1Y0-350 Citrix NetScaler 10 Essentials and Networking practice exam

Section 1: Configuring basic NetScaler settings (e.g. hostname, NetScaler IP, NTP,etc)

1.1

Specific Task: Set initial Hostname, NetScaler IP, subnet and gateway

Objective: How to set initial hostname, NetScaler IP, subnet, and gateway

1. An engineer has installed a NetScaler virtual appliance on a supported Citrix XenServer host.

   Which three details are required to set up the initial configuration by using the NetScaler VPX console? (Choose three.)

   a. MIP
   b. SNIP
   c. NSIP
   d. VLAN ID
   e. Subnet Mask
   f. Default Gateway

   Answer: c.e.f.

   Explanation: After installing a Citrix NetScaler VPX virtual appliance, an engineer needs to access it to configure the basic settings. Initially, an engineer must access the NetScaler command line through the respective management application of the virtualization host (either Citrix XenCenter for Citrix XenServer or VMware vSphere client for VMware ESX) to specify a NetScaler IP (NSIP) address, subnet mask, and default gateway. The NSIP is the management address at which the engineer can then access the NetScaler command line, through an SSH client, or access the configuration utility. The engineer can use either of these access methods, or the console, to continue with basic configuration.

   Source: Citrix NetScaler VPX Getting Started Guide – Release 10
   http://support.citrix.com/article/CTX132363

Section 2: Configuring network-related settings of the NetScaler implementation (e.g. vLans, routes, NAT/RNAT,etc)

2.1

Specific Task: Enable feature and configure mode advance (Mac based forwarding (MBF) and edge configuration)

Objective: Given a scenario, determine what should be configured on a NetScaler Appliance.

2. **Scenario:** An engineer is implementing load balancing for FTP site. It is required by an application to use active mode. The engineer decided to use Direct Server Return (DSR) Feature on the NetScaler Appliance.

   What two steps are required to accomplish this task? (Choose two.)

a. Enable USIP (use source IP) mode.
b. Enable USNIP (use subnet IP) mode.
c. Enable MBF (Mac Based Forwarding) mode.
d. Enable DRADV (Direct Route Advertisement) mode.
e. Configure static routes to NetScaler appliance on the backend servers
f. Configure NetScaler appliance as a default gateway on the backend servers.

   Answer: a.c.

   Explanation: When an engineer configures the DSR feature on the NetScaler appliance, the client request passes through the NetScaler appliance. However, the response from the backend server is sent directly to the client bypassing the NetScaler appliance. The following must be configured on the NetScaler appliance: Media Access Control (MAC) Based Forwarding (MBF) must be enabled globally on the appliance. Use Source IP (USIP) mode must be enabled on the services. “-m mac” must be enabled on the virtual server (VServer). For some connection types, “-connfailover STATELESS” must be enabled on the VServer. The default gateway of the servers should be the router interface to ensure that the responses from the servers bypass the appliance. A non_arping loopback interface with the same IP address as that of the VServer must be configured on the servers.

   Source: How to Configure the Direct Server Return on a NetScaler Appliance
   http://support.citrix.com/article/CTX110501

Section 3: Securing the NetScaler implementation and traffic (i.e. configuring SSL options, Access Control Lists, etc.)

3.1

Specific Task: Configure SSL options

Objective: How and what to consider for configuring SSL options

3. **Scenario:** A company is utilizing NetScaler to provide a B2B web service with government agency. The security requirement mandates the usage of SSL tunnels between web servers and the SSL tunnels cannot be terminated anywhere else other than the web servers.

   The engineer should configure _____ on the NetScaler to meet the requirements.

   a. SSL Bridging
   b. Transparent SSL Acceleration
   c. SSL Offloading with End-to-End Encryption
   d. SSL Acceleration with HTTP on the Front-End and SSL on the Back-End

   Answer: a.

   Explanation: An SSL bridge configured on the NetScaler appliance enables the appliance to bridge all secure traffic directly to the web server. The appliance does not offload or accelerate the bridged traffic. The Web server must handle all SSL-related processing. Also, features such as content switching, SureConnect, and cache redirection do not work, because the traffic passing through the NetScaler is encrypted.

   Source: Citrix NetScaler Traffic Management Guide - Release 10, Page 564 and 571
   http://support.citrix.com/article/CTX132359

Section 5: Configuring SSL OffLoading

5.1

Specific Task: Create, verify and import certificates and link certificate chains

Objective: How and Why to create, verify, and import certificates and link certificate chains

4. An engineer plans to create an SSL offload virtual server.

   Select the right sequence of steps necessary for the engineer to accomplish the task.

   a. create private key; create a certificate; create CSR; Submit CSR to a certification authority; create an ssl vServer and configure to use the certificate
   b. create CSR; create private key; create an ssl vServer and configure to use the private key; submit CSR to a certification authority; upload the certificate to NetScaler; bind the certificate with the private key
   c. create public key; create CSR; submit CSR to a certification authority; upload the certificate to NetScaler; create certificate/public key pair; create an ssl vServer and configure to use the certificate/public key pair
   d. create private key; create CSR; submit CSR to a certification authority; upload the certificate to NetScaler; create certificate/private key pair; create an ssl vServer and configure to use the certificate/private key pair

   Answer: d.

   Explanation: A private key is created first, then the CSR (certificate signing request) is created based on the key file. The CSR is submitted to a certification authority. Once the cert is received it needs to be uploaded to NetScaler and bound with the private key to create a certificate-key pair. After that the certificate can be used to configure an SSL offload virtual server.

   Source: How to Generate and Install a Public SSL Certificate on a NetScaler Appliance http://support.citrix.com/article/CTX109260

Section 6: Configuring acceleration and optimization of traffic handling

6.1

Specific Task: Enable and configure compression.

Objective: Given a scenario, determine how the HTTP compression should be configured on a NetScaler Appliance.

5. An engineer plans to configure the HTTP compression for a load balancing vServer to ensure that only responses that are bigger than 1 kB will be compressed.

   Which step should the engineer take to meet the requirements?

   a. Configure global compression parameters.
   b. Configure dataLength parameter of vServer.
   c. Create a new compression policy and bind it globally.
   d. Create a new compression policy and bind it to the vServer.

   Answer: a.

   Explanation: To configure the smallest response size to be compressed by NetScaler you need to configure global compression parameters. This option can't be configured on the policy or policyLabel level.

   Source: NetScaler > NetScaler 10 > Optimization > Compression > Setting Global Compression Parameters
   http://support.citrix.com/proddocs/topic/ns-optimization-10-map/ns-compression-setglobalparams-tsk.html
   FAQ: Compression on a NetScaler Appliance
   http://support.citrix.com/article/CTX113822

Section 8: Monitoring of network-related activities and performance using features like bandwidth monitoring, ECV (extended content verification) monitoring, etc.

8.1

Specific Task: Configure monitoring

Objective: When, how, and why to configure monitoring

6. Which two items can be configured with monitor options? (Choose two)

   a. Servers
   b. Services
   c. Virtual Servers
   d. Service Groups
   e. Persistency Groups

Answer: b.d.

Explanation: To manage a high-traffic load balancing setup, the NetScaler appliance needs to track the state of each load balanced server in near real time, so that it can divert traffic from any load balanced server that is not responding and send that traffic to a load balanced server that is responding. Therefore, a monitor is bound to each service. The monitor is configured to test the service by sending periodic probes to the service. (This is sometimes referred to as performing a health check.) If the monitor receives a timely response to its probes, it marks the service as UP. If it does not receive a timely response to the designated number of probes, it marks the service as DOWN.

Source: Citrix NetScaler Traffic Management Guide - Release 10, Page 228
http://support.citrix.com/article/CTX132359

Section 9: Troubleshooting issues on NetScaler

9.1

Specific Task: Troubleshoot Authentication, Authorization and Access (AAA) issues

Objective: How to troubleshoot authentication, authorization and access (AAA) issues

7. **Scenario:** A company uses NetScaler to deliver Citrix XenDesktop VDI to Internet users. The help desk received complaints from a few users that could not login to Citrix Access Gateway.

   Which step should an engineer take to troubleshoot the issue?

   a. cat aaad.debug
   b. show tech support
   c. configure monitoring
   d. enable Call Home feature

   Answer: a.

Explanation: The most efficient way to discover the reason why the user does not get the desired access is to use the aaa.debug command on the NetScaler, which shows the AAA login and the group extraction taking place.

Source: How to Troubleshoot AAA Group Access Issues in Access Gateway Enterprise Edition
http://support.citrix.com/article/CTX126589