Implementing DirectAccess by Using the Getting Started Wizard/ Deploying an Advanced DirectAccess Solution

Eli Chang

MSSA Cohort #2

Lab Summary 7

2/18/2020

Implementing DirectAccess by Using the Getting Started Wizard/ Deploying an Advanced DirectAccess Solution

As many users at the company work outside of the organization, security administrators concern about security from the external connections. The team wants to reduce the number of support calls and have more options to manage remote computers. Thus, the team determined to deploy DirectAccess as a solution for the concern. The DirectAccess server acts as an IPsec tunnel mode endpoint. Eventually, the DirectAccess will be enabled for all mobile clients after the proof of concept deployment.

Configuring DirectAccess on the DirectAccess server

When configuring DirectAccess, there are different types of components that the organization should support: DA server and clients, network location serer, internal resources, AD domain, Group policy, PKI, DNS, and NAP enforcement server. However, the NAP server is not necessary for Windows Server 2016 because of the removal. During deploying the DA server role, the domain member, network adapters, and topology are essential to be selected. In the lab, the administrators decided to use the Edge option, which requires two network adapters. One network adapter connects to the internal network; the other adapter does to the Internet so that the firewalls can be located between the DA and internal network or the DA and the Internet.

Configuring AD DS, DNS, and CRL distribution

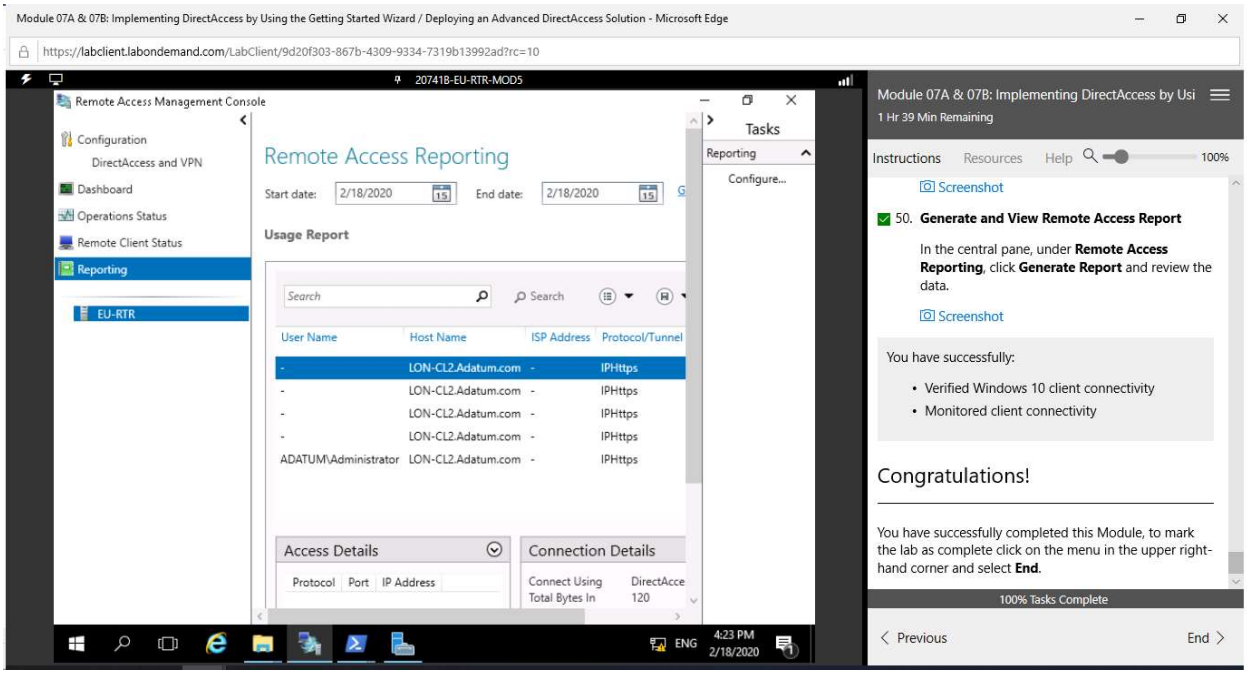
Following the steps, NLS and CRL records should be created in the DNS manager. The clients will use the NLS record to locate the network location, whereas the CRL record is for the internal clients to check the revocation status. The NLS is essential because if the users from outside try to connect and cannot connect to the NLS, then it is from outside. If they can connect to the NLS, then it is from inside.

The NLS requirement

The NLS is essential in the DirectAccess deployment because if the clients from the intranet cannot find the location, they cannot access intranet resources. Also, it should be implemented on the NLB cluster because of its highly availability. It should have an HTTPS server certificate, so the DA clients must have the CA, issued by the HTTPS certificate. The DA clients on the internal network should be able to resolve the name of NLS from the DNS server. Lastly, NLS should not be able to access DA clients on the Internet.

DirectAccess Tunneling Protocol Options

There are four options for DA tunneling protocol: ISATAP, 6to4, Teredo, and IP-HTTPS. ISATAP option is to enable DA clients to connect to the server over the IPv4 networks. The ISATAP queries should be configured in the DNS servers to use ISATAP. Another option is 6to4, which is to connect to the DA server over the IPv4-based Internet with IPv6 packets encapsulated in the IPv4 header. Teredo is used when the clients are located behind an IPv4 NAT device in UDP port 3544. The last option is IP-HTTPS (This is the option used in the lab). Usually, other options are not available; this option comes to save the clients. In the lab, other options set to disabled but can be configured as enabled in real life.


Module 07A & 07B: Implementing DirectAccess by Using the Getting Started Wizard / Deploying an Advanced DirectAccess Solution - Microsoft Edge
https://labclient.labondemand.com/LabClient/9d20f303-867b-4309-9334-7319b13992ad?rc=10
20741B-EU-RTR-MOD5
Remote Access Management Console
Configuration
DirectAccess and VPN
Dashboard
Operations Status
Remote Client Status
Reporting
EU-RTR
Remote Access Reporting
Start date: 2/18/2020
End date: 2/18/2020
Usage Report
Search
User Name
Host Name
ISP Address
Protocol/Tunnel
LON-CL2.Adatum.com
IPHttps
ADATUM\Administrator
Access Details
Protocol
Port
IP Address
Connection Details
Connect Using
Total Bytes In
Tasks
Reporting
Configure...
ENG
4:23 PM
2/18/2020
Module 07A & 07B: Implementing DirectAccess by Usi
1 Hr 39 Min Remaining
Instructions
Resources
Help
100%
Screenshot
50. Generate and View Remote Access Report
In the central pane, under Remote Access Reporting, click Generate Report and review the data.
Screenshot
You have successfully:
Verified Windows 10 client connectivity
Monitored client connectivity
Congratulations!
You have successfully completed this Module, to mark the lab as complete click on the menu in the upper right-hand corner and select End.
100% Tasks Complete
Previous
End