicht um den Home-Server der Benutzer handeln, setzen Sie die folgende notes.ini-Variablen:

```
NTS_TRAVELER_AS_LOOKUP_SERVER=true
```

18.5.3. Aktivieren von REST-Services

4. Im nächsten Schritt müssen Sie REST-Services aktivieren. Wählen Sie dazu im Admin-Client im Register **Konfiguration** die Ansicht **Web > Internet-Sites**.
5. Wenn es noch kein Internet-Site-Dokument für den Traveler-Server gibt, erstellen Sie eines, ansonsten bearbeiten Sie das vorhandene Dokument.
6. Wählen Sie im Register Konfiguration den Bereich Domino Access-Services ganz unten. Wir müssen die Services Mail und Freebusy aktivieren, welche in der Liste nicht angeboten werden. Fügen Sie dazu der Reihe nach im Feld **Neues Schlüsselwort** die Begriffe »Mail« und »Free-Busy« zur Liste **Aktivierte Services** hinzu:

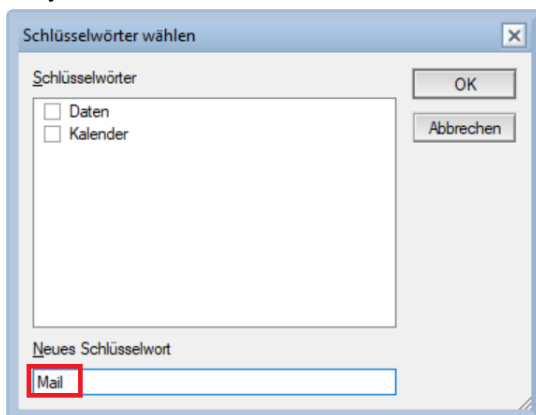


Abbildung 18.28: Schlüsselwort »Mail« hinzufügen

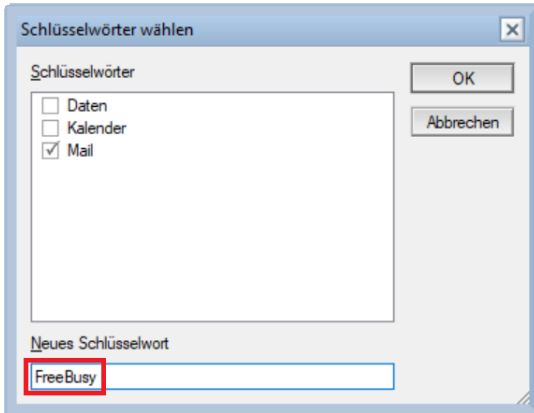


Abbildung 18.29: Schlüsselwort »FreeBusy« hinzufügen



Abbildung 18.30: Feld Aktivierte Services nach dem Hinzufügen der Schlüsselwörter

Internet-Site-Dokumente greifen nur, wenn Sie im Serverdokument, Register Allgemein, im Feld **Internet-Konfigurationen aus Server-Internet-Site-Dokumenten laden** aktiviert haben.

7. Website-Dokumente für REST-Services verwenden Maskenauthentifizierung. Um den korrekten Zugriff sicherzustellen, fügen Sie eine Regel vom Typ »Sitzungsauthentifizierung überschreiben« hinzu und tragen Sie im Feld **URL** den folgenden Wert ein:
/api/
8. Speichern Sie das Dokument und starten Sie den HTTP-Task neu.

Sie können überprüfen, ob die REST-Services erfolgreich aktiviert wurden, indem Sie in Ihrem Browser die folgende URL eintippen:

[http://\[IhrServer\]/api](http://[IhrServer]/api)

Das sollte eine Liste im JSON-Format ergeben. Überprüfen Sie, ob die Services Mail und Freebusy mit enabled=true in der Liste stehen.

```
{
  "services": [
    {
      "name": "Calendar",
      "enabled": false,
      "version": "11.0.1.v02_00",
      "href": "\\api\\calendar"
    },
    {
      "name": "FreeBusy",
      "enabled": true,

```

```

    "version":"11.0.1.v02_00",
    "href":"\api/freebusy"
  },
  {
    "name":"Core",
    "enabled":true,
    "version":"11.0.1.v02_00",
    "href":"\api/core"
  },
  {
    "name":"Data",
    "enabled":false,
    "version":"11.0.1.v02_00",
    "href":"\api/data"
  },
  {
    "name":"TravelerAdmin",
    "enabled":true,
    "version":"11.0.1.0",
    "href":"\api/traveler"
  },
  {
    "name":"Mail",
    "enabled":true,
    "version":"11.0.1.v02_00",
    "href":"\api/mail"
  },
  {
    "name":"autoupdate",
    "enabled":false,
    "version":"10.0.0",
    "href":"\api/autoupdate"
  }
]
}

```

18.5.4. Verwenden von TLS-Zertifikaten

Exchange ActiveSync verlangt eine SSL-/TLS-Verbindung. Die Outlook-Clients müssen dem Herausgeber des Zertifikats vertrauen, es muss sich aber nicht um ein kommerzielles Zertifikat handeln, sondern Sie können auch ein selbst erstelltes verwenden. (Zum Erstellen eines eigenen Zertifikats lesen Sie Kap. 14.7.5 Eigene Zertifikate erstellen, ab Seite 403.)

Die Verteilung des Zertifikats kann über eine Windows-Gruppenrichtlinie erfolgen, wenn dieses noch nicht in der Liste der vertrauenswürdigen Herausgeber enthalten ist.

18.5.5. Einstellungen für Outlook anpassen

18.5.5.1. Anpassungen im Serverdokument

Home-Server

Um sicherzustellen, dass Outlook-Benutzer ihre Maildateien delegieren können, fügen Sie den Mailserver zum Serverdokument des Traveler-Servers, Register Sicherheit, zum Feld **Vertrauenswürdige Server** hinzu.

Größenbeschränkungen

Wenn Sie Größenbeschränkungen verwenden, stellen Sie im Serverdokument, Register **Transaktionsprotokollierung**, im Feld **Größenbeschränkung erzwingen** die Option »Belegten Speicherplatz in Datei beim Hinzufügen eines Dokuments prüfen« ein:



Abbildung 18.31: Serverdokument, Register Transaktionsprotokollierung

18.5.5.2. Anpassungen im Konfigurationsdokument

SMTP innerhalb der Domäne deaktivieren

Deaktivieren Sie im Konfigurationsdokument (sollte keines existieren, erstellen Sie eines) auf dem Register **Router/SMTP > Allgemein** das Feld **SMTP ist innerhalb der lokalen Internetdomäne zulässig**:

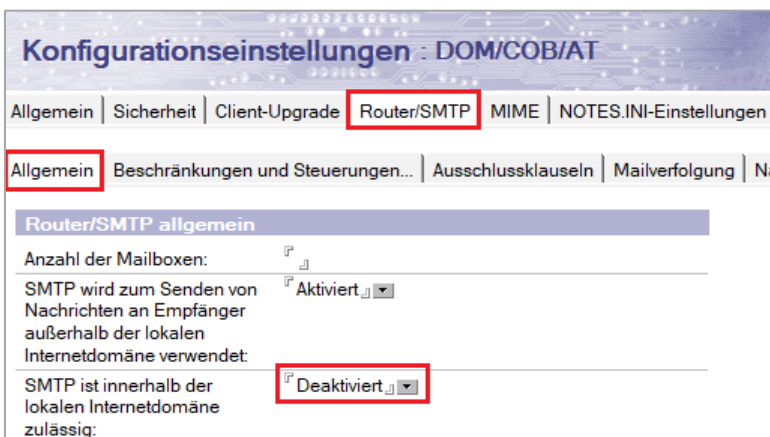


Abbildung 18.32: Konfigurationsdokument, Register Router/SMTP

Diese Einstellung erzwingt das Routen von MIME-Nachrichten als Notes-Mails, was es Outlook-Benutzern ermöglicht, verschlüsselte Mails zu lesen.

Mailkonvertierung

Sorgen Sie dafür, dass im Register **MIME > Konvertierungsoptionen > Ausgang** im Feld **Nachrichteninhalt** der Wert »Von Notes in einfachen Text und HTML« ausgewählt ist.

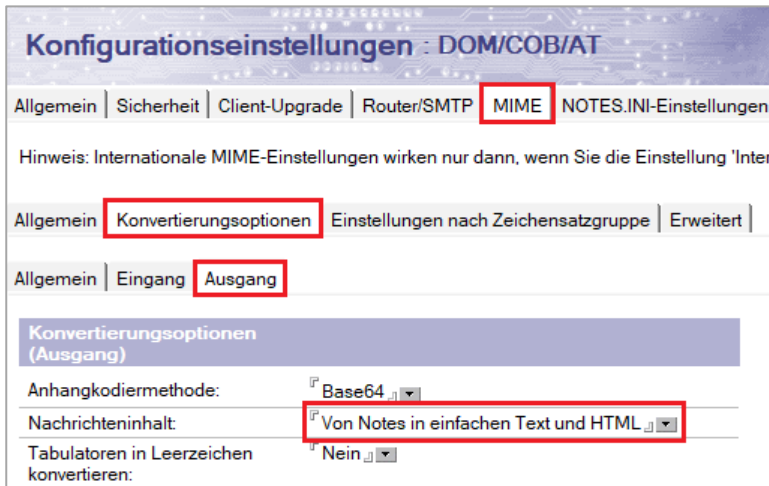


Abbildung 18.33: Konfigurationsdokument, Register MIME > Konvertierungsoptionen > Ausgang

Abwesenheitstyp

Setzen Sie im Register **Router/SMTP > Erweitert > Steuerung** das Feld **Abwesenheitstyp** auf »Service«, damit das Versenden von Abwesenheitsmeldungen automatisch beendet wird, wenn die Frist abläuft.

18.5.5.3. Anpassungen in der Mailrichtlinie

Nehmen Sie für HTMO folgende Anpassungen in der Mailrichtlinie vor.

Sorgen Sie dafür, dass im Register **Kalender und Aufgaben** die Felder wie folgt eingestellt sind:

1. Wählen Sie das Register **Anzeige** und ändern Sie die folgenden Einstellungen:

Neue (nicht verarbeitete Benachrichtigungen) anzeigen: »Ja«.

Abgesagte Benachrichtigungen automatisch verarbeiten: »Ja«. Wählen Sie die Zusatzfunktion: »Im Kalender als 'Abgesagt' anzeigen«.



Abbildung 18.34: Anpassungen für HTMO in der Mailrichtlinie, Register Kalender und Aufgaben > Anzeige

Wählen Sie für alle Parameter in der Spalte **Wie diese Einstellung angewendet wird** die Option »Wert festlegen und Änderungen verhindern«.

2. Wechseln Sie nun zum Register **Benachrichtigungen** und ändern Sie die folgenden Einstellungen:

Folgende Besprechungsbenachrichtigungen im Maileingang des Benutzers anzeigen: »Alle«.

Besprechungsbenachrichtigungen aus dem Maileingang des Benutzers entfernen, nachdem der Benutzer sie verarbeitet hat: »Ja«.

Besprechungsänderungen automatisch verarbeiten und Änderungen in Besprechungen übernehmen: »Ja«.

Verarbeitung von Besprechungsänderungen mit anstehenden neuen Planungen auslassen: »Ja«.

Mich standardmäßig über Besprechungsänderungen informieren, wenn ich Besprechungen ablehne: Nicht ausgewählt.

Wählen Sie auch hier für alle Parameter in der Spalte **Wie diese Einstellung angewendet wird** die Option »Wert festlegen und Änderungen verhindern«.

Kalendereinträge in Mailansichten anzeigen	Wie diese Einstellung angewendet wird:	Übernehmen von übergeordneter Richtlinie:	Zwingend in untergeordneten Richtlinien:
Folgende Besprechungsbenachrichtigungen im Maileingang des Benutzers anzeigen:	Alle	Wert festlegen und Änderungen v	<input type="checkbox"/> Übernehmen <input type="checkbox"/> Zwingend
Besprechungsbenachrichtigungen aus dem Maileingang des Benutzers entfernen, nachdem der Benutzer sie verarbeitet hat:	<input checked="" type="checkbox"/> Ja	Wert festlegen und Änderungen v	<input type="checkbox"/> Übernehmen <input type="checkbox"/> Zwingend
Nicht verarbeitete Besprechungsbenachrichtigungen in der Miniansicht 'Neue Benachrichtigungen' anzeigen:	<input type="checkbox"/> Ja	Wert nicht festlegen	<input type="checkbox"/> Übernehmen <input type="checkbox"/> Zwingend
Kalenderdokumente nicht in der Mailansicht 'Alle Dokumente' anzeigen:	<input type="checkbox"/> Ja	Wert nicht festlegen	<input type="checkbox"/> Übernehmen <input type="checkbox"/> Zwingend
Besprechungseinladungen nicht in der Mailansicht 'Gesendet' anzeigen:	<input type="checkbox"/> Ja	Wert nicht festlegen	<input type="checkbox"/> Übernehmen <input type="checkbox"/> Zwingend
Optionen für Aktualisierungsbenachrichtigungen			
Wie diese Einstellung angewendet wird:	Übernehmen von übergeordneter Richtlinie:	Zwingend in untergeordneten Richtlinien:	
Wenn ich zur Besprechung eingeladene Personen hinzufüge oder entferne, andere Teilnehmer informieren:	<input type="checkbox"/> Ja	Wert nicht festlegen	<input type="checkbox"/> Übernehmen <input type="checkbox"/> Zwingend
Besprechungsänderungen automatisch verarbeiten und Änderungen in Besprechungen übernehmen	<input checked="" type="checkbox"/> Ja	Wert festlegen und Änderungen v	<input type="checkbox"/> Übernehmen <input type="checkbox"/> Zwingend
Verarbeitung von Besprechungsänderungen mit anstehenden neuen Planungen auslassen	Ja	Wert festlegen und Änderungen v	<input type="checkbox"/> Übernehmen <input type="checkbox"/> Zwingend
Mich standardmäßig über Besprechungsänderungen informieren, wenn ich Besprechungen delegiere:	<input type="checkbox"/> Ja	Wert nicht festlegen	<input type="checkbox"/> Übernehmen <input type="checkbox"/> Zwingend
Mich standardmäßig über Besprechungsänderungen informieren, wenn ich Besprechungen ablehne:	<input type="checkbox"/> Ja	Wert festlegen und Änderungen v	<input type="checkbox"/> Übernehmen <input type="checkbox"/> Zwingend

Abbildung 18.35: Anpassungen für HTMO in der Mailrichtlinie

18.5.5.4. Anpassungen in der Sicherheitsrichtlinie

Für HTMO ist die Verwendung eines ID-Vaults Voraussetzung. Wenn Sie noch keinen eingerichtet haben, richten Sie ihn jetzt ein. Weiterführende Informationen zum Einrichten eines ID-Vaults finden Sie in Kap. 6.2.1 Einen ID-Vault einrichten, ab Seite 138.

Setzen Sie in der Sicherheitsrichtlinie, Register ID-Vault, die Einstellung **Notes-basierte Programme dürfen die Notes-ID-Vault verwenden** auf »Ja«:

18.5.5.5. Internetadressen für Räume angeben

Sorgen Sie dafür, dass alle Räume und Ressourcen über eine Internetadresse verfügen.

18.5.5.6. Das Abschneiden von Nachrichten steuern

Per Vorgabe werden Nachrichten, die älter als 30 Tage sind, beim Synchronisieren abgeschnitten und zeigen nur noch eine Zusammenfassung. Sie können das Zeitlimit von 30 Tagen anpassen oder dieses Verhalten auch ganz deaktivieren und immer ganze Nachrichten synchronisieren.

Um das Zeitlimit zu ändern, setzen Sie die folgende Variable in der notes.ini:

```
NTS_SUMMARY_SYNC_LIMIT_OVERRIDE=<Tage>
```

Um das Abschneiden von Nachrichten ganz zu deaktivieren, setzen Sie die folgende Variable in der Datei notes.ini:

```
NTS_SUMMARY_SYNC_ENABLED=false
```

18.5.6. Installation des HTMO-Outlook-Add-Ins

Laden Sie das Paket »HCL Traveler for MS Outlook (HTMO)« von HCL FlexNet herunter. Dieses steht als EXE-Datei (HTMO_301.exe) und als gezippte MSI-Datei zur Verfügung.

Haben Sie die Benutzerkontensteuerung aktiviert, deaktivieren Sie diese oder führen Sie die Installation als Administrator aus, indem Sie mit der rechten Maustaste auf die ausführbare Datei klicken und im Kontextmenü **Als Administrator ausführen** wählen.

Die Software installiert vor dem eigentlichen Installationsvorgang bei Bedarf folgende Komponenten:

- Microsoft .NET framework 4.5.2
- Microsoft Visual Studio Tools for Office (VSTO)

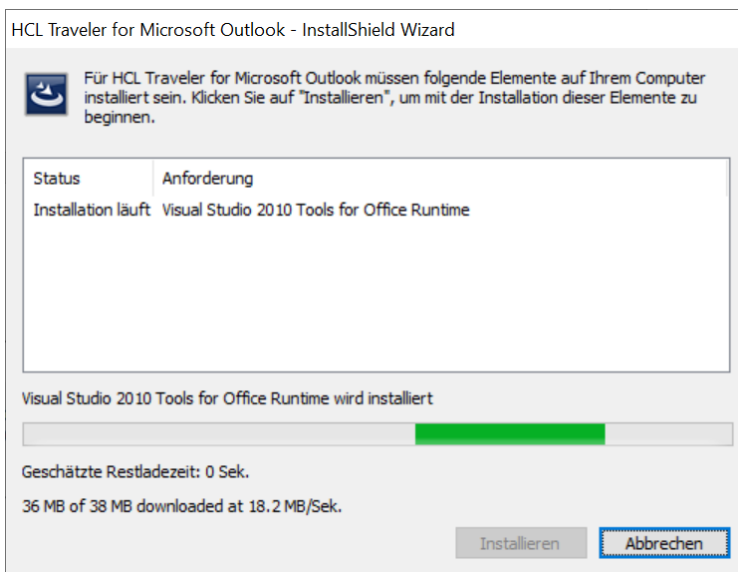


Abbildung 18.36: Installation HTMO – Installation erforderlicher Komponenten



Abbildung 18.37: Installation HTMO – Willkommensdialog

Klicken Sie auf **Weiter >**.

Akzeptieren Sie die Bedingungen der Lizenzvereinbarung und starten Sie die Installation:

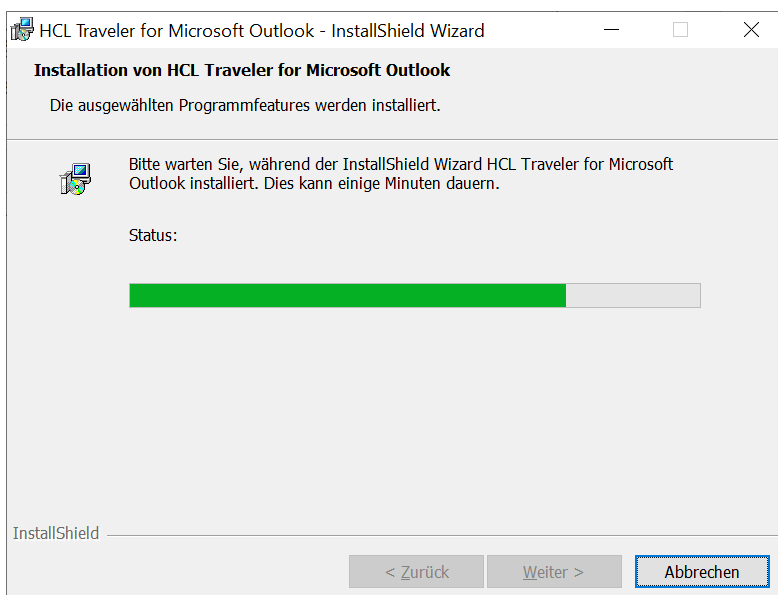


Abbildung 18.38: Installationsverlauf

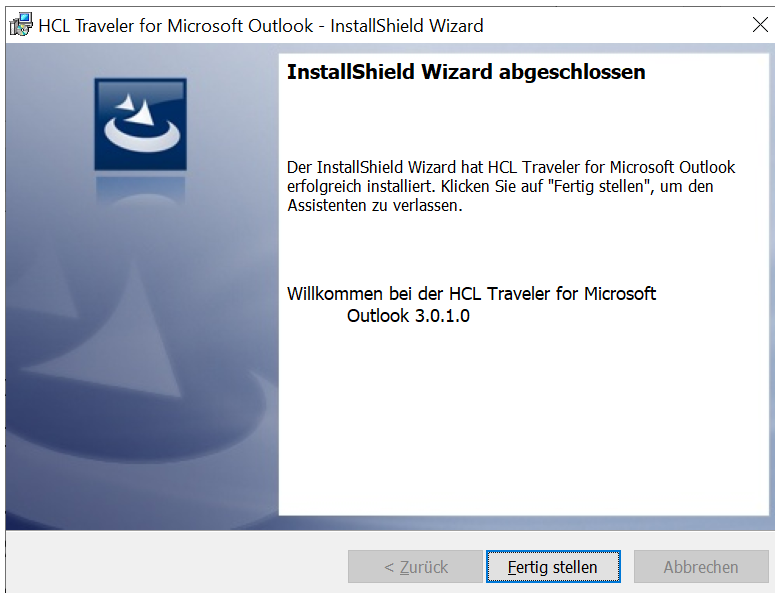


Abbildung 18.39: Installation HTMO – Installation abgeschlossen

18.5.7. Outlook mit dem Traveler verbinden

Richten Sie in Outlook ein neues Konto ein.

Aktivieren Sie **Ich möchte mein Konto manuell einrichten** und klicken Sie auf **Verbinden**:

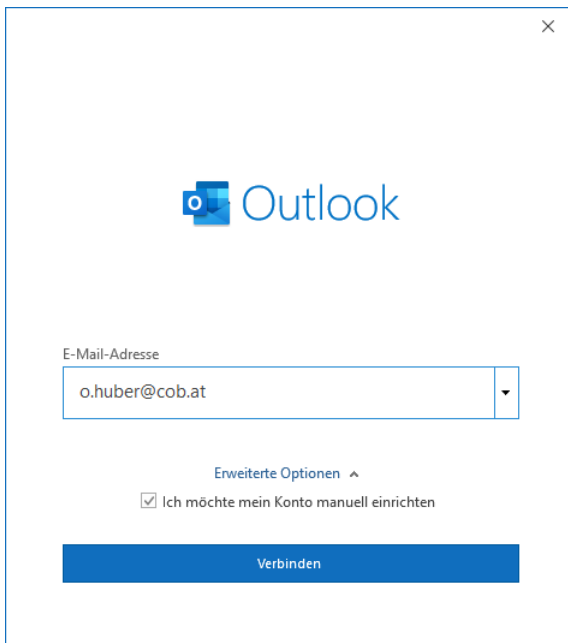


Abbildung 18.40: Outlook-Konto einrichten

Wählen Sie **Sonstiges**:

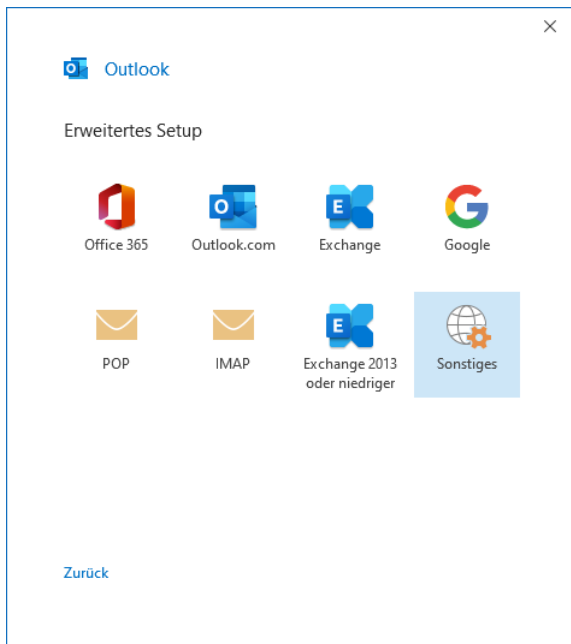


Abbildung 18.41: Outlook-Konto einrichten – Erweitertes Setup

Wählen Sie **HCL Traveler für Microsoft Outlook** und klicken Sie auf **Verbinden**:

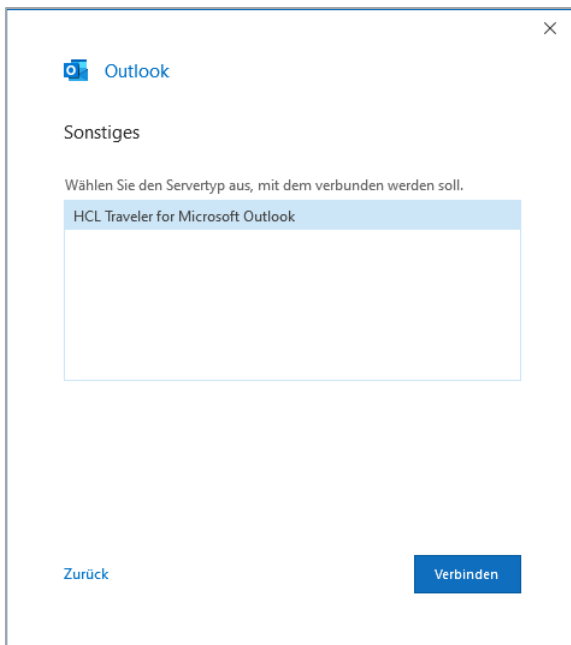


Abbildung 18.42: Outlook-Konto einrichten – Sonstiges

Geben Sie Namen, E-Mail-Adresse und Server an und klicken Sie auf **Weiter** >:

HCL Traveler for Microsoft Outlook - konfiguration

Erweitert

Ihr Name:
Beispiel: John Smith

E-Mail-Adresse:
Beispiel: John.Smith@hcl.com

Mail-Server meines Unternehmens

Servername:

Abbildung 18.43: Outlook-Konto einrichten – Erweitert

Geben Sie Ihr Internetkennwort ein und klicken Sie auf **Anmelden**:

Kennwort

HCL

Benutzername:
o.huber@cob.at

Kennwort:

Kennwort speichern

Abbildung 18.44: Outlook-Konto einrichten – Kennwort eingeben

Der HTMO-Client zeigt im nächsten Schritt den Status an (siehe Abbildung 18.45). Konnte er sich erfolgreich mit dem Traveler-Server verbinden, erhalten Sie in allen Bereichen grüne Häkchen.

Sehen Sie in einem oder mehreren Bereichen ein rotes X, überprüfen Sie alle Einstellungen nochmals.

Klicken Sie auf **Fertigstellen**.

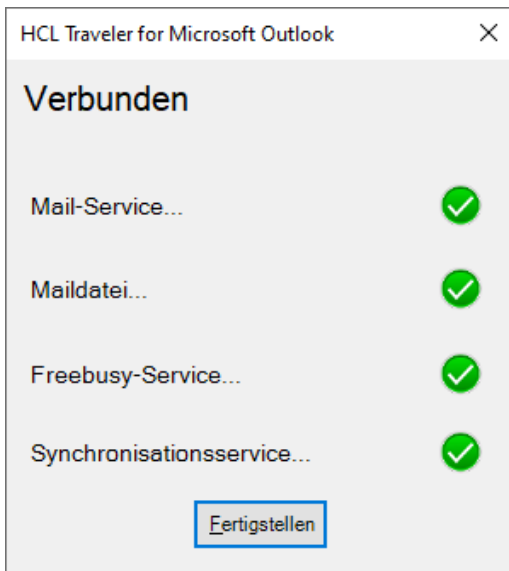


Abbildung 18.45: Outlook-Konto einrichten – Verbunden

18.5.8. HTMO-Benutzer überwachen

Um zu sehen, welche Benutzer mit Microsoft Outlook via HTMO-Schnittstelle auf den Domino-Server zugreifen, sind einige Schritte erforderlich:

1. Setzen Sie in der Datei notes.ini des Domino-Administrators die Variable OutlookEnv=1.
2. Starten Sie den Domino-Administrator und verbinden Sie sich mit dem Traveler-Server, der für HTMO konfiguriert wurde.
3. Navigieren Sie zum Register **Server > Status** und wählen Sie die Ansicht **Microsoft Outlook-Benutzer**:

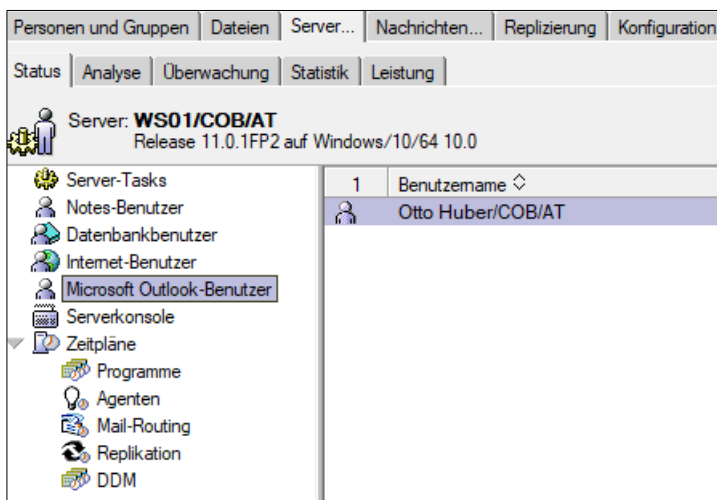


Abbildung 18.46: Die Ansicht Server... > Status > Microsoft Outlook-Benutzer

19. Anhänge

Anhang A: Serverkonsolenbefehle (Auswahl)

Befehl	Erklärung
<code>dbcache show</code>	Zeigt an, welche Datenbanken aktuell im Cache liegen.
<code>dbcache flush</code>	Schreibt die Datenbanken aus dem Cache auf die Festplatte zurück.
<code>broadcast "(!) Nachricht" "Benutzername"</code>	Sendet eine kurze Meldung an alle bzw. angegebene aktive Benutzer. Die Meldung wird im Notes-Client als Dialog im Vordergrund angezeigt, z. B.: br "(!)Der Server wird in 5 Minuten heruntergefahren" br "(!)Sicherung eingespielt" "Franz Huber/COB/AT" Achtung: Es müssen hierarchische Namen eingegeben werden!
<code>drop "Benutzer1" "Benutzer2" oder drop all</code>	Bricht alle Benutzersitzungen oder nur die angegebene ab.
<code>exit</code>	Führt ein Server-Shutdown durch. Wenn die Serverkonsole mit einem Passwort gesperrt ist, muss <code>exit [Passwort]</code> eingegeben werden.
<code>help</code>	Zeigt alle Befehle mit einer kurzen Erklärung an.
<code>load <Task></code>	Lädt das angegebene Programm., z. B.: <code>load router</code>
<code>pull <Server> push <Server></code>	Schickt an den angegebenen Server eine Anforderung für eine Ein-Weg-Replizierung.
<code>replicate <Server> [<Datenbank>]</code>	Schickt an den angegebenen Server eine Anforderung für eine Zwei-Weg-Replizierung. Wird keine Datenbank angegeben, werden alle gemeinsamen Repliken repliziert.
<code>restart server</code>	Fährt den Server herunter, wartet zehn Sekunden und startet ihn wieder.
<code>restart task <Task></code>	Startet den angegebenen Task neu.
<code>route Servername</code>	Leitet übertragungsbereite Mails an den angegebenen Server weiter
<code>set configuration <Variable>=<Wert></code>	Schreibt Einstellungen in die notes.ini, z. B.: <code>se con ServerTasksAt2=Updall</code>
<code>set secure <Passwort></code>	Sperrt die Serverkonsole. Mit <code>set secure [Aktuelles Passwort]</code> heben Sie die Sperre wieder auf.
<code>set systemtime</code>	Synchronisiert die Zeit mit dem Betriebssystem.
<code>show cluster</code>	Zeigt Informationen über den Cluster an.
<code>show directory</code>	Zeigt die Struktur des Domino-Datenverzeichnisses an.

Befehl	Erklärung
<code>show diskpace</code> laufwerk	Zeigt den freien Speicher des angegebenen Laufwerks (z. B. C:) an.
<code>show memory</code>	Zeigt den verfügbaren Arbeitsspeicher zusammen mit dem virtuellen Speicher (aus der Auslagerungsdatei) an
<code>show port</code> <Anschlussname>	Zeigt den Datenverkehr und Fehlerstatistiken des angegebenen Anschlusses (z. B. LAN0) an. Das Ergebnis ist abhängig vom verwendeten LAN-Protokoll.
<code>show schedule</code>	Zeigt auf dem Server terminierte Tasks an (Replikation, Mailweiterleitung, Programmausführung etc.).
<code>show server</code>	Zeigt Informationen über den Server an.
<code>show statistics</code>	Zeigt vom Server protokollierte Statistiken an.
<code>show tasks [only]</code>	Zeigt Serverinformationen und den Status der aktiven Servertasks (gleichzeitig laufender Programme) an. Ohne dem Parameter <code>only</code> sieht man auch Benutzersitzungen.
<code>show users</code>	Zeigt alle offenen Benutzersitzungen sowie von Benutzern geöffnete Datenbanken an.
<code>show xdir</code>	Zeigt Informationen über alle via Verzeichnishilfe (Directory Assistance) eingebundene externen Verzeichnisse an.
<code>tell <task></code> <Parameter>	Kommuniziert mit Servertasks wie Router, Replikator oder Indexer, etwa um einen Prozess zu beenden, ohne den Server herunterfahren zu müssen; z. B.: <code>tell router quit ...</code> beendet den Mail-Router. <code>tell router c ...</code> komprimiert die Datei mail.box. <code>tell router -?</code> ... zeigt eine Hilfe an
<code>trace <Server></code>	Zeigt den Verbindungsaufbau zum angegebenen Server an (nur für das Protokoll NRPC).
<code>quit</code>	Führt ein Server-Shutdown durch. Wenn die Serverkonsole mit einem Passwort gesperrt ist, muss <code>quit [Passwort]</code> eingegeben werden.

Tabelle 19.1: Übersicht über die wichtigsten Serverkonsolenbefehle

Anhang B: Domino-Serverprogramme (Auswahl)

Befehlszeile	Bezeichnung	Beschreibung	NOTES.INI
AdminP	Administrationsprozess	Automatisiert eine Vielzahl von administrativen Aufgaben.	ServerTasks
AMgr	Agent-Manager	Führt zeitplangesteuerte Agenten am Server aus.	ServerTasks
Ca	CA-Prozess	Bietet eine Domino-basierende Zertifikatsstelle.	ServerTasks
CalConn	Kalender-Connector	Bearbeitet Anforderungen für Informationen über freie Zeit von einem anderen Server.	ServerTasks
Catalog	Cataloger	Aktualisiert den Datenbankkatalog.	ServerTasksAt#
Chronos	Chronos	Aktualisiert Volltextindizes, die für ein stündliches Update konfiguriert wurden.	-
Collect	Statistik-Collector	Sammelt Serverstatistiken in einer Datenbank	ServerTasks
Compact	Datenbank-Kompriermierprogramm	Komprimiert Datenbanken und setzt erweiterte Einstellungen.	ServerTasksAt#
Convert	Mail-Konvertierungs-Tool	Wechselt die Gestaltung von Datenbanken.	-
DAOSMgr	DAOS-Manager	Wartet den DAOS-Katalog.	ServerTasks
dbmt	Database Management Tool	Wartet Mail- und andere Datenbanken.	ServerTasks ServerTasksAt#
Design	Designer	Aktualisiert die Gestaltung von Datenbanken, die auf Schablonen beruhen.	ServerTasksAt#
Dircat	Directory Cataloger	Erstellt und aktualisiert Verzeichniskataloge	ServerTasks
Event	Event-Monitor	Überwacht Serverereignisse.	-
Fixup	Datenbank-Fixup	Sucht und repariert beschädigte Datenbanken.	ServerTasksAt#
HTTP	Webserver	Webserver	ServerTasks
IMAP	IMAP-Dienst	Bietet Maildienste für IMAP-Clients.	ServerTasks
LDAP	Verzeichnisdienst	Bietet Verzeichnisdienste für LDAP-Clients.	ServerTasks
POP3	POP3-Dienst	Bietet Maildienste für POP3-Clients.	ServerTasks
Replica	Replikator	Repliziert Datenbanken mit anderen Servern.	ServerTasks
RnRMgr	Rooms und Resources-Manager	Reserviert Räume und Ressourcen.	ServerTasks
Router	Mail-Router	Leitet Mail an andere Server weiter.	ServerTasks
Sched	Planungs-Manager	Verwaltet Besprechungszeiten und -daten sowie verfügbare Teilnehmer.	ServerTasks
Statlog	Statistik-Logger	Speichert Datenbankaktivitäten im Serverprotokoll.	ServerTasksAt#
Stats	Stats	Erzeugt Statistiken für entfernte Server.	ServerTasks
UpdAll	Indexer	Aktualisiert Ansichts- und Volltextindizes. Ist im Gegensatz zu Update parametrierbar und	ServerTasksAt#

Befehlszeile	Bezeichnung	Beschreibung	NOTES.INI
		kann aufgerufen werden, um bestimmte Aufgaben zu erledigen.	
Update	Indexer	Aktualisiert Ansichts- und Volltextindizes.	ServerTasks

Tabelle 19.2: Übersicht über die wichtigsten Domino-Serverprogramme

Ersetzen Sie die # in ServerTasksAt# durch die gewünschte Stunde zwischen 0 und 23 Uhr.

Anhang C: Parameter für Konfigurationsdateien

Einstellung	Beschreibung
Username	Der eindeutige Name des Benutzers (Verwendung der Umgebungsvariable %USERNAME% möglich)
KeyFileName	Pfad zur ID-Datei des Benutzers, z. B. N:\notes\ids\fnameier.id
Domino.Name	Domino-Server, an dem die Anmeldung erfolgen soll. (Muss nicht der Mailserver des Benutzers sein.)
Domino.Address	Adresse des Anmeldeservers, entweder die IP-Adresse oder der Hostname
Domino.Port	Anschlussname, normalerweise TCPIP
Domino.Server	1 – für die Verbindung zu einem Domino-Server 0 – für keine Verbindung
AdditionalServices	1 – erzwingt die Anzeige des Dialogfelds »Zusätzliche Services«, selbst wenn ausreichende Informationen für diese Services verfügbar sind. -1 – unterdrückt die Anzeige des Dialogfelds »Zusätzliche Services«
AdditionalServices.NetworkDial	1 – Um eine Netzwerkwahlverbindung zu Internet-Konten zu konfigurieren, die über das Dialogfeld »Zusätzliche Services« erstellt wurden
Mail.Incoming.Name	Name des Kontos für eingehende Mails
Mail.Incoming.Server	Name des Servers für eingehende Mails (POP oder IMAP)
Mail.Incoming.Protocol	1 – POP3 2 – IMAP
Mail.Incoming.Username	Benutzer- oder Anmeldename des Mailkontos
Mail.Incoming.Password	Kennwort des Mailkontos
Mail.Incoming.SSL	Mit 0 deaktivieren, mit 1 aktivieren Sie das SSL-Protokoll für eingehende Internet-Mails
Mail.Outgoing.Name	Name des Kontos für ausgehende Mails
Mail.Outgoing.Server	Name des Servers für ausgehende Mails (SMTP)
Mail.Outgoing.Address	Die Internet-Mailadresse des Benutzers, z. B. franz.meier@cob.at
Mail.InternetDomain	Name der Internet-Maildomäne, z. B. cob.at
Directory.Name	Ein ausführlicher Name für das Verzeichniskonto
Directory.Server	Name des Verzeichnisservers (LDAP)
News.Name	Name des Nachrichtenkontos
Proxy.HTTP	HTTP-Proxy-Server und -Port, z. B. proxy.isp.com:8080
Proxy.FTP	FTP-Proxy-Server und -Port, z. B. proxy.isp.com:8080
Proxy.SSL	SSL-Proxy-Server und -Port, z. B. proxy.isp.com:8080
Proxy.HTTPTunnel	HTTP-Tunnel-Proxy-Server und -Port, z. B. proxy.isp.com:8080
Proxy.SOCKS	Socks-Proxy-Server und -Port, z. B. proxy.isp.com:8080
Proxy.None	Kein Proxy für folgende Hosts und Domänen

Einstellung	Beschreibung
Proxy.UseHTTP	Verwendet HTTP-Proxy für den FTP-, Gopher- und SSL Security-Proxy
Proxy.Username	Benutzername, wenn Anmeldung erforderlich ist
Proxy.Password	Benutzerkennwort
Replication.Threshold	Ausgehende Mail übertragen, wenn sich folgende Anzahl von Nachrichten in der lokalen Mailbox befindet
Replication.Schedule	Aktiviert den Replizierungszeitplan
IM.Server	Name des Instant-Messaging-Servers. Nicht möglich, wenn die notes.ini die Angabe IM_NO_SETUP=1 enthält. Ist diese Variable auf 1 gesetzt, wird der Dialog zur Instant-Messaging-Konfiguration während der Konfiguration nicht angezeigt und alle IM-Variablen in der Konfigurationsdatei werden ignoriert. Wenn der Benutzer Instant Messaging konfigurieren möchte, kann er diese Variable in der notes.ini weglassen oder sie auf 0 festlegen (IM_NO_SETUP=0).
IM.Port	Port des Instant-Messaging-Servers (beliebige positive Zahl)
IM.ConnectWhen	Legt fest, wann die Verbindung zu Instant Messaging hergestellt werden soll: 0 – Bei der Notes-Anmeldung (Vorgabe) 2 – Manuell
IM.Protocol	Wählen Sie eine der folgenden Einstellungen: 0 – Direkt zum Instant-Messaging-Server 1 – Direkt zum Instant-Messaging-Server mittels HTTP-Protokoll 2 – Direkt zum Instant-Messaging-Server mittels HTTP-Einstellungen in IE 3 – Einen Proxy verwenden
IM.ProxyType	Erforderlich, wenn IM.Protocol auf 3 gesetzt ist. Wählen Sie eine der folgenden Einstellungen: 0 – SOCKS4-Proxy 1 – SOCKS5-Proxy 2 – HTTPS-Proxy 3 – HTTP-Proxy
IM.ProxyServer	Der Name des Instant-Messaging-Proxy-Servers. Nur erforderlich, wenn IM.Protocol=3 festgelegt ist.
IM.ProxyPort	Der Port des Instant-Messaging-Proxy-Servers (beliebige positive Zahl). Nur erforderlich, wenn IM.Protocol=3 festgelegt ist.
IM.ServerNameResolve	Wird nur verwendet, wenn IM.ProxyType=1 gesetzt ist (SOCKS5), ist aber nicht erforderlich. Verwenden Sie einen der folgenden Werte: 0 – IM.ServerNameResolve deaktivieren 1 – IM.ServerNameResolve aktivieren
IM.ProxyUsername	Der Name des IM-Users. Nur erforderlich, wenn IM.Protocol auf 3 gesetzt und IM.ProxyType nicht SOCKS4 ist

Tabelle 19.3: Übersicht über die wichtigsten Parameter für Konfigurationsdateien

20. Index

\$ExpandGroups.....	203	Anhangskomprimierung.....	277
@GetMachineInfo	130	Anhangskonsolidierung.....	277
Abwesenheitsnachrichten einrichten	236	Anonyme Benutzer.....	376
Access Control List.....	358	Ansichten mit hoher Nutzung.....	264
ACL	358	AntiVirus-Software	84
Active Content	362	Anwendungsschablonen.....	305
Active Directory.....	184	Apache Tika	268
AD	184	Application Level Firewall.....	30
admin4.nsf.....	113	Asymmetrische Verschlüsselung.....	320
Administration Process	112	Attachment Consolidation.....	277
Administration Requests	113	Ausführungskontrollliste	
Administrationsanforderungen.....	113	Administrations-ECL bearbeiten.....	364
Administrations-ECL.....	364	Sicherheitswarnung	363
Administrationsprozess.....	112	Übersicht.....	362
Administrationsserver setzen	118	Ausführungskontrollliste (ECL).....	362
Aufbewahrungsdauer steuern.....	117	Authentifizierung	336
Löschen von Namen verhindern	118	Details	336
Namenssuche beschleunigen	118	Überblick	25
Planungstyp	114	Author Fields.....	367
Schedule Type	114	Automatisch befüllte Gruppen	177
Vorgaben anpassen	116	Autopop.....	177
Administrationsserver	29	Auto-populated Groups	177
Administrator mit voller Berechtigung	110	Autorenfelder	367
Administratoren	109	Autorisierung	25
Adressierung		Benannte Notes-Netzwerke.....	30, 204
Gruppen auflösen.....	203	Benutzer anlegen.....	152
AES.....	320	Benutzer löschen.....	173
Agent Manager	95, 312	Benutzer sperren.....	172
Konsolenbefehle	314	Benutzer umbenennen	166
Aktualisieren auf Version 11.x	81	Benutzer verlängern	163

Benutzerdefinierte Kennwortrichtlinie	347	Custom Password Policy	347
Benutzerverwaltung.....	152	DAOS	277
Notes-Benutzer anlegen	152	deaktivieren	281
Notes-Benutzer aussperren.....	172	Einrichten	278
Notes-Benutzer löschen.....	173	Speicher verschieben.....	282
Notes-Benutzer sperren	341	Tier-2-Speicher.....	282
Notes-Benutzer umbenennen	166	Überblick.....	277
Notes-ID verlängern.....	163	daoscat.nsf	280
Notes-ID-Kennwörter zurücksetzen	160	DAOS-Katalog	280
CA, Certificate Authority	387	DAOS-Manager (DAOSMgr).....	280
cache.ndk.....	472	DAS (Direct Attached Storage)	32
CA-Prozess (CA).....	149	Database Designer	309
catalog.nsf	290	Database Instance ID	104
cert.id.....	25	Database Maintenance Tool.....	256
Certificate Authority, CA	387	Dateiformat.....	246
Certificate Signing Request	395	Dateiserver-Roaming.....	157
Certification Log	115	Datenbanken	24, 243
certlog.nsf.....	115, 166	Access Control List	358
Chiffprat	320	ACL.....	358
Chronos	270	Aktivitäten aufzeichnen.....	287
Cluster	24, 435	Anhangskomprimierung	277
Active-Active-Cluster	436	Dateiformat.....	246
Active-Passive-Cluster	436	DBIID.....	104
Details	435	Details	243
Einrichten	437	Dokumentdatenkomprimierung	276
Failover	435	Dokumentlöschungen protokollieren.....	289
Load Balancing	435	Eigenschaft LargeSummary setzen.....	256
Streaming-Cluster-Replikation (SCR).....	436	Gestaltung aktualisieren	308
Symmetrischer Cluster	445	Gestaltungskomprimierung	274
Übersicht	24	Instanz-ID.....	104
Community Server	61	Kopie erstellen.....	294
Computerspezifische Formeln.....	129	Links erstellen	286
Condensed Directory Catalog.....	238	ODS.....	246
Configuration Directory	79	organisieren	244
Consistent Access Control List.....	361	Replik erstellen.....	294
Content Language.....	45	Replik-ID.....	293
Credential Store.....	410, 415	Schablone wechseln.....	310
Cross Certificate	337	Schablonen	24, 305
CSR	395	Übersicht	24

Umbenennen.....	286	Als Applikation starten	56
Umleitung erstellen.....	283	Als Dienst (Service) starten	57
Verschieben	286	Installieren	34, 495
Zugriffskontrollliste	358	Merkmale im Detail	23
Datenbankinstanz-ID	104	Plattformen.....	23
Datenbank-Link	286	Übersicht.....	23
Datenbankschablonen	305	Domino-Server-Roaming	157
Datenbankumleitung erstellen.....	283	aktivieren	157, 158
DBIID	104	Übersicht.....	157
DBMT.....	256	Domino-Verzeichnis	28
DDM.....	462	Konfigurationsverzeichnis	29
ddm.nsf	462	Primärverzeichnis	29
Dead Mail Processing	232	Domino-Webadministrator.....	409
Dead Message	231	Domino-Web-Administrator	90
Deletion Stubs.....	296	domlog.nsf	383
Delivery	202	DPAPI (Data Protection API)	350
Derby-Datenbank.....	432	Durchgangsserver.....	74
Defragmentieren	433	Dynamische Gruppen.....	176
Design Compression	274	EAS	487
Dial-In-Server	74	ECL.....	362
Dienstmanager	57	Eclipse.....	467
Digitale Signatur	321	Effective Policy.....	126
Directory ACL	357	Eingabeaufforderung als Administrator ausführen	58
Directory Assistance	180	Einmalige Notes-Anmeldung	352
Directory Indexer.....	271	Einwählserver.....	74
Document Body Compression	276	Ereignisgeneratoren.....	461
Dokumentdatenkomprimierung	276	erstellen.....	462
Dokumentlöschungen protokollieren	289	Typen	461
Domäne.....	29	Übersicht.....	461
domcfg.nsf	380	Ereignishandler	458
Domino Attachment and Object Services	277	Benachrichtigungsmethoden	458
Domino Directory	28	einrichten	459
Domino Domain Monitoring.....	462	Event Generators.....	461
Domino Named Networks, DNN	204	Event Handler	458
Domino Namend Networks (DNN)	30	Notification Methods	458
Domino-Datenbanken	24	events4.nsf	89, 454, 458
Domino-Domäne.....	29	Exchange ActiveSync	487
Domino-Domänenüberwachung	462	Execution Control List	362
Domino-Server.....	23	Extended Directory Catalog	238

Index

Feiertage	199	Installation.....	64
erstellen	199	HCL Domino-Designer	468
Im Domino-Verzeichnis aktualisieren.....	199	HCL Nomad	473
In den Kalender importieren.....	199	HCL Notes	
verwalten.....	199	Basic-Client.....	467
Feldbeschränkungen.....	256	Client-Pakete	468
FIPS.....	320	Mehrbenutzerinstallation	469
Fix Pack, FP	40	Standard-Client.....	467
Forward Secrecy.....	390	HCL SafeLinx	401
Full Access Administrator.....	110	HCL Traveler for Microsoft Outlook	488
Gegenzertifikat	337	HCL Verse.....	413
Auf Anfrage erstellen.....	337	Hierarchische Namen	
Gegenzertifizieren	337	Allgemein	25
Geheim Schlüssel	319	Komponenten	26
Gemeinsame Notes-Anmeldung	350	High Usage Views	264
Geplante Nachrichten	227	Hot Fixes	40
Geschützte Gruppen	178	HSTS	393
Gestaltung.....	243	HTMO	488
Aktualisieren	308	HTTP Strict Transport Security.....	393
Wechseln.....	310	HTTPS.....	387
Gestaltungselemente.....	243	Hypertext Transfer Protocol Secure.....	387
Gestaltungskomprimierung	274	ICL	149
Global Edition	72	ID-Datei	25
Größenbeschränkungen	233, 234	ID-Dateien	26
Gruppen.....	175	Allgemein	26
Automatisch befüllte Gruppen	177	Eigenschaften	27
Delegieren	178	Gegenzertifizieren	339
Dynamische Gruppen.....	176	Sichere Kopie erstellen.....	339
Erstellen	176	Typen.....	26
Geschützte Gruppen	178	Verschlüsselung.....	329
Löschen	178	IMAP.....	474, 475
Statische Gruppen	175	Begrüßung (Greeting) anpassen	485
Typen	176	Benutzer anlegen	477
Umbenennen	178	Beschreibung.....	475
Verschachtelte Gruppen	175	Datenbank konvertieren.....	476
Werkzeug Gruppen verwalten.....	179	IMAP-Site-Dokument zu erstellen	476
Gruppentypen	176	Konfiguration von Outlook	478
HCL Docs.....	413	Öffentliche Ordner einbinden	482
HCL Domino-Administrator	468	Übersicht	474

Verwenden von Öffentlichen Ordner in Outlook.....	483
Zugriff auf Ordner konfigurieren.....	481
Indirect-Datei	249, 255
inetlockout.nsf.....	356
Inhaltssprache	45
Inline View Indexing	263
iNotes Redirect	412
iNotes Web Access	411
Installation	
Domino-Administrator.....	64
Domino-Server	34, 495
Fix Pack.....	40
Sprachen	41
Traveler.....	418
Interim Fixes.....	40
Intermediate Certificate.....	399
Interne Verschlüsselung.....	329
Internet Password Lockout.....	355
Internetkennwort.....	353
Hash-Versionen	354
Sperrn.....	355
Synchronisierung	357
Internetkennwortsperrung	355
Internet-Mail	
aktivieren	209
Aktivieren	209
RFC822-Standard	213
ISpy.....	462
Issued Certificate List	149
Kennwortqualität.....	343
Komprimieren	
Durch interne Reorganisation	253
Mithilfe einer Kopie	254
Mithilfe einer Replik.....	255
Konfigurationsverzeichnis	29
Konsistente Zugriffskontrollliste.....	300, 361
KYRTOOL	
Download.....	395
Einführung	395
Schlüsselring erstellen.....	398
Language Packs.....	41
LDAP	
Base DN.....	186
Konfiguration von LDAP am Konfiguration von Outlook	485
Suchbasis	186
LE4D (Let's Encrypt 4 Domino).....	402
Leserfelder	366
Lizenztyp International	72
Log Filter	453
log.nsf.....	451
Löschinfos.....	296
LZ1-Anhangskomprimierung.....	277
Mail.....	203
Beschränkungen setzen	225
Body.....	208
Envelope	208
Header.....	208
TNEF-Konvertierung.....	209
Mail Conversion Utility (Convert)	310
Mailboxen	
Anzahl festlegen.....	219
Transaktionsprotokollierung abschalten...219	
Mailer.....	203
Mailformate.....	201
Compound Document, CD.....	201
Mehreilige Nachricht	214
MIME	201
Multi-Part Message.....	214
Richtext.....	201
Mail-In-Datenbanken	202, 222
erstellen.....	222
Mail-Konvertierungs-Tool (Convert).....	310
Mail-Router.....	203
Mail-Routing	201
Absenderadresse konfigurieren.....	213
Abwesenheitsnachrichten.....	236
Adressierung	203
Anzahl Mailboxen.....	219

Benannte Notes-Netzwerke	204	Netzwerkkomprimierung	53
Dead Mail Processing	232	Netzwerkverschlüsselung	53, 321
Delivery	203	New Relic	457
Domino-Domäne	29	NIFNSF	265
Geplante Nachrichten	227	NLO-Datei	277
Internet-Mail aktivieren	209	Nomad	473
Komponenten	201	Non Delivery Report	230
Mailer	203	Notes Basic-Client	467
Notes Named Networks, NNN	204	Notes Index Facility	261
Notes-Mail	203	Notes Large Object	277
Relay-Host	220	Notes Named Networks (NNN)	30
Router	203	Notes Redirect File	285
Routing-Kosten	207	Notes Shared Login, NSL	350
Smart-Host	221	Notes Single Logon	352
SMTP-Server	210	Notes Standard-Client	467
Transfer	203	Notes Views	261
Übertragung	202, 203	notes.ini	
Unzustellbare Nachricht	231	Bearbeiten	91
Unzustellbare Nachrichten automatisch verarbeiten	232	Definition	91
Unzustellbare Nachrichten manuell verarbeiten	231	Eintrag via Konfigurationsdokument hinzufügen	92
Verbindungsdokumente	30	Eintrag via Konsolenbefehl hinzufügen	93
Zustellung	202, 203	Eintrag via Texteditor hinzufügen	91
Zustellungsfehlerbericht	230	Eintrag via Webadministrator hinzufügen ..	93
MarvelClient	473	Notes-Ansichten	261
Masterschablone	306	Notes-ID	25
Mehrbenutzerinstallation	469	Aus dem Vault löschen	174
Microsoft Active Directory	184	Im Vault als inaktiv markieren	174
Multi-Part Message	214	Kennwort zurücksetzen	
Multiprotokollserver	204	Über den Domino-Administrator	161
Multi-User Installation	469	Über eine Self-Service-Anwendung ..	162
NAB	28	sperren	341
Named Encryption Key, NEK	410	verlängern	163
names.nsf	29	Notes-Mail	203
NAS	32	NRPC	25
NDR	230	ODS	246
Nested Groups	175	Öffentlicher Schlüssel	320
Network Attached Storage	32	Öffentlicher Zugriff	367
Network Encryption	321	Öffentliches Adressbuch	28

On Demand Full text Indexing.....	266	Serverkonsolenbefehl absetzen	99
On Disk Structure, ODS.....	246	Protected Groups.....	178
OOO.....	236	Protokolle	
Open Authorization-Protokoll (OAuth)	410	NRPC.....	25
OpenSSL.....	394	Protokollfilter	453
Format konvertieren.....	396	Public Access	367
Privaten Serverschlüssel erstellen.....	395	Public Address Book.....	28
Übersicht.....	394	Public Key.....	320
Zertifikate überprüfen	397	pubnames.ntf.....	29
Zertifikatsanforderung erstellen.....	395	Purge Interval Replication Control (PIRC)	303
Ordnergestaltung aktualisieren.....	310	pwdresetsample.nsf	138
Organisationseinheiten.....	27	PwdResetSample.nsf	162
Organizational Unit (OU)	27	PwdResetSmple.nsf.....	143
OU	27	Querzulassung	28, 337
Out of Office.....	236	Quotas	233
OU-Zertifizierer erstellen.....	169	Rapid Application Development & Deployment (RADD).....	24
Password Quality	343	Reader Fields.....	366
Path-Through-Server.....	74	Realm	376
pernames.ntf.....	29	Registrierung	
Persönliches Adressbuch.....	28	Aus Textdatei.....	156
PIRC	303	Einzelnen Benutzer registrieren	152
Policies.....	123	OU-Zertifizierer erstellen.....	169
Überblick	123	Regressions	40
Policy Master	123	Relay-Host	220
Policy Setting	123	Relaying erlauben.....	478
POODLE-Attacke.....	388	Replica	294
POP3	474	Replica (Servertasks)	294
Benutzer anlegen	477	Replica ID	293
Beschreibung	474	Replication History	296
POP3-Site-Dokument zu erstellen	474	Replication Stub.....	298
Übersicht.....	474	Replik.....	294
Primäres Domino-Verzeichnis	29	Replikation.....	24, 293
Primary Domino Directory	79	Replikator (Replica).....	294
Privaten Serverschlüssel erstellen	395	Replik-ID	293
Privater Schlüssel.....	320	Replikrumpf	298
Programmdokument		Replizierung	24, 293
Batchdatei starten.....	99	Client-zu-Server-Replikation	296
Erstellen.....	97	Konflikte	295
Programm beim Hochfahren des Domino- Servers starten.....	98	Löschinfos.....	296

Purge Interval Replication Control (PIRC)	303	Schlüsselringdatei.....	394
Replik.....	294	SCT.....	275
Replik erstellen.....	297	Secret Encryption Key.....	319
Replik-ID.....	293	Secure Sockets Layer.....	388
Replikrumpf.....	298	Selektive Replikation.....	293
Replizierprotokoll.....	296	Server Availability Threshold (SAT).....	443
Replizierarten.....	295	Server Availability Index (SAI).....	443
Selektive Replikation.....	293	Server Language Packs.....	41
Server-zu-Server-Replikation.....	296	Server Name Indication	
Übersicht.....	293	Aktivierung.....	394
Verbindungsdocument erstellen.....	301	Übersicht.....	394
Reverse Proxy.....	401	Server_Availability_Threshold.....	443
RFC822-Standard.....	213	Server_MaxUsers.....	442
Richtlinien.....	123	Serverinstallation	
Computerspezifische Formeln verwenden	129	Anleitung.....	34, 495
Explizit.....	125	Hardwareausstattung.....	32
Organisationsbezogen.....	124	Unterstützte Betriebssysteme.....	31
Überblick.....	123	Serverkonsolen	
Richtliniendokument.....	123	Direkte Konsole.....	85
Richtlinieneinstellung.....	123	Domino-Console.....	88
RnRMgr.....	192	Entfernte Konsole im Domino-Administrator	86
Roaming.....	157	Konsolen im Domino-Web-Administrator	90
aktivieren.....	157, 158	Serverprogramme.....	94
Roaming-Benutzer.....	157	Auf Betriebssystemebene starten.....	96
Rooms & Resources Manager.....	192	Über die notes.ini starten.....	96
Root Certificate.....	399	Über die Serverkonsole starten.....	95
Router.....	203	Über Programmdokumente starten.....	97
RSA-Verschlüsselung.....	320	Servertasks.....	94
SAN (Storage Area Network).....	32	Administrationsprozess (AdminP).....	112
SAN (Subject Alternative Name).....	406	Agent Manager (AMgr).....	312, 313
Schablonen.....	24	Agentenmanager.....	312
Erstellen.....	306	Autopop.....	177
Signieren.....	307	AutoRepair.....	446
Systemschablonen.....	305	Calendar Connector (CalConn).....	189
Übersicht.....	305	CA-Prozess (CA).....	149
Wechseln.....	310	Catalog.....	290
Zentralschablone.....	275	Chronos.....	270
Schedule Type.....	114	Cluster Database Directory Manager (clbdbir)	441
Scheduled Messages.....	227		

Cluster-Replikator (clrepl).....	439	Smart-Host	221
DAOS-Manager (DAOSMgr).....	280	SMTP	208
Database Designer (Design)	309	aktivieren	209
Database Maintenance Tool (dbmt) ..	249, 256	Authentifizierung erlauben.....	477
Directory Cataloger (Dircat).....	238	TLS aktivieren	217
Ereignismonitor (Event)	458	SMTP-Server	202
Fixup.....	260	Starten	210
HTTP	373	SNI.....	394
Indexer (Update).....	271	Aktivierung	394
ISpy	462	Übersicht.....	394
Mail-Konvertierungs-Tool (Convert).....	310	SSL.....	388
Mail-Router (Router)	202, 203	Stammzertifikat	399
Query Vault (qvault).....	147	Statische Gruppen	175
Repair Cleanup (RprCleanup).....	448	Statistiken.....	453
Replikator (Replica).....	294	Bei externen Diensten veröffentlichen	457
Rooms and Resources Manager (RnRMgr)	189	Konfiguration.....	454
.....	189	Übersicht.....	453
Schedule Manager (Sched)	189	statrep.nsf.....	454, 457
SMTP-Listener	210	Streaming-Cluster-Replikation (SCR).....	436
Statistik Logging (Statlog).....	288	Subject Alternative Names (SAN)	406
Statistic Collector (Collect).....	454, 455	Symmetrische Verschlüsselung.....	319
UpdAll	272	Symmetrischer Cluster	445
Verzeichnis-Indexer (Update).....	271	Konfiguration	446
Verzeichniskatalogdienst (Dircat).....	238	Tuning.....	448
Serverzugriffskontrollliste	340	Übersicht.....	445
Service Manager	57	Systemdatenbanken	
SHA-2	320	admin4.nsf.....	113
Sicherheit		catalog.nsf	290
Ausführungskontrollliste	362	certlog.nsf	115
Autorenfelder.....	367	daoscat.nsf.....	280
Benutzerdefinierte Kennwortrichtlinie.....	347	ddm.nsf	462
ECL	362	domcfg.nsf	380
Gemeinsame Notes-Anmeldung	350	domlog.nsf	383
Konsistente Zugriffskontrollliste	361	events4.nsf	454, 458
Leserfelder.....	366	log.nsf	451
Öffentlicher Zugriff	367	names.nsf	28
Serverzugriffskontrollliste	340	statrep.nsf.....	454, 457
Symmetrische Verschlüsselung	319, 320	Telnet	215, 485
Verschlüsselungsverfahren	319	Templates	305
Single Copy Template.....	275		

Index

Thread-ID	91	Unternehmensschlüssel.....	25
TLS.....	321	Unzustellbare Nachricht	231
TLS, Transport Layer Security	388	Automatische Verarbeitung	232
TLS-Zertifikat erstellen	394	Manuelle Verarbeitung	231
Über anerkannte Zertifizierungsstelle	395	Upgrade auf Version 11.x	81
Über eigene Zertifizierungsstelle	403	Verbindungsdokumente	30
Über LE4D (Let's Encrypt 4 Domino).....	403	Verschachtelte Gruppen.....	175
TNEF-Konvertierung	209	Verschlüsselung.....	319
Transaction Logging.....	103	Asymmetrische Verschlüsselung	320
Transaktion.....	103	Chiffprat	320
Transaktionsprotokoll.....	103	Geheim Schlüssel	319
Transaktionsprotokollierung		Öffentlicher Schlüssel	320
Ansichtsprotokollierung	108	Privater Schlüssel	320
Archivierend.....	105	Symmetrische Verschlüsselung	319
Datenbanken ausschließen	107	Verfahren.....	319
Einrichten	106	Verschlüsselungsverfahren	319
Linear	105	Verse.....	413
Übersicht	103	Verteilte Verzeichnisarchitektur	29
Umlaufend.....	105	Verzeichnis-ACL.....	357
View Logging.....	108	Verzeichnishilfe	
Transfer	202	Erstellen.....	180
Transport Layer Security, TLS	388	Überblick.....	180
Traveler	417	Verzeichnis-Indexer.....	271
Benutzer hinzufügen	424	Verzeichniskatalog	238
Benutzer löschen	425	Verzeichniszugriffskontrollliste.....	357
Derby-Datenbank	432	View Logging	108
Derby-Datenbank defragmentieren	433	Volltextindex	266
Entferntes Löschen.....	428	Aktualisierungsintervalle.....	269
Entferntes Löschen durch Administrator..	429	Als separater Thread.....	270
Entferntes Löschen durch Anwender	429	Automatische aktualisieren.....	269
Entferntes Löschen zurücknehmen.....	430	Bestimmte Dateitypen indizieren	268
Geräte verwalten	425	Erstellen.....	267
Geräte zurücksetzen	428	Löschen	270
Installation.....	418	Manuell aktualisieren	269
Protokollierung.....	431	Überblick.....	266
Remote Wipe.....	428	Verschieben.....	270
Starten und beenden	423	webadmin.nsf.....	90
Übersicht	417	Webserver.....	371
Übertragung.....	202	Anmeldemaske bereitzustellen	381

Basic Authentication.....	376	Wirksame Richtlinie.....	126
Protokollierung aktivieren	383	X400-Namenskonventionen.....	25
Session Authentication	377	Zentrale Verzeichnisarchitektur	29
Sitzungsauthentifizierung	377	Zentralschablone	275
Standardauthentifizierung.....	376	Zertifikat	25
starten	373	Zertifikatsanforderung erstellen	395
URL-Umleitung	412	Zertifizierer	25
Websiteregeln erstellen.....	412	Zertifizierung	
Windows Management Instrumentation Service	41	CA-Prozess (CA)	149
Windows-Dienst	57	cert.id	25
Über die Befehlszeile starten und stoppen ..	58	Domino-Zulassungsstelle.....	149
Über Dienstmanager starten und stoppen ...	57	Gegenzertifikat erstellen	337
Windows-Firewall		Gegenzertifizieren.....	337
Verbindung zulassen.....	61	ID-Typen.....	26
Windows-Verwaltungsinstrumentation.....	41	Issued Certificate List	149
Windows-Wissen		Querzulassung.....	28, 337
Dienste über die Befehlszeile starten und ..	58	Unternehmensschlüssel.....	25
stoppen.....	58	Zertifikat	25
Dienstmanager starten.....	57	Zertifizierer	25
Editor als Administrator ausführen	91	Zertifizierungsprotokoll	115
Eingabeaufforderung als Administrator ..	58	Zertifizierungsstelle.....	387
ausführen	58	Zugriffskontrollliste	358
Telnet.....	215, 485	Zustellung	202
Windows-Firewall	61	Zustellungsfehlerbericht.....	230
winmail.dat	209	Zwischenzertifikat.....	399

21. Danksagungen

Ich danke der Firma HCL, die mir als Partner die Software gratis zum Testen zur Verfügung gestellt hat.

