


Übungsprotokoll

SYTS – Systemintegration und Infrastruktur

	Übungsdatum: KW 50/2022 – KW /2022	Klasse: 4AHIT	Name: Felix Schneider
	Abgabedatum: 11.10.2022	Gruppe: SYTS_2	Note:
Leitung: DI (FH) Alexander MESTL	Mitübende: -		
Übungsbezeichnung: Standorte, ausgekreuzte DNS und mehr			

Inhaltsverzeichnis:

1	Aufgabenstellung.....	3
2	Abstract (English).....	3
3	Theoretische Grundlagen.....	4
3.1	Auskreuzen der DNS-Server	4
4	Übungsdurchführung.....	5
4.1	Ersten Domaincontroller aufsetzen	5
4.1.1	AD, DHCP, DNS	5
4.2	Zweiten Domaincontroller aufsetzen	5
4.2.1	IP-Adressen	5
4.2.2	Features installieren.....	5
4.2.3	Zum DC hochstufen.....	5
4.2.4	Features konfigurieren	6
4.2.4.1	DHCP (Failover).....	6
4.2.4.2	DNS.....	6
4.2.4.3	Fertig?.....	7
4.3	Standorte konfigurieren.....	8
4.3.1	Standort umbenennen	8
4.3.2	Neuen Standort hinzufügen.....	8
4.3.3	Subnetze hinzufügen.....	9
4.4	Dritten Domaincontroller aufsetzen	10
4.4.1	Standardinstallation	10
4.4.2	Zum Standort hinzufügen	10
4.4.3	DHCP und DNS.....	10
4.5	Remote Verbindung aufbauen	10
4.5.1	Transfer Net	10
4.5.2	Remotezugriff.....	10
4.5.3	Routing und RAS	10
4.5.3.1	Statische Route konfigurieren	12
4.5.4	Zum RODC hochstufen	13

1 Aufgabenstellung

Wir werden in unserem bisher existierenden "Default-Standort" einen zweiten DC aufsetzen - das ist aus Sicherheitsgründen ohnehin zu empfehlen (eigentlich ein "Muss") und außerdem können wir dadurch dann die standort-interne Replikation analysieren.

Als nächsten Schritt werden wir einen zweiten (sozusagen "entfernten") Standort anlegen, beiden dann existierenden Standorten vernünftige Namen geben und am neuen Standort einen "Read-Only-DC" in Betrieb nehmen. Damit werden wir dann die standort-übergreifende Replikation beobachten.

Literatur-Tipps: Server 2019-Buch, Kapitel 7.4, 7.6 und 11 (zu finden unter den "Dateien")

2 Abstract (English)

We will set up a second DC in our existing "default site" - this is recommended for security reasons anyway (actually a "must") and also allows us to analyze the site-internal replication.

As a next step, we will create a second (so to speak "remote") site, give both then existing sites reasonable names and put a "read-only DC" into operation at the new site. We will then use this to observe cross-site replication.

Literature tips: Server 2019 book, chapters 7.4, 7.6 and 11 (found under the "Files").

3 Theoretische Grundlagen

3.1 Auskreuzen der DNS-Server

Folgendes Setup:

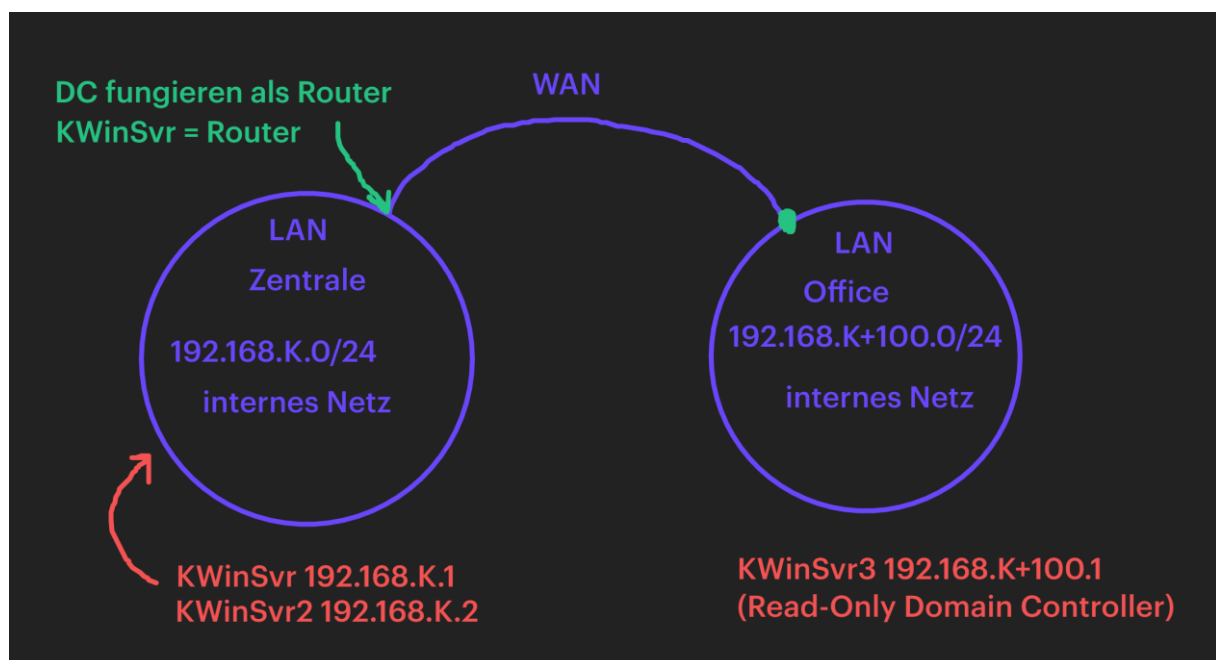
	Primäre DNS-Server	Sekundäre DNS-Server
Domain-Controller 1 192.168.23.1	192.168.23.2	192.168.23.1
Domain-Controller 2 192.168.23.2	192.168.23.1	192.168.23.2

Was Sie bei diesem Setup erkennen könnte, ist, dass die Server immer gegenseitig als primären DNS-Server auf den anderen DNS-Server verweisen und erst der sekundäre DNS-Server ist man selbst. Folgendes Setup würde das gleiche Ergebnis erzielen:

	Primäre DNS-Server	Sekundäre DNS-Server
Domain-Controller 1 192.168.23.1	192.168.23.2	127.0.0.1
Domain-Controller 2 192.168.23.2	192.168.23.1	127.0.0.1

Der Grund für dieses „Auskreuzen“ ist die Sicherheit und Aufrechterhaltung eines Servers bei einem Ausfall des anderen.

Das prinzipielle Setup unseres Netzes mit zwei Standorten sieht so aus:



4 Übungsdurchführung

4.1 Ersten Domaincontroller aufsetzen

Einfach einen neuen Domaincontroller aufsetzen, falls dieser noch nicht vorhanden ist.

4.1.1 AD, DHCP, DNS

Konfigurieren Sie alle Dienste standardmäßig. Später kann es sein, dass diese nochmals verändert werden.

4.2 Zweiten Domaincontroller aufsetzen

4.2.1 IP-Adressen

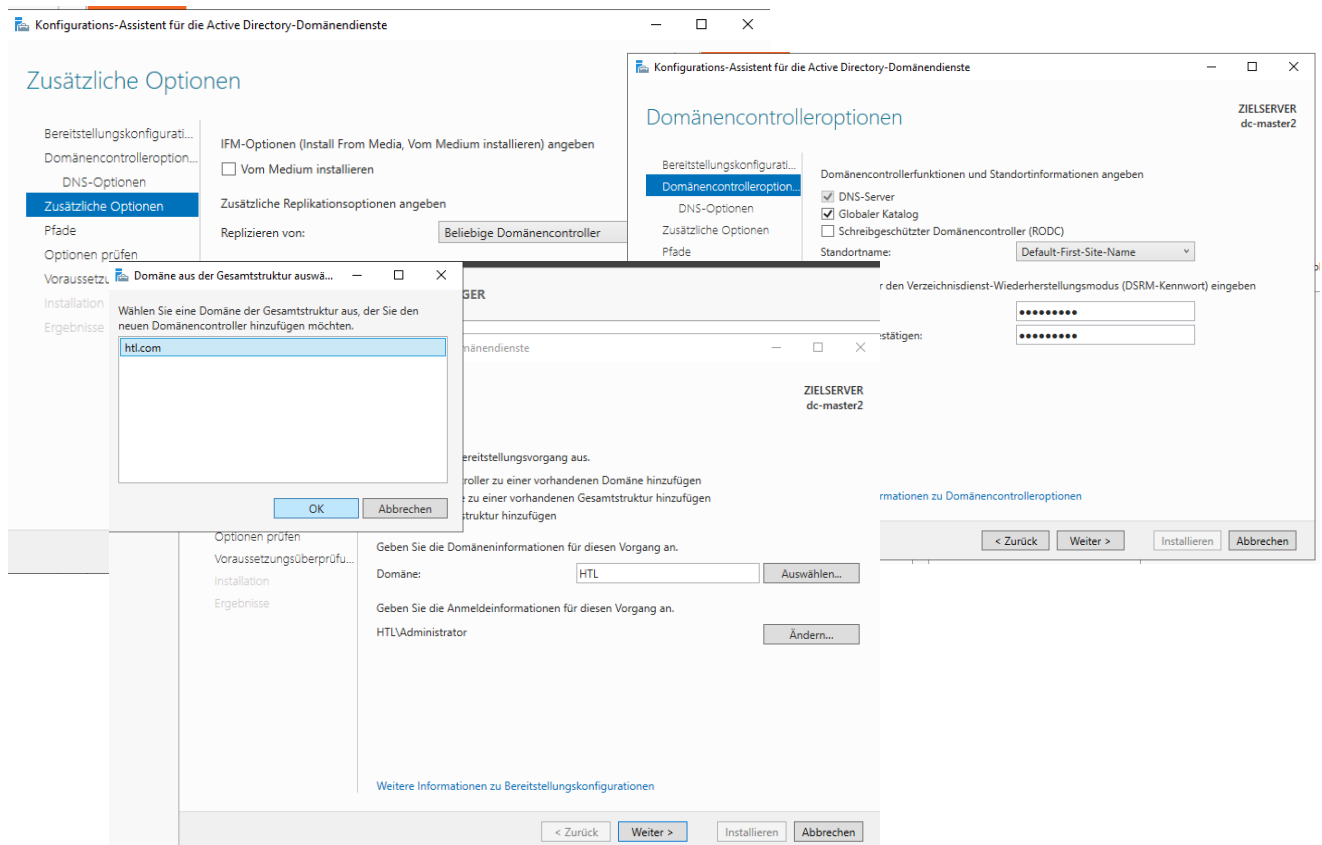
Konfigurieren Sie die IP-Adressen der internen Netzwerkkarten wie in [obiger Anleitung](#).

4.2.2 Features installieren

Installieren Sie AD, DHCP und DNS.

4.2.3 Zum DC hochstufen

Treten Sie dafür der bereits erstellten Domain bei – wie in den Screenshots dargestellt. Neustarts helfen bei Nichtfunktionalität.



4.2.4 Features konfigurieren

4.2.4.1 DHCP (Failover)

Konfigurieren Sie bei DHCP einen gemeinsamen Adresspool, der zwischen den Servern synchronisiert wird. Dies machen Sie, indem Sie DHCP am Server 2 absichtliche NICHT konfigurieren. Anschließend gehen Sie zum Server 1 und stellen folgendermaßen ein, dass mit Server 2 ein Failover konfiguriert wird.

Stellen Sie den Partnerserver ein und erstellen Sie auch einen gemeinsamen geheimen Schlüssel (12346789).

Failover konfigurieren

Den Partnerserver angeben, der für Failover verwendet werden soll

Geben Sie den Hostnamen oder die IP-Adresse des DHCP-PartnerServers an, mit dem das Failover konfiguriert werden soll.

Sie können einen Server in der Liste der Server mit einer vorhandenen Failoverkonfiguration auswählen, oder Sie können die Liste der autorisierten DHCP-Server durchsuchen und in dieser Liste einen Server auswählen.

Alternativ können Sie den Hostnamen oder die IP-Adresse des PartnerServers eingeben.

Partnerserver:

☐ Vorhandene Failoverbeziehungen, die mit diesem Server konfiguriert sind, wiederverwenden

Failover konfigurieren

Neue Failoverbeziehung erstellen

Erstellen Sie eine neue Failoverbeziehung mit dem Partner "dc-master2.htl.com".

Name der Beziehung:

Maximale Clientvorlaufzeit: Stunde Minuten

Modus:

☐ Lastenausgleich in Prozent
 Lokaler Server: %
 Partnerserver: %

☐ Intervall für Zustands-Switchover: Minuten

☒ Nachrichtenauthentifizierung aktivieren

Gemeinsamer geheimer Schlüssel:

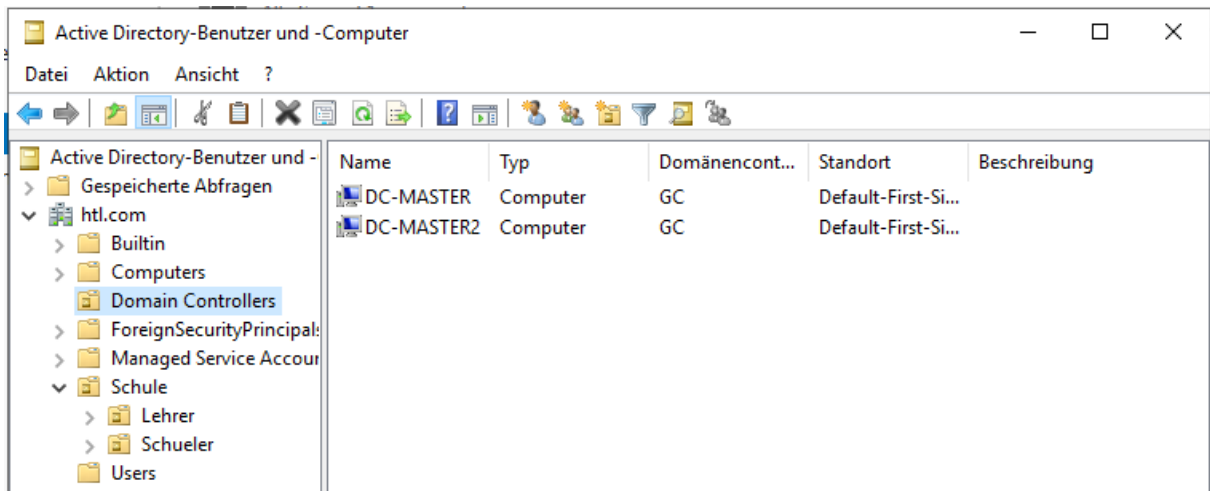
Anschließend wählen Sie die Option Failover-Bereich replizieren aus.

4.2.4.2 DNS

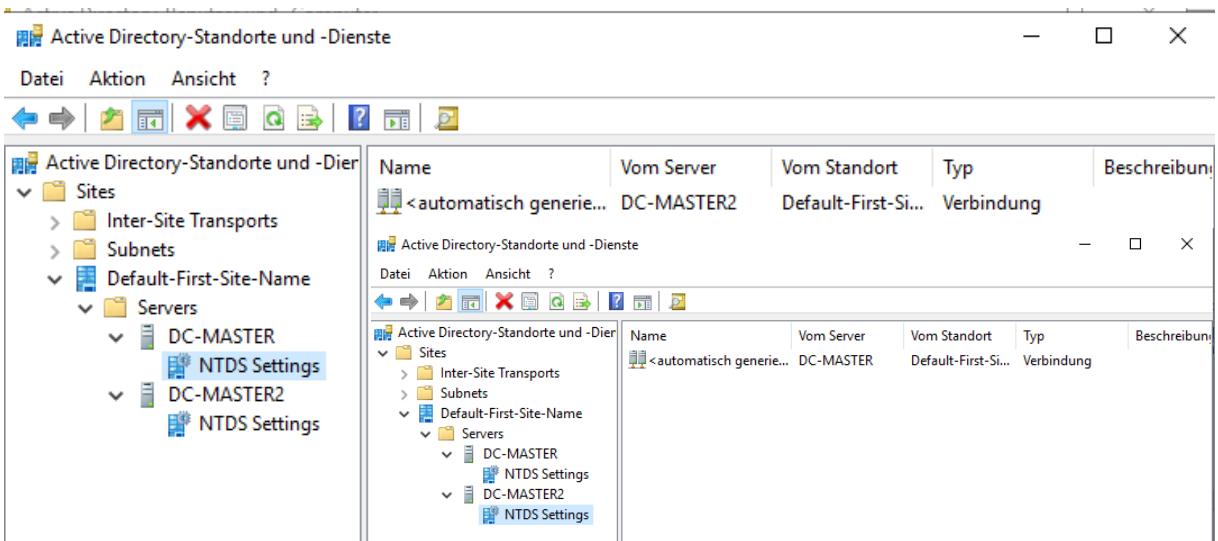
DNS muss nicht weiters konfiguriert werden.

4.2.4.3 Fertig?

Nach diesen Konfigurationen sollten unter AD-DC beide Domain Controller auftauchen:



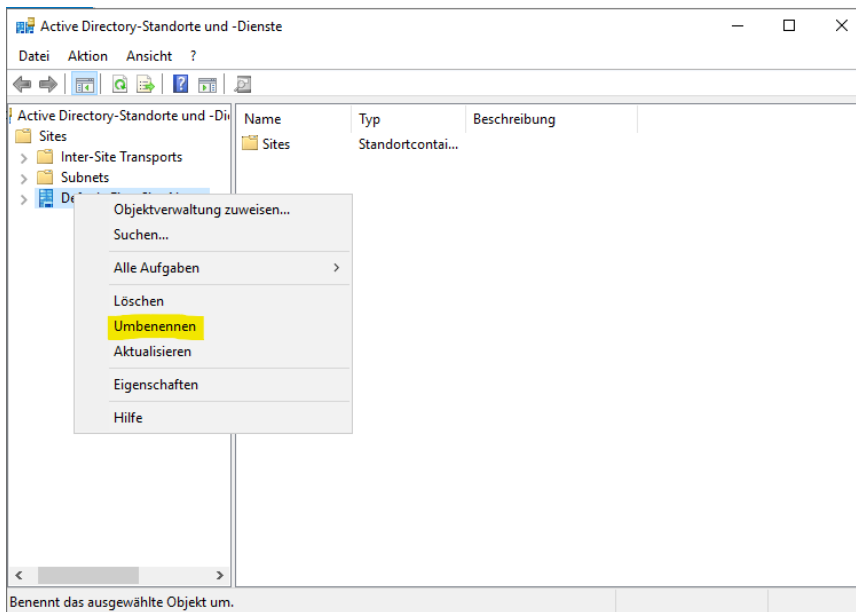
Darüber hinaus finden Sie in den Standorten und Diensten zwei Server, die sich gegenseitig replizieren (Achtung: Es sind zwei Screenshots ineinander). Dies ist bereits automatisch konfiguriert worden:



4.3 Standorte konfigurieren

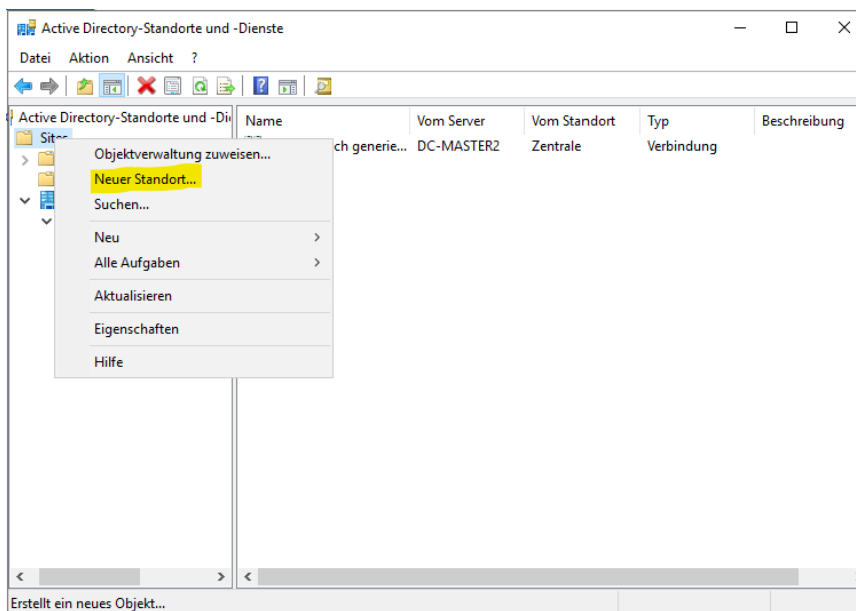
4.3.1 Standort umbenennen

Als erster nennen wir den Standort um, zum Beispiel in Zentrale.



4.3.2 Neuen Standort hinzufügen

Dann können wir einen neuen Standort namens „Office“ hinzufügen:



Wählen Sie ein Standortverknüpfungsobjekt aus, in dem die Konfigurationen, wie zum Beispiel die Replikationszeit, gespeichert sind.

Neues Objekt - Standort

Erstellen in: htl.com/Configuration/Sites

Name: Office

Wählen Sie ein Standortverknüpfungsobjekt für diesen Standort. Standortverknüpfungsobjekte finden Sie im Container für interne und standortübergreifende Transporte.

Verknüpfungsname	Transport
DEFAULTIPSITELINK	IP

OK Abbrechen

Active Directory-Domänendienste

Der Standort "Office" wurde erstellt. So schließen Sie die Konfiguration von "Office" ab:

Stellen Sie sicher, dass "Office" mit anderen Standorten über Standortverknüpfungen verknüpft ist.

Fügen Sie dem Subnetzcontainer die Subnetze für "Office" hinzu.

Installieren Sie mindestens einen Domänencontroller in "Office", oder verschieben Sie vorhandene Domänencontroller an den Standort.

Diese Meldung wird erst beim nächsten Neustart von "Active Directory-Standorte und -Dienste" wieder angezeigt.

OK Hilfe

4.3.3 Subnetze hinzufügen

Fügen Sie den beiden Standorten die Subnetze hinzu. Diesen sollten ca. so aussehen:

ZENTRALE	OFFICE
192.168.23.0/24	192.168.123.0/24

Neues Objekt - Subnetz

Erstellen in: htl.com/Configuration/Sites/Subnets

Geben Sie das Adresspräfix mithilfe der Netzwerkpräfix-Schreibweise an (Adressen-/Präfixlänge). Dabei zeigt die Präfixlänge die Anzahl der festen Bits an. Sie können entweder ein IPv4- oder ein IPv6-Subnetzpräfix eingeben.
[Weitere Informationen zum Eingeben von Adresspräfixen.](#)

IPv4-Beispiel: 157.54.208.0/20

IPv6-Beispiel: 3FFE:FFFF:0:C000::/64

Präfix: 192.168.23.0/24

Präfixname in den Active Directory-Domänendiensten: 192.168.23.0/24

Standortobjekt für dieses Präfix auswählen.

Standortname
Office
Zentrale

OK Abbrechen Hilfe

4.4 Dritten Domaincontroller aufsetzen

4.4.1 Standardinstallation

Setzen Sie einen dritten Domaincontroller als Read-Only Domain Controller auf und installieren Sie außerdem AD, DHCP und DNS.

IP-Adresse
192.168.123.1

4.4.2 Zum Standort hinzufügen

Fügen Sie diesen Domaincontroller dann zum Standort „Office“ hinzu, wenn Sie den Server zum DC hochstufen.

4.4.3 DHCP und DNS

Konfigurieren Sie die Rollen standardmäßig.

4.5 Remote Verbindung aufbauen

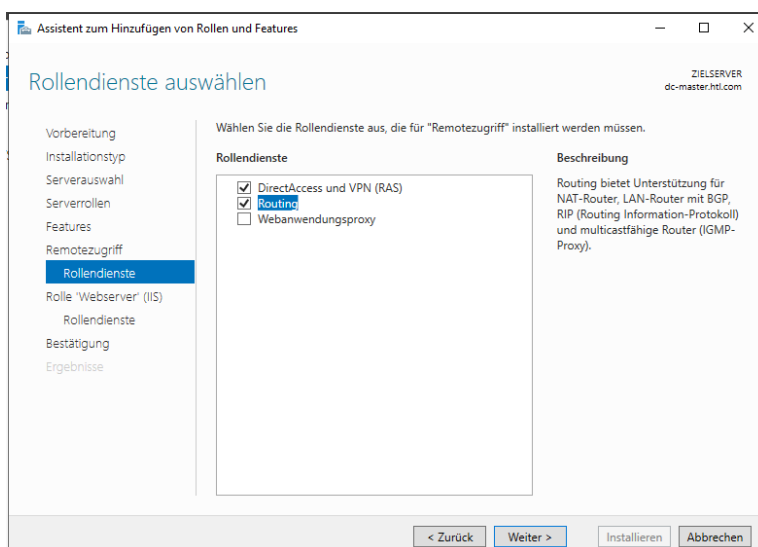
4.5.1 Transfer Net

Konfigurieren Sie eine dritte Netzwerkkarte bei DC1 und DC3, welche wiederum eigene IP-Adressen bekommen.

	DC1	DC3
Transfer Net	172.20.23.1	172.20.23.2

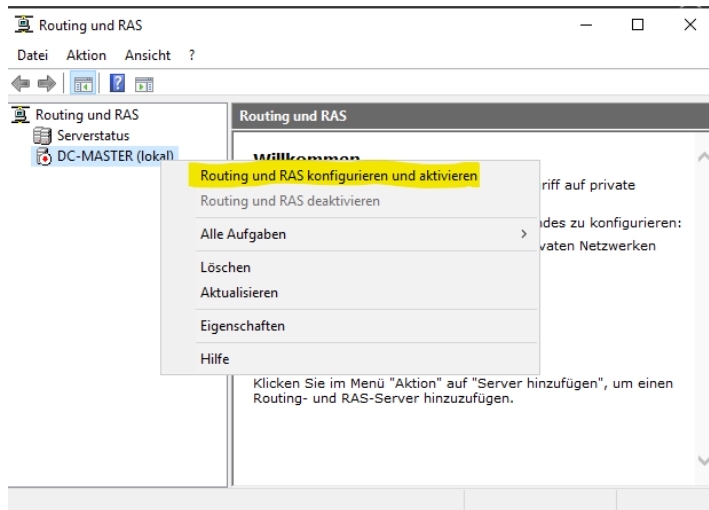
4.5.2 Remotezugriff

Installieren Sie auf DC1 und DC3 die Rolle Remoteverbindung mit folgenden Diensten:



4.5.3 Routing und RAS

Nun konfigurieren Sie noch Routing und RAS, indem Sie die gleichnamigen Tools öffnen und diese aktivieren:

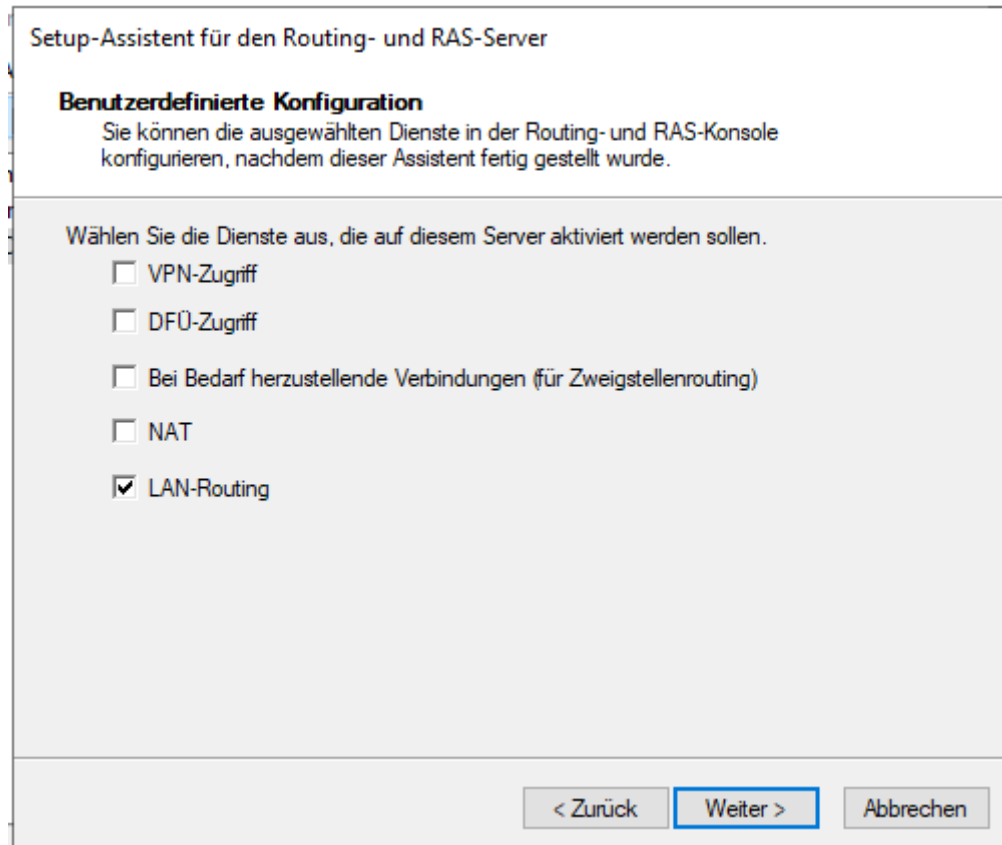


Setup-Assistent für den Routing- und RAS-Server

Konfiguration

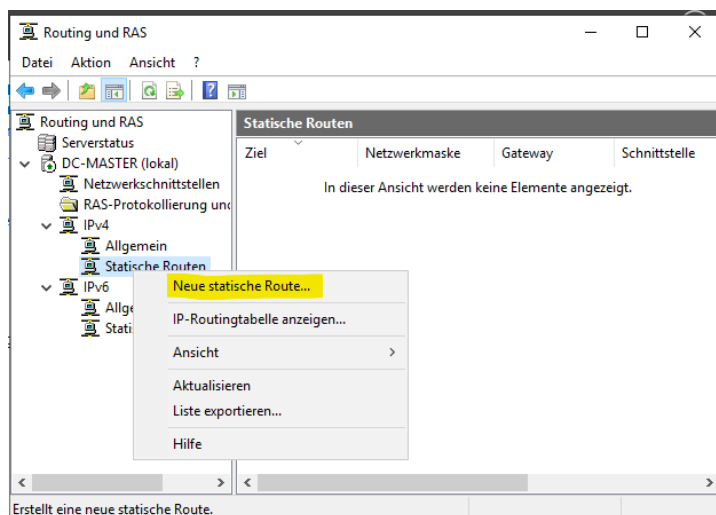
Sie können eine beliebige Kombination an Diensten wählen, oder Sie können diesen Server benutzerdefiniert anpassen.

- ☐ RAS (DFÜ oder VPN)
Ermöglicht Remoteclients, eine Verbindung mit diesem Server über eine Einwahlverbindung oder eine sichere VPN-Internetverbindung herzustellen.
- ☐ Netzwerkadressübersetzung (NAT)
Ermöglicht internen Clients, eine Internetverbindung mit einer einzelnen öffentlichen IP-Adresse herzustellen.
- ☐ VPN-Zugriff und NAT
Ermöglicht Remoteclients, eine Verbindung mit diesem Server über das Internet, und lokalen Clients eine Internetverbindung über eine einzige öffentliche IP-Adresse herzustellen.
- ☐ Sichere Verbindung zwischen zwei privaten Netzwerken
Verbindet dieses Netzwerk mit einem Remotenetzwerk, wie z.B. einer Zweigstelle.
- ☒ Benutzerdefinierte Konfiguration
Wählen Sie eine beliebige Routing- und RAS-Featurekombination aus.



4.5.3.1 Statische Route konfigurieren

Konfigurieren Sie auf dem DC1 und dem DC3 eine statische Route, die natürlich gegenseitig aufeinander verweist.



Statische IPv4-Route

Schnittstelle: Ethernet 2

Ziel: 192 . 168 . 123 . 0

Netzwerkmaske: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 23 . 1

Metrik: 256

☐ Bei Bedarf herzustellende Wählverbindungen über diese Route initiieren

OK Abbrechen

DC3:

Statische IPv4-Route

Schnittstelle: Ethernet 2

Ziel: 192 . 168 . 23 . 0

Netzwerkmaske: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 23 . 1

Metrik: 256

☐ Bei Bedarf herzustellende Wählverbindungen über diese Route initiieren

OK Abbrechen

4.5.4 Zum RODC hochstufen

Nachdem Sie die statische Route definiert haben können Sie den dritten Server zum Domain Controller hochstufen und bei der Konfiguration Read-Only auswählen.