Implementing RPC over HTTPS in a single Exchange Server 2003 environment

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article I will show you how to deploy the RPC over HTTPS feature from Exchange Server 2003 and Outlook 2003 to connect to your Exchange Server with your favourite Outlook Client over HTTPS. This article specially deals with a single Exchange / Domain Controller environment for small organizations.

Let's begin

As I wrote above we will use a single Exchange / Domain Controller setup for this article. The configuration is as follow:

 Exchange Server 2003 Standard with SP1 and Windows Server 2003 Standard SP1 as an Active Directory Domain Controller
 Windows XP Professional Computer with SP2 and Microsoft Office Outlook 2003 with SP2

Step by Step

The following steps are necessary to implement RPC over HTTPS in a single Exchange Server environment:

- Configure an Exchange Server 2003 back-end server as an RPC proxy server
- Configure the RPC virtual directory for Basic authentication and SSL
- Configure the RPC proxy server to use specified ports for RPC over HTTP
- Set the NT Directory Services (NTDS) port on all global catalog servers that act as Exchange Server 2003 back-end servers
- Create a Microsoft Office Outlook 2003 Profile for your users to use with RPC over HTTPS
- Test the Connection

Configure an Exchange Server 2003 back-end server as an RPC proxy server

You must install the RPC over HTTP Proxy component on the Windows Server 2003. The RPC over HTTP Proxy component is responsible for the encapsulation of RPC pakets over HTTP(S) and is a component of Windows Server 2003 so you can install this feature like any other Windows feature with the help of the Add/Remove components wizard.

Networking Services	X
To add or remove a component, click the check box. A shaded box me of the component will be installed. To see what's included in a compone	ans that only part ent, click Details.
Sub <u>c</u> omponents of Networking Services:	
🗹 📇 Domain Name System (DNS)	1.7 MB 🔺
🗆 📇 Dynamic Host Configuration Protocol (DHCP)	0.0 MB
🗹 🚑 Internet Authentication Service	0.0 MB
🗆 👵 Remote Access Quarantine Service	0.1 MB
🗹 💂 RPC over HTTP Proxy	0.0 MB
Element Simple TCP/IP Services	0.0 MB
🔲 🚐 Windows Internet Name Service (WINS)	0.9 MB 💌
Description: Enables RPC/DCOM to travel over HTTP via the Interne Server (IIS).	et Information
Total disk space required: 6.9 MB	Details
Space available on disk: 865.9 MB	<u>10</u> ,033110
ΟΚ	Cancel

Figure 1: Installing the RPC over HTTP Proxy

Configure the RPC virtual directory for Basic authentication and SSL

The next step is to configure the newly created RPC virtual directory in IIS to use Basic Authentication and SSL.

Basic Authentication is required to work with RPC over HTTPS and if you use Basic Authentication you must use SSL because Basic Authentication sends the user credentials in cleartext.

Start the Internet Information Service Manager, navigate to the *Default Website* and rightclick the *RPC* Virtual Directory. Navigate to the *Directory Security* tab and disable the Checkbox for *Enable Anonymous Access* and enable the *Basic Autehntication* checkbox. You could leave the *Integrated Windows Authentication* checkbox unchanged.

Imable anonymous access User name: IUSR_LONDON Password: Image: IUSR_LONDON Password: Image: Imag	thentication N	Methods	
Base the following Windows user account for anonymous access: User name: IUSR_LONDON Browse Password: Image:	nable <u>a</u> no	nymous access	
User name: IUSR_LONDON Browse, Password: ••••••••• Authenticated access •••••••• For the following authentication methods, user name and password are required when: • anonymous access is disabled, or • access is restricted using NTFS access control lists Integrated Windows authentication Digest authentication for Windows domain servers Tagic authentication (password is sent in clear text)	Use the followi	ng Windows user account for anonymous access:	
Password: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	User name:	IUSR_LONDON Browse,,	
Authenticated access For the following authentication methods, user name and password are required when: anonymous access is disabled, or access is restricted using NTFS access control lists ✓ Integrated Windows authentication ✓ Digest authentication for Windows domain servers ✓ access is not control is the time of time of the time of time of the time of t	Password:		
Authenticated access For the following authentication methods, user name and password are required when: - anonymous access is disabled, or - access is restricted using NTFS access control lists Integrated Windows authentication Digest authentication for Windows domain servers asjc authentication (password is sent in clear text)			
Authenticated access For the following authentication methods, user name and password are required when: - anonymous access is disabled, or - access is restricted using NTFS access control lists Integrated Windows authentication Digest authentication for Windows domain servers asjc authentication (password is sent in clear text)			
 Authenticated access For the following authentication methods, user name and password are required when: anonymous access is disabled, or access is restricted using NTFS access control lists ✓ Integrated Windows authentication Digest authentication for Windows domain servers ✓ Pasic authentication (password is sent in clear text) 			
For the following authentication methods, user name and password are required when: - anonymous access is disabled, or - access is restricted using NTFS access control lists ✓ Integrated Windows authentication Digest authentication for Windows domain servers Asjc authentication (password is sent in clear text)			
 anonymous access is disabled, or anonymous access is disabled, or access is restricted using NTFS access control lists Integrated Windows authentication Digest authentication for Windows domain servers asic authentication (password is sent in clear text) 	Authenticated	access	
- access is restricted using NTFS access control lists Integrated Windows authentication Digest authentication for Windows domain servers asic authentication (password is sent in clear text)	Authenticated	access ng authentication methods, user name and passwo	ord
 Integrated Windows authentication Digest authentication for Windows domain servers asic authentication (password is sent in clear text) 	-Authenticated For the followin are required wi - apon	access ng authentication methods, user name and passwo hen: ymous access is disabled, or	ord
Digest authentication for Windows domain servers asic authentication (password is sent in clear text)	Authenticated For the followin are required wi - anon - acces	access ng authentication methods, user name and passwo hen: ymous access is disabled, or ss is restricted using NTFS access control lists	ord
Pagest authentication (password is sent in clear text)	Authenticated For the followin are required wi - anon - acces	access ng authentication methods, user name and passwo hen: ymous access is disabled, or ss is restricted using NTFS access control lists Windows authentication	ord
	Authenticated For the following are required with anon - acces	access ng authentication methods, user name and passwo hen: ymous access is disabled, or ss is restricted using NTFS access control lists Wi <u>n</u> dows authentication pentication for Windows domain servers	ord
	Authenticated - For the followir are required wi - anon - acces Integrated Digest auth	access ng authentication methods, user name and passwo hen: ymous access is disabled, or ss is restricted using NTFS access control lists Windows authentication mentication for Windows domain servers whication for Windows domain servers	ord

Figure 2: Configuration of the RPC Virtual Directory

If you enable the *Basic Authentication* checkbox you will get the following warning:

IIS Man	ager X
1	The authentication option you have selected results in passwords being transmitted over the network without data encryption. Someone attempting to compromise your system security could use a protocol analyzer to examine user passwords during the authentication process. For more detail on user authentication, consult the online help. This warning does not apply to HTTPS(or SSL) connections. Are you sure you want to continue?
	Yes <u>No</u> <u>H</u> elp

Figure 3: Basic Authentication warning

If you use SSL for the Virtual Directory you can safely ignore the Warning of the IIS Manager.

Next you must enable SSL for the RPC Virtual Directory. For this article I assume that you already have an SSL certificate implemented. Enable the checkbox *Require 128-bit encryption* for additional security.

Secure Communications	×
Require secure channel (SSL)	
Require <u>1</u> 28-bit encryption	
Client certificates	
Ignore client certificates	
C Accept client certificates	
C Require client certificates	
Enable client certificate mapping Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.	<u>fit</u>
OK Cancel	Help

Figure 4: Enable SSL for the RPC Virtual Directory

Configure the RPC proxy server to use specified ports for RPC over HTTP

Now we need to configure the RPC Proxy Server on Exchange Server 2003 to use a specific Port Range. The Registry Key already exists but you must modify the Data. The path to the Registry is:

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\RPC\RPCPROXY.

Change the data as you can see in the following picture. You must use the Port Range 6001-6002 for the NetBIOS and DNS FQDN and the Port 6004 also for the NetBIOS and DNS FQDN.



Figure 5: Configuring the RPC Proxy Directory

Set the NT Directory Services (NTDS) port on all Global Catalog Servers that act as Exchange Server 2003 back-end Servers

Again we must modify the Registry to specify a static port for the NSPI (Name Service Provider Interface) Interface settings.

Start Regedit and navigate to:

HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\NTDS\P ARAMETERS.

Create a *REG_MULTI_SZ* Record named *NSPI interface protocol sequence* with the data NCACN_HTTP:6004 as you can see in the following picture.

🙀 Registry Editor			
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>H</u> elp			
🗈 💼 msvsmon80 🛛 🔺	Name	Туре	Data
🕀 💼 Mup	(Default)	REG_SZ	(value not set)
	Configuration NC	REG_SZ	CN=Configuration,DC=nwtraders,DC=msft
	Database backup path	REG_SZ	C:\WINDOWS\NTDS\dsadata.bak
	Database log files path	REG_SZ	C:\WINDOWS\NTDS
	Database logging/recovery	REG_SZ	ON
H- NDProxy	DS Drive Mappings	REG_MULTI_SZ	c:\=\\?\Volume{72a04ad2-a752-11d7-9dcc-806e6f6e6963}\
	DSA Database file	REG_SZ	C:\WINDOWS\NTDS\ntds.dit
	DSA Working Directory	REG_SZ	C:\WINDOWS\NTDS
	Bolobal Catalog Promotion Complete	REG_DWORD	0x00000001 (1)
	Hierarchy Table Recalculation int	REG_DWORD	0x000002d0 (720)
	Real Idapserverintegrity	REG_DWORD	0x00000001 (1)
	Machine DN Name	REG_SZ	CN=NTDS Settings, CN=LONDON, CN=Servers, CN=Default-First-Site-Na
🗄 💼 Nla	Berformance Counter Version	REG_DWORD	0x00000011 (17)
🗄 💼 nm	and Root Domain	REG_SZ	DC=nwtraders,DC=msft
⊡ NntpSvc	🔀 Schema Delete Allowed	REG_DWORD	0x00000000 (0)
🕀 💼 Npfs	👸 Schema Update Allowed	REG_DWORD	0x00000000 (0)
🖻 🧰 NTDS	👸 Schema Version	REG_DWORD	0x0000001e (30)
Diagnostics	BStrict Replication Consistency	REG_DWORD	0×00000001 (1)
Parameters	👸 System Schema Version	REG_DWORD	0x0000001e (30)
Performance	NSPI interface protocol sequences	REG_MULTI_SZ	ncacn_http:6004
RID Values			
H- NtmsSyc			
🗄 🧰 ose			
🕀 💼 Outlook			
🕀 🧰 Parport			
🕀 💼 PartMgr			
🗄 💼 Parvdm			
E PCI			
PCIIde			
Figure 6. Configuring the NTDS -	-NSPI Protocol seau	Jence	
	1		
Vou must restart the Same	dftor opplying th	Degistry	
Fou must restant the Selvel	ratter applying th	ie Registry	Ney.

Create a Microsoft Office Outlook 2003 Profile for your users to use with RPC over HTTPS

As a next step we must configure the Microsoft Outlook 2003 Profile to use RPC over HTTPS.

Navigate to the *Control Panel* at your Windows XP Professional Workstation and click the *Mail* icon. Add a new Mail profile or modify an existing Profile. Navigate to the Connection Tab and enable the Checkbox *Connect to my Exchange mailbox using HTTP* and then click the *Exchange Proxy Settings* Button.

۲	icrosoft Exchange Server	×
	General Advanced Security Connection Remote Mail	
	Connection	
	Use these settings when connecting to my Exchange server when working offline:	
	Connect using my Local Area Network (LAN)	
	Connect using my phone line	
	$igodoldsymbol{ imes}$ Connect using Internet Explorer's or a 3rd party dialer	
	Modem	
	Use the following Dial-Up Networking connection:	
	V	
	Properties Add	
	Exchange over the Internet	
	Connect to my Exchange mailbox using HTTP	
	Exchange Proxy Settings	
	OK Cancel Apply	

Figure 7: Enable RPC Proxy Settings

Enter the following information (with your Server Information) you can see in the following picture.

Exchange Proxy Settings
Microsoft Office Outlook can communicate with Microsoft Exchange Server over the Internet by nesting Remote Procedure Calls (RPC) within HTTP packets. Select the protocol and the identity verification method that you want to use. If you don't know which options to select, contact your Exchange Server Administrator.
Connection settings
Use this URL to connect to my proxy server for Exchange:
https:// london.nwtraders.msft
Connect using SSL only
Mutually authenticate the session when connecting with SSL
Principal name for proxy server:
msstd:london.nwtraders.msft
The fact petworks, connect using HTTP first, then connect using TCP/IP
On slow petworks, connect using HTTP first, then connect using TCP/IP
Proxy authentication settings
Use this authentication when connecting to my proxy server for Exchange:
Basic Authentication
OK Cancel

Figure 8: Exchange Proxy Settings **Test the Connection**

After enabling the RPC Proxy settings your Outlook connection to the Exchange Server should be established successfully. The question is now: How to determine that it is a RPC over HTTPS connection?

The answer is simple. Right click the Outlook icon in the taskbar while you are holding the CTRL Key. The Context menu opens and now you have the option to see the Exchange Server Connection Status.

_	[-		V	1	1
London.nwtraders.msft	Directory	Intel 2114. HTTPS	Established	1/0	1051
London.nwtraders.msft	Directory	Intel 2114. HTTPS	Established	1/0	110
London.nwtraders.msft London.nwtraders.msft	Mail Mail	Intel 2114. HTTPS	Established	2/0 30/0	926 109
London.nwtraders.mst	Mail	Intel 2114 HTTPS	Established	3/0	57
· ·		oft Evolution Servers			
Reconnect Click to restore conn	ectivity to your Microso	JI C EXchange Der Versi			

Figure 9: Test the RPC over HTTPS connection

Congratulations! You have successfully enabled your Exchange Server 2003 / Microsoft Outlook 2003 environment to use the RPC over HTTPS feature.

Conclusion

Implementing Exchange Server 2003 with RPC over HTTPS in a single Exchange / Domain Controller environment is really simple if you follow the instructions from this article or the RPC over HTTP Deployment Scenarios Guide for Exchange Server 2003. With this feature enabled, all your external users can use Outlook over the Internet as they were locally connected to your LAN. If you have an ISA Server 2004 at your Firewall you can benefit from the advanced Features of ISA Server 2004 to publish the Exchange Server over RPC/HTTPS.

Related Links

RPC over HTTP Deployment Scenarios Guide for Exchange Server 2003 http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/ex2k3rpc.mspx Configuring the Outlook 2003 RPC over HTTP Client http://www.msexchange.org/tutorials/outlookrpchttp.html Troubleshooting RPC over HTTPS (Part 1) http://www.msexchange.org/tutorials/Troubleshooting-RPC-over-HTTPS-Part1.html