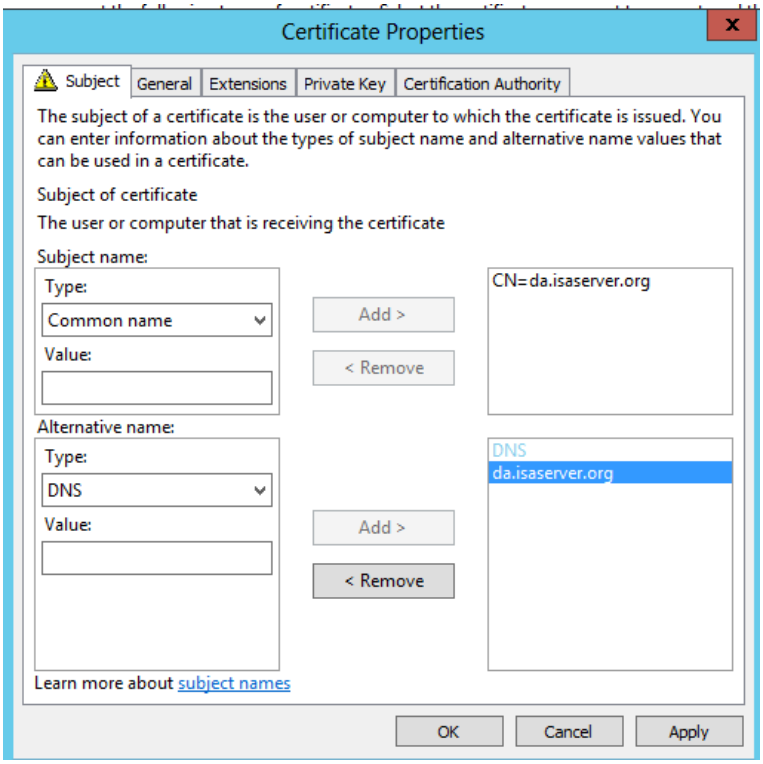
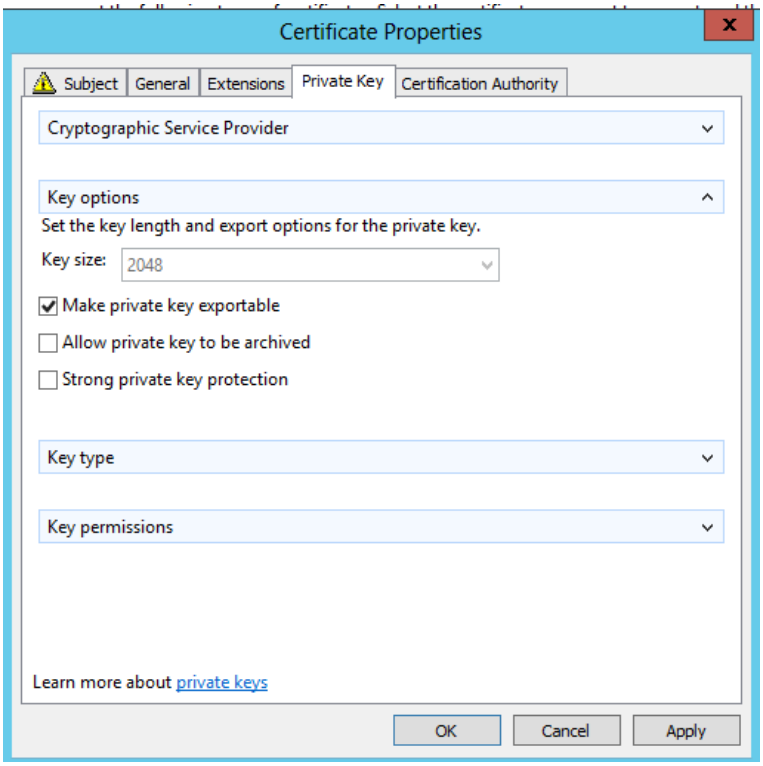
Windows Server 2012 DirectAccess Multisite und NLB Deployment

Korrektes Zertifikat fuer IP-HTTPS ausstellen



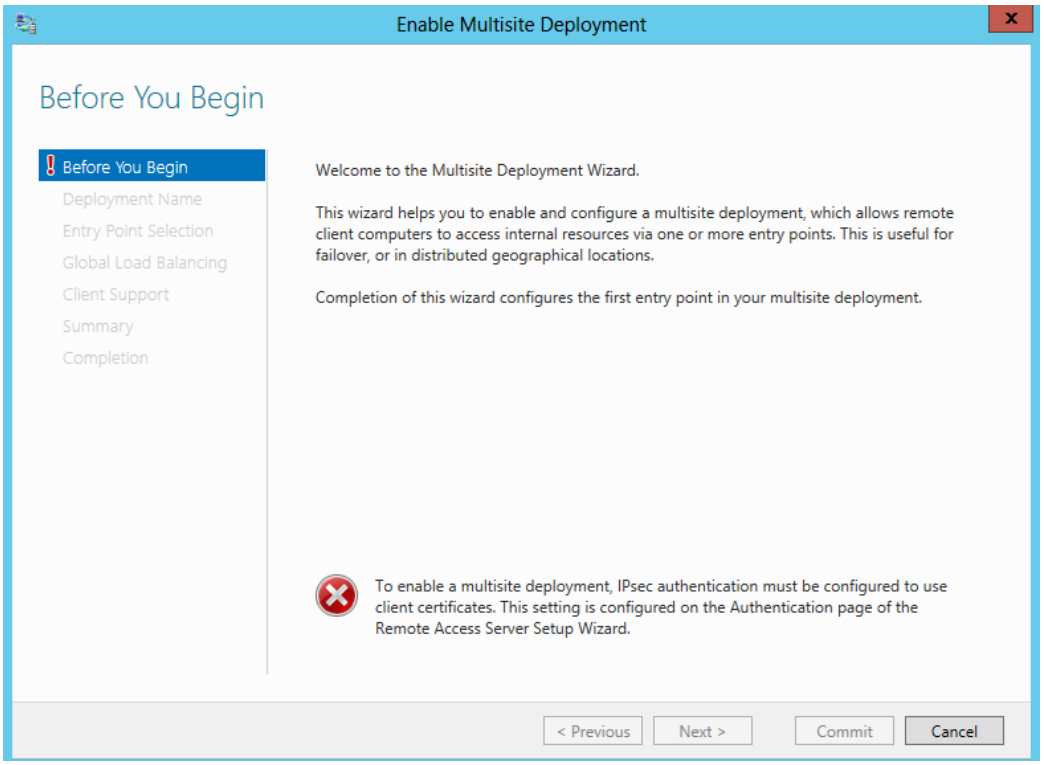
Private Key exportable weil dieses auf dem anderen DA Server importiert werden muss fuer NLB Cluster



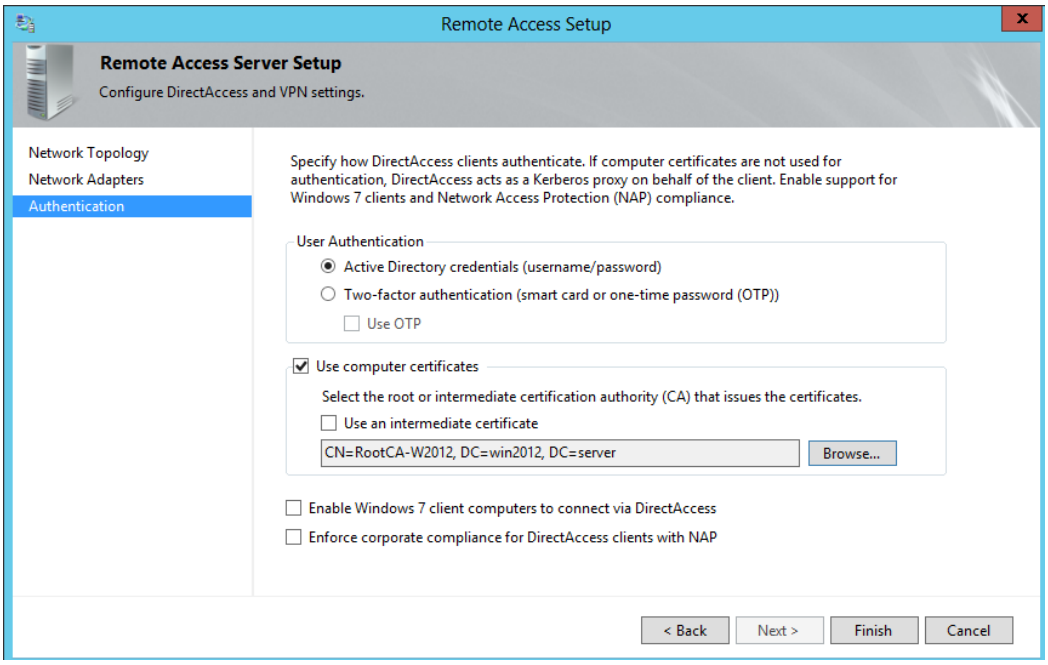
Zertifikat mit .PFX exportieren und auf dem anderen DA Server importieren

Multisite Deployment

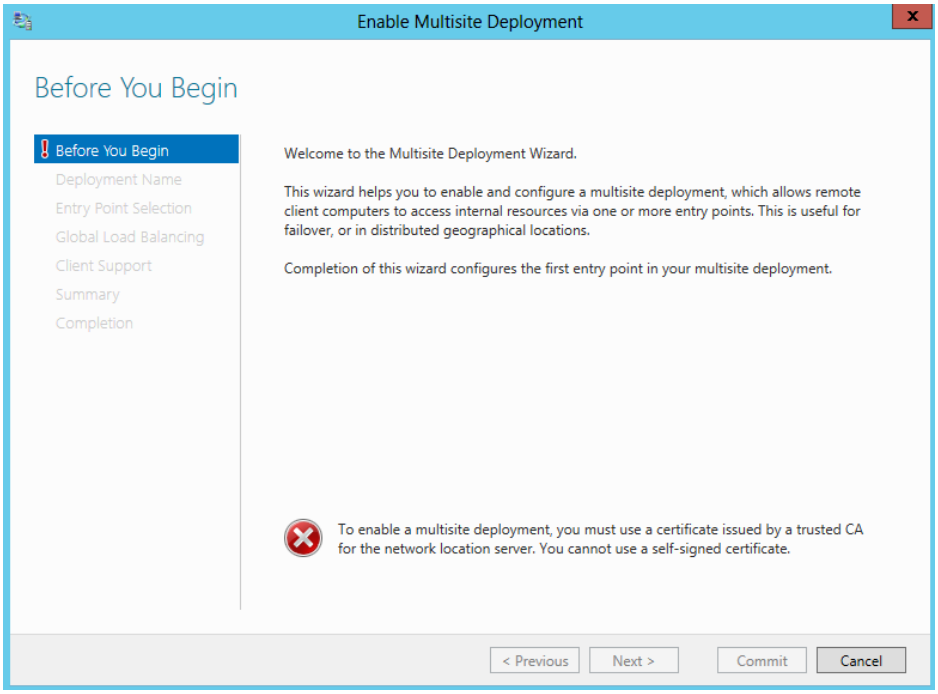
Als erstes das Multisite Deployment testen



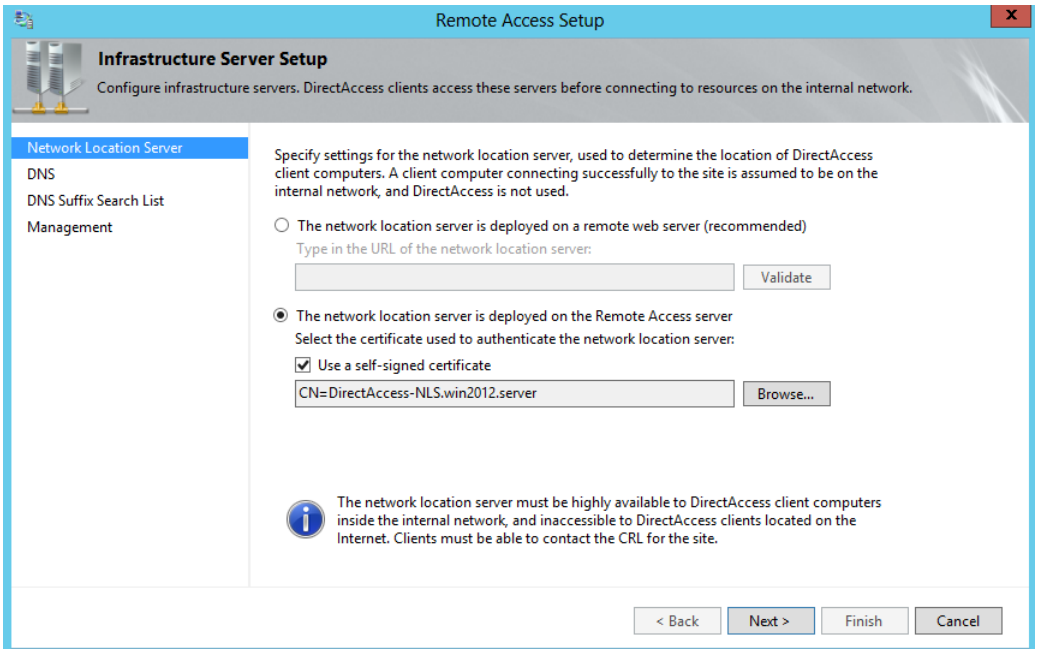
Kein KDC-Proxy, hier werden Zertifikate benoetigt

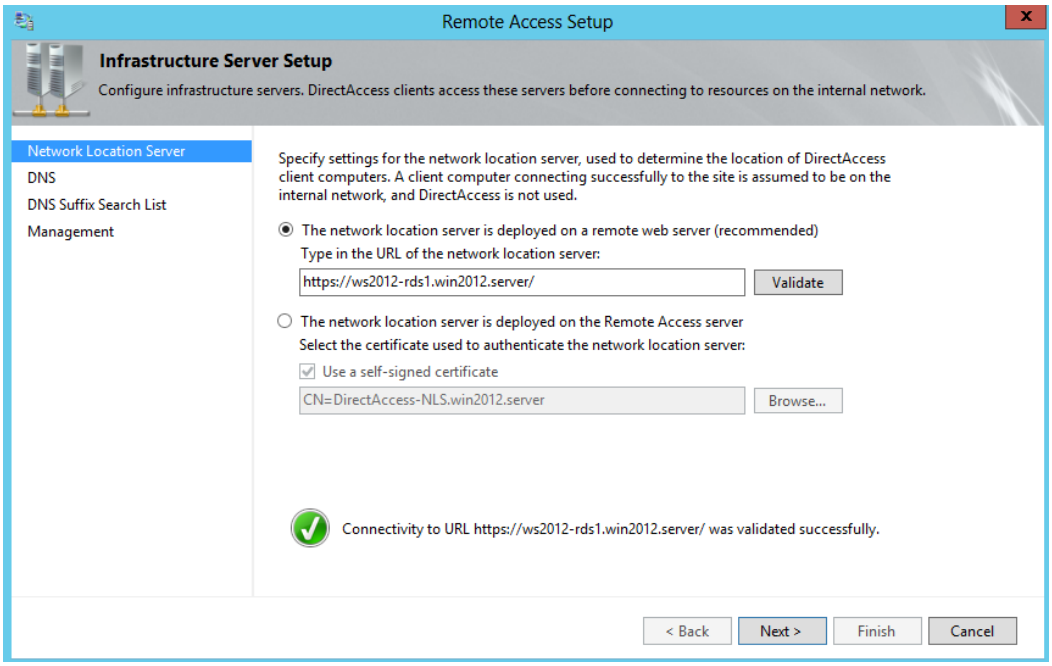


Der NLS Server darf kein Self Signed Certificate haben

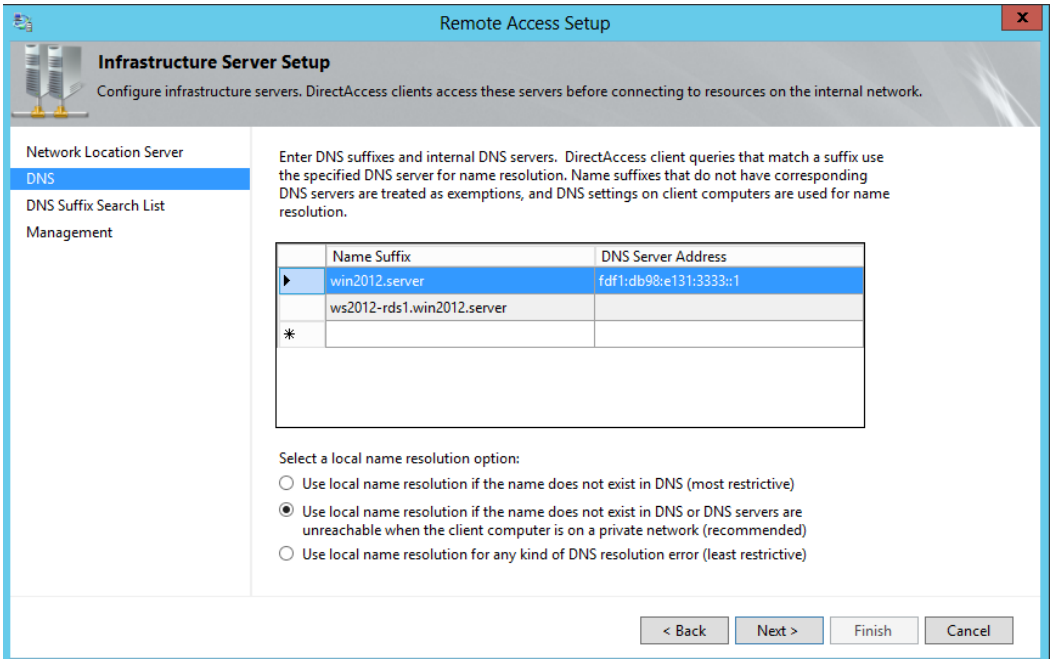


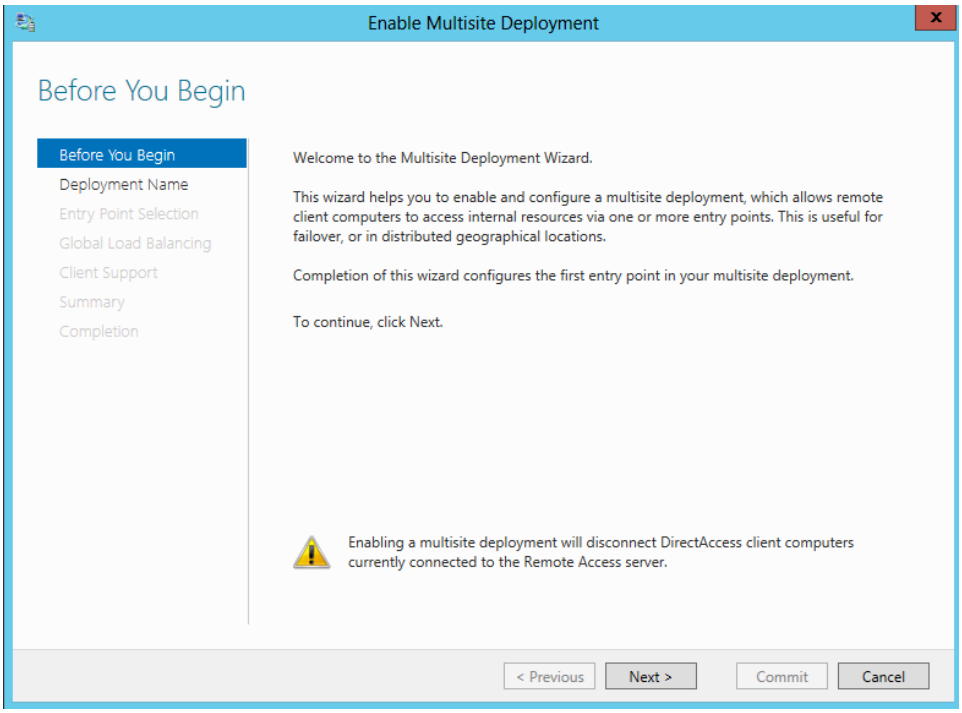
Am besten den NLS Server wie bei UAG auf eine andere, hochverfuegbare Maschine legen



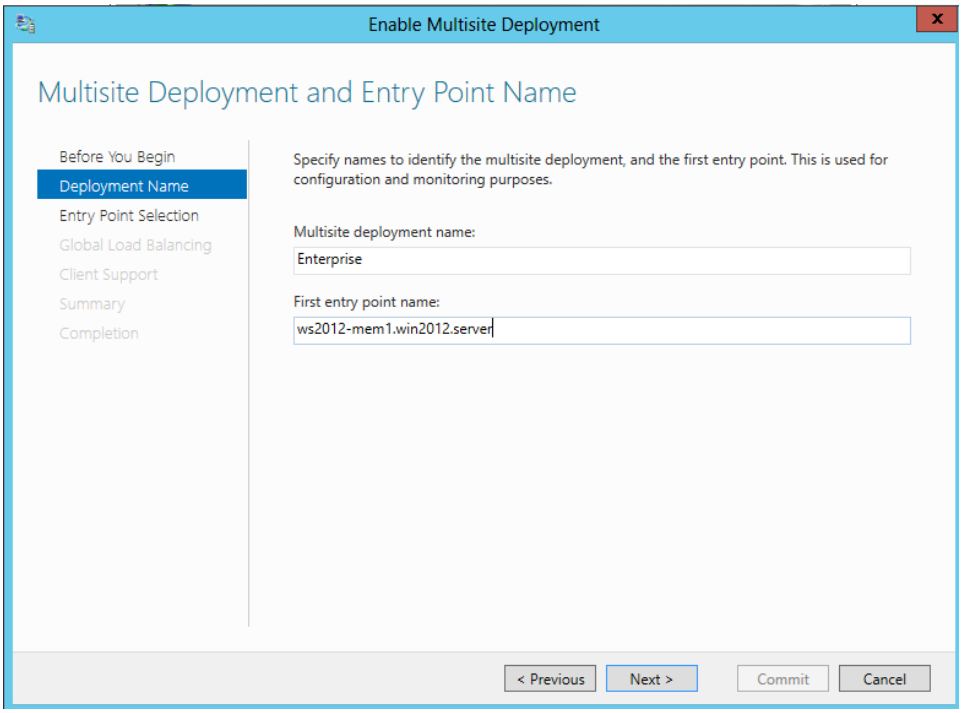


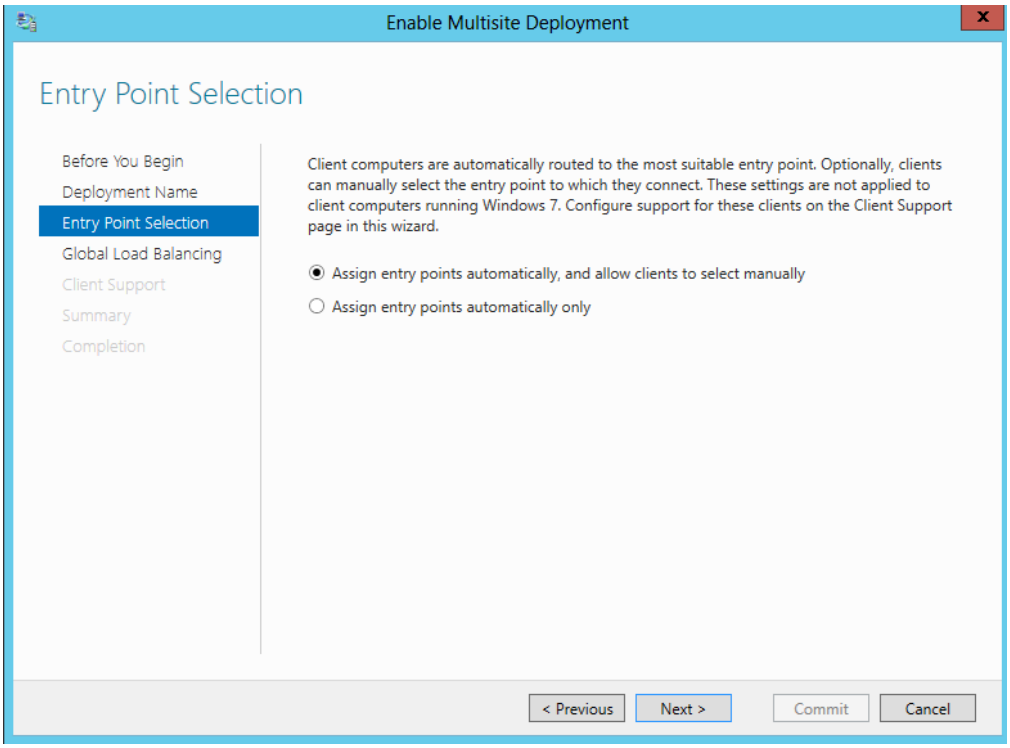
ACHTUNG: Wie bei Forefront UAG ist der NLS Server von DA Clients nicht erreichbar und sollte hochverfuegbar betrieben werden



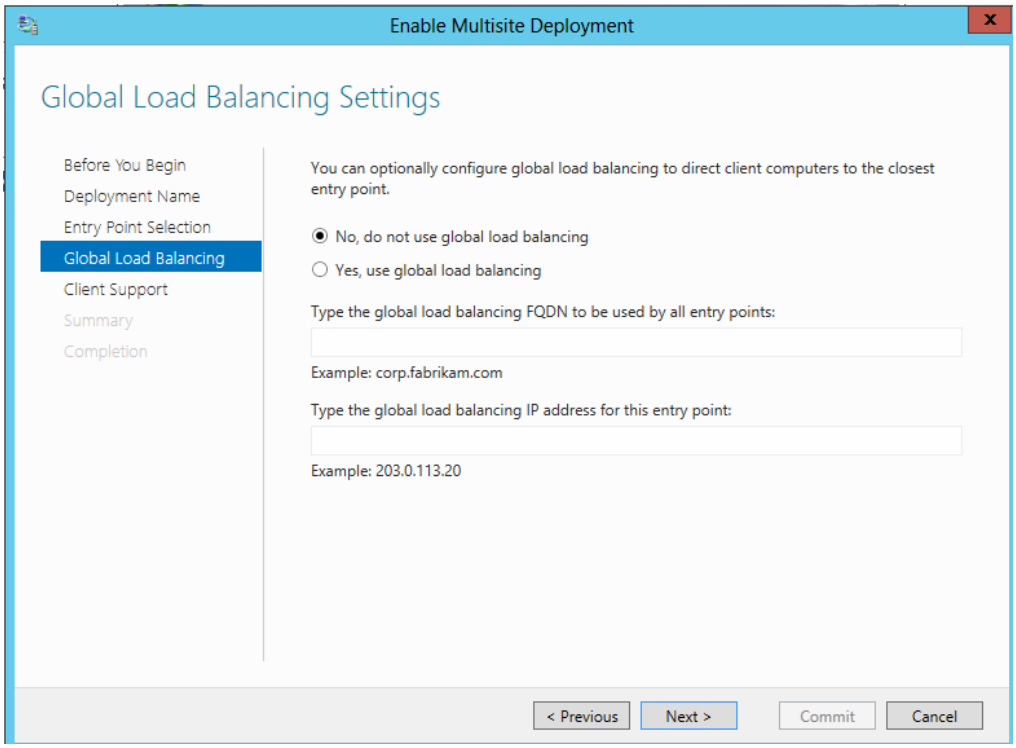


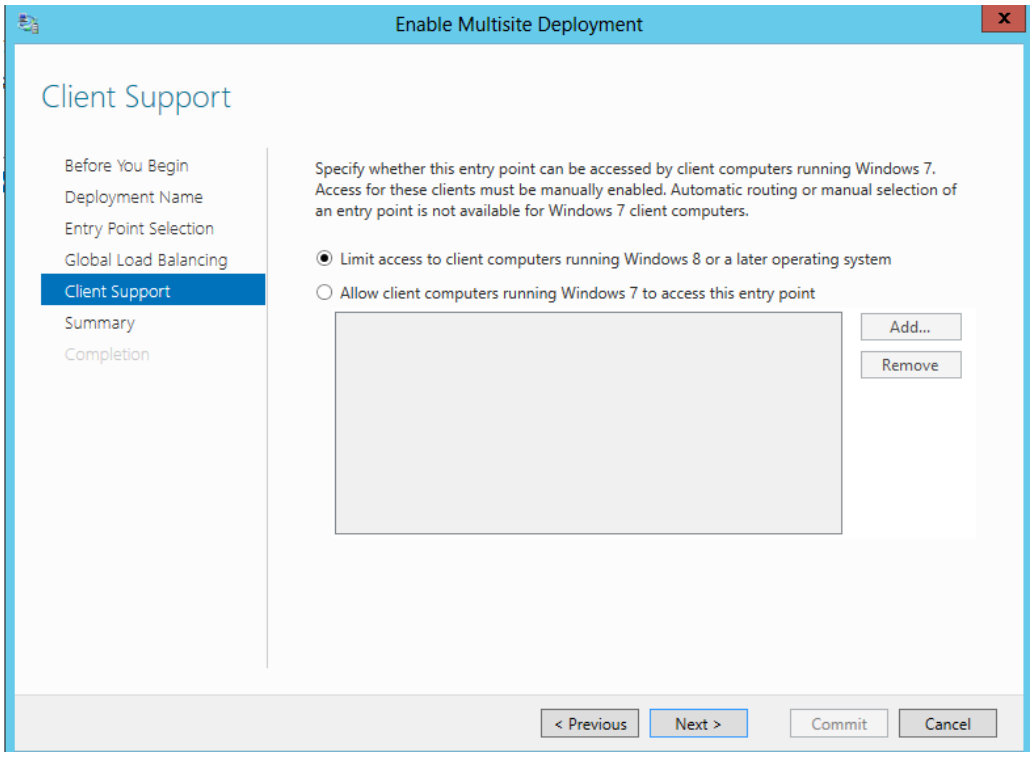
Entry Point Name ist in diesem Fall der Servername, besser waeren geografische Lokationen, siehe spaeter in diesem Artikel. Aenderung ist spaeter noch moeglich.



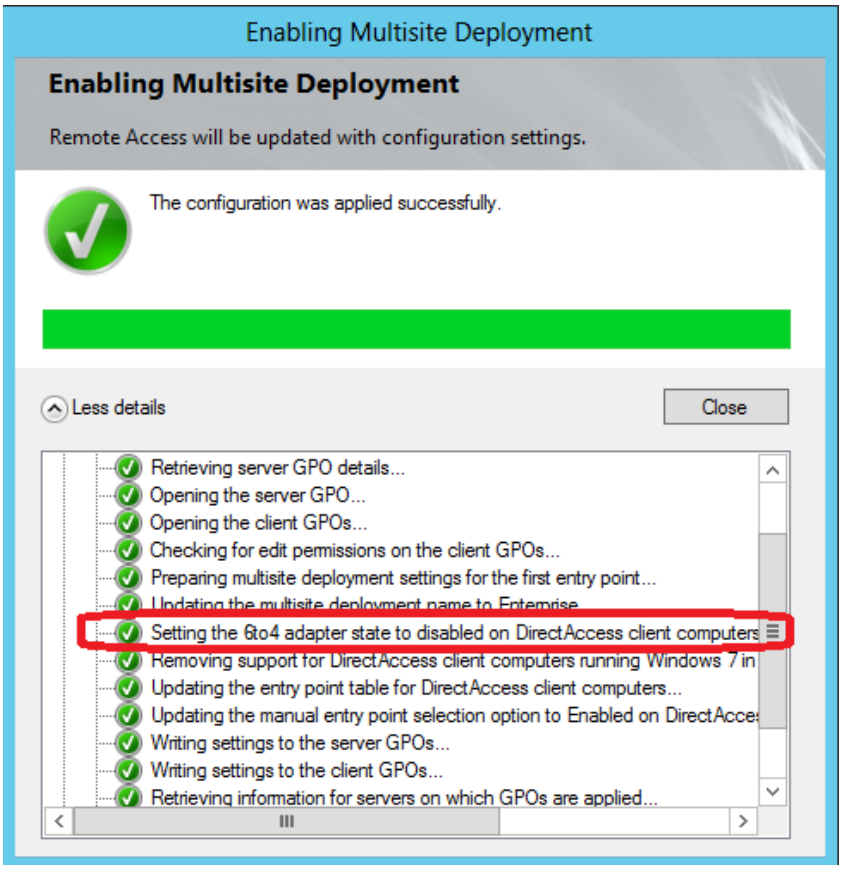


Wenn kein Global Load Balancer verfuegbar ist, abwaehlen. Der GLB wuerde automatisch den DA Client an die nahste Lokation verbinden!

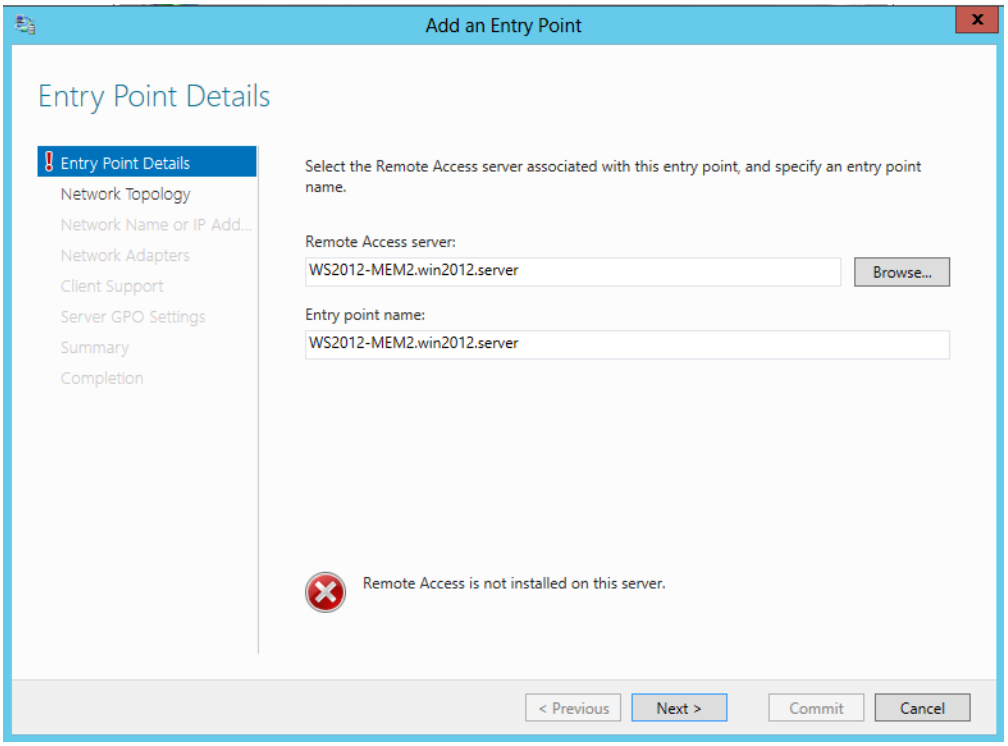




6to4 wird bei Multisite nicht supported

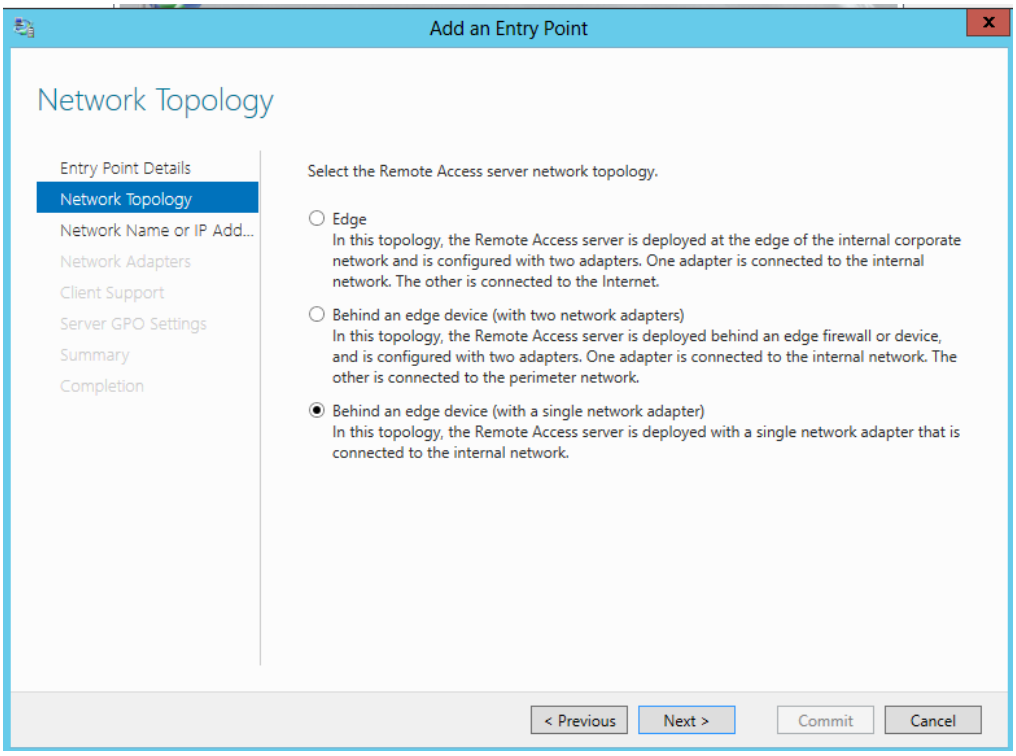


Zweiten DA Server am zweiten Standort hinzufuegen

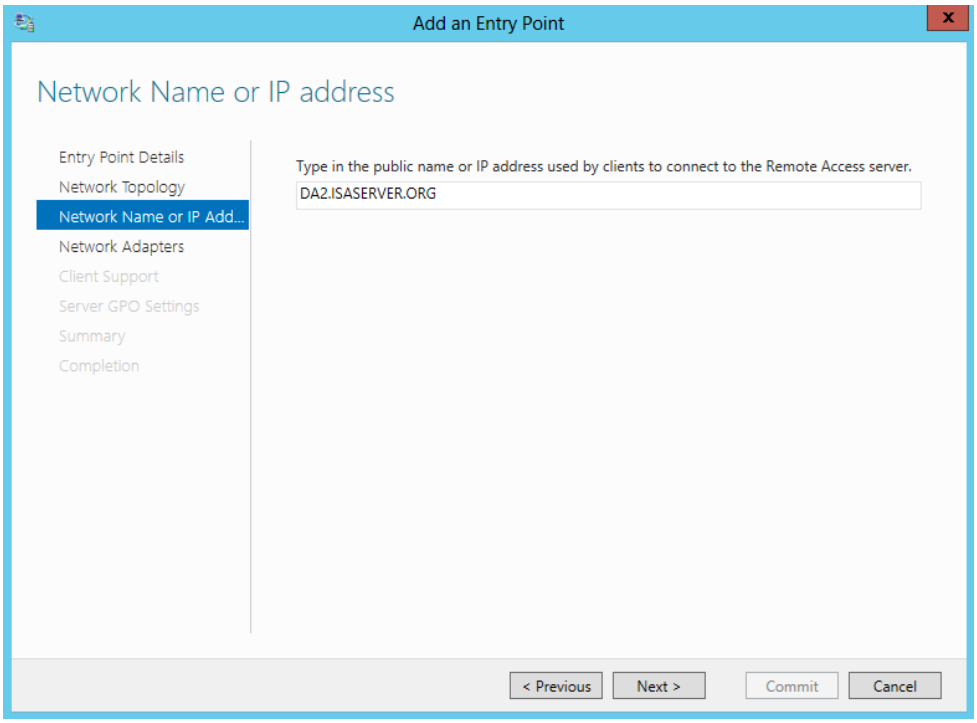


Rolle Remotezugriff hinzufuegen

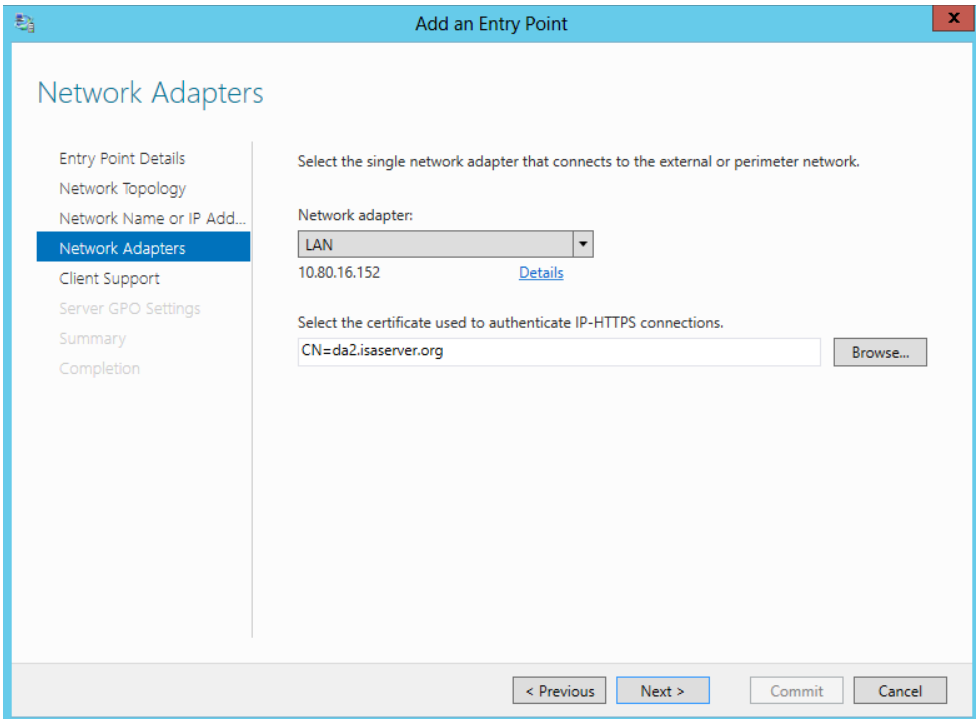
Wenn der Remote Server noch nicht konfiguriert wurde

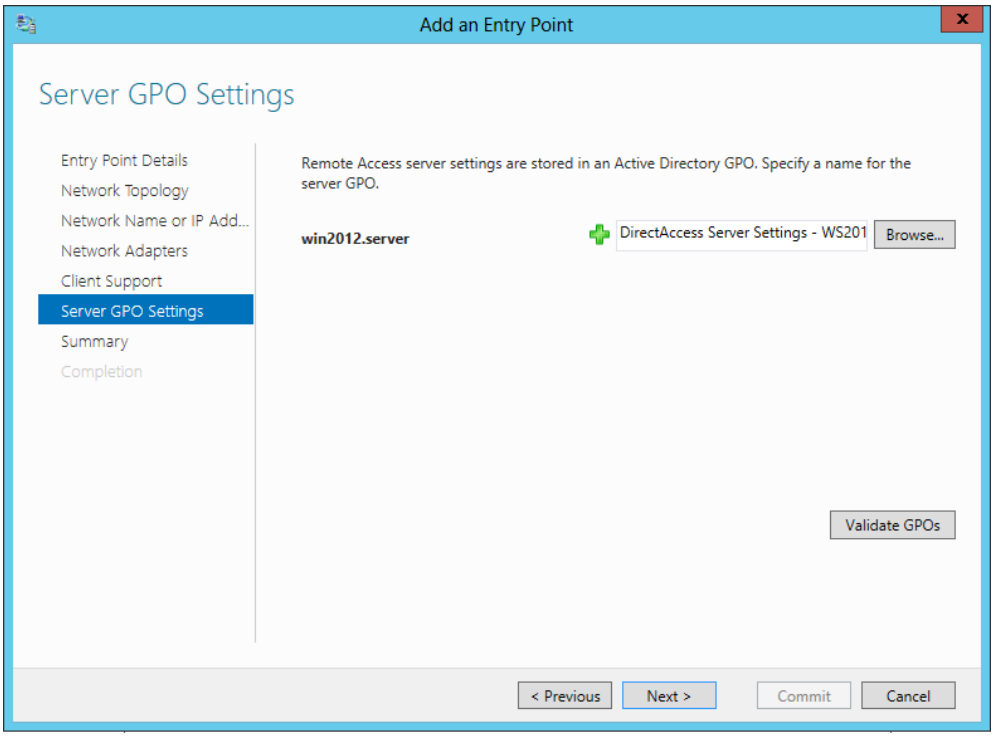


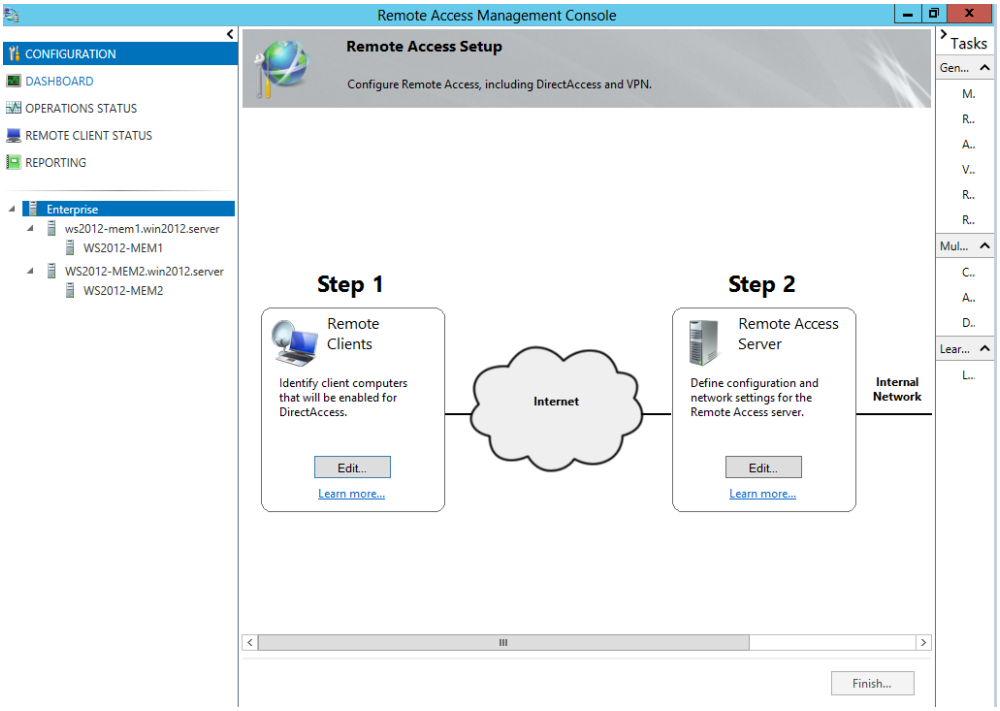
Der Name muss ein anderer sein und idealerweise dem Standort des neuen DA Server entsprechen.



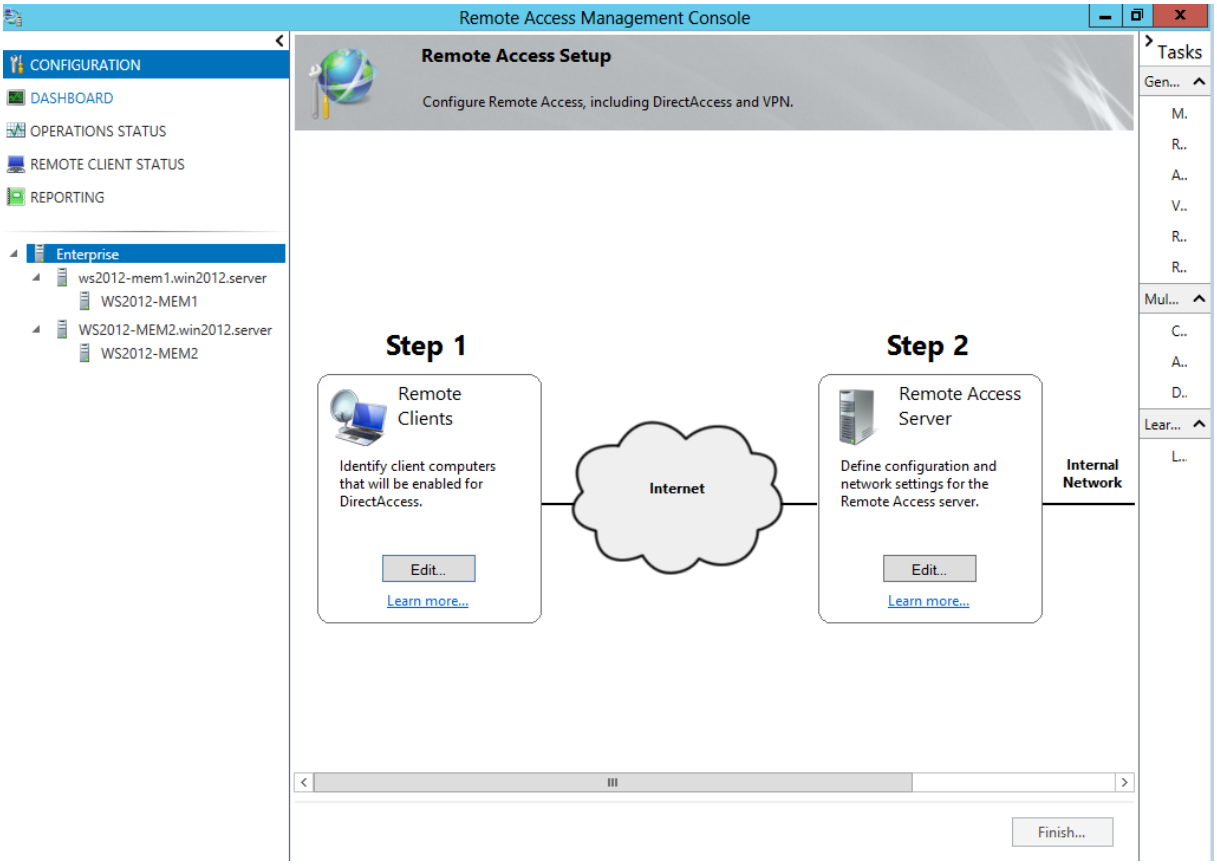
Ein entsprechendes Zertifikat muss vorhanden sein

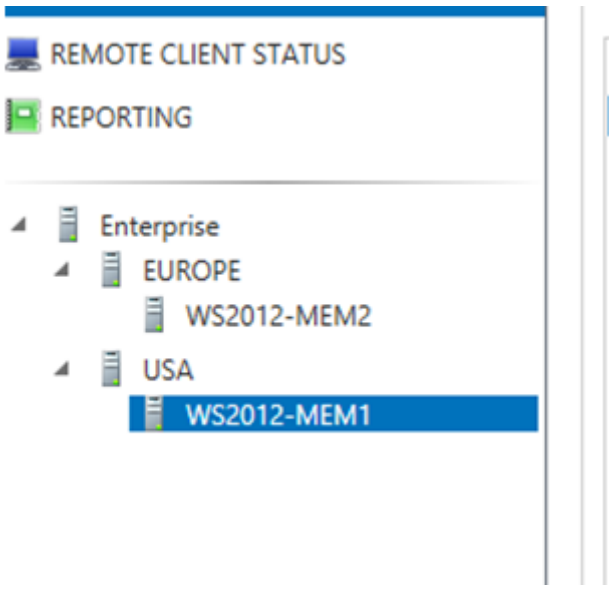



Add an Entry Point
Server GPO Settings
Entry Point Details
Network Topology
Network Name or IP Add...
Network Adapters
Client Support
Server GPO Settings
Summary
Completion
Remote Access server settings are stored in an Active Directory GPO. Specify a name for the server GPO.
win2012.server
DirectAccess Server Settings - WS201
Browse...
Validate GPOs
< Previous
Next >
Commit
Cancel

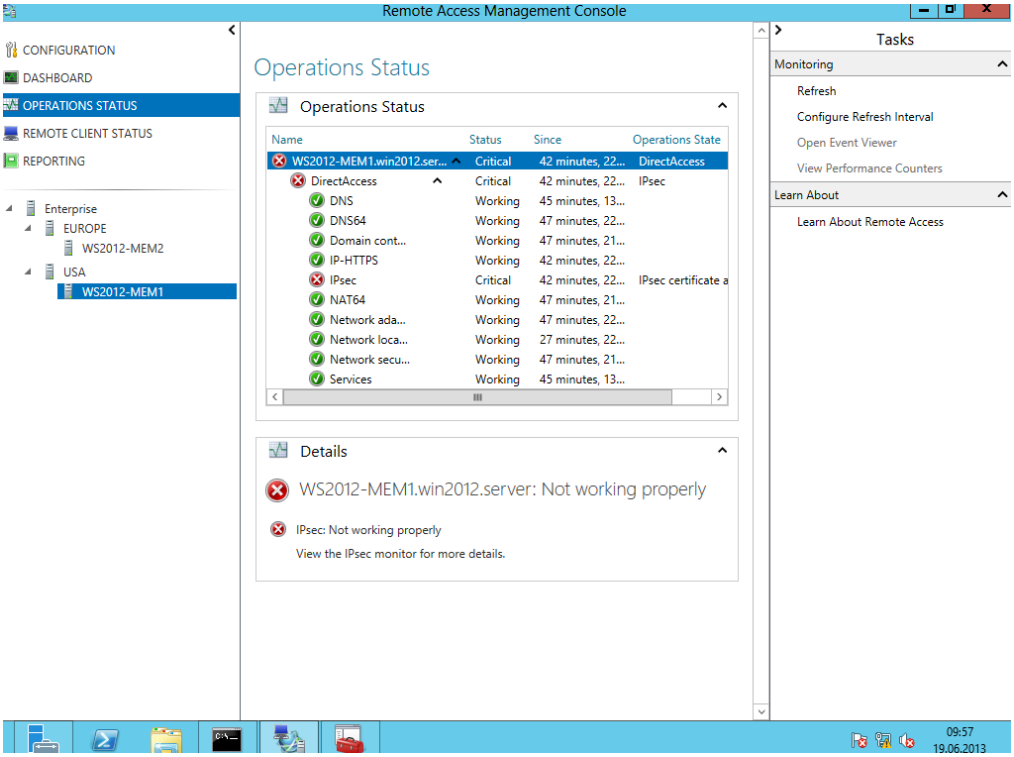

Remote Access Management Console
CONFIGURATION
DASHBOARD
OPERATIONS STATUS
REMOTE CLIENT STATUS
REPORTING
Enterprise
ws2012-mem1.win2012.server
WS2012-MEM1
WS2012-MEM2.win2012.server
WS2012-MEM2
Remote Access Setup
Configure Remote Access, including DirectAccess and VPN.
Tasks
Step 1
Remote Clients
Identify client computers that will be enabled for DirectAccess.
Edit...
Learn more...
Internet
Step 2
Remote Access Server
Define configuration and network settings for the Remote Access server.
Edit...
Learn more...
Internal Network
Finish...

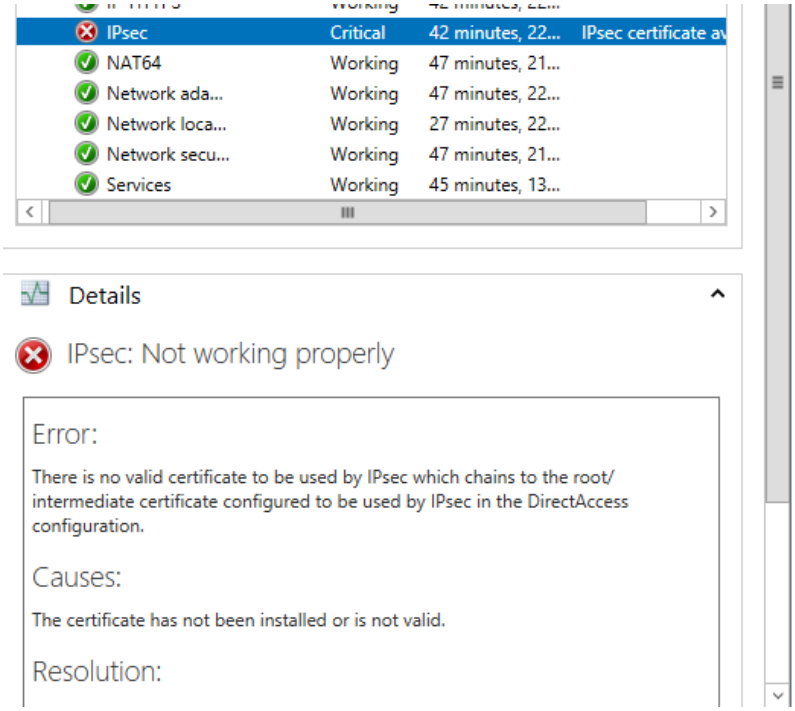
Entry Points umbenennen



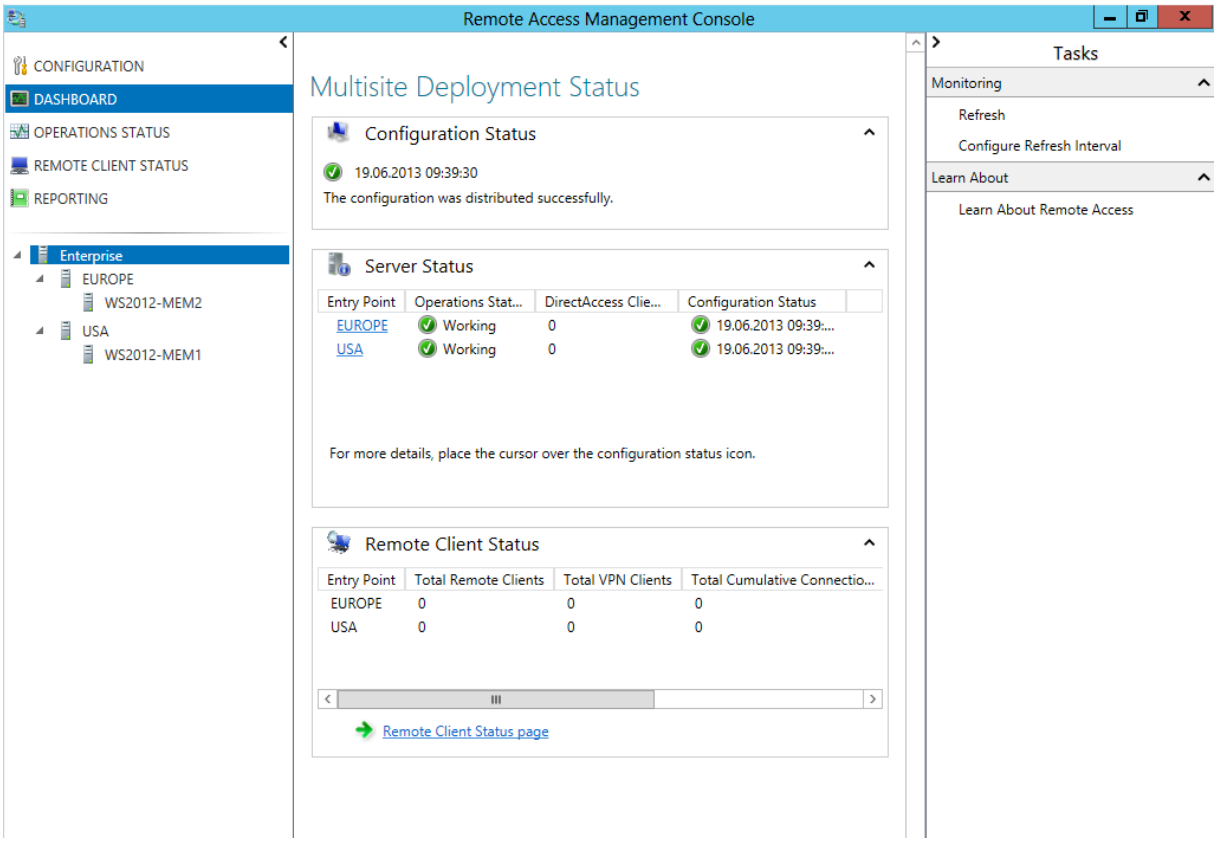


Computer Zertifikat fuer DA Server

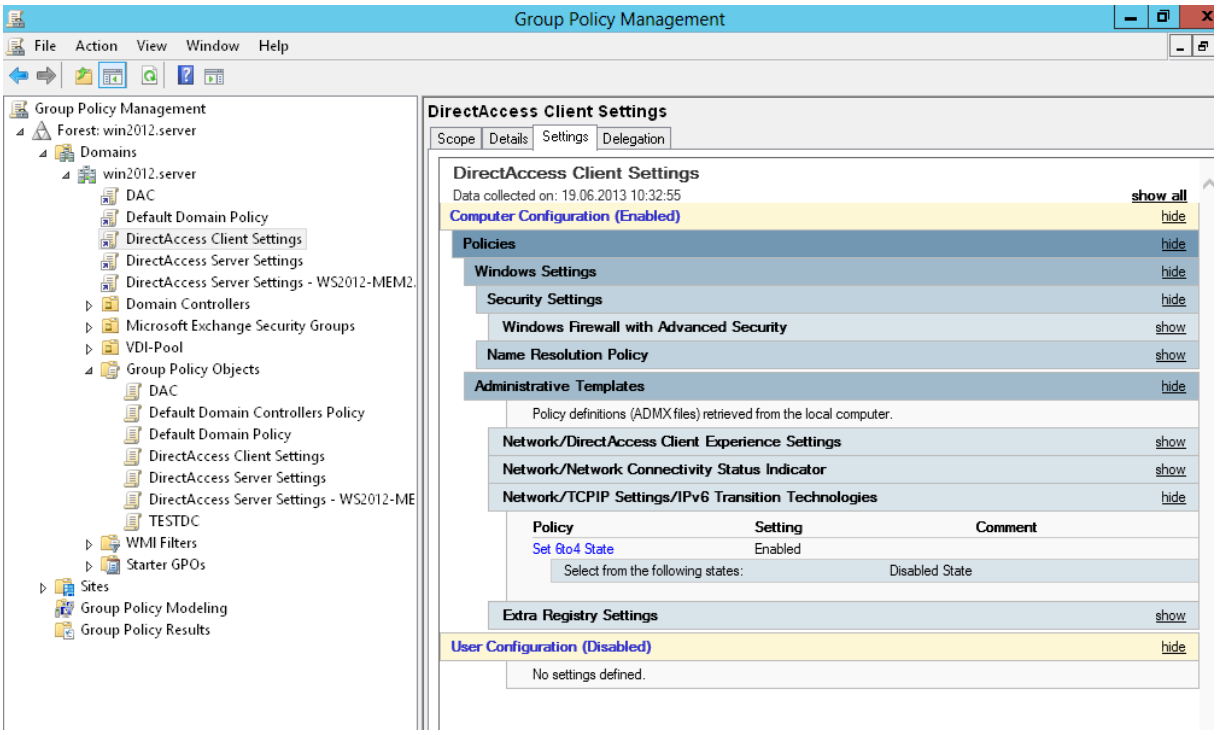




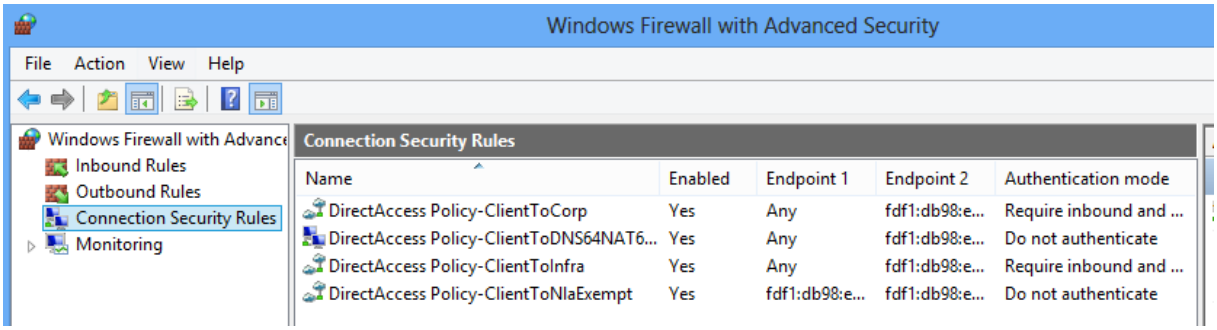
Status



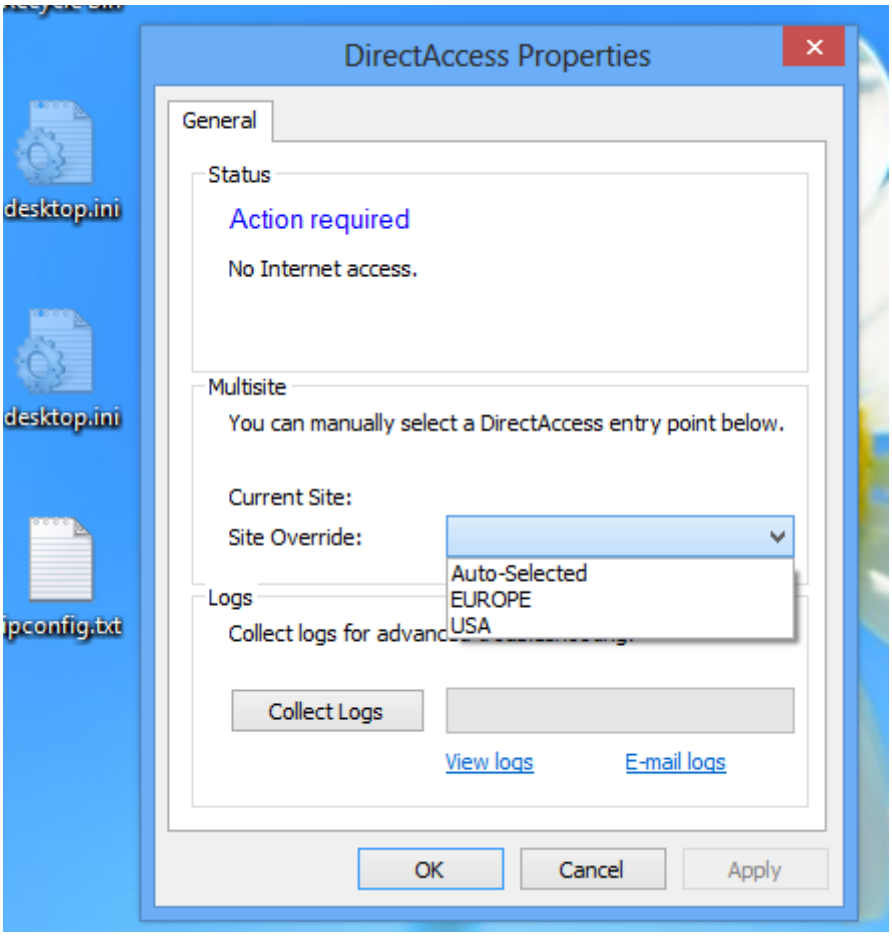
Group Policies



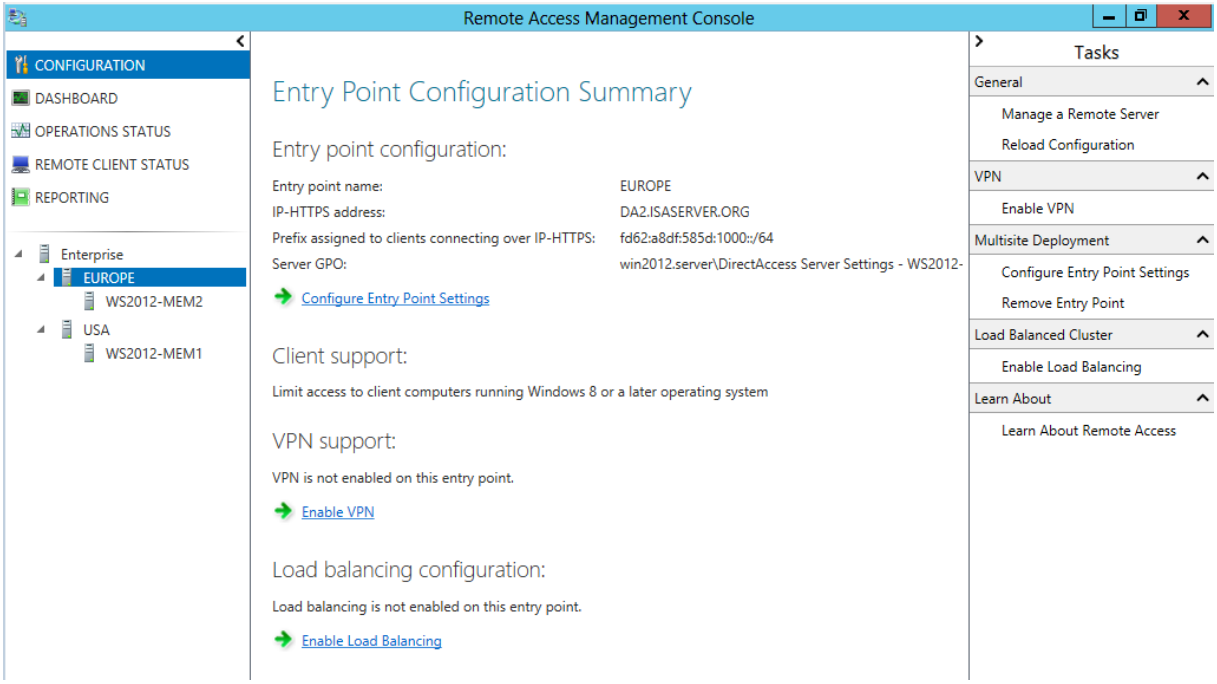
Firewalleinstellungen am Client

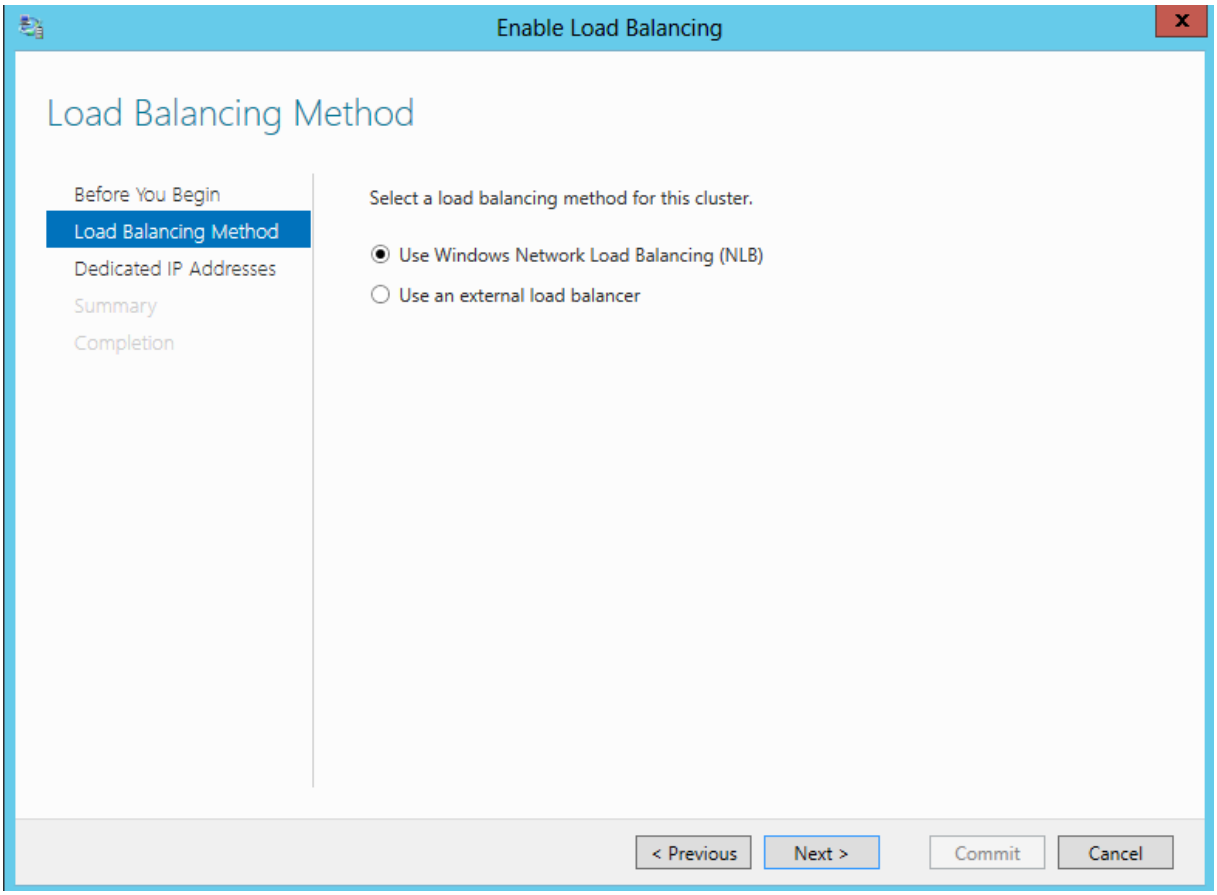


Multisite Auswahl am DA Client

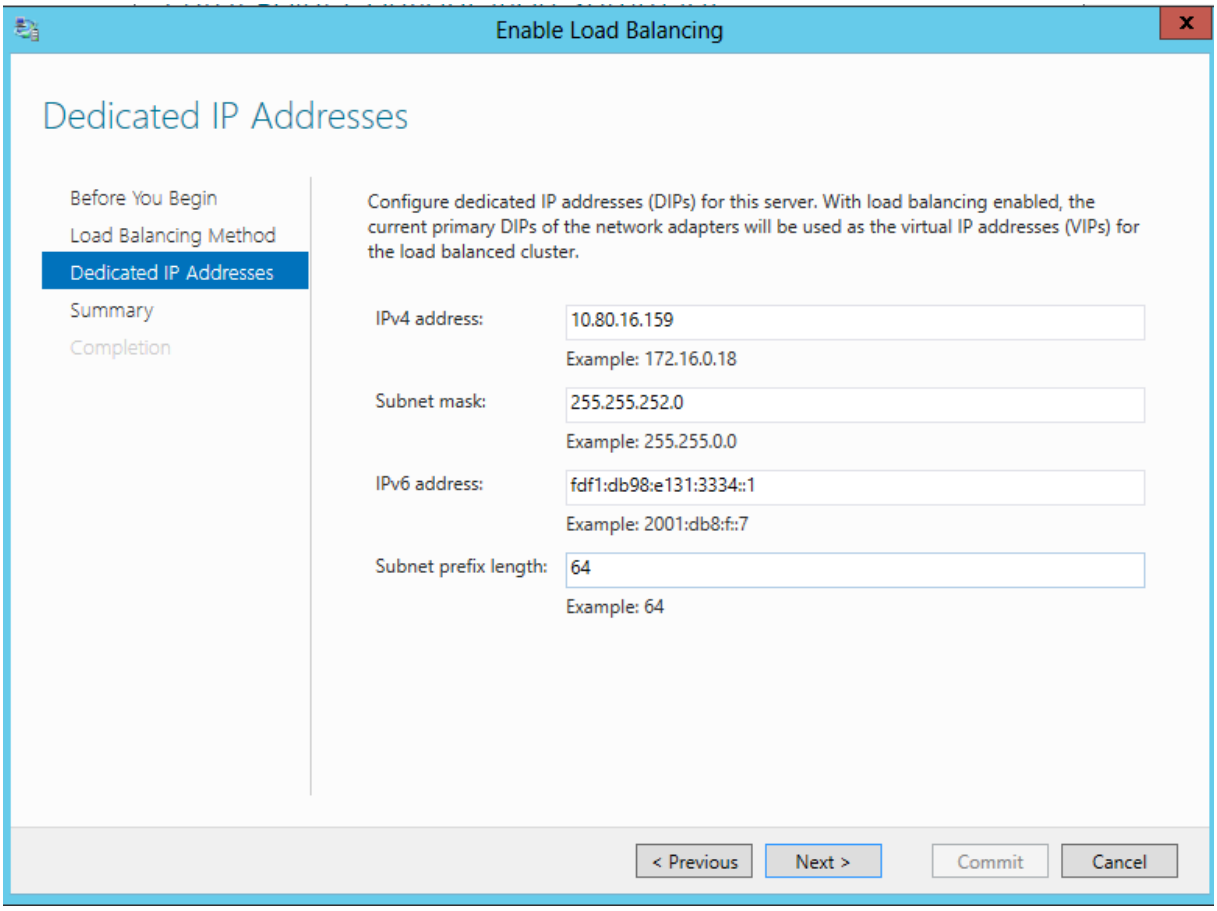


Load Balancing

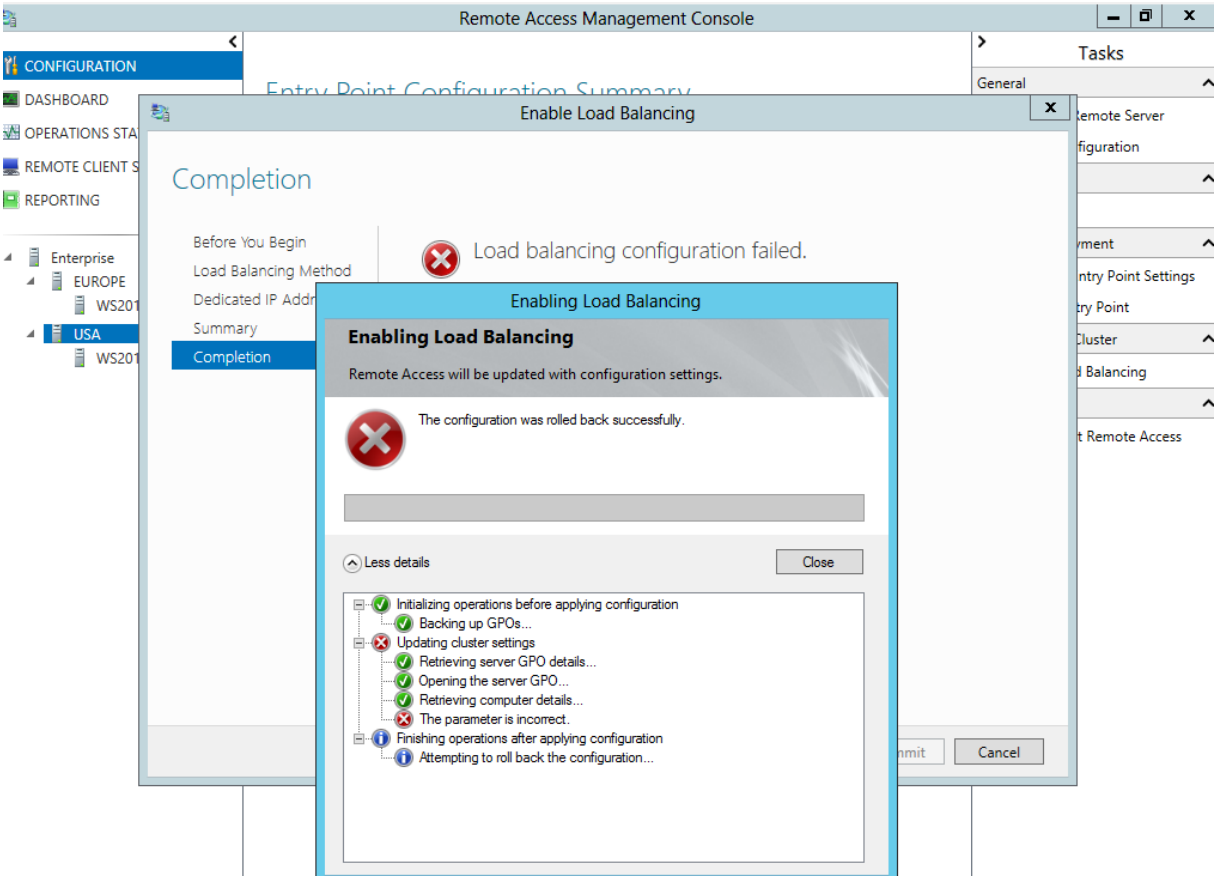




Achtung bei den IP Adressen. Die ehemaligen DIP werden VIP


Enable Load Balancing
Dedicated IP Addresses
Before You Begin
Load Balancing Method
Dedicated IP Addresses
Summary
Completion
Configure dedicated IP addresses (DIPs) for this server. With load balancing enabled, the current primary DIPs of the network adapters will be used as the virtual IP addresses (VIPs) for the load balanced cluster.
IPv4 address:
10.80.16.159
Example: 172.16.0.18
Subnet mask:
255.255.252.0
Example: 255.255.0.0
IPv6 address:
fdf1:db98:e131:3334::1
Example: 2001:db8:f::7
Subnet prefix length:
64
Example: 64
< Previous
Next >
Commit
Cancel

Error

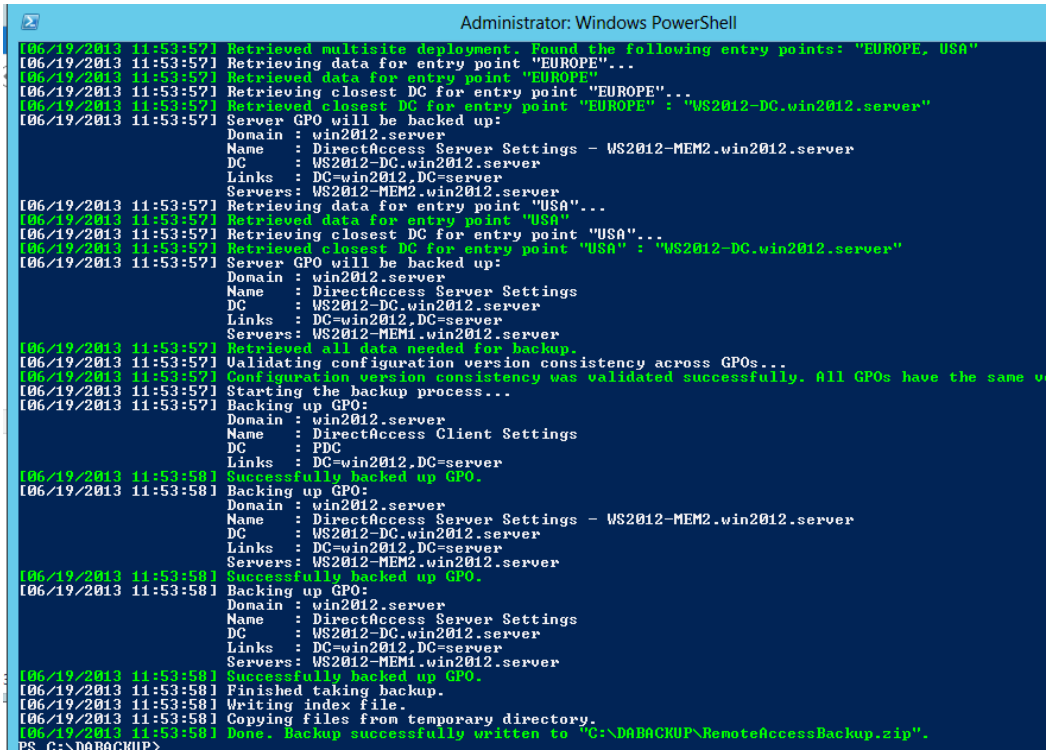

Remote Access Management Console
CONFIGURATION
DASHBOARD
OPERATIONS STA
REMOTE CLIENT S
REPORTING
Enterprise
EUROPE
USA
Tasks
General
Enable Load Balancing
Completion
Before You Begin
Load Balancing Method
Dedicated IP Addr
Summary
Completion
Load balancing configuration failed.
Enabling Load Balancing
Enabling Load Balancing
Remote Access will be updated with configuration settings.
The configuration was rolled back successfully.
Less details
Close
Initializing operations before applying configuration
Backing up GPOs...
Updating cluster settings
Retrieving server GPO details...
Opening the server GPO...
Retrieving computer details...
The parameter is incorrect.
Finishing operations after applying configuration
Attempting to roll back the configuration...
Cancel

Known issues:
http://technet.microsoft.com/de-de/library/jj134175.aspx

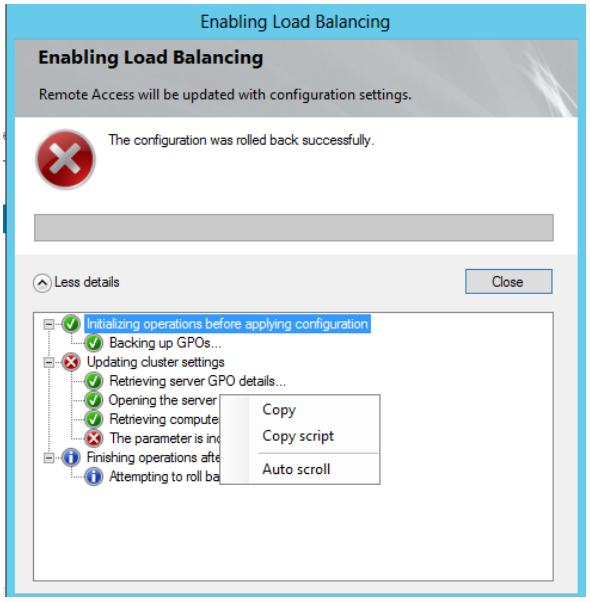
Auch an weitere Fixe denken

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



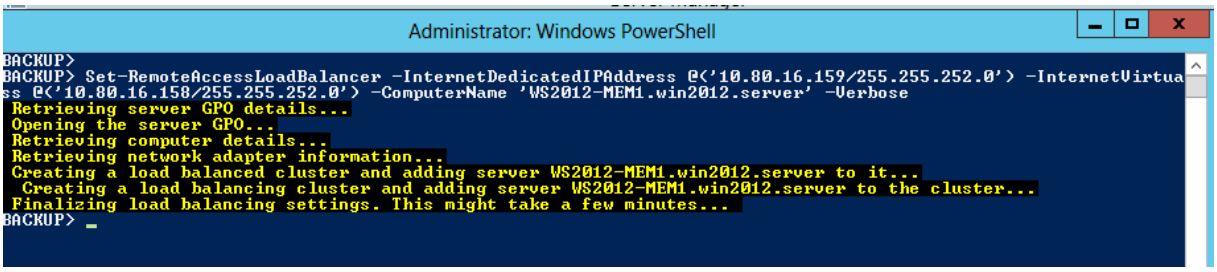
Copy Script



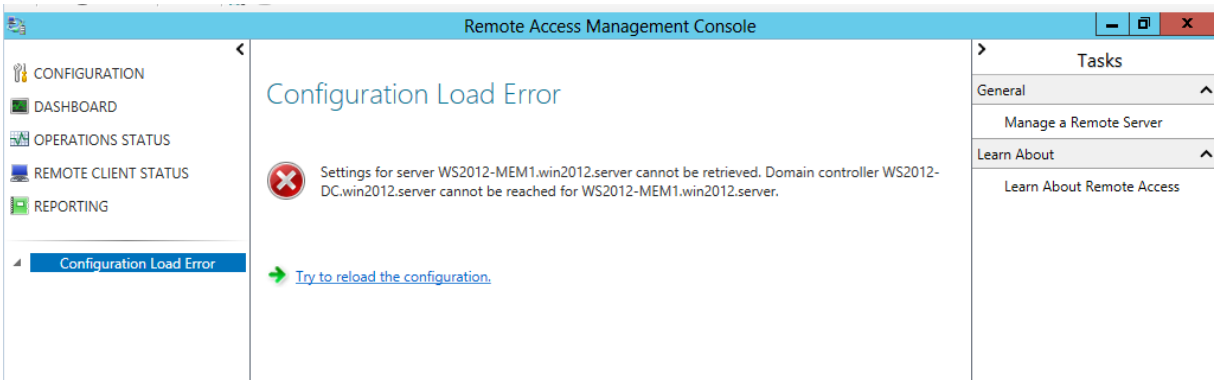
Mit Notepad editieren

IPv6 Adressen entfernen

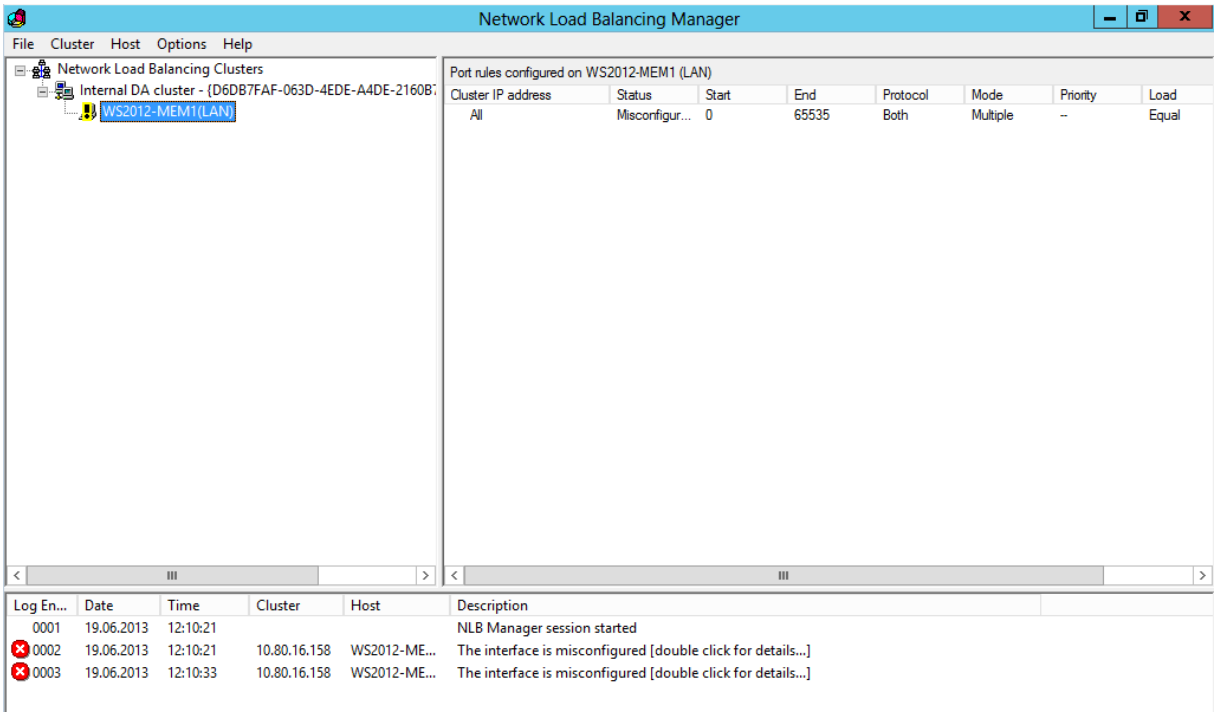
Geaendertes Script per Powershell ausfuehren



Danach



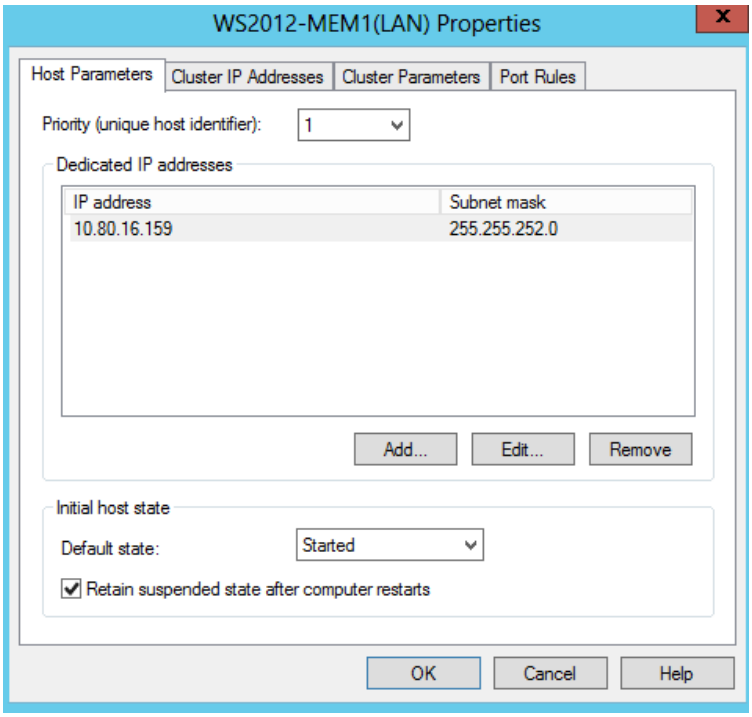
NLB Konsole



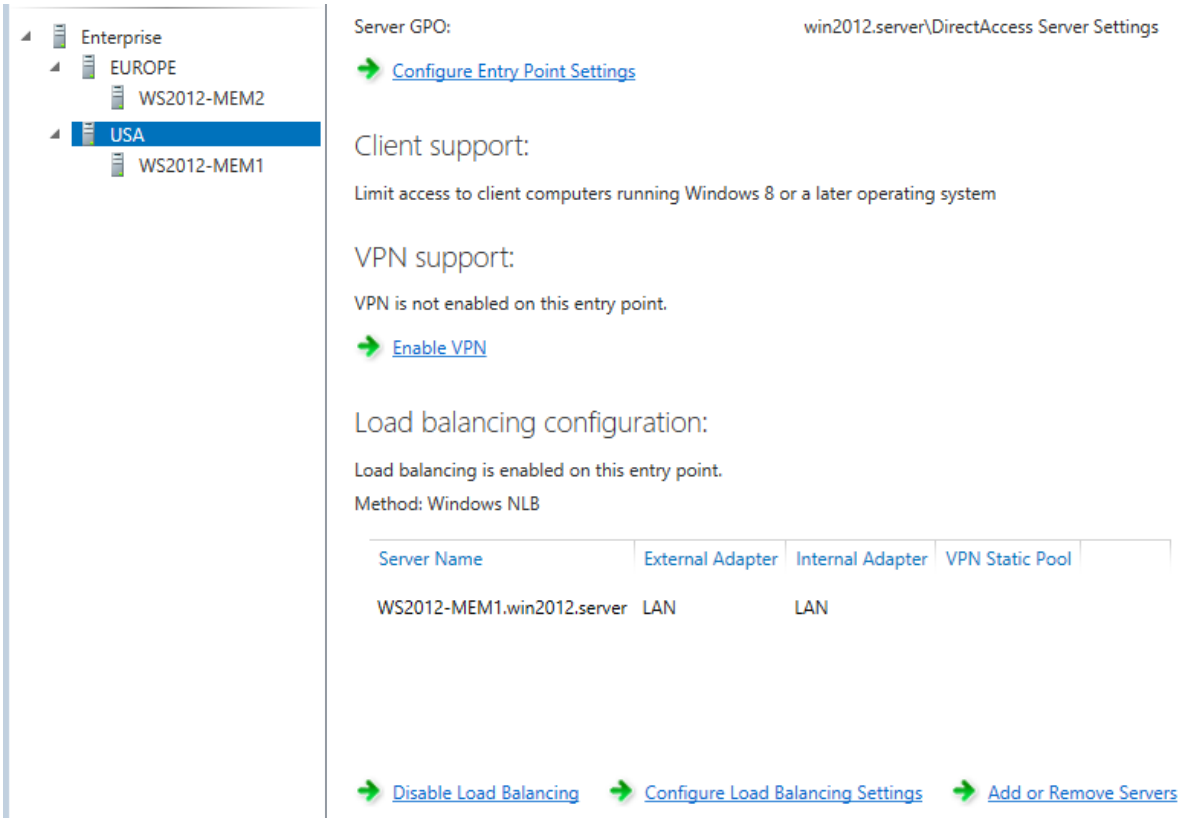
Der NLB Prozess hat die DIP nicht in die VIP auf der NIC geaendert und die neue VIP hinzugefuegt. In den NIC Properties die DIP aendern, NLB Kontrollkaestchen

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

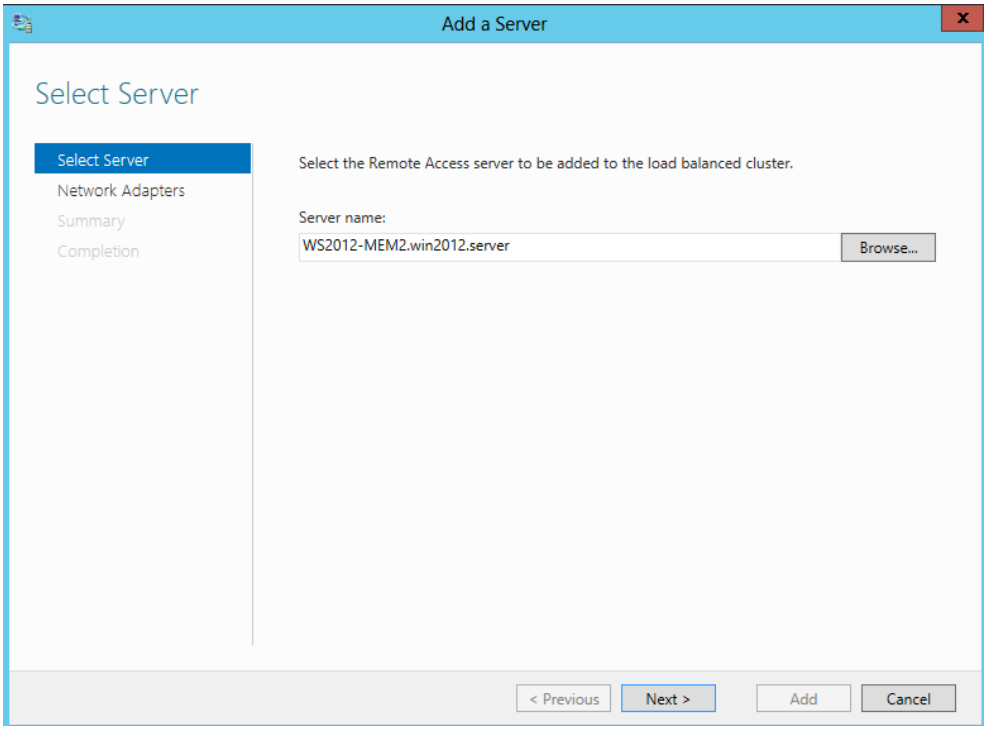
Default State auf Start stellen fuer NLB Knoten



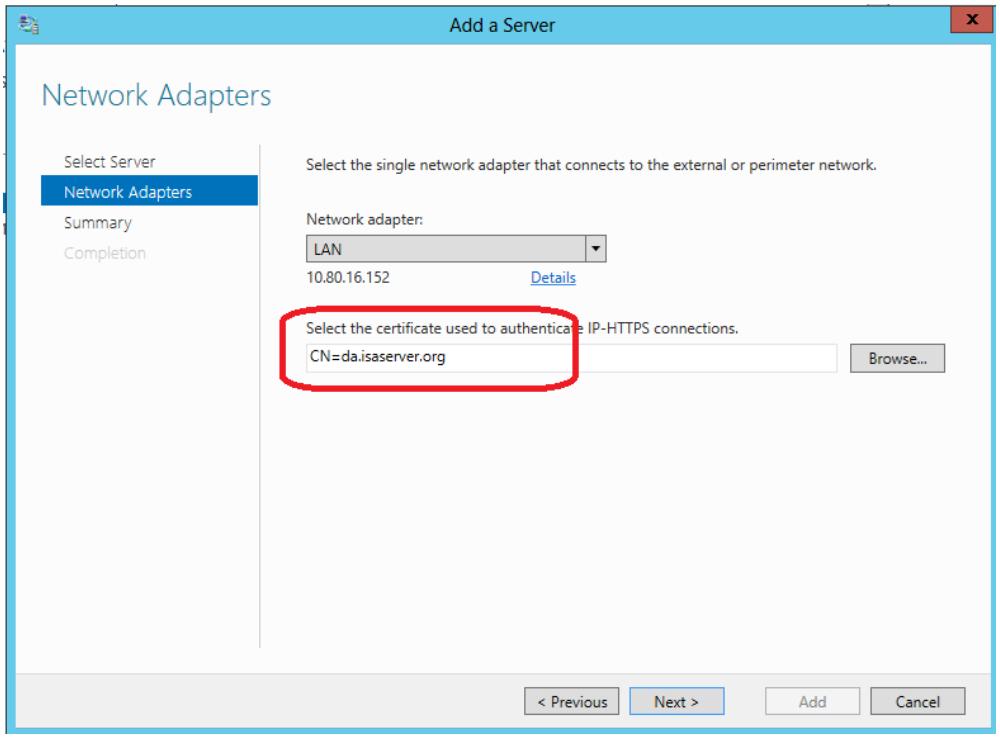
Danach ist alles OK



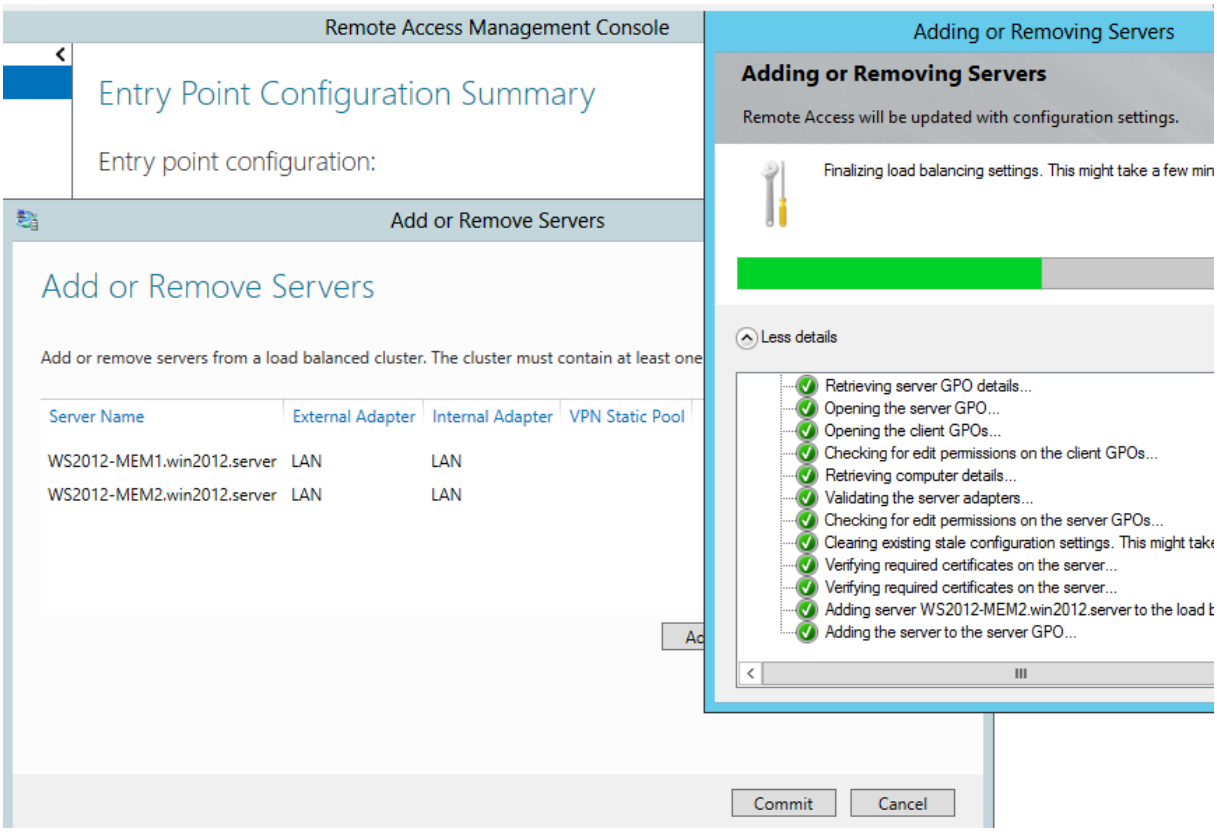
Server hinzufuegen



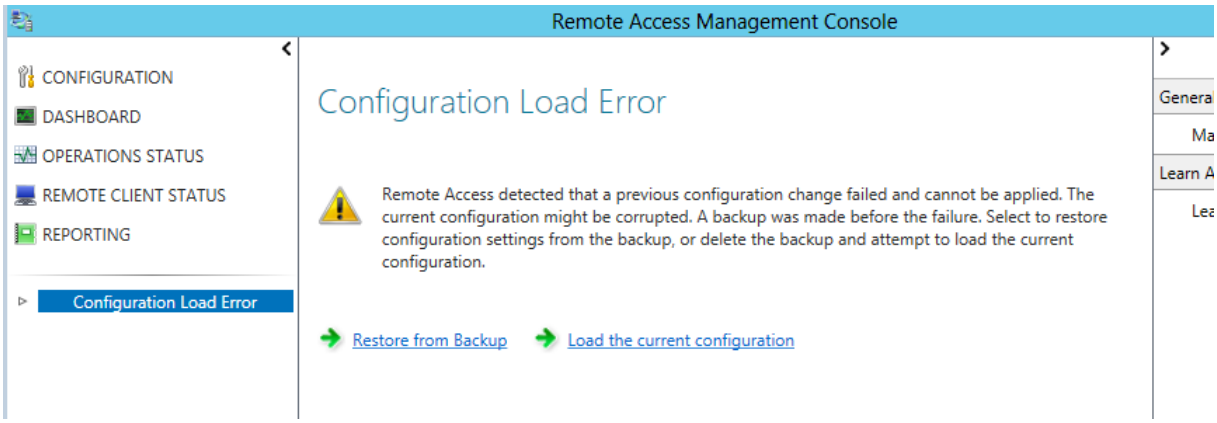
Darauf achten, dass das Zertifkat das richtige ist



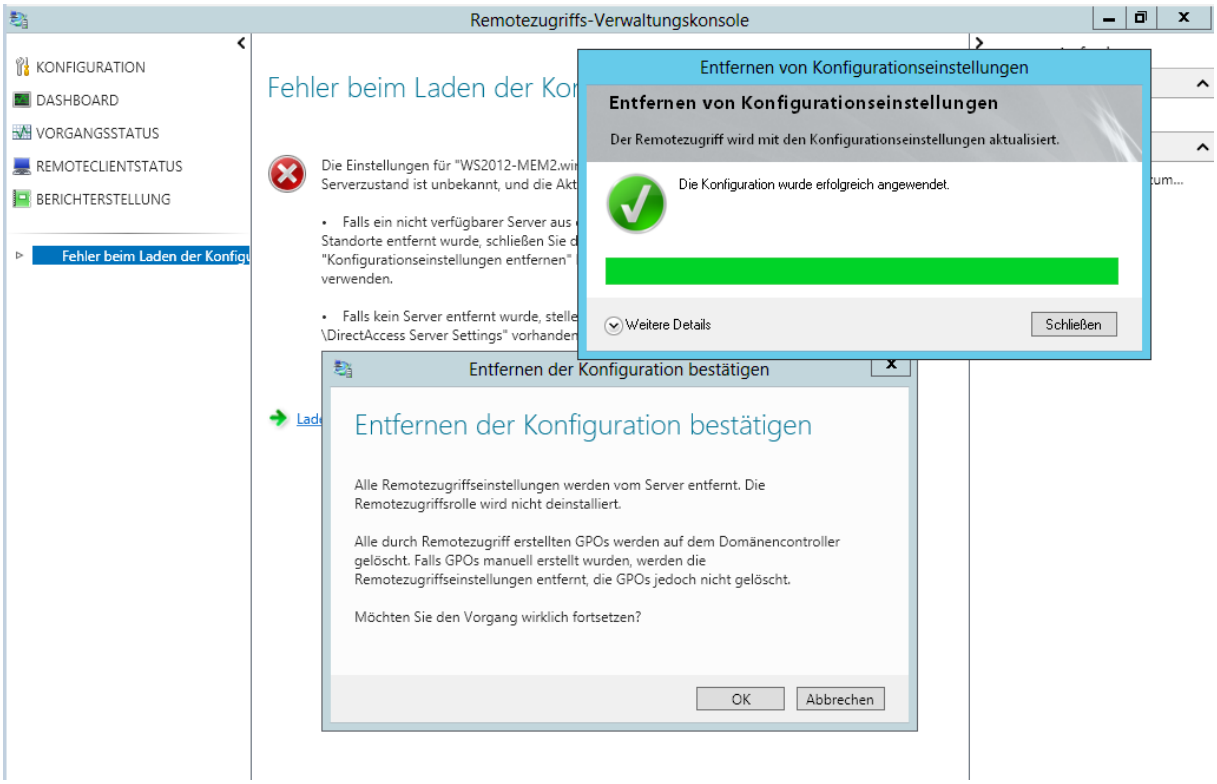
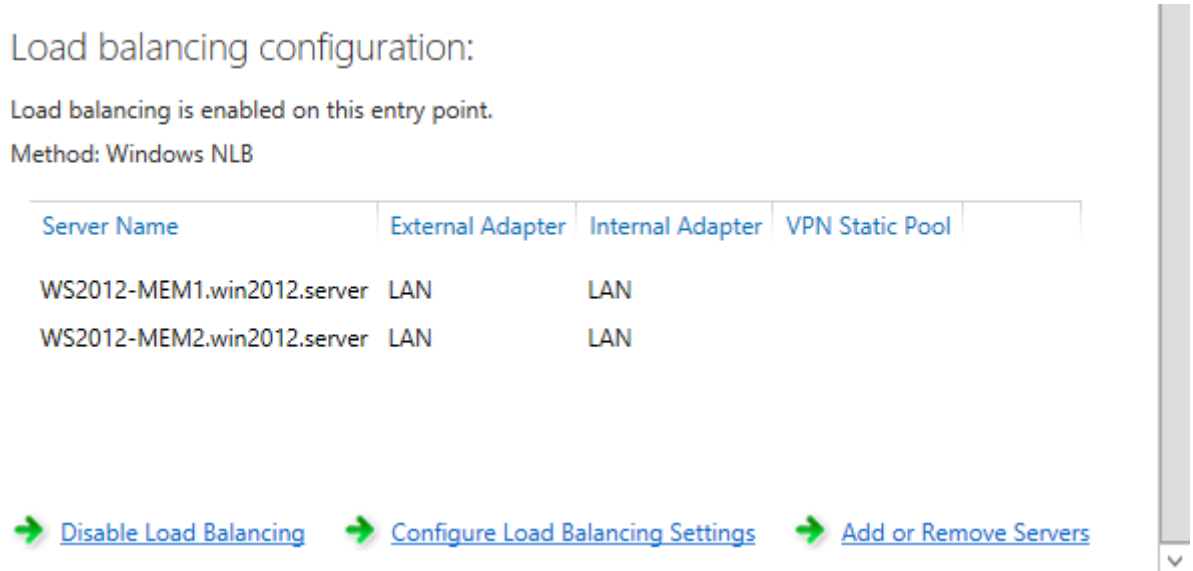
Konfiguration aktivieren



Error



Konfiguration entfernen



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