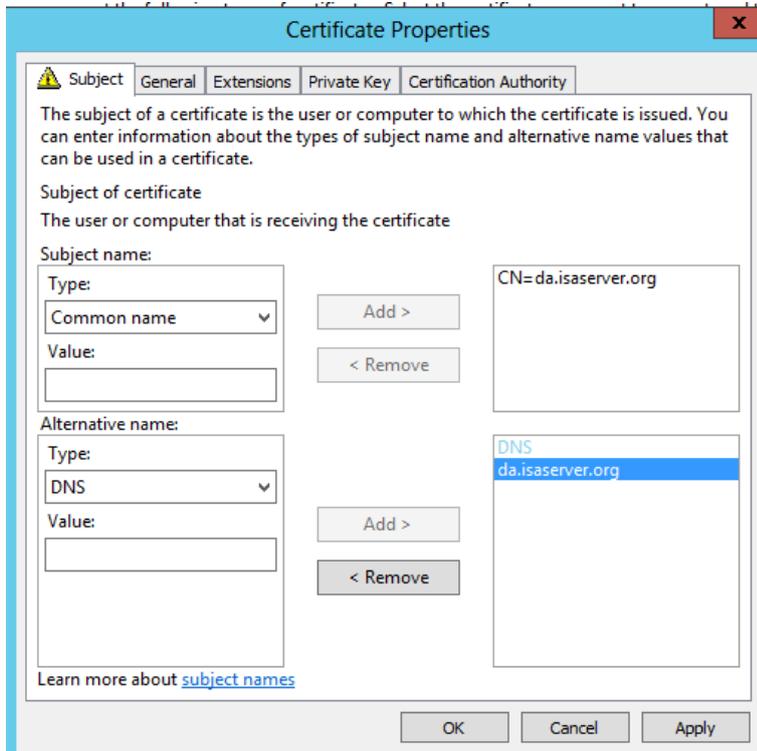
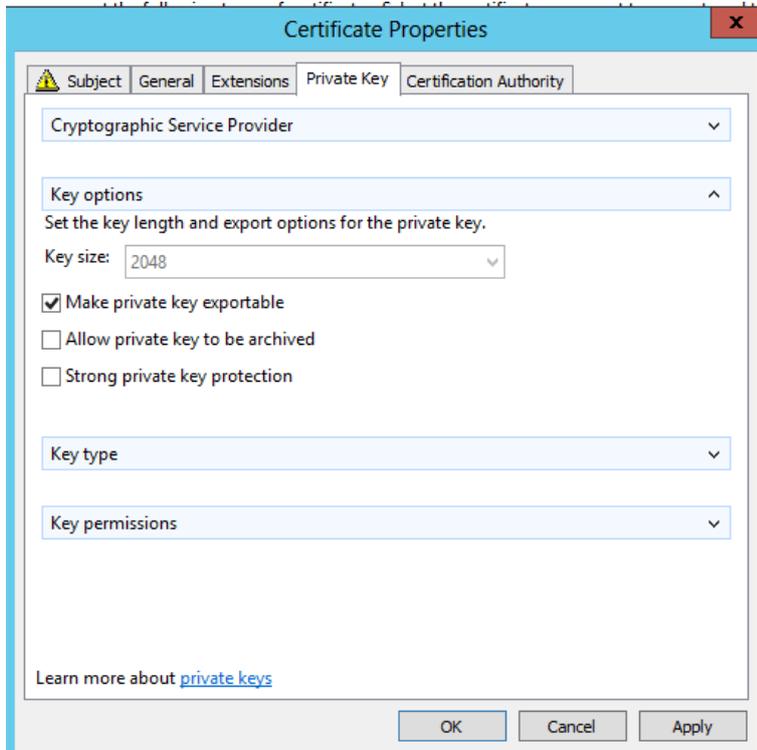


## Windows Server 2012 DirectAccess Multisite und NLB Deployment

Korrektes Zertifikat fuer IP-HTTPS ausstellen



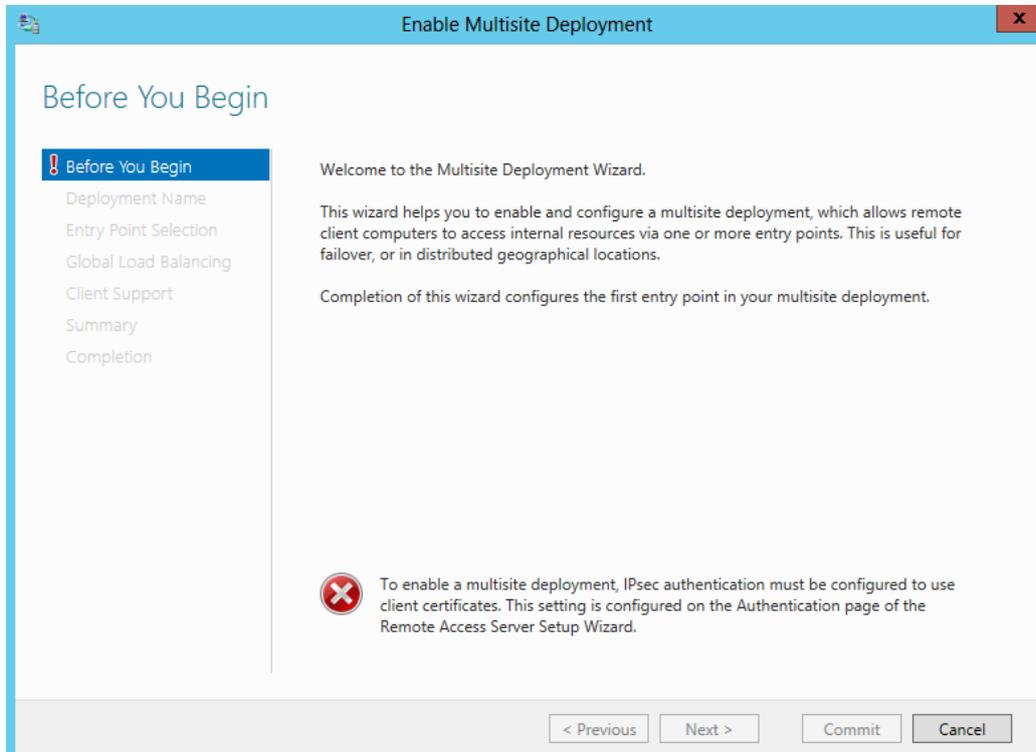
Private Key exportable weil dieses auf dem anderen DA Server importiert werden muss fuer NLB Cluster



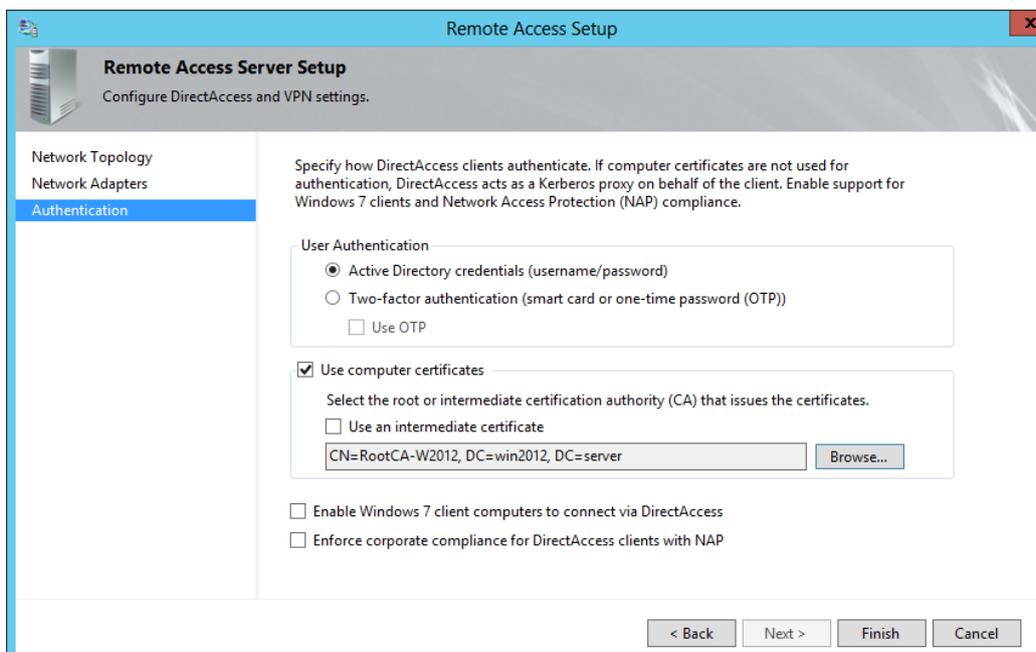
Zertifikat mit .PFX exportieren und auf dem anderen DA Server importieren

## Multisite Deployment

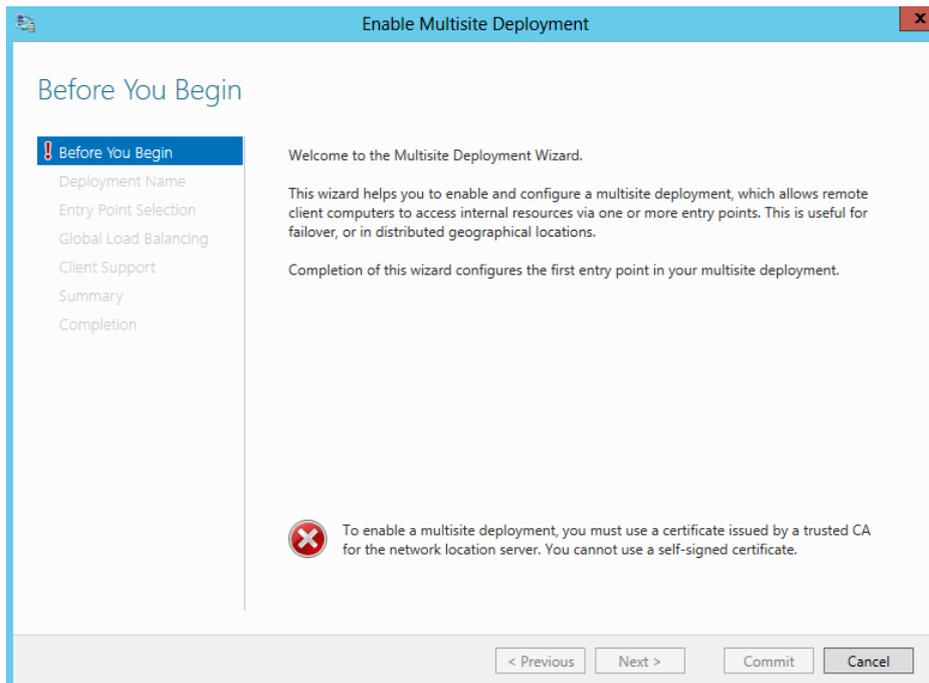
Als erstes das Multisite Deployment testen



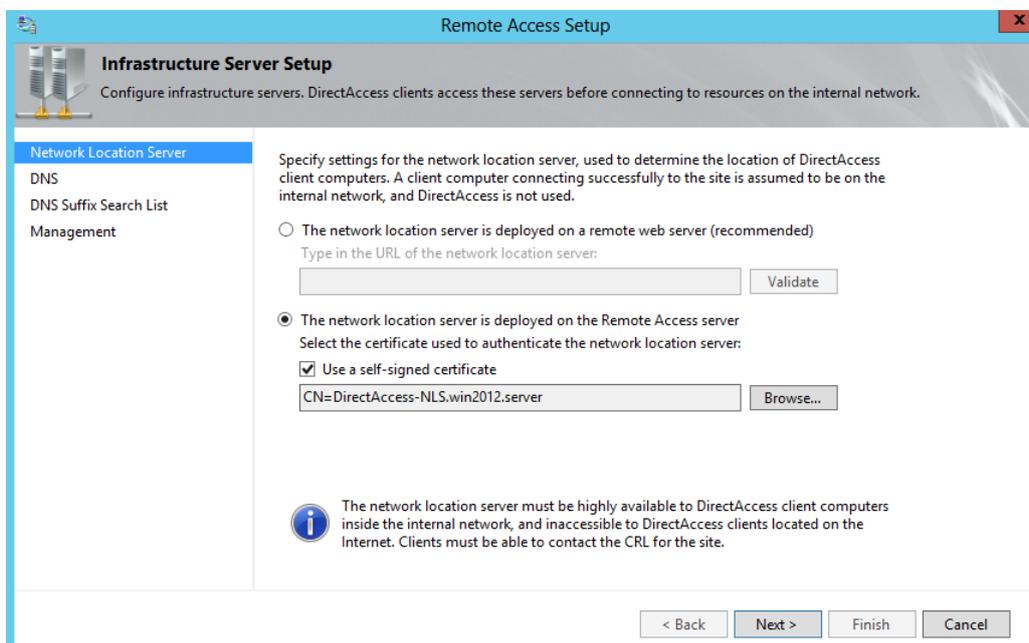
Kein KDC-Proxy, hier werden Zertifikate benoetigt

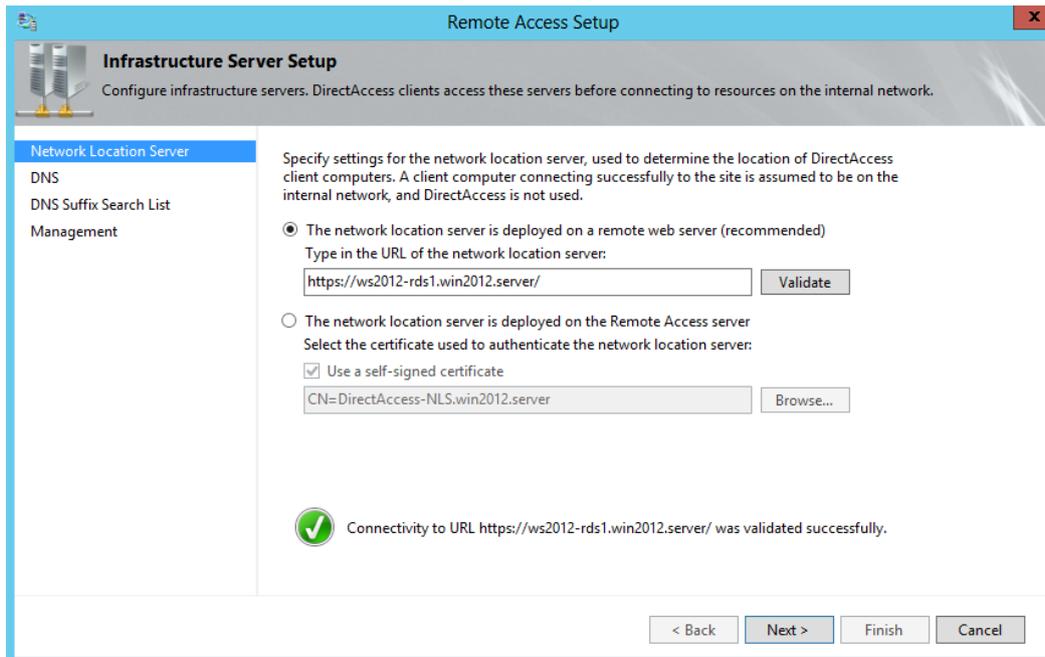


## Der NLS Server darf kein Self Signed Certificate haben

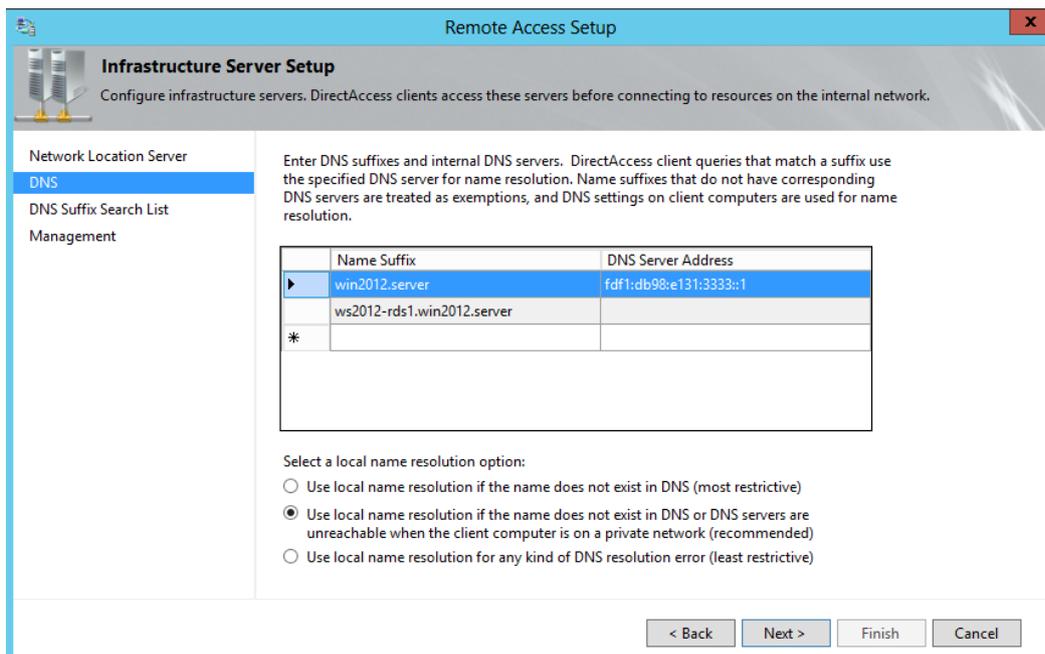


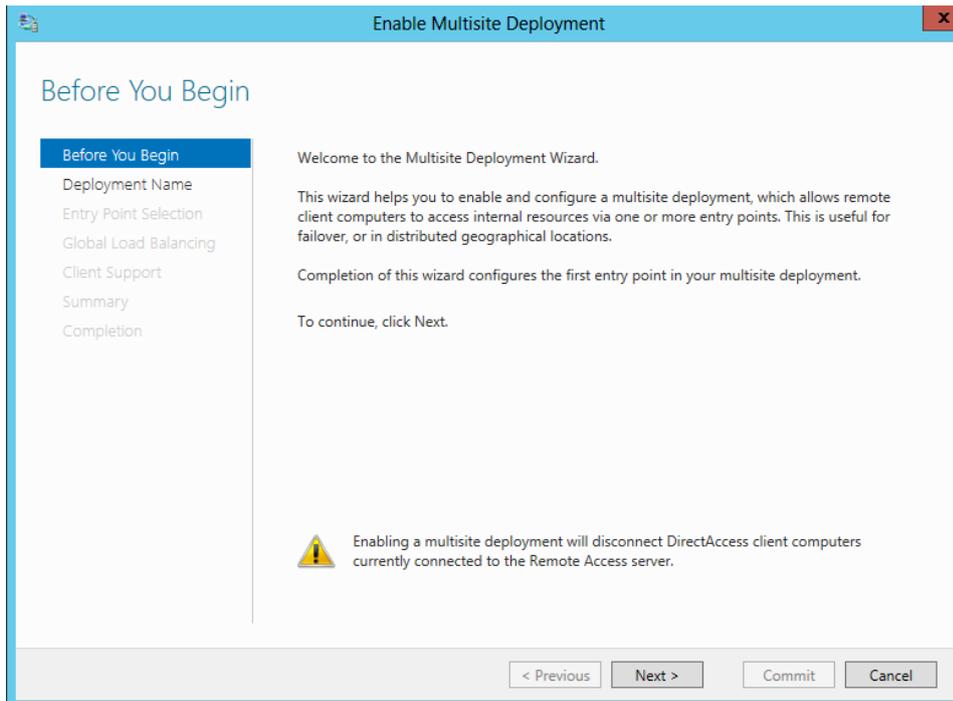
Am besten den NLS Server wie bei UAG auf eine andere, hochverfuegbare Maschine legen



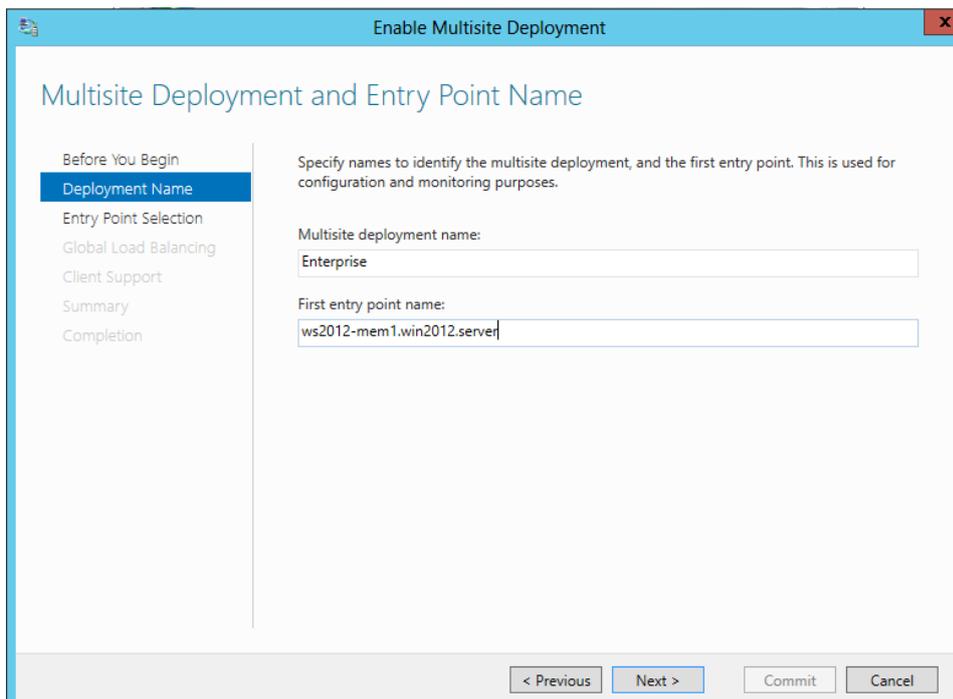


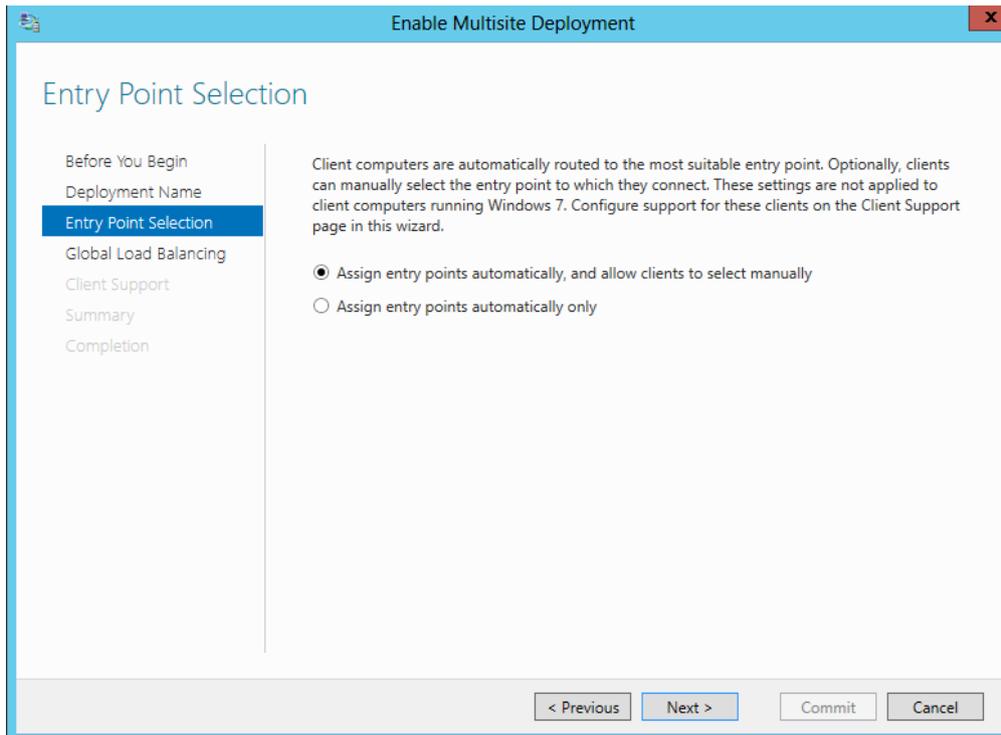
**ACHTUNG:** Wie bei Forefront UAG ist der NLS Server von DA Clients nicht erreichbar und sollte hochverfügbar betrieben werden



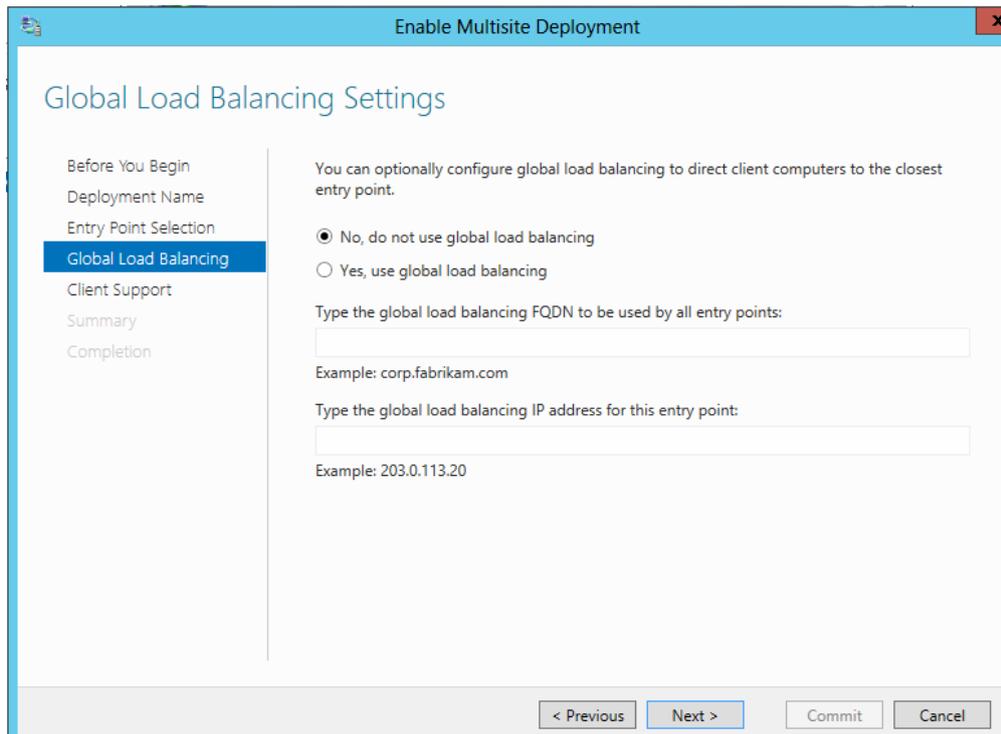


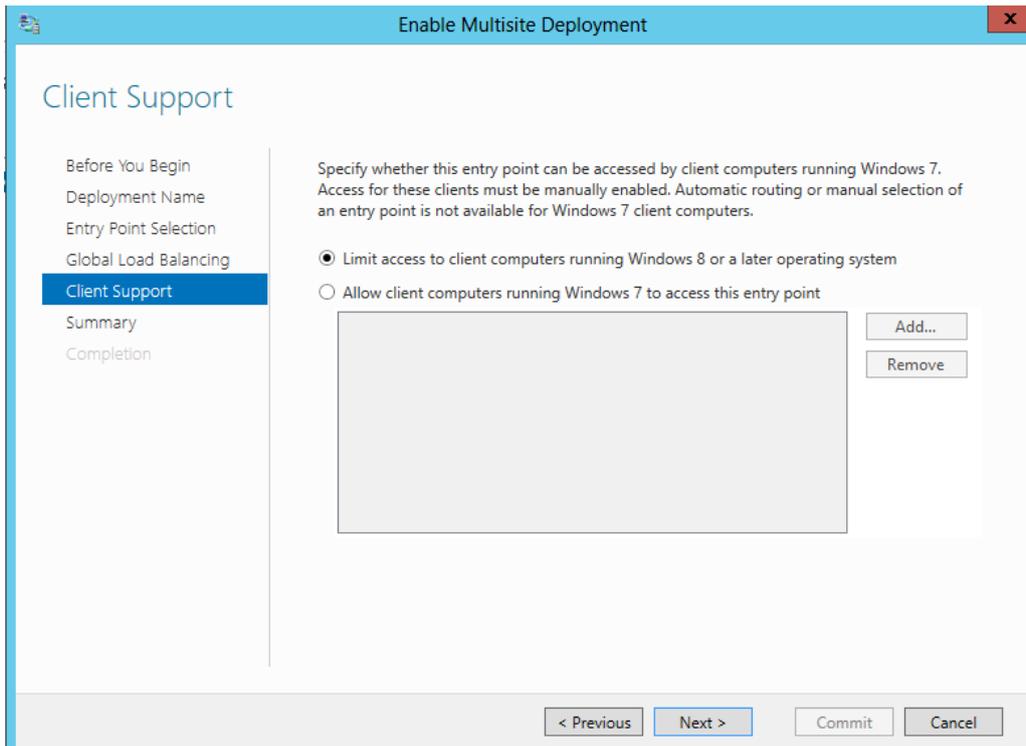
Entry Point Name ist in diesem Fall der Servername, besser waeren geografische Lokationen, siehe spaeter in diesem Artikel. Aenderung ist spaeter noch moeglich.



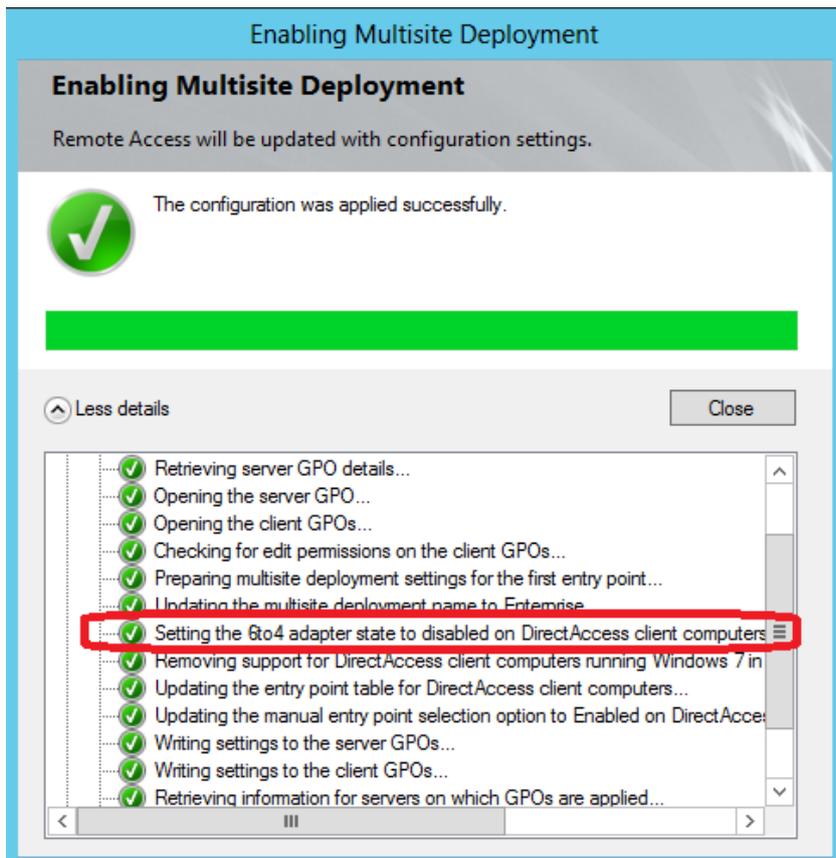


Wenn kein Global Load Balancer verfügbar ist, abwählen. Der GLB würde automatisch den DA Client an die nächste Lokation verbinden!





6to4 wird bei Multisite nicht supported



## Zweiten DA Server am zweiten Standort hinzufuegen

The screenshot shows the 'Add an Entry Point' wizard in the 'Entry Point Details' step. The title bar reads 'Add an Entry Point'. The left sidebar contains a list of steps: 'Entry Point Details' (selected), 'Network Topology', 'Network Name or IP Add...', 'Network Adapters', 'Client Support', 'Server GPO Settings', 'Summary', and 'Completion'. The main area contains the following text: 'Select the Remote Access server associated with this entry point, and specify an entry point name.' Below this, there are two input fields: 'Remote Access server:' with the value 'WS2012-MEM2.win2012.server' and a 'Browse...' button, and 'Entry point name:' with the value 'WS2012-MEM2.win2012.server'. At the bottom, there is a red error icon and the message 'Remote Access is not installed on this server.' The bottom navigation bar includes '< Previous', 'Next >', 'Commit', and 'Cancel' buttons.

## Rolle Remotezugriff hinzufuegen

Wenn der Remote Server noch nicht konfiguriert wurde

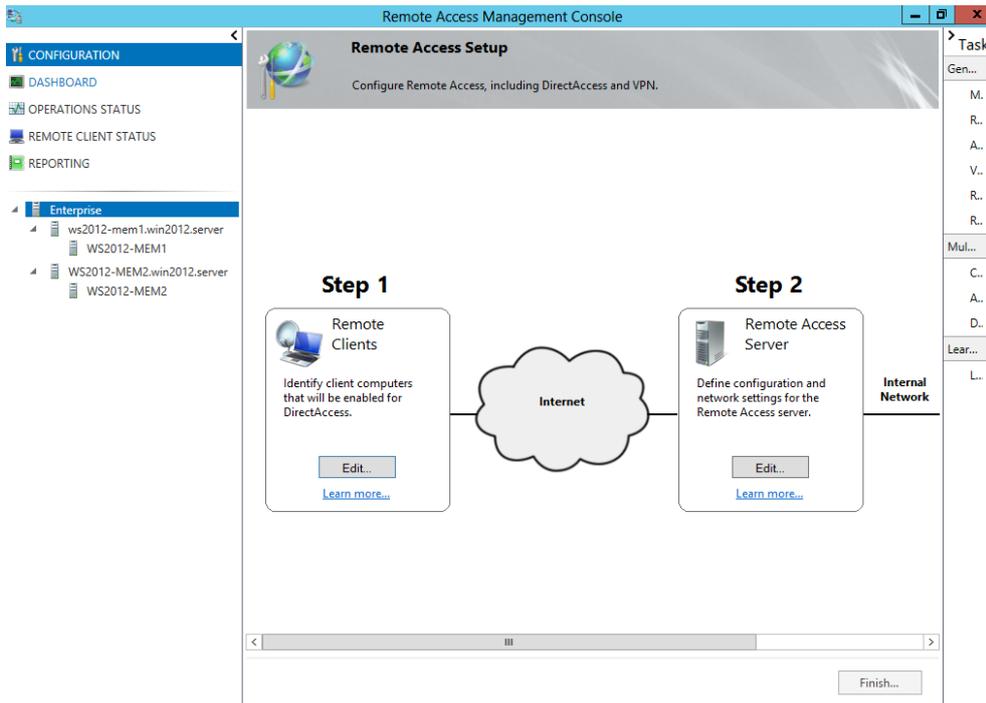
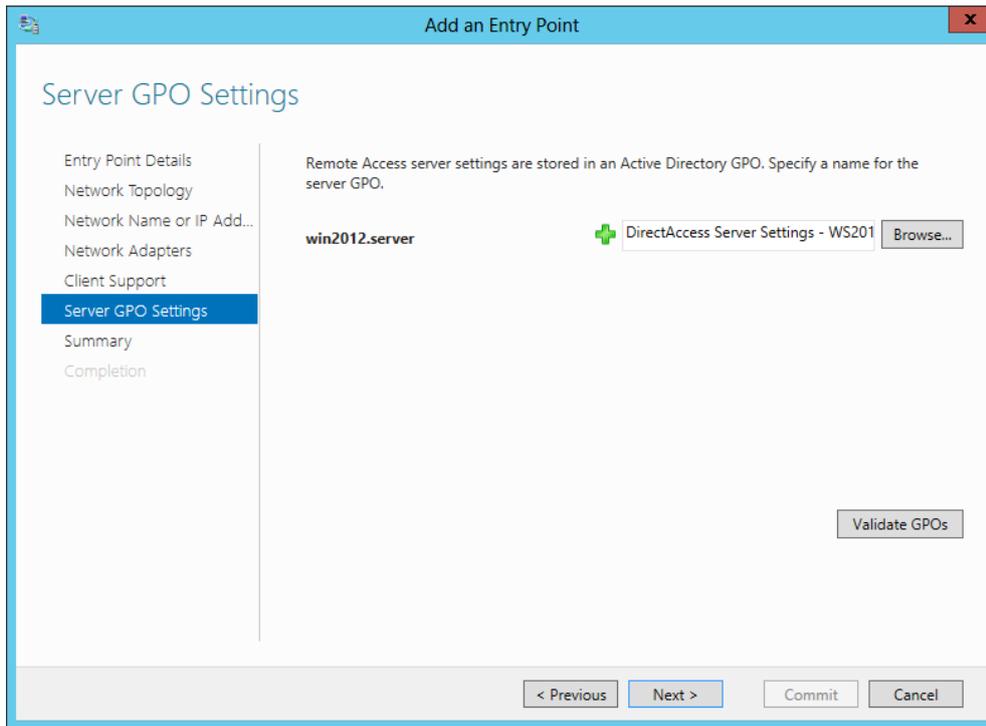
The screenshot shows the 'Add an Entry Point' wizard in the 'Network Topology' step. The title bar reads 'Add an Entry Point'. The left sidebar contains a list of steps: 'Entry Point Details', 'Network Topology' (selected), 'Network Name or IP Add...', 'Network Adapters', 'Client Support', 'Server GPO Settings', 'Summary', and 'Completion'. The main area contains the following text: 'Select the Remote Access server network topology.' Below this, there are three radio button options: 'Edge' (with a description: '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.'), 'Behind an edge device (with two network adapters)' (with a description: 'In this topology, the Remote Access server is deployed behind an edge firewall or device, and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the perimeter network.'), and 'Behind an edge device (with a single network adapter)' (with a description: 'In this topology, the Remote Access server is deployed with a single network adapter that is connected to the internal network.'). The bottom navigation bar includes '< Previous', 'Next >', 'Commit', and 'Cancel' buttons.

Der Name muss ein anderer sein und idealerweise dem Standort des neuen DA Server entsprechen.

The screenshot shows the 'Add an Entry Point' wizard window. The title bar reads 'Add an Entry Point'. The main heading is 'Network Name or IP address'. On the left, a navigation pane lists steps: 'Entry Point Details', 'Network Topology', 'Network Name or IP Add...' (highlighted), 'Network Adapters', 'Client Support', 'Server GPO Settings', 'Summary', and 'Completion'. The main area contains the instruction: 'Type in the public name or IP address used by clients to connect to the Remote Access server.' Below this is a text input field containing 'DA2.ISASERVER.ORG'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Commit', and 'Cancel'.

Ein entsprechendes Zertifikat muss vorhanden sein

The screenshot shows the 'Add an Entry Point' wizard window at the 'Network Adapters' step. The title bar reads 'Add an Entry Point'. The main heading is 'Network Adapters'. The left navigation pane is the same as in the previous screenshot, but 'Network Adapters' is highlighted. The main area contains the instruction: 'Select the single network adapter that connects to the external or perimeter network.' Below this, there is a 'Network adapter:' label followed by a dropdown menu showing 'LAN'. Underneath the dropdown is the IP address '10.80.16.152' with a blue 'Details' link. The next instruction is 'Select the certificate used to authenticate IP-HTTPS connections.' Below this is a text input field containing 'CN=da2.isaserver.org' and a 'Browse...' button. At the bottom, there are four buttons: '< Previous', 'Next >', 'Commit', and 'Cancel'.



# Entry Points umbenennen

The screenshot shows the Remote Access Management Console window. The title bar reads "Remote Access Management Console". The main content area is titled "Remote Access Setup" and contains the instruction "Configure Remote Access, including DirectAccess and VPN." Below this, there is a diagram illustrating the setup process:

- Step 1: Remote Clients** - Identify client computers that will be enabled for DirectAccess. Includes an "Edit..." button and a "Learn more..." link.
- Internet** - Represented by a cloud icon connecting the two steps.
- Step 2: Remote Access Server** - Define configuration and network settings for the Remote Access server. Includes an "Edit..." button and a "Learn more..." link.
- Internal Network** - A line connecting the Remote Access Server to the internal network.

On the left side, there is a navigation pane with the following items:

- CONFIGURATION
  - DASHBOARD
  - OPERATIONS STATUS
  - REMOTE CLIENT STATUS
  - REPORTING
- Enterprise
  - ws2012-mem1.win2012.server
    - WS2012-MEM1
  - WS2012-MEM2.win2012.server
    - WS2012-MEM2

On the right side, there is a "Tasks" pane with a list of tasks: Gen..., M., R., A., V., R., R., Mul..., C., A., D., Lear..., L...

At the bottom right of the main content area, there is a "Finish..." button.

This screenshot shows a portion of the Remote Access Management Console, specifically the "REMOTE CLIENT STATUS" and "REPORTING" sections. The navigation pane on the left is expanded to show the following structure:

- Enterprise
  - EUROPE
    - WS2012-MEM2
  - USA
    - WS2012-MEM1** (highlighted)

# Computer Zertifikat fuer DA Server

Remote Access Management Console

Operations Status

Name	Status	Since	Operations State
WS2012-MEM1.win2012.ser...	Critical	42 minutes, 22...	DirectAccess
DirectAccess	Critical	42 minutes, 22...	IPsec
DNS	Working	45 minutes, 13...	
DNS64	Working	47 minutes, 22...	
Domain cont...	Working	47 minutes, 21...	
IP-HTTPS	Working	42 minutes, 22...	
IPsec	Critical	42 minutes, 22...	IPsec certificate a
NAT64	Working	47 minutes, 21...	
Network ada...	Working	47 minutes, 22...	
Network loca...	Working	27 minutes, 22...	
Network secu...	Working	47 minutes, 21...	
Services	Working	45 minutes, 13...	

Details

- WS2012-MEM1.win2012.server: Not working properly
- IPsec: Not working properly  
View the IPsec monitor for more details.

Tasks

- Monitoring
  - Refresh
  - Configure Refresh Interval
  - Open Event Viewer
  - View Performance Counters
- Learn About
  - Learn About Remote Access

09:57  
19.06.2013

IP-HTTPS	Working	42 minutes, 22...	
IPsec	Critical	42 minutes, 22...	IPsec certificate a
NAT64	Working	47 minutes, 21...	
Network ada...	Working	47 minutes, 22...	
Network loca...	Working	27 minutes, 22...	
Network secu...	Working	47 minutes, 21...	
Services	Working	45 minutes, 13...	

Details

IPsec: Not working properly

Error:

There is no valid certificate to be used by IPsec which chains to the root/intermediate certificate configured to be used by IPsec in the DirectAccess configuration.

Causes:

The certificate has not been installed or is not valid.

Resolution:

## Status

The screenshot displays the Remote Access Management Console interface. The left-hand navigation pane shows a tree structure under 'Enterprise' with sub-nodes for 'EUROPE' (containing 'WS2012-MEM2') and 'USA' (containing 'WS2012-MEM1'). The main content area is titled 'Multisite Deployment Status' and contains three sections:

- Configuration Status:** Shows a green checkmark and the timestamp '19.06.2013 09:39:30' with the message 'The configuration was distributed successfully.'
- Server Status:** A table with columns: Entry Point, Operations Stat..., DirectAccess Clie..., and Configuration Status.
 

Entry Point	Operations Stat...	DirectAccess Clie...	Configuration Status
<a href="#">EUROPE</a>	Working	0	19.06.2013 09:39:...
<a href="#">USA</a>	Working	0	19.06.2013 09:39:...
- Remote Client Status:** A table with columns: Entry Point, Total Remote Clients, Total VPN Clients, and Total Cumulative Connectio...
 

Entry Point	Total Remote Clients	Total VPN Clients	Total Cumulative Connectio...
EUROPE	0	0	0
USA	0	0	0

A 'Tasks' pane on the right includes 'Monitoring' (Refresh, Configure Refresh Interval) and 'Learn About' (Learn About Remote Access).

## Group Policies

The screenshot shows the Group Policy Management console. The left pane displays a tree view for 'Forest: win2012.server' with 'DirectAccess Client Settings' selected. The right pane shows the configuration details for 'DirectAccess Client Settings'.

**DirectAccess Client Settings**  
 Scope: Details | Settings | Delegation

Data collected on: 19.06.2013 10:32:55

**Computer Configuration (Enabled)**

- Policies**
  - Windows Settings
  - Security Settings
    - Windows Firewall with Advanced Security
    - Name Resolution Policy
  - Administrative Templates
    - Policy definitions (ADMX files) retrieved from the local computer.
  - Network/DirectAccess Client Experience Settings
  - Network/Network Connectivity Status Indicator
  - Network/TCPIP Settings/IPv6 Transition Technologies

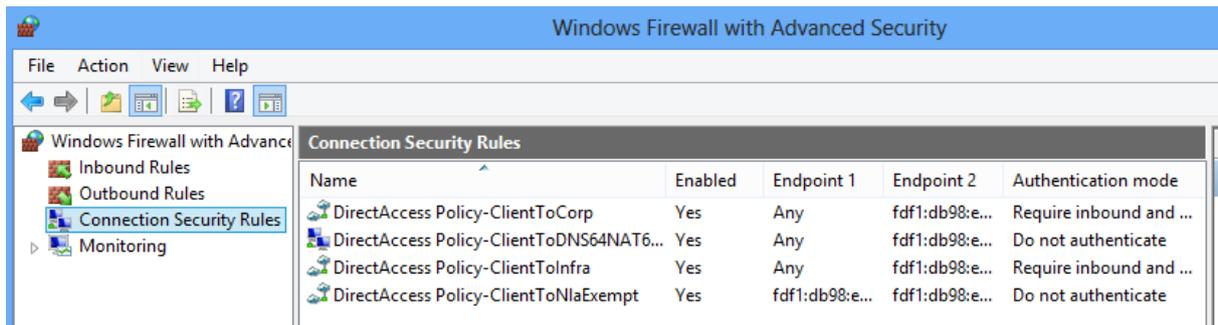
Policy	Setting	Comment
Set 6to4 State	Enabled	
Select from the following states: Disabled State		

- Extra Registry Settings**

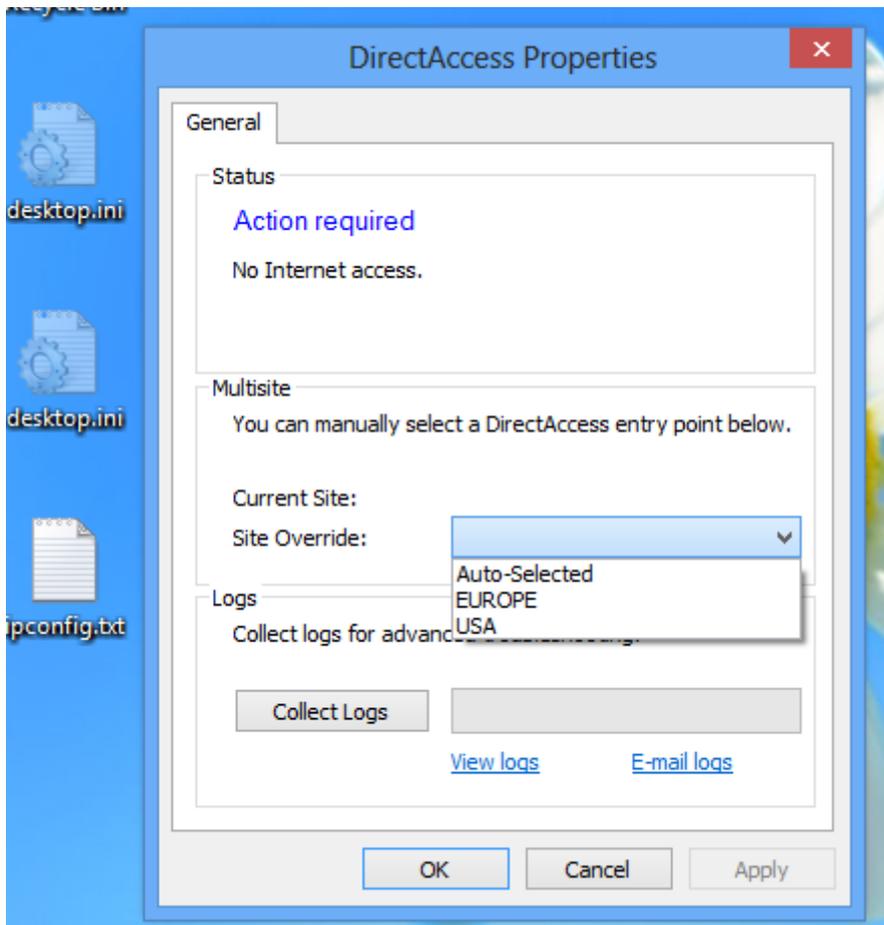
**User Configuration (Disabled)**

- No settings defined.

## Firewalleinstellungen am Client



## Multisite Auswahl am DA Client



# Load Balancing

The screenshot shows the Remote Access Management Console interface. The left sidebar contains a navigation tree with 'Enterprise' expanded to show 'EUROPE', 'USA', and their respective servers. The main pane displays the 'Entry Point Configuration Summary' for the 'EUROPE' entry point. The configuration details are as follows:

Entry point name:	EUROPE
IP-HTTPS address:	DA2.ISASERVER.ORG
Prefix assigned to clients connecting over IP-HTTPS:	fd62:a8df:585d:1000::/64
Server GPO:	win2012.server\DirectAccess Server Settings - WS2012-

Below the configuration details, there are three sections with links to modify settings:

- Client support:** Limit access to client computers running Windows 8 or a later operating system.
- VPN support:** VPN is not enabled on this entry point. Link: [Enable VPN](#)
- Load balancing configuration:** Load balancing is not enabled on this entry point. Link: [Enable Load Balancing](#)

The right-hand 'Tasks' pane lists various actions such as 'Manage a Remote Server', 'Reload Configuration', 'Enable VPN', and 'Configure Entry Point Settings'.

The screenshot shows the 'Enable Load Balancing' wizard. The current step is 'Load Balancing Method'. The wizard is titled 'Enable Load Balancing' and has a progress indicator on the left side with steps: 'Before You Begin', 'Load Balancing Method' (current), 'Dedicated IP Addresses', 'Summary', and 'Completion'.

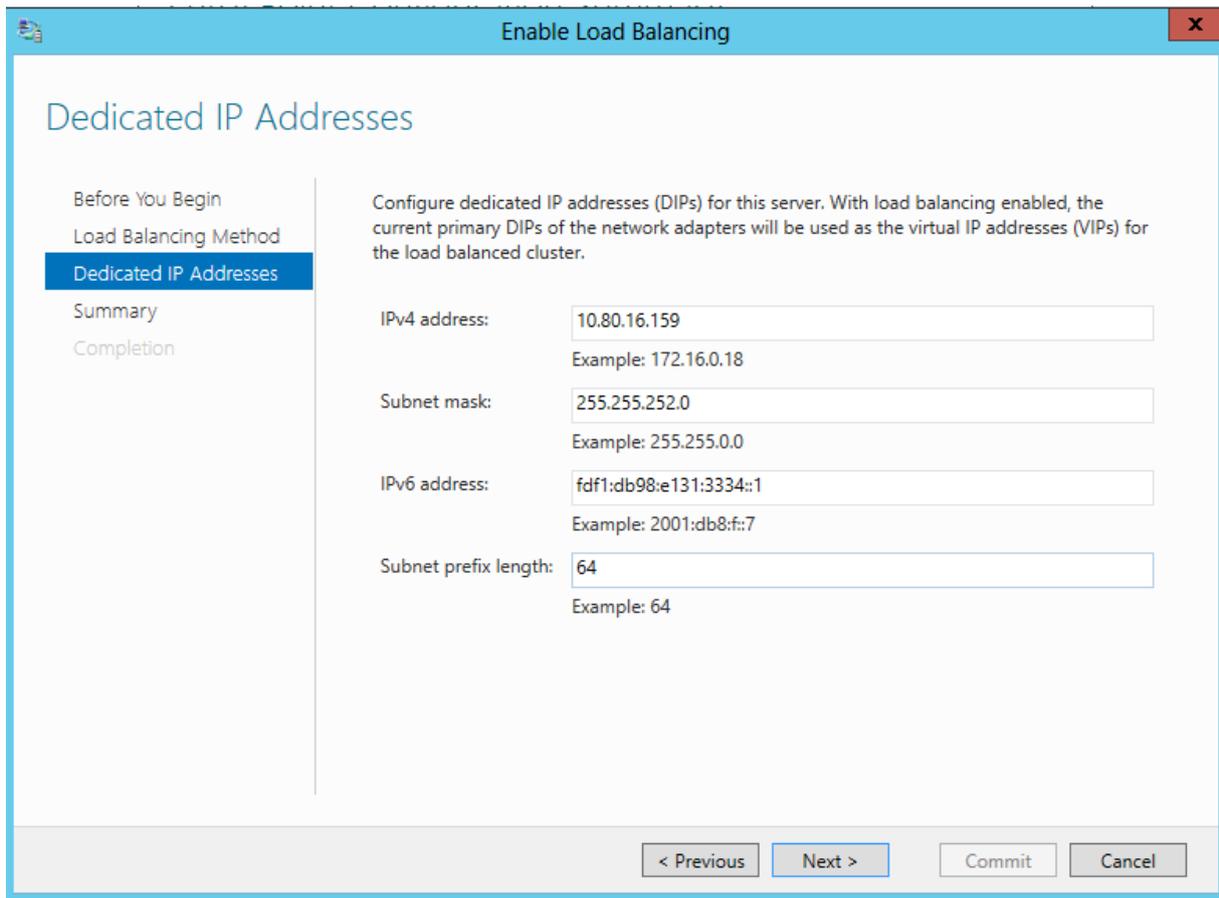
The main content area contains the following text and options:

Select a load balancing method for this cluster.

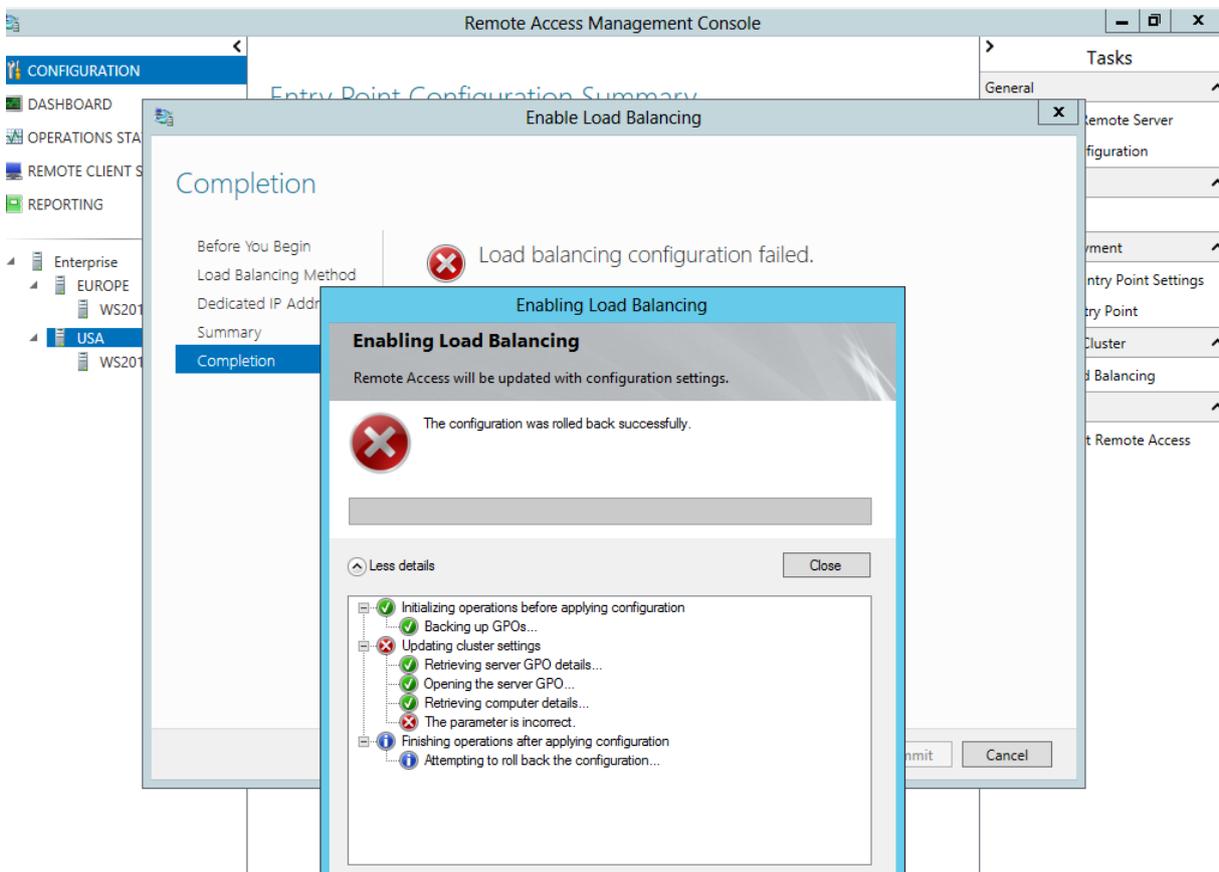
- Use Windows Network Load Balancing (NLB)
- Use an external load balancer

At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Commit', and 'Cancel'.

Achtung bei den IP Adressen. Die ehemaligen DIP werden VIP



## Error



Known issues:

<http://technet.microsoft.com/de-de/library/jj134175.aspx>

Auch an weitere Fixe denken

Hotfix verfuegbar fuer falsche Subnetzmasken nach NLB Member Hinzufuegung:

<http://support.microsoft.com/kb/2836232>

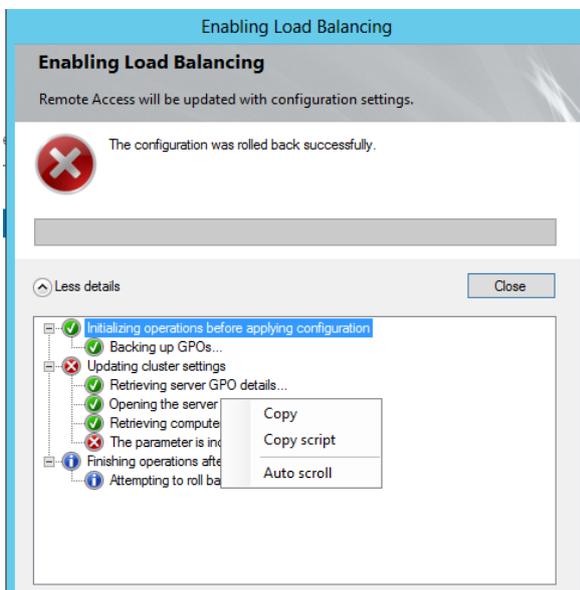
Weitere Hotfix Listen:

<http://blog.msedge.org.uk/2012/12/directaccess-hotfix-summary.html>

Backup der GPO

```
Administrator: Windows PowerShell
[06/19/2013 11:53:57] Retrieved multicite deployment. Found the following entry points: "EUROPE, USA"
[06/19/2013 11:53:57] Retrieving data for entry point "EUROPE"...
[06/19/2013 11:53:57] Retrieved data for entry point "EUROPE"
[06/19/2013 11:53:57] Retrieving closest DC for entry point "EUROPE"...
[06/19/2013 11:53:57] Retrieved closest DC for entry point "EUROPE" : "WS2012-DC.win2012.server"
[06/19/2013 11:53:57] Server GPO will be backed up:
Domain : win2012.server
Name : DirectAccess Server Settings - WS2012-MEM2.win2012.server
DC : WS2012-DC.win2012.server
Links : DC=win2012.DC=server
Servers: WS2012-MEM2.win2012.server
[06/19/2013 11:53:57] Retrieving data for entry point "USA"...
[06/19/2013 11:53:57] Retrieved data for entry point "USA"
[06/19/2013 11:53:57] Retrieving closest DC for entry point "USA"...
[06/19/2013 11:53:57] Retrieved closest DC for entry point "USA" : "WS2012-DC.win2012.server"
[06/19/2013 11:53:57] Server GPO will be backed up:
Domain : win2012.server
Name : DirectAccess Server Settings
DC : WS2012-DC.win2012.server
Links : DC=win2012.DC=server
Servers: WS2012-MEM1.win2012.server
[06/19/2013 11:53:57] Retrieved all data needed for backup.
[06/19/2013 11:53:57] Validating configuration version consistency across GPOs...
[06/19/2013 11:53:57] Configuration version consistency was validated successfully. All GPOs have the same v
[06/19/2013 11:53:57] Starting the backup process...
[06/19/2013 11:53:57] Backing up GPO:
Domain : win2012.server
Name : DirectAccess Client Settings
DC : DC
Links : DC=win2012.DC=server
[06/19/2013 11:53:58] Successfully backed up GPO.
[06/19/2013 11:53:58] Backing up GPO:
Domain : win2012.server
Name : DirectAccess Server Settings - WS2012-MEM2.win2012.server
DC : WS2012-DC.win2012.server
Links : DC=win2012.DC=server
Servers: WS2012-MEM2.win2012.server
[06/19/2013 11:53:58] Successfully backed up GPO.
[06/19/2013 11:53:58] Backing up GPO:
Domain : win2012.server
Name : DirectAccess Server Settings
DC : WS2012-DC.win2012.server
Links : DC=win2012.DC=server
Servers: WS2012-MEM1.win2012.server
[06/19/2013 11:53:58] Successfully backed up GPO.
[06/19/2013 11:53:58] Finished taking backup.
[06/19/2013 11:53:58] Writing index file.
[06/19/2013 11:53:58] Copying files from temporary directory.
[06/19/2013 11:53:58] Done. Backup successfully written to "C:\DABACKUP\RemoteAccessBackup.zip".
PS C:\DABACKUP>
```

Copy Script



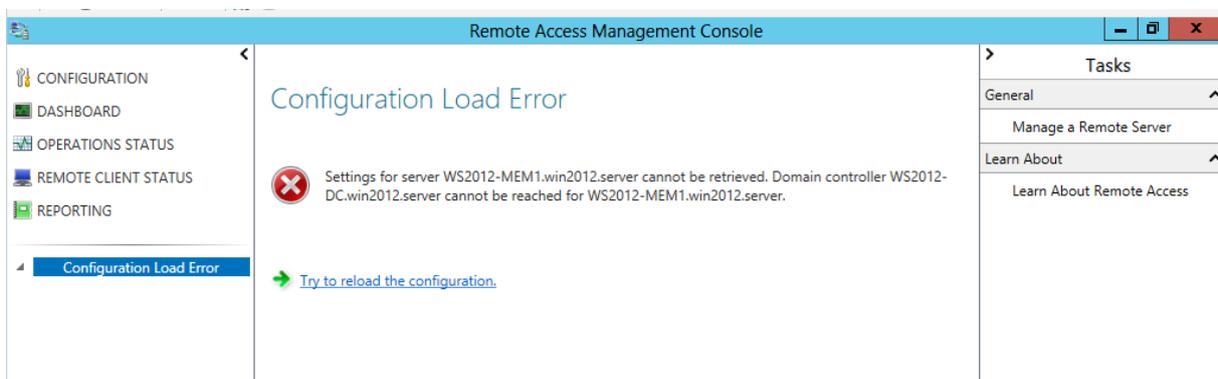
Mit Notepad editieren

IPv6 Adressen entfernen

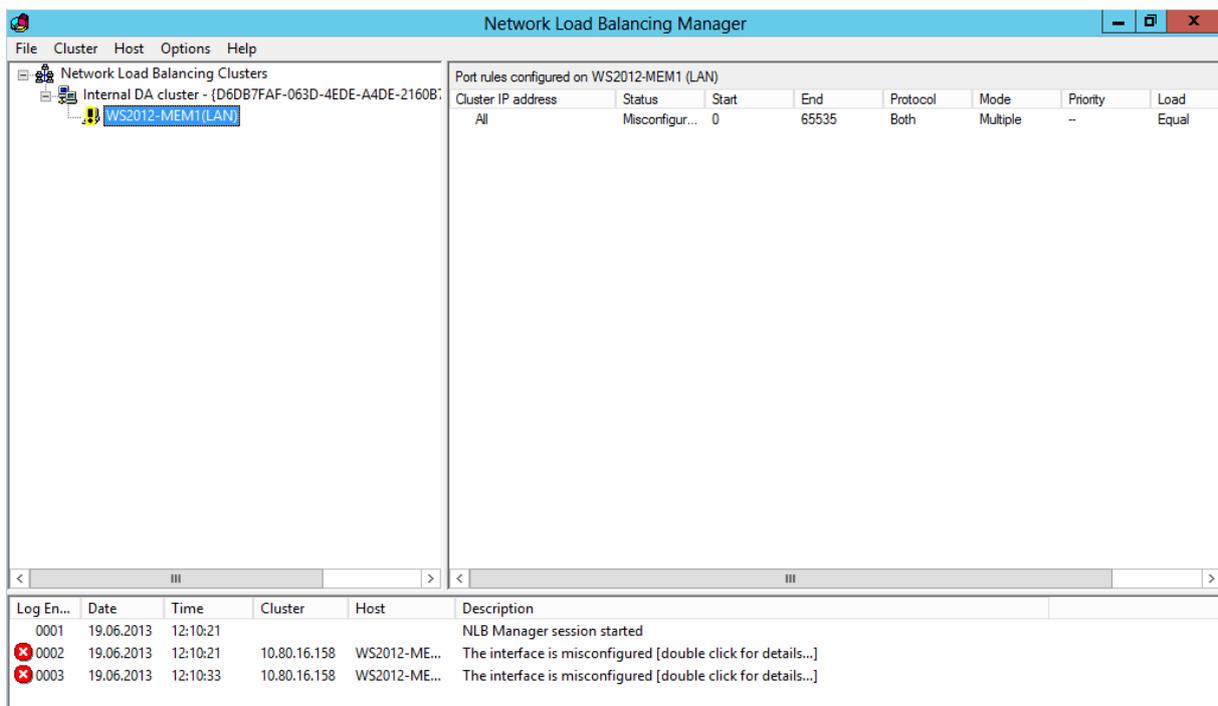
Geaendertes Script per Powershell ausfuehren

```
Administrator: Windows PowerShell
BACKUP> Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress @('10.80.16.159/255.255.252.0') -InternetVirtualIP @('10.80.16.158/255.255.252.0') -ComputerName 'WS2012-MEM1.win2012.server' -Verbose
Retrieving server GPO details...
Opening the server GPO...
Retrieving computer details...
Retrieving network adapter information...
Creating a load balanced cluster and adding server WS2012-MEM1.win2012.server to it...
Creating a load balancing cluster and adding server WS2012-MEM1.win2012.server to the cluster...
Finalizing load balancing settings. This might take a few minutes...
BACKUP>
```

Danach



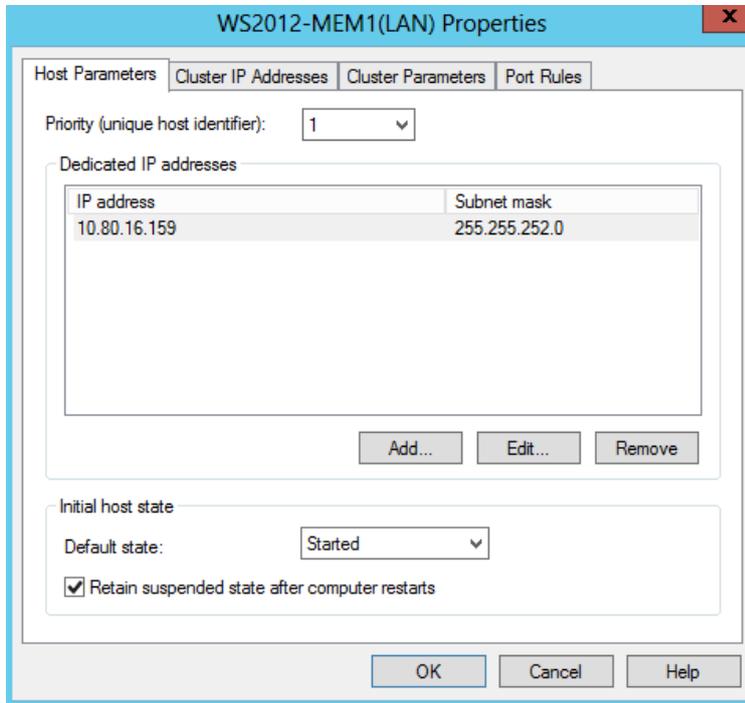
NLB Konsole



Der NLB Prozess hat die DIP nicht in die VIP auf der NIC geaendert und die neue VIP hinzugefuegt. In den NIC Properties die DIP aendern, NLB Kontrollkaestchen

einmal deaktivieren und aktivieren und auf NLB Convergence warten. Danach ist in der URA-Konsole alles gruen

Default State auf Start stellen fuer NLB Knoten



Danach ist alles OK

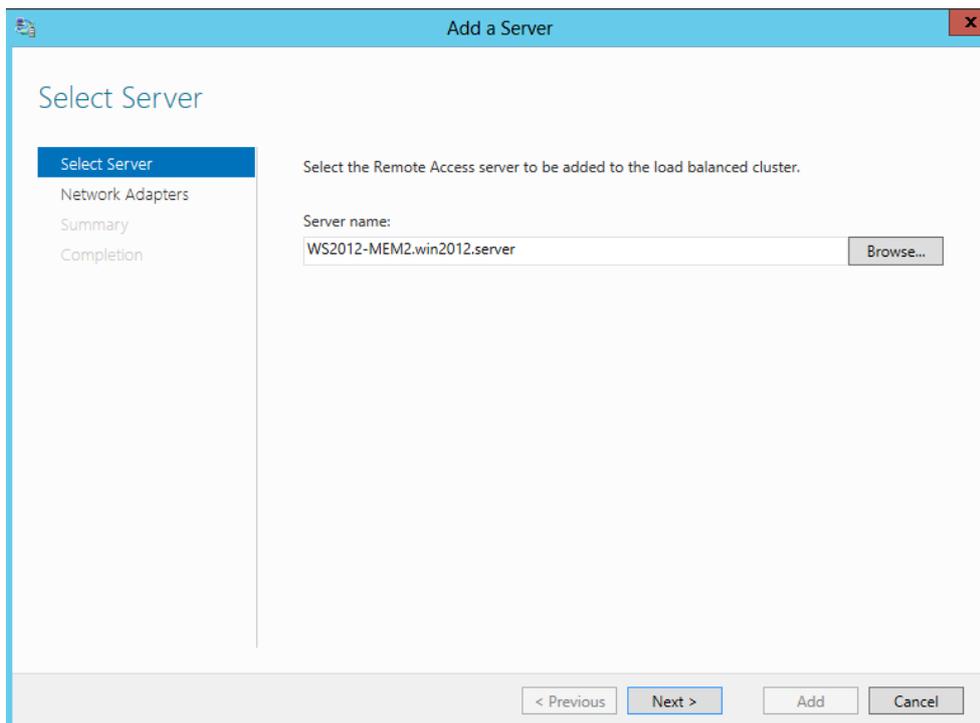
The screenshot shows the Group Policy Editor with the following settings for the 'win2012.server\DirectAccess Server Settings' GPO:

- Server GPO:** win2012.server\DirectAccess Server Settings
- Configure Entry Point Settings:** [Configure Entry Point Settings](#)
- Client support:** Limit access to client computers running Windows 8 or a later operating system
- VPN support:** VPN is not enabled on this entry point. [Enable VPN](#)
- Load balancing configuration:** Load balancing is enabled on this entry point. Method: Windows NLB

Server Name	External Adapter	Internal Adapter	VPN Static Pool
WS2012-MEM1.win2012.server	LAN	LAN	

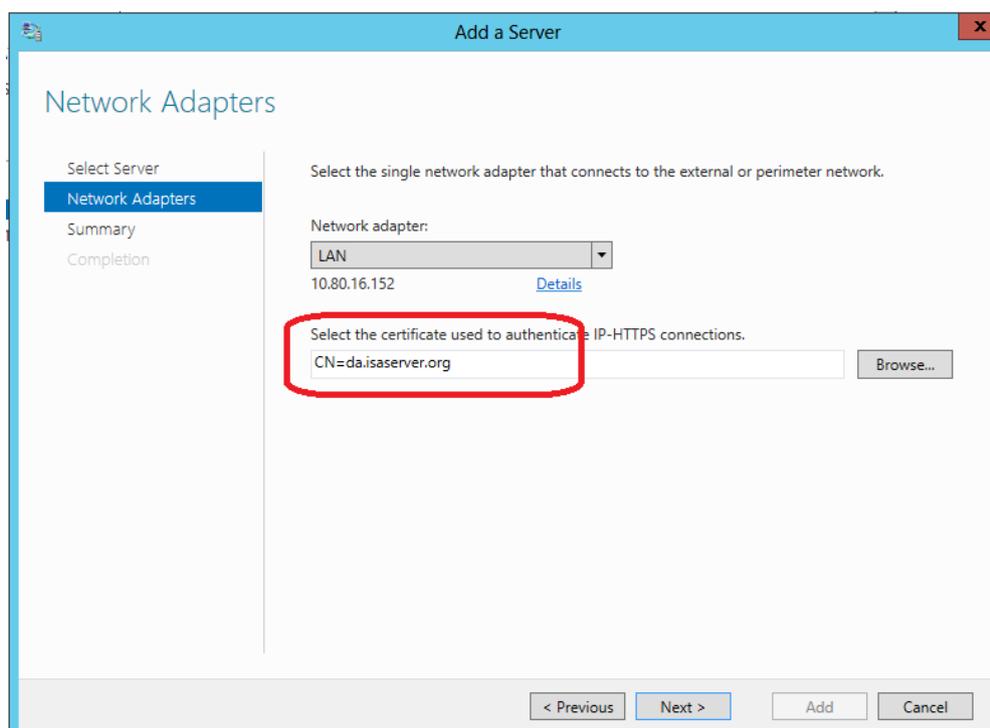
At the bottom, there are three links: [Disable Load Balancing](#), [Configure Load Balancing Settings](#), and [Add or Remove Servers](#).

## Server hinzufuegen



The screenshot shows the 'Add a Server' wizard window. The title bar reads 'Add a Server'. The main heading is 'Select Server'. On the left, a navigation pane lists 'Select Server' (highlighted), 'Network Adapters', 'Summary', and 'Completion'. The main area contains the instruction: 'Select the Remote Access server to be added to the load balanced cluster.' Below this, there is a 'Server name:' label and a text input field containing 'WS2012-MEM2.win2012.server'. A 'Browse...' button is to the right of the input field. At the bottom, there are four buttons: '< Previous', 'Next >', 'Add', and 'Cancel'.

Darauf achten, dass das Zertifikat das richtige ist



The screenshot shows the 'Add a Server' wizard window at the 'Network Adapters' step. The title bar reads 'Add a Server'. The main heading is 'Network Adapters'. On the left, a navigation pane lists 'Select Server', 'Network Adapters' (highlighted), 'Summary', and 'Completion'. The main area contains the instruction: 'Select the single network adapter that connects to the external or perimeter network.' Below this, there is a 'Network adapter:' label and a dropdown menu showing 'LAN'. Below the dropdown, the IP address '10.80.16.152' is displayed, with a 'Details' link. A red rectangle highlights the 'Select the certificate used to authenticate IP-HTTPS connections.' instruction and the text input field below it, which contains 'CN=da.isaserver.org'. A 'Browse...' button is to the right of the input field. At the bottom, there are four buttons: '< Previous', 'Next >', 'Add', and 'Cancel'.

## Konfiguration aktivieren

The screenshot shows the Remote Access Management Console interface. The main window displays the 'Entry Point Configuration Summary' with the text 'Entry point configuration:'. A modal dialog box titled 'Adding or Removing Servers' is open, showing a progress bar and a list of tasks. The tasks are:

- Retrieving server GPO details...
- Opening the server GPO...
- Opening the client GPOs...
- Checking for edit permissions on the client GPOs...
- Retrieving computer details...
- Validating the server adapters...
- Checking for edit permissions on the server GPOs...
- Clearing existing stale configuration settings. This might take...
- Verifying required certificates on the server...
- Verifying required certificates on the server...
- Adding server WS2012-MEM2.win2012.server to the load b...
- Adding the server to the server GPO...

The dialog box also includes a 'Commit' button and a 'Cancel' button.

## Error

The screenshot shows the Remote Access Management Console interface displaying a 'Configuration Load Error' message. The message text is:

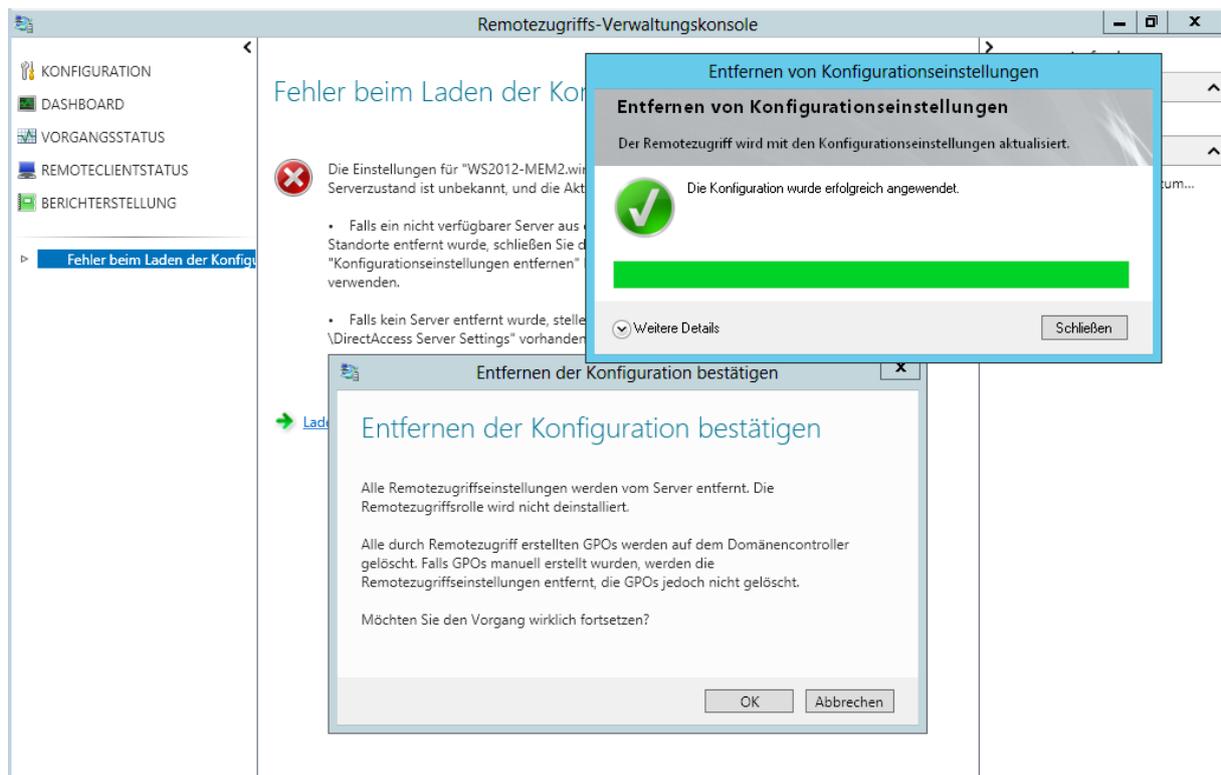
Remote Access detected that a previous configuration change failed and cannot be applied. The current configuration might be corrupted. A backup was made before the failure. Select to restore configuration settings from the backup, or delete the backup and attempt to load the current configuration.

Below the message, there are two buttons:

- [Restore from Backup](#)
- [Load the current configuration](#)

The console also shows a navigation menu on the left with options: CONFIGURATION, DASHBOARD, OPERATIONS STATUS, REMOTE CLIENT STATUS, and REPORTING. The 'Configuration Load Error' is selected in the menu.

## Konfiguration entfernen



Nochmal probieren. Sollte es dann nicht funktionieren, kann der Trick helfen den zweiten NLB Knoten in der NLB Konsole zum NLB Cluster hinzuzufügen und dann die NLB Konfiguration in der Remote Access Management Console nochmal durchzuführen und den zweiten Knoten hinzuzufügen.

### Load balancing configuration:

Load balancing is enabled on this entry point.

Method: Windows NLB

Server Name	External Adapter	Internal Adapter	VPN Static Pool
WS2012-MEM1.win2012.server	LAN	LAN	
WS2012-MEM2.win2012.server	LAN	LAN	

[→ Disable Load Balancing](#)   [→ Configure Load Balancing Settings](#)   [→ Add or Remove Servers](#)