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.geekcert.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

A network engineer wants to hide the IP address of the outgoing packets by changing it to the IP of the

VIP.

Which feature should the administrator use?

A. ACL

B. PBR

C. RNAT

D. Rewrite

Correct Answer: C

QUESTION 2

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

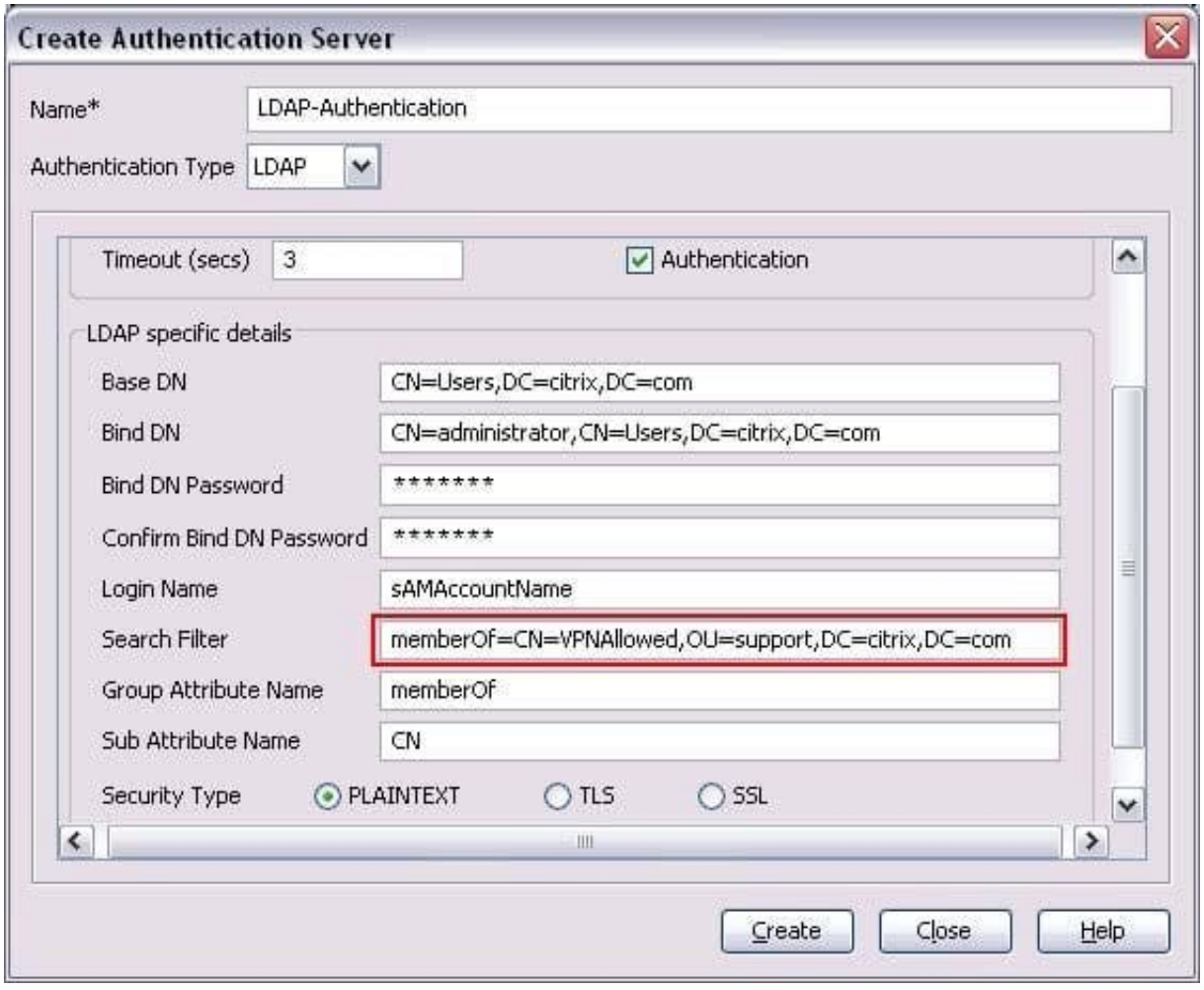
Configuring a NetScaler Appliance to Extract the Active Directory Group To configure a NetScaler appliance to extract the Active Directory group and enable clients to access the NetScaler VPN based on the Active Directory groups by using the Lightweight

Directory Access Protocol (LDAP) authentication, compete 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:



Note: Ensure that you start the value to the Search Filter filed 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 3

What is the key benefit to enabling Session Reuse on an SSL offload VServer?

A. The number of HTTP requests to the backend services are decreased.

B. Resumed SSL sessions are more secure than sessions that require renegotiation.

C. Reusing existing sessions decreases the number of TCP connections made to backend services.

D. A partial SSL handshake is sent over the existing SSL connection, reducing CPU and bandwidth usage.

Correct Answer: D

QUESTION 4

In which two places could a NetScaler Engineer enable TCP Buffering? (Choose two.)

A. Service

B. Globally

C. HTTP profile

D. Virtual server

Correct Answer: AB

QUESTION 5

A network engineer needs to configure load balancing for secured web traffic that does NOT terminate at the NetScaler device.

Which type of session persistence method can the engineer select for this scenario?

A. Source IP

B. Cookie Insert

C. URL Passive

D. SRCIPDESTIP

Correct Answer: A