3. Installation der CSS

3.1 Einrichtung eines Dienstkontos und der notwendigen Berechtigungen für den CSS

Soll der CSS auf einem Domänencontroller installiert werden, so ist ein Dienstkonto einzurichten:

ISA 2004 Enterprise Edition
Installieren des Konfigurationsspeicherservers auf einem Domänencontroller

In einigen Szenarien kann es von Vorteil sein, die Konfigurationsspeicherserver-Komponente von Microsoft Internet Security & Acceleration (ISA) Server 2004 auf einem Domänencontroller zu installieren. Dies ist beispielsweise der Fall, wenn die Administrations- und Hardwareressourcen einer Niederlassung, die durch eine Firewall geschützt werden muss, beibehalten werden sollen.

In den meisten Szenarien wird der Konfigurationsspeicherserver-Dienst unter dem Netzwerkdienstkonto ausgeführt. Bei der Installation des ISA Server-Konfigurationsspeicherservers auf einem Domänencontroller müssen Sie ein anderes Konto angeben, unter dem der Konfigurationsspeicherserver-Dienst ausgeführt wird. Das liegt daran, dass das Netzwerkdienstkonto nicht verwendet werden kann, wenn der Konfigurationsspeicherserver auf einem Domänencontroller ausgeführt wird.

Sie können den Konfigurationsspeicherserver-Dienst mit den Anmeldeinformationen eines Benutzers der Gruppe Domänen-Admins (Domänenadministrator) ausführen. Für eine sichere Konfiguration empfehlen wir jedoch, die Anmeldeinformationen eines Benutzers anzugeben, der kein Domänenadministrator ist. In diesem Fall müssen Sie folgende Schritte ausführen, um sicherzustellen, dass der Benutzer über die erforderlichen Berechtigungen für den Dienst verfügt:

1. Installieren Sie den Konfigurationsspeicherserver wie unter Installieren des Konfigurationsspeicherservers beschrieben.
2. Geben Sie beim Installationsvorgang auf der Seite Dienstkonto für Konfigurationsspeicherserver des Installations-Assistenten die Anmeldeinformationen des Benutzers an, der kein Domänenadministrator ist.
3. Suchen Sie im Ordner Programme\Microsoft ISA Server\ADAMData die Datei Dnsdomain.bat, wobei Dnsdomain für den DNS-Namen des Computers steht, auf dem ADAM (Active Directory Application Mode) ausgeführt wird.
4. Geben Sie in die Befehlszeile Dnsdomain ein, um die Datei auszuführen.

Anmerkung

- Die Datei Dnsdomain.bat wird ca. eine Minute nach Abschluss der ADAM-Installation im Verzeichnis angezeigt.

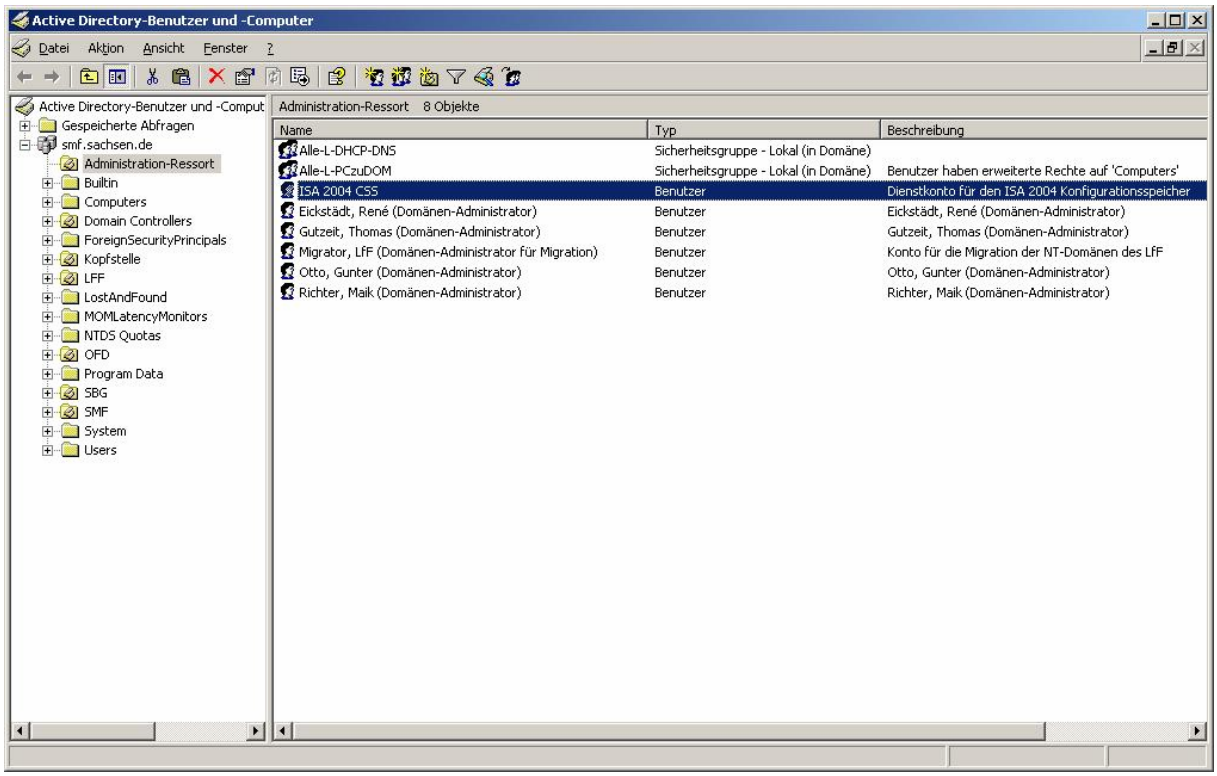
Auszug aus der ISA 2004 EE Dokumentation

Dieses Dienstkonto ist in der OU „Administration-Ressort“ angelegt, verfügt aber über keinerlei administrativen Rechte. Der Account ist Mitglied der Gruppe „SMF\Domänen-Benutzer“ und besitzt ein entsprechend starkes Passwort (zehn Zeichen incl. Sonderzeichen). Dieses läuft nie ab.

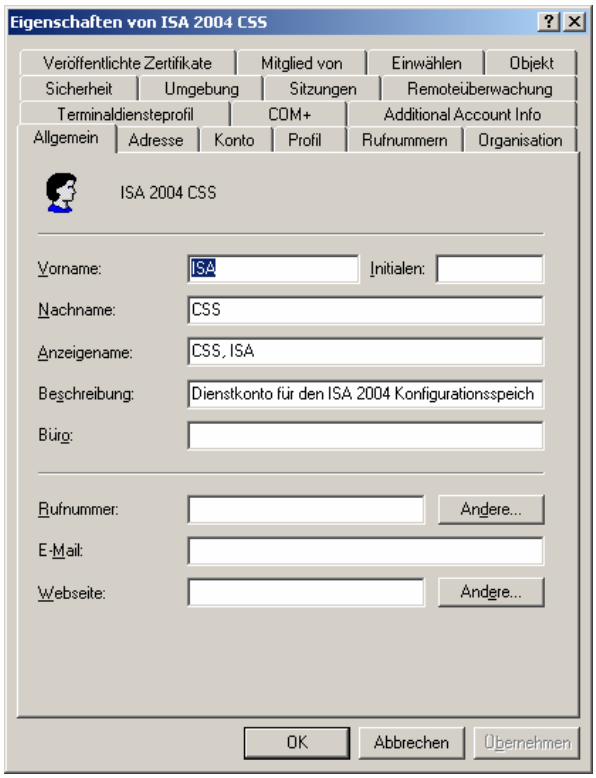
Weiterhin muss dieses Konto folgende Berechtigungen besitzen:

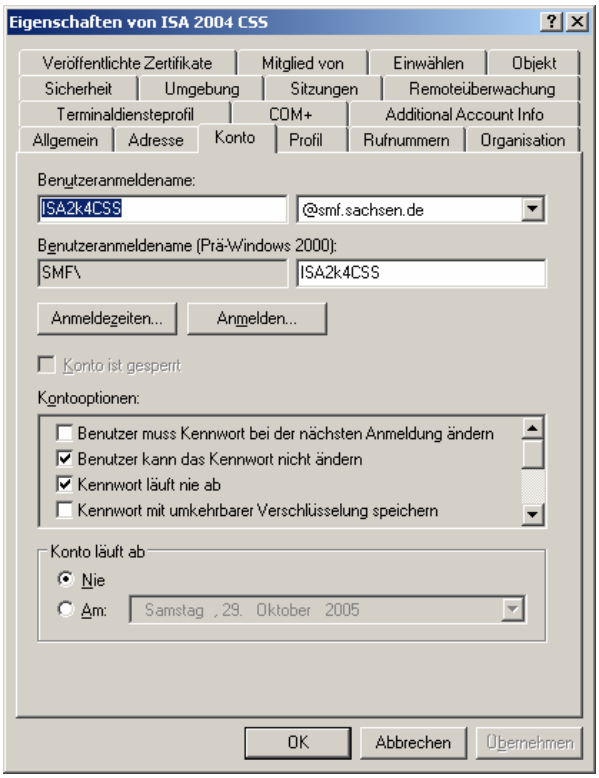
- „Anmelden als Dienst“
- „Generieren von Sicherheitsüberwachungen“
- „ServiceConnectionPoint erstellen“

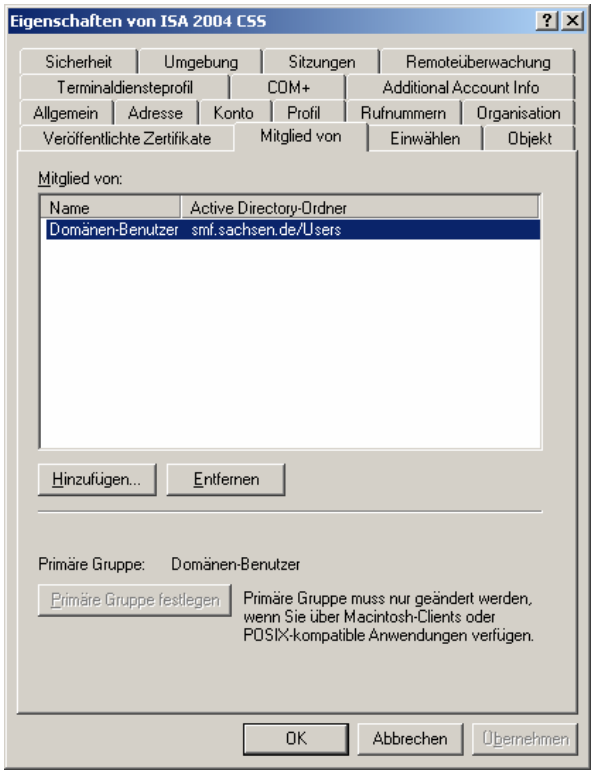
Das letztgenannte Recht ist mittels „ADSI Edit“ auf den Namenskontext „DC=smf, DC=sachsen,DC=de,OU=Domain Controllers, CN=SMF-DC-01“ zu vergeben (dies ist für jeden als CSS genutzten DC durchzuführen), die beiden anderen Rechte werden über die Konfiguration der „Default Domain Controllers Policy“ gesetzt.



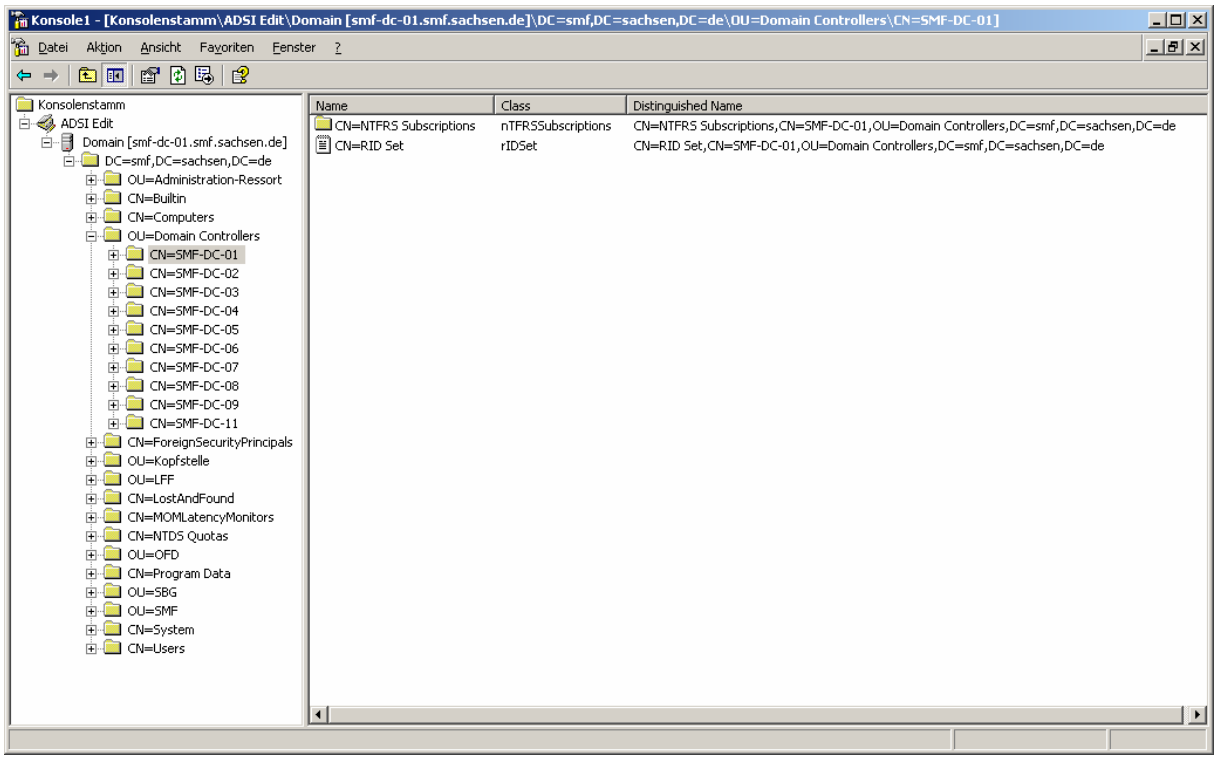
Eingerichtetes Dienstkonto für den CSS

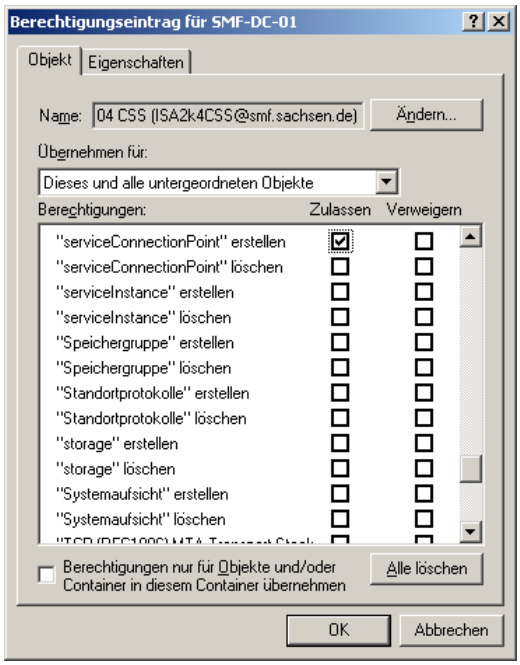


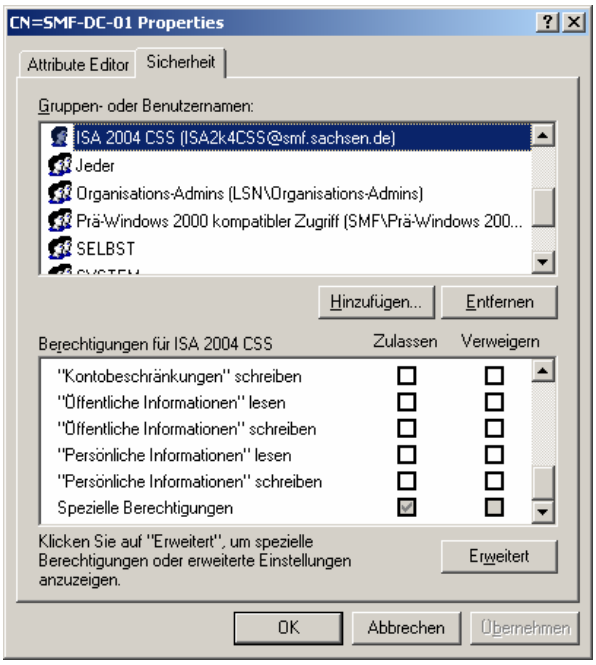




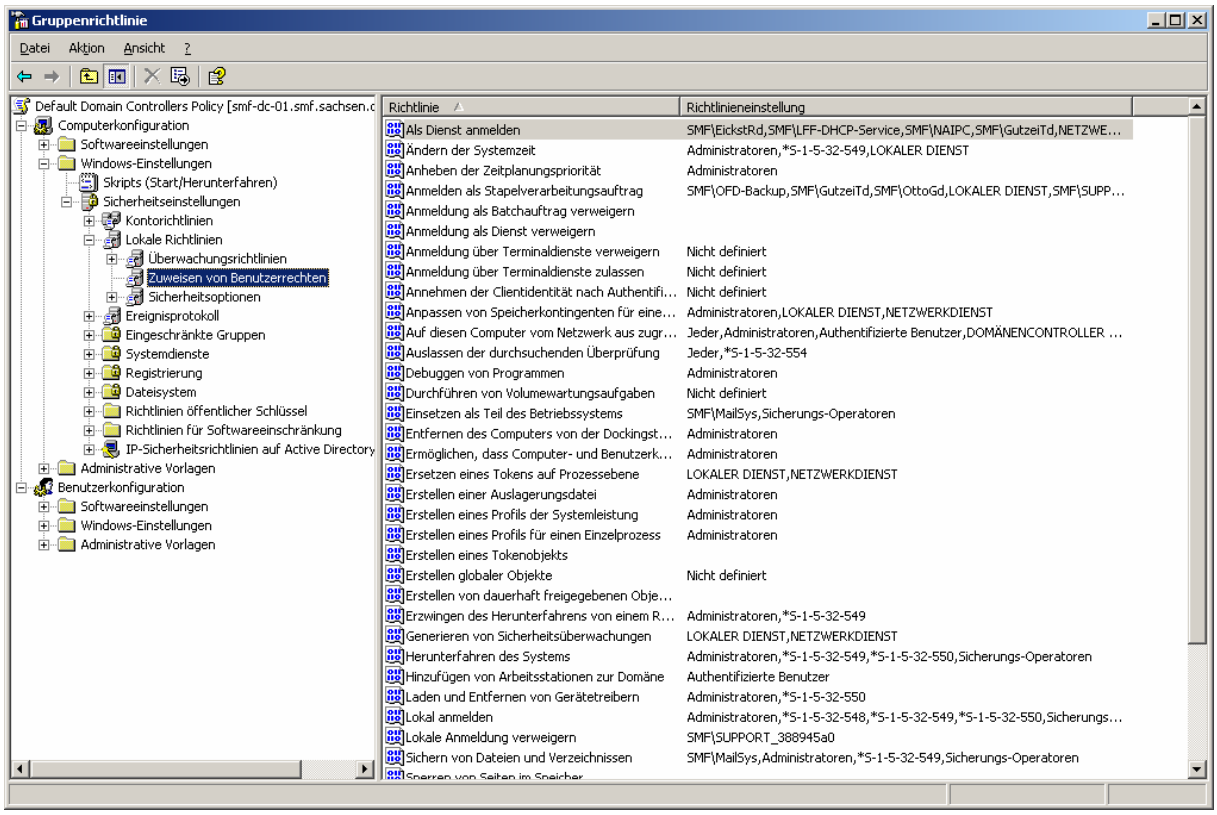
Eigenschaften des Dienstkontos für den CSS

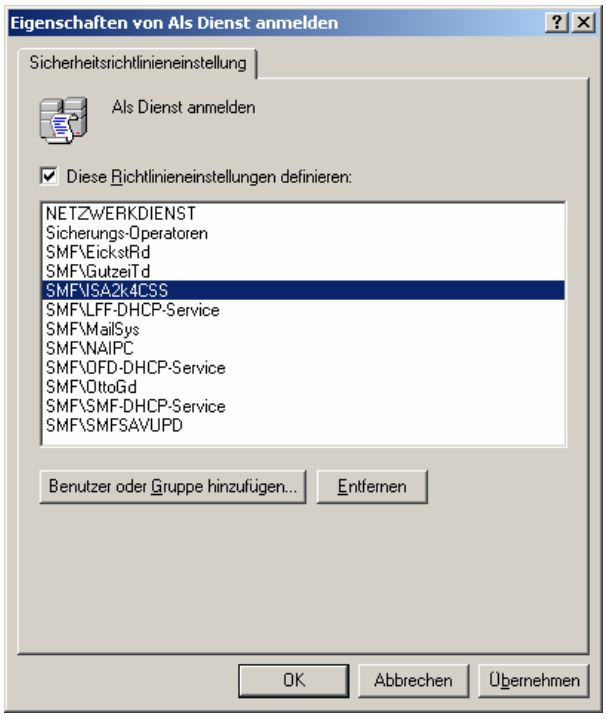


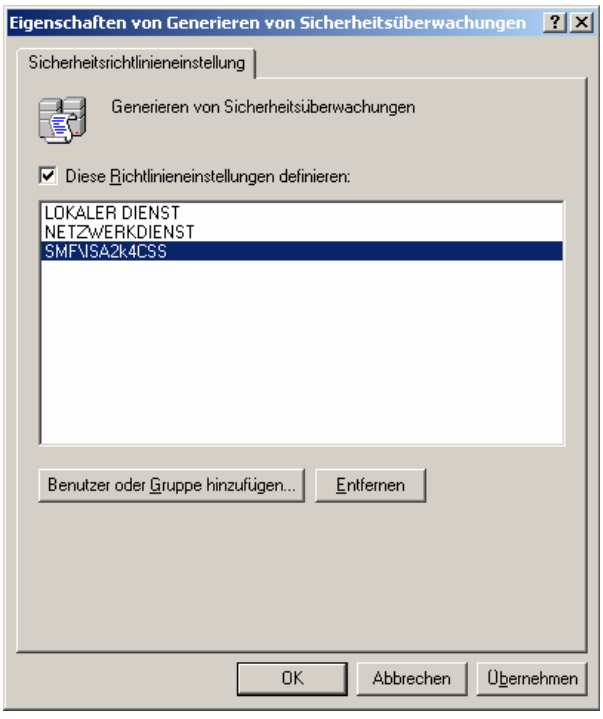




Zuweisen des Rechtes „ServiveConnectionPoint erstellen“ für das CSS-Dienstkonto



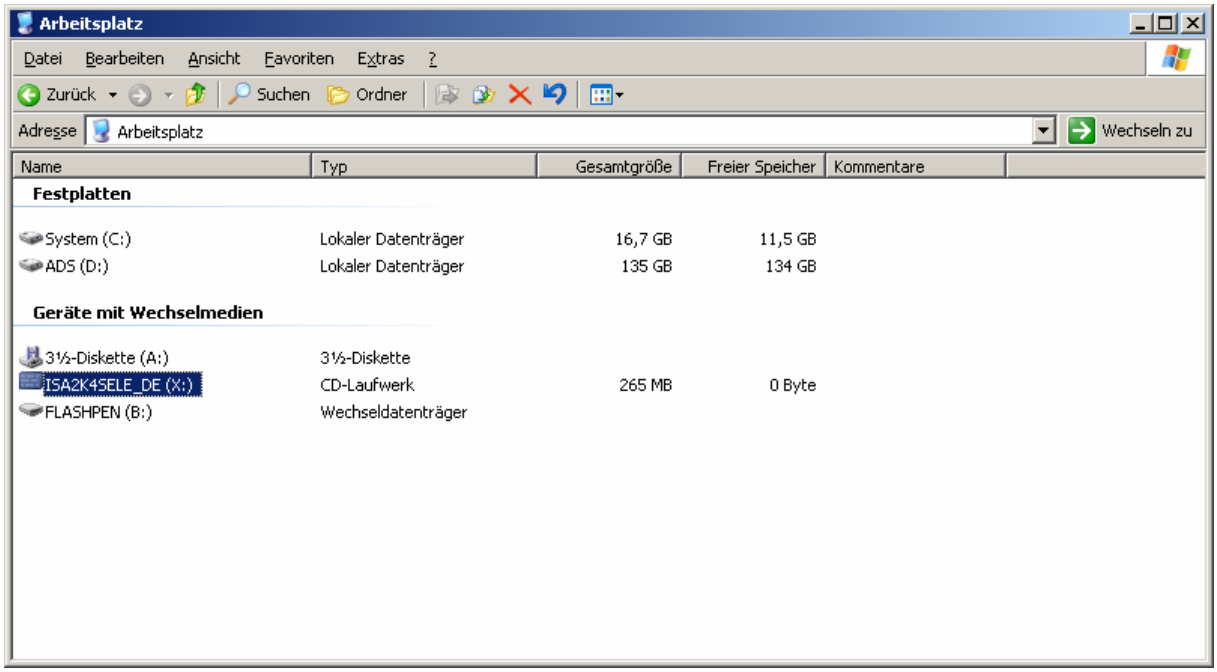


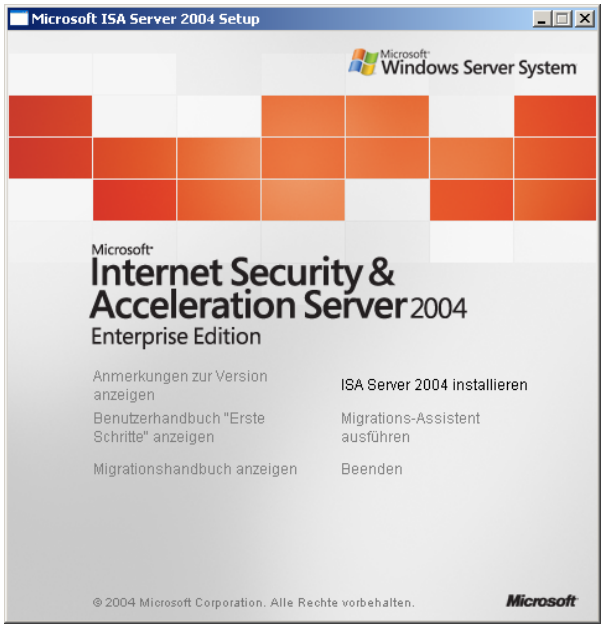


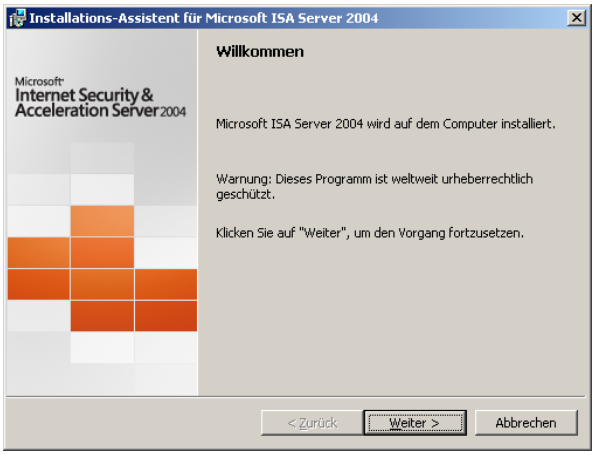
Zuweisen der Benutzerrechte für das CSS-Dienstkonto in der „Default Domain Controllers Policy“

3.2 Installation des ersten CSS

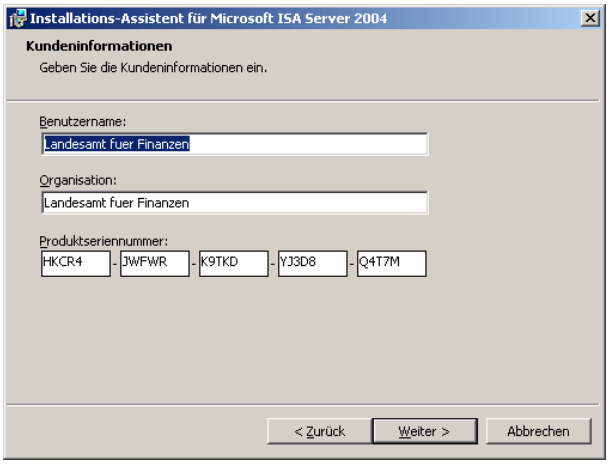
Der erste Konfigurationsspeicherserver (CSS) wird auf dem ersten Domänen-controller der Kopfstelle (SMF-DC-01) installiert. für diesen Vorgang ist ein Konto der Gruppe „Domänen-Administratoren“ zu verwenden. Die einzelnen Schritte werden in der Folge chronologisch dargestellt:








Installations-Assistent für Microsoft ISA Server 2004
Lizenzvertrag
Lesen Sie bitte den folgenden Lizenzvertrag.
ENDBENUTZER-LIZENZVERTRAG FÜR MICROSOFT-SOFTWARE
MICROSOFT INTERNET SECURITY & ACCELERATION SERVER 2004
Enterprise Edition
Ich stimme den Bedingungen des Lizenzvertrags zu
Ich lehne die Bedingungen des Lizenzvertrags ab
< Zurück
Weiter >
Abbrechen


Installations-Assistent für Microsoft ISA Server 2004
Kundeninformationen
Geben Sie die Kundeninformationen ein.
Benutzername:
Landesamt fuer Finanzen
Organisation:
Landesamt fuer Finanzen
Produktseriennummer:
HKCR4 - JWFWR - K9TKD - YJ3D8 - Q4T7M
< Zurück
Weiter >
Abbrechen

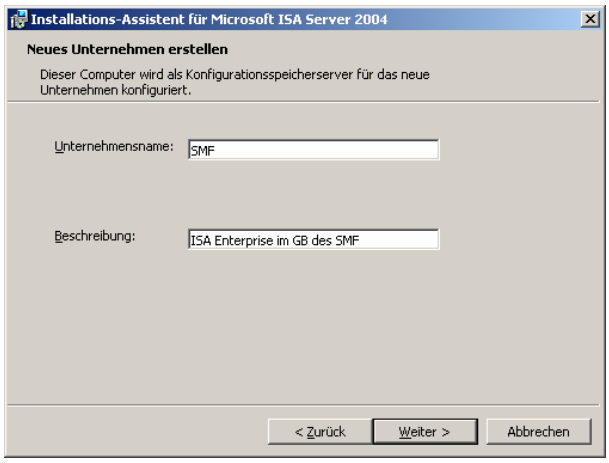

Installations-Assistent für Microsoft ISA Server 2004
Setup-Szenarien
Wählen Sie das Szenario, das diese Installation am besten beschreibt.
ISA Server-Dienste installieren
Der Computer wird ein ISA Server-Arraymitglied, auf dem ISA Server-Dienste ausgeführt werden.
Konfigurationsspeicherserver installieren
Der Computer speichert die Konfiguration, die von ISA Server-Arrays verwendet wird. ISA Server-Arraycomputer stellen eine Verbindung mit diesem Server her, um die Konfiguration abzurufen.
ISA Server-Dienste und Konfigurationsspeicherserver installieren
Der Computer wird ein ISA Server-Arraymitglied, auf dem zusätzlich die Unternehmenskonfiguration gespeichert wird.
ISA Server-Verwaltung installieren
Der Computer wird zur Remoteverwaltung des ISA Server-Unternehmens verwendet.
< Zurück
Weiter >
Abbrechen

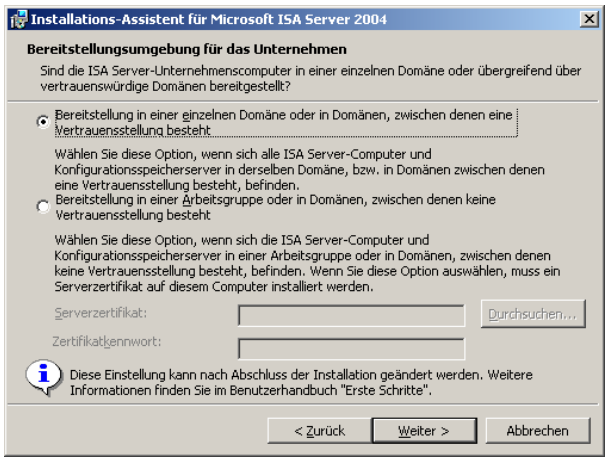

Installations-Assistent für Microsoft ISA Server 2004
Komponentenauswahl
Die ausgewählten Funktionen werden installiert.
Klicken Sie auf ein Symbol in der Liste, um die Installationsart der Funktion anzuzeigen oder zu ändern.
ISA Server
Erweiterte Protokollierung
ISA Server-Verwaltung
Firewallclient-Installationsfreigabe
Nachrichtenüberwachung
Konfigurationsspeicherserver
Funktionsbeschreibung
Speichert die Unternehmenskonfiguration für ISA Server-Arrays.
Diese Funktion erfordert 63 MB auf der Festplatte.
Installieren nach:
C:\Programme\Microsoft ISA Server\
Ändern...
Hilfe
Speicherplatz
< Zurück
Weiter >
Abbrechen

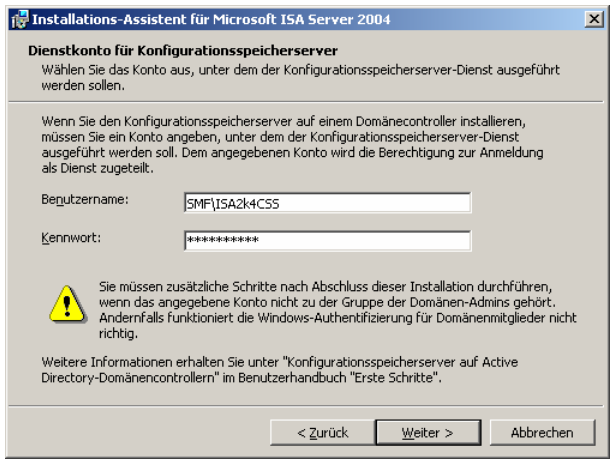

Installations-Assistent für Microsoft ISA Server 2004
Komponentenauswahl
Die ausgewählten Funktionen werden installiert.
Klicken Sie auf ein Symbol in der Liste, um die Installationsart der Funktion anzuzeigen oder zu ändern.
ISA Server
Erweiterte Protokollierung
ISA Server-Verwaltung
Firewallclient-Installationsfreigabe
Nachrichtenüberwachung
Konfigurationsspeicherserver
Funktionsbeschreibung
Speichert die Unternehmenskonfiguration für ISA Server-Arrays.
Diese Funktion erfordert 63 MB auf der Festplatte.
Installieren nach:
D:\Microsoft ISA Server\
Ändern...
Hilfe
Speicherplatz
< Zurück
Weiter >
Abbrechen

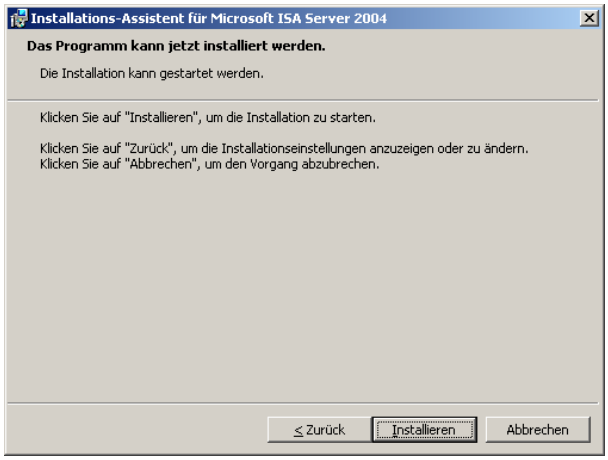

Installations-Assistent für Microsoft ISA Server 2004
Unternehmensinstallationsoptionen
Möchten Sie ein neues Unternehmen erstellen oder eine vorhandene Unternehmenskonfiguration auf diesen Konfigurationsspeicherserver replizieren?
Neues ISA Server-Unternehmen erstellen
Verwenden Sie diese Option, um ein neues ISA Server-Unternehmen während der Installation zu erstellen. Dieser Computer wird ein Konfigurationsspeicherserver, den Arrays verwenden können.
Replikat der Unternehmenskonfiguration erstellen
Verwenden Sie diese Option, um die Konfigurationseinstellungen des Unternehmens, die auf einem Konfigurationsspeicherserver gespeichert sind, auf diesen Computer zu kopieren. Durch diese Option wird die Fehlertoleranz verbessert, indem ein Replikat der Unternehmenskonfiguration angeboten wird. ISA Server-Arrays können diesen Konfigurationsspeicherserver ebenfalls verwenden.
< Zurück
Weiter >
Abbrechen

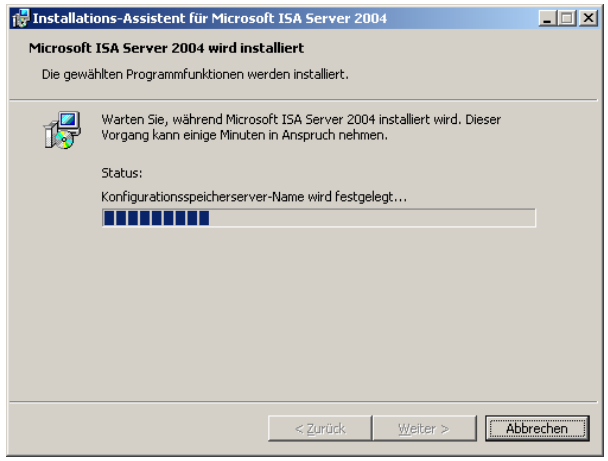

Installations-Assistent für Microsoft ISA Server 2004
Neues Unternehmen
Dieser Computer wird als neuer Konfigurationsspeicherserver konfiguriert.
Es wird empfohlen, dass Sie ein einzelnes Unternehmen in Ihrer Organisation erstellen. Arrays können nur von dem Unternehmen verwaltet werden, zu dem sie gehören. Das Erstellen mehrerer Unternehmen erschwert die zentrale Verwaltung aller Arraycomputer in der Organisation.
Klicken Sie auf "Zurück" und wählen Sie die Option "Replikat der Unternehmenskonfiguration erstellen", wenn das Unternehmen bereits auf einem anderen Konfigurationsspeicherserver konfiguriert ist.
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen, wenn dies der erste Konfigurationsspeicherserver in der Organisation ist.
< Zurück
Weiter >
Abbrechen

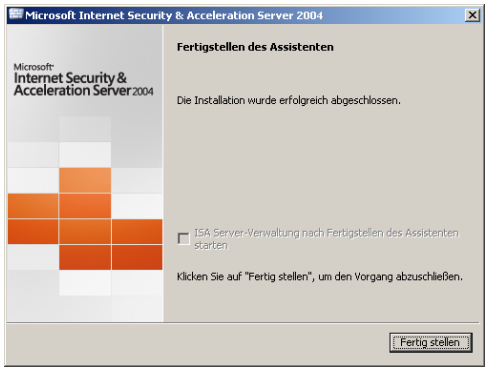

Installations-Assistent für Microsoft ISA Server 2004
Neues Unternehmen erstellen
Dieser Computer wird als Konfigurationsspeicherserver für das neue Unternehmen konfiguriert.
Unternehmensname:
SMF
Beschreibung:
ISA Enterprise im GB des SMF
< Zurück
Weiter >
Abbrechen

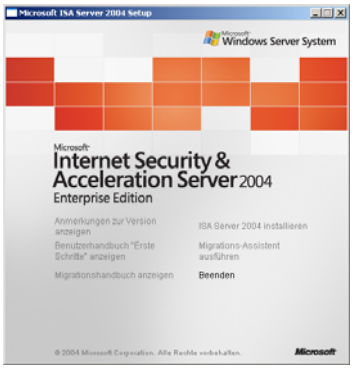

Installations-Assistent für Microsoft ISA Server 2004
Bereitstellungsumgebung für das Unternehmen
Sind die ISA Server-Unternehmenscomputer in einer einzelnen Domäne oder übergreifend über vertrauenswürdige Domänen bereitgestellt?
Bereitstellung in einer einzelnen Domäne oder in Domänen, zwischen denen eine Vertrauensstellung besteht
Wählen Sie diese Option, wenn sich alle ISA Server-Computer und Konfigurationsspeicherserver in derselben Domäne, bzw. in Domänen zwischen denen eine Vertrauensstellung besteht, befinden.
Bereitstellung in einer Arbeitsgruppe oder in Domänen, zwischen denen keine Vertrauensstellung besteht
Wählen Sie diese Option, wenn sich die ISA Server-Computer und Konfigurationsspeicherserver in einer Arbeitsgruppe oder in Domänen, zwischen denen keine Vertrauensstellung besteht, befinden. Wenn Sie diese Option auswählen, muss ein Serverzertifikat auf diesem Computer installiert werden.
Serverzertifikat:
Durchsuchen...
Zertifikatkennwort:
Diese Einstellung kann nach Abschluss der Installation geändert werden. Weitere Informationen finden Sie im Benutzerhandbuch "Erste Schritte".
< Zurück
Weiter >
Abbrechen


Installations-Assistent für Microsoft ISA Server 2004
Dienstkonto für Konfigurationsspeicherserver
Wählen Sie das Konto aus, unter dem der Konfigurationsspeicherserver-Dienst ausgeführt werden sollen.
Wenn Sie den Konfigurationsspeicherserver auf einem Domänecontroller installieren, müssen Sie ein Konto angeben, unter dem der Konfigurationsspeicherserver-Dienst ausgeführt werden soll. Dem angegebenen Konto wird die Berechtigung zur Anmeldung als Dienst zugeteilt.
Benutzername:
SMF\ISA2k4CSS
Kennwort:
Sie müssen zusätzliche Schritte nach Abschluss dieser Installation durchführen, wenn das angegebene Konto nicht zu der Gruppe der Domänen-Admins gehört. Andernfalls funktioniert die Windows-Authentifizierung für Domänenmitglieder nicht richtig.
Weitere Informationen erhalten Sie unter "Konfigurationsspeicherserver auf Active Directory-Domänencontrollern" im Benutzerhandbuch "Erste Schritte".
< Zurück
Weiter >
Abbrechen

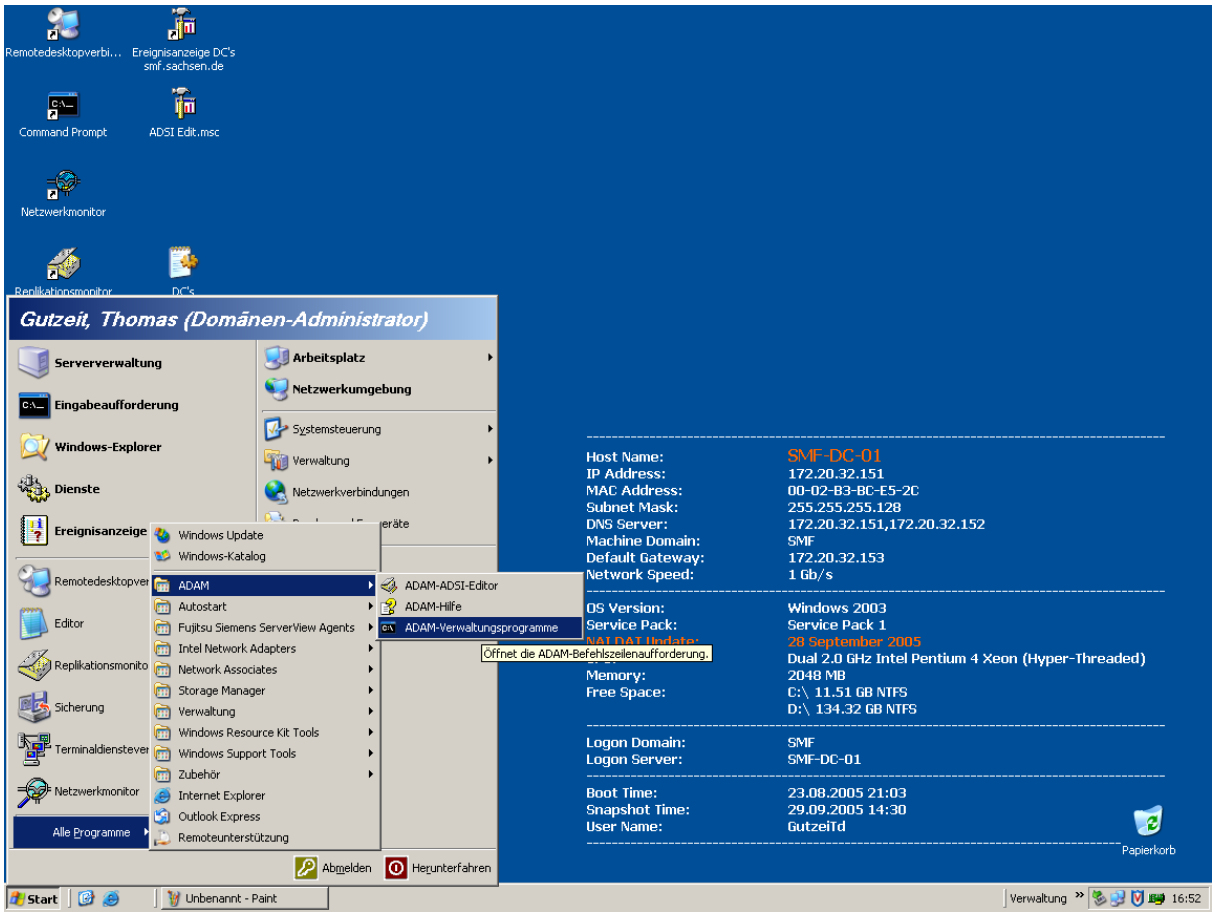

Installations-Assistent für Microsoft ISA Server 2004
Das Programm kann jetzt installiert werden.
Die Installation kann gestartet werden.
Klicken Sie auf "Installieren", um die Installation zu starten.
Klicken Sie auf "Zurück", um die Installationseinstellungen anzuzeigen oder zu ändern.
Klicken Sie auf "Abbrechen", um den Vorgang abzubrechen.
< Zurück
Installieren
Abbrechen


Installations-Assistent für Microsoft ISA Server 2004
Microsoft ISA Server 2004 wird installiert
Die gewählten Programmfunktionen werden installiert.
Warten Sie, während Microsoft ISA Server 2004 installiert wird. Dieser Vorgang kann einige Minuten in Anspruch nehmen.
Status:
Konfigurationsspeicherserver-Name wird festgelegt...
< Zurück
Weiter >
Abbrechen

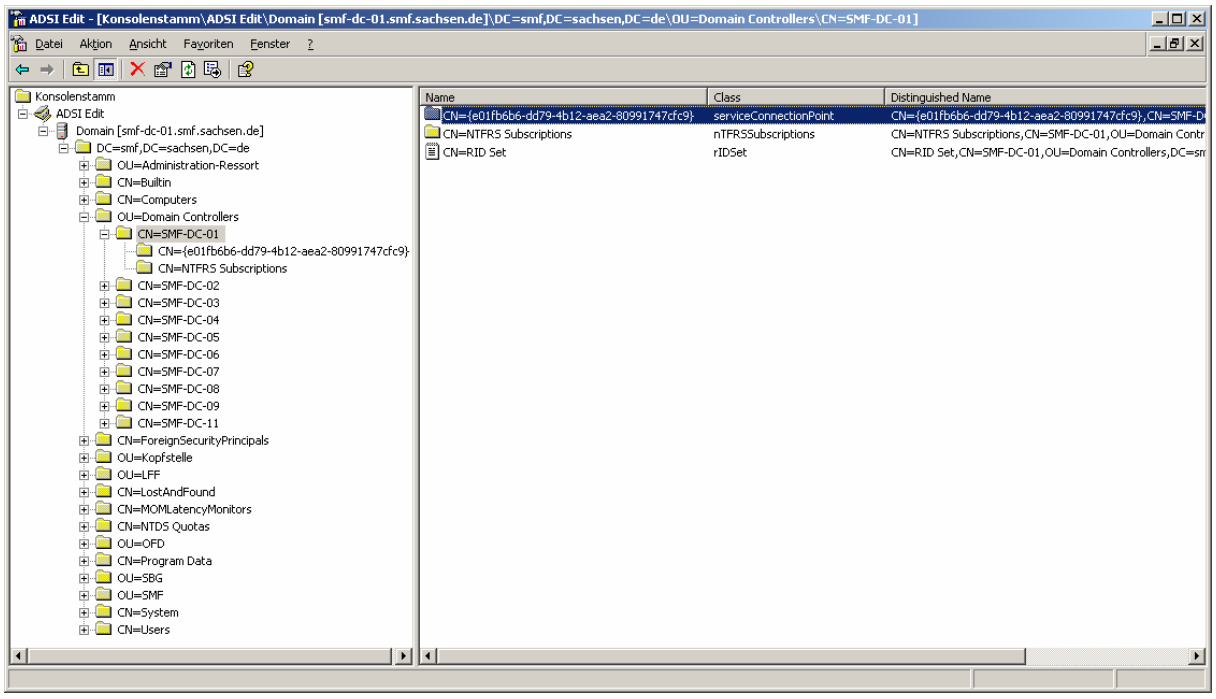

Microsoft Internet Security & Acceleration Server 2004
Microsoft
Internet Security & Acceleration Server 2004
Fertigstellen des Assistenten
Die Installation wurde erfolgreich abgeschlossen.
ISA Server-Verwaltung nach Fertigstellen des Assistenten starten
Klicken Sie auf "Fertig stellen", um den Vorgang abzuschließen.
Fertig stellen


Microsoft ISA Server 2004 Setup
Windows Server System
Microsoft
Internet Security & Acceleration Server 2004
Enterprise Edition
Anmerkungen zur Version anzeigen
ISA Server 2004 installieren
Benutzerhandbuch "Erste Schritte" anzeigen
Migrations-Assistent ausführen
Migrationshandbuch anzeigen
Beenden
Microsoft

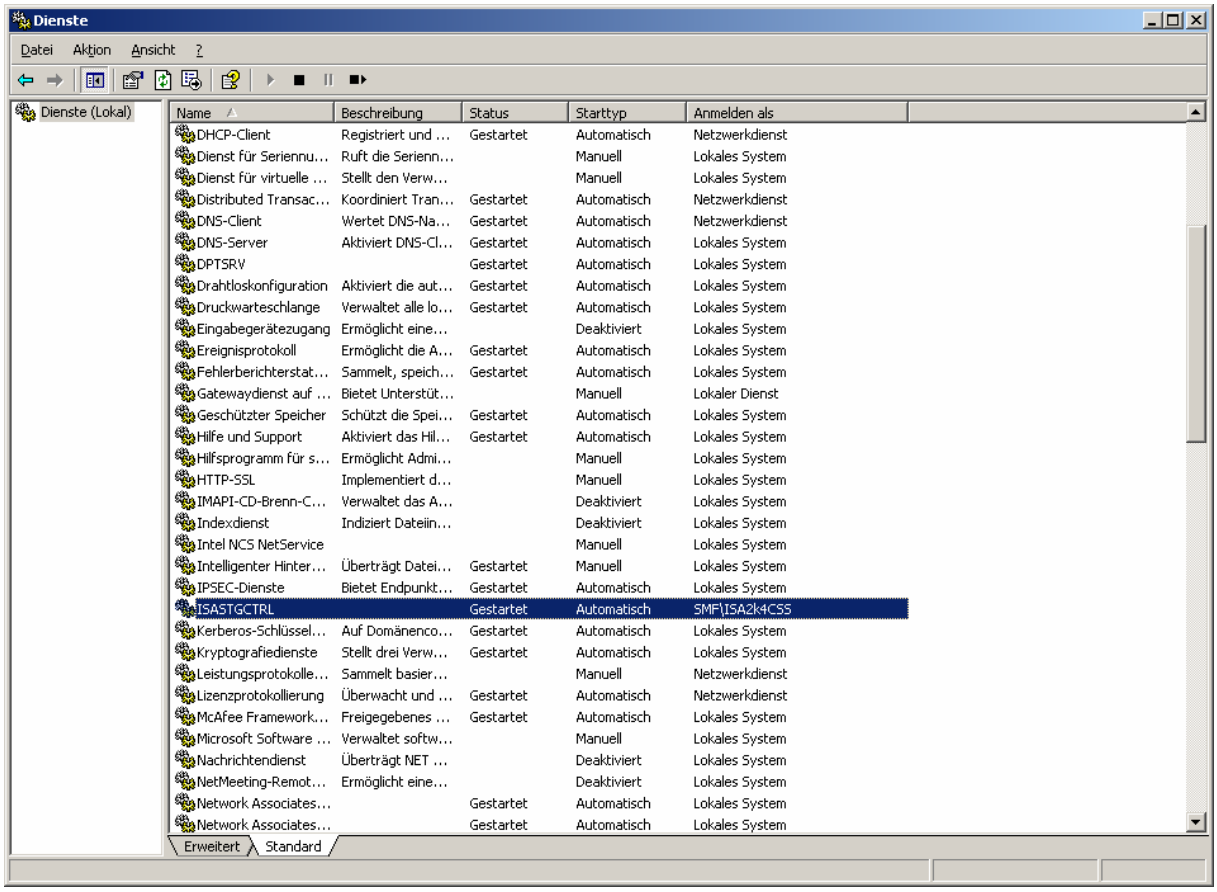
Nach erfolgreicher Installation ist ein neuer Eintrag für das ADAM im Startmenü zu finden:



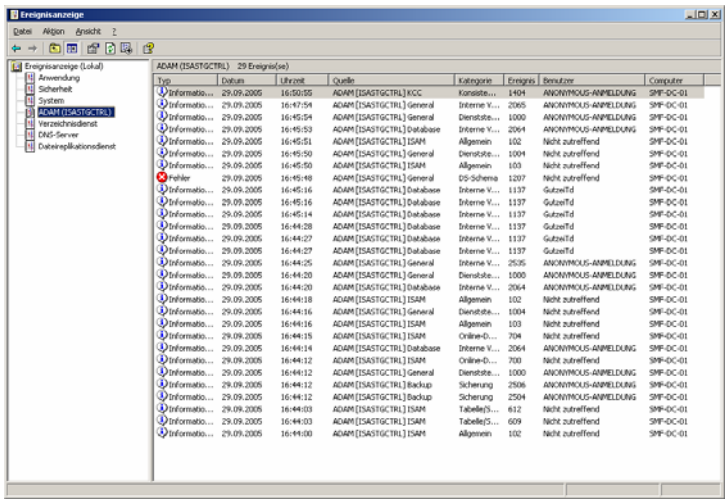
Weiterhin wurde unter „DC=smf, DC=sachsen,DC=de,OU=Domain Controllers, CN=SMF-DC-01“ ein entsprechender ServiceConnectionPoint erstellt:

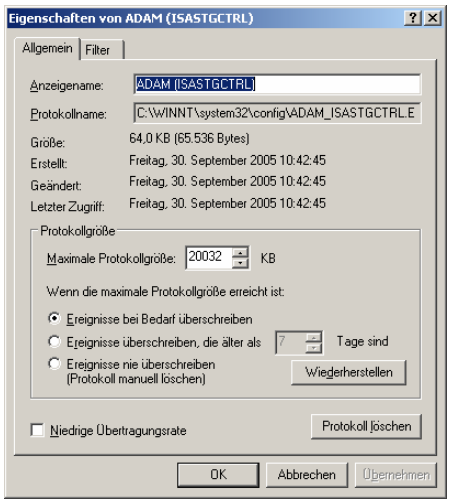


Für den CSS wurde ebenfalls ein neuer Dienst installiert und gestartet:



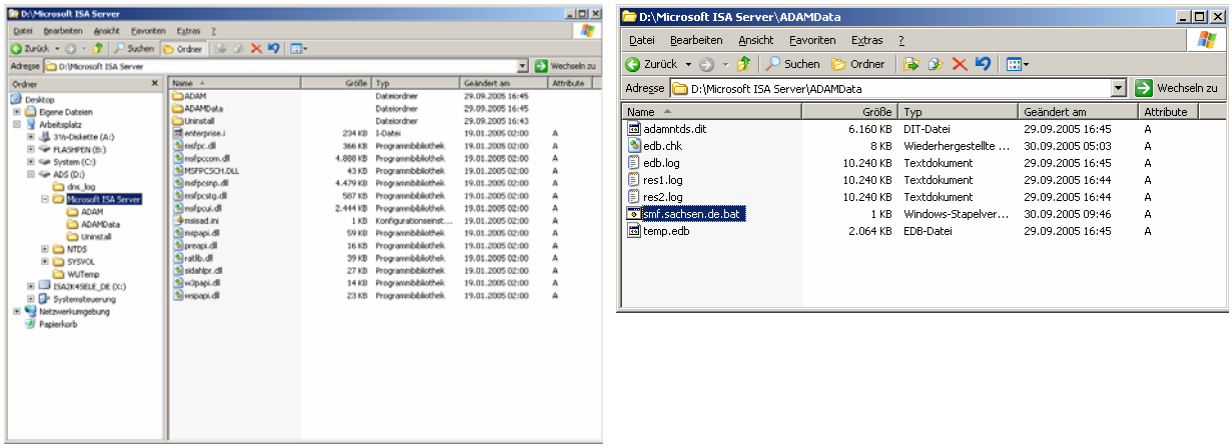
In der Ereignisanzeige ist ein neues Eventlog für das ADAM angelegt, dessen Größe wurde auf 20032 KByte erhöht:





3.3 Tätigkeiten nach Abschluss der Installation

Nach erfolgreicher Installation ist die Datei „smf.sachsen.de.bat“ (dnsdomain.bat) auszuführen. Diese wird wenige Minuten nach Abschluss der Installation automatisch im Ordner „Microsoft ISA Server\ADAMData\“ angelegt. Durch diese Datei werden SPN’s (ServicePrincipalName) des ADAM in das AD geschrieben.



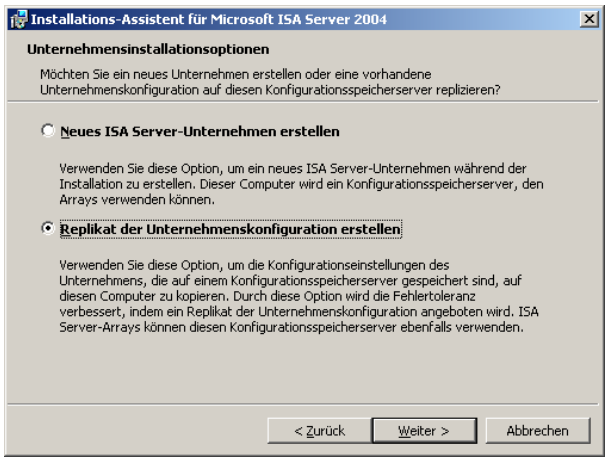
Speicherort der Datei „dnsdomain.bat“

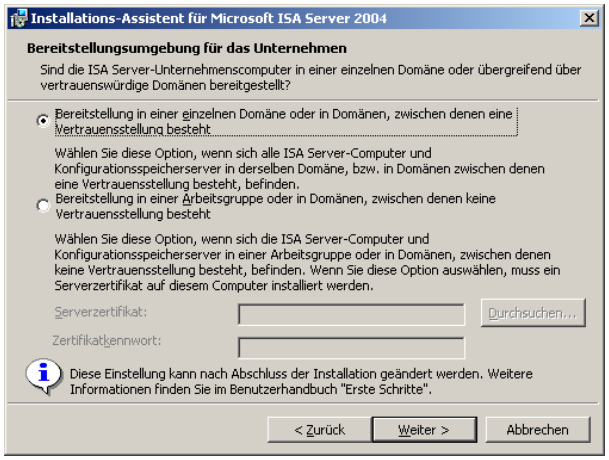
Der Aufruf dieser Datei auf der Kommandozeile sollte das erfolgreiche Schreiben der SPN’s bestätigen:

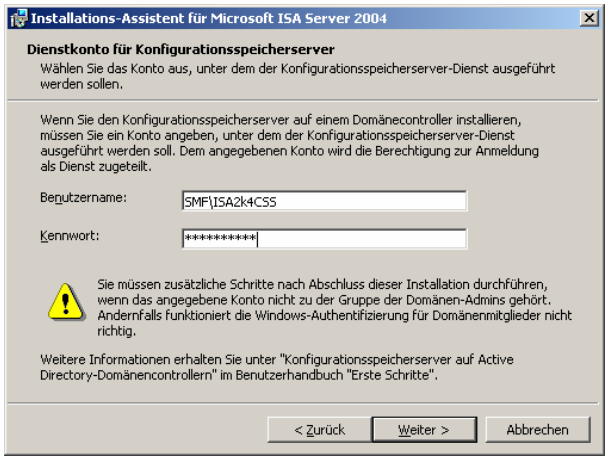
```
D:\Microsoft ISA Server\ADAMData>smf.sachsen.de.bat

D:\Microsoft ISA Server\ADAMData>C:\WINNT\ADAM\repadmin.exe /writespn smf.sachsen.de ADD
"CN=ISA 2004 CSS,OU=Administration-Ressort,DC=smf,DC=sachsen,DC=de" E3514235-4B06-11D1-AB04-
00C04FC2DCD2-ADAM/SMF-DC-01:2171
Die angeforderten SPNs wurden erfolgreich geschrieben.

D:\Microsoft ISA Server\ADAMData>C:\WINNT\ADAM\repadmin.exe /writespn smf.sachsen.de ADD
"CN=ISA 2004 CSS,OU=Administration-Ressort,DC=smf,DC=sachsen,DC=de" E3514235-4B06-11D1-AB04-
00C04FC2DCD2-ADAM/smf-dc-01.smf.sachsen.de:2171
Die angeforderten SPNs wurden erfolgreich geschrieben.

D:\Microsoft ISA Server\ADAMData>C:\WINNT\ADAM\repadmin.exe /writespn smf.sachsen.de ADD
"CN=ISA 2004 CSS,OU=Administration-Ressort,DC=smf,DC=sachsen,DC=de" ldap/SMF-DC-01:2171
Die angeforderten SPNs wurden erfolgreich geschrieben.

D:\Microsoft ISA Server\ADAMData>C:\WINNT\ADAM\repadmin.exe /writespn smf.sachsen.de ADD
"CN=ISA 2004 CSS,OU=Administration-Ressort,DC=smf,DC=sachsen,DC=de" ldap/smf-dc-
01.smf.sachsen.de:2171
Die angeforderten SPNs wurden erfolgreich geschrieben.

D:\Microsoft ISA Server\ADAMData>
```

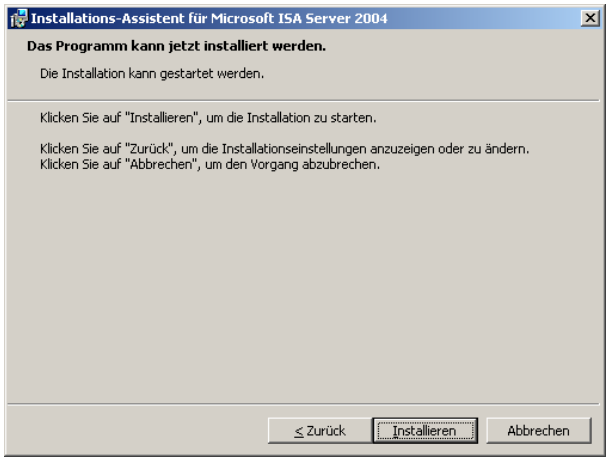
3.4 Installation des zweiten bzw. der weiteren CSS

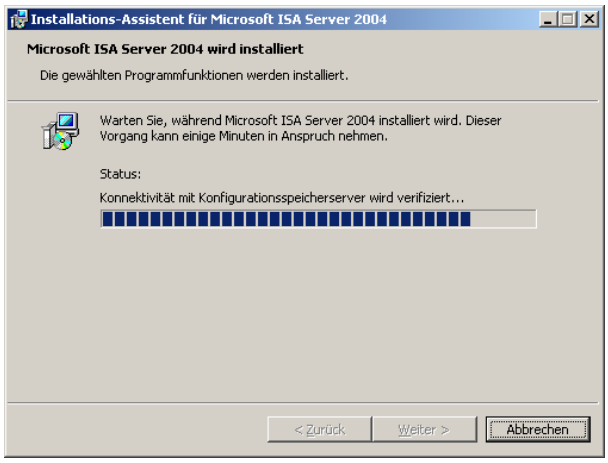
Alle weiteren CSS werden als Replikatserver (Replikat der Unternehmenskonfiguration) erstellt, d.h. alle bisherigen Konfigurationen werden vom ersten CSS repliziert. In der Folge sind nur die von der erstmaligen CSS-Installation abweichenden Punkte dargestellt:

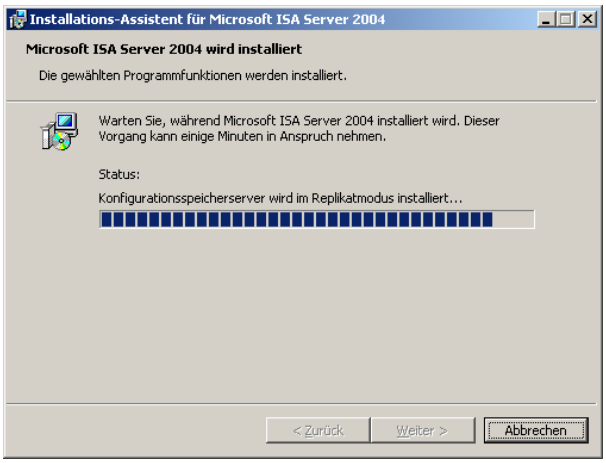










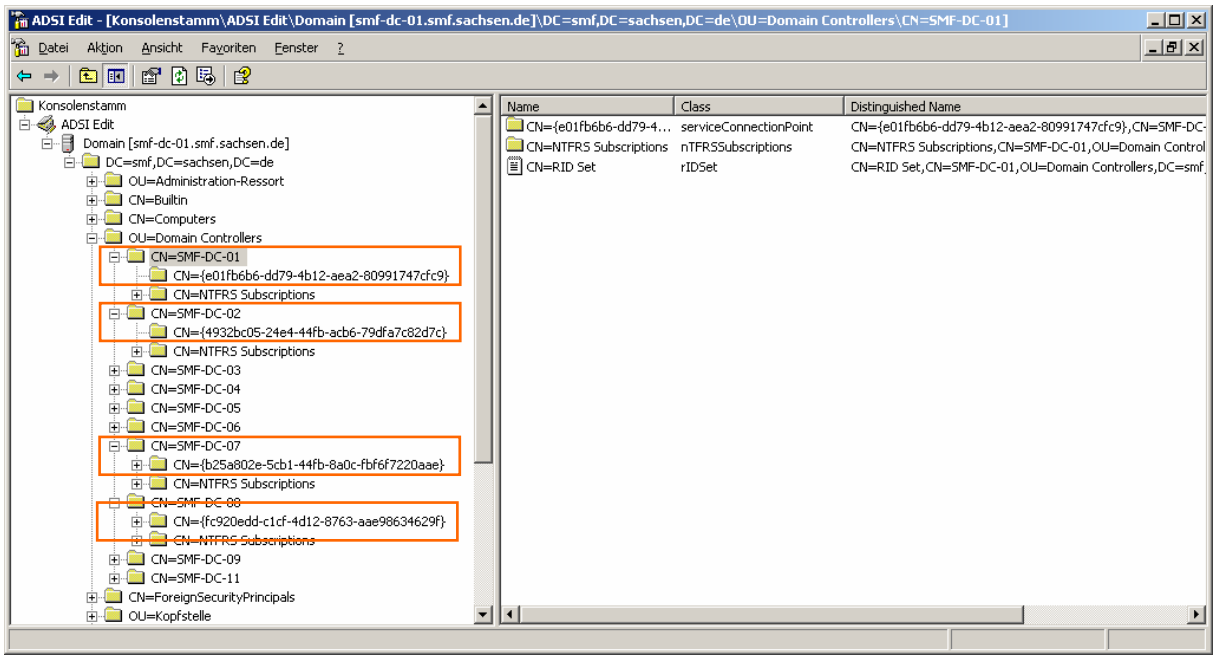


Abschließend ist wieder die Datei „smf.sachsen.de.bat“ zu starten:

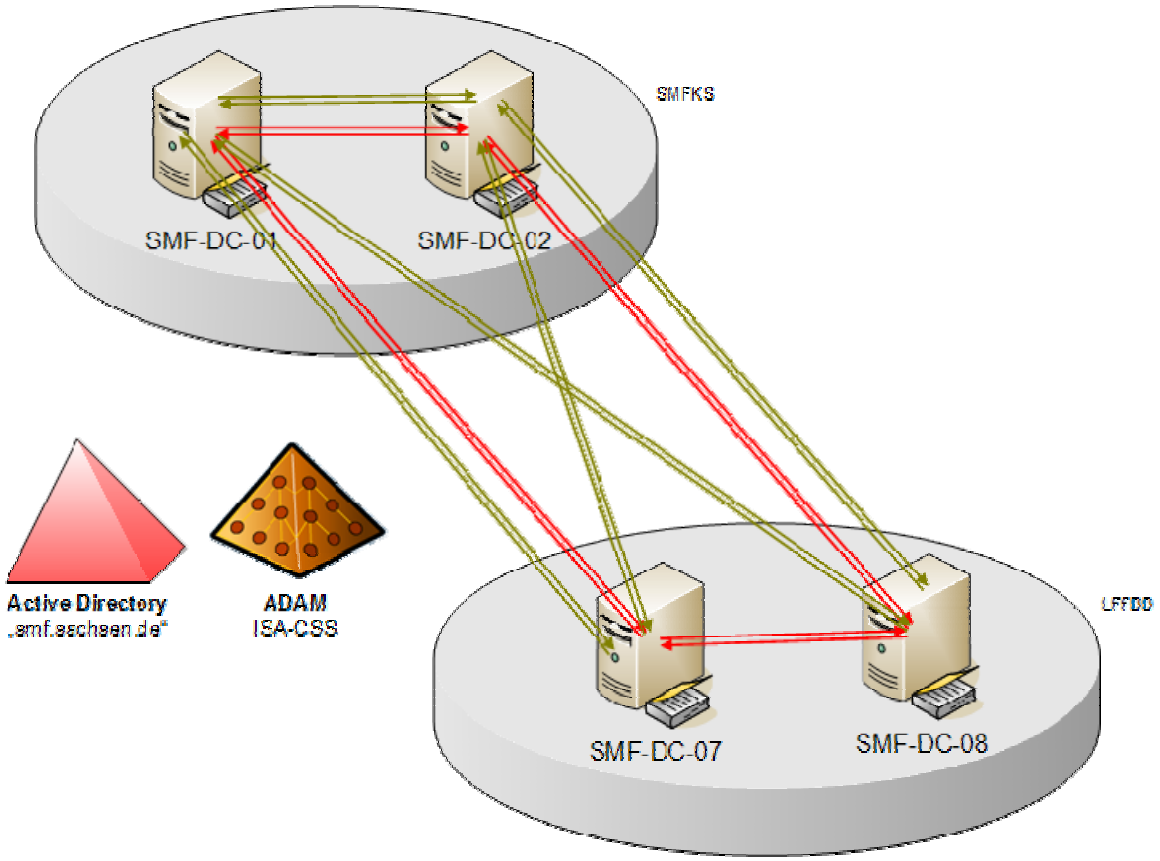
```
D:\Microsoft ISA Server\ADAMData>smf.sachsen.de.bat

D:\Microsoft ISA Server\ADAMData>C:\WINNT\ADAM\repadmin.exe /writespn smf.sachsen.de ADD
"CN=ISA 2004 CSS,OU=Administration-Ressort,DC=smf,DC=sachsen,DC=de" E3514235-4B06-11D1-AB04-
00C04FC2DCD2-ADAM/SMF-DC-02:2171
Die angeforderten SPNs wurden erfolgreich geschrieben.

D:\Microsoft ISA Server\ADAMData>C:\WINNT\ADAM\repadmin.exe /writespn smf.sachsen.de ADD
"CN=ISA 2004 CSS,OU=Administration-Ressort,DC=smf,DC=sachsen,DC=de" E3514235-4B06-11D1-AB04-
00C04FC2DCD2-ADAM/smf-dc-02.smf.sachsen.de:2171
Die angeforderten SPNs wurden erfolgreich geschrieben.

D:\Microsoft ISA Server\ADAMData>C:\WINNT\ADAM\repadmin.exe /writespn smf.sachsen.de ADD
"CN=ISA 2004 CSS,OU=Administration-Ressort,DC=smf,DC=sachsen,DC=de" ldap/SMF-DC-02:2171
Die angeforderten SPNs wurden erfolgreich geschrieben.

D:\Microsoft ISA Server\ADAMData>C:\WINNT\ADAM\repadmin.exe /writespn smf.sachsen.de ADD
"CN=ISA 2004 CSS,OU=Administration-Ressort,DC=smf,DC=sachsen,DC=de" ldap/smf-dc-
02.smf.sachsen.de:2171
Die angeforderten SPNs wurden erfolgreich geschrieben.

D:\Microsoft ISA Server\ADAMData>
```

Diese Schritte sind auf allen als CSS genutzten Domänencontrollern ebenfalls durchzuführen.

Nach Abschluss der CSS-Installationen sollten alle „ServiceConnectionPoints“ und die „ServicePrincipaleNames“ angelegt sein:



Durch das ADAM (KCC und ISTG) wurde automatisch die in der nächsten Grafik abgebildete Replikationstopologie (rot=AD, braun=ADAM) erstellt. Hierbei sind alle CSS in einem Standort zusammengefasst. Zur Optimierung der Replikation können mit Hilfe des Tools „adamsites.exe“ weitere Standorte und Standortverknüpfungen angelegt werden.



3.5 Optimierung der Replikationstopologie mittels „adamsites.exe“

Durch Verwendung des Kommandozeilentools „adamsites.exe“ (http://www.microsoft.com/isaserver/downloads/2004/default.mspx) kann die Replikationstopologie der CSS konfiguriert und verbessert werden. Mit Hilfe dieses Tools sollen in ADAM

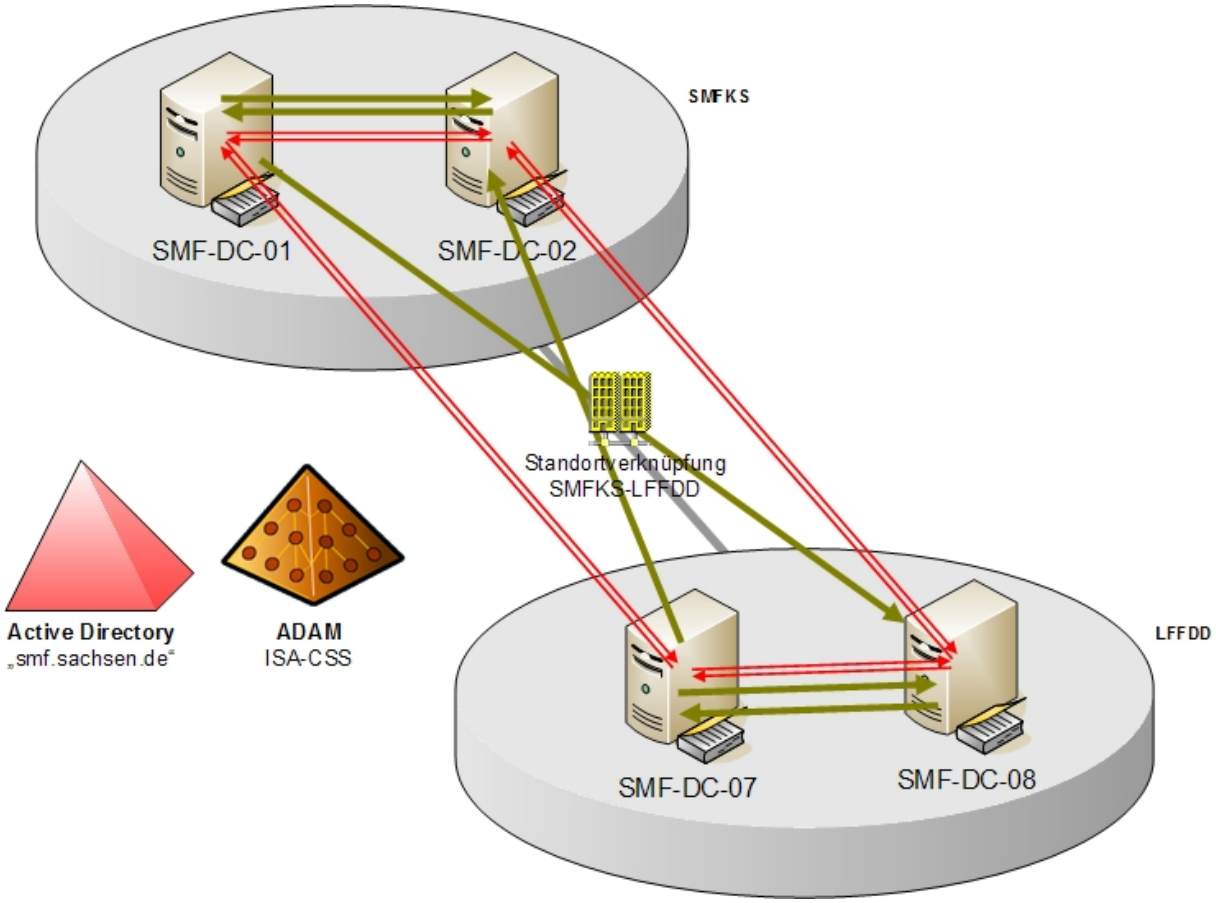
- zwei neue Standorte angelegt,
- ein Standort gelöscht (Default „Standardname des ersten Standortes“),
- Sitelinks gelöscht bzw. erstellt und
- die Server in ihre entsprechenden Sites verschoben werden.

Abschließend wird diese Konfiguration gesichert.

```
D:\Microsoft ISA Server>AdamSites Sites
Site: Default-First-Site-Name
There are 4 servers in this site.
        SMF-DC-01
        SMF-DC-02
        SMF-DC-07
        SMF-DC-08

D:\Microsoft ISA Server>AdamSites Backup D:\ISA_EE_Configuration_default.bak

D:\Microsoft ISA Server>AdamSites Site Create SMFKS
Site created successfully.
To allow connectivity to this site, create a site link that connects
this site to existing sites.

D:\Microsoft ISA Server>AdamSites Site Create LFFDD
Site created successfully.
To allow connectivity to this site, create a site link that connects
this site to existing sites.

D:\Microsoft ISA Server>AdamSites Sites
Site: Default-First-Site-Name
There are 4 servers in this site.
        SMF-DC-01
        SMF-DC-02
        SMF-DC-07
        SMF-DC-08
Site: LFFDD
There are no servers in this site.
Site: SMFKS
There are no servers in this site.

D:\Microsoft ISA Server>AdamSites SiteLink Create SMFKS-LFFDD 2 SMFKS LFFDD 100 60

D:\Microsoft ISA Server>AdamSites SiteLink Create Default-First-Site-Name-SMFKS 2 Default-
First-Site-Name SMFKS 100 60

D:\Microsoft ISA Server>AdamSites MoveServer SMF-DC-07 Default-First-Site-Name LFFDD

D:\Microsoft ISA Server>AdamSites MoveServer SMF-DC-08 Default-First-Site-Name LFFDD

D:\Microsoft ISA Server>AdamSites MoveServer SMF-DC-01 Default-First-Site-Name SMFKS

D:\Microsoft ISA Server>AdamSites MoveServer SMF-DC-02 Default-First-Site-Name SMFKS

D:\Microsoft ISA Server>AdamSites Sites
Site: Default-First-Site-Name
There are no servers in this site.
Site: LFFDD
There are 2 servers in this site.
        SMF-DC-07
        SMF-DC-08
Site: SMFKS
There are 2 servers in this site.
        SMF-DC-01
        SMF-DC-02

D:\Microsoft ISA Server>AdamSites SiteLink View SMFKS-LFFDD
```

```
Site Link: SMFKS-LFFDD
        Cost:100
        Replication Interval:60
        Description:CN=SMFKS-LFFDD
        Sites:
                LFFDD
                SMFKS

D:\Microsoft ISA Server>AdamSites SiteLink Delete Default-First-Site-Name-SMFKS

D:\Microsoft ISA Server>AdamSites Site Delete Default-First-Site-Name

D:\Microsoft ISA Server>AdamSites SiteLink Delete Defaultipsitelink

D:\Microsoft ISA Server>AdamSites Sites
Site: LFFDD
There are 2 servers in this site.
        SMF-DC-07
        SMF-DC-08
Site: SMFKS
There are 2 servers in this site.
        SMF-DC-01
        SMF-DC-02

D:\Microsoft ISA Server>AdamSites Sitelinks
Site Link: SMFKS-LFFDD
        Cost:100
        Replication Interval:60
        Description:CN=SMFKS-LFFDD
        Sites:
                LFFDD
                SMFKS

D:\Microsoft ISA Server>AdamSites Backup D:\ISA_EE_Configuration_Running.bak

D:\Microsoft ISA Server>
```

Die angelegte Replikationstopologie stellt sich so dar:



Diese Informationen können auch mittels ADAM ADSI Edit überprüft werden. Dabei müssen Verbindungen zu den drei vom ISA CSS verwendeten Namenskontexten hergestellt werden: