Windows Server 2012 Walkthroughs

CCDC Regionals 2023

Jacob Motley

Contents

INSTALL TFTP ON WIN SERV 2012

http://woshub.com/how-to-install-tftp-server-on-windows-server-2012-r2/

DO NOT USE THE ABOVE LINK!!!

it was my starting point. I've left a simplified walkthrough below, so that you do not have to suffer as I have.

If you are lost though, feel free to take a look at the walkthrough. it includes screenshots that might be helpful ~Jacob~

In Server Manager, install the "Windows Deployment Services" role in the "Add Roles and Features Wizard". Then, in "Role Services" only select "Transport Server." Click next and install.

Open file manager and create a folder here > C:\tftp

open Registry Editor (powershell: "regedit") and navigate to HKLM\SYSTEM\CurrentControlSet\services\WDSServer\Providers\WDSTFTP

Create a new string paramater with the name "RootFolder" and set the value to the folder you created earlier (C:\tftp)

Edit the security of this file to include only the tftp user

Start WDS with this command: WDSUTIL /Start-TransportServer

Now return to the "Add Roles and Features Wizard" in Server Manager. Install the "TFTP Client" feature, and the "Deployment Server" role you deselected earlier from the WDS Section.

In Server Manager, in the left column select "WDS", right click the server, and click "Windows Deployment Services Management Console"

Expand Servers and right click the server. Click Configure Server

Click Next, Next, and on the "Folder Location" screen, change the path from "C:\RemoteInstall" to "C:\tftp" Click "yes" on the pop up and hit next. Do not integrate with AD, make it a standalone server.

Click next and ensure the "add images to the server now" box is checked. Click Finish, then cancel.

Create a file in the C:\tftp\boot folder called test.txt. This will be the file you test the tftp server with.

Remove the "Deployment Server" role you installed earlier through the "remove roles and features wizard" in server manager.

Restart the server.

Run the following command to test the tftp server: tftp -i localhost get boot\test.txt

You should see that the file has successfully downloaded.

On the client, enable the tftp client role (possibly turn off firewall for a minute)

L2TP IPsec with preshared key VPN setup 2012

LINKS USED:

Fixing the client and server registry editor:

https://www.minitool.com/news/vpn-error-789.html

Overall Walkthrough:

https://www.snel.com/support/how-to-set-up-an-l2tp-ipsec-vpn-on-windows-server-2019/#:~:text=Navigate%20to%20the%20security%20tab%20and%20click%20on,who%20wants%20to%20connect%20to%20the%20VPN%20server.

Personalized walkthrough:

Run the following commands in powershell as admin:

```
Install-WindowsFeature RemoteAccess

Install-WindowsFeature DirectAccess-VPN -IncludeManagementTools

Install-WindowsFeature Routing -IncludeManagementTools
```

Server Manager > Tools > Remote Access Management

Run the Remote Access Setup Wizard

Deploy VPN Only

Right click the server and click "Configure and Enable Routing and Remote Access"

Click next and then select "Custom Configuration"

Select only VPN Access

Finish and then start service

Right click the server and click "Properties"

Under the security tab select the box that allows L2TP/IKEv2 connections.

Enter a secure password for the VPN and save it. This will be used by clients to connect to the VPN. Click OK

Under the IPv4 tab select "static address pool" and click "add"

Make the start and end address within your subnet. Don't allow an IP that is currently being used.

START IP ADDRESS: 172.20.242.100

END IP ADDRESS: 172.20.242.150

Click apply and close that window.

Right click the server, All Tasks > Restart

Open your firewall rules and add a new inbound rule. Predefined, "Routing and Remote Access." Click next

Check the "L2TP-In" box and click next. Allow the connection and finish.

In Active directory Users and Computers, add a VPN user. Create a secure password for this account. This account will be used to log in to the VPN. The password should be unique.

Make sure to not require the user to change their password on next login.

Right click the user and select "Properties"

Under the "Dial In" tab, allow access under the Network Access Permission section. Click OK.

Open services.msc

Stop and Start the "IKE and AuthIP IPsec Keying Modules" service.

The next steps must be completed on both the server as well as the client that will the VPN.

Open regedit

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent

Right click, new > DWORD (32-bit) Value

Name the value "AssumeUDPEncapsulationContextOnSendRule"

Set the value to 1 (Hexadecimal)

~Set the value to 2 (Hexadecimal) for the server~

Restart the machine for the effects to take place.

Test the VPN

https://www.snel.com/support/learn-how-to-connect-l2tp-ipsec-vpn-on-windows-10/

Ensure at the firewall level we are allowing UDP Ports 500 and 4500 from outside in.

Install Sysmon and configuration

Config:

https://raw.githubusercontent.com/olafhartong/sysmon-modular/master/sysmonconfig.xml

Sysmon:

http://live.sysinternals.com/Sysmon64.exe

in the downloads folder, run the following command:

```
.\Sysmon64.exe -i sysmonconfig.xml
```

HOW TO CONFIGURE SPLUNK FORWARDER FOR THESE (first configure splunk normally)...

https://medium.com/@smurf3r5/splunking-with-sysmon-c321fe87c567

Go here: C:\Program Files\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local\inputs.conf

Add this and save:

```
[WinEventLog://Microsoft-Windows-Sysmon/Operational]

checkpointInterval = 5

current_only = 0

disabled = 0

start_from = oldest
```

Download splunk forwarder and install instructions

```
wget -O splunkforwarder-7.3.8-bdc98854fc40-x64-release.msi 'https://download.splunk.com/products/universalforwarder/releases/7.3.8/windows/splunkforwarder-7.3.8-bdc98854fc40-x64-release.msi'
```

^^This does not work anymore, is used only as reference now. Use below method first.

DON'T TYPE THIS IN CMD OR POWERSHELL

Just paste this URL in chrome :)

https://download.splunk.com/products/universalforwarder/releases/9.0.2/windows/splunkforwarder-9.0.2-17e00c557dc1-x64-release.msi

INSTALLATION INSTRUCTIONS:

Open the downloaded file.

Check the box to accept the license agreement, and make sure "An on-premises Splunk Enterprise instance" is selected. Click Customize Options.

On the "Install UniversalForwarder to:" screen, click next, next.

On the "Install UniversalForwarder as:" screen, ensure "Local System" is selected, then click next.

Select every log type. Ensure every box under "Windows Event Logs" and "Active Directory Monitoring" is checked. Do not check the boxes under "Performance". Those are not important. Then click next.

For the Username of the Administrator Account, make it "admin" and do not generate a random password. Make the password something you will remember. Click next.

Do not configure anything on the Deployment Server. Click Next.

On the "Receiving Indexer" screen, the IP should be the internal IP Address of the splunk machine. Make the port 9997. Click Next.

Click Install to install the forwarder, and wait for it to install.

Click Finish.

Finally, confirm with splunk people to ensure events are being forwarded to splunk. If it isn't working within 10 minutes, uninstall the program (stop the service if necessary) and re-install following the same steps.

IF USING CENTRAL LOGGER TO RECEIVE LOGS, AND THEN FORWARD TO SPLUNK...

Configure as above, except do not check any of the boxes on the Log types to send. Only browse to the file of the centralized logging program and forward it to splunk.

Un-Black Hole GitHub

set primary dns to 8.8.8.8

set secondary dns to 1.1.1.1

in ipv6 settings remove ::1 as the primary dns

check github.com

SETTING UP FTP SERVER WINDOWS

Add a windows server behind ESXI

Name the server something easy to re-type.

Powershell > sconfig

Option 2, rename then restart server.

Add the IIS Server role, as well as FTP Server and FTP Service roles.

While it installs, add a user and group for the FTP service.

Group: FTP Users

User: FTP

Add a secure password

After it installs, open IIS manager and open your server.

Open Server Sertificates, and create a Self-Signed Certificate.

Name it FTP Cert

Open FTP Firewall Support

Add a data channel port range

Ex: 60000-60100

Add an External IP Address, make sure it is not one that is being used and Apply

Make sure a firewall rule is in place that re-routes traffic going to that External IP Address back to the machine you are using.

Open Windows Firewall with advanced settings and add an inbound firewall rule that allows TCP traffic through ports 21 and the data channel port range you set.

Restart the FTP Service

Services > Microsoft FTP Service

Back in IIS Manager, in the left column select Sites and, in the right, “Add FTP Site…”

Name the site

“FTP Site” will do fine

Add the content path for the FTP Site

C:\inetpub\ftproot

Set SSL to “Allow SSL” and select the SSL Certificate you created earlier. Hit Next

Set Basic Authentication, and Allow Access to Specified roles or user groups

Make the group the FTP User group you made earlier, and give them read and write permissions.

Hit Finish, and then attempt to connect to the server from OUTSIDE the firewall.