Lesson 12: Implementing an Advanced DNS Solution

MOAC 70-412: Configuring Advanced Windows Server 2012 Services

Microsoft
Official Academic Course

WILEY

Overview

- Objective 4.2 – Configure advanced file services.
  - Configure Security for DNS including DNSSEC, DNS Socket Pool, and Cache Locking
  - Configure DNS logging
  - Configure delegated administration
  - Configure recursion
  - Configure netmask ordering
  - Configure a GlobalNames zone

Configuring Security for DNS

Lesson 12: Implementing an Advanced DNS Solution

Security for DNS

- Windows Server 2012 adds a number of new features to domain name system (DNS) security.
- Securing the DNS server and DNS records prevents false records from being added and prevents clients from receiving incorrect DNS query responses, which can lead them to visit phishing sites or worse.
- To prevent DNS being used to attack systems, implement DNS Security (DNSSEC), Cache Locking, and other security measures.

DNS Security (DNSSEC)

- A client that uses DNS to connect is always vulnerable to redirection to an attacker's servers unless the zone has been secured using DNSSEC.
- The process for securing a zone using DNSSEC is called ***signing the zone***.
- Once signed, any queries on the signed zone will return digital signatures along with the normal DNS resource records.
- The digital signatures are verified using the public key of the server or zone from the ***trust anchor***.
- DNSSEC uses trust anchors represented by public keys that define the top of a chain of trust.
- The trust anchor verifies that a digital signature and its associated data is valid.

DNS Security (DNSSEC)

- ***DNS Security (DNSSEC)*** is a suite of protocols defined by the Internet Engineering Task Force (IETF) for use on IP networks.
- DNSSEC provides DNS clients, or resolvers, with proof of identity of DNS records and verified denial of existence.
- DNSSEC does *not* provide availability or confidentiality information.

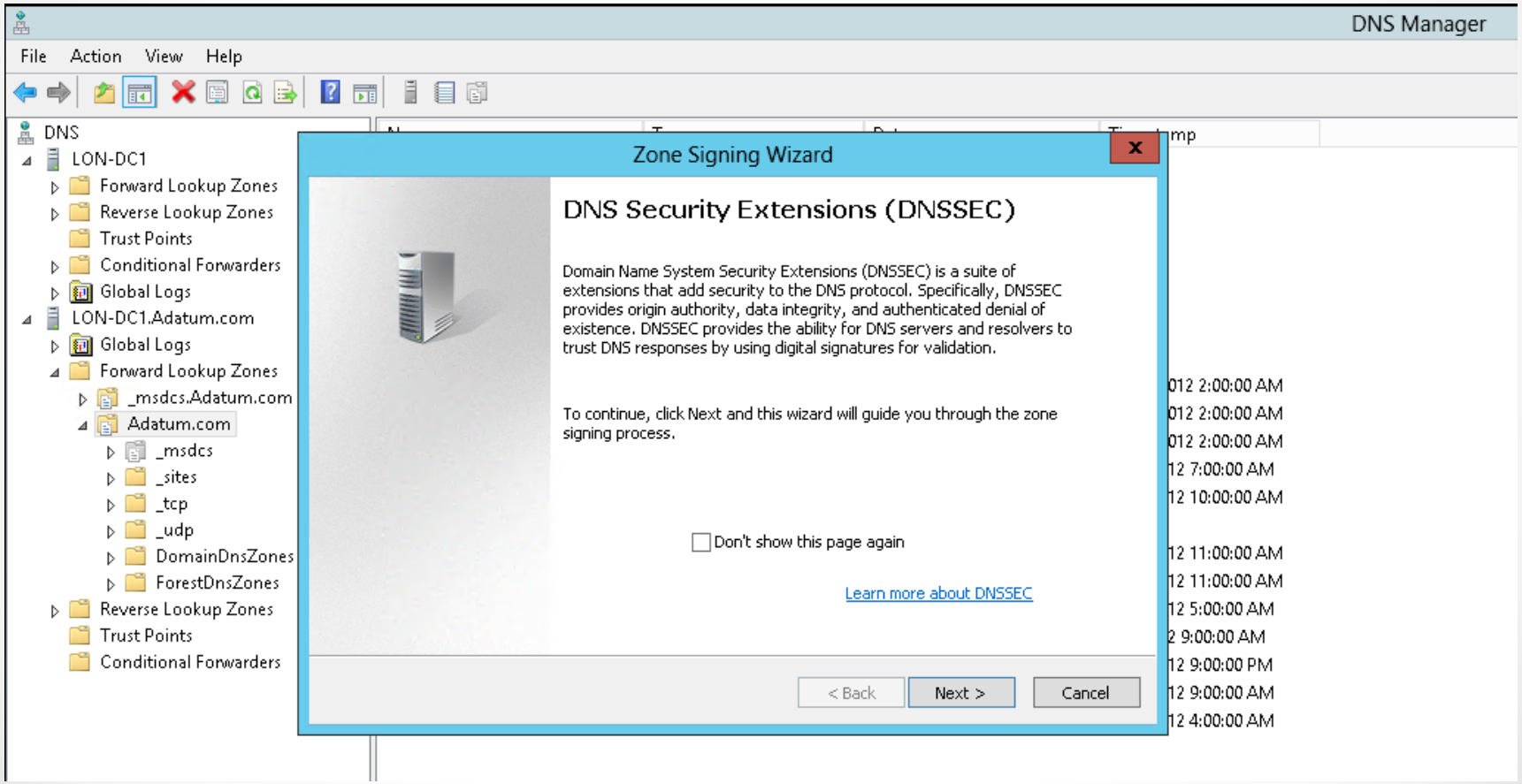
DNS Security (DNSSEC)

- DNSSEC can be enabled on an Active-Directory Integrated zone (ADI) or on a primary zone.
- DNSSEC is installed as part of the DNS Server role.
- To enable DNSSEC, Windows Server 2012 provides a DNSSEC Zone Signing Wizard.
- This wizard runs from the DNS console and configures the ***Zone Signing Parameters*** and all the settings required for ensuring the zone is signed correctly and securely.

DNS Security (DNSSEC)

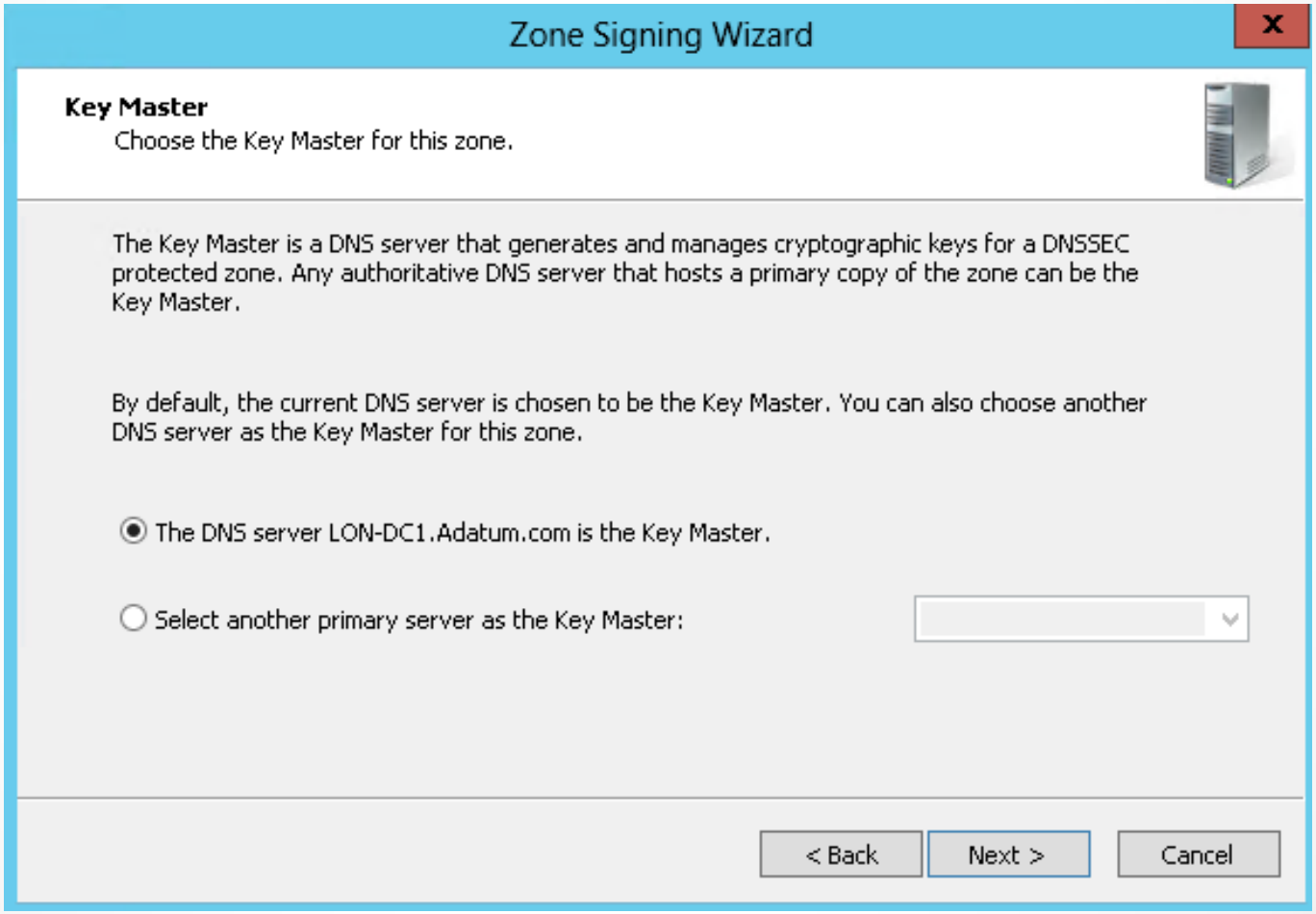
- DNSSEC uses a series of keys, including the ***Key Signing Key (KSK)*** and the ***Zone Signing Key (ZSK)***, to secure the server and the zones.
- The KSK is an authentication key that signs all the DNSKEY records at the root of the zone, and it is part of the chain of trust.
- The ZSK is used to sign zone data.
- ***Automated key rollover*** is the process by which a DNSSEC key management strategy is made easier with automated key regeneration.

DNS Security (DNSSEC)

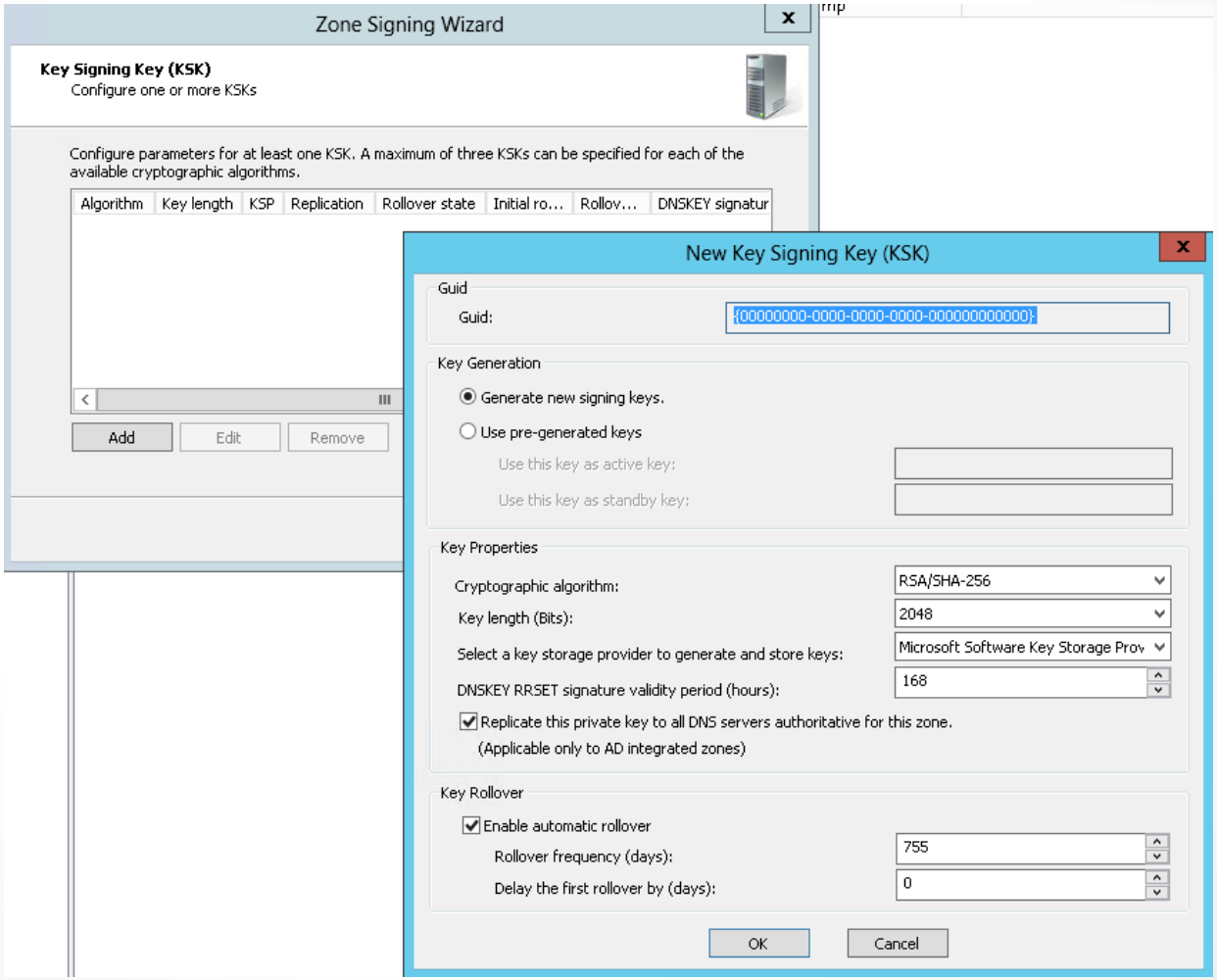


DNS Security (DNSSEC)

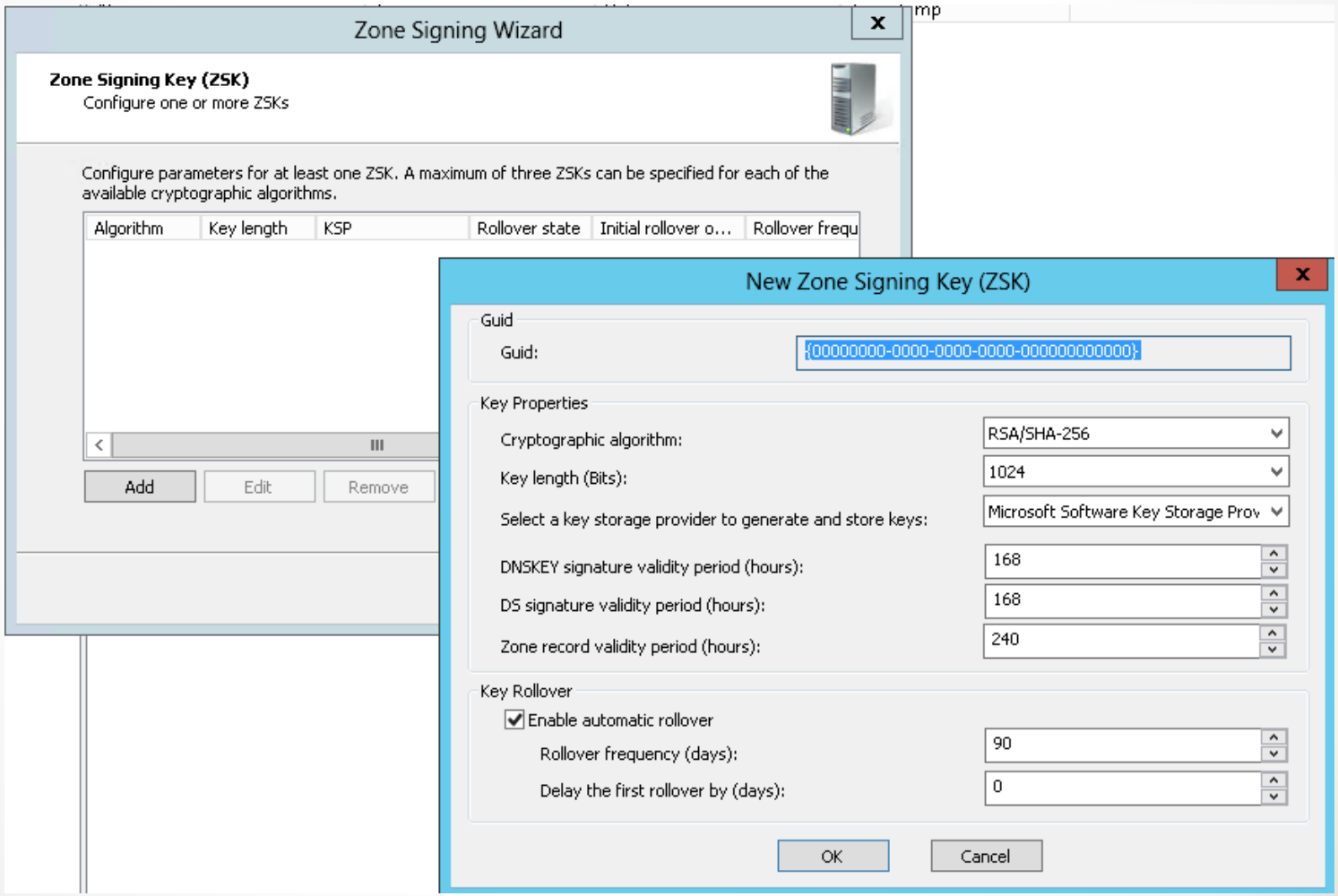
DNS Security (DNSSEC)



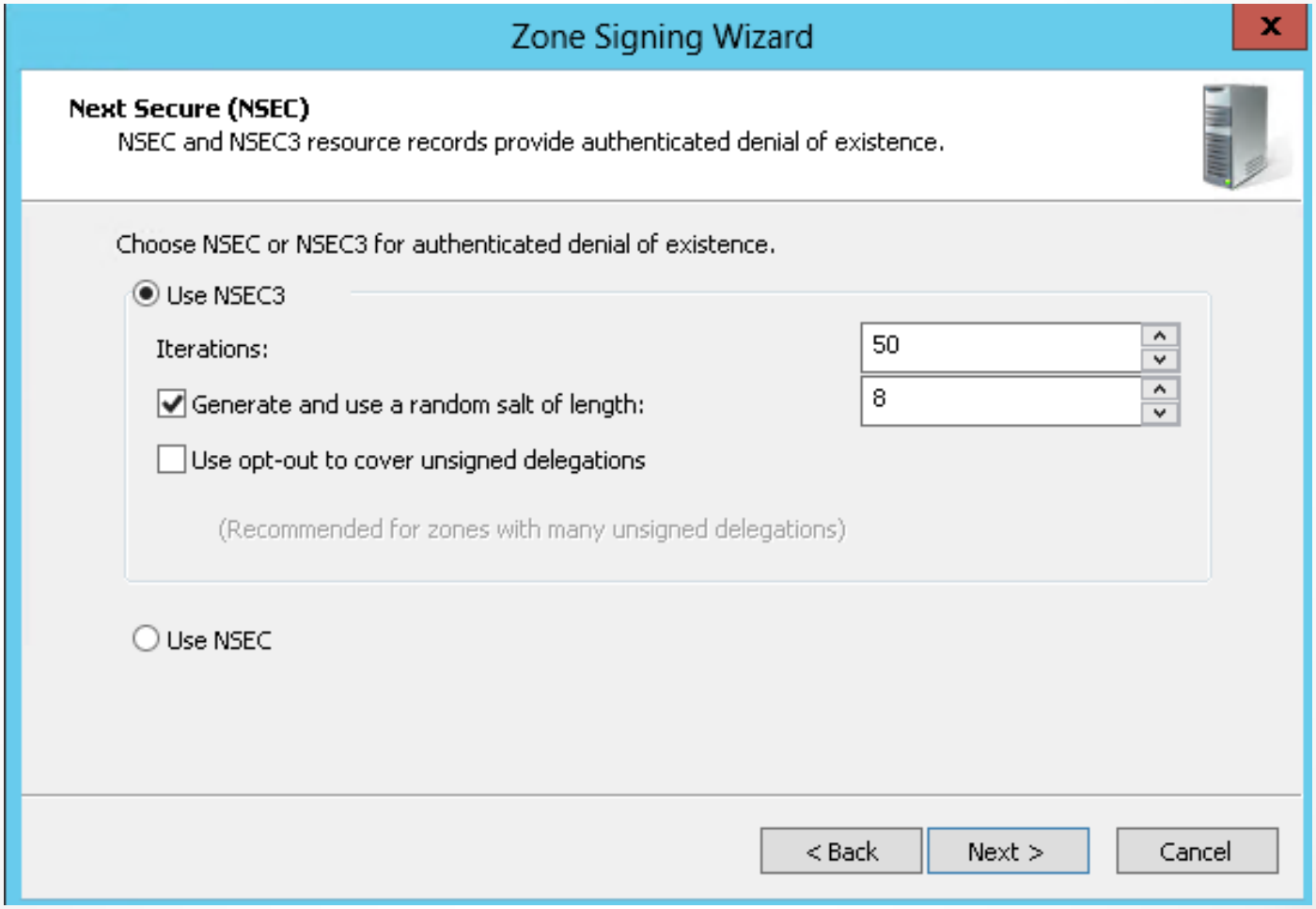
DNS Security (DNSSEC)



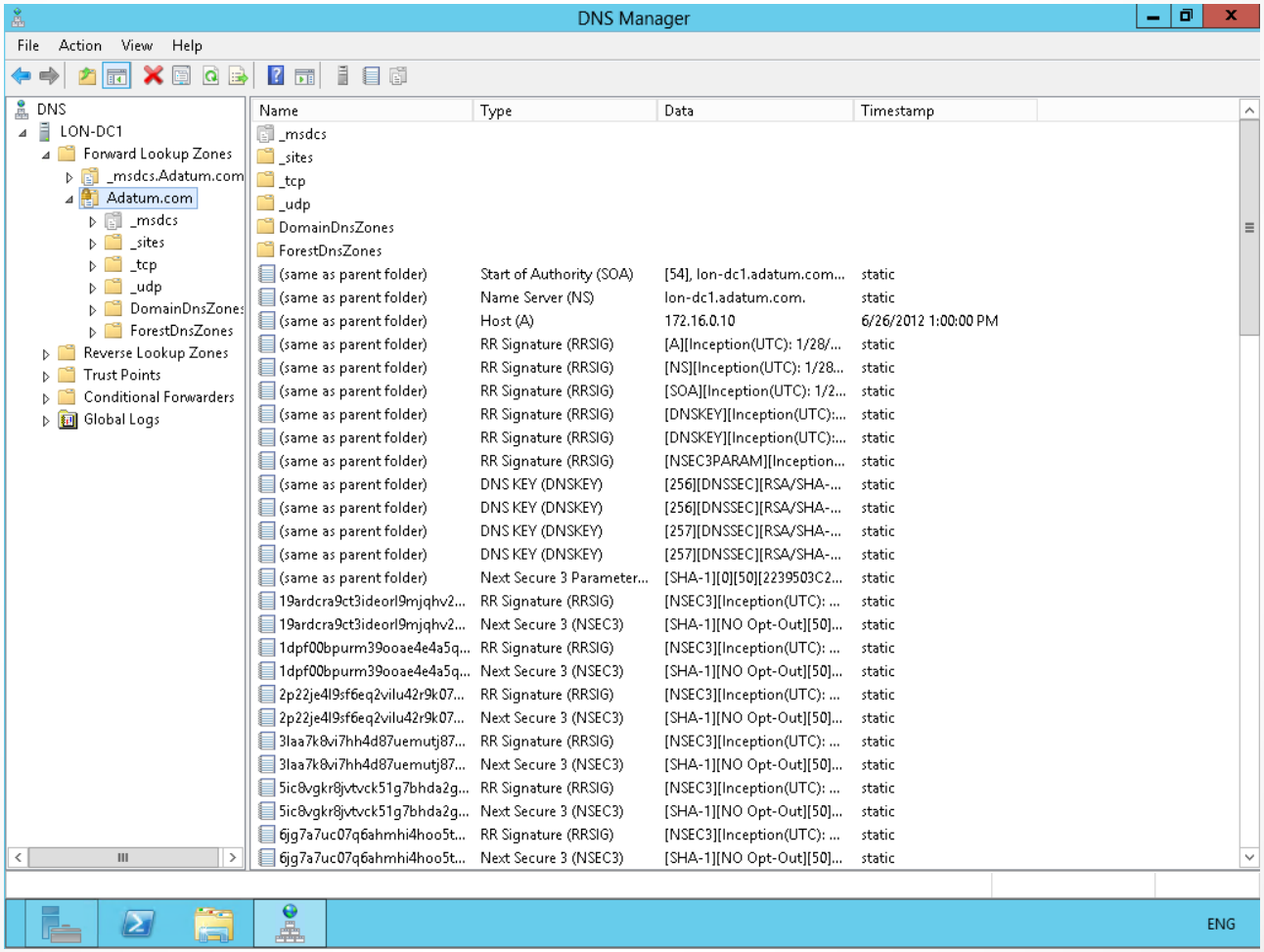
DNS Security (DNSSEC)



DNS Security (DNSSEC)



DNS Security (DNSSEC)



DNS Socket Pool

- The ***DNS socket pool*** is a tool used to allow source port randomization for DNS queries, which reduces the chances of an attacker guessing the IP address and port (socket) used by DNS traffic.
- The DNS socket pool protects against DNS spoofing attacks.
- To be able to tamper with DNS traffic, an attacker needs to know the correct socket and the randomly generated transaction ID.
- DNS socket pooling is enabled by default in Windows Server 2012.
- The default size of the DNS socket pool is 2500, and the available settings range from 0 to 10,000.
  - The larger the number of ports available to the pool, the more secure the communication.

DNS Socket Pool

- Windows Server 2012 also allows for an exclusion list to be created. The preferred method to set the socket pool size is through the use of the dnscmd command-line tool as shown here:
  1. Launch an elevated command prompt.
  2. Type the following command:

     ```
     dnscmd /Config /SocketPoolSize <value>
     ```
- The value must be between 0 and 10,000.

DNS Cache Locking

- DNS cache locking prevents an attacker from replacing records in the resolver cache while the Time to Live (TTL) is still in force.
- When cache locking is enabled, records cannot be overwritten.

DNS Cache Locking

- The preferred method to set the DNS cache locking value is through the use of the dnscmd command-line tool as shown here:
  1. Launch an elevated command prompt.
  2. Type the following command:

     `dnscmd /Config /CacheLockingPercent <percent>`
  3. Restart the DNS Service to apply the new settings by using the **`net stop DNS`** command followed by the **`net start DNS`** command.

DNS Debug Logging

- DNS logging is a troubleshooting tool that allows for detailed, file-based analysis of all DNS packets and messages.
- Event Viewer is an essential tool in the successful management and troubleshooting of a DNS server. Windows Server 2012 provides a specific DNS server application log.
- Dns.log contains the debug logging activity. By default, this is located in the %SYSTEMROOT%\System32\Dns folder

DNS Delegated Administration

- DNS is a key service within your network. Administration of the service should be restricted to those who really need it.
- The principle of least privilege should always apply to DNS administration.

DNS Delegated Administration

- To delegate administration privileges to a specific user or security group, add that user or group to the DNS Admins security group.
  - Members of this group can view and modify all DNS data, settings, and the configuration of DNS servers within their home domain.
- It is best practice to add individual users to the Global or Universal group and then to add the Global or Universal groups to the Domain Local Groups (such as the DNS Admins Group).

DNS Recursion

- ***Recursion*** in DNS is the process by which a client makes a query to a DNS server for an IP address associated with a Fully Qualified Domain Name (FQDN).
- The server then establishes that IP address through one or many separate queries to other servers and returns the address to the querying client.
- If the DNS server is configured for recursion, the server makes a recursive query to other DNS servers (usually through root hints on the Internet) and eventually provides the authoritative answer to the querying client.

DNS Recursion

- If recursion is disabled and root hints and forwarders are not used on any DNS servers, then *no* external queries will ever be resolved.
- In short, your network will never be able to connect to named resources on the Internet.

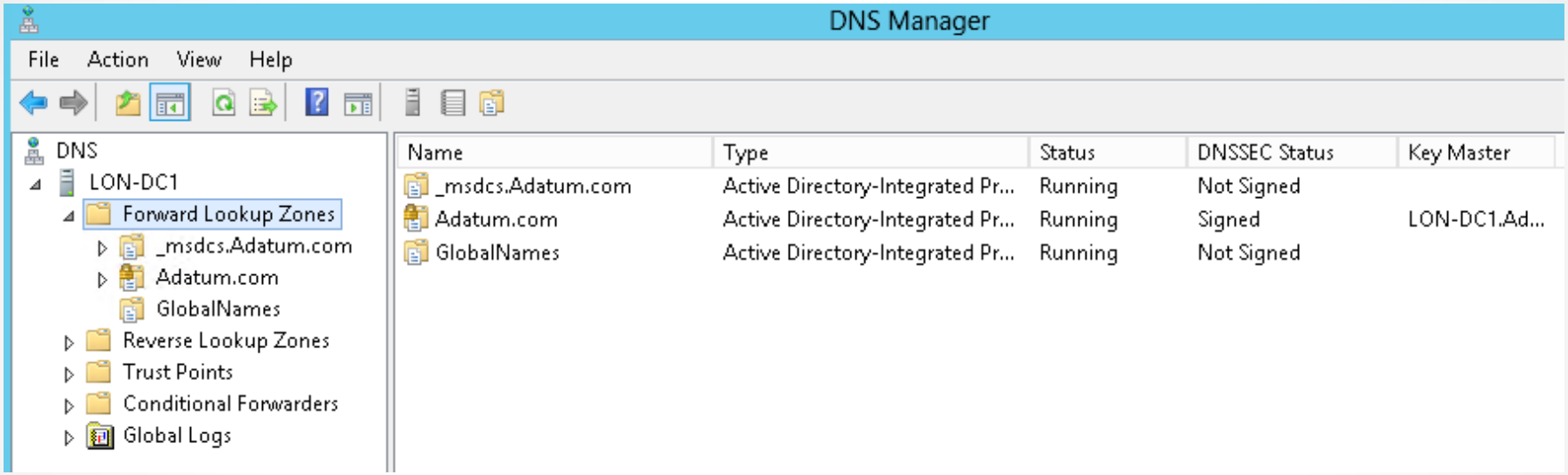
Netmask Ordering

- ***Netmask ordering*** prioritizes DNS responses based on the subnet of the requesting client.
- If several A records exist for a single name, then the one that exists in the requesting client's subnet is returned.
- Netmask ordering is enabled by default in Windows Server 2012.
- It is also possible to change the subnet mask used to define the subnets.
  - The default is a Class C network.

GlobalNames Zone

- Windows Server 2012 DNS provides support for single-label names without the need for NETBIOS or WINS.
- This allows a large multi-DNS environment to support a single name, such as address book, rather than an FQDN, such as addressbook.adatum.com.
- In an environment where there are several DNS suffixes such as contoso.com adatum.com and fabrikam.net, it is necessary to manually create a GlobalNames zone within DNS to allow a single-label name to be resolved.

GlobalNames Zone



Lesson Summary

- Windows Server 2012 adds new features to domain name system (DNS) security. You learned how to configure security for your DNS server and DNS zones using DNSSEC, socket pooling, cache locking, and the Name Resolution Policy Table (NRPT).
- DNSSEC can be enabled on an Active-Directory Integrated zone (ADI) or on a primary zone.
- The DNS socket pool is a tool used to allow source port randomization for DNS queries, which reduces the chances of an attacker guessing the IP address and port (socket) used by DNS traffic.
- The preferred method to set the DNS cache locking value is through the use of the dnscmd command-line tool.

Lesson Summary

- DNS logging is a troubleshooting tool that allows for detailed, file-based analysis of all DNS packets and messages. There are benefits and drawbacks of DNS Debug logging and how to configure it.
- Domain Admins have full permissions by default to manage all aspects of the DNS server, but only in the domain where the Domain Admins security group is located. A member of the Enterprise Admins group has similar permissions but throughout the entire forest.

Lesson Summary

- Recursion in DNS is the process by which a client makes a query to a DNS server for an IP address associated with a Fully Qualified Domain Name (FQDN).
- Netmask ordering prioritizes DNS responses based on the subnet of the requesting client.
- Windows Server 2012 DNS provides support for single-label names without the need for NETBIOS or WINS.