Exam Report: 9.1.5 Practice Questions

Date: 11/27/2019 10:03:17 am
Time Spent: 8:52

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 44%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

You manage a company network with a single Active Directory domain running on two domain controllers. The two domain controllers are also DNS servers and hold an Active Directory-integrated copy of the zone used on the private network.

The network has five subnets with DHCP servers delivering IP address and other configuration to host computers. All host computers run Windows 10.

You want to ensure that all client computers use the DNS server for DNS host name resolution. Hosts should not be able to automatically discover DNS host names, even for computers on their own subnet.

What should you do?

- Configure the HOSTS file on each client with the IP address of the DNS server on the local subnet.
- Edit the default domain Group Policy object (GPO). Enable the Turn off Multicast Name Resolution policy.
- Configure dynamic DNS (DDNS) on your DHCP servers.
- ~~Configure one of your DNS servers as an authoritative DNS server.~~

Explanation

To prevent client computers from automatically resolving DNS host names on the local subnet, use a GPO to enable the Turn off Multicast Name Resolution policy. This disables Link-Local Multicast Name Resolution (LLMNR). For example, you can use Group Policy Management to edit the Default Domain policy by going **to Computer Configuration\Administrative Templates\Network\DNS Client** and enabling the Turn off Multicast Name Resolution policy.

By default, all Windows clients (Vista and later) have LLMNR enabled. Configuring clients to get DNS server addresses from a DHCP server does not disable LLMNR.

Configuring an authoritative DNS server will not disable LLMNR on the Windows clients. Configuring (DDNS) on your DHCP servers also does not not disable LLMNR on the Windows clients. The IP address of the DNS server should be assigned to the client systems by the DHCP server, not manually configured in the HOSTS file.

References

LabSim for Server Pro 2016, Section 9.1.
[AllQuestions_ServerPro_2017.exm DNS SINGLE 01]

Question 2: Incorrect

You manage the branch office for your company network. The branch office has a single Active Directory domain, branch1.westsim.private. All computers in the branch office are members of the domain.

The branch office consists of two subnets and 50 host computers. Each subnet has its own DHCP server, while a single server on Subnet2 is both the domain controller and DNS server. Dynamic

updates are enabled on the DNS zone.

On Subnet1, you have a shared printer attached to Wrk5. Only computers on Subnet1 use this shared printer.

How can you most easily make sure that all hosts on Subnet1 will continue to connect to the shared printer by name, even if the DNS server becomes unavailable?

- Edit the default domain GPO to enable the Turn off Multicast Name Resolution policy.
- View the settings in the Default Domain GPO to verify that theTurn off Multicast Name Resolution option is not enabled.
- ~~Configure a static entry for the shared printer in the HOSTS file on each client in Subnet1.~~
- Use DHCP to deliver the IP address of the shared printer to each client on Subnet1.

Explanation

In this scenario, you need to provide for DNS name resolution on the local subnet in the event that the DNS server fails. To make sure you can rely on the Link-Local Multicast Name Resolution feature (LLMNR), which is enabled on clients by default, verify that LLMNR has not been disabled.

Enabling the Turn off Multicast Name Resolution policy in Group Policy disables Link-Local Multicast Name Resolution. DHCP servers can not be configured to deliver IP addresses of printers. Configuring a static entry for the shared printer in the HOSTS file on each client in Subnet1 would take too much of your time.

References

LabSim for Server Pro 2016, Section 9.1.
[AllQuestions_ServerPro_2017.exm DNS SINGLE 02]

Question 3: Incorrect

The Domain Name service is made up of several components. Drag each component on the left to its appropriate description on the right. (Each component may used once, more than once, or not at all.)

The last part of a domain name (.com, .edu, .gov).

✓ Top-level domain (TDL)

Used to store entries for host names, IP addresses, and other information in the zone database.

✓ Records

Also called the root domain, it denotes a fully qualified, unambiguous domain name.

~~Fully qualified domain name (FQDN)~~ . (dot) domain

A DNS server that has a full and complete copy of all the records for a particular domain.

✓ Authoritative server

Maps a DNS host name to an IPv4 (32-bit) address.

~~Host name~~ Records

Includes the host name and all domain names separated by periods.

~~. (dot) domain~~ Fully qualified domain name (FQDN)

Explanation

The Domain Name Service includes, but is not limited to, the following components:

- **. (dot) domain**: also called the root domain, it denotes a fully qualified unambiguous domain name.
- **Top-level domain (TDL)**: the last part of a domain name (.com, .edu, .gov).

- **Fully qualified domain name (FQDN)**: includes the host name and all domain names separated by periods.
- **Host name**: the part of a domain name that represents a specific host.
- **Records**: used to store entries for host names, IP addresses, and other information in the zone database. For example, an A record maps a DNS hostname to an IPv4 (32-bit) address. This is the most common resource record type.
- **Authoritative server**: a DNS server that has a full and complete copy of all the records for a particular domain.

References

LabSim for Server Pro 2016, Section 9.1.
[AllQuestions_ServerPro_2017.exm DNS SINGLE 03]

Question 4: Correct

You are system administrator with hundreds of host workstations to manage and maintain. You need to enable hosts on your network to find the IP addresses of alphanumeric host names such as srv1.myserver.com.

Which of the following would you use?

- ○ DHCP server
- ○ Dynamic DNS (DDNS) server
- ○ HOSTS file
- ◉ DNS server

Explanation

Use a DNS server to provide hostname-to-IP address resolution.

Using a HOSTS file would requires that you manually edit and maintain a very large file on every host in your part of the organization. A DHCP server can used to assign the address of the DNS server to each workstation after the DNS server is up and running. DDNS enables clients or the DHCP server to update records in the zone database after the DNS server is up and running.

References

LabSim for Server Pro 2016, Section 9.1.
[AllQuestions_ServerPro_2017.exm DNS SINGLE 04]

Question 5: Correct

Listed below are several DNS record types. Drag the record type on the left the appropriate function on the right.

Provides alternate names to hosts that already have a host record.
- ✓ CNAME

Points an IP address to a host name.
- ✓ PTR

Points a host name to an IPv6 address.
- ✓ AAAA

Points a host name to an IPv4 address.
- ✓ A

Identifies servers that can be used to deliver mail.
- ✓ MX

Explanation

Records are used to store entries for host names, IP addresses, and other information in the

zone database. Below are some common DNS record types:

- The A record maps an IPv4 (32-bit) DNS hostname to an IP address. This is the most common resource record type.
- The AAAA record maps an IPv6 (128-bit) DNS hostname to an IP address.
- The PTR record maps an IP address to a host name (it "points" to an A record).
- The MX record identifies servers that can be used to deliver email.
- The CNAME record provides alternate names (or aliases) to hosts that already have a host record. Using a single A record with multiple CNAME records means that when the IP address changes, only the A record needs to be modified.

References

LabSim for Server Pro 2016, Section 9.1.
[AllQuestions_ServerPro_2017.exm DNS SINGLE 05]

Question 6: Correct

Which of the following DNS components automatically creates and deletes host records when an IP address lease is created or released?

- Forward lookup
- DHCP Relay
- Dynamic NAT
- Dynamic DNS

Explanation

Dynamic DNS (DDNS) enables clients or the DHCP server to update records in the zone database automatically whenever an IP address lease is created or renewed.

A forward lookup is the process of resolving a host name to an IP address. A DHCP relay is used to forward DHCP requests to a DHCP server in a different subnet. Dynamic NAT is used to automatically map internal IP addresses with a dynamic port assignment.

References

LabSim for Server Pro 2016, Section 9.1.
[AllQuestions_ServerPro_2017.exm DNS SINGLE 06]

Question 7: Incorrect

Which of the following describes an additional domain?

- Additional domains are second-level domains with names registered to an individual or organization for use on the Internet.
- Additional domains are managed by the Internet Corporation of Assigned Names and Numbers (ICANN).
- An additional domain has a full and complete copy of all the records for a particular domain.
- ~~An additional domain represents a specific host. For example, "www" is the host name of www.example.com.~~

Explanation

Additional domains are second-level domains with names registered to an individual or organization for use on the Internet. These names are based on an appropriate top-level domain, depending on the type of organization or geographic location where a name is used. Yahoo.com and microsoft.com are examples of additional domains in your DNS structure.

The host name is the part of a domain name that represents a specific host. For example, "www" is the host name of www.example.com. An authoritative server is a DNS server that has a full and complete copy of all the records for a particular domain. TDLs are the last part of a domain name (.com, .edu, .gov) and are managed by the Internet Corporation of Assigned Names and Numbers (ICANN).

References

LabSim for Server Pro 2016, Section 9.1.
[AllQuestions_ServerPro_2017.exm DNS SINGLE 07]

Question 8: Incorrect

You are a network engineer working for WestSim Corporation. The company has an Internet domain named westsim.com. The private network uses the namespace of private.westsim.com. Your company manages its own Domain Name System (DNS) servers that are authoritative for both of the company's name spaces.

Your network consists of several subnets at multiple locations. Sites are connected with WAN links.

www.private.westsim.com is an intranet web server that is commonly used throughout the company. You want to ensure that users can always access this server by name, even if an authoritative DNS server is not available.

What should you do?

- Configure each client computer's alternate DNS server with the IP address of a second private DNS server.
- Configure each client computer's HOSTS file with an entry for www.private.westsim.com.
- Configure each client computer's LMHOSTS file with an entry for www.private.westsim.com.
- ~~Configure each client computer's alternate DNS server with the IP address of the company's public DNS server.~~

Explanation

Entries in a computer's HOSTS file are automatically loaded into the DNS cache and can be used to resolve DNS names when a DNS server is not available. One benefit of configuring a HOSTS file is to provide DNS name resolution fault tolerance if all DNS servers happen to go down. Configuring a HOSTS file for every client computer can be time consuming, although one way to ease the administrative burden is to create a single preconfigured hosts file and distribute it to all users.

Configuring an alternate DNS server address for clients is a good idea, but this action will not help if all DNS servers happen to become unavailable as the alternate DNS server will also be unavailable.

References

LabSim for Server Pro 2016, Section 9.1.
[AllQuestions_ServerPro_2017.exm DNS SINGLE 08]