

Citrix

Exam 1Y0-351

Citrix NetScaler 10.5 Essentials and Networking

Version: 7.0

[Total Questions: 178]

Question No : 1

A network engineer notes that a high availability pair (HA) is NOT synchronizing correctly and decides to open a ticket with Citrix Support.

When opening the new ticket with Citrix Support, the engineer should run show _____ and _____. (Choose the correct set of options to complete the sentence.)

- A. ha node; provide any public IP addresses listed
- B. ha node; provide the hello and dead interval data
- C. techsupport on the primary device; send the output to Citrix Support
- D. techsupport on both the primary and secondary devices; send the output to Citrix support

Answer: D

Question No : 2

Which three command-line interface commands should a NetScaler Engineer execute to configure an authentication virtual server? (Choose three.)

- A. add authentication vserver <name> ssl <ipaddress>
- B. bind ssl certkey
- C. set authentication vserver <name> -authenticationDomain
- D. show authentication vserver <name>
- E. add ssl certkey

Answer: A,B,C

Question No : 3

Scenario: A NetScaler Engineer wants to make it easier for the help desk group to access the active node in a high-availability pair. Members of the help desk group must be able to access the NetScaler in a secure way without being notified of warnings in their web browsers.

Which two of the listed steps must the engineer take to meet the requirements of the scenario? (Choose two.)

- A. Enable management access to the VIP.
- B. Enable management access to the SNIP.
- C. Bind a trusted certificate to the internal service.
- D. Bind the ns-server-certificate to the SNIP to the internal service.
- E. Create a self-signed certificate on the NetScaler and assign it to the internal service.

Answer: B,C

Question No : 4

Which built-in TCP profile should a NetScaler Engineer choose to optimize backend server connections, where the servers reside on the same LAN as the appliance?

- A. nstcp_default_tcp_lfp
- B. nstcp_default_tcp_lnp
- C. nstcp_default_tcp_lan
- D. nstcp_default_profile

Answer: C

Question No : 5

Scenario: An application that uses HTTP for connections and other protocols for different types of content has been deployed. Load balancing virtual servers have been created for each protocol and the engineer now needs to ensure that once a load balancing decision has occurred, further requests for different content are served from the same server.

How could the engineer achieve this?

- A. Create a persistency group.
- B. Set the Spillover method to DYNAMICCONNECTION.
- C. Add a new virtual server for each protocol that is not directly addressable.
- D. Set each virtual server to use Source IP Hash as the load balancing method.

Answer: A

Explanation:

Summary

A Web application may use HTTP and HTTPS in the same session. This article describes the configuration necessary to ensure persistence is maintained across both HTTP and

HTTPS connections.

Background

The NetScaler allows us to configure persistency groups to accommodate exactly such a need. A practical example of this might be a shopping cart where items are browsed over HTTP, but purchased over HTTPS. If persistency were not maintained, it's possible the shopping cart might be lost, the user logged out, or other adverse actions. By using persistency groups, the HTTP and HTTPS vServers are grouped together into one persistent entity.

Procedure

From the GUI:

1. Click and expand the Load Balancing node.
2. Click Persistency Groups.
3. Click Add.
4. Populate the Group Name field.
5. Choose between COOKIEINSERT, SOURCEIP or RULE from the Persistence dropdown and configure a timeout.
6. Choose a backup persistence method if desired.
7. Select the vServers to be grouped from the Available Virtual Servers list.
8. Click Add to move the vServers from the available list to the configured list.

From the command line interface (CLI):

Issue the following commands:

1. bind lb group <name of group> <vserver 1>
2. bind lb group <name of group> <vserver 2>
3.
4. set lb group <name of group> -persistenceType <persistence method> -persistenceBackup <backup persistence method>

Question No : 6

As a result of connecting two NetScaler interfaces in the same L2 broadcast domain/VLAN (unless link aggregation is configured), the NetScaler will _____. (Choose the correct option to complete the sentence.)

- A. restart
- B. disable one interface
- C. cause a network loop
- D. disable both interfaces

Answer: C

Question No : 7

On which two types of virtual servers is the SOURCEIP persistence type supported?
(Choose two.)

- A. HTTPS
- B. RTSP
- C. SSL_Bridge
- D. SIP_UDP

Answer: A,C

Question No : 8

Scenario: A network engineer would like to prevent blacklisted remote clients from accessing NetScaler hosted application services. An IP address blacklist database is maintained by an external company and available to query over the Internet.

The engineer would like to reject any connections from IP addresses that are contained in the blacklist.

What could the engineer configure to achieve this goal?

- A. SSL offload
- B. HTTP callout
- C. URL transformation
- D. SSL certification revocation list check

Answer: B

Question No : 9

Scenario: A company is hosting an external, Internet-facing website that is load balanced by a NetScaler. The backend servers are on a 1 Gbps network and clients connect over 3G

connections. The Server Administrator reviewed the performance metrics on the backend servers and noticed a lot of overall network retirements and retransmissions.

Which NetScaler feature would help improve the network performance of the backend servers in this scenario?

- A. SureConnect
- B. Compression
- C. TCP Buffering
- D. Surge Protection

Answer: C

Question No : 10

What is the default load-balancing method?

- A. Round Robin
- B. Source IP Hash
- C. Least Connection
- D. Least Response Time

Answer: C

Question No : 11

On a load-balancing virtual server with multiple bound services, Redirect URL will be invoked when _____. (Choose the correct phrase to complete the sentence.)

- A. a backup virtual server has been configured
- B. Health Based Spillover has been configured
- C. one of the bound services is marked as DOWN
- D. the load-balancing virtual server is marked as DOWN

Answer: D

Question No : 12

Scenario: A call center has deployed Access Gateway Enterprise to provide its employees with access to work resources from home. Due to the number of available licenses, only selected employees should access the environment remotely based on their user account information.

How could the engineer configure access to meet the needs of this scenario?

- A. Configure a Pre-authentication Policy.
- B. Configure an Authentication Server using a search filter.
- C. Configure an Authentication Policy using Client based expressions.
- D. Add the selected employee accounts to the Local Authentication policy.

Answer: B

Explanation:

<http://support.citrix.com/article/CTX111079>

When you type log in credentials on the log in page of the NetScaler VPN and press Enter, the credentials are sent to the Active Directory for validation. If the user name and password are valid, then the Active Directory sends the user attributes to the NetScaler appliance.

The memberOf attribute is one of the attributes that the Active Directory sends to the NetScaler appliance. This attribute contains the group name of which you are defined as a member in the Active Directory. If you are a member of more than one Active Directory group, then multiple memberOf attributes are sent to the NetScaler appliance.

The NetScaler appliance then parses this information to determine if the memberOf attribute matches the Search filter parameter set on the appliance. If attribute matches, then you are allowed to log in to the network.

The following are the sample attributes that the Active Directory can send to NetScaler appliance:

```
dn: CN=johnd,CN=Users,DC=citrix,DC=com
changetype: add
memberOf: CN=VPNAllowed,OU=support,DC=citrix,DC=com
cn: johnd
givenName: john
objectClass: user
sAMAccountName: johnd
```

Configuring a NetScaler Appliance to Extract the Active Directory Group

To configure a NetScaler appliance to extract the Active Directory group and enable clients to access the NetScaler VPN based on the Active Directory groups by using the Lightweight Directory Access Protocol (LDAP) authentication, complete the following procedure:

Determine the Active Directory Group that has access permission.

To configure the NetScaler appliance for Group Extraction, you must define the group a user needs to be a member of to allow access to the network resources.

Note: To determine that exact syntax, you might need to refer to the Troubleshooting Group Extraction on the NetScaler appliance section.

Determine the Search Filter syntax.

Enter the appropriate syntax in the Search Filter field of the Create Authentication Server dialog box, as shown in the following sample screenshot:

Create Authentication Server

Name* LDAP-Authentication

Authentication Type LDAP

Timeout (secs) 3 Authentication

LDAP specific details

Base DN CN=Users,DC=citrix,DC=com

Bind DN CN=administrator,CN=Users,DC=citrix,DC=com

Bind DN Password *****

Confirm Bind DN Password *****

Login Name sAMAccountName

Search Filter memberOf=CN=VPNAllowed,OU=support,DC=citrix,DC=com

Group Attribute Name memberOf

Sub Attribute Name CN

Security Type PLAINTEXT TLS SSL

Create Close Help

Note: Ensure that you start the value to the Search Filter field with memberOf= and do not have any embedded spaces in the value.

To configure the LDAP authentication with Group Extractions from the command line interface of the NetScaler appliance with the values similar to the ones in the preceding screenshot, run the following command:

```
add authentication ldapaction LDAP-Authentication
-serverip 10.3.4.15
-ldapBase "CN=Users,DC=citrix,DC=com"
-ldapBindDn "CN=administrator,CN=Users,DC=citrix,DC=com"
-ldapBindDnPassword ..dd2604527edf70
-ldapLoginName sAMAccountName
```



```
-searchFilter "memberOf=CN=VPNAllowed,OU=support,DC=citrix,DC=com"  
-groupAttrName memberOf  
-subAttributeName CN
```

Note: Ensure that you set the subAttributeName parameter to CN.

Troubleshooting Group Extraction on the NetScaler appliance

To troubleshoot group extraction on the NetScaler appliance, consider the following points:
If the LDAP policy fails after configuring it for Group Extraction, it is best to create a policy that does not have the group extraction configured to ensure that LDAP is configured appropriately.

You might need to use the LDAP Data Interchange Format Data Exchange (LDIFDE) utility from Microsoft that extracts the attributes from the Active Directory server to determine the exact content of the memberOf group.

You need to run this utility on the Active Directory server. The following is the syntax for the command to run the LDIFDE utility:

```
ldifde -f <File_Name> -s <AD_Server_Name> -d "dc=<Domain_Name>,dc=com" -p  
subtree -r "(&(objectCategory=person)(objectClass=User)(givenname=*))" -l  
"cn,givenName,objectclass,samAccountName,memberOf"
```

When you run the preceding command, a text file, with the name you specified for File_Name parameter, is created. This file contains all objects from the Active Directory.

The following is an example from a text file so created:

```
dn: CN=johnd,CN=Users,DC=citrix,DC=com  
changetype: add  
memberOf: CN=VPNAllowed,OU=support,DC=citrix,DC=com  
cn: johnd  
givenName: john  
objectClass: user  
sAMAccountName: johnd
```

Question No : 13

Which protocol is responsible for exchanging site metric, network metric, and persistence information between sites using Global Server Load Balancing (GSLB)?

- A. SSH
- B. MEP
- C. RPC
- D. NITRO

Answer: B

Question No : 14

Which troubleshooting tool will show policy hits and verify that a policy expression is being invoked?

- A. nspepi
- B. nsapimgr
- C. nstrace.sh
- D. nsconmsg

Answer: D

Question No : 15

Which two of the following settings could be configured using a TCP profile that is bound to a service? (Choose two.)

- A. TCP buffer size
- B. Window scaling
- C. TCP Server time-out values
- D. Source IP for specific subnet
- E. Allowed bandwidth throughput
- F. Number of max concurrent TCP connections

Answer: A,B

Question No : 16

A NetScaler Engineer created an HTTP service and did NOT bind any monitors to the service.

Which monitor will the NetScaler automatically bind to the HTTP service?

- A. tcp