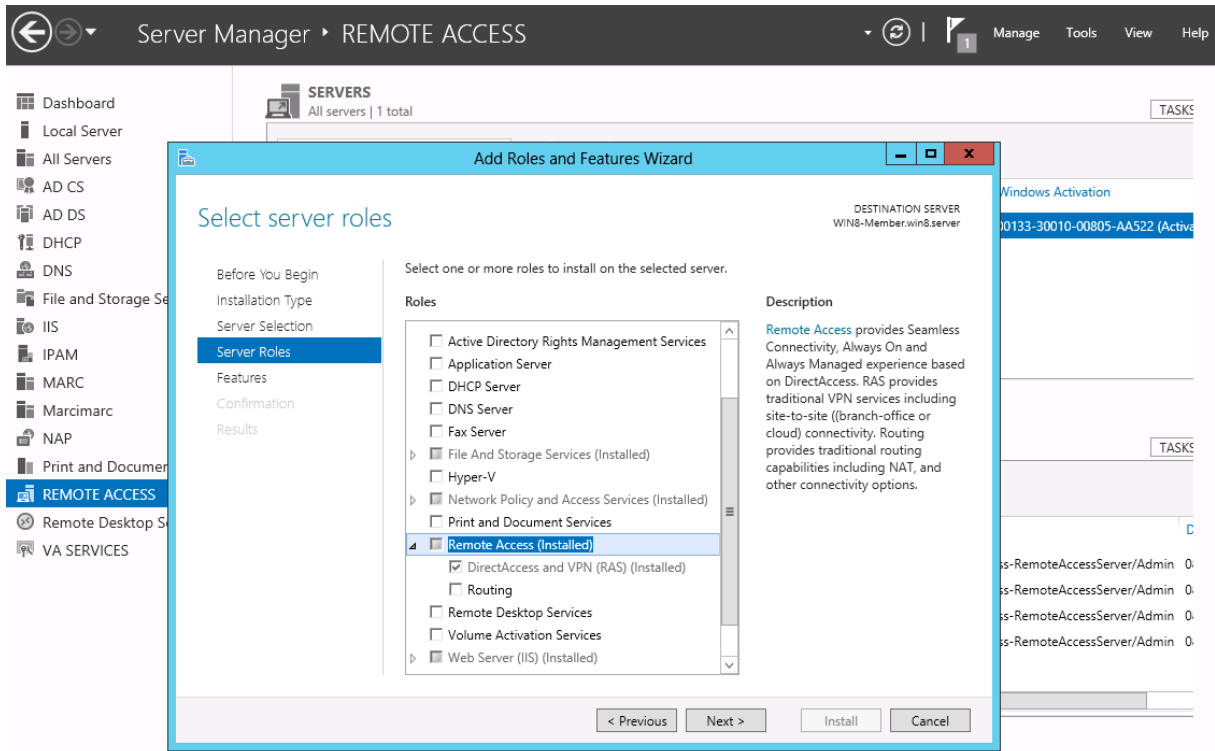
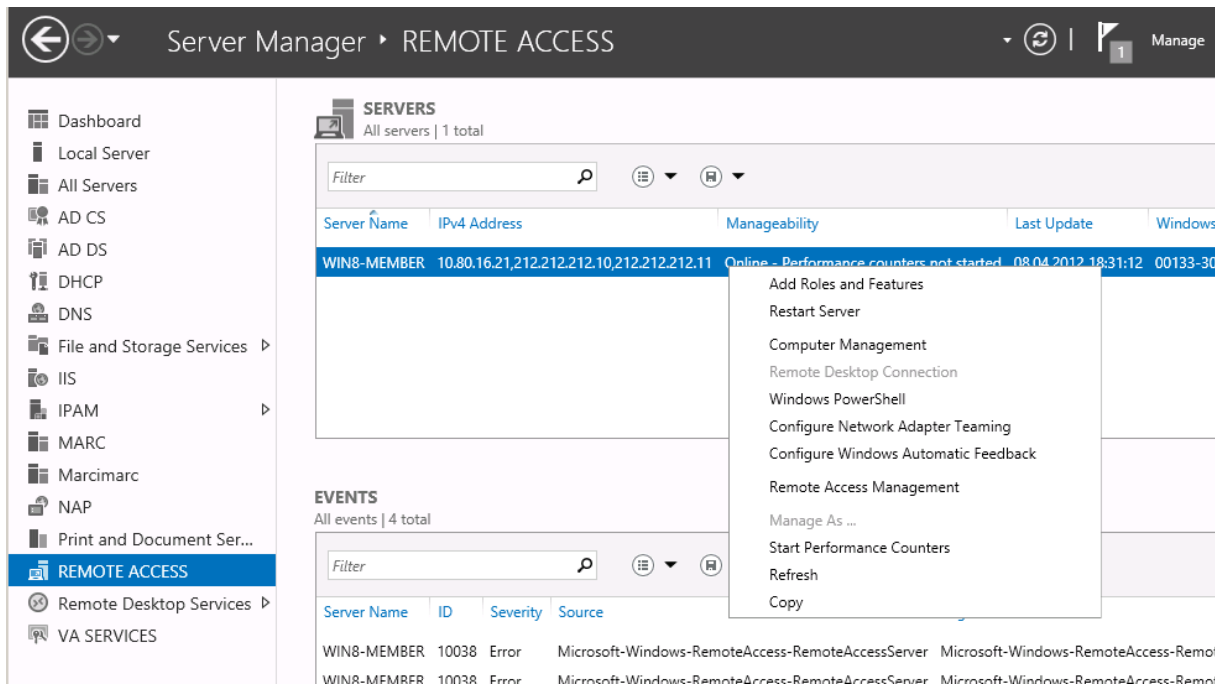


Windows Server 8 (2012?) DirectAccess

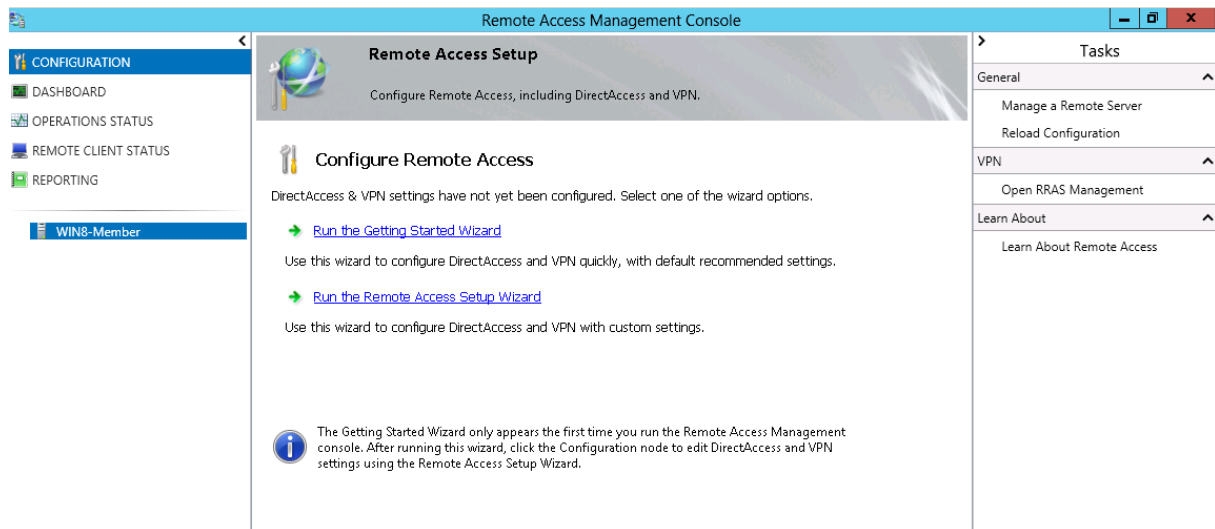
Remote Access Rolle installieren



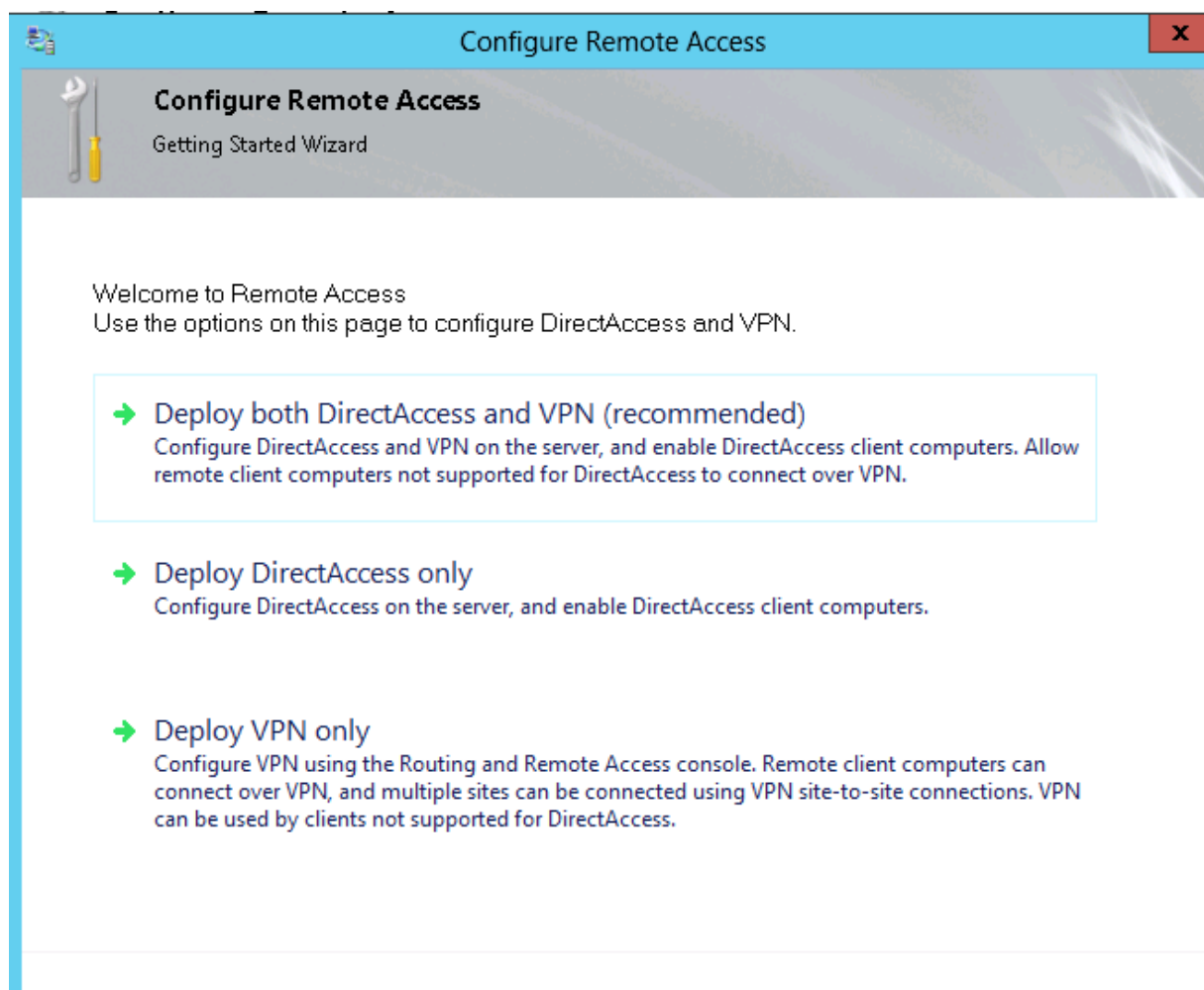
Remote Access Management starten



Remote Access Assistent kann ueber den Server Manager Wizard gestartet werden oder ueber die Remote Access Konsole



Getting Started Assistent



Configure Remote Access

Remote Access Server Setup

Configure DirectAccess and VPN settings.

Select the network topology of the server.

- Edge
- Behind an edge device (with two network adapters)
- Behind an edge device (with a single network adapter)

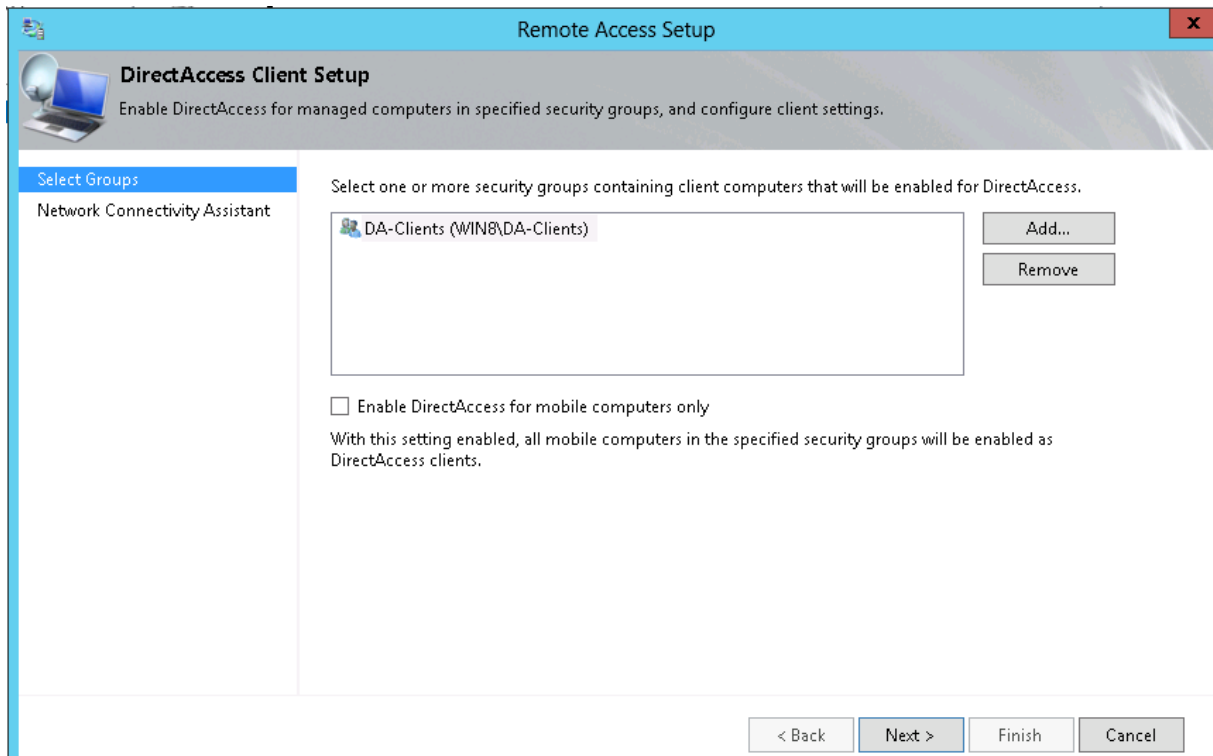
In this topology, the Remote Access server is deployed at the edge of the internal corporate network and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the Internet.

Type the public name or IPv4 address used by clients to connect to the Remote Access

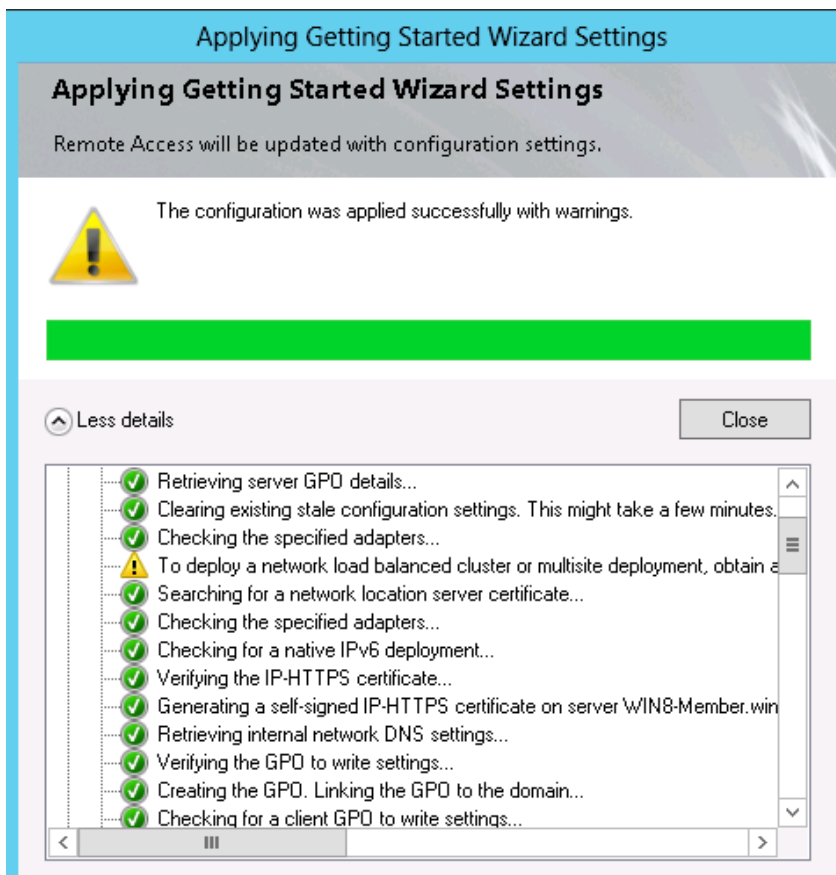
< Back Next > Finish Cancel

DirectAccess GPO Einstellungen anpassen.

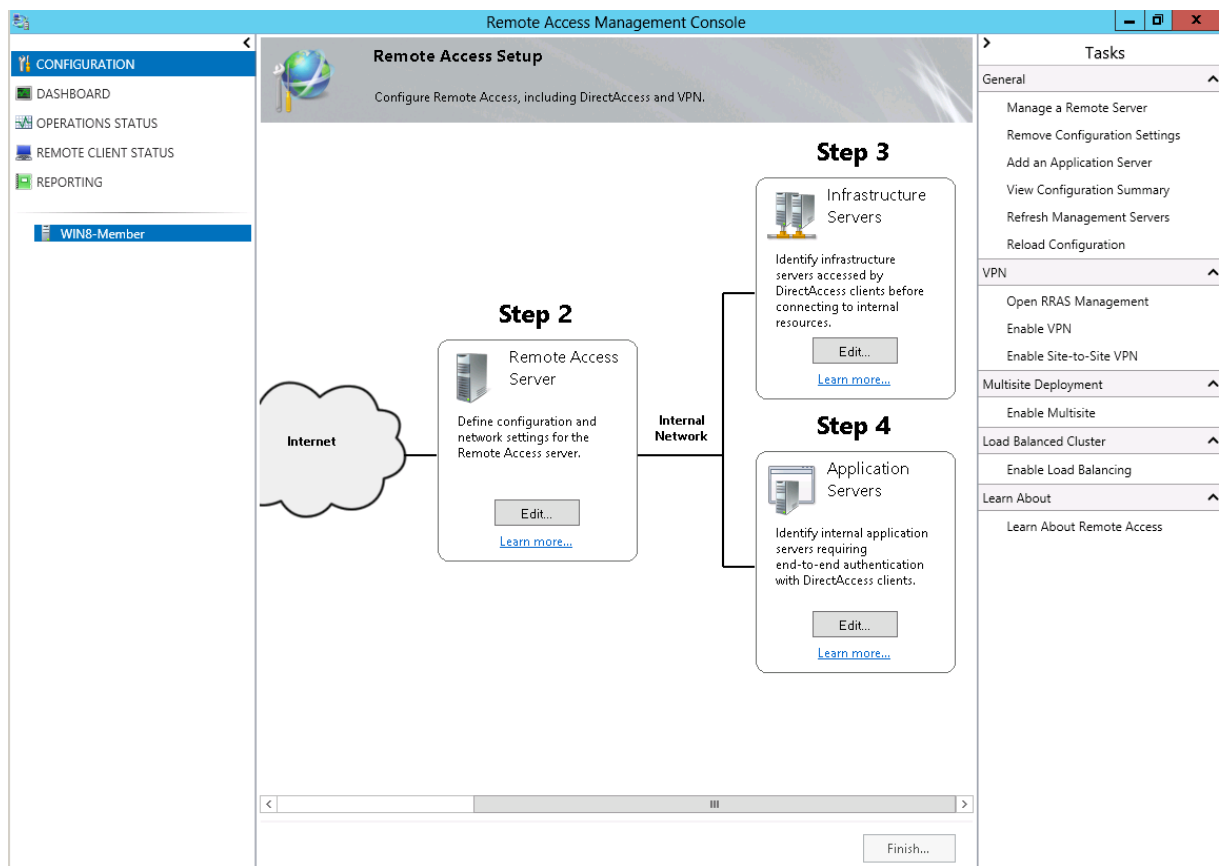
Gruppe Domänen Computer austauschen gegen DA-Gruppe und WMI Filter entfernen



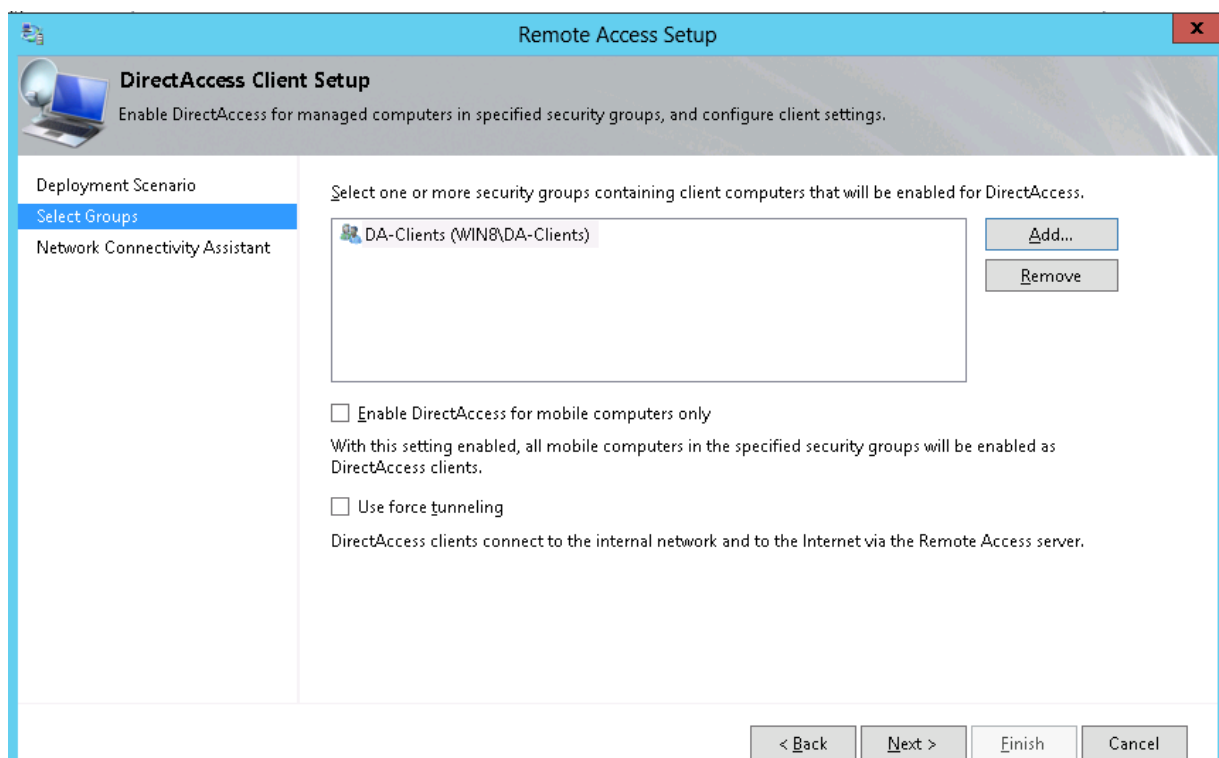
DA Assistent laeuft durch



Fertig. Der bekannte Assistent



Step 1



Sehr cool: Wenn man das Kontrollkaestchen fuer Mobile Computer setzt, wird ein WMI Filter fuer die DirectAccess Client Policy gesetzt

Remote Access Setup

DirectAccess Client Setup

Enable DirectAccess for managed computers in specified security groups, and configure client settings.

Deployment Scenario
Select Groups
Network Connectivity Assistant

The Network Connectivity Assistant (NCA) runs on DirectAccess client computers to provide DirectAccess connectivity information, diagnostics, and remediation support.

Resources that validate connectivity to internal network:

| | Resource | Type | Type |
|---|--|------|------|
| ▶ | http://directaccess-WebProbeHost.win8.server | | HTTP |
| * | | | |

Helpdesk email address:

DirectAccess connection name:

Allow DirectAccess clients to use local name resolution

< Back Next > Finish Cancel

Remote Access Setup

Remote Access Server Setup

Configure DirectAccess and VPN settings.

Network Topology
Network Adapters
Authentication

Select the network topology of the server.

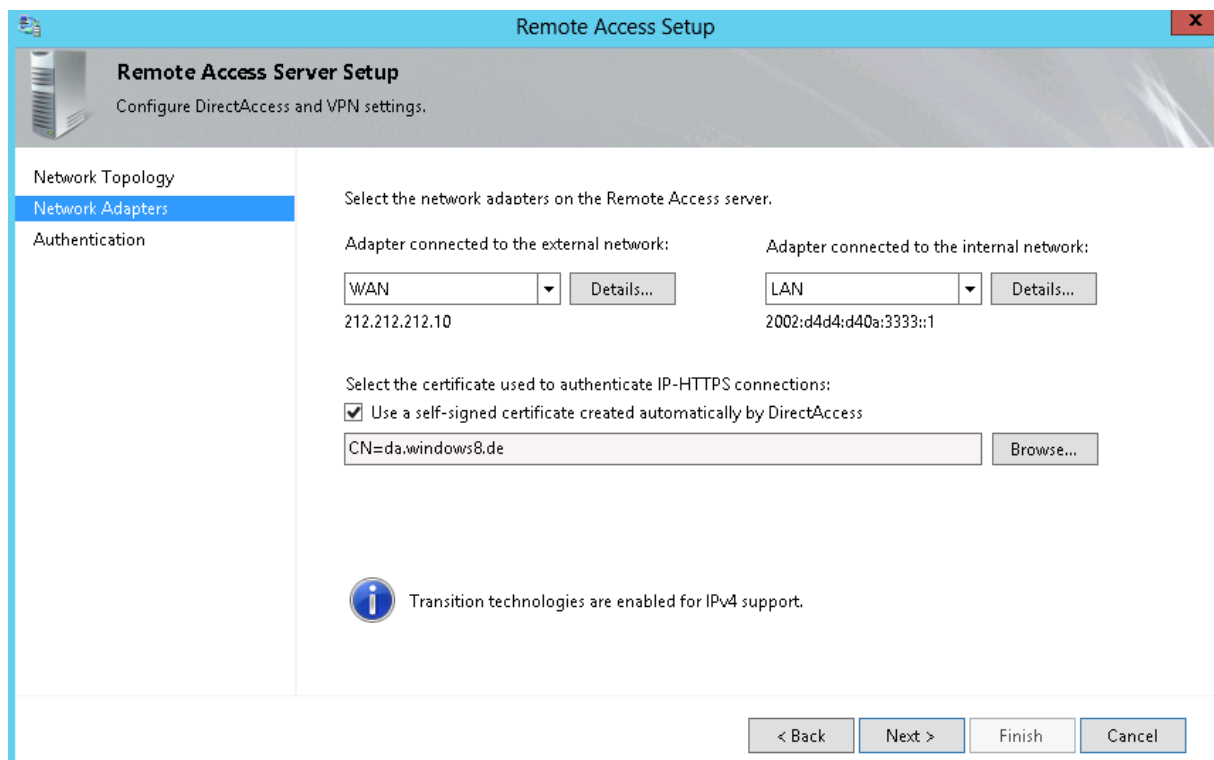
Edge
 Behind an edge device (with two network adapters)
 Behind an edge device (with a single network adapter)

In this topology, the Remote Access server is deployed at the edge of the internal corporate network and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the Internet.

Type the public name or IPv4 address used by clients to connect to the Remote Access

< Back Next > Finish Cancel

Self signed Certificates



Remote Access Setup
Configure DirectAccess and VPN settings.

Network Adapters

Select the network adapters on the Remote Access server.


Adapter connected to the external network: WAN 212.212.212.10 [Details...]

Adapter connected to the internal network: LAN 2002:d4d4:d40a:3333::1 [Details...]

Select the certificate used to authenticate IP-HTTPS connections:

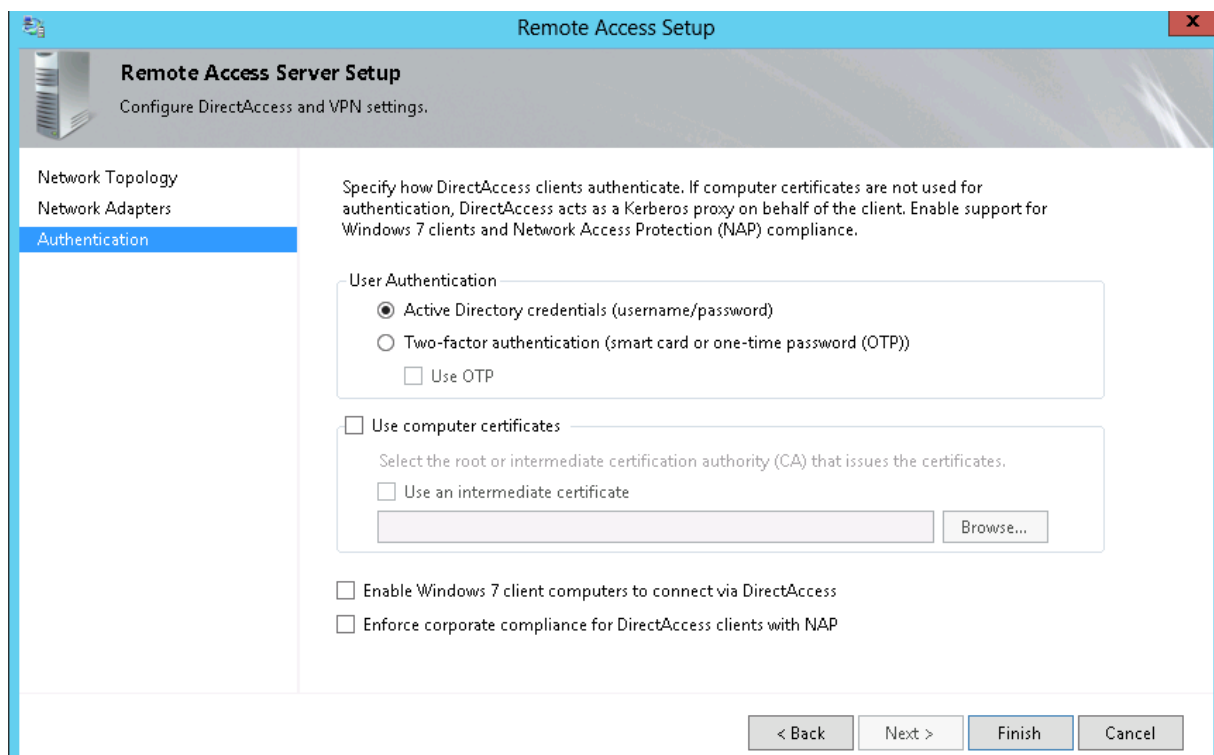
Use a self-signed certificate created automatically by DirectAccess

CN=da.windows8.de [Browse...]

 Transition technologies are enabled for IPv4 support.

< Back Next > Finish Cancel

Werden per GPO verteilt (siehe spaeter)



Remote Access Setup
Configure DirectAccess and VPN settings.

Authentication

Specify how DirectAccess clients authenticate. If computer certificates are not used for authentication, DirectAccess acts as a Kerberos proxy on behalf of the client. Enable support for Windows 7 clients and Network Access Protection (NAP) compliance.

User Authentication

Active Directory credentials (username/password)

Two-factor authentication (smart card or one-time password (OTP))

Use OTP

Use computer certificates

Select the root or intermediate certification authority (CA) that issues the certificates.

Use an intermediate certificate

[Browse...]

Enable Windows 7 client computers to connect via DirectAccess

Enforce corporate compliance for DirectAccess clients with NAP

< Back Next > Finish Cancel

Windows 7 Clients werden erstmal ausgesperrt

NLS Server auf dem DA Server selbst ☺

Remote Access Setup

Infrastructure Server Setup


Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Network Location Server

Specify settings for the network location server, used to determine the location of DirectAccess client computers. A client computer connecting successfully to the site is assumed to be on the internal network, and DirectAccess is not used.

The network location server is deployed on a remote web server (recommended)
Type in the URL of the network location server:

The network location server is deployed on the Remote Access server
Select the certificate used to authenticate the network location server:
 Use a self-signed certificate

 The network location server must be highly available to DirectAccess client computers inside the internal network, and inaccessible to DirectAccess clients located on the Internet. Clients must be able to contact the CRL for the site.

< Back Next > Finish Cancel

Remote Access Setup

Infrastructure Server Setup

Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

DNS

Enter DNS suffixes and internal DNS servers. DirectAccess client queries that match a suffix use the specified DNS server for name resolution. Name suffixes that do not have corresponding DNS servers are treated as exemptions, and DNS settings on client computers are used for name resolution.

| | Name Suffix | DNS Server Address |
|---|-------------------------|-----------------------|
| ▶ | win8.server | 2002:d4d4:d40a:3333:1 |
| | win8-member.win8.server | |
| * | | |

Select a local name resolution option:

Use local name resolution if the name does not exist in DNS (most restrictive)

Use local name resolution if the name does not exist in DNS or DNS servers are unreachable when the client computer is on a private network (recommended)

Use local name resolution for any kind of DNS resolution error (least restrictive)

< Back Next > Finish Cancel

Remote Access Setup

Infrastructure Server Setup

Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Network Location Server
DNS
DNS Suffix Search List
Management

Add additional suffixes to search for short unqualified name in multiple locations. If a query fails for a suffix, the other suffixes are appended to the name and the DNS query is repeated for the alternate FQDN.

Configure DirectAccess clients with DNS client suffix search list


Detected domain suffixes:

Domain suffixes to use:

<Primary DNS suffix of client>
win8.server

Add -> <- Remove

New Suffix: Add

 The primary domain DNS suffix appears first in the list.

< Back Next > Finish Cancel

Remote Access Setup

Infrastructure Server Setup

Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Network Location Server
DNS
DNS Suffix Search List
Management

Specify management servers used for DirectAccess client management. For example update and remediation servers.

Management servers:

| | Management Servers (IP Address, IPv6 Prefix, FQDN) |
|---|--|
| ▶ | WIN8DC.WIN8.SERVER |
| * | |

< Back Next > Finish Cancel

Erweiterte Tasks

Enable Multisite klingt spannend. Das war ja bei Forefront UAG DA ein Lebenswerk (zumindest lt. Doku, eingerichtet habe ich das noch nicht ☹)

The screenshot shows a 'Tasks' menu with several expandable categories:

- General**
 - Manage a Remote Server
 - Remove Configuration Settings
 - Add an Application Server
 - View Configuration Summary
 - Refresh Management Servers
 - Reload Configuration
- VPN**
 - Open RRAS Management
 - Enable VPN
 - Enable Site-to-Site VPN
- Multisite Deployment**
 - Enable Multisite
- Load Balanced Cluster**
 - Enable Load Balancing
- Learn About**
 - Learn About Remote Access

Dashboard

The screenshot shows the 'Remote Access Management Console' dashboard. The left sidebar contains navigation options: CONFIGURATION, DASHBOARD (selected), OPERATIONS STATUS, REMOTE CLIENT STATUS, REPORTING, and a server list with 'WIN8-Member' selected. The main content area is titled 'Remote Access Dashboard' and contains two main sections:

- Server Status**
 - Operations Status**: Lists various services with green checkmarks, including 6to4, DNS, DNS64, Domain controller, IP-HTTPS, IPsec, Kerberos, Management servers, NAT64, Network adapters, Network location server, Network security, and Services. A link to 'Operations Status page' is provided.
 - Configuration Status**: Shows a timestamp '08.04.2012 18:12:47' and the message 'The configuration was distributed successfully.'
- Remote Client Status**: A table showing client statistics:

| | | | |
|------------------------------------|---|-----------------------------|--------------------------|
| Total active clients: | 1 | Total transferred data: | 19,59 KB in/39,88 KB out |
| Total active DirectAccess clients: | 1 | Maximum client connections: | 1 |
| Total active VPN clients: | 0 | Total active unique users: | 0 |
| Total cumulative connections: | 1 | | |

A link to 'Remote Client Status page' is provided.

The right sidebar contains a 'Tasks' menu with options: Monitoring (Refresh, Configure Refresh Interval, Start Tracing, Generate Usage Report), Learn About (Learn About Remote Access).

Operations Status

Remote Access Management Console

Operations Status

| Name | Status | Since | Operations State |
|-------------------------|---------|-----------------------|------------------|
| WIN8-Member.win8.server | Working | 7 minutes, 59 seco... | |
| DirectAccess | Working | 7 minutes, 59 seco... | |
| 6to4 | Working | 1 hours, 07 minute... | |
| DNS | Working | 1 hours, 06 minute... | |
| DNS64 | Working | 1 hours, 07 minute... | |
| Domain controller | Working | 1 hours, 07 minute... | |
| IP-HTTPS | Working | 1 hours, 06 minute... | |
| IPsec | Working | 1 hours, 07 minute... | |
| Kerberos | Working | 1 hours, 06 minute... | |
| Management servers | Working | 7 minutes, 59 seco... | |
| NAT64 | Working | 1 hours, 07 minute... | |
| Network adapters | Working | 1 hours, 07 minute... | |
| Network location server | Working | 1 hours, 06 minute... | |
| Network security | Working | 1 hours, 07 minute... | |
| Services | Working | 1 hours, 06 minute... | |

Details

WIN8-Member.win8.server is working properly

Tasks

- Monitoring
 - Refresh
 - Configure Refresh Interval
 - Open Event Viewer
 - View Performance Counters
 - Disable Connectivity Check (PING)
- Learn About
 - Learn About Remote Access

Remote Client Status

Remote Access Management Console

Remote Access Clients Status

Connected Clients

| User Name | Host Name | ISP Address | Protocol/Tunnel | Duration |
|--------------------|-----------------|-------------|-----------------|----------|
| WIN8\Administrator | WIN8\WIN8-BETAS | - | IPHttps | 0:10:16 |

Access Details

| Protocol | Port | IP Address |
|----------|------|------------------------------|
| 6 | 88 | fdef:d98:402c:7777::a50:1014 |

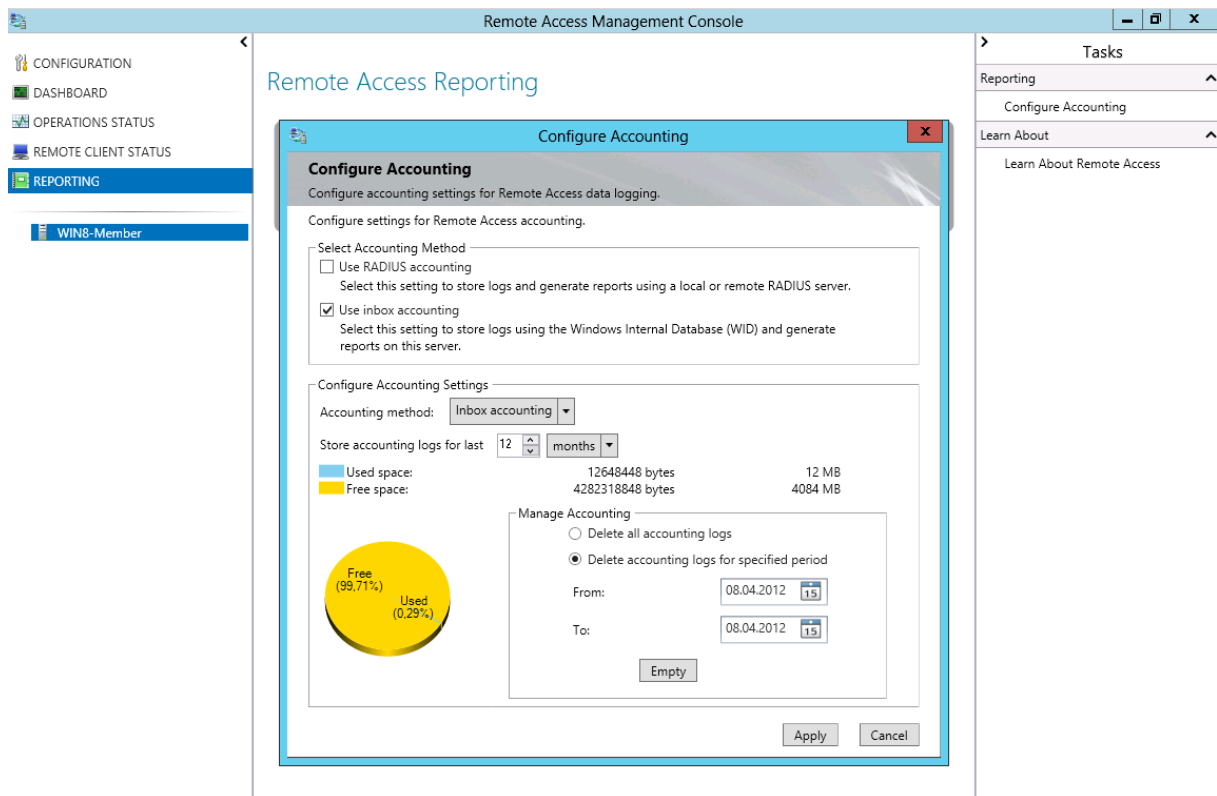
Connection Details

| | |
|------------------|----------------------------------|
| Connect Using | DirectAccess |
| Access Status | User mode/Full access |
| Total Bytes In | 20552 |
| Total Bytes Out | 42768 |
| Connection start | 08.04.2012 18:20:55 |
| Authentication | Machine Kerberos & User Kerberos |
| ISP Address | - |

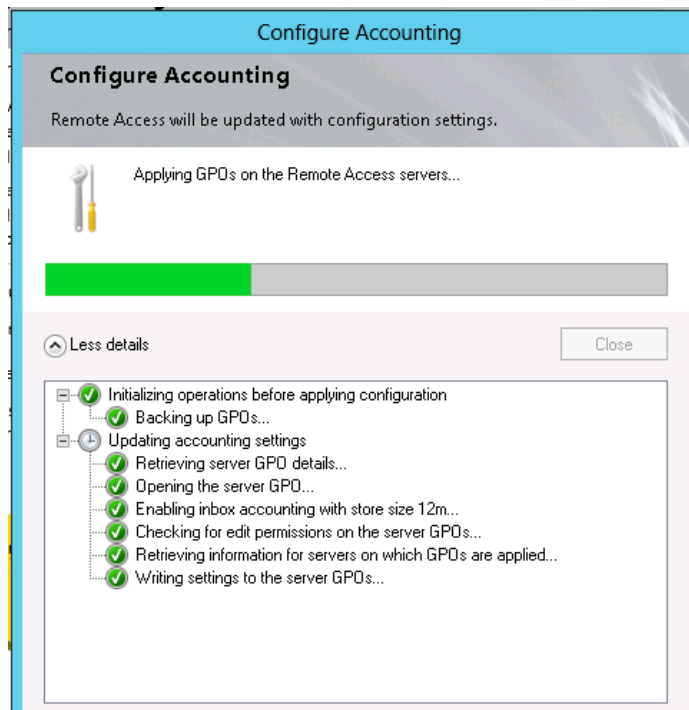
Tasks

- Monitoring
 - Refresh
 - Configure Refresh Interval
 - Disconnect VPN Clients
- Learn About
 - Learn About Remote Access

Reporting



Accounting wird eingerichtet



Remote Access Management Console

Remote Access Reporting

Start date: 08.04.2012 15 End date: 08.04.2012 15 [Generate Report](#)

Usage Report

Search

| User Name | Host Name | ISP Address | Protocol/Tunnel | Duration |
|--------------------|------------------|-------------|-----------------|----------|
| WIN8\Administrator | WIN8\WIN8-BETA\$ | - | IPHttps | 0:00:09 |

Access Details

| Protocol | Port | IP Address |
|----------|------|------------|
| | | |

Connection Details

| | |
|------------------|----------------------------------|
| Connect Using | DirectAccess |
| Access Status | User mode/Full access |
| Total Bytes In | 0 |
| Total Bytes Out | 0 |
| Connection start | 08.04.2012 18:32:28 |
| Authentication | Machine Kerberos & User Kerberos |
| ISP Address | - |

Server Load Statistics

Tasks

- Reporting
 - Configure Accounting
 - Learn About
- Learn About Remote Access

Configuration Summary

Remote Access Review

Remote Access Review

Summary of Remote Access configuration settings.

Remote Clients

- DirectAccess client access and remote management is enabled
- DirectAccess security groups:
 - WIN8\DA-Clients
- Force tunneling is disabled
- Resource used to verify internal network connectivity:
HTTP:http://directaccess-WebProbeHost.win8.server
- DirectAccess connection name: Workplace Connection

Remote Access Server

DirectAccess Configuration

- Public name or address to which clients connect: da.windows8.de
- Network adapter connected to the external network: WAN.
- Network adapter connected to the internal network: LAN.
- Internal network subnets: 2002:d4d4:d40a:1::/64
- DirectAccess clients authenticate using the DirectAccess server as a Kerberos proxy
- IP-HTTPS certificate:
CN=da.windows8.de
- Two-factor authentication is not enabled

Infrastructure Servers

- Network location server certificate:
CN=win8-member.win8.server
- DNS suffixes used by clients to determine DNS queries to be directed to internal DNS servers:

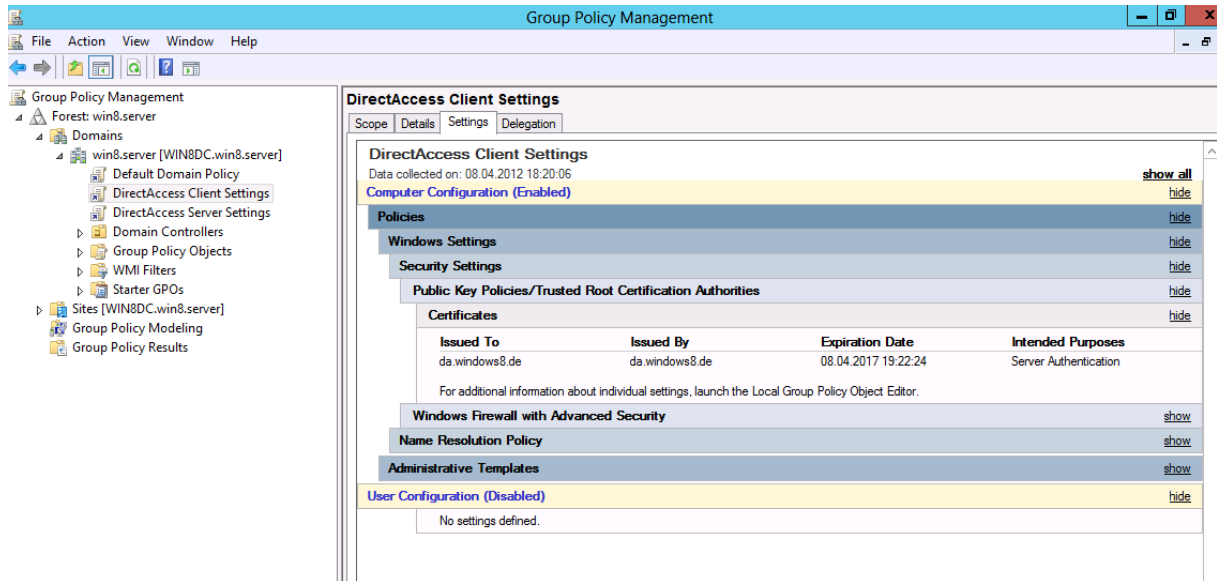
| Name Suffix | DNS Server Address |
|-------------------------|------------------------|
| win8.server | 2002:d4d4:d40a:3333::1 |
| win8-member.win8.server | |

- Local name resolution option:

[Save to a file](#) | [Print](#)

DA Group Policy fuer Clients

Self Signed Cert wird verteilt als RootCA Certificate



Da macht man(n) es sich einfach. Revocation Checking wird deaktiviert

Administrative Templates [hide](#)

Policy definitions (ADMX files) retrieved from the local computer.

- Network/DirectAccess Client Experience Settings** [show](#)
- Network/DNS Client** [show](#)
- Network/Network Connectivity Status Indicator** [show](#)
- Network/TCP/IP Settings/IPv6 Transition Technologies** [show](#)
- System/Kerberos** [hide](#)

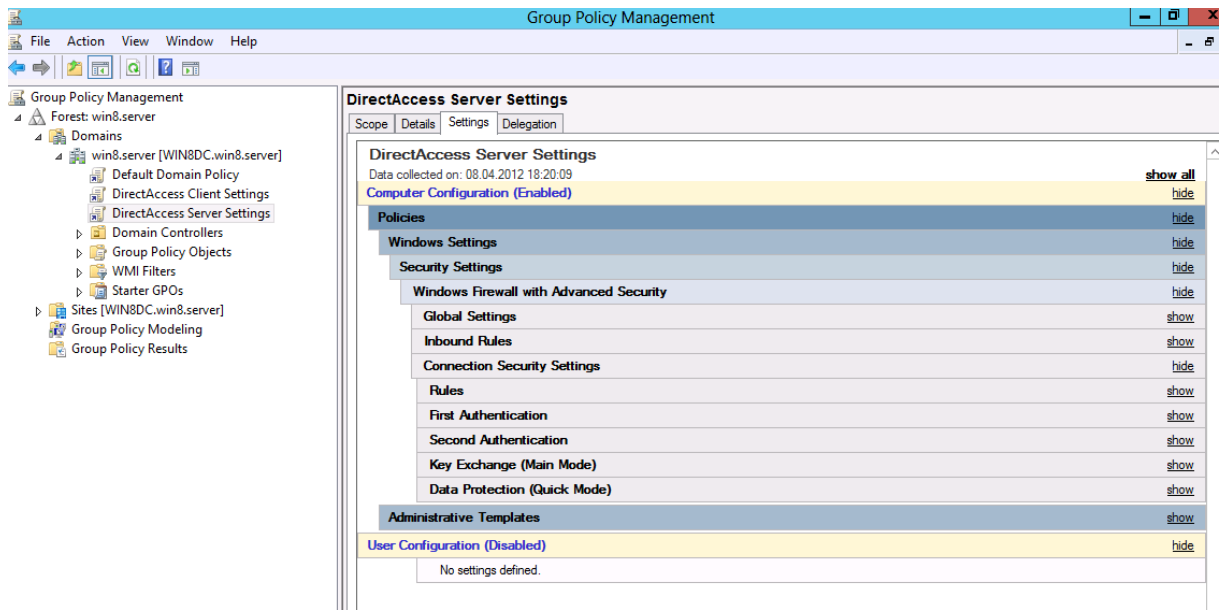
| Policy | Setting | Comment |
|--|---------|---------|
| Disable revocation checking for the SSL certificate of KDC proxy servers | Enabled | |
| Specify KDC proxy servers for Kerberos clients | Enabled | |

Define KDC proxy servers settings:

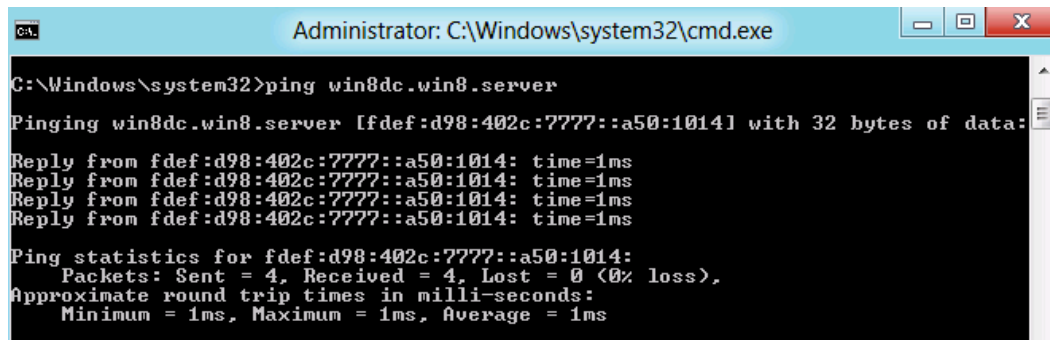
```
* <https da.windows8.de />
```

Syntax:
Enter the DNS suffix name as the Value Name.
DNS suffix name allows three formats with decreasing preference order:
Full Match: host.contoso.com
Suffix Match: .contoso.com
Default Match: *
Enter the proxy server names as the Value.
The proxy server names must be enclosed with tags <https />
To add multiple proxy server names, separate entries with a space or comma ", "
Example:
Value Name: .contoso.com
Value: <https proxy1.contoso.com proxy2.contoso.com />
Another Example:
Value Name: *
Value: <https proxy.contoso.com />

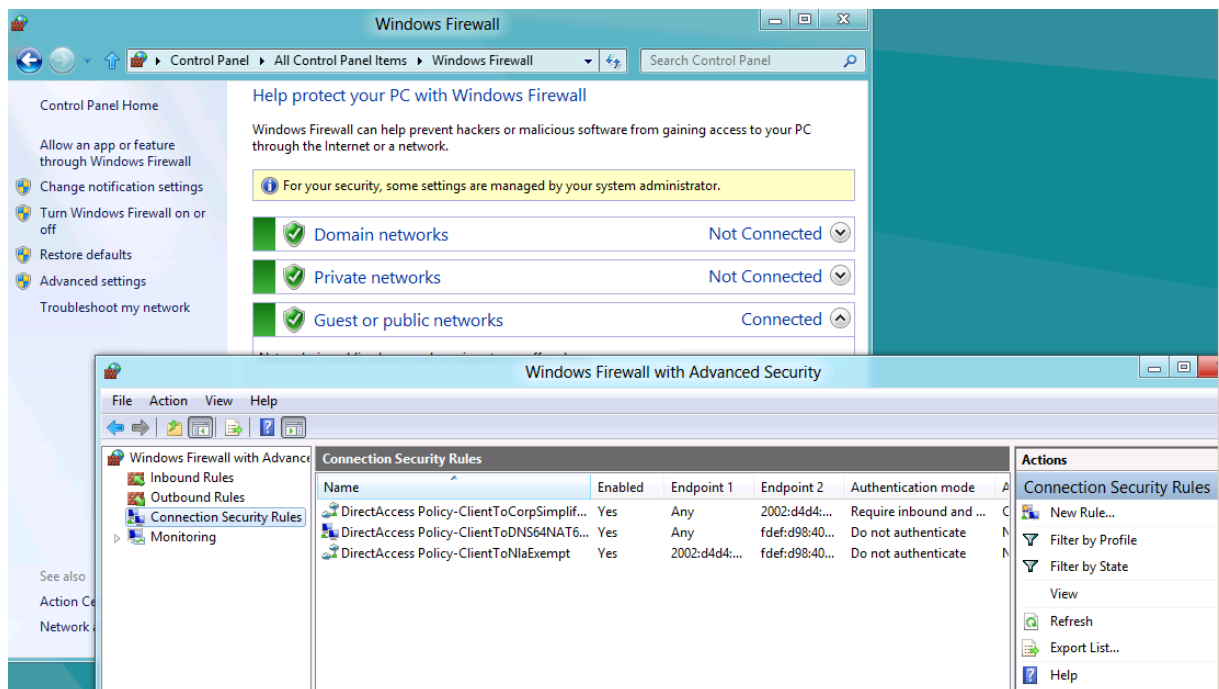
DirectAccess Group Policy fuer DA Server



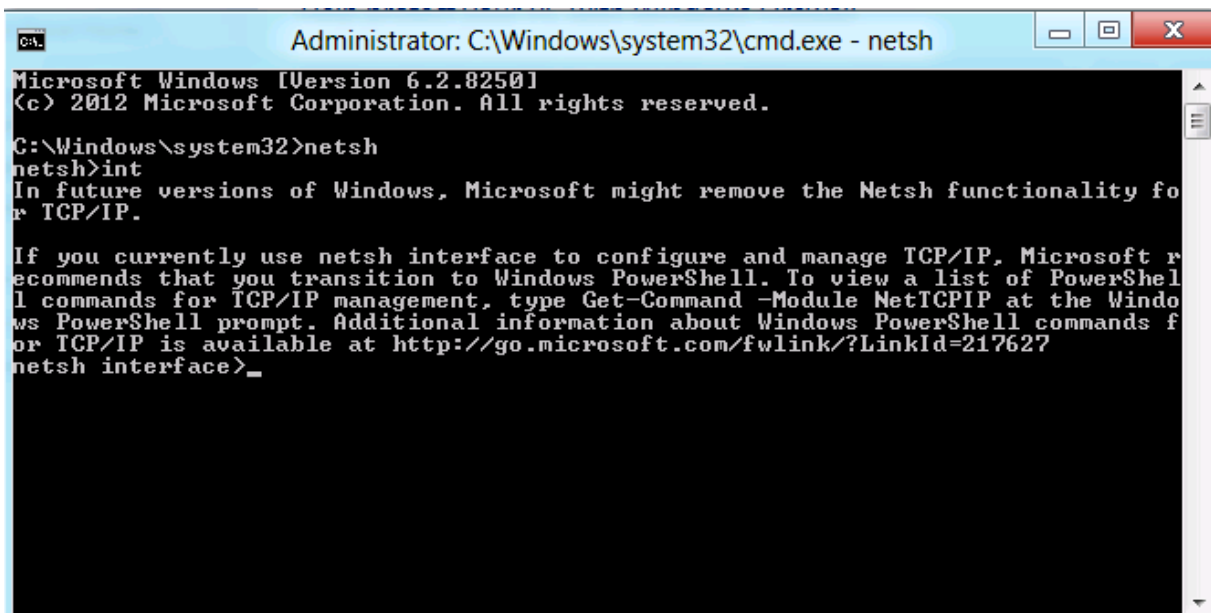
DA Connectivity am Client testen



Windows Firewall Einstellungen



Troubleshooting jetzt mit Powershell statt NETSH

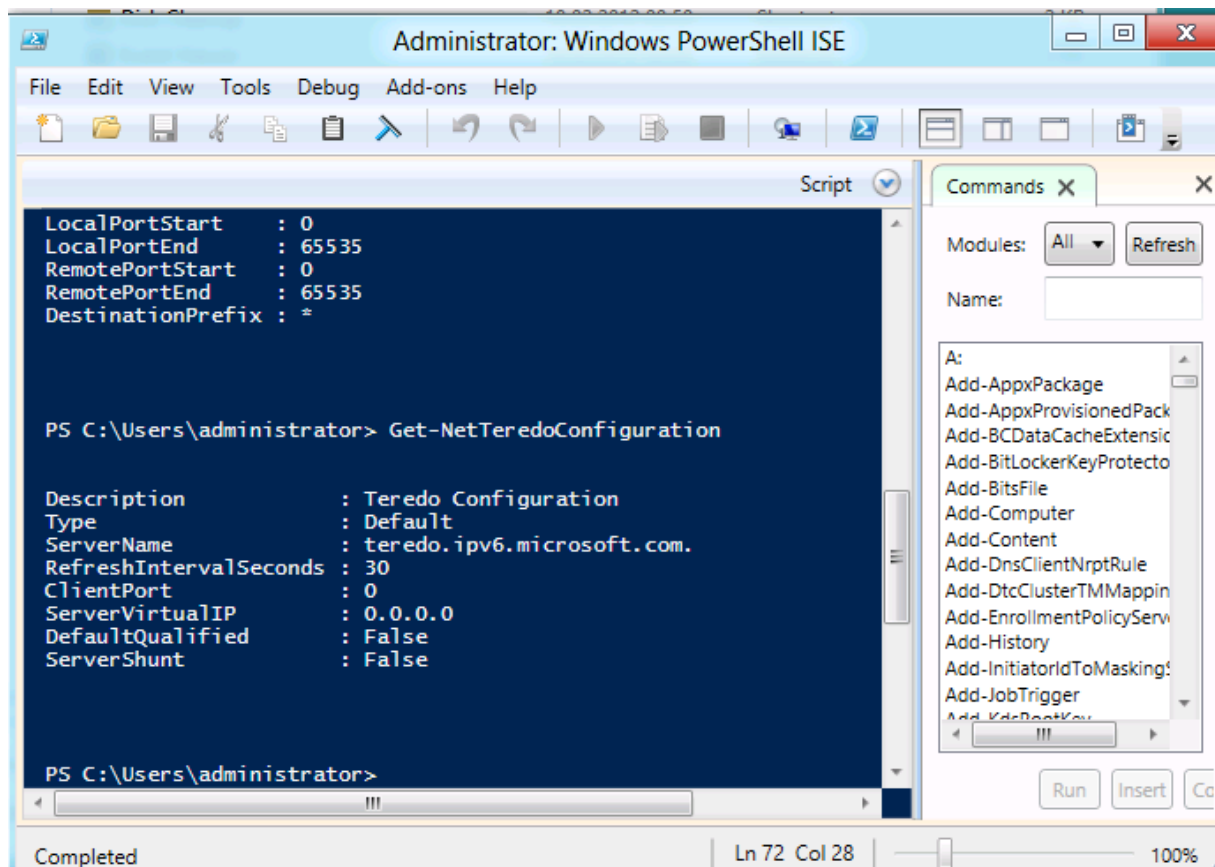


```
Administrator: C:\Windows\system32\cmd.exe - netsh
Microsoft Windows [Version 6.2.8250]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh
netsh>int
In future versions of Windows, Microsoft might remove the Netsh functionality for TCP/IP.

If you currently use netsh interface to configure and manage TCP/IP, Microsoft recommends that you transition to Windows PowerShell. To view a list of PowerShell commands for TCP/IP management, type Get-Command -Module NetTCPIP at the Windows PowerShell prompt. Additional information about Windows PowerShell commands for TCP/IP is available at http://go.microsoft.com/fwlink/?LinkId=217627
netsh interface>_
```

Powershell



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script
LocalPortStart : 0
LocalPortEnd : 65535
RemotePortStart : 0
RemotePortEnd : 65535
DestinationPrefix : *

PS C:\Users\administrator> Get-NetTeredoConfiguration

Description      : Teredo Configuration
Type              : Default
ServerName        : teredo.ipv6.microsoft.com.
RefreshIntervalSeconds : 30
ClientPort        : 0
ServerVirtualIP   : 0.0.0.0
DefaultQualified  : False
ServerShunt       : False

PS C:\Users\administrator>

Commands X
Modules: All Refresh
Name:
A:
Add-AppxPackage
Add-AppxProvisionedPack
Add-BCDataCacheExtensic
Add-BitLockerKeyProtecto
Add-BitsFile
Add-Computer
Add-Content
Add-DnsClientNrptRule
Add-DtcClusterTMMappin
Add-EnrollmentPolicyServ
Add-History
Add-InitiatorIdToMasking!
Add-JobTrigger
Add-KdrBootKey
Run Insert Co
Completed Ln 72 Col 28 100%
```

DA Konfiguration entfernen

The screenshot displays the Remote Access Management Console interface. The main window is titled "Remote Access Setup" and shows "Step 3" of the configuration process. A dialog box titled "Removing Configuration Settings" is open, indicating that Remote Access will be updated with configuration settings. The dialog box contains a progress bar and a list of tasks being performed, all marked with green checkmarks. The tasks include:

- Retrieving server GPO details...
- Opening the server GPO...
- Checking for edit permissions on the server GPOs...
- Opening the client GPOs...
- Checking for edit permissions on the client GPOs...
- Unregistering the DNS entry used to check client connectivity...
- Unregistering the web probe in DNS...
- Clearing settings from the client GPO...
- Deleting GPO win8.server\DirectAccess Client Settings...
- Clearing settings from the application server GPO...
- Uninstalling Remote Access on server WIN8-MEMBER.win8.server...
- Clearing settings from the server GPO...
- Deleting GPO win8.server\DirectAccess Server Settings...

The console also shows a "Tasks" panel on the right with various options like "Manage a Remote Server", "Remove Configuration Settings", and "Add an Application Server". The left sidebar shows navigation options like "CONFIGURATION", "DASHBOARD", "OPERATIONS STATUS", "REMOTE CLIENT STATUS", and "REPORTING". A cloud icon labeled "Internet" is visible on the left side of the console.