Standard Operating Procedure

lyit | Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Title	Windows Server DNSSEC Deployment
Document Number:	SOP2020-1
By:	Chinthuja Madhavan
Approved:	Ruth Lennon
Status:	Released

Revision History and Document Management

Initial Draft	02MAY20	
Release:		
Revision:		

Summary of the Policy/Purpose of this SOP

This SOP describes the configuration of DNS with DNSSEC in Test lab using AD Integrated DNS Zone.

The Guest OS on these VMs will be Windows 2016 Standard.

It describes the following tasks:

1. Creation of the zone
2. Enable DNSSEC in the zone
3. Validation of DNS request using Group policy Management
4. Linking GPO and Domain

Scope of this SOP

This SOP is intended to inform a technician of Windows Server DNSSEC Deployment.

Actors

Responsible:	
Accountable:	
Consulted:	
Informed:	

Contents

Revision History and Document Management 1
Summary of the Policy/Purpose of this SOP 1
Scope of this SOP 1
Actors 1
Resources and Prerequisites 3
Inputs - Guest OS Specification 3
Actions 4
Zone Creation 4
Enable DNSSEC in a zone 4
Validation of DNS request using Group policy Management 4
Linking GPO and Domain 4
Acceptance Tests 4
Output 5

Resources and Prerequisites

1. A suitable host
    i. Windows 10 with Hyper-V
    ii. Windows 2016 with Hyper-V
2. A domain controller of GUI version which is updated and upgraded and assigned an ip address, dns server set and features such as Active directory domain services and DNS server added.
3. Access to documentation, for reference
    i. Microsoft Server
    ii. Hyper-V
4. Hard disk space to accommodate the proposed build and clones.

Inputs - Guest OS Specification

Guest OS	Windows 2016 Standard
VM Name	Dc1-tullamore
Processors / Cores	1
Main memory	1GB
Network Adapters	VLAN76
Admin username and password	Administrator,Abhilash@25

Table 1

Actions

Zone Creation

1. Once logged into the VM, Go to Server Manager > Tools > DNS.
2. The DNS Manager opens up. Right click on Forward Lookup Zones > New Zone > Click Next.
3. For Zone type- Choose Primary zone, Tick the check box to store the zone in Active Directory available only if DNS server is a suitable domain controller > Click Next.
4. Tick the box to all dns servers running on domain controllers in this domain:domain controller(dc1-tullamore)
5. Mention the zone name > Next > Next > Finish.
6. Right click on the zone created > New Host >Give Name and IP address > Add Host > Click Ok.

Enable DNSSEC in a zone

1. Select the new zone created. Right Click > DNSSEC > Sign the zone.
2. Click Next.
3. Zone signing wizard pops up. Choose customize zone signing parameters > Click Next.
4. Choose the DNS server dc1-tullamore as key master > Click Next.
5. Click Next.
6. On Key Signing Key Click Add button > Go for default values > Click OK.
7. Click Next > Next > Add > Choose default values > OK > Next.
8. Choose Use NSEC3 > Next.
9. Tick both checkboxes under Trust Anchors.
10. Click Next > Next > Next > Finish.

Validation of DNS request using Group policy Management

11. Go to Group Policy Management > Domains >Group policy objects
12. Right Click > New GPO > Assign a Name > Click OK.
13. Right Click on it > Edit.
14. Computer Configuration > Policies > Window Settings > Name Resolution Policy.
15. Under Name Resolution Policy enter the zone name on text box near Suffix.
16. Tick Checkbox Enable DNSSEC in the rule.
17. Under DNSSEC Settings, tick the box below Validation.
18. Click Create > Click Apply.

Linking GPO and Domain

19. Group policy Management > Domains > dc1-tullamore > Right Click > Link an existing GPO.
20. Under Group policy objects choose the GPO created > Click OK.
21. Go To command prompt > Execute command **gpupdate /force**.

Acceptance Tests

On the Windows PowerShell Execute below commands to verify successful validation of DNSSEC.

1. Get-DnsClientNrptPolicy

2. Get-DnsServerTrustAnchor -Name Test
3. Get-DnsServerTrustPoint
4. Resolve-DnsName -Name dc1-tullamore -Type A -Server dc1-tullamore
5. Resolve-DnsName -Name dc1-tullamore -Type A -Server dc1-tullamore -dnssecok

Output

1. Create a SOP for DNSSEC Configuration.