

**Test Lab Guide: Demonstrate DNS Security Extensions (DNSSEC) in Windows Server "8" Beta**

Microsoft Corporation

Published: February 2012

**Abstract**

This paper contains an introduction to Windows Server "8" Beta DNSSEC and step-by-step instructions for extending the Windows Server "8" Beta Base Configuration test lab to demonstrate DNSSEC operation.

**Copyright information**

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2012 Microsoft. All rights reserved.

Active Directory, Hyper-V, Microsoft, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[Introduction 5](#_Toc317868209)

[In this guide 6](#_Toc317868210)

[Test lab overview 6](#_Toc317868211)

[Hardware and software requirements 7](#_Toc317868212)

[Steps for Configuring the DNSSEC Test Lab 8](#_Toc317868213)

[Step 1: Set up the Base Configuration Test Lab 8](#_Toc317868214)

[Install the DNS Server role on APP1 9](#_Toc317868215)

[Configure APP1 as a DNS resolver 10](#_Toc317868216)

[Step 3: Configure DC1 10](#_Toc317868217)

[Sign a DNS zone 10](#_Toc317868218)

[View and modify DNSSEC settings 11](#_Toc317868219)

[Share the DNSSEC keyset 12](#_Toc317868220)

[Step 4: Import the trust point onto APP1 12](#_Toc317868221)

[Step 5: Configure Name Resolution Policy 13](#_Toc317868222)

[Step 6: Demonstrate DNSSEC validation using CLIENT1 14](#_Toc317868223)

[Snapshot the Configuration 15](#_Toc317868224)

# Introduction

DNS Security Extensions (DNSSEC) is a suite of extensions that add security to the DNS protocol. RFCs 4033, 4034, 4035, and 5155 specify the core DNSSEC extensions and add origin authority, data integrity, and authenticated denial of existence to DNS. In addition to several new concepts and operations for both the DNS server and the DNS client, DNSSEC introduces new resource records (DNSKEY, RRSIG, NSEC, NSEC3, and DS) to DNS.

DNSSEC allows for all the records in a DNS zone to be cryptographically signed. When a DNS server hosting a signed zone receives a query, it returns the digital signatures in addition to the records requested. A resolver or another server can obtain the public key of the public/private key pair and validate that the responses are authentic and have not been tampered with. In order to do so, the resolver or server must be configured with a trust anchor for the signed zone, or for a parent of the signed zone.

Windows Server 2008 R2 introduced support for DNSSEC, and provided the ability to generate keys and host a signed zone. However, there were several limitations to the support, as listed below.

* Zones could only be signed offline, over a file-based copy of the zone. It was not possible to generate signatures or update signatures on a zone while the zone was online.
* The processes of key generation and zone signing were manual, and required the command-line utility dnscmd
* Dynamic updates to DNS records were not supported
* There was no built-in support for automatic key rollovers

Windows Server "8" Beta introduces support for online signing and automated key management as part of updating the DNSSEC support in the DNS server’s authoritative functions. The new supported features include the following.

On the authoritative DNS server:

* Support for DNS dynamic updates in DNSSEC signed zones
* Support for updated DNSSEC standards, including NSEC3 and RSA/SHA-2
* Automated trust anchor distribution through Active Directory
* Automated trust anchor rollover support through RFC 5011
* Updated user interface with deployment and management wizards
* Windows PowerShell based command line interface for easy management and scripting

On the non-authoritative DNS resolver:

* Validation of records signed with updated DNSSEC standards (NSEC3, RSA/SHA-2)
* Automated trust anchor rollover support through RFC 5011
* Easy extraction of the root trust anchor

## In this guide

This guide provides step-by-step instructions for setting up a test lab based on the Windows Server "8" Beta Base Configuration and deploying DNSSEC using two server computers and one client computer. The resulting DNSSEC test lab demonstrates DNS validation functionality.

Important

The following instructions are for configuring a DNSSEC test lab using the minimum number of computers. Individual computers are needed to separate the services provided on the network and to clearly show the desired functionality. This configuration is neither designed to reflect best practices nor does it reflect a desired or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a separate test lab network.

Attempting to adapt this DNSSEC test lab configuration to a pilot or production deployment can result in configuration or functionality issues.

## Test lab overview

In this test lab, DNSSEC is deployed with:

* One computer running Windows Server "8" Beta named DC1 that is configured as an intranet domain controller, Domain Name System (DNS) server, and Dynamic Host Configuration Protocol (DHCP) server.
* One intranet member server running Windows Server "8" Beta named APP1 that is configured as a general application server and DNS server.
* One member client computer running Windows 8 Consumer Preview named CLIENT1 that is configured as a DNS resolver client.

The DNSSEC test lab consists of one subnet that simulates an intranet named Corpnet (10.0.0.0/24).

Computers connect using a hub or switch. See the following figure.

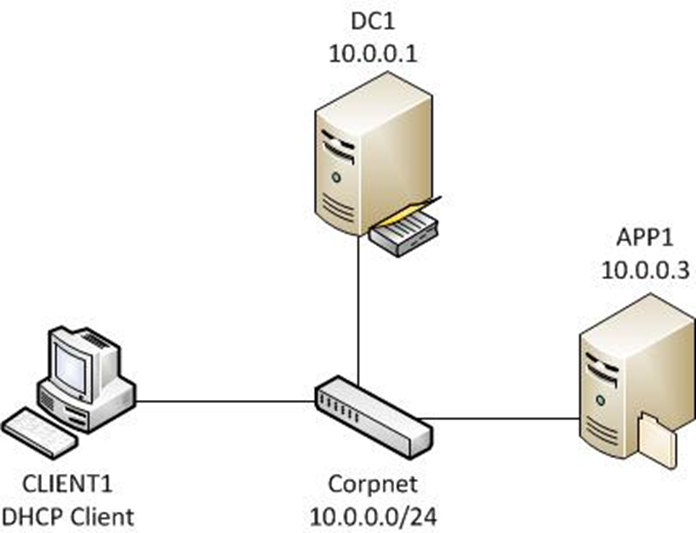


Figure DNSSEC Test Lab Configuration

The test lab instructions demonstrate the configuration of DNSSEC using the Zone Signing wizard. Steps to view and modify the DNSSEC configuration are presented, and DNSSEC operation is verified using a test DNS client.

## Hardware and software requirements

The following are required components of the test lab:

* The product disc or files for Windows Server "8" Beta.
* The product disc or files for Windows 8 Consumer Preview.
* Computers that meet the minimum hardware requirements for Windows Server "8" Beta.

# Steps for Configuring the DNSSEC Test Lab

There are six steps to follow when setting up a DNSSEC test lab based on the Test Lab Guide Base Configuration.

1. Set up the Base Configuration test lab.

The DNSSEC test lab requires the [Test Lab Guide: Windows Server "8" Beta Base Configuration](http://go.microsoft.com/fwlink/p/?LinkId=236358) Corpnet subnet as its starting point.

1. Configure APP1.

APP1 is already a member server computer that is configured with IIS and also acts as a file server. For the DNSSEC test lab, APP1 must be configured as a DNS resolver.

1. Configure DC1.

DC1 is already configured as a domain controller, DNS and DHCP server for the Corpnet subnet. For the DNSSEC test lab, DC1 must be configured as the key master for a signed DNS zone.

1. Configure APP1 as a trust point for DNSSEC validation.

APP1 does not host any DNS zones, and is used to perform DNSSEC validation of the signed zone hosted by DC1. For the DNSSEC test lab, APP1 must be configured as a trust point.

1. Configure Name Resolution Policy

DNSSEC validation settings will be applied to a test client via group policy and NRPT.

1. Demonstrate DNSSEC validation using CLIENT1.

CLIENT1 is a client computer running Windows 8 Consumer Preview. For the DNSSEC test lab, CLIENT1 will be used to test and demonstrate DNS validation operation.

This guide provides steps for configuring the computers of the Base Configuration test lab, configuring DNSSEC, and demonstrating DNSSEC operation. The following sections provide details about how to perform these tasks.

## Step 1: Set up the Base Configuration Test Lab

Set up the Base Configuration test lab for the Corpnet subnet using the procedures in the “Steps for Configuring the Corpnet Subnet” section of the [Test Lab Guide: Windows Server "8" Beta Base Configuration](http://go.microsoft.com/fwlink/p/?LinkId=236358). Connect **DC1**, **APP1**, and **CLIENT1** to the Corpnet subnet.

**Step 2: Configure APP1**

APP1 configuration for the DNSSEC test lab consists of the following procedure:

* Install the DNS Server role
* Configure APP1 as a DNS resolver

The following sections explain these procedures in detail.

### Install the DNS Server role on APP1

Configure APP1 as a DNS server. Install the DNS server role, but do not create a hosted zone. APP1 will not host any DNS zones, and will be used to perform DNSSEC validation of the signed zone hosted by DC1. The DNS settings will be deployed as part of DNSSEC configuration in subsequent steps.

**To install the DNS Server role on APP1**

|  |
| --- |
| 1. In the **Dashboard** console of Server Manager, under **Configure this local server**, click **Add roles and features**. 2. Click **Next** three times to get to the server role selection screen. 3. In the **Select Server Roles** dialog, select **DNS Server**, click **Add Features** when prompted, and then click **Next**. 4. In the **Select features** dialog, click **Next**. 5. Click **Next** on the DNS Server screen, and then click **Install**. 6. Allow the installation to complete, and then click **Close**. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.    **Install-WindowsFeature DNS -IncludeManagementTools** |

### Configure APP1 as a DNS resolver

To perform validation of DNS queries, APP1 must not be authoritative for the records that are being queried. This is because an authoritative server does not need to validate its own responses. For the purposes of this lab, in order to demonstrate trust point configuration, APP1 will be configured as a caching-only DNS server. Deploying DNS servers as caching-only resolvers will be common in a mixed-mode environment, where some DNS servers are Windows Server 8 while others are down-level versions of Windows Server.

To configure APP1 as a DNS resolver

|  |
| --- |
| 1. On **APP1**, from the Start screen, click **DNS**. 2. Expand **APP1**, and verify that no forward or reverse lockup zones are present. 3. Right-click **APP1** in the console tree, and then click **Properties**. 4. Click the **Forwarders** tab, and then click **Edit**. 5. Type **10.0.0.1**, and then click **OK**. 6. Wait for Server FQDN to resolve to DC1. 7. Clear the checkbox for **Use root hints if no forwarders are available**, and then click **OK**. |

## Step 3: Configure DC1

DC1 configuration for the DNSSEC test lab consists of the following procedures:

* Sign a DNS zone
* View and modify the DNSSEC settings
* Share the DNSSEC keyset for trust point import

The following sections explain these procedures in detail.

### Sign a DNS zone

DC1 is already an authoritative DNS server for the corp.contoso.com zone. In this step, you will sign the zone with default settings for DNSSEC using the zone signing wizard.

To sign the corp.contoso.com DNS zone

|  |
| --- |
| 1. On **DC1**, from the Start screen, click **DNS**. 2. Expand **DC1**, expand **Forward Lookup Zones**, and select **corp.contoso.com**. 3. Right-click **corp.contoso.com**, point to **DNSSEC**, and click **Sign the zone**. 4. On the introductory Zone Signing Wizard screen, click **Next**. 5. In the sign zone wizard, select **Use recommended settings to sign the zone**, and then click **Next**. 6. Note the default parameters displayed on the review page, and click **Next**. 7. Verify that the zone is signed successfully, and click **Finish**. 8. Right-click **corp.contoso.com**, and click **Refresh**. 9. Note that several new records have been added to the zone, and that the icon for the zone has changed to indicate that it has been signed by DNSSEC. |

### View and modify DNSSEC settings

The corp.contoso.com zone is now signed using all built-in default parameters. To view or change the DNSSEC settings, access the DNSSEC properties dialog for the zone.

To view or modify DNSSEC settings

|  |
| --- |
| 1. Right-click **corp.contoso.com**, point to **DNSSEC**, and click **Properties**. 2. DC1 is the only Active Directory-integrated DNS server for the corp.contoso.com zone. If another DNS server were available, you could specify that it be the key master on the **Key Master** tab. 3. Click the **KSK** tab. All of the default settings for the KSK are listed in the summary pane. To make changes to DNSKEY RRSET validity period or automatic rollover frequency, click **Edit**. You can manually initiate KSK failover by clicking the **Rollover** link on this tab. Links are also provided to add or remove KSKs. 4. Click the **ZSK** tab. All of the default settings for the ZSK are listed in the summary pane. To make changes to DNSKEY signature validity period, DS signature validity period, zone record validity period, or automatic rollover frequency, click **Edit**. You can manually initiate ZSK failover by clicking the **Rollover** link on this tab. Links are also provided to add or remove ZSKs. 5. Click the **Next Secure (NSEC)** tab. Use this tab to specify authenticated denial of existence using NSEC or NSEC3 (default). For NSEC3, specify the number of hash iterations and salt field parameters. 6. Click the **Trust Anchor** tab. Trust anchor distribution and automated key rollover can be enabled here. To enable other DNS servers in the forest that are AD-integrated to validate responses from the AD-integrated signed zone, select the “Distribute Trust Anchors to all servers in the forest” checkbox. Trust anchors must be manually configured on caching resolvers if the signed zoned is file-backed, if the caching resolver is not AD-integrated, or if the caching resolver is in a different AD forest. 7. Click the **Advanced** tab. Examine the options for setting signing and polling parameters. 8. Click **Cancel** to close the DNSSEC properties dialog. |

### Share the DNSSEC keyset

A trust anchor must be manually configured on the APP1 caching resolver since it is a standalone (non-AD-integrated) DNS server. To manually configure trust anchors, copy the “dsset-zonename” file found under **%windir%\system32\dns** on the key master server hosting a primary copy of the signed zone to the caching resolver. Use the following procedure to share the %windir%\system32\dns location on DC1.

To share the DNS directory on DC1

|  |
| --- |
| 1. On **DC1**, launch Windows Explorer, and then browse to the **Windows\System32\dns** directory. 2. Right-click **dns**, point to **Share with**, and then click **Advanced sharing**. 3. On the **Sharing** tab, click **Advanced Sharing**. 4. Select the **Share this folder** checkbox, and then click **OK**. 5. Click **Close** in the dns Properties dialog, and then close Windows Explorer. |

## Step 4: Import the trust point onto APP1

To validate DNSSEC data, APP1 must be provisioned with a trust anchor for the corp.contoso.com zone. To add this trust anchor to APP1, use the following procedure.

To import the trust point onto APP1

|  |
| --- |
| 1. On **APP1**, from the Start screen, click **DNS**. 2. Expand **APP1**, and select **Trust Points** in the console tree. 3. Right-click **Trust Points**, point to **Import**, and then click **DNSKEY**. 4. Under File to Import, type **\\DC1\dns\keyset-corp.contoso.com**, and then click OK. 5. Verify that trust points were imported for corp.contoso.com. |

## Step 5: Configure Name Resolution Policy

A Windows 8 Consumer Preview DNS client only performs DNSSEC validation on domain names where it is configured to do so by the Name Resolution Policy Table (NRPT). This determines the DNS client’s behavior when issuing queries and processing responses. In this step, you will create a group policy setting to configure CLIENT1 to perform DNSSEC validation.

To configure Name Resolution Policy

|  |
| --- |
| 1. On **DC1**, from the Start screen, click **Group Policy Management**. 2. Expand **Forest: corp.contoso.com**, expand **Domains**, expand **corp.contoso.com**, and then select **Group Policy Objects**. 3. Right-click **Group Policy Objects**, and then click **New**. 4. Under **Name**, type **DNSSEC**, and then click **OK**. 5. Right-click the **DNSSEC** GPO, and then click **Edit**. 6. In Group Policy Management Editor, expand **Computer Configuration>Policies>Windows Settings>Name Resolution Policy**. 7. Next to Suffix, type **corp.contoso.com**. 8. On the DNSSEC tab, select **Enable DNSSEC in this rule**, and **Require DNS clients to check that name and address data has been validated**. 9. Click **Create** to create the NRPT rule. 10. Click **Apply** to apply the NRPT setting. 11. Close the Group Policy Management Editor. 12. Right-click **corp.contoso.com** in the console tree, and click **Link an Existing GPO**. 13. Click **DNSSEC**, and then click **OK**. 14. Expand Group Policy Objects, and select the **DNSSEC** GPO. 15. On the **Scope** tab, select **Authenticated Users** under Security Filtering, click **Remove**, and then click **OK** in the confirmation dialog box that appears. 16. Click **Add**, click **Object Types**, select **Computers**, click **OK**, type **CLIENT1**, and then click **OK**. 17. Close Group Policy Management console. |

## Step 6: Demonstrate DNSSEC validation using CLIENT1

Use the following procedures to update the NRPT policy on CLIENT1 and then

To demonstrate DNSSEC operation on CLIENT1

|  |
| --- |
| 1. On CLIENT1, from the Start screen, type **PowerShell**. Right-click **Windows PowerShell**, and then click **Run as administrator**. 2. In the PowerShell window, type **gpupdate**, and then hit **ENTER** to update group policy. 3. Type **Get-DnsClientNrptPolicy** and hit **ENTER**. The applied NRPT is displayed. Note that DnsSecValidationRequired is set to True for the corp.contoso.com domain. 4. Test validated DNS resolution from DC1. Type **Resolve-DnsName dc1.corp.contoso.com -Server 10.0.0.1 -DnssecOk**, and then hit **ENTER**. Note that the data returned from DC1 includes a signature and RRSIG value. 5. Type **ipconfig /flushdns** and then hit **ENTER** to clear the DNS resolver cache. 6. Test validated DNS resolution from APP1. Type **Resolve-DnsName dc1.corp.contoso.com -Server 10.0.0.3 -DnssecOk**, and then hit **ENTER**. Note that APP1 is also performing DNSSEC validation as a caching-only DNS server with a trust anchor for corp.contoso.com. |

# Snapshot the Configuration

This completes the DNSSEC test lab. To save this configuration so that you can quickly return to a working DNSSEC configuration from which you can test other DDNS modular test lab guides (TLGs), TLG extensions, or for your own experimentation and learning, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then perform a graceful shutdown.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots **DNSSEC TLG**. If your lab uses physical computers, create disk images to save the DNSSEC test lab configuration.

**Additional Resources**

For more information about DHCP see the [Domain Name System TechNet portal](http://technet.microsoft.com/en-us/network/bb629410.aspx).

For a list of all of the Windows Server “8” Beta TLGs, see [Windows Server “8” Beta Test Lab Guides](http://go.microsoft.com/fwlink/?LinkID=243062) in the TechNet Wiki.

For a list of additional Microsoft TLGs, see [Test Lab Guides](http://go.microsoft.com/fwlink/?LinkID=202817) in the TechNet Wiki.

To provide the authors of this guide with feedback or suggestions for improvement, send an email message to [tlgfb@microsoft.com](file:///C:\Users\josephd\Documents\SharePoint%20Drafts\tlgfb@microsoft.com).