
How to migrate from Forefront UAG DirectAccess to Windows Server 2012 R2 DirectAccess

Abstract

In this article I will show you how to migrate from DirectAccess in Forefront UAG to DirectAccess in Windows Server 2012 R2.

Let's begin

Microsoft introduced DirectAccess in Windows Server 2008 R2. A DirectAccess deployment in Windows Server 2008 R2 was a complicated process for Administrator and due to the lack of built-in DNS64/NAT64 components, Administrators had to use other devices to provide DNS64 and NAT64 services.
In January 2010 Microsoft introduced Forefront Unified Access Gateway (UAG) as a successor of the Microsoft Intelligent Application Gateway (IAG). Forefront UAG has a powerful integration of DirectAccess based on Windows Server 2008 R2 with several enhancements like NAT64 and DNS64, built-in high availability and better monitoring capabilities. Until Microsoft brought Windows Server 2012 to the market, Forefront UAG was the only solution to provide DirectAccess in midsized and large companies.

In February 2012 Microsoft introduced a whitepaper how to migrate DirectAccess from Forefront UAG to Windows Server 8 (Windows Server 8 was the codename for Windows Server 2012). This was the first statement from Microsoft that shows the decision to make Windows Server 2012 as the strategic platform for DirectAccess.

In December 2013 Microsoft announced on the Server and cloud platform team blog, that Forefront UAG has been discontinued. Many customers now have Forefront UAG DirectAccess deployed and over the next years they must migrate their existing DirectAccess solutions from Forefront UAG to Windows Server 2012 or later DirectAccess.

The DirectAccess implementation in Windows Server 2012 and higher has many improvements over DirectAccess in Forefront UAG. The most important changes and enhancements are listed here:

- Direct Access and RRAS coexistence
- Simplified Direct Access management for small and medium organization administrators
- No requirements for a Public Key Infrastructure (PKI) in some DirectAcces combinations
- Built-in NAT64 and DNS64 support for accessing IPv4-only resources
- Support for Direct Access server behind a NAT device
- Load balancing support

- Improved IP-HTTPS performance (HTTPS null encryption in Windows 8 clients)
- Support for multiple domains
- Support for OTP (token based authentication)
- Automated support for force tunneling
- Multisite support
- Windows PowerShell support
- User and server health monitoring
- Integrated DCA in Windows 8

The DirectAccess configuration wizards in Forefront UAG and Windows Server 2012 R2 are nearly identical. The following picture shows the Forefront UAG DirectAccess console.

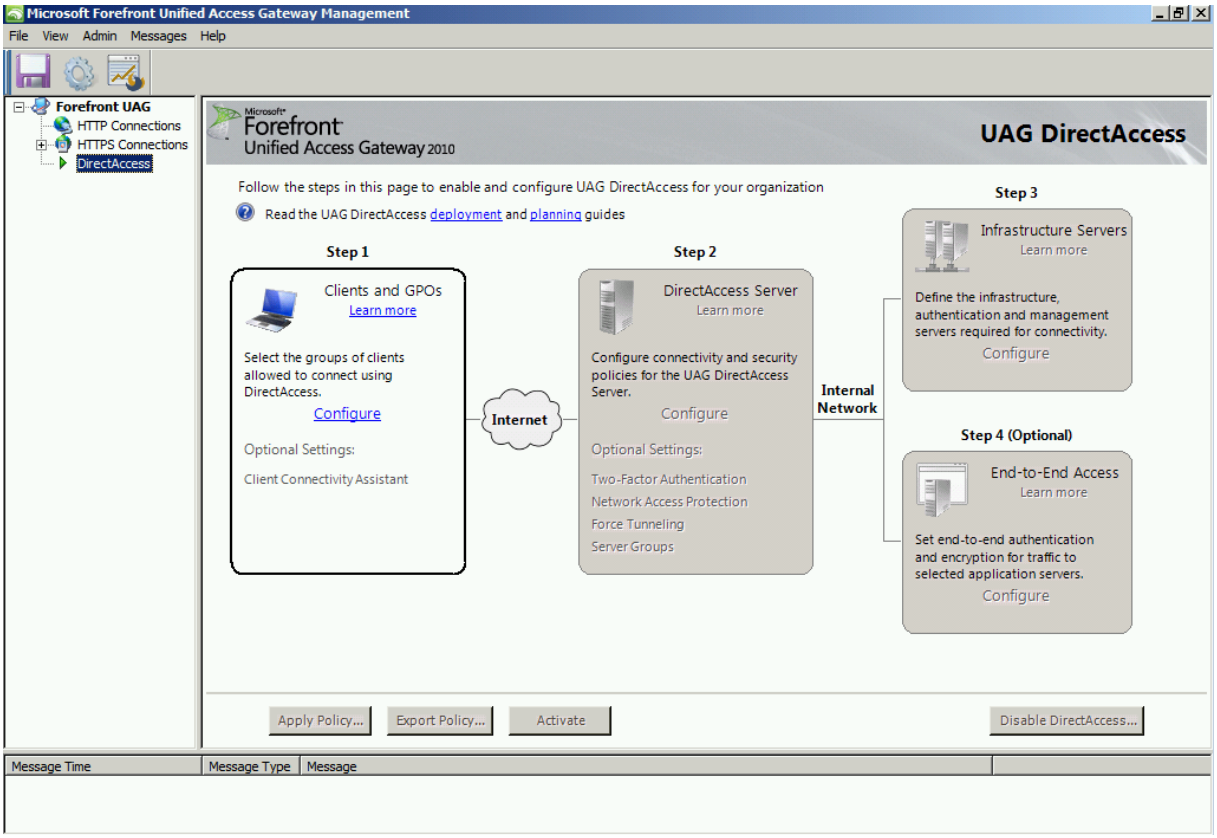

Figure 1: DirectAccess console in Forefront UAG

The following picture shows the Windows Server 2012 R2 DirectAccess console.

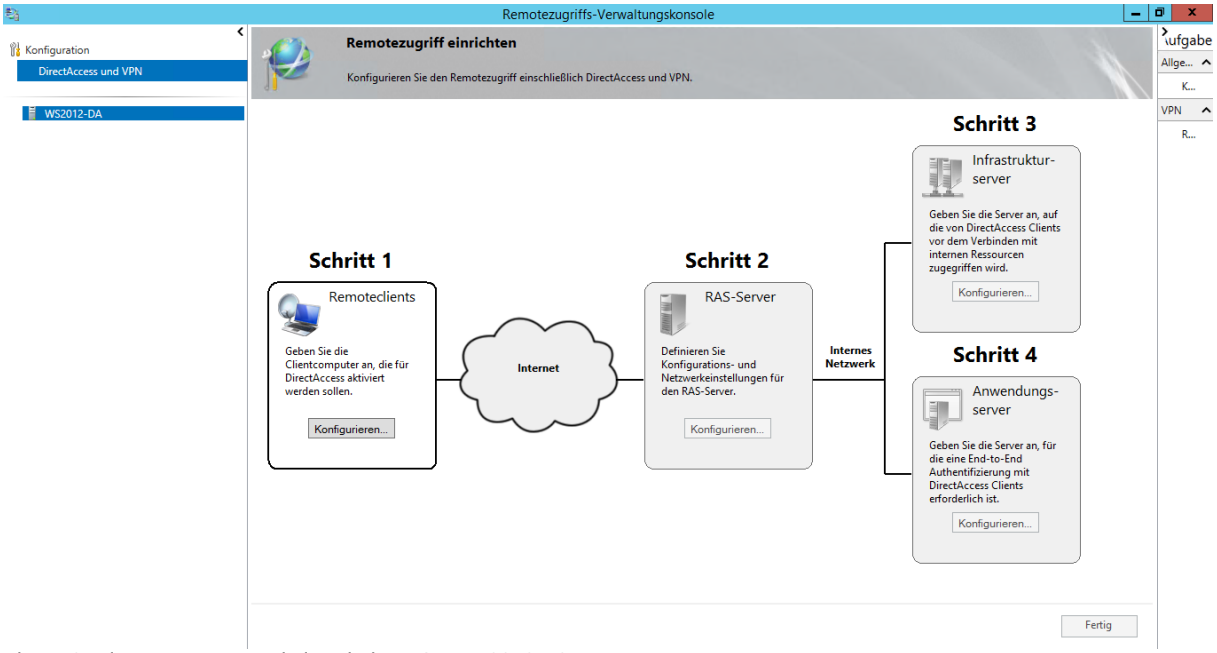

Figure 2: DirectAccess console in Windows Server 2012 R2

Migration steps

There are two methods how to migrate from DirectAccess in Forefront UAG to DirectAccess in Windows Server 2012 R2:

- Side-by-Side Migration of Forefront UAG DirectAccess
- Offline Migration of Forefront UAG DirectAccess

Side-by-Side Migration of Forefront UAG DirectAccess

A side-by-side migration keeps the Forefront UAG DirectAccess server running while you deploy Windows Server 2012 R2 DirectAccess. You will deploy a new DirectAccess Server with Windows Server 2012 R2 and with the help of the Group Policy and the Group Policy Security filtering concepts you can easily migrate DirectAccess clients from Forefront UAG to Windows Server 2012 R2 step-by-step over a short or long migration time window.

There are four steps for DirectAccess migration:

Step 1: Export Forefront UAG DirectAccess configuration settings
Step 2: Note the names of Group Policy Objects (GPOs) used by Forefront UAG DirectAccess (client GPO, Gateway GPO and Application Server GPO)
Step 3: Set up a Windows Server 2012 R2 machine as a Remote Access server, by installing the Remote Access role
Step 4: Configure infrastructure settings for the Remote Access server, including IP addresses, NLS Server, DNS settings, certificates, Active Directory security groups for clients, and Group Policy objects (GPOs).

Important:

If ISATAP has been deployed in the internal network you should disable ISATAP by deleting the DNS A record ISATAP from your internal DNS Server Forward Lookup

Zones and wait for DNS replication on all domain controllers. After that wait additional 24 hours that all ISATAP clients has removed their ISATAP addresses and deactivated their ISATAP interface. Clean up DNS AAAA records. For Managed out functionality of DirectAccess clients from internal clients use Group Policies or the HOSTS files on the clients to specify the Forefront UAG Server as the ISATAP router until the entire migration has been finished.

Configure Windows Server 2012 R2 as an ISATAP router

On the Windows Server 2012 R2 note the ISATAP prefix provided by Forefront UAG:
Get-NetRoute | ?{ $_.DestinationPrefix -match ":8000::/64" } | Select-Object -ExpandProperty DestinationPrefix

Before installing the Remote Access role on the Windows Server 2012 R2 disable the ISATAP interface to prevent the Windows Server 2012 R2 to become a ISATAP client:

Set-NetIsatapConfiguration -State Disabled

Install the Windows Server 2012 R2 Remote Access role and configure DirectAccess. After that change the ISATAP prefix of the Windows Server 2012 R2 DirectAccess server to be the same as the Forefront UAG ISATAP prefix by typing the following command:

Set-DAServer -InternalIPv6Prefix <UAG ISATAP Prefix>

This cmdlet changes the DNS64 address on the Windows Server 2012 R2 DirectAccess server to use the Forefront UAG prefix, but it doesn't update the address on the firewall rule to allow DNS queries to reach DNS64.

To complete this step run the following commands on the Windows Server 2012 R2 DirectAccess server:

```
$dns64Address = (Get-DAClientDnsConfiguration).NrptEntry | ?{
$_.DirectAccessDnsServers -match ':3333::1' } | Select-Object -First 1 -
ExpandProperty DirectAccessDnsServers
$serverGpoName = (Get-RemoteAccess).ServerGpoName
$serverGpoDc = (Get-DAEntryPointDC).DomainControllerName
$gpoSession = Open-NetGPO -PolicyStore $serverGpoName -DomainController
$serverGpoDc
Get-NetFirewallRule -GPOSession $gpoSession | ? {$_.Name -in @('0FDEEC95-
1EA6-4042-8BA6-6EF5336DE91A', '24FD98AA-178E-4B01-9220-
D0DADA9C8503')} | Set-NetFirewallRule -LocalAddress $dns64Address
Save-NetGPO -GPOSession $gpoSession
gpupdate /force
```

On the Windows Server 2012 R2 DirectAccess server run the following commands to obtain the IPv6 prefix of the Forefront UAG server for Teredo clients:

```
$UAGIPv4Address="<UAG's first external IPv4 address>"
[Byte[]] $TeredoServerAddressBytes = `
```

[System.Net.IPAddress]::Parse("2001::").GetAddressBytes()[0..3] + `
[System.Net.IPAddress]::Parse($UAGIPv4Address).GetAddressBytes() + `
[System.Net.IPAddress]::Parse("::").GetAddressBytes()[0..7]
Write-Host "The UAG's Teredo prefix is $([System.Net.IPAddress]$TeredoServerAddressBytes)/64"

On the Forefront UAG server, run the following command to obtain the Teredo interface's index:

Netsh int ipv6 show route

On the Forefront UAG server run the following command to enable Forefront UAG to publish its Teredo client prefix to the ISATAP subnet:

Netsh int ipv6 add route prefix=<teredo prefix> interface=<teredo interface index> publish=yes

Since 6to4 clients will no longer be able to connect via Forefront UAG to backend servers, you should disable 6to4 on all clients using a Group Policy (Computer Configuration/Policies/Administrative Templates/Network/TCP/IP Settings/IPv6 Transition Technologies/6to4 State setting to Disabled State).

Create an ISATAP DNS record for the Windows Server 2012 R2 DirectAccess server to publish the Server as an ISATAP router alongside Forefront UAG and wait 24 hours for DNS replication.

On the Windows Server 2012 R2 DirectAccess server enable DNS AAAA name resolution by running the following command:

Set-NetDnsTransitionConfiguration -OnlySendAQuery $false

When all clients are migrated from Forefront UAG to the Windows Server 2012 DirectAccess server, you can remove the Forefront UAG ISATAP DNS records from the DNS server.

Collect the Forefront UAG DirectAccess configuration settings by exporting the configuration or by taking screenshots of the configuration to be able to compare the settings with DirectAccess configuration steps in Windows Server 2012 R2.

Install and configure the DirectAccess Server in Windows Server 2012 R2. Until the wizard has been finished, the wizard will create Group Policy objects in Active Directory. Make sure that these objects have different names as the Forefront UAG Group Policies. Apply these Group Policies based on Group Policy Security filtering on different Security Groups. With this concept it is easy to migrate DirectAccess clients from Forefront UAG to Windows Server 2012 R2. Change the security group membership of Forefront UAG DirectAccess clients to the security group used by Windows Server 2012 R2 DirectAccess. After the new Group policy has been applied, the DirectAccess client should no use Windows Server 2012 R2 DirectAccess.

Offline Migration of Forefront UAG DirectAccess

For an offline migration of Forefront UAG DirectAccess to Windows Server 2012 R2 DirectAccess you have to shut down the Forefront UAG Server before the Windows Server 2012 R2 Remote Access server is activated. This enables you to use existing IP addresses, certificates and DNS FQDNs.
The offline migration method creates server downtime and should be planned carefully and requires that all clients must be migrated to the new DirectAcess Server at once, and a rollback may be complicated if something goes wrong.

An offline migration consists of the following steps:

Step 1: Install the Remote Access role on the Windows Server 2012 R2 computer
Step 2: Configure server IP addresses
Step 3: Obtain a server certificate for IP-HTTPS connections
Step 4: Prepare group Policy objects for the Remote Access server, DirectAccess clients, and application servers if required
Step 5: Configure DirectAccess

The Offline Migration steps are listed here in details. I don't write the entire procedure of an Offline Migration in this article because the process is not very different from deploying a new DirectAccess Server in Windows Server 2012 R2.
The Offline migration is the easiest way to migrate DirectAccess from Forefront UAG compared to the side-by-side migration but an Offline Migration may work only in small and medium sized companies with a handful of DirectAccess clients. Please note that all DirectAccess clients should be physically reachable by the DirectAccess Administrators because you disable Forefront UAG DirectAccess first before deploying the new DirectAccess Server. Clients must be located in the internal network to get the new Group Policies for DirectAccess.

Conclusion

DirectAccess in Forefront UAG was a great solution to enhance the DirectAccess experience for end-users but it was sometimes hard to configure because of the infrastructure dependencies. DirectAccess in Windows Server 2012 has many improvements which makes DirectAccess deployments much easier. In my opinion the possibility to deploy a Windows Server 2012 R2 DirectAccess Server behind a NAT device with private IP addresses and only one Network card is the greatest improvement. Migration from DirectAccess in Forefront UAG to Windows Server 2012 R2 is an easy step if you plan the migration process carefully.

Related links

Important Changes to the Forefront Product Line
http://blogs.technet.com/b/server-cloud/archive/2013/12/17/important-changes-to-the-forefront-product-line.aspx
Migrate from Forefront UAG SP1 DirectAccess to Windows Server 2012
http://technet.microsoft.com/en-us/library/hh831658.aspx
Side-by-Side Migration of Forefront UAG DirectAccess
http://technet.microsoft.com/en-us/library/hh831623.aspx
Offline Migration of Forefront UAG DirectAccess
http://technet.microsoft.com/en-us/library/hh831481.aspx

Windows Server 2012 Direct Access – Part 1 What's New
http://blogs.technet.com/b/meamcs/archive/2012/05/03/windows-server-2012-direct-access-part-1-what-s-new.aspx