

### Copyright

Alle Rechte vorbehalten.  
(c) Ingenieurbüro Manfred Dillmann  
www.madicon.de

Kein Teil dieser Dokumentation darf, in welcher Form auch immer (Druck, Fotokopie, Mikrofilm o.ä.), ohne schriftliche Genehmigung des Ingenieurbüros Manfred Dillmann reproduziert oder unter Verwendung elektronischer Systeme vervielfältigt oder verbreitet werden.

### Haftungsausschluss

Diese Schulungsunterlage wurde mit großer Sorgfalt erstellt und mehrfach geprüft. Trotzdem können Fehler nicht gänzlich ausgeschlossen werden.

Das Ingenieurbüro Manfred Dillmann übernimmt für fehlerhafte Angaben und deren mögliche Folgen keinerlei juristische Verantwortung noch irgendeine Haftung.

### Internet Links

Diese Schulungsunterlage kann Links oder Verweise auf fremde Internet Seiten enthalten. Auf die Inhalte und Gestaltung dieser Internetseiten hat das Ingenieurbüro Manfred Dillmann keinen Einfluss, hierfür sind alleine die Anbieter dieser Seiten verantwortlich.

### Ausgabe/Softwareversion

Schulungsunterlage  
Stand der Schulungsunterlage: Ausgabe 3 vom 23.11.2016  
Autor: Dipl.-Ing. Manfred Dillmann

IBM Notes/Domino Software

Für die Erstellung der Screenshots wurde Version 8.5 englisch eingesetzt. Das Programm-Logo auf dem Deckblatt stammt von IBM.

## 1.2. Kursraum Einrichtung

Die Installation der Kursraumumgebung wird zu Beginn des Seminars zusammen mit den Kursteilnehmern durchgeführt. So haben Administratoren, welche selbst eher selten eine Notes/Domino Umgebung installieren die Möglichkeit, jeden einzelnen Schritt noch einmal nachzuvollziehen.

### Installation mit mehreren Domänen

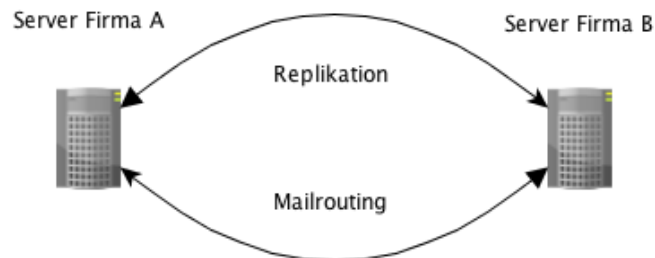


Sofern eine ausreichende Anzahl von PCs zur Verfügung steht und genügend Teilnehmer anwesend sind wäre das Wunschziel eine Notes/Domino Umgebung mit 3 Domänen/Organisationen zu installieren.

## 2. Arbeiten mit mehreren Domänen/Organisationen

### 2.1. Kommunikation zwischen fremden Domänen/Organisationen

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



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

Lediglich die Authentifizierung, also der "Handshake" bei der Verbindungsaufnahme der Domino Server, wird nicht "einfach so" funktionieren, denn die beteiligten Server-IDs stammen nun einmal aus unterschiedlichen Organisationen (sind also "Abkömmlinge" unterschiedlicher CERT.IDs).

#### **Wir erinnern uns**

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

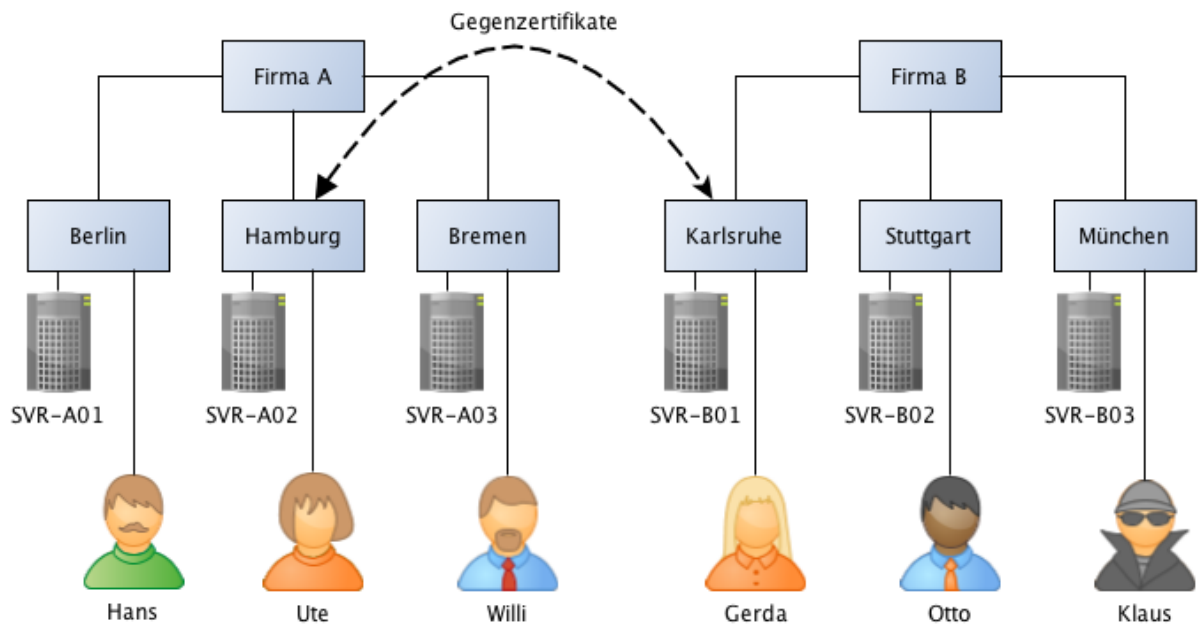
*Erfolgt nun ein Verbindungsversuch zwischen z.B. zwei Domino Servern, so überprüft jeder der beteiligten Domino Server, ob die Gegenseite auch über dieses Zertifikat verfügt. Sofern dies der Fall ist, wird die nachfolgende Kommunikation problemlos stattfinden. Ansonsten kommt es auf der Domino Serverkonsole (oder auch in der LOG.NSF) zu Fehlermeldungen.*

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

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

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

## Gegenzertifikate auf der Abteilungsebene (OU)



Hier erfolgt die Gegenzertifizierung auf der Ebene von Abteilungen.

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

Am Standort Hamburg wären nun nur noch für Ute und den Server SVR-A02 ein Zugriff auf den Domino Server SVR-B01 am Standort Karlsruhe möglich. Gerda und der Domino Server SVR-B01 am Standort Karlsruhe erhalten einen Zugriff auf den Domino Server SVR-A02 in Hamburg.

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

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

### Fazit

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

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

## 2.3. Einrichten der Gegenzertifizierung

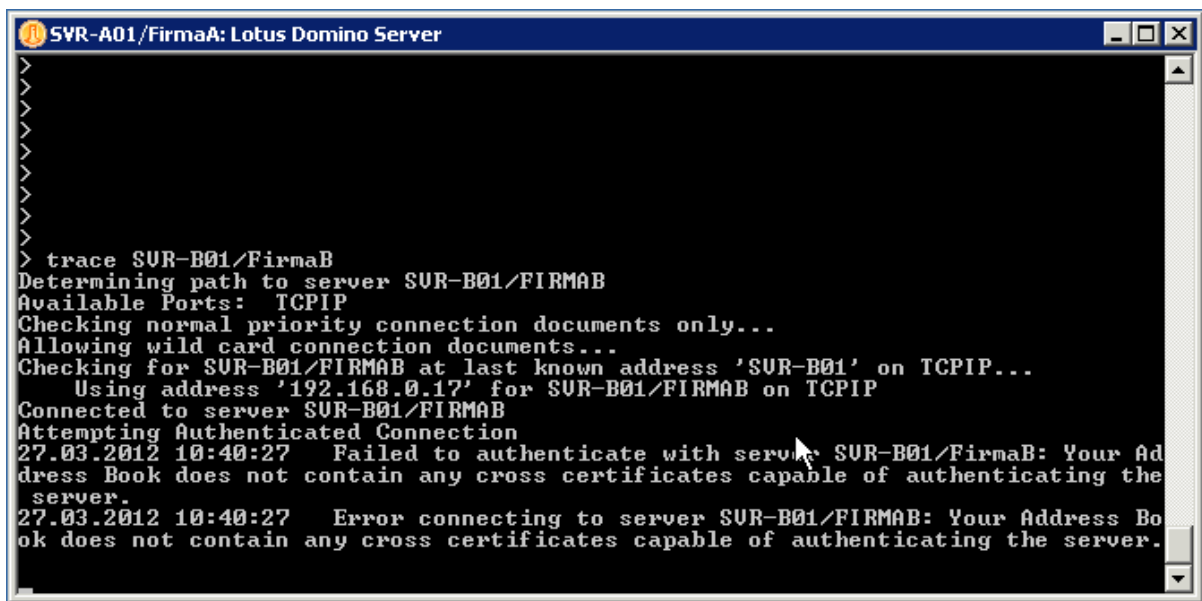
In dieser Lektion wird gezeigt, wie ein Gegenzertifikat schnell und komfortabel erstellt werden kann.

### **Hinweis**

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

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

### *Meldung beim Verbindungsaufbau zwischen Domino Servern ohne Gegenzertifikat*



```
SVR-A01/FirmaA: Lotus Domino Server
>
>
>
>
>
>
>
> trace SUR-B01/FirmaB
Determining path to server SUR-B01/FIRMAB
Available Ports: TCPIP
Checking normal priority connection documents only...
Allowing wild card connection documents...
Checking for SUR-B01/FIRMAB at last known address 'SUR-B01' on TCPIP...
    Using address '192.168.0.17' for SUR-B01/FIRMAB on TCPIP
Connected to server SUR-B01/FIRMAB
Attempting Authenticated Connection
27.03.2012 10:40:27 Failed to authenticate with server SUR-B01/FirmaB: Your Ad
dress Book does not contain any cross certificates capable of authenticating the
server.
27.03.2012 10:40:27 Error connecting to server SUR-B01/FIRMAB: Your Address Bo
ok does not contain any cross certificates capable of authenticating the server.
```

Eine Kommunikation zwischen Domino Servern aus unterschiedlichen Organisationen ist "einfach so" nicht möglich. Versucht man z.B. mit dem Konsolen-Befehl TRACE eine Verbindung aufzubauen (eine Erreichbarkeit über das Netzwerk vorausgesetzt), so erscheint die im Screenshot gezeigte Fehlermeldung.

### **Meldungen an der Serverkonsole**

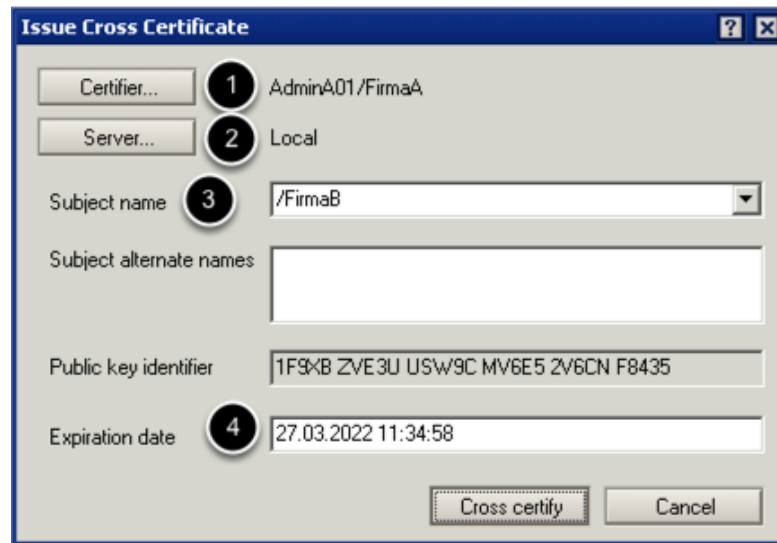
1. *Attempting Authenticated Connection*
2. *Failed to authenticate with server SVR-B01/FirmaB: Your Address Book does not contain any cross certificates capable of authenticating the server.*
3. *Error connecting to server SVR-B01/FIRMAB: Your Address Book does not contain any cross certificates capable of authenticating the server.*

### **Erklärung**

1. Es wird versucht, eine Verbindung aufzubauen, hierbei überprüfen sich die beiden Partner (Authentifizierung).
2. Die Authentifizierung schlägt fehl, weil in der NAMES.NSF kein Gegenzertifikat zur Bestätigung des fremden Domino Servers existiert.
3. Es ist kein Verbindungsaufbau möglich, da in der NAMES.NSF kein Gegenzertifikat zur Bestätigung des fremden Domino Servers existiert.

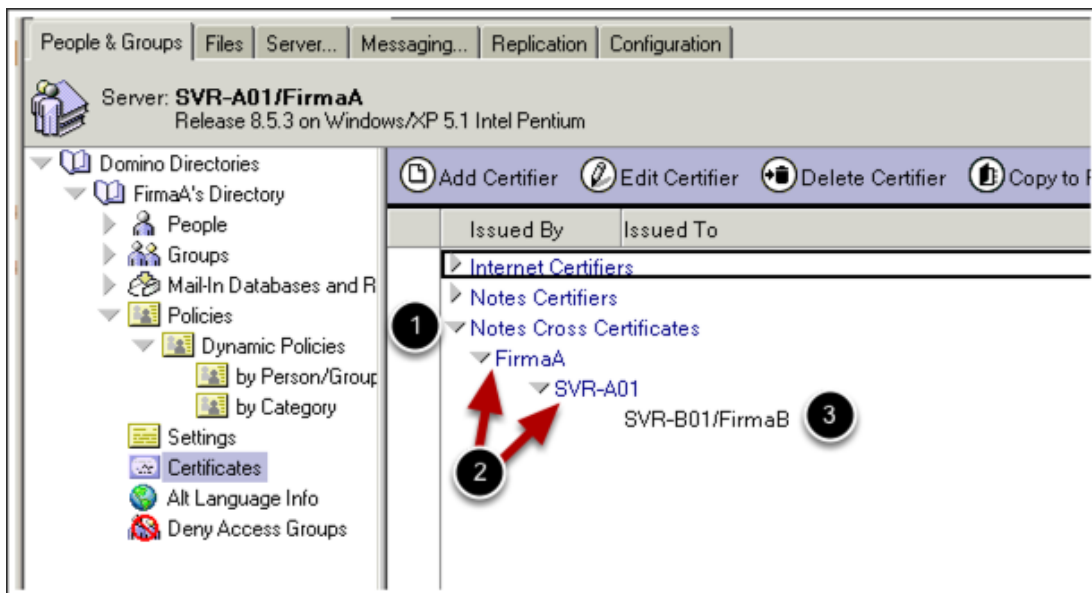
Meldungen in ähnlicher Form werden übrigens auch auf der Serverkonsole der Gegenseite angezeigt.

Dies würde uns für die Kommunikation der Domino Server nichts nützen. Klicken Sie also auf die Schaltfläche **'Advanced...'**. Es erscheint folgender Dialog.



Auch hier bitte wieder NICHT sofort auf die Schaltfläche **'Cross certify'** klicken, denn die Angaben im Dialog sind noch nicht für die Erstellung des Gegenzertifikates für die Domino Server geeignet.

1. Über die Schaltfläche **'Certifier...'** wählen Sie aus, wer aus der eigenen Notes/Domino Umgebung der Gegenseite vertraut. Dies sollte die Server-ID-Datei des eigenen Domino Servers sein.
2. Wo soll das Gegenzertifikat gespeichert werden? Lokal in der NAMES.NSF des Clients (nicht sinnvoll) oder in der NAMES.NSF auf dem eigenen Server? Wählen Sie durch die Schaltfläche **'Server...'** einen eigenen Domino Server aus.
3. Auf welcher Ebene möchten Sie der Gegenseite vertrauen? Vorab ausgewählt ist die Organisationsebene, aber Sie können durch einen Klick auf den Auswahlpfeil rechts explizit den Domino Server der Gegenseite festlegen.
4. Wie lange soll das Gegenzertifikat gültig sein? Voreingestellt ist eine Gültigkeitsdauer von 10 Jahren. Da man später durch das einfache Löschen des Gegenzertifikatdokumentes die Verbindung zur Gegenseite jederzeit beenden kann können hier auch problemlos längere Laufzeiten angegeben werden.



Wählen Sie im Domino Administrator das Register 'People & Groups' und selektieren Sie dann den Navigationspunkt 'Certificates'.

1. Übersicht der existierenden Gegenzertifikate. Falls erforderlich, diesen Bereich durch einen Klick aufklappen.
2. Wer in der eigenen Notes/Domino Umgebung vertraut der Gegenseite? Im Beispiel ist es der Domino Server SVR-A01/FirmaA.
3. Wem schenken wir unser Vertrauen? Im Beispiel dem Domino Server SVR-B01/FirmaB der Gegenseite.

Hiermit sind alle erforderlichen Schritte in der eigenen Notes/Domino Umgebung abgeschlossen.

**Hinweis**

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

Sofern alle Schritte korrekt ausgeführt wurden, steht einer Verbindungsaufnahme der beteiligten Server nichts mehr im Wege. An der Serverkonsole sieht der Verbindungsaufbau mittels TRACE-Befehl nun so aus.

Server Connection: SVR-A01/FirmaA to SVR-B01/FirmaB			
Basics		Replication/Routing	Schedule
<b>Replication</b>		<b>Routing</b>	
Replication task:	<input type="checkbox"/> Disabled	Routing task:	<input type="checkbox"/> Mail Routing
Replicate databases of:	<input type="checkbox"/> Low & Medium & High priority	Route at once if:	<input type="checkbox"/> 1 messages pending
Replication type:	<input type="checkbox"/> Pull Push	Routing cost:	<input type="checkbox"/> 1
Files/Directory paths to replicate:	<input type="checkbox"/> (all if none specified)	Router type:	<input type="checkbox"/> Push Only
Files/Directory paths to NOT replicate:	<input type="checkbox"/>		

Auf dem Register 'Replication/Routing' wird die Replikation deaktiviert und die für das Mailrouting erforderlichen Parameter auf Standardeinstellung belassen.

Server Connection: SVR-A01/FirmaA to SVR-B01/FirmaB	
Basics	
<b>Scheduled Connection</b>	
Schedule:	<input type="checkbox"/> Enabled
Connect at times:	<input type="checkbox"/> 00:00 - 23:59 each day
Repeat interval of:	<input type="checkbox"/> 5 minutes
Days of week:	<input type="checkbox"/> Sun, Mon, Tue, Wed, Thu, Fri, Sat

Die Einstellungen für den gewünschten Zeitplan legen Sie mit für Ihre Umgebung sinnvollen Werten fest.

**Hinweis**

Der eingestellte Zeitplan (Feld 'Repeat interval of') hat keine Auswirkung, da die Einstellungen auf dem Register 'Replication/Routing' -> 'Route at once if' angeben, dass schon bei einer anstehenden eMail der Routingvorgang ausgelöst wird.

Die Einstellungen sind somit abgeschlossen und Sie können das Verbindungsdokument speichern. Auf der Gegenseite ist ebenfalls ein Mailrouting Verbindungsdokument erforderlich, damit das Mailrouting in beide Richtungen funktioniert.

**Hinweis**

Sie können an der Domino Server Konsole mittels des Befehls

`SHOW SCHEDULE`

überprüfen, ob der als Quellserver festgelegte Domino Server den im Verbindungsdokument festgelegten Zeitplan in seine Ausführungsliste übernommen hat.

1. Erstellen Sie eine lokale Replik der gewünschten Datenbank(en). Es ist nicht empfehlenswert, eine auf einem Domino Server gespeicherte Datenbank im laufenden Betrieb "weg zu kopieren". Der Domino Server hat die Datenbank möglicherweise gerade selbst im Zugriff - eine defekte oder nicht vollständige Kopie könnte die Folge sein.
2. Stellen Sie ggf. die ACL der lokalen Replik "neutral" ein. Man könnte z.B. alle existierenden ACL Einträge löschen und dem verbleibenden Eintrag '-Default-' Managerrechte zuweisen. So kann die Gegenseite diese Datenbank sofort ohne Zugriffsprobleme verwenden und die ACL den eigenen Vorstellungen entsprechend anpassen.
3. Senden Sie die Datenbank als Anhang einer eMail an den zuständigen Administrator der Gegenseite.

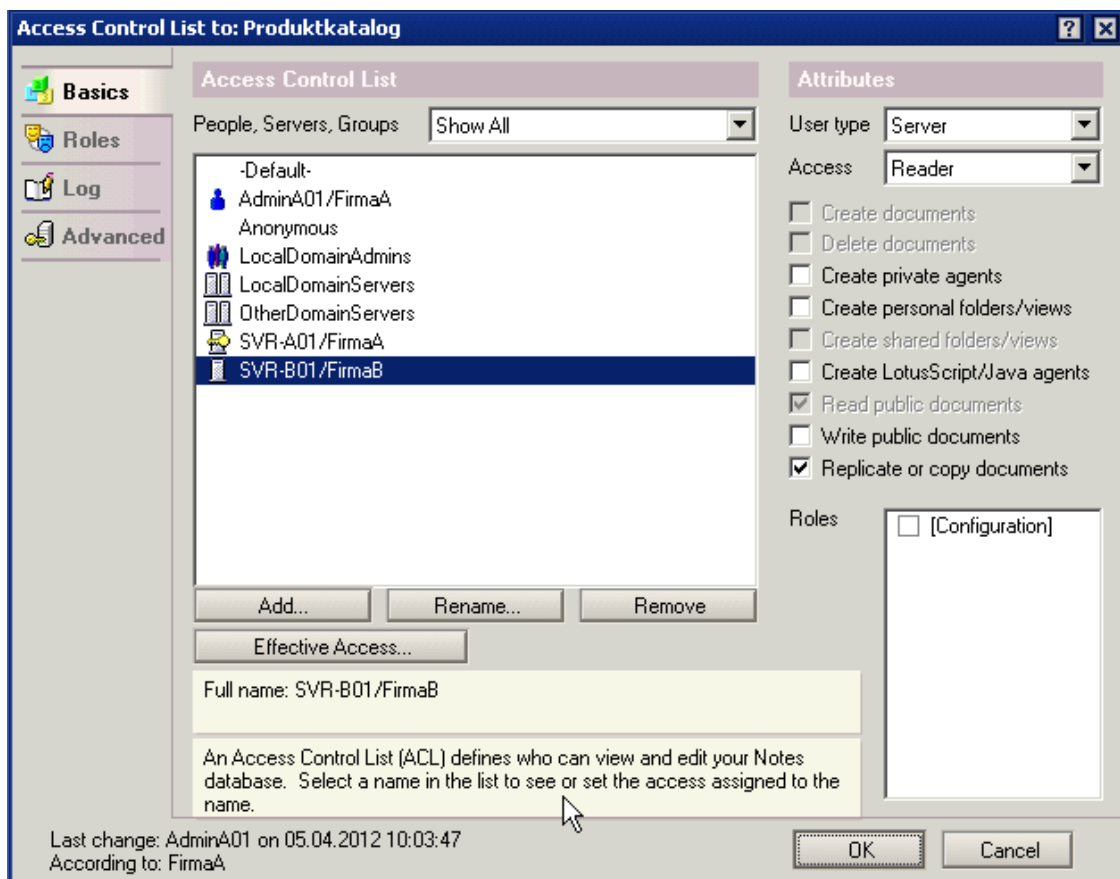
Nach dem erfolgreichen Transfer der gewünschten Notes Datenbank muss der Gegenseite noch ein Zugriff in der Datenbank-ACL gewährt werden. Die hierzu erforderlichen Einstellungen finden Sie im nächsten Abschnitt.

### ACL Einstellungen

Administratoren haben oft das Problem, eine geeignete und für die eigenen Belange passende Einstellung für die ACL (Zugriffskontrollliste) der eigenen Datenbank zu finden. Das mag daran liegen, dass man zu kompliziert denkt und dann unsicher ist bzw. zu keiner Lösung kommt.

Denken Sie bei der Festlegung für die ACL-Einstellungen der eigenen Datenbank nicht gleichzeitig daran, was auf der Gegenseite eingestellt sein müsste. Dies ist nicht *Ihre* Aufgabe und spielt im Moment auch keine Rolle da Sie nur für die ACL der eigenen Datenbank verantwortlich sind.

### Beispiel 1: ACL Einstellung zur reinen Weitergabe von Informationen





### Hinweis

Es ist grundsätzlich bei der Replikation mit fremden Domino Servern sinnvoll, die zu replizierenden Datenbanken im Feld '**Files/Directory path to replicate**' explizit anzugeben.

So vermeiden Sie, dass z.B. Templates (die im Lieferumfang befindlichen Systemschablonen haben immer die gleichen Replik-IDs) repliziert werden.

Scheduled Connection	
Schedule:	<input checked="" type="checkbox"/> Enabled
Connect at times:	<input checked="" type="checkbox"/> 00:00 - 23:59 each day
Repeat interval of:	<input checked="" type="checkbox"/> 30 minutes
Days of week:	<input checked="" type="checkbox"/> Sun, Mon, Tue, Wed, Thu, Fri, Sat

Den Zeitplan auf dem Register '**Schedule**' legen Sie mit für Ihre Umgebung sinnvollen Werten fest.

Sobald Sie das Verbindungsdokument gespeichert haben, sollte der als Quellserver angegebene Domino Server die zyklische Replikation starten.

### Hinweis

Sie können an der Domino Server Konsole mittels des Befehls

```
SHOW SCHEDULE
```

überprüfen, ob der als Quellserver festgelegte Domino Server den im Verbindungsdokument festgelegten Zeitplan in seine Ausführungsliste übernommen hat.

## 2.6. Domänendokumente

Um das Arbeiten mit mehreren Domänen komfortabler zu machen und um bestimmte Aspekte des Mailroutings steuern zu können, können benachbarte oder nicht benachbarte Domänendokumente verwendet werden.

Da Domänendokumente lediglich einen Einfluss auf das Mailrouting haben, spricht man gemeinhin nicht von Domänen-/Organisationsdokumenten, sondern nur von Domänendokumenten.

Durch die Felder auf dem Register '**Restrictions**' können Sie steuern, wer Mails an die benachbarte Domain senden darf.

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

Auf dem Register '**Calendar Information**' wird der Server der benachbarten Domäne benannt, welcher Zeitplanungsanfragen für die benachbarte Domäne beantwortet.

#### **Fazit**

Benachbarte Domänendokumente sind grundsätzlich nur dann erforderlich, wenn man das Routing von Nachrichten durch die eigene Domäne zur benachbarten Domäne einschränken möchte oder wenn domänenübergreifende Kalenderabfragen funktionieren müssen.

## Nicht benachbartes Domänendokument

The screenshot shows the 'Domain FirmaC' configuration interface. The 'Basics' tab is active. The following fields are visible:

Domain type:	Non-adjacent Domain	1
Mail sent to domain:	FirmaC	2
Route through domain:	FirmaB	3
Domain description:	Keine direkte Verbindung zu FirmaC	4

Auf dem Register '**Basics**' werden folgende Einstellungen vorgenommen:

1. Im Feld '**Domain type**' wählen Sie die Option '**Non-adjacent Domain**' (nicht benachbarte Domäne).
2. An welche Domain soll die Nachricht gesendet werden? Dies ist die nicht benachbarte Domäne, zu der keine direkte Verbindung existiert.
3. Über welche benachbarte Domäne soll die Nachricht gesendet werden?
4. Die Angabe im Feld '**Domain description**' ist optional.

Die verbleibenden Register '**Restrictions**' und '**Calendar Information**' sind mit den Registern bei den benachbarten Domänendokumenten identisch. Die Beschreibung der einzelnen Felder finden Sie dort.

Wenn ein Domänendokument für eine nicht benachbarte Domäne existiert, reduziert sich die Adressierung einer eMail, welcher ein Sender aus Domäne A an einen Empfänger in Domäne C sendet auf das übliche Format.

AdminC01/FirmaC@FirmaC

Anhand der Information im nicht benachbarten Domänendokument weiß der Domino Server in Domäne A wie er die Nachricht nach Domäne C routen kann.

### Fazit

Nicht benachbarte Domänendokumente werden benötigt, wenn man Nachrichten zu fremden Domänen senden möchte, zu denen man keine direkte Verbindung hat. Sie sind nicht zwingend erforderlich, vereinfachen aber die Adressierung von Nachrichten.

### Einbindung fremder Verzeichnisse über die NOTES.INI

Die Einbindung fremder Verzeichnisse kann in der Datei NOTES.INI des eigenen Servers durch Nutzung des Parameters NAMES erfolgen.

NAMES=NAMES.NSF, NAMES-FirmaB.NSF, NAMES-FirmaC.NSF

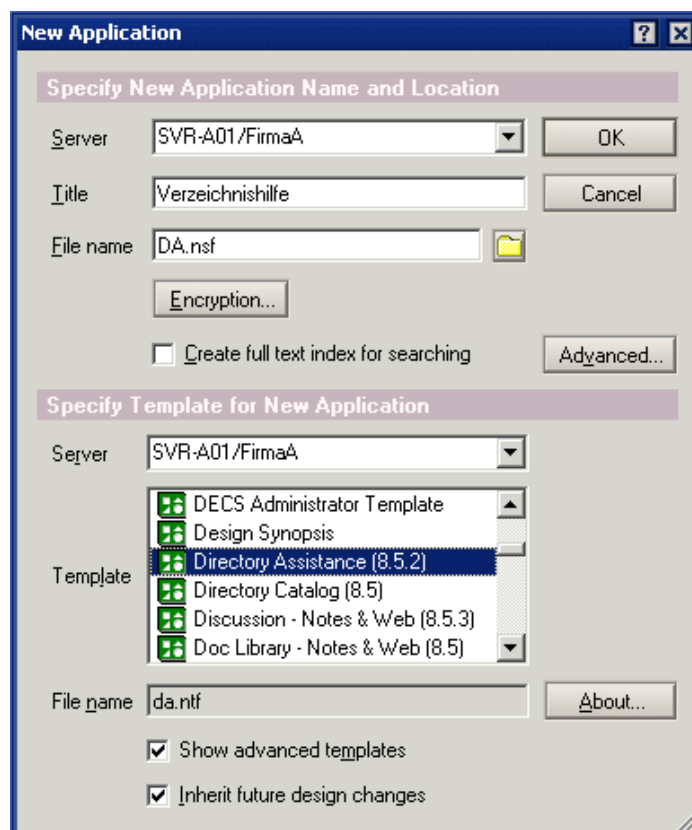
Möchte man direkt ein Verzeichnis eines fremden Servers einbinden, so ist dies in folgender Form möglich.

NAMES=NAMES.NSF, CN=SVR-B01/O=FirmaB!!NAMES.NSF

### Hinweis

Die Reihenfolge, in welcher die fremden Verzeichnisse in der NOTES.INI angegeben werden, bestimmt auch die Suchreihenfolge beim Adressieren von Mails.

### Nutzung der Verzeichnishilfe



Die Verzeichnishilfe stellt eine leistungsfähigere Alternative zur Verwendung des Parameters NAMES=... in der Datei NOTES.INI dar.

Bei Nutzung der Verzeichnishilfe wird eine neue Datenbank auf Basis der Schablone '**Directory Assistance**' (DA.NTF) erstellt, diese Datenbank im Serverdokument eingetragen und in der Datenbank die gewünschten fremden Verzeichnisse benannt.

Erstellen Sie zunächst die neue Datenbank mit den im Screenshot angegebenen Parametern und wählen Sie die korrekte Schablone aus.

DIRECTORY ASSISTANCE								
Basics   Naming Contexts (Rules)   Domino								
	OrgUnit4	OrgUnit3	OrgUnit2	OrgUnit1	Organization	Country	Enabled	Trusted for Credentials
N.C. 1:	<input type="text" value="/*"/>	<input type="text" value="/*"/>	<input type="text" value="/*"/>	<input type="text" value="/*"/>	<input type="text" value="/*"/>	<input type="text" value="/*"/>	<input type="text" value="Yes"/>	<input type="text" value="No"/>
N.C. 2:	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="No"/>	<input type="text" value="No"/>
N.C. 3:	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="No"/>	<input type="text" value="No"/>
N.C. 4:	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="No"/>	<input type="text" value="No"/>
N.C. 5:	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="No"/>	<input type="text" value="No"/>

Auf dem Register '**Naming Contexts (Rules)**' können Namensbestandteile des fremden Verzeichnisses festgelegt werden. Für später ausgeführte Suchläufe kann so gesteuert werden, dass nur noch bestimmte fremde Verzeichnisse durchsucht werden.

Würde man als Beispiel einen Eintrag in der Form

`*/*/*/FirmaB/*`

wählen und bei der späteren Adressierung einer eMail würde der Anwender z.B. **Hans Wurst/FirmaB** eingeben, so würde lediglich das fremde Verzeichnis durchsucht, wo **FirmaB** für die Organisationsebene festgelegt wurde.

#### Hinweis

Da Anwender beim Adressieren von eMails i.d.R. bestenfalls den Vor- und Nachnamen eingeben lohnt es sich kaum die insgesamt 5 möglichen Namensschemata auszufüllen. In den meisten Fällen wird der im Screenshot gezeigte Standard verwendet.

DIRECTORY ASSISTANCE			
Basics   Naming Contexts (Rules)   Domino			
Replicas			
Application links:	<input type="text"/>		
	<b>OR</b>		
	Server Name	Domino Directory Filename	Enabled
Replica1:	<input type="text" value="SVR-A01/FirmaA"/>	<input type="text" value="NAMES-FirmaB.NSF"/>	<input type="text" value="Yes"/>
Replica2:	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="No"/>
Replica3:	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="No"/>
Replica4:	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="No"/>
Replica5:	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="No"/>

Auf dem letzten Register '**Domino**' (diese Register kann auch LDAP heißen, sofern Sie den Domänentyp auf dem Register '**Basic**' entsprechend gewählt haben) werden entweder Links zum fremden Verzeichnis (Feld '**Applications Links**') eingefügt, oder bis zu 5 Repliken des fremden Verzeichnisses namentlich eingetragen.

Durch die Verwendung mehrerer Links bzw. das namentliche Eintragen von bis zu 5 Repliken kann der Domino Server bei Problemen mit einem fremden Verzeichnis auf eine andere Replik umschalten.

### 3. Benutzerverwaltung

#### 3.1. Automatisches Befüllen von Gruppen

Im Kontext der Benutzerverwaltung ist die Pflege der im Verzeichnis (NAMES.NSF) gespeicherten Gruppen ein wichtiger, aber auch zeitintensiver Prozess.

Um den Aufwand zur Pflege der Gruppen zu reduzieren hat IBM die Maske zur Gruppendefinition um eine Option zum automatischen Befüllen der Gruppe erweitert.

#### *Gruppendokument mit automatischer Befüllung der Mitglieder*

Multi-purpose group : Anwender-auf-SVR-A01

Basics | Comments | Administration

Basics

Group name: Anwender-auf-SVR-A01

Group type: Multi-purpose

Category:

Description:

Mail Domain:

Internet Address:

Auto Populate Method: Home Server (1)

Home Server(s): SVR-A01/FirmaA (2)

Additional Members: (3)

Excluded Members: (4)

Members: (5)

Auf dem Register 'Basic' finden Sie die Einstellungen um die Gruppe automatisch mit Mitgliedern zu befüllen.

1. Im Feld '**Auto Populate Method**' wählen Sie die Option '**Home Server**'. Es werden alle Personen, welche ihre Maildatenbank auf dem im Feld '**Home Server(s)**' angegebenen Domino Server gespeichert haben als Mitglied dieser Gruppe eingetragen.
2. Im Feld '**Home Server(s)**' wählen Sie den oder die gewünschten Domino Server aus.
3. Welche Personen oder Gruppen sollen zusätzliche Mitglieder dieser Gruppe werden?
4. Welche Personen sollen nicht automatisch in die Gruppe aufgenommen werden?
5. Hier werden die Mitglieder angezeigt, sobald die Gruppe automatisch befüllt wurde.

Nach dem Speichern der neuen Gruppe sollten die Mitglieder innerhalb von 30 Minuten (Vorgabe) angezeigt werden.

Auto Populate Method: Home Server

Home Server(s): SVR-A01/FirmaA

Additional Members:

Excluded Members:

Members: AdminA01/FirmaA  
Hans Berger/FirmaA

### 3.2. Rekursive Auflösung von Gruppenmitgliedschaften

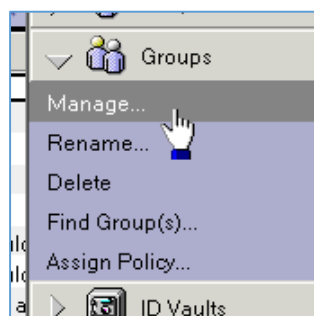
In Notes/Domino Umgebungen dürfen Gruppen weitere Gruppen als Mitglieder enthalten, d.h. die Gruppen dürfen ineinander verschachtelt werden.

Für Belange des Mailroutings ist die maximale Verschachtelungstiefe auf fünf und für sonstige Zwecke auf maximal sechs Ebenen festgelegt.

Bei intensiver Nutzung der Verschachtelung stellt sich in der Praxis oft die Frage, in welchen Gruppen nun ein bestimmter Anwender gelistet ist. OHNE den Einsatz der Verschachtelung ist diese Frage durch einen einfachen Suchlauf zu beantworten.

Wenn Gruppen stark verschachtelt sind, hilft das Gruppen-Verwaltungstool im Domino Administrator.

#### *Aufruf des Gruppen-Verwaltungstools*



1. Öffnen Sie den Domino Administrator.
2. Wählen Sie das Register '**People & Groups**'.
3. Wählen Sie rechts bei den Gruppenwerkzeugen die Option '**Manage...**'.

Der Dialog zur Verwaltung der Gruppen wird am Bildschirm angezeigt.

### 3.3. Abwesenheitsservice generiert Out-of-Office Meldungen

In älteren Notes/Domino Versionen wurden Abwesenheitsnachrichten immer durch einen Agenten, welcher in der Maildatenbank der Anwender gespeichert ist, generiert.

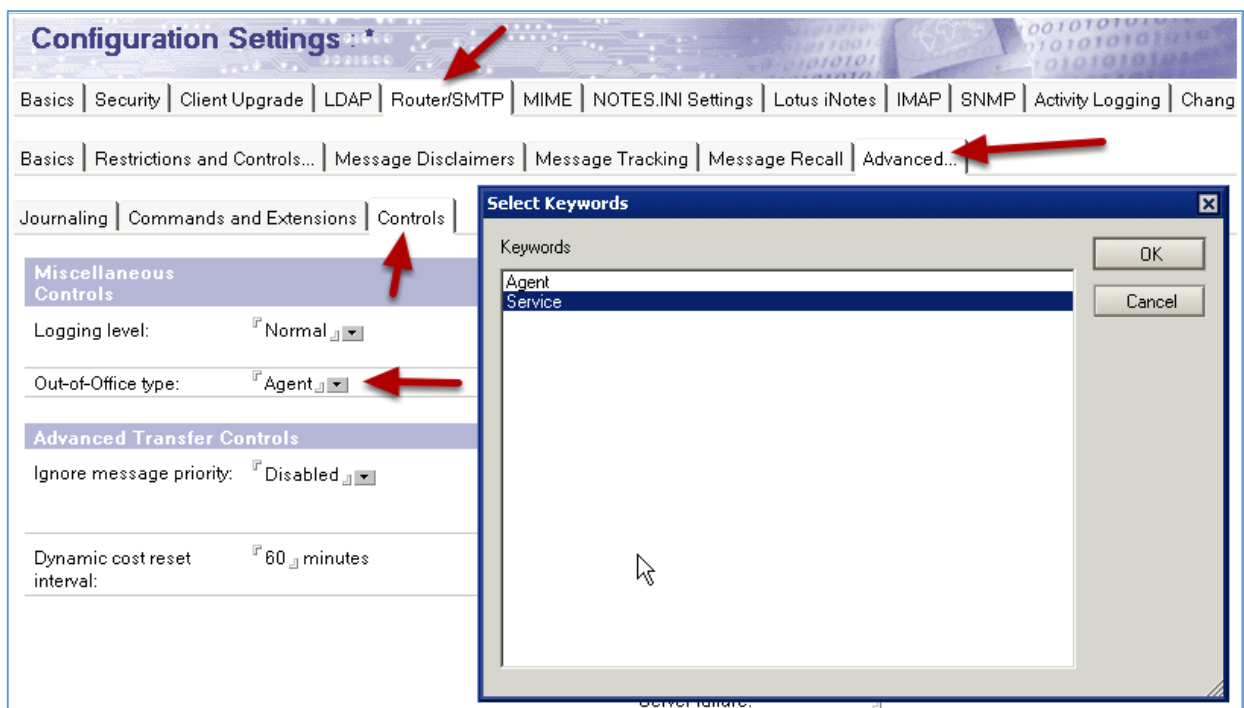
Da der Zeitplan für die Ausführung dieses Agenten auf ein Intervall von mehreren Stunden (Vorgabe) eingestellt war, kann man nicht von einer zeitnahen Benachrichtigung des Absenders einer eMail sprechen. Zudem war die minimal mögliche Zeitspanne für eine Abwesenheit auf einen Tag festgelegt.

Seit Notes/Domino Version 8.x kann die Generierung der Abwesenheitsnachrichten durch den Abwesenheitsservice erfolgen. Es ergeben sich folgende Vorteile.

- Abwesenheitsnachrichten werden in Echtzeit, also unmittelbar nach Eingang einer eMail erstellt.
- Die minimal mögliche Zeitspanne für eine Abwesenheit wird auf eine Stunde verkürzt.

Die Nutzung des Abwesenheitsservice ist optional und auch nach der Installation einer ganz neuen Notes/Domino Umgebung nicht automatisch aktiviert. Unter der Voraussetzung, dass ein Version 8.x Domino Server verwendet wird und die Maildatenbanken der Anwender auf dem Template der Version 8.x basieren, kann der Abwesenheitsservice für einen Domino Server aktiviert werden.

#### Aktivierung des Abwesenheitsservice im Konfigurationsdokument



1. Öffnen Sie den Domino Administrator.
2. Wählen Sie das Register **'Configuration'**.
3. Wählen Sie links in der Navigation den Punkt **'Server' -> 'Configurations'**.
4. Öffnen Sie das für den gewünschten Server relevante Konfigurationsdokument oder erstellen Sie ein neues Konfigurationsdokument.
5. Wählen Sie das Register **'Router/SMTP' -> 'Advanced' -> 'Controls'**.
6. Im Feld **'Out-of-Office typ'** wählen Sie die Option **'Service'**.
7. Speichern und schließen Sie das Konfigurationsdokument.

Spätestens nach einem Neustart des betroffenen Domino Servers sollte der Abwesenheitsservice aktiv sein.



### 3.4. ID-Vault (automatisches Backup von Anwender ID-Dateien)

Anwender ID-Dateien bilden den Zugangsschlüssel zur Nutzung einer Notes/Domino Infrastruktur. Da sie neben dem Benutzernamen, den von Zulassungsstellen übernommenen Zertifikaten, dem öffentlichen und privaten Schlüssel des Anwenders möglicherweise auch geheime Verschlüsselungsschlüssel enthalten, ist das Vorhalten eines Backups jeder einzelnen Anwender ID-Datei unabdingbar.

Da Anwender ID-Dateien altern (Ablaufdatum) und sich ändern (neuer Benutzername, Abteilungswechsel, Kennwortänderung usw.), ist eine konventionelle Einmal-Sicherung (z.B. einmal direkt nach der Registrierung eines Anwenders) in der Praxis meist nicht ausreichend. Eine solche im Backup aufbewahrte Anwender ID-Datei ist irgendwann abgelaufen und der Benutzername oder sonstige Inhalte sind ebenfalls nicht mehr zutreffend.

Nur durch ein dynamisches Backup (erneute Sicherung nach jeder Änderung der Anwender ID-Datei) können diese Probleme vermieden werden.

In Versionen vor Notes/Domino 8.5 existierte für diesen Zweck die sogenannte ID-Wiederherstellung. Hierbei wurden aktuelle Sicherungen der Anwender ID-Dateien via Mailrouting in einer Datenbank (IDTresor) gespeichert und konnten von dort bei Problemen mit defekten Anwender ID Dateien oder vergessenen Kennwörtern aus dieser Datenbank extrahiert werden. Die zur Nutzung der ID Wiederherstellung erforderlichen Schritte wurden jedoch in der Praxis oft als umständlich und aufwändig empfunden. Wenn Sie sich hierzu ein eigenes Bild machen möchten, lesen Sie bitte die entsprechenden Kapitel in der Administratoren Hilfedatenbank nach.

Ab Version Notes/Domino 8.5 existiert nun der ID Vault, welcher in dieser Lektion vorgestellt und in der nächsten Lektion im Kursraum implementiert werden soll.

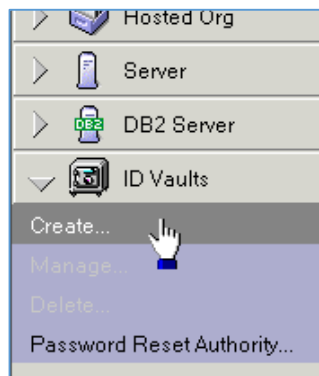
#### *Was ist der ID Vault?*

- ID Vault ist eine Domino Datenbank, welche geschützte Kopien der User-IDs vorhält.
- Administratoren und Benutzer erhalten mit dem ID Vault ein Werkzeug zur einfachen Verwaltung von Anwender ID-Dateien.
- Möglichkeit der Wiederherstellung/Kennwortrücksetzung durch autorisierte Benutzer (z.B. Helpdesk, Poweruser, etc.).
- Unterstützung für 3rd Party Programme (C, Java, JavaScript oder LotusScript).
- Automatische Synchronisation mehrerer Anwender ID-Dateien (z.B. beim Einsatz von Notebook und Desktop-PC).
- Wenig bis keine Benutzeraktivität erforderlich.
- Man kann Anwender ID-Dateien extrahieren, um z.B. auf die im ID Vault verschlüsselt abgelegten Daten zuzugreifen (Auditor-Rolle in der Vault Datenbank).
- Der Notes Anmeldedialog kann Hinweise zur Vorgehensweise bei vergessenem Kennwort enthalten (grünes "+" Symbol direkt im Anmeldedialog).
- Die Zuordnung von Anwendern zu einem ID Vault erfolgt über Richtlinien in Verbindung mit Sicherheits-Einstellungsdokumenten.

#### *Voraussetzungen*

- Notes Client und Domino Server Version 8.5 oder höher.
- Vault Trust Certificates (werden automatisch erstellt).
- Richtliniendokumente in Verbindung mit Sicherheitseinstellungsdokumenten (beide Dokumente können auf Wunsch während der Einrichtung des ID Vaults automatisch erstellt werden).
- Der Notes Client muss zwingend einen gültigen Eintrag für den Home-/Mailserver in den Arbeitsumgebungsdokumenten besitzen.

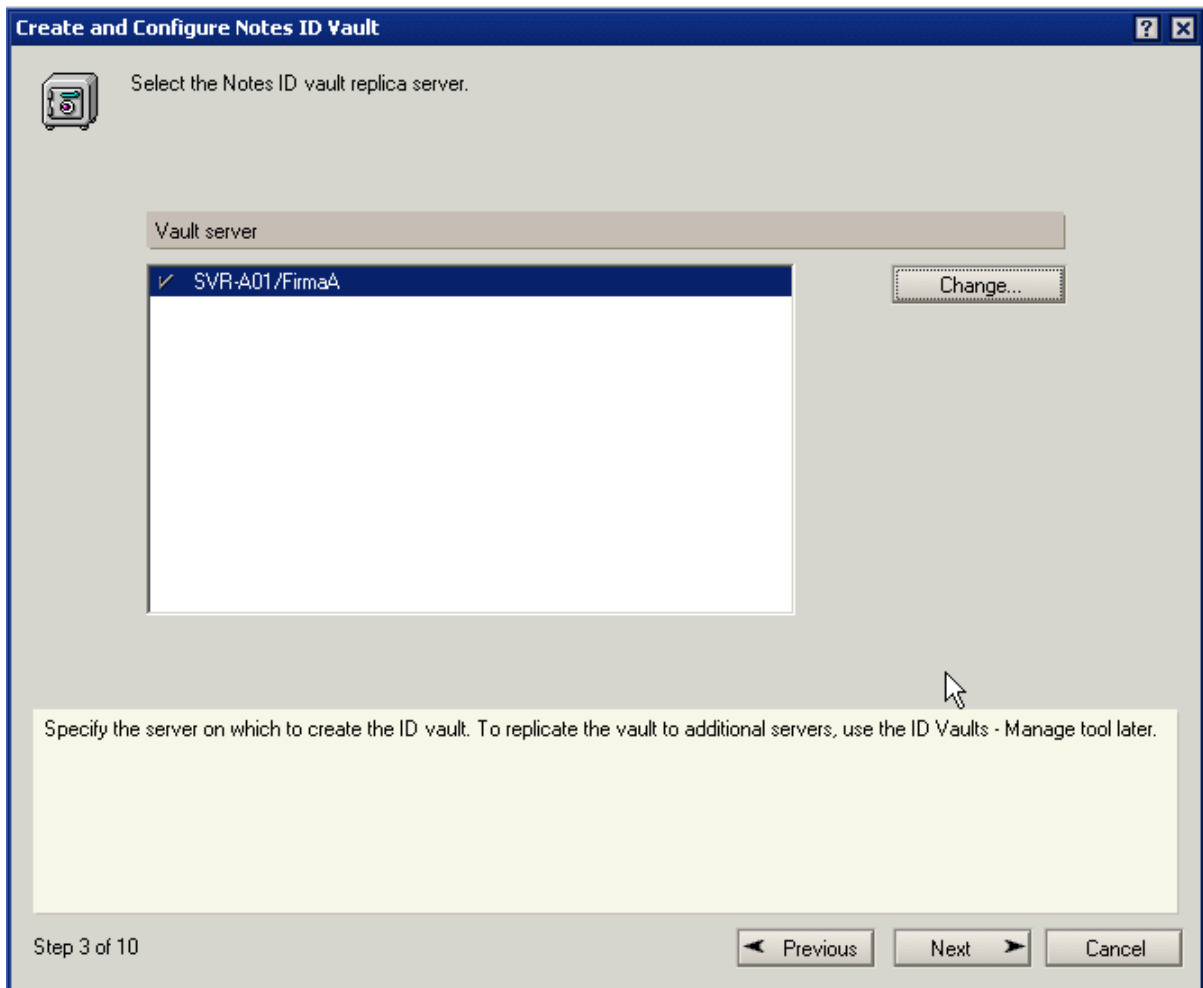
## Einrichtung des ID Vaults



Öffnen Sie den Administrations-Client und wählen Sie rechts in der Werkzeugleiste die Option 'ID Vaults' -> 'Create'. Die Konfiguration erfolgt in den folgenden Dialogen (zuvor wird noch eine Informationsseite angezeigt) in insgesamt 10 Schritten.

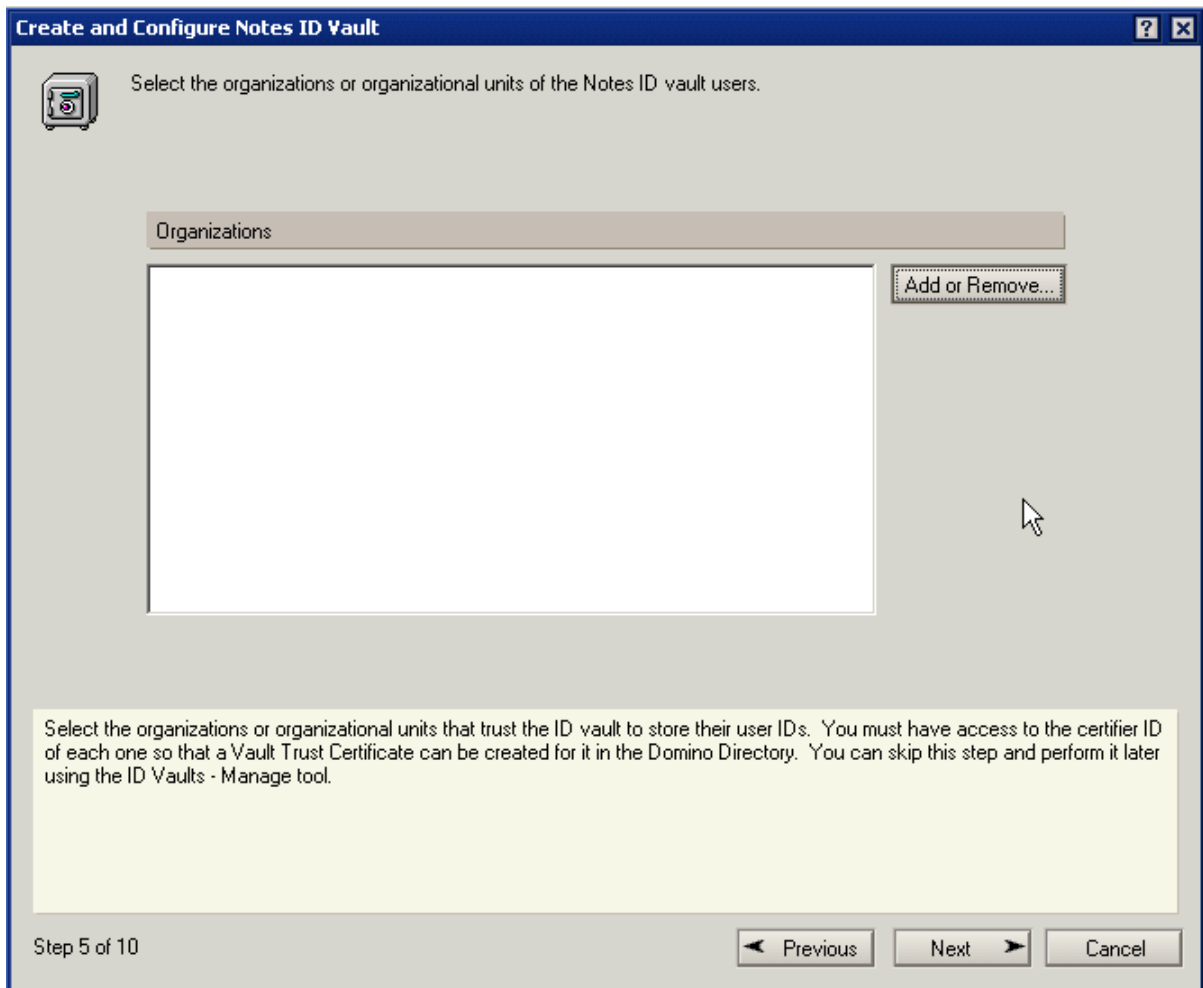
A screenshot of the 'Create and Configure Notes ID Vault' dialog box. The title bar reads 'Create and Configure Notes ID Vault'. The main area contains a vault icon and the text 'Specify a name and description for the Notes ID vault.' Below this are two input fields: 'Notes ID vault name' with the value 'IDTresor' and 'Notes ID vault description (optional - will also be Notes ID vault database title)' with the value 'Backup aller User-IDs'. A text box at the bottom provides instructions: 'The name you specify is used to form the hierarchical name, the database file name and the ID file name for the Notes ID vault. The name can not be the same as any organization or organizational unit. Example: 'ACMEVault' results in the hierarchical vault name '/ACMEVault', the vault database file name 'acmevault.nsf' and the vault ID file 'acmevault.id'. Once the Notes ID vault is created in the last step of this tool, you cannot change its name.' At the bottom, it says 'Step 1 of 10' and has 'Previous', 'Next', and 'Cancel' buttons.

Im ersten Schritt geben Sie den '**Notes ID vault name**' (Dateiname der ID Vault Datenbank) und die '**Notes ID Vault description**' (Titel der ID Vault Datenbank) an.

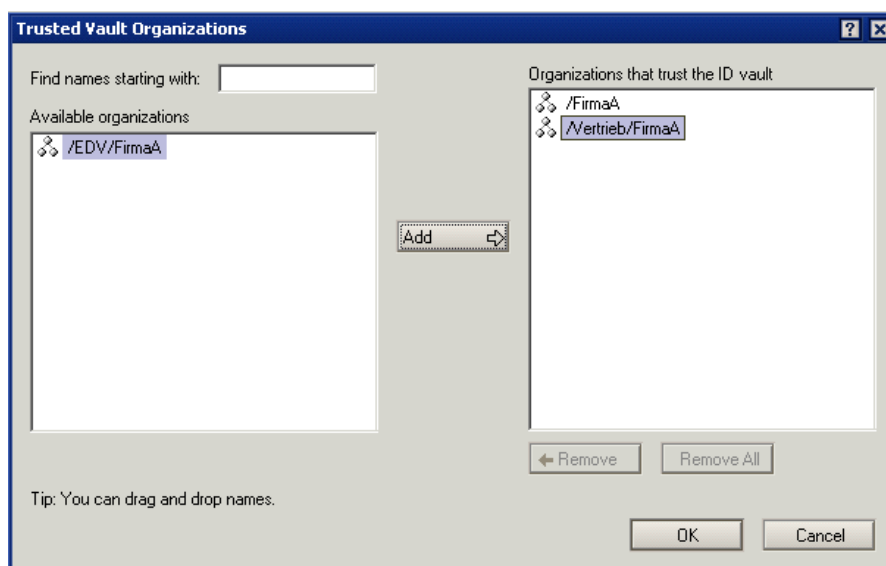


Auf welchem Server wird die ID Vault Datenbank erstellt? Es lässt sich in diesem Dialog nur ein Domino Server auswählen.

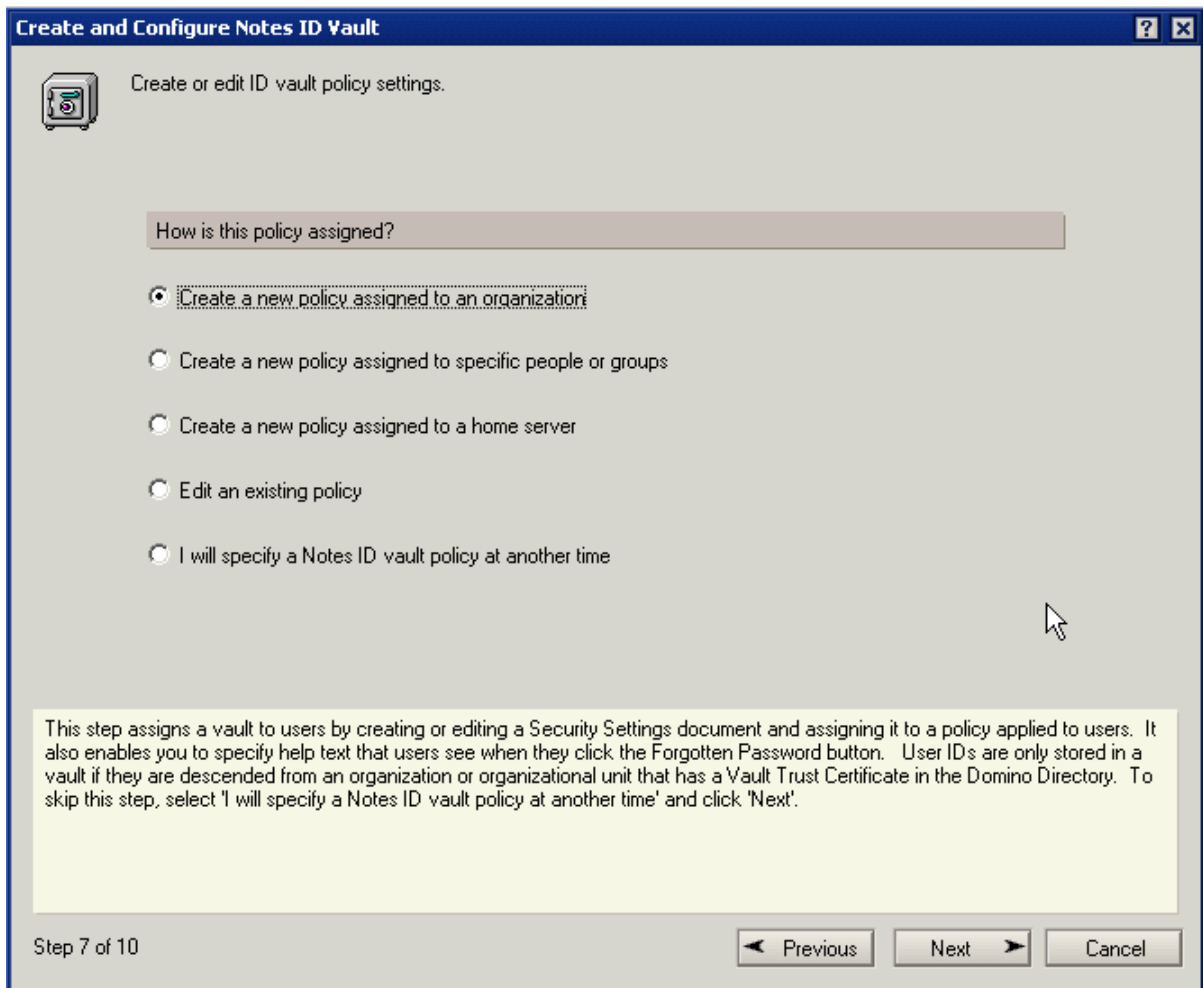
Sie können später auch jederzeit Repliken auf weiteren Domino Servern anlegen.



Welche Organisationen (O) und/oder Abteilungen (OU) vertrauen diesem ID Vault um die Anwender ID-Dateien in der ID Vault Datenbank zu speichern? In einem der folgenden Schritte müssen Sie auf jede ID-Datei der hier ausgewählten Zulassungsstellen einen Zugriff haben und das Kennwort eingeben. Nach einem Klick auf die Schaltfläche 'Add or Remove' erscheint der folgende Dialog.

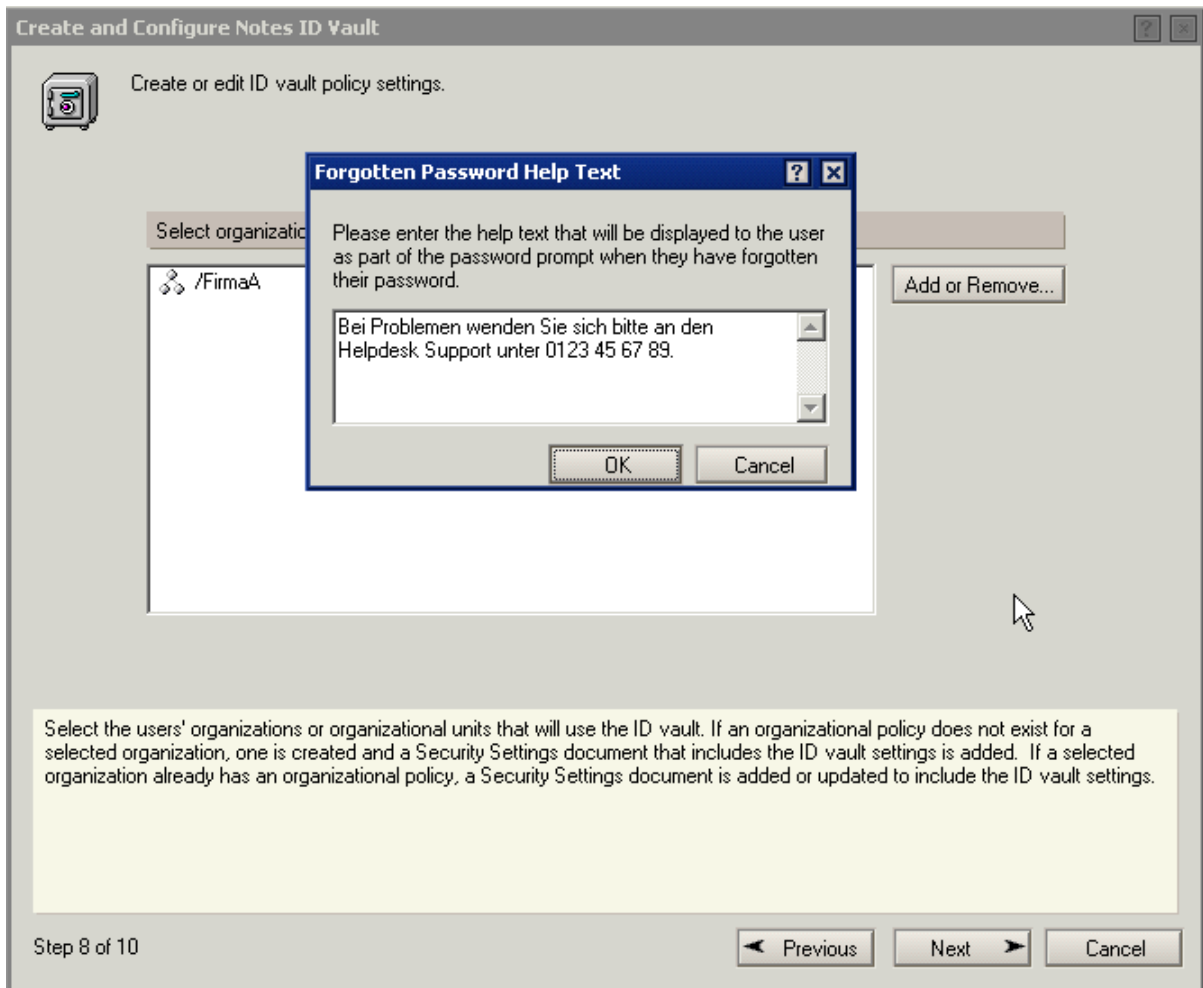


Wählen Sie die gewünschten Organisationen oder Abteilungen aus.

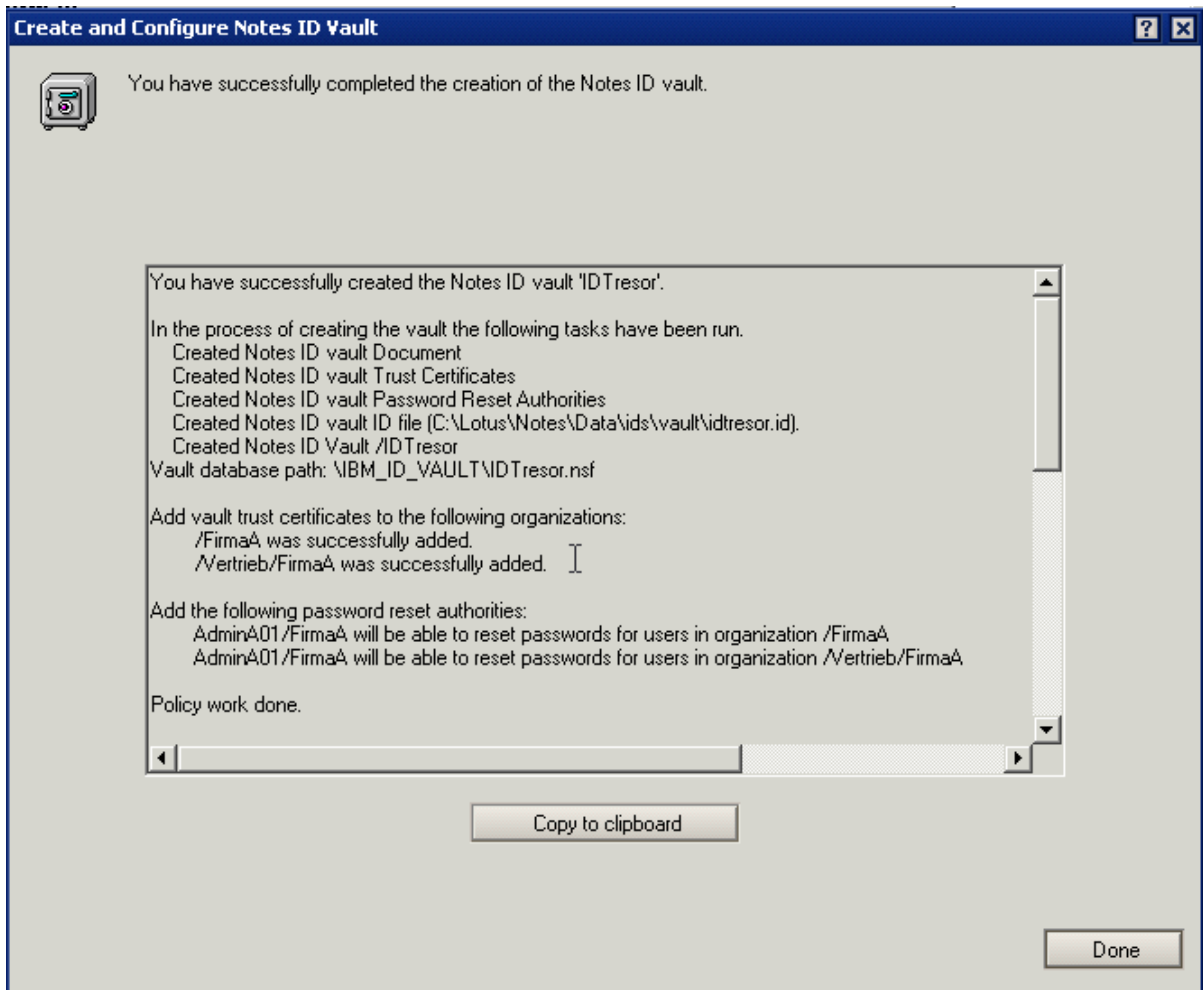


In diesem Schritt kann eine neue Richtlinie (Organisationsebene oder Explizit) erstellt oder auch eine bestehende Richtlinie editiert und verwendet werden.

Im Beispiel wird eine neue organisationsbezogene Richtlinie erstellt.



Sobald man im Schritt 8 auf die Schaltfläche **'Next'** klickt, kann ein Text angegeben werden, den die Anwender im Notes Anmeldedialog nach einem Klick auf ein grünes Plus (+) Zeichen angezeigt bekommen.



Der ID Vault wurde erstellt. Zur späteren Referenz kann die im Dialog angezeigte Information in die Zwischenablage kopiert und dann z.B. in einer Dokumentationsdatenbank gespeichert werden.

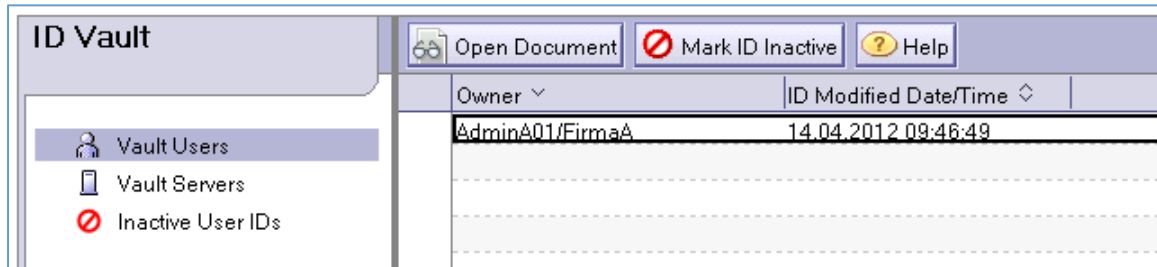
### Überprüfung der ID Vault Einrichtung

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

- **ID Vault Database.** Wurde im Verzeichnis IBM\_ID\_FAULT unterhalb des Data-Verzeichnisses gespeichert.
- **ID Vault Document** (in NAMES.NSF gespeichert). Wählen Sie im Domino Administrator das Register '**Configuration**' und dann links in der Navigation den Punkt '**Security**' -> '**ID Vaults**'.
- **Password Reset Certificates** (in NAMES.NSF gespeichert). Wählen Sie im Domino Administrator das Register '**Configuration**' und dann links in der Navigation den Punkt '**Security**' -> '**Certificates**' -> '**Certificates**'.
- **Vault Trust Certificates** (in NAMES.NSF gespeichert). Wählen Sie im Domino Administrator das Register '**Configuration**' und dann links in der Navigation den Punkt '**Security**' -> '**Certificates**' -> '**Certificates**'.
- **Policy-/Settingsdocuments** (in NAMES.NSF gespeichert). Wählen Sie im Domino Administrator das Register '**People & Groups**' und dann links in der Navigation den Punkt '**Policies**' oder '**Settings**'.

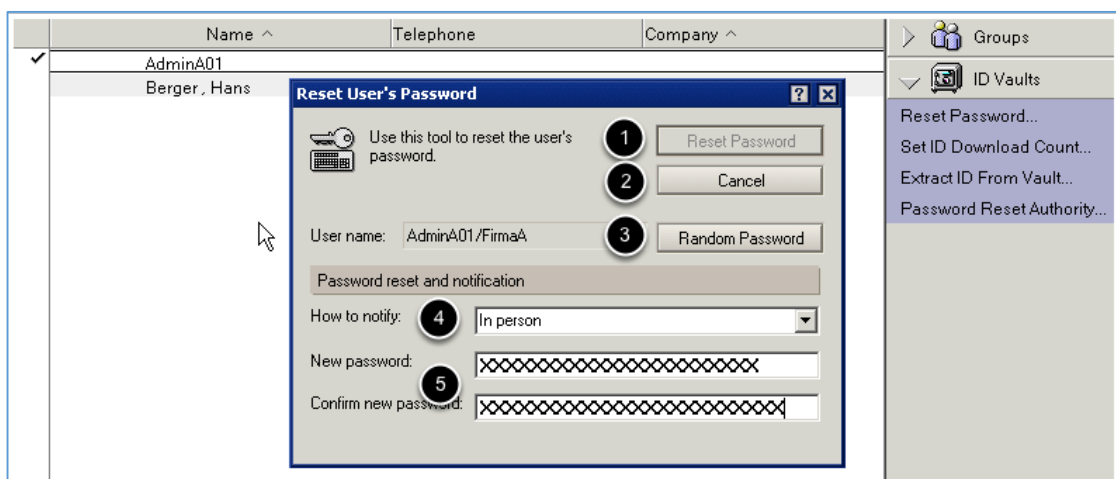
Zum Ausprobieren können Sie das Hochladen einer Anwender ID-Datei beschleunigen indem Sie in den Sicherheitseinstellungen eine Veränderung an der ID-Datei vornehmen. Im Beispiel (siehe Screenshot) wurde das mit der durch den Pfeil gekennzeichneten Option gemacht.

Unmittelbar nach dem Bestätigen dieser Änderung sollte die Anwender ID-Datei im ID Vault verfügbar sein.



Zur Kontrolle können Sie die ID Vault Datenbank (ist im Verzeichnis IBM\_ID\_VAULT unterhalb des Data-Verzeichnisses des Domino Servers gespeichert) öffnen und das erfolgreiche Hochladen der Anwender ID-Datei in der Ansicht '**Vault Users**' kontrollieren.

### *Nutzung des ID Vaults - Anwender hat das Kennwort vergessen*



Um einem Anwender bei vergessenem Kennwort zu helfen, öffnen Sie den Domino Administrator und selektieren das Register '**People & Grups**'. Wählen Sie links in der Navigation aus Ihrem Domino Verzeichnis die Ansicht '**People**'.

Selektieren Sie das gewünschte Personendokument und wählen Sie dann rechts in der Werkzeugleiste die Option '**ID Vaults**' -> '**Reset Password...**'. Im nachfolgenden Dialog haben Sie nun die folgenden Optionen.

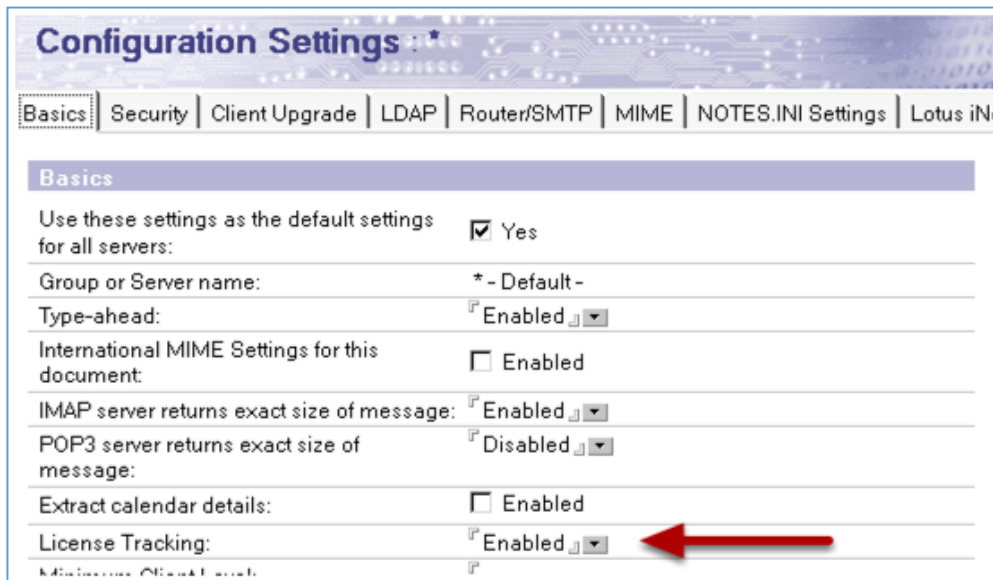
1. '**Reset Password**'. Durch diese Schaltfläche wird die Kennworrücksetzung gestartet.
2. '**Cancel**'. Der Vorgang wird abgebrochen.
3. '**Random Password**'. Es wird ein zufälliges Passwort erzeugt und im Klartext in den Feldern '**New password**' und '**Confirm new password**' angezeigt.
4. '**How to notify**'. Bei der Voreinstellung teilen Sie dem betroffenen Anwender das neue Kennwort direkt z.B. am Telefon mit. Wählen Sie hingegen die Option '**By E-mail to manager**', können Sie eine Person angeben an die ein per Zufall generiertes Kennwort per eMail gesendet wird.
5. '**New password**'/'**Confirm new password**'. Eingabe und Bestätigung des selbst festgelegten Kennwortes.



### 3.5. Überwachung der Anwenderlizenzen – Lizenzverfolgung

Die Lizenzverfolgung ermöglicht die Überwachung der tatsächlich aktiv von Anwendern genutzten Lizenzen. Nach der Aktivierung der Lizenzverfolgung werden Verbindungen von Anwendern mit dem Domino Server erfasst und in der Datenbank '**Domino User License Tracking**' (USERLICENSES.NSF) gespeichert.

#### Aktivierung der Lizenzverfolgung



Öffnen Sie den Domino Administrator und wählen Sie das Register '**Configuration**'. Selektieren Sie links in der Navigation den Punkt '**Server**' -> '**Configuration**'.

Erstellen Sie ein neues oder öffnen Sie ein schon zuvor erstelltes Konfigurationsdokument. Aktivieren Sie auf dem Register '**Basics**' die Option '**License Tracking**'. Speichern und schließen Sie das Konfigurationsdokument.

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

Jeden Tag um 00:00 Uhr wird eine Anforderung an den Administrationsprozess generiert, welcher Informationen zu neuen Anwendern und zu Anwendern, welche seit 30 Tagen keinen Serverzugriff hatten, enthält. Diese Informationen werden durch den Administrationsprozess in Form von Dokumenten in der Datenbank USERLICENSES.NSF gespeichert.

Die Erstellung der Datenbank USERLICENSES.NSF wird durch den Administrationsprozess ausgeführt (nach eigenen Tests ca. 1/2 Stunde nach Mitternacht) und die Datenbank lediglich auf dem Administrationsserver erstellt - nicht auf weiteren Domino Servern.

Sobald die Datenbank USERLICENSES.NSF erstellt wurde, wird sie für einen einfachen Zugriff im Administrations-Client auf dem Register '**People & Groups**' angezeigt.

#### **Hinweis**

*Möglicherweise müssen Sie den Domino Administrator neu starten, damit die Datenbank bei Ihnen angezeigt wird.*

## 4. Mailrouting

### 4.1. Mehr Details zu gerouteten Mails in der Datenbank LOG.NSF

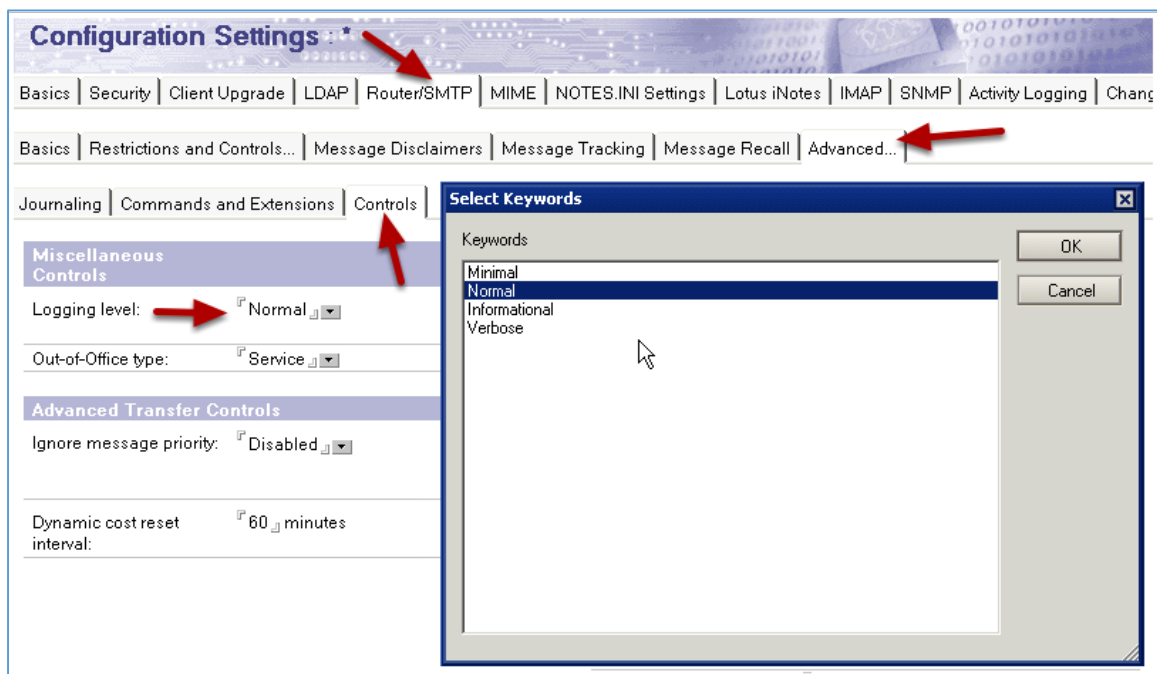
#### Vorgabe

Ohne eine entsprechende Konfiguration eines Domino Servers sind die auf der Konsole eines Domino Servers angezeigten und somit auch in der Datenbank LOG.NSF gespeicherten Informationen bzgl. einer transferierten eMail in der folgenden Form verfügbar.

14.12.2012 15:07:33 Router: Message 00584E36 delivered to Hans Berger/FirmaA

Sind weitere Details (z.B. Absender oder Größe der eMail) erwünscht, so kann dies in den Konfigurationsdokumenten der Domino Server festgelegt werden.

#### Einstellung der erfassten Information für geroutete eMails im Konfigurationsdokument



Öffnen Sie den Domino Administrator und wählen Sie das Register '**Configuration**'. Selektieren Sie links in der Navigaton den Punkt '**Server**' -> '**Configuration**'.

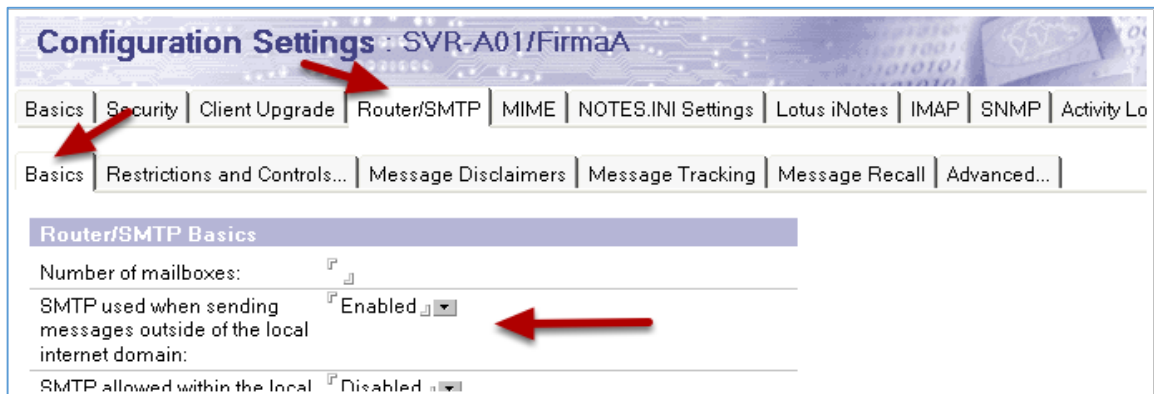
Öffnen Sie ein existierendes Konfigurationsdokument oder erstellen Sie ein neues Konfigurationsdokument.

Wählen Sie das Register '**Router/SMTP**' -> '**Advanced**' -> '**Controls**'. Im Feld '**Logging level**' finden Sie als Vorgabe die Auswahl '**Normal**', welche die oben gezeigten Details bei einer gerouteten eMail auf der Console und in der LOG.NSF generiert.

Bei Auswahl der Option '**Informational**' werden die folgenden Details erfasst - diese Stufe dürfte für die meisten Anforderungen ausreichend sein.

- 14.04.2012 18:22:46 Router: Message 00584E36 delivered to Hans Berger/FirmaA from AdminA01/FirmaA Size: 1K Time: 00:00:00 Hop Count: 1

## Ausgehende SMTP Nachrichten beim Einsatz eines Domino Servers



Die Konfiguration für ausgehende SMTP Nachrichten wird im Konfigurationsdokument des gewünschten Domino Servers vorgenommen.

Öffnen Sie den Domino Administrator und wählen das Register '**Configuration**'. Wählen Sie links in der Navigation den Punkt '**Server**' -> '**Configurations**'. Öffnen Sie ein bestehendes oder erstellen Sie für den gewünschten Server ein neues Konfigurationsdokument.

Wählen Sie das Register '**Router**' -> '**Basics**'. Stellen Sie die Option '**SMTP used when sending messages outside of the local internet domain**' auf '**Enabled**'.

Speichern und schließen Sie das Konfigurationsdokument.

### **Hinweis**

Wenn die Änderungen schnell wirksam werden sollen, verwenden Sie an der Domino Server Konsole den Befehl `TELL ROUTER UPDATE CONFIG`.

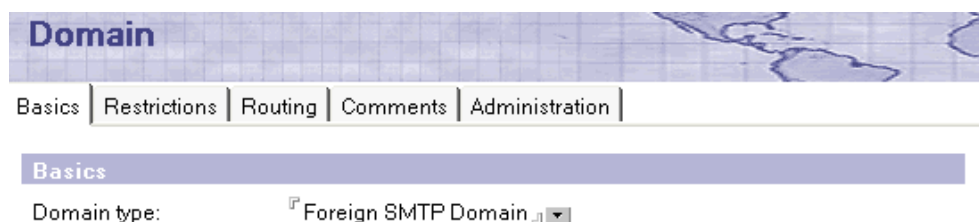
Wenn Sie nur einen Domino Server einsetzen, ist grundsätzlich keine weitere Konfiguration erforderlich. Falls in Ihrer Notes/Domino Umgebung jedoch mehrere Domino Server verwendet werden, führen Sie zusätzlich die folgenden Schritte aus.

## Ausgehende SMTP Nachrichten beim Einsatz mehrerer Domino Server

Sofern weitere Domino Server für das Mailrouting eingesetzt werden, müssen Sie noch folgende Dokumente erstellen.

### **Domänenendokument**

Bei dem ersten zusätzlich erforderlichen Dokument handelt es sich um ein Domänenendokument.



Öffnen Sie den Domino Administrator und wählen Sie das Register '**Configuration**'. Selektieren Sie links in der Navigation den Punkt '**Messaging**' -> '**Domains**'. Erstellen Sie durch die Aktionsschaltfläche '**Add Domain**' ein neues Domänenendokument.

## SMTP Verbindungsdokument

Um die Konfiguration abzuschließen, wird noch ein SMTP Verbindungsdokument benötigt.

Server Connection: SVR-A01/FirmaA to All-SMTP-Servers	
Basics   Replication/Routing   Schedule   Comments   Administration	
<b>Basics</b>	
Connection type: 1	SMTP
Source server: 2	SVR-A01/FirmaA
Source domain: 3	FirmaA
Connect via: 4	Direct connection
Destination server: 5	All-SMTP-Servers
Destination domain: 6	The-Internet
SMTP MTA relay host: 7	

Öffnen Sie den Domino Administrator und wählen Sie das Register **'Configuration'**. Selektieren Sie links in der Navigation den Punkt **'Server'** -> **'Connections'**. Erstellen Sie durch die Aktionsschaltfläche **'Add Connection'** ein neues Verbindungsdokument.

Auf dem Register **'Basic'** legen Sie die folgenden Einstellungen fest.

1. **'Connection Type'**. Legen Sie den Verbindungstyp auf **'SMTP'** fest.
2. **'Source Server'**. Welcher Domino Server routet die SMTP Mails? Ein Domino Server, welcher im Konfigurationsdokument das Routen von SMTP Mails außerhalb der eigenen Domäne aktiviert hat.
3. **'Source Domain'**. Die eigene Notes/Domino Domäne.
4. **'Connection via'**. Diese Einstellung ist bei Netzwerkverbindungen auf **'Direct connection'** eingestellt. Alternativ kann eine **'Dial-up connection'** (Wählverbindung) ausgewählt werden.
5. **'Destination server'**. Obgleich man ja nicht im Voraus weiß, an welche SMTP Mailserver Nachrichten gesendet werden, darf dieses Feld NICHT leer bleiben und kann mit einer frei wählbaren Zeichenkette (im Beispiel: All-SMTP-Servers) ausgefüllt werden.
6. **'Destination domain'**. Die virtuelle Domäne, welche im zuvor erstellten Domänendokument angegeben wurde.
7. **'SMTP MTA relay host'**. Falls der Domino Server (Feld **'Source server'**) Nachrichten bei einem Relay host "abliefern" soll, kann der Hostname oder die IP-Adresse in diesem Feld eingetragen werden.

Server Connection: SVR-A01/FirmaA to All-SMTP-Servers	
Basics   Replication/Routing   Schedule   Comments   Administration	
<b>Replication</b>	
Replication task:	Disabled
Replicate databases of:	Low & Medium & High priority
Replication type:	Pull Push
Files/Directory paths to replicate:	(all if none specified)
Files/Directory paths to NOT replicate:	
Replication time limit:	minutes
<b>Routing</b>	
Routing task:	SMTP Mail Routing
Route at once if:	1 messages pending
Routing cost:	1

Auf dem Register **'Replication/Routing'** wird lediglich im Feld **'Routing Task'** die Option **'SMTP Mail Routing'** festgelegt. Alle anderen Einstellungen verbleiben auf den Standardvorgaben.

### Hinweis

Lediglich die Replikation wurde im Feld **'Replication task'** deaktiviert, da es sich ja um ein Verbindungsdokument für Mailrouting-Einstellungen handelt.

Folgende Einstellungen stehen zur Verfügung.

1. **'Message Recall'**. Hier kann der Nachrichtenrückruf ein- oder ausgeschaltet werden.
2. **'Allow recall of messages with unread status'**. Hier kann festgelegt werden, ob nur ungelesene oder auch gelesene Nachrichten zurückgerufen werden dürfen.
3. **'Do not allow recall of messages older than'**. Hier wird festgelegt, dass nur Nachrichten mit einem maximalen Alter (in Minuten, Stunden, Tagen oder Wochen einstellbar) zurückgerufen werden dürfen.

Speichern und schließen Sie das Konfigurationsdokument.

### Hinweis

Jeder Anwender kann grundsätzlich durch die Vorgaben in seiner Maildatenbank selbst entscheiden, ob an ihn geschickte Nachrichten zurückgerufen werden dürfen.

### Einstellungen zum Nachrichtenrückruf durch Richtlinien

Durch ein Maileinstellungsdokument in Kombination mit einer Richtlinie können die Einstellungen im Konfigurationsdokument überschrieben werden.

Öffnen Sie den Administrations-Client und wählen Sie das Register **'People & Groups'**. Selektieren Sie links in der Navigation im Domino Verzeichnis den Punkt **'Settings'**. Öffnen Sie ein bestehendes Maileinstellungsdokument oder erstellen Sie ein neues durch die Aktionsschaltfläche **'Add settings...'** -> **'Mail'**.

Selektieren Sie im Maileinstellungsdokument das Register **'Mail'** -> **'Message Recall'**.

**Mail Settings - Mail Settings Standard**

Basics | Mail | Calendar and To Do | Access and Delegation | Lotus iNotes | Client Detection | Comments | Administration

Basics | Letterhead | Follow Up | Attention Indicators | Message Recall | Message Disclaimers

**Message Recall** How to apply this setting:

User is allowed to recall sent messages:	1 Yes	<input type="checkbox"/> Don't set value
Other users are allowed to recall messages they sent to this user:	2 Yes	Set value whenever modified
Allow recall of messages with unread status:	3 Unread only	<input type="checkbox"/> Don't set value
Do not allow recall of messages older than:	2 days 4	<input type="checkbox"/> Don't set value

Folgende Einstellungen stehen zur Verfügung.

1. Der Anwender, für den dieses Maileinstellungsdokument gilt, darf gesendete Nachrichten zurückrufen.
2. Andere Anwender dürfen Nachrichten zurückrufen, welche an den Anwender, für den dieses Maileinstellungsdokument gilt, gesendet wurden.
3. Dürfen nur ungelesene oder auch schon gelesene Nachrichten zurückgerufen werden?
4. Wie alt dürfen Nachrichten sein, damit sie noch zurückgerufen werden dürfen? Die Einstellung kann in Minuten, Stunden, Tagen und Wochen erfolgen.

### Fazit

Im Vergleich zur Nutzung eines Server Konfigurationsdokumentes (die dort gemachten Einstellungen gelten für alle Anwender, welche ihre Maildatenbank auf dem betroffenen Server gespeichert haben), können die Einstellungen bei der Nutzung eines Maileinstellungsdokumentes mit zugeordneter Richtlinie feiner und nur für bestimmte Anwender geltend eingestellt werden.

## 5. Notes/Domino Datenbanken (NSF-Dateien)

### 5.1. Einsatz einer aktuellen ODS (On Disk Structure)

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

Aktuell sind folgende ODS Varianten verfügbar:

- **ODS Version 52** = Notes 9.0.1 optionales Datenbank Format (erfordert den NOTES.INI Parameter CREATE\_R9\_DATABASES=1)
- **ODS Version 51** = Notes 8.5 optionales Datenbank Format (erfordert den NOTES.INI Parameter CREATE\_R85\_DATABASES=1)
- **ODS Version 48** = Notes 8 optionales Datenbank Format (erfordert den NOTES.INI Parameter CREATE\_R8\_DATABASES=1)
- **ODS Version 43** = Notes 8/8.5 Vorgabe Datenbank Format
- **ODS Version 43** = Notes 7
- **ODS Version 43** = Notes 6 Datenbank Format

Folgende Aspekte sind bei der Betrachtung der ODS wissenswert.

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

#### *Einsatz der ODS 52 auf einem Version 9.0.1 Domino Server*

Der Einsatz der ODS Version 52 auf einem Version 9.0.1 Domino Server bietet folgende Vorteile.

- Eine in seltenen Fällen aufgetretene Datenkorruption in Notes Datenbanken beim Einsatz von mittlerer oder hoher Verschlüsselung wird durch den Einsatz der ODS 52 verhindert.
- Ein Problem mit Dateianhängen größer 2 GByte wird behoben. Weitere Informationen hierzu liefert die IBM Technote #1648607:  
<http://www-01.ibm.com/support/docview.wss?rs=899&uid=swg21648607>

### *Ändern der ODS für ALLE Datenbanken*

Möchte man alle Datenbanken des Domino Servers komprimieren, so wird dies nicht gelingen, wenn der Domino Server während der Komprimierung läuft.

Der Grund hierfür ist, dass der Domino Server bestimmte Datenbanken (z.B. names.nsf, admin4.nsf, log.nsf usw.) im laufenden Betrieb andauernd im Lese-/Schreibmodus geöffnet hat und daher kein "Umkopieren" (Copystyle Compaction) durchführen kann.

Um diese Datenbanken dennoch auf die ODS 51 umzustellen, befolgen Sie die folgenden Schritte.

1. Beenden Sie den Domino Server.
2. Öffnen Sie eine Betriebssystem Kommando-Shell ("DOS Fenster").
3. Wechseln Sie in das Programmverzeichnis des Domino Servers, z.B. durch die Anweisung '**CD C:\Lotus\Domino**'.
4. Geben Sie den Befehl '**NCOMPACT.EXE -c**' ein.

Da der Domino Server nicht mehr läuft, können so ALLE NSF Dateien auf die neue ODS umgestellt werden.

### *Ändern der ODS für Schablonen (\*.NTF) und Mailboxen (\*.BOX)*

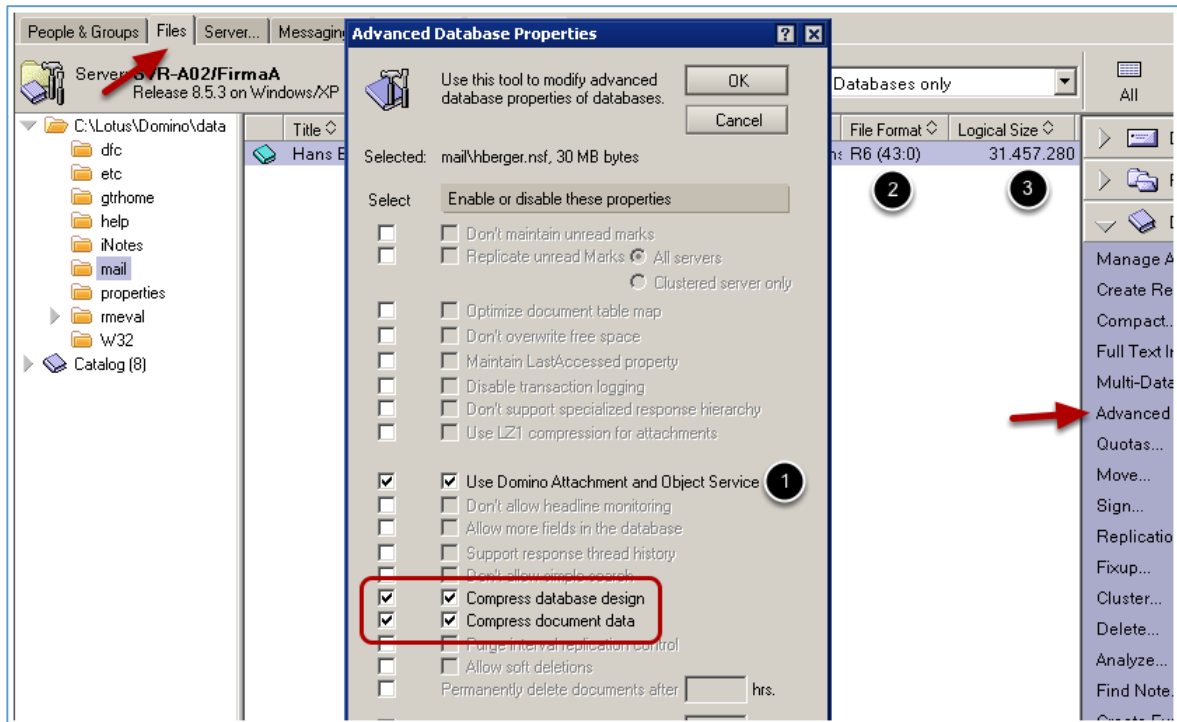
Ab Domino Server 9.0.1 wurde der COMPACT-Befehl um den Parameter

`_*`

*(Minus-Zeichen direkt gefolgt vom Stern)*

erweitert. Somit können nun auch alle Schablonen (\*.NTF) und Mailboxen (\*.BOX) auf die neue ODS-Version umgestellt werden.

Sofern Sie diese Datenbankeigenschaften für eine größere Anzahl von Datenbanken aktivieren möchten, verwenden Sie den Domino Administrator.



Öffnen Sie den Domino Administrator und wählen Sie das Register 'Files'. Markieren Sie eine oder mehrere Datenbanken und wählen Sie dann rechts in der Werkzeugleiste die Option 'Advanced Properties'.

Der im Screenshot gezeigte Dialog erlaubt es nun die gewünschten Datenbankeigenschaften festzulegen.

#### Hinweise

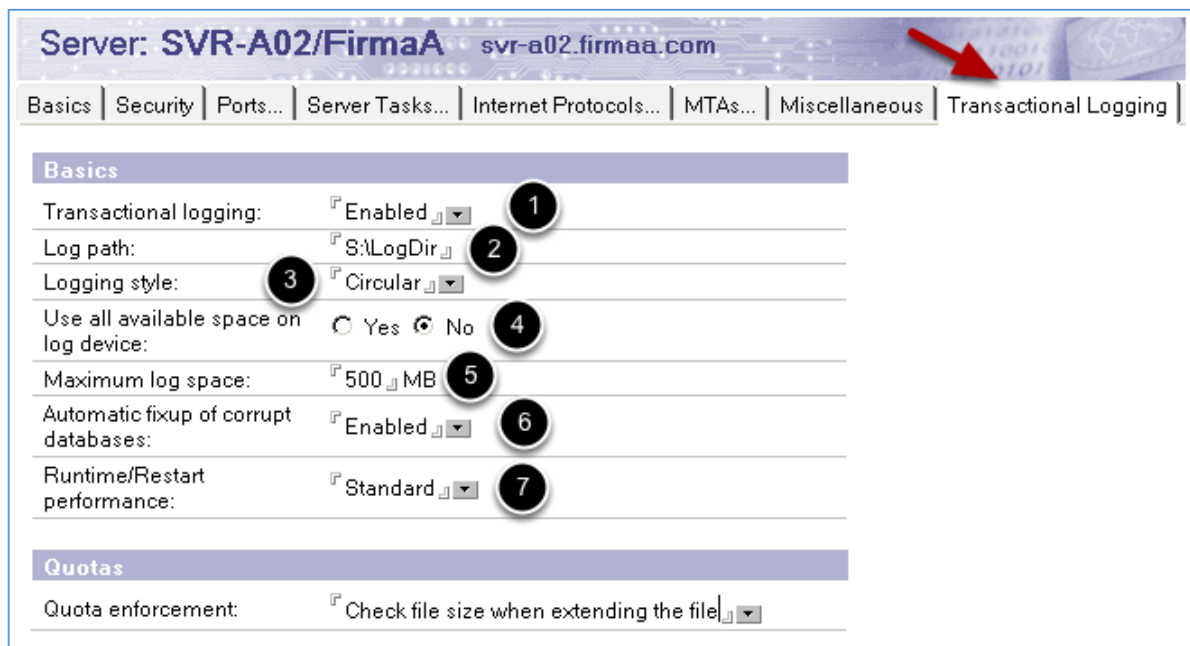
1. *Obgleich die ODS noch nicht aktualisiert wurde (siehe Punkt 2.), steht im Dialog schon die Option 'Use Domino Attachment and Object Service' zur Verfügung. DAOS kann natürlich erst dann für die Datenbank genutzt werden, wenn die ODS auf mindestens Version 51 aktualisiert wurde.*
2. *Die Datenbank hat zur Zeit noch ODS 43 (Notes/Domino Version 6).*
3. *Die Größe der im Beispiel verwendeten Datenbank (es handelt sich um eine nahezu leere Maildatenbank) beträgt ca. 31,5 MByte. Nach der Aktualisierung auf mindestens ODS 51 sollte dieser Wert erheblich kleiner sein.*

#### Größenänderung einer leeren Maildatenbank durch die Designkomprimierung

SVR-A02/FirmaA Release 8.5.3 on Windows/XP 5.1 Intel Pentium					
					Show me: Databases only
Server	Title	Filename	Physical Path	File Format	Logical Size
svr\Domino\data	Hans Berger	hberger.nsf	C:\Lotus\Domino\data\mail\hberger.nsf	R85 (51:0)	17.301.504

Nach der Umstellung auf mindestens ODS 51 reduziert sich die Größe der im Beispiel gezeigten Maildatenbank auf ca. 17,3 MByte - eine Ersparnis im Speicherplatzverbrauch von ca. 45%.



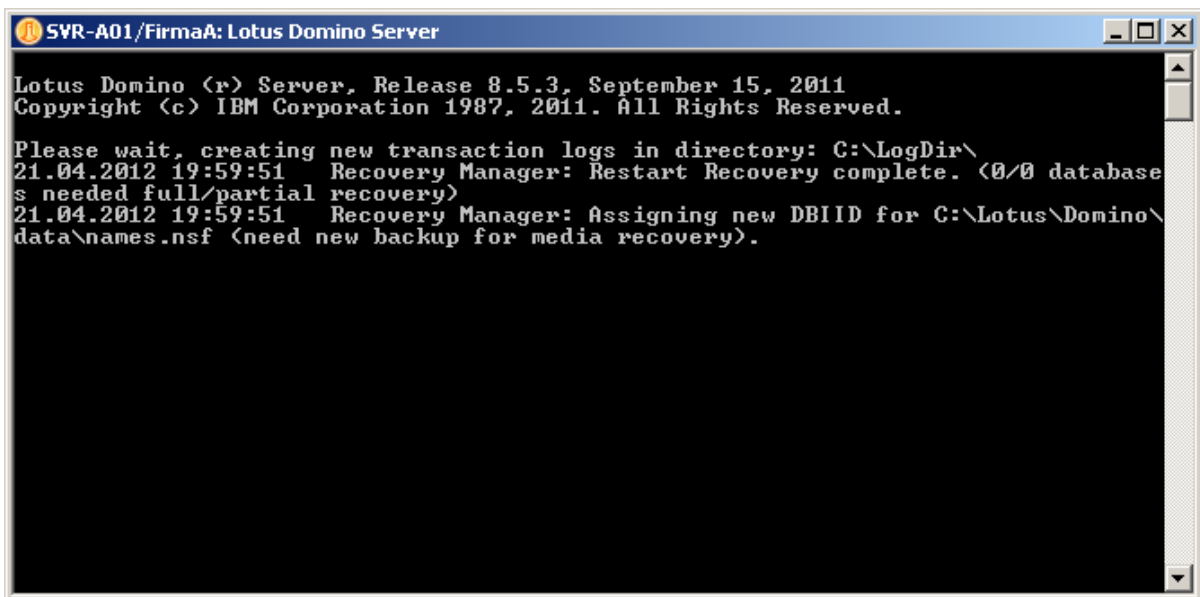


Öffnen Sie den Domino Administrator und wählen Sie das Register **'Configuration'**. Selektieren Sie links in der Navigation den Punkt **'Server' -> 'All Server Documents'**.

Öffnen Sie das gewünschte Serverdokument und wählen Sie das Register **'Transactional Logging'**. Die folgenden Optionen stehen zur Auswahl.

1. **'Transactional logging'**. Ein- oder Ausschalten der Transaktionsprotokollierung.
2. **'Log path'**. Wo soll das Transaktionslog gespeichert werden?
3. **'Logging stye'**. Auswahl der gewünschten Variante der Transaktionsprotokollierung - Details siehe weiter unten.
4. **'Use all available space on log device'**. Soll der gesamte Speicherplatz auf dem unter Punkt 2. angegebenen Laufwerk verwendet werden? Diese Option steht nicht beim Logging Style **'Archived'** zur Verfügung.
5. **'Maximum log space'**. Festlegung des max. zulässigen Speicherplatzes für das Transaktionslog in MByte. Diese Option steht nicht beim Logging Style **'Archived'** zur Verfügung.
6. **'Automatic fixup of corrupt databases'**. Wenn diese Option aktiviert (Vorgabe) ist, werden beschädigte Datenbanken einem automatischen Fixup unterzogen, wenn das Problem nicht durch die im Tra nsaktionslog gespeicherten Informationen behoben werden kann. Ist diese Option nicht aktiviert, muss der Konsolenbefehl **'LOAD FIXUP -J'** manuell ausgeführt werden.
7. **'Runtime/Restart performance'**. Der Domino Server schreibt regelmäßig sogenannte Wiederherstellungsprüfpunkteinträge (Checkpoints) in die Transaktionslog Dateien. Hierbei untersucht der Domino Server jede für die Transaktionsprotokollierung aktive Datenbank und ermittelt, wie viele Transaktionen erforderlich sind, um die Datenbank bei einem Systemfehler wiederherstellen zu können. Wird die Option **'Favor runtime'** gewählt, so werden weniger Wiederherstellungsprüfpunkteinträge geschrieben - der Domino Server arbeitet hierdurch schneller, aber die Wiederherstellung dauert länger. Die Option **'Favor restart recovery time'** schreibt mehr Wiederherstellungsprüfpunkteinträge, hierdurch ist eine schnellere Wiederherstellung möglich.

## Bedeutung der Datenbank Instanz-ID (DBIID)



```
SVR-A01/FirmaA: Lotus Domino Server
Lotus Domino (r) Server, Release 8.5.3, September 15, 2011
Copyright (c) IBM Corporation 1987, 2011. All Rights Reserved.

Please wait, creating new transaction logs in directory: C:\LogDir\
21.04.2012 19:59:51 Recovery Manager: Restart Recovery complete. (0/0 database
s needed full/partial recovery)
21.04.2012 19:59:51 Recovery Manager: Assigning new DBIID for C:\Lotus\Domino\
data\names.nsf (need new backup for media recovery).
```

Sobald der Domino Server nach der Aktivierung der Transaktionsprotokollierung neu gestartet wurde, erscheinen die im Screenshot gezeigten Meldungen an der Domino Konsole.

**Please wait, creating new transaction logs in directory: C:\LogDir\**

Im Beispiel werden die Transaktionslog Dateien im angegebenen Pfad erstellt.

**Recovery Manager: Assigning new DBIID for C:\Lotus\Domino\data\names.nsf (need new backup for media recovery)**

Der Domino Server vergibt der Datenbank NAMES.NSF eine neue Datenbank Instanz-ID.

Bei der Datenbank Instanz-ID handelt es sich um eine eindeutige Kennung für jede auf einem bestimmten Domino Server gespeicherte Datenbank. Diese eindeutige Kennung ist erforderlich, damit die im Transaktionslog gespeicherten Informationen eindeutig ihrer "Quelle" zugeordnet werden können.

### **Hinweis**

*Die Replik-ID einer Notes Datenbank wäre nicht eindeutig, weil man eine bestimmte Datenbank z.B. mehrfach als Replik in verschiedenen Verzeichnissen auf dem Domino Server ablegen kann.*

Sobald die Datenbank Instanz-ID vergeben wird, weist die Meldung '**need new backup for media recovery**' darauf hin, dass ein Vollbackup der Datenbank erstellt werden muss. Dies ist erforderlich, weil eine Wiederherstellung einer Datenbank nur möglich ist, wenn das letzte vollständige Backup und die im Transaktionslog gespeicherten Änderungen mit eindeutiger Beziehung zur Datenbank verfügbar sind.

### Hinweis

Stellen Sie zunächst sicher, dass Transaktionsprotokollierung aktiviert wurde und dass die Datenbanken auf mindestens ODS 51 konvertiert wurden.

Öffnen Sie den Domino Administrator und wählen Sie das Register '**Configuration**'. Selektieren Sie links in der Navigation den Punkt '**Server**' -> '**All Server Documents**'. Öffnen Sie das gewünschte Serverdokument und selektieren Sie das Register '**DAOS**'.

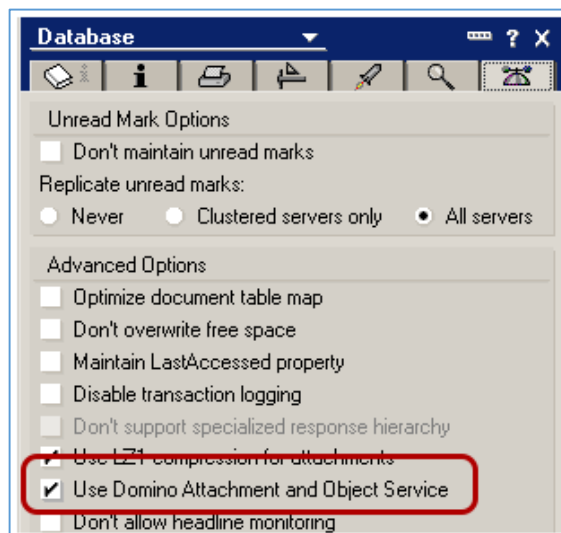
Folgende Einstellmöglichkeiten stehen zur Verfügung.

1. '**Store file attachments in DAOS**'. DAOS ein- oder ausschalten.
2. '**Minimum size of object before Domino will store in DAOS**'. Nur Dateien, welche über die hier angegebene Mindestgröße in Bytes verfügen, werden ausgelagert. Wegen dem erforderlichen Verwaltungsaufwand macht es keinen Sinn, z.B. ein kleines GIF-Bild mit einer Größe von 159 Byte auszulagern.
3. '**DAOS base path**'. Wo sollen die ausgelagerten Dateianhänge gespeichert werden? Die Speicherung sollte auf einem performanten und redundant ausgelegten Speichermedium erfolgen.
4. '**Defer object deletion for**'. Wenn es für eine im DAOS Pfad gespeicherte Datei (also einen bestimmten Anhang) keine Referenzen mehr in den Datenbanken gibt (die entsprechenden Dokumente wurden bereits alle gelöscht), so kann auch die NLO-Datei gelöscht werden. Dies erfolgt mit der hier angegebenen Verzögerung, angegeben in Tagen.

Speichern und schließen Sie das Serverdokument.

Starten Sie abschließend den Domino Server neu. Hierbei wird der **DAOS Verwaltungstask** (DAOSMGR) gestartet und die **DAOS Verwaltungsdatenbank** (DAOSCAT.NSF) erstellt.

### DAOS für gewünschte Datenbanken aktivieren



Um DAOS für eine einzelne Datenbank zu aktivieren, öffnen Sie den Dialog zur Anzeige der Datenbankeigenschaften (die gewünschte Datenbank öffnen -> Menü '**File**' -> '**Application**' -> '**Properties**') und wählen Sie das Register '**Advanced**'.

Aktivieren Sie die Option '**Use Domino Attachment and Object Service**'.

Im Beispiel ist schon eine deutliche Reduzierung des von der Datenbank selbst beanspruchten Speicherplatzes zu erkennen. Der Dateianhang selbst wurde hierbei nur 1 x als NLO-Datei im DAOS Pfad gespeichert.

### DAOS NLO Dateien

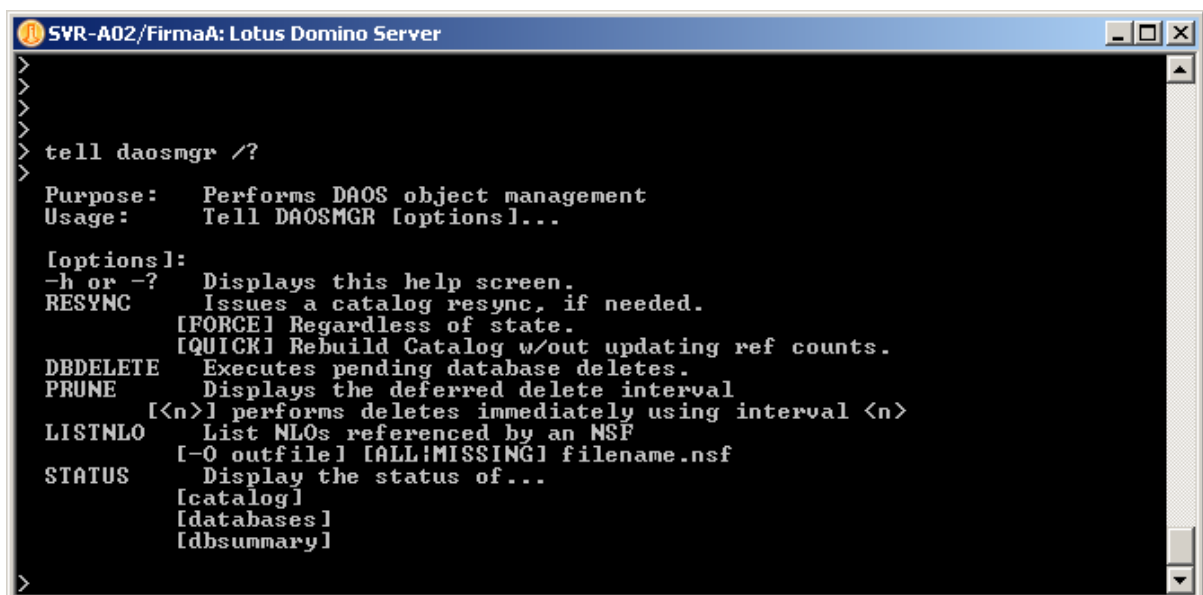


Ausgelagerte Dateianhänge werden im angegebenen DAOS Pfad als Dateien mit der Endung NLO (Notes Large Object) gespeichert und sind grundsätzlich mit der ID-Datei des Domino Servers verschlüsselt.

Im Screenshot sehen Sie die Entwickler Hilfedatenbank aus dem obigen Beispiel.

1. **DAOS Pfad.** Unterhalb des im Serverdokument angegebenen DAOS Pfad werden fortlaufend nummerierte Unterverzeichnisse (0001, 0002 usw.) angelegt und darin die NLO Dateien gespeichert.
2. **NLO Dateien.** Die Dateianhänge werden im DAOS Pfad als Dateien mit der Endung NLO (Notes Large Object) gespeichert und grundsätzlich mit der ID-Datei des Domino Servers verschlüsselt.
3. **Größe der NLO Dateien.** Die als NLO-Datei abgelegten Dateianhänge werden komprimiert, sofern die Komprimierung beim Erstellen des Dateianhangs im Notes Client aktiviert (Vorgabe) war. Im Screenshot handelt es sich um die gleiche Datei (HELP85\_DESIGNER.NSF), einmal mit und einmal ohne Komprimierung des Anhangs.

### DAOS Konsolenbefehle



### Server Mailboxen (mail.box, mail1.box usw.)

Wenn eine eMail mit Anhängen an mehrere Empfänger mit Maildatenbanken auf dem gleichen Domino Server gesendet wird, kann das Routing optimiert werden, wenn die Dateianhänge schon in der/den Mailbox(en) des Server aus der eMail gelöst und als NLO Datei gespeichert werden.

Der Domino Server muss dann nur noch die wesentlich kleineren eMails ohne die Dateianhänge in den Maildatenbanken der Empfänger speichern. Daher sollte DAOS für alle Server Mailboxen aktiviert werden.

### DAOS Estimator

IBM bietet kostenfrei den DAOS Estimator zum Herunterladen von den IBM Webseiten an (einfach per Google nach "DAOS Estimator" suchen). Es handelt sich um ein kleines Kommandozeilen-Tool, welches keine Installation erfordert und einfach in das Programmverzeichnis des Domino Servers kopiert wird.

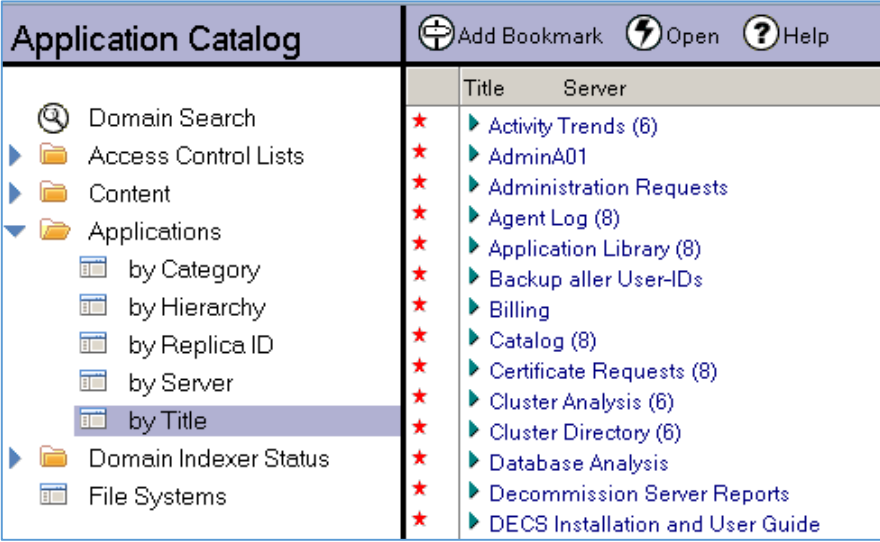
Wenn man dann z.B. auf dem Windows Server die Datei DAOSEST.EXE von einer Betriebssystemkonsole aus startet, erhält man nach der Analyse diverse Kennwerte, u.a. auch eine Aussage, wie viel Speicherplatz man durch den Einsatz von DAOS einsparen kann.

## 5.5. Domänenkatalog und Domänensuche

Die Domänensuche ermöglicht es, mit einer einzigen Suchanfrage eine Volltextsuche über eine beliebige Anzahl von Notes Datenbanken, Anhängen und sonstigen Dateien auszuführen. Diese Suche ist nicht auf einen einzigen Domino Server begrenzt, sondern kann über alle Domino Server einer Domäne erfolgen.

Die Voraussetzung für die Nutzung ist mindestens ein Domino Server, der den Domänensuchindex aufbaut und die Suchanfragen entgegen nimmt. Zur Verwaltung und Steuerung wird der sogenannte Domänenkatalog, eine auf der Datenbankschablone CATALOG.NTF basierende Notes Datenbank, eingesetzt.

### Die Datenbank CATALOG.NSF

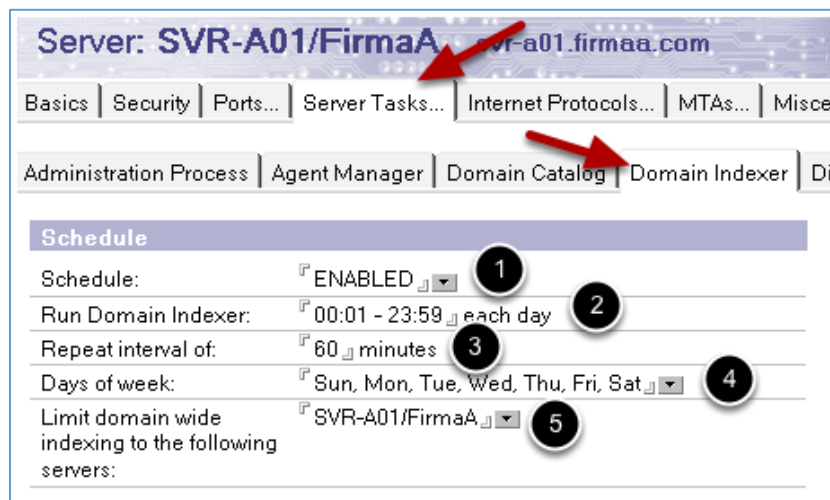


Application Catalog		Add Bookmark	Open	Help
	Title	Server		
Domain Search	★	▶ Activity Trends (6)		
Access Control Lists	★	▶ AdminA01		
Content	★	▶ Administration Requests		
Applications	★	▶ Agent Log (8)		
by Category	★	▶ Application Library (8)		
by Hierarchy	★	▶ Backup aller User-IDs		
by Replica ID	★	▶ Billing		
by Server	★	▶ Catalog (8)		
by Title	★	▶ Certificate Requests (8)		
Domain Indexer Status	★	▶ Cluster Analysis (6)		
File Systems	★	▶ Cluster Directory (6)		
	★	▶ Database Analysis		
	★	▶ Decommission Server Reports		
	★	▶ DECS Installation and User Guide		

Die Datenbank CATALOG.NSF als Basis für die Domänensuche existiert grundsätzlich auf jedem Domino Server. Entsprechend eines Eintrags in der Datei NOTES.INI des Domino Servers wird diese Datenbank nachts um 01:00 Uhr aktualisiert oder falls sie noch nicht vorhanden ist, auf Basis der Datenbankschablone CATALOG.NTF erstellt.

### ServerTasksAt1=Catalog

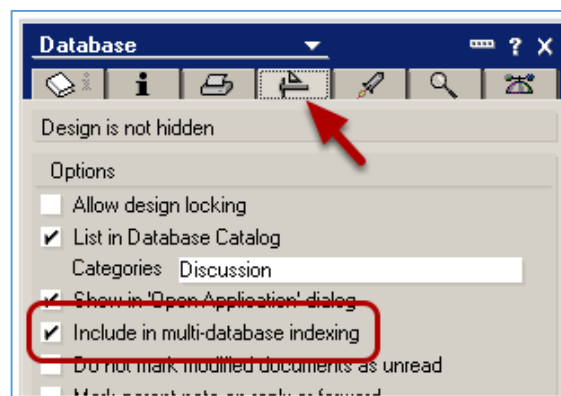
Wechseln Sie nun auf das Register 'Server Tasks...' -> 'Domain Indexer'.



Der für die Volltextsuche erforderliche Index wird durch einen eigenen Servertask, den Domänen Indexer, gebildet. Es lassen sich die folgenden Optionen festlegen.

1. **'Schedule'**. Diese Option legt fest, ob der Domänen Indexer auf diesem Domino Server aktiv ist.
2. **'Run Domain Indexer'**. Innerhalb welcher Zeitspanne ist der Domänen Indexer aktiv?
3. **'Repeat interval of'**. Wie oft läuft der Domänen Indexer? Vorgabe: 60 Minuten.
4. **'Days of week'**. An welchen Wochentagen ist der Domänen Indexer aktiv?
5. **'Limit domain wide indexing to the following servers'**. Bleibt das Feld leer, so können alle Datenbanken mit aktivierter Option zur Aufnahme in die Domänensuche in den Suchindex aufgenommen werden. Sobald Domino Server eingetragen werden, ist die Indizierung auf die angegebenen Server beschränkt.

#### Aktivierung der Domänensuche für die gewünschten Datenbanken



Für eine einzelne Datenbank können Sie die Domänensuche wie folgt aktivieren. Öffnen Sie die gewünschte Datenbank. Wählen Sie den Menüpunkt 'File' -> 'Application' -> 'Properties' und selektieren Sie das Register 'Design' im Dialog zur Festlegung der Datenbankeigenschaften.

### Hinweis

Bei dem für die Erstellung dieser Schulungsunterlage verwendeten Domino Server Version 8.5.3 zeigte sich ein Verhalten, welches vom Autor in der Vergangenheit bei verschiedenen Domino Versionen beobachtet wurde - der Domänensuchindex wurde nach der Aktivierung zwar für Datenbanken wie die im Screenshot gezeigte `HELP85_IWA_EN.NSF` erstellt, aber nicht für selbst ausgewählte Datenbanken.

Sollte das auf Ihrem Domino Server ebenfalls passieren, befolgen Sie die Angaben im nächsten Abschnitt.

### Aufnahme von eigenen Datenbanken in den Domänensuchindex - Problemlösung

Es mag weitere Ansätze zur Lösung des oben beschriebenen Problems geben. Folgende Vorgehensweise hat beim Autor in der Vergangenheit mit unterschiedlichsten Domino Versionen funktioniert. Bei der Lösung geht es im Grunde lediglich darum, die bestehende Datenbank `CATALOG.NSF` durch eine neue zu ersetzen.

Die Datenbank `CATALOG.NSF` lässt sich nicht im laufenden Betrieb des Domino Server löschen - auch nicht beim Einsatz von ggf. sonst nützlichen Tricks (z.B. Konsolenbefehl `'DBCACHE FLUSH'`). Daher sind folgende Schritte erforderlich.

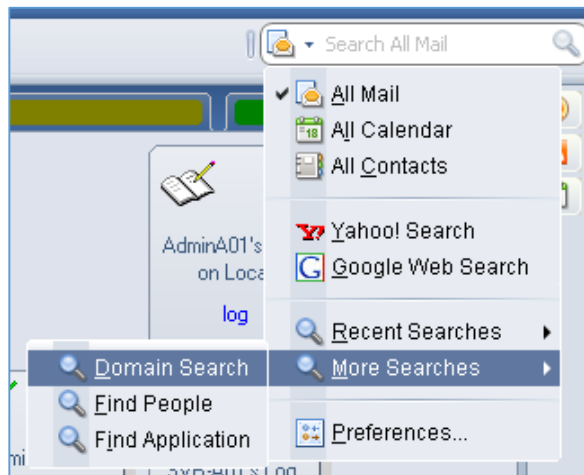
1. Beenden Sie den Domino Server.
2. Löschen Sie die Datenbank `CATALOG.NSF` über das Dateisystem (z.B. Windows Explorer).
3. Starten Sie den Domino Server erneut. Da die Datenbank `CATALOG.NSF` fehlt, wird der Domänen Indexer Task NICHT geladen.
4. Sobald der Domino Server gestartet ist, geben Sie den Konsolenbefehl **'LOAD CATALOG'** ein. Hierdurch wird eine neue Datenbank `CATALOG.NSF` erstellt. Die Datenbank erhält die gleiche Replik-ID wie zuvor - alle `CATALOG.NSF` Datenbanken auf allen Domino Servern der Domäne haben immer die gleiche Replik-ID (sogenannte Wildcard-Repliken).
5. Da der Domänen Indexer Task noch nicht läuft (und dieser auch im Moment nicht mittels Konsolenbefehl **'LOAD DOMIDX'** gestartet werden kann), ist ein weiterer Neustart des Domino Servers erforderlich.
6. Führen Sie einen weiteren Neustart der Domino Servers durch. Da nun die Datenbank `CATALOG.NSF` existiert, wird auch beim Hochfahren des Domino Servers der Domänen Indexer Task geladen. Entsprechend des eingestellten Zeittaktes wird der Domänen Indexer Task nun auch die selbst gewählten Datenbanken indizieren.

Sie werden sich ggf. fragen, warum das nun mit der neu erstellen Datenbank `CATALOG.NSF` funktioniert. Eine exakte, technisch nachvollziehbare Aussage ist dem Autor nicht bekannt, allerdings scheint die Datenbank `CATALOG.NSF` intern "irgendwie" anders zu sein, wenn Sie bei im Serverdokument aktivierter Domänensuche neu erstellt wird. Zumindest ist der Titel der Datenbank plötzlich ein anderer.



1. Titel **'Calalog (8)'**. Diese Datenbank wurde vom Domino Server entsprechend der Anweisung in der `NOTES.INI` vor der Aktivierung erstellt.
2. Titel **'Domain Catalog'**. Das ist der Titel der Datenbank, welche durch die oben genannten Schritte neu erstellt wurde.

## Durchführen einer Domänensuche



Im Notes Client ab Version 8 befindet sich oben rechts ein permanent verfügbares Eingabefeld um Suchläufe zu starten. Wenn Sie hier auf den kleinen, nach unten gerichteten schwarzen Pfeil klicken, erscheinen die im Screenshot gezeigten Auswahlmöglichkeiten.

Selektieren Sie den Punkt **'More Searches' -> 'Domain Search'**. Es erscheint die **'Domain Search Form'**.

A screenshot of the 'Domain Search Form' interface. It features a search input field containing the text 'Hausmesse'. Below the input field, there are radio buttons for 'documents' (selected) and 'applications'. A 'Search' button with a magnifying glass icon and a 'Reset' button with a circular arrow icon are positioned to the right. Below these, there are radio buttons for 'Terse results' and 'Detailed results' (selected), and a 'Sort by:' dropdown menu set to 'relevance'. A red arrow points to the 'Detailed results' radio button. A 'More' button is located at the bottom left of the form.

Geben Sie den gewünschten Suchbegriff im Feld **'Containing'** ein. Wenn Sie die Option **'Detailed results'** aktivieren, erhalten Sie in den Suchergebnissen zusätzlich auch die Information, aus welcher Datenbank ein gefundenes Dokument stammt. Klicken Sie auf den Link **'Search'**.

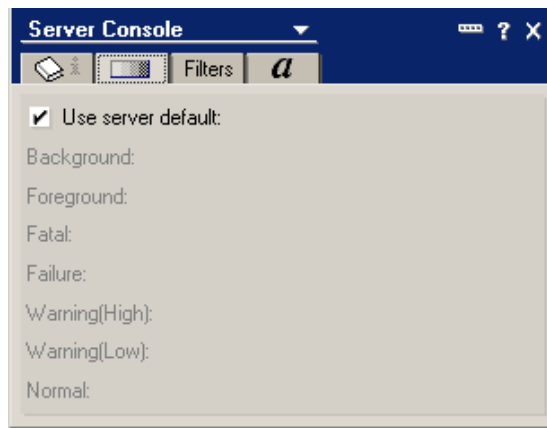
A screenshot of the 'Domain Search Results' page. It shows the search query '(Hausmesse)' and two results. The results are displayed in a table with columns for Relevance, Type, Date, Title, and (Author). The first result is 'Veranstaltungen 2012 in (Diskussion)' from 'AdminA01/FirmaA' dated 04.06.2012. The second result is 'Neuer Laserpointer XV35 S in (Produktkatalog)' from 'AdminA01/FirmaA' dated 23.04.2012. The titles are highlighted in blue, indicating they are active links. Navigation buttons for 'Previous', 'Next', and 'Help' are visible at the top and bottom of the results area.

Relevance	Type	Date	Title	(Author)
	📄	04.06.2012	<a href="#">Veranstaltungen 2012</a> in (Diskussion)	(AdminA01/FirmaA)
	📄	23.04.2012	<a href="#">Neuer Laserpointer XV35 S</a> in (Produktkatalog)	(AdminA01/FirmaA)

So werden die Suchergebnisse angezeigt. Der blau angezeigte Titel des Dokumentes ist ein aktiver Link und zeigt nach einem Klick das zugeordnete Dokument am Bildschirm an.



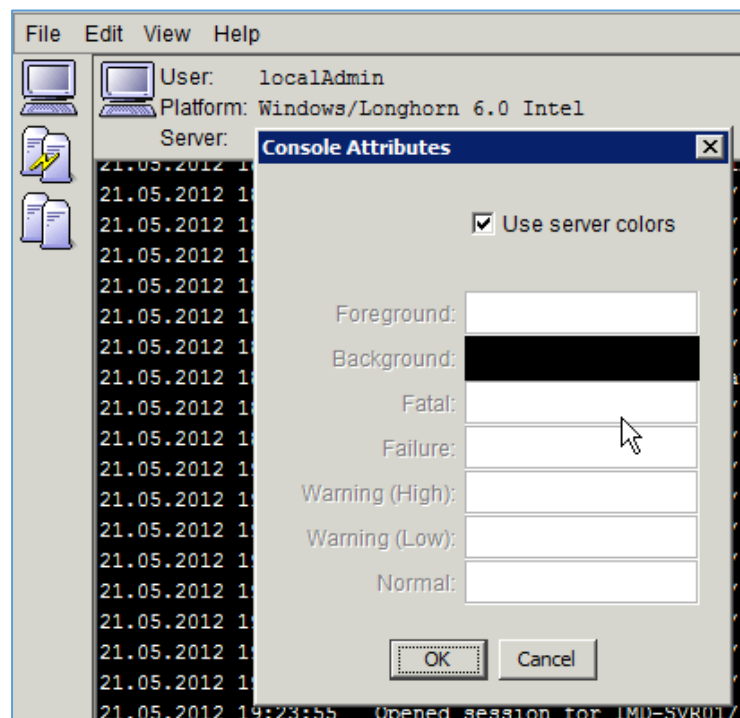
## Console im Domino Administrator



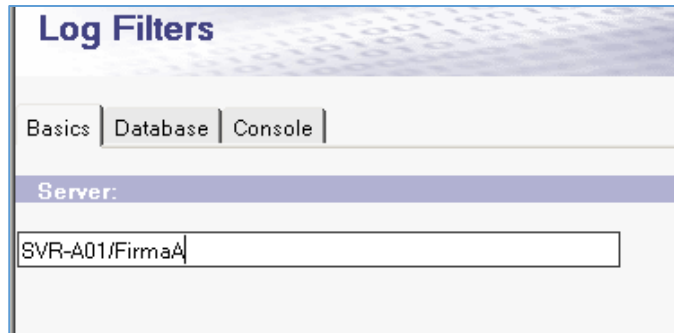
Obgleich die in der Datenbank EVENTS4.NSF eingestellten Farben auch für die im Domino Administrator verfügbare Remote-Console gelten, können die Farben hier trotzdem individuell eingestellt werden.

Öffnen Sie den Domino Administrator und wählen Sie das Register **'Server'** und das Unterregister **'Status'**. Wählen Sie links in der Navigation den Punkt **'Server Console'**. Durch einen Rechtsklick in das Konsolenfenster wählen Sie im Popup-Menü die Option **'Console Properties'**. Sie können nun die gewünschten Farben (siehe Screenshot) festlegen.

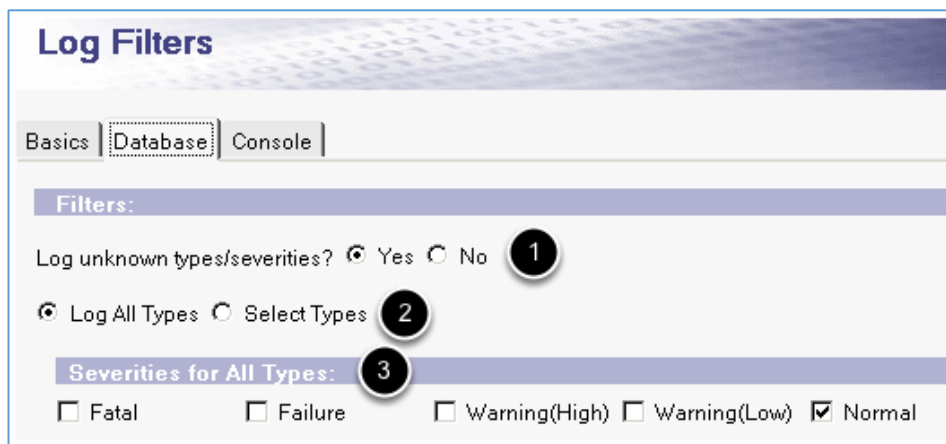
## Lotus Domino Console



Auch die seit Notes/Domino 6 verfügbare Lotus Domino Console verwendet grundsätzlich die in der Datenbank EVENTS4.NSF eingestellten Farben. Möchten Sie hier individuelle Farben verwenden, so wählen Sie den Menüpunkt **'Edit'** -> **'Console Attributes'**. Sie können nun die gewünschten Farben (siehe Screenshot) festlegen.

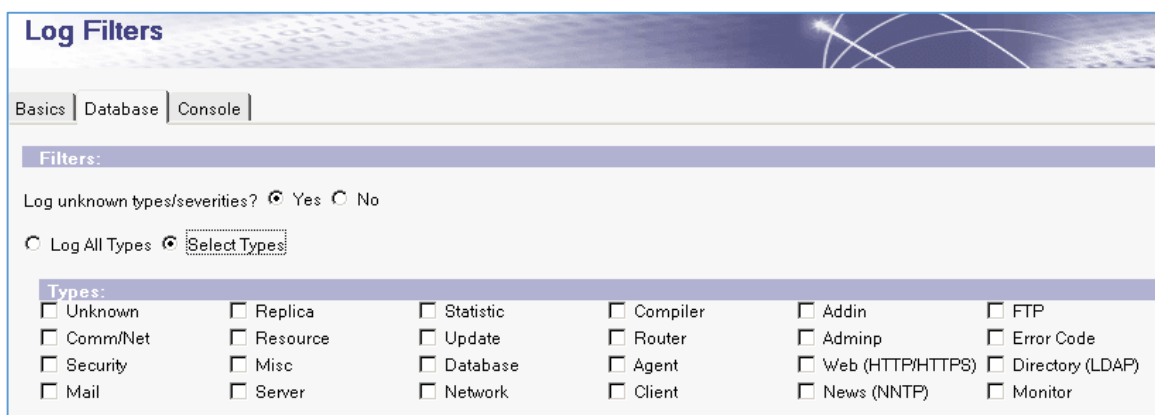


Auf diesem Register geben Sie den Domino Server an, für den der LOG Filter gelten soll.



Auf dem Register '**Database**' legen Sie die folgenden Optionen für die in der Datenbank LOG.NSF gespeicherten Informationen fest:

1. '**Log unknown types/severities?**'. Diese Option bestimmt, ob auch unbekannte Ereignistypen oder Warnstufen (diese könnten z.B. durch ein Server-Addin eines Drittanbieters generiert werden) erfasst werden sollen.
2. '**Log All Types**'. Ist diese Option aktiviert, können Sie die unter Punkt 3 gezeigten Warnstufen auswählen.
3. '**Severities for All Types**'. Sofern die Option '**Log All Types**' aktiviert wurde, stehen die im Screenshot gezeigten Warnstufen zur Auswahl.



Sofern Sie die Option '**Select Types**' aktiviert haben, stehen die im Screenshot gezeigten Ereignistypen zur Auswahl.

Angefangen hatte die Statistik- und Ereignisüberwachung ehemals mit den beim Domino Server im laufenden Betrieb gesammelten Statistikwerten. *Was bedeutet das?*

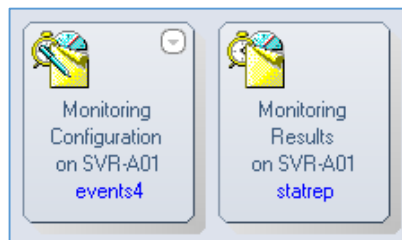
Sobald ein Domino Server gestartet wird, bildet er im Speicher eine Liste mit Kenngrößen (Statistikwerten) aus den unterschiedlichsten Bereichen. Hierbei handelt es sich z.B. um den verfügbaren Festplattenspeicherplatz, um die Anzahl der Deadmails oder die Anzahl der gerouteten Mails. Sie können sich die Liste der verfügbaren Statistikwerte durch den Befehl

SHOW STAT

an der Domino Server Konsole anzeigen lassen. Im Screenshot ist zu erkennen dass im Beispiel 747 einzelne Statistikwerte zur Verfügung stehen - diese Zahl hängt von der Konfiguration des einzelnen Domino Servers ab.

Da der Domino Server diese Werte nach einem Neustart neu erfasst, war die damals erste verfügbare Funktion das "Einsammeln und Speichern" der Statistikwerte in einer Notes Datenbank.

*Speichern der Statistikwerte in der Datenbank 'Monitoring Results' (STATREP.NSF)*



Obleich die Datenbank zur Speicherung der Statistikwerte zwischenzeitlich den Titel '**Monitoring Results**' trägt, lautet der Dateiname doch immer noch STATREP.NSF (**Statistik Reports**). In dieser Datenbank werden die Statistikwerte in einem einstellbaren Zeittakt gespeichert. Die Aktivierung der Speicherung und die Festlegung des Zeittaktes erfolgt in der Datenbank '**Monitoring Configuration**' (EVENTS4.NSF).

#### **Hinweis**

*Sobald man die beiden Datenbanken im Arbeitsbereich geöffnet hat (siehe Screenshot), erkennt man die enge Beziehung der beiden schon am Datenbanksymbol - es unterscheidet sich lediglich durch den zusätzlich verfügbaren Stift bei der Datenbank EVENTS4.NSF - diesen Unterschied kann man durchaus so interpretieren, dass in der Datenbank EVENTS4.NSF eingestellt wird, welche Werte in der Datenbank STATREP.NSF gespeichert werden.*

Die beiden Datenbanken sind auch im Domino Administrator verfügbar.

- '**Monitoring Configuration**'. Öffnen Sie den Domino Administrator und wählen Sie das Register '**Configuration**'. Selektieren Sie links in der Navigation den Punkt '**Monitoring Configuration**'. Es stehen dort weitere Ansichten zur Auswahl zur Verfügung.
- '**Monitoring Results**'. Öffnen Sie den Domino Administrator und wählen Sie das Register '**Server**' -> '**Analysis**'. Selektieren Sie links in der Navigation den Punkt '**Monitoring Results**'. Auch hier stehen weitere Ansichten zur Auswahl zur Verfügung.

#### **Hinweis**

*Die Datenbank STATREP.NSF ist nicht automatisch verfügbar und wird daher im Domino Administrator möglicherweise noch nicht angezeigt. Erst wenn der erforderliche Servertask gestartet wurde, wird die Datenbank erstellt.*

Für jeden Server, auf dem der COLLECT Task gestartet wurde, sollte schon ein entsprechendes Dokument existieren. Öffnen Sie das gewünschte Dokument mit einem Doppelklick.

**Server Statistic Collection**

Created: 26.03.2012

Basics | Options

**Collecting server** 1

Server:  
SVR-A01/FirmaA

**Collect from** 2

All servers in this domain  
 All servers that are not explicitly listed to be collected  
 From the following servers:

Server(s):  
SVR-A01/FirmaA

#### Register 'Basics'

1. **'Collecting server'**. Welcher Domino Server sammelt die Statistikwerte ein und speichert sie in der Datenbank STATREP.NSF?
2. **'Collect from'**. Von welchen Servern sollen die Statistikwerte eingesammelt werden? Dies kann von allen Domino Servern der Domäne (der COLLECT Task muss dort nicht gestartet sein) oder von bestimmten Domino Servern erfolgen.

**Server Statistic Collection**

Created: 26.03.2012

Basics | Options

Log statistics to a database

1 Database to receive reports (file name): statrep.nsf

2 Collection report interval: 120 minutes

3 Collection alarm interval: 30 minutes

4 Statistic Filters:

- Adminp
- Agent
- Calender
- Comm
- DAOS
- Database
- DECS
- Disk
- FT
- HTTP
- ICM

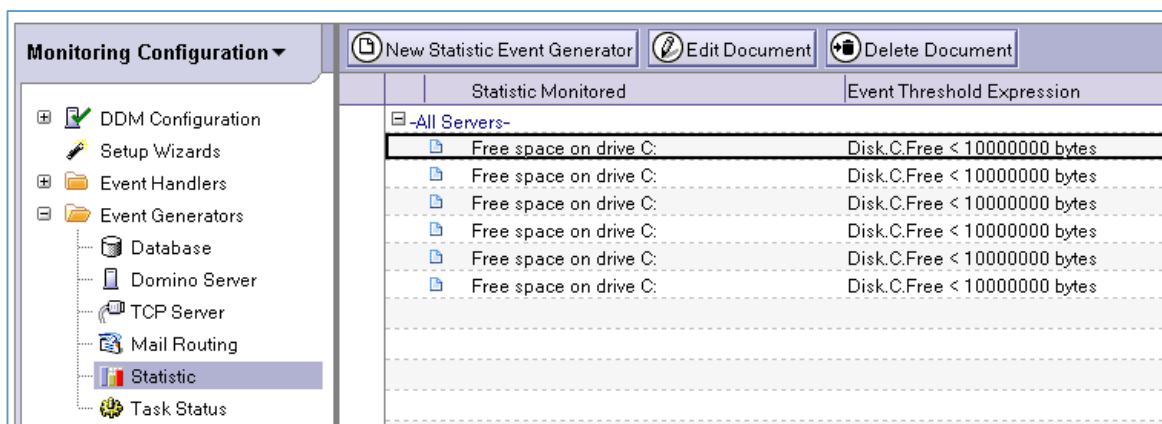
### Hinweis

Möglicherweise ist die unter dem Navigationspunkt **'Advanced'** verfügbare Ansicht **'Spreadsheet Export'** von Interesse. Die Ansicht ist so konzipiert, dass sich die für die Dokumente angezeigten Informationen in der Ansicht für den Export in eine Tabellenkalkulationsanwendung eignen.

Die in den Statistikreport-Dokumenten festgehaltenen Informationen liefern somit die Veränderung von Statistikwerten über längere Zeiträume. Bei den z.B. in der Ansicht **'System'** angezeigten Informationen wie dem verfügbaren Speicherplatz auf den Festplatten, wäre es wünschenswert, wenn man beim Über- oder Unterschreiten von selbst definierten Grenzwerten darauf hingewiesen würde.

Diese Funktionalität existiert in Form von sogenannten Alarmdokumenten und führt uns zum nächsten Abschnitt.

### Überwachung von selbst definierten Grenzwerten durch Alarmdokumente



Kein Notes/Domino Administrator hat im "Tagesgeschäft" die Zeit, die für seine Umgebung relevanten Statistikwerte fortlaufend durch das Betrachten der in der Datenbank STATREP.NSF gespeicherten Dokumente zu überwachen. Daher gibt es die Möglichkeit selbst Grenzwerte zu definieren um bei der Über- bzw. Unterschreitung darüber in Form von Alarmdokumenten informiert zu werden.

Öffnen Sie die Datenbank EVENTS4.NSF und selektieren Sie links in der Navigation unter dem Punkt **'Event Generators'** die Ansicht **'Statistic'**. Wie im Screenshot zu sehen, könnten bei Ihnen ebenfalls schon **'Event Generator'** Dokumente existieren.

### Hinweis

Wundern Sie sich bitte nicht, wenn auch bei Ihnen (wie im Screenshot zu sehen) mehrere gleiche Dokumente existieren. Sie können entweder alle oder die überzähligen Dokumente löschen und danach eigene, für Ihre Umgebung passende Dokumente erstellen.

Erstellen Sie durch die Aktionsschaltfläche **'New Statistic Event Generator'** ein neues Dokument.

**Statistic Event Generator**

Event Number: AAAA-8UKN6K

Basics | **Threshold** | Other

**Threshold**

Generate the event when:

The statistic is LESS THAN the threshold value

The statistic is GREATER THAN the threshold value

The statistic is a MULTIPLE of the threshold value

Threshold:  bytes

### Register 'Threshold'

Auf diesem Register kann der Grenzwert, welcher die Erstellung des Alarmdokumentes auslöst, festgelegt werden. Hierbei steht zur Auswahl, ob ein kleinerer oder ein größerer Statistikwert oder das Vielfache eines Statistikwertes das Ereignis auslöst. Den Grenzwert selbst trägt man in das Feld 'Threshold' ein.

**Statistic Event Generator**

Event Number: AAAA-8UKN6K

Basics | **Event** | Other

**Event**

Generate a Statistic event of severity:

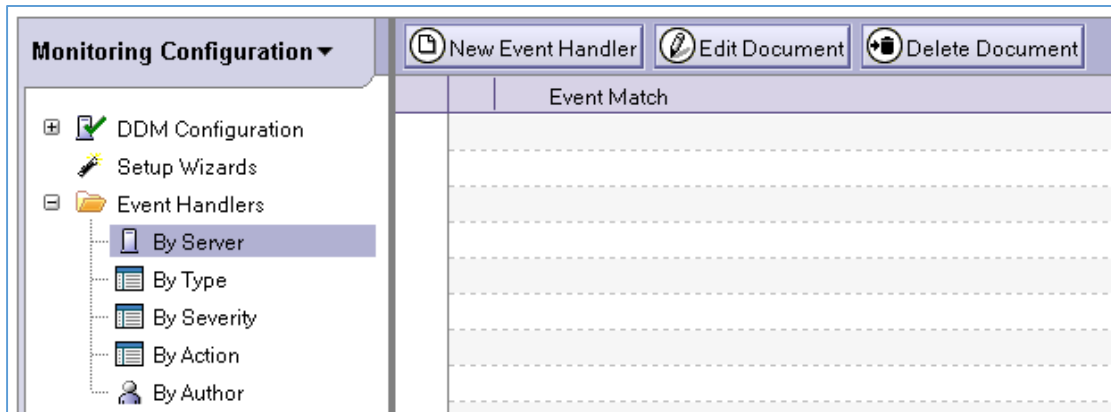
**Enablement**

Disable this event generator

### Register 'Other'

1. **'Generate a Statistic event of severity'**. Hiermit legt man nach eigener Einschätzung eine Warnstufe (Fatal, Failure, Warning high, Warning low oder Normal) fest. Diese Warnstufen können später dazu verwendet werden, sich über alle Alarme (oder auch Ereignisse, Details hierzu werden später besprochen) einer bestimmten Warnstufe informieren zu lassen.
2. **'Create a new event handler for this event'**. Event Handler dienen dazu, sich auf unterschiedliche Arten über definierte Ereignisse informieren zu lassen. Die Details hierzu werden später besprochen.
3. **'Disable this event generator'**. Durch diese Option kann der Event Generator z.B. temporär abgeschaltet werden.

Speichern und schließen Sie das Dokument durch die Aktionsschaltfläche 'Save & Close'.

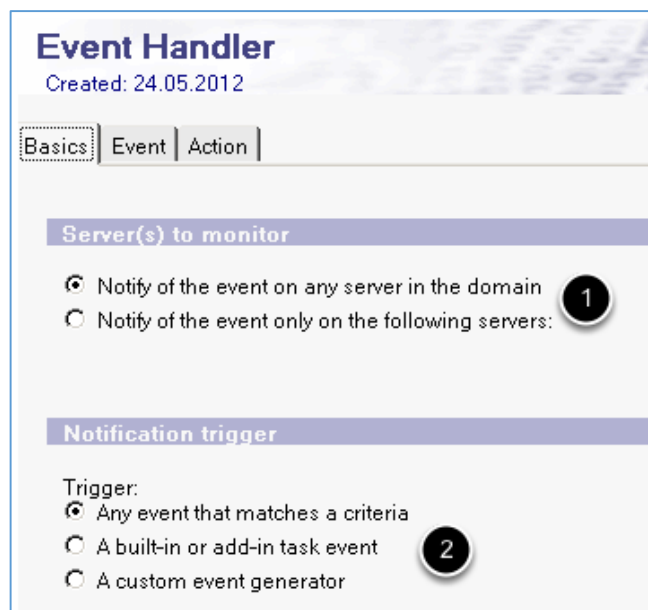


Öffnen Sie die Datenbank EVENTS4.NSF und wählen Sie links in der Navigation unter dem Punkt **'Event Handlers'** die Ansicht **'By Server'**. Durch die Aktionsschaltfläche **'New Event Handler'** können Sie ein neues Dokument erstellen.

**Hinweis**

Da es im **'Event Handler'** Dokument relativ viele Einstellungen gibt, können Sie alternativ für die ersten Versuche auch ein zuvor erstelltes **'Statistic Event Generator'** Dokument öffnen und auf dem Register **'Other'** die Schaltfläche **'Create a new event handler for this event'** anklicken. Sie werden dann in mehreren Teilschritten zum fertigen **'Statistic Event Generator'** Dokument geführt.

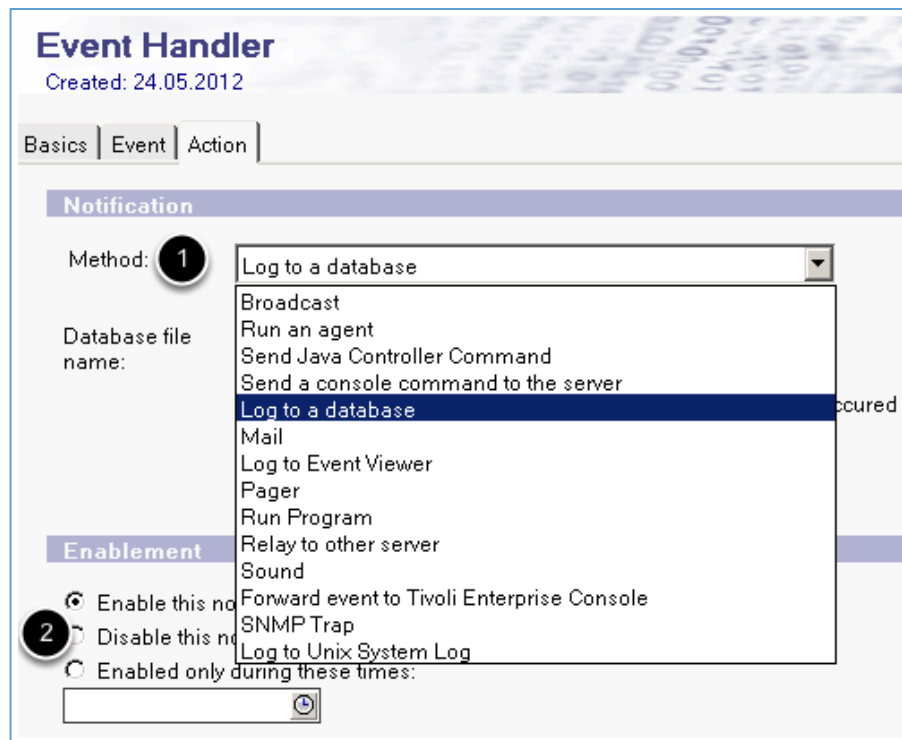
Im **'Event Handler'** Dokument stehen folgende Optionen zur Verfügung.



Register **'Basics'**

**Server(s) to monitor (1).**

Soll der **'Event Handler'** für alle Domino Server der Domäne gelten oder sollen nur bestimmte Maschinen überwacht werden?



#### Register 'Action'

1. **'Method'**. Wie soll die Benachrichtigung erfolgen? Es stehen verschiedene Methoden zur Auswahl (siehe Screenshot), je nach gewählter Methode sind direkt im Bereich unter dem Auswahlfeld weitere Angaben erforderlich. So erfordert die Benachrichtigung per eMail die Angabe einer oder mehrerer Mailadressen.
2. **'Enablement'**. Ist dieser **'Event Handler'** aktiviert, deaktiviert oder nur zu bestimmten Zeiten aktiv?

Speichern und schließen Sie das **'Event Handler'** Dokument durch die Aktionsschaltfläche **'Save & Close'**.

#### **Hinweis**

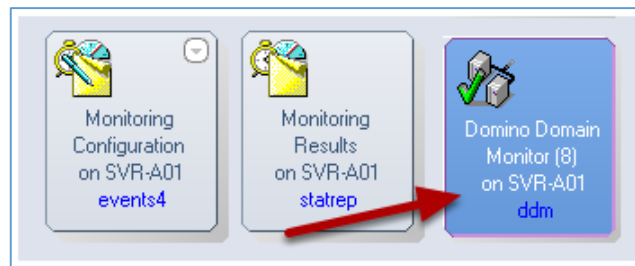
Für schon bestehende Alarmdokumente wird nach der Aktivierung des **'Event Handlers'** z.B. keine eMail mehr verschickt. So soll verhindert werden, dass bei jedem erneuten Auftreten eine weitere eMail verschickt wird. Wenn Sie jedoch das Alarmdokument löschen, wird es beim nächsten Auftreten des Statistikereignisses neu erstellt und dann auch der **'Event Handler'** ausgelöst.



Diese Dokumente werden zwar für das Erstellen von 'Event Generators' oder 'Event Handlers' benötigt, werden aber i.d.R. nicht durch den Administrator erstellt oder verändert und daher hier nicht weiter besprochen.

## 6.4. DDM – Domino Domain Monitoring

Als Ergänzung zur Statistik- und Ereignisüberwachung (Monitoring) hat IBM mit Notes/Domino Version 7 die Funktionalität Domino Domain Monitoring (DDM) eingeführt. DDM bietet für alle Domino Server einer Domäne eine Überwachung spezifiziert durch Probes, welche die Überwachung der Server, einzelner Serverdienste (Tasks) und Datenbanken steuern.



Die Konfiguration der Überwachung erfolgt auch in der Datenbank EVENTS4.NSF, aber die Ergebnisdokumente werden in der neu verfügbaren Datenbank DDM.NSF gespeichert.

### DDM Probes - was soll überwacht werden?

	Total	Enabled	Type	Probe Description
DDM Configuration	58	0		Lotus Notes Template Development
DDM Probes	11	0		Administration
By Author	7	0		Application Code
By Probe Server	4	0		Database
By Type	10	0		Directory
DDM Filters	12	0		Messaging
Server Collection Hierarc	4	0		Operating System
Open Monitoring...	2	0		Replication
Setup Wizards	5	0		Security
Event Handlers	1	0		Server
Event Generators	2	0		Web
Console Attributes	58	0		

Welche Ereignisse durch das Domino Domain Monitoring überwacht und protokolliert werden, wird in der Datenbank EVENTS4.NSF durch die sogenannten 'Probe' Dokumente bestimmt.

Öffnen Sie die Datenbank EVENTS4.NSF und selektieren Sie links in der Datenbanknavigation eine der Ansichten unterhalb des Punktes 'DDM Configuration' -> 'DDM Probes'. Im Screenshot sind 58 verschiedene 'Probes' Dokumente bereits vorhanden (Standard der Version Notes/Domino 8.5.3) - diese werden von IBM automatisch zur Verfügung gestellt und sollen dem Administrator einen einfachen Einstieg - es müssen lediglich die gewünschten 'Probes' aktiviert werden - in das Domino Domain Monitoring bieten.

### New DDM Database Probe

Basics | **Schedule**

---

**Schedule**

How often should this probe run?

Run multiple times per day  
 Daily  
 Weekly  
 Monthly

---

On which days should this probe run?

Sunday  
 Monday  
 Tuesday  
 Wednesday  
 Thursday  
 Friday  
 Saturday

---

At what time should this probe run?

#### Register 'Schedule'

Die Ausführung lässt sich mehrmals pro Tag, täglich, wöchentlich oder monatlich festlegen.

Speichern und schließen Sie das Dokument durch die Aktionsschaltfläche 'Save & Close'.

#### DDM Ereignisse

The screenshot shows the DDM interface with the following data visible in the event list:

#	Date	Server	Open Events By Severity
30			Failure
13			Warning (High)
9			Warning (Low)
2			Security
	Di 27.03	SVR-A01/FirmaA	Failed to authenticate with server SVR-A01/FirmaA. The server's Domino Directory does not contain any cross certificates capable of authenticating the server.
	Di 27.03	SVR-A01/FirmaA	AdminB01/FirmaB from host [192.168.1.100] failed to authenticate: The server's Domino Directory does not contain any cross certificates capable of authenticating the server.
2			Security: Access
5			Server

Die durch DDM generierten Ereignisse werden in Form von Dokumenten in der Datenbank DDM.NSF gespeichert.

#### Hinweis

Die Aktionsschaltflächen 'Assign...' und 'Change State' werden nur angezeigt, wenn die entsprechenden Rollen in der Datenbank-ACL aktiviert sind.

Sobald Sie eines der Ereignisdokumente öffnen, werden detaillierte Informationen zum gemeldeten Ereignis angezeigt.