



1Y0-351^{Q&As}

Citrix NetScaler 10.5 Essentials and Networking

Pass Citrix 1Y0-351 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/1y0-351.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Citrix
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

When a content-switching virtual server is used and idle client connections must stay established longer than the default NetScaler value, in which two locations could an engineer adjust the client timeout setting? (Choose two.)

- A. Global Timeout Settings
- B. Load-balancing services
- C. Load-balancing virtual server
- D. Content-switching virtual server

Correct Answer: AD

QUESTION 2

Scenario: A company has three HTTP servers that are load balanced using NetScaler. When users connect to the HTTP application they often receive inconsistent data or are advised that they need to log on again. Which step should the engineer take to correct this?

- A. Remove Down State Flush.
- B. Change the idle timeout value for the service.
- C. Configure persistence with appropriate timeouts.
- D. Change the global TCP Client Idle Time-Out value.

Correct Answer: C

QUESTION 3

Scenario: A NetScaler Engineer is troubleshooting a high-availability issue. The engineer needs to determine if the port being used by the high-availability heartbeats is blocked.

Which port is used by high-availability heartbeats?

- A.
- B.
- C.
- D.

Correct Answer: A

QUESTION 4



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.

Correct Answer: B

<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 -s -d "dc=,dc=com" -p subtree -r "(and  
(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 5

What is the purpose of the flash cache option in integrated caching?

- A. To completely wipe a cache group when the targeted selector is hit in the cache
- B. To use the flash memory for storage for a specific cache group to improve performance
- C. To queue simultaneous requests of an object and answer all with the same response from the server
- D. To answer the client request without checking if the object has expired, objects are checked periodically instead

Correct Answer: C

[Latest 1Y0-351 Dumps](#)

[1Y0-351 VCE Dumps](#)

[1Y0-351 Brindumps](#)