



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.



1Y0-440 MCQs
1Y0-440 TestPrep
1Y0-440 Study Guide
1Y0-440 Practice Test
1Y0-440 Exam Questions



killexams.com

Citrix

1Y0-440

Architecting a Citrix Networking Solution (CCE-AppDS)

ORDER FULL VERSION

<https://killexams.com/pass4sure/exam-detail/1Y0-440>



Question: 99

_____ content type supports sending NITRO commands to NetScaler. (Choose the correct option to complete sentence.)

- A. Application/sgml
- B. Text/html
- C. Application/json
- D. Text/enriched

Answer: B

Question: 100

Scenario: A Citrix Architect needs to assess a NetScaler Gateway deployment that was recently completed by a customer and is currently in pre-production testing. The NetScaler Gateway needs to use ICA proxy to provide access to a XenApp and XenDesktop environment. During the assessment, the customer informs the architect that users are NOT able to launch published resources using the Gateway virtual server.

Click the Exhibit button to view the troubleshooting details collected by the customer.

Issue Details
• External users trying to launch a Shared Hosted Desktop via a NetScaler gateway connection receive an ICA file from StoreFront. • However, they are unable to launch the Shared Hosted Desktop. • The following ports are open on the firewall between the NetScaler gateway and the internal network where the Virtual Delivery Agent machines are located: Bidirectional: TCP 80, TCP 443, TCP 2598, TCP 1494 • Users located on the internal network who connect directly to the StoreFront server are able to launch the Shared Hosted Desktop.

What is the cause of this issue?

- A. The required ports have NOT been opened on the firewall between the NetScaler gateway and the Virtual Delivery Agent (VDA) machines.
- B. The StoreFront URL configured in the NetScaler gateway session profile is incorrect.
- C. The Citrix License Server is NOT reachable.
- D. The Secure Ticket Authority (STA) servers are load balanced on the NetScaler.

Answer: D

Question: 101

Scenario: A Citrix Architect needs to deploy SAML integration between NetScaler (Identity Provider) and ShareFile (Service Provider).

The design requirements for SAML setup are as follows:

- NetScaler must be deployed as the Identity Provider (IDP).

- ShareFile server must be deployed as the SAML Service Provider (SP).
- The users in domain workspacelab.com must be able to perform Single Sign-on to ShareFile after authenticating at the NetScaler.
- The User ID must be UserPrincipalName.
- The User ID and Password must be evaluated by NetScaler against the Active Directory servers SFOADS-001 and SFO-ADS-002.
- After successful authentication, NetScaler creates a SAML Assertion and passes it back to ShareFile.
- Single Sign-on must be performed.
- SHA 1 algorithm must be utilized.

The verification environment details are as follows:

- Domain Name: workspacelab.com
- NetScaler AAA virtual server URL https://auth.workspacelab.com
- ShareFile URL https://sharefile.workspacelab.com

Which SAML IDP action will meet the design requirements?

- A. add authentication samIdPProfile SAMI-IDP CsamISPCertName Cert_1 CsamIdPCertName Cert_2 C assertionConsimerServiceURL “https://auth.workspacelab.com/samIIssueName auth.workspacelab.com -signatureAlg RSA-SHA256-digestMethod SHA256-encryptAssertion ON serviceProviderUD sharefile.workspacelad.com
- B. add authentication samIdPProfile SAMI-IDP CsamISPCertName Cert_1 CsamIdPCertName Cert_2 C assertionConsimerServiceURL https://sharefile.workspacelab.com/saml/acs” CsamIIssuerName sharefile.workspacelab.com CsignatureAlg RSA-SHA256 CdigestMethod SHA256 CserviceProviderID sharefile.workspacelab.com
- C. add authentication samIdPProfile SAMI-IDP CsamISPCertName Cert_1 CsamIdPCertName Cert_2 C assertionConsimerServiceURL https://sharefile.workspacelab.com/saml/acs” CsamIIssuerName auth.workspacelab.com CsignatureAlg RSA-SHA1-digestMethod SHA1 CencryptAssertion ON C serviceProviderID sharefile.workspacelab.com
- D. add authentication samIdPProfile SAMI-IDP CsamISPCertName Cert_1 CsamIdPCertName Cert_2 C assertionConsimerServiceURL https://sharefile.workspacelab.com/saml/acs” CsamIIssuerName sharefile.workspacelab.com CsignatureAlg RSA-SHA1 CdigestMethod SHA1 CencryptAssertion ON C serviceProviderID sharefile.workspacelab.com

Answer: C

Question: 102

13 nc. These are placed behind a Cisco ASA 5505 Firewall is configured to block traffic using access control lists. The network address translation (NAT) is also performed on the firewall.

The following requirements were captured by the architect during the discussion held as part of the NetScaler security implementation project with the customer’s security team:

The NetScaler device:

- Should monitor the rate of traffic either on a specific virtual entity or on the device. It should be able to mitigate the attacks from a hostile client sending a flood of requests. The NetScaler device should be able to stop the HTTP, TCP, and DNS based requests.
- Needs to protect backend servers from overloading.
- Needs to queue all the incoming requests on the virtual server level instead of the service level.
- Should provide access to resources on the basis of priority.
- Should provide protection against well-known Windows exploits, virus-infected personal computers, centrally managed automated botnets, compromised web servers, known spammers/hackers, and phishing proxies.
- Should provide flexibility to enforce the desired level of security check inspections for the requests originating from a specific geolocation database.
- Should block the traffic based on a pre-determined header length, URL length, and cookie length. The device should ensure that characters such as a single straight quote (*); backslash(), and semicolon (;) are either blocked, transformed, or dropped while being sent to the backend server.

Which two security features should the architect configure to meet these requirements? (Choose two.)

- A. Pattern sets
- B. Rate limiting
- C. HTTP DDOS
- D. Data sets
- E. APPQOE

Answer: BE

Explanation:

Reference: <https://docs.citrix.com/en-us/citrix-adc/12-1/appexpert/appqoe.html> <https://docs.citrix.com/en-us/citrix-adc/12-1/appexpert/rate-limiting.html>

Question: 103

Scenario: A Citrix Architect needs to assess an existing NetScaler Gateway deployment. During the assessment, the architect collected key requirements for VPN users, as well as the current session profile settings that are applied to those users.

Click the Exhibit button to view the information collected by the architect.

Requirements			
• Users should use the NetScaler Gateway plugin to authenticate and connect to internal resources, including intranet web pages and StoreFront. • After authenticating users should be directed to the organization's intranet portal. • Once connected, outbound traffic from the client device should only pass through the NetScaler Gateway if it is directed toward an intranet resource.			
Configurations			
Name	Type	Setting	Configuration
Item 1	Network Configuration	Home Page	home.workspacelabs.net
Item 2	Client Experience	Split Tunnel	ON
Item 3	Client Experience	Clientless Access	ON
Item 4	Client Experience	Client Choices	Not enabled
Item 5	Published Applications	ICA Proxy	OFF

Which configurations should the architect change to meet all the stated requirements?

A. Item 4
B. Item 3
C. Item 5
D. Item 2
E. Item 1

Answer: E

Question: 104

Scenario: A Citrix Architect needs to assess an existing on-premises NetScaler deployment which includes Advanced Endpoint Analysis scans. During a previous security audit, the team discovered that certain endpoint devices were able to perform unauthorized actions despite NOT meeting pre-established criteria.

The issue was isolated to several endpoint analysis (EPA) scan settings.

Click the Exhibit button to view the endpoint security requirements and configured EPA policy settings.

Requirements

- Endpoints should be scanned to determine whether they are connecting from within the company intranet (192.168.10.0/24) and belong to the company Windows domain (workspacelab.com).
 - Endpoints meeting both of these criteria are permitted to continue to the authentication page.
 - Endpoints NOT meeting 1 or more of these criteria should NOT be permitted to authenticate.
- All endpoints should also be scanned to confirm that an approved antiVirus client ("Antivirus") is running.
 - Endpoints that have an antivirus client running can access intranet resources.
 - Endpoints that do NOT have an antivirus client running should be added to quarantine group that can only access the XenApp and XenDesktop environment.

Configurations

Name	Type	Bind Point	Action	Priority	Associated Policy Expressions
Item 1	Preauthentication setting	Global-NetScaler Gateway	Allow	N/A	ns_true
Item 2	Preauthentication policy	NetScaler Gateway VPN virtual server	N/A	10	REQ_IPSOURCEIP == 192.168.10.0 -netmask 255.255.255.0 && CLIENT.SYSTEM (DOMAIN_SUFFIX_ anyof_workspacelab EXISTS
Item 3	Preauthentication profile	Item 2	Allow	N/A	N/A
Item 4	Session policy	NetScaler Gateway VPN virtual server	N/A	20	ns_true
Item 5	Session profile	Item 4	Security: - Default Authorization Action: DENY Security-Advanced Settings: - Client Security Check String: CLIENT.APPLICATION.PROCESS (antivirus.exe) EXISTS - Quarantine Group: quarantine Published Applications: - ICA Proxy: OFF	N/A	N/A
Item 6	Session policy	AAA Group: quarantine	N/A	30	ns_true
Item 7	Session profile	Item 6	Security: - Default Authorization Action: DENY Published Applications: - ICA Proxy: On	N/A	N/A

Which setting is preventing the security requirements of the organization from being met?

A. Item 6

- B. Item 7
- C. Item 1
- D. Item 3
- E. Item 5
- F. Item 2
- G. Item 4

Answer: F

Question: 105

Scenario: A Citrix Architect holds a design discussion with a team of Workspacelab members, and they capture the following requirements for the NetScaler design project.

A pair of NetScaler MPX appliances will be deployed in the DMZ network and another pair in the internal network.

High availability will be accessible between the pair of NetScaler MPX appliances in the DMZ network.

- Multi-factor authentication must be configured for the NetScaler Gateway virtual server.
- The NetScaler Gateway virtual server is integrated with the StoreFront server.
- Load balancing must be deployed for users from the workspacelab.com domain.
- The workspacelab users should be authenticated using Cert Policy and LDAP.
- All the client certificates must be SHA 256-signed, 2048 bits, and have UserPrincipalName as the subject.
- Single Sign-on must be performed between StoreFront and NetScaler Gateway.

After deployment, the architect observes that LDAP authentication is failing.

Click the Exhibit button to review the output of aaad debug and the configuration of the authentication policy.

Exhibit 1

```

Sun Feb 25 11:41:30 2018
/home/ build/rs_120_53_3_RTM/usr.src/netcaler/aaad/ldap_common.
c[398]: ns_ldap_check_result 0-399: checking LDAP result. Expecting
101 (LDAP_RES_SEARCH_RESULT)
Sun Feb 25 11:41:30 2018
/home/ build/rs_120_53_3_RTM/usr.src/netcaler/aaad/ldap_common.
c[436]: ns_ldap_check_result 0-399: ldap_result found expected result
LDAP_RES_SEARCH_RESULT
Sun Feb 25 11:41:30 2018
/home/ build/rs_120_53_3_RTM/usr.src/netcaler/aaad/ldap_drv.
c[357]: receive_ldap_user_search_event 0-399: received LDAP_OK
Sun Feb 25 11:41:30 2018
/home/ build/rs_120_53_3_RTM/usr.src/netcaler/aaad/naaad.c[4196]:
unregister_timer 0-399: releasing timer 175
Sun Feb 25 11:41:30 2018
/home/ build/rs_120_53_3_RTM/usr.src/netcaler/aaad/ldap_drv.c[387]:
receive_ldap_user_search_event 0-399: Binding user... 0 entries
Sun Feb 25 11:41:30 2018
/home/ build/rs_120_53_3_RTM/usr.src/netcaler/aaad/ldap_drv.c[388]:
receive_ldap_user_search_event 0-399: Admin authentication (Bind)
succeeded, now attempting to search the user hrl@workspacelab.com
Sun Feb 25 11:41:30 2018
/home/ build/rs_120_53_3_RTM/usr.src/netcaler/aaad/ldap_drv.c[393]:
receive_ldap_user_search_event 0-399: ldap_first_entry returned null,
user hrl@workspacelab.com not found
Sun Feb 25 11:41:30 2018
/home/ build/rs_120_53_3_RTM/usr.src/netcaler/aaad/naaad.c[3322]:
send_reject_with_code 0-399: Not trying cascade again
Sun Feb 25 11:41:30 2018
/home/ build/rs_120_53_3_RTM/usr.src/netcaler/aaad/naaad.c[3324]:
send_reject_with_code 0-399: sending reject to kernel for :
hrl@workspacelab.com
Sun Feb 25 11:41:30 2018
/home/ build/rs_120_53_3_RTM/usr.src/netcaler/aaad/naaad.c[3327]:
send_reject_with_code 0-399: Rejecting with error code 4009

```

Exhibit 2

```

add authentication ldapAction ldap-sam -serverName 192.168.10.11 -
serverPort 636 -ldapBase "DC=workspacelab, DC=com" -ldapBindDN
administrator@workspacelab.com -ldapBindDnPassword
54e394e320d69a5b3418746e4dc9e83ebf0a1c7ffd869abd3e040b42d38e4b2e -
encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -
groupAttrName memberOf -subAttributeName cn -secType SSL -
ssoNameAttribute cn
add authentication ldapPolicy ldap-samaccount ns_true ldap-sam
add authentication certAction cert-upn -twoFactor ON -userNameField
Subject:CN
add authentication certPolicy cert ns_true cert-upn

```

What is causing this issue?

A. Usernamefield is set as subsection

- B. Password used is incorrect
- C. User does NOT exist in database
- D. IdapLoginName is set as sAMAccountName

Answer: A

Question: 106

Scenario: A Citrix Architect has met with a team of Workspacelab members for a design discussion.

They have captured the following requirements for NetScaler design project:

- The authentication must be deployed for the users from the workspacelab.com and vendorlab.com domains.
- The workspacelab users connecting from the internal (workspacelab) network should be authenticated using LDAP.
- The workspacelab users connecting from the external network should be authenticated using LDAP and RADIUS.
- The vendorlab users should be authenticated using Active Directory Federation Service.
- The user credentials must NOT be shared between workspacelab and vendorlab.
- Single Sign-on must be performed between StoreFront and NetScaler Gateway.
- A domain drop down list must be provided if the user connects to the NetScaler gateway virtual server externally.

Which method must the architect utilize for user management between the two domains?

- A. Create shadow accounts for the users of the Workspacelab domain in the Vendorlab domain.
- B. Create a global catalog containing the objects of Vendorlab and Workspacelab domains.
- C. Create shadow accounts for the Vendorlab domain in the Workspacelab domain.
- D. Create a two-way trust between the Vendorlab and Workspacelab domains.

Answer: B

Question: 107

A Citrix Architect has deployed NetScaler Management and Analytics System (NMAS) to monitor a high availability pair of NetScaler VPX devices.

The architect needs to deploy automated configuration backup to meet the following requirements:

- The configuration backup file must be protected using a password.
- The configuration backup must be performed each day at 8:00 AM GMT.
- The configuration backup must also be performed if any changes are made in the ns.conf file.
- Once the transfer is successful, auto-delete the configuration file from the NMAS.

Which SNMP trap will trigger the configuration file backup?

- A. netScalerConfigSave
- B. sysTotSaveConfigs
- C. netScalerConfigChange
- D. sysconfigSave

Answer: A

Explanation:

Reference: <https://docs.citrix.com/en-us/netscaler-mas/12/instance-management/how-to-backup-andrestore-using-mas.html#configuring-instance-backup-settings>

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.