

DNS Einträge

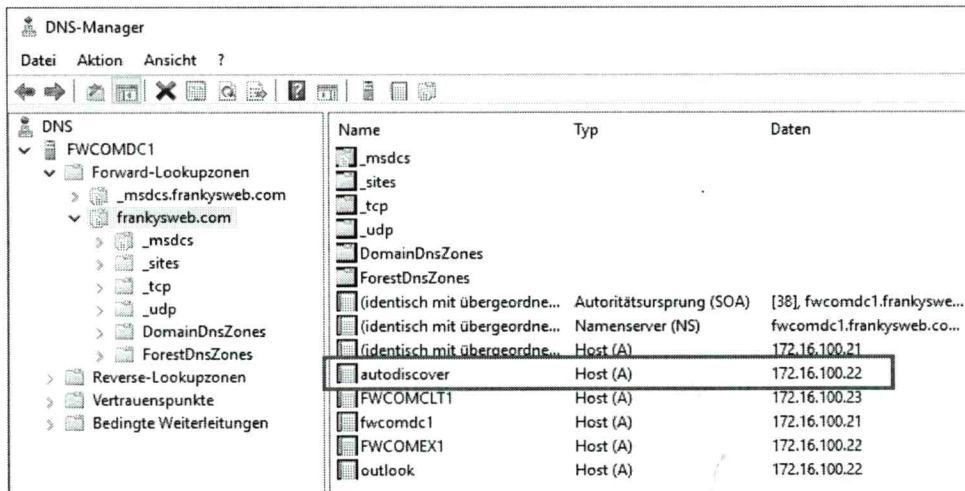
Im Wesentlichen gibt es drei Möglichkeiten Autodiscover per DNS verfügbar zu machen.

Da Outlook eine feste Namenskonvention für Autodiscover voraussetzt, sollten nur in besonderen Fällen andere DNS Namen verwendet werden. Ein DNS HOST-A oder CNAME Eintrag sollte daher unbedingt „autodiscover.domain.tld“ lauten, für den SRV Eintrag gilt „_autodiscover._tcp.domain.tld“.

HOST-A und SRV Eintrag lassen sich parallel nutzen. Eine parallele Nutzung von CNAME und HOST-A ist nicht möglich.

HOST-A

Der HOST-A Eintrag verweist direkt auf die IP-Adresse eines Exchange Servers von dem die Autodiscover.xml abgerufen werden kann. Der folgende Screenshot zeigt den Autodiscover Eintrag für die Domain frankysweb.com:



In Organisationen mit mehreren Exchange Servern kann hier auch die IP-Adresse eines Loadbalancers angegeben werden. Der Loadbalancer muss dann die Anfrage des Clients an einen Exchange Server weiterleiten.

Es ist ebenfalls möglich mehrere HOST-A Einträge mit dem Namen „autodiscover“ anzulegen, die auf unterschiedliche IP-Adressen verweisen. Mittels DNS-Roundrobin lässt sich so eine rudimentäre Form der Lastverteilung zwischen zwei Exchange Servern realisieren. Der folgende Screenshot zeigt eine DNS-Roundrobin Konfiguration mit zwei Exchange Servern.

The screenshot shows the DNS Manager interface with the hierarchy expanded to **FWCOMDC1 > Forward-Lookupzonen > _msdcs.frankysweb.com > _msdcs**. The right pane displays a list of DNS records:

Name	Typ	Daten
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(identisch mit übergeordne...	Autoritätsursprung (SOA)	[39], fwcomdc1.frankysweb.com
(identisch mit übergeordne...	Namensserver (NS)	fwcomdc1.frankysweb.com
(identisch mit übergeordne...	Host (A)	172.16.100.21
autodiscover	Host (A)	172.16.100.23
autodiscover	Host (A)	172.16.100.22
FWCOMCLT1	Host (A)	172.16.100.23
fwcomdc1	Host (A)	172.16.100.21
FWCOMEX1	Host (A)	172.16.100.22
outlook	Host (A)	172.16.100.22

Below the DNS Manager, a command prompt shows the results of two `nslookup` commands for `autodiscover.frankysweb.com`:

```
C:\>nslookup autodiscover.frankysweb.com
Server: localhost
Address: ::1

Name: autodiscover.frankysweb.com
Addresses: 172.16.100.23
           172.16.100.22

C:\>nslookup autodiscover.frankysweb.com
Server: localhost
Address: ::1

Name: autodiscover.frankysweb.com
Addresses: 172.16.100.22
           172.16.100.23
```

Bei der DNS-Abfrage ändert sich via RoundRobin die bevorzugte IP-Adresse.

SRV

Ein SRV Record ist ein DNS Eintrag zur Dienstidentifizierung. Der SRV-Eintrag enthält also Informationen zu einem Dienst/Service der auf einem Host läuft. Bei einem SRV-Eintrag müssen der Name des Dienstes, das Protokoll, die Portnummer und der Host angegeben werden auf dem der jeweilige Dienst läuft. Das folgende Beispiel zeigt den Autodiscover SRV Eintrag für frankysweb.com

The screenshot shows the DNS Manager interface with the hierarchy expanded to **FWCOMDC1 > Forward-Lookupzonen > _msdcs.frankysweb.com > _msdcs**. The right pane displays a list of DNS records:

Name	Typ	Daten
_gc	Dienstidentifizierung (SRV)	[0][100][3268] FWCOMDC1.frankysweb.com.
_kerberos	Dienstidentifizierung (SRV)	[0][100][88] FWCOMDC1.frankysweb.com.
_kpasswd	Dienstidentifizierung (SRV)	[0][100][464] FWCOMDC1.frankysweb.com.
_ldap	Dienstidentifizierung (SRV)	[0][100][389] FWCOMDC1.frankysweb.com.
_autodiscover	Dienstidentifizierung (SRV)	[0][100][443] FWCOMEX1.frankysweb.com.

The **Eigenschaften von _autodiscover** dialog box is open, showing the following details:

- Dienstidentifizierung (SRV) - Sicherheit
- Domäne: frankysweb.com
- Dienst: _autodiscover
- Protokoll: _tcp
- Priorität: 0
- Gewichtung: 100
- Portnummer: 443
- Host, der diesen Dienst anbietet: FWCOMEX1.frankysweb.com

Wie im Screenshot zu sehen ist, verweist der SRV-Eintrag für Autodiscover auf einem Server der Autodiscover anbietet (EXCHANGESERVER.frankysweb.com), ähnlich wie eine Weiterleitung. Dieser Eintrag sorgt dafür, dass Outlook die Autodiscover.xml vom Server FWCOMEX1 abrufen.

Der SRV Eintrag kann auch auf den HOST-A Eintrag autodiscover.frankysweb.com verweisen.

CNAME

Ein CNAME Eintrag, auch als Alias bezeichnet, verweist einen definierten Namen an einen definierten Host. Ein CNAME kann nicht auf mehrere Hosts verweisen. Ähnlich des SRV-Eintrags wird mittels CNAME (Alias) an einen Server weitergeleitet. Das folgende Beispiel zeigt den CNAME für frankysweb.com

The screenshot shows the DNS Manager interface for the domain frankysweb.com. The left pane shows the hierarchy: DNS > Forward-Lookupzones > _msdcs.frankysweb.com > frankysweb.com. The right pane shows the list of records. The record 'autodiscover' is highlighted, showing it is an Alias (CNAME) pointing to 'FWCOMEX1.frankysweb.com'.

Name	Typ	Daten
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(identisch mit übergeordnete...)	Autoritätsursprung (SOA)	[39], fwcomdc1.frankysweb.com., hostmaster
(identisch mit übergeordnete...)	Namenserver (NS)	fwcomdc1.frankysweb.com.
(identisch mit übergeordnete...)	Host (A)	172.16.100.21
FWCOMCLT1	Host (A)	172.16.100.23
fwcomdc1	Host (A)	172.16.100.21
FWCOMEX1	Host (A)	172.16.100.22
outlook	Host (A)	172.16.100.22
autodiscover	Alias (CNAME)	FWCOMEX1.frankysweb.com

Below the DNS Manager, a command prompt shows the command 'nslookup autodiscover.frankysweb.com' and its output:

```
C:\Users\Administrator>nslookup autodiscover.frankysweb.com
Server: localhost
Address: ::1

Name:    FWCOMEX1.frankysweb.com
Address: 172.16.100.22
Aliases: autodiscover.frankysweb.com
```

Zertifikat

Da Outlook für den Abruf der Autodiscover.xml eine HTTPs Verbindung zugrunde legt, muss Exchange Server über ein SSL-Zertifikat verfügen, welches Outlook als gültig akzeptiert.

Damit Outlook ein Zertifikat als gültig akzeptiert und keine Warnungen anzeigt, müssen folgende Bedingungen erfüllt sein:

- Das Zertifikat wurde von einer vertrauenswürdigen Stammzertifizierungsstelle ausgestellt
- Das Zertifikat befindet sich innerhalb des Gültigkeitszeitraum
- Alle DNS-Namen die Outlook für den Zugriff benutzt, sind auf dem Zertifikat vorhanden (siehe Kapitel Konfiguration / Exchange Server)

Stammzertifizierungsstelle

Das Zertifikat muss von einer vertrauenswürdigen Stammzertifizierungsstelle ausgestellt werden. Interne Zertifizierungsstellen müssen dem Windows Zertifikatsspeicher für vertrauenswürdige Stammzertifizierungsstellen hinzugefügt werden.

The screenshot shows the 'Zertifikate (Lokaler Computer)' window in Windows. The left pane shows the hierarchy: Zertifikate > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate. The right pane shows the list of trusted root certificates, including 'Baltimore CyberTrust Root', 'Class 3 Public Primary Certification...', 'Copyright (c) 1997 Microsoft Corp.', 'FWCA', 'FWEX1', 'GlobalSign', 'Microsoft Authenticode(tm) Root...', 'Microsoft Root Authority', 'Microsoft Root Certificate Authority...', 'Microsoft Root Certificate Authority...', 'Microsoft Root Certificate Authority...', 'NO LIABILITY ACCEPTED, (c)97 Ve...', 'Symantec Enterprise Mobile Root...', 'thawte Primary Root CA', 'Thawte Timestamping CA', 'UTN-USERSFirst-Object', 'VeriSign Class 3 Public Primary...', and 'WMSvc-SHA2-FWEX1'.