

1Y0-440

Number: 1Y0-440
Passing Score: 800
Time Limit: 120 min



Website: <https://vceplus.com> - <https://vceplus.co>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

Exam A

QUESTION 1

Scenario: A Citrix Architect needs to plan for a customer environment in which more than 10,000 users will need access. The networking infrastructure needs to be able to handle the expected usage.



<https://vceplus.com/>

Which business driver should be prioritized based on the customer's requirement?

- A. Increase flexibility
- B. Enable mobile work styles
- C. Simplify management
- D. Increase Scalability
- E. Reduce Costs
- F. Increase Security



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

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 SFO-ADS-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 samlIdPProfile SAMI-IDP –samlSPCertName Cert_1 –samlIdPCertName Cert_2 –assertionConsumerServiceURL “https://auth.workspacelab.com/samlIssueName auth.workspacelab.com -signatureAlg RSA-SHA256-digestMethod SHA256-encryptAssertion ON -serviceProviderUD sharefile.workspacelad.com
- B. add authentication samlIdPProfile SAMI-IDP –samlSPCertName Cert_1 –samlIdPCertName Cert_2 –assertionConsumerServiceURL https://sharefile.workspacelab.com/saml/acs” –samlIssuerName sharefile.workspacelab.com –signatureAlg RSA-SHA256 –digestMethod SHA256 –serviceProviderID sharefile.workspacelab.com
- C. add authentication samlIdPProfile SAMI-IDP –samlSPCertName Cert_1 –samlIdPCertName Cert_2 –assertionConsumerServiceURL https://sharefile.workspacelab.com/saml/acs” –samlIssuerName auth.workspacelab.com –signatureAlg RSA-SHA1-digestMethod SHA1 –encryptAssertion ON –serviceProviderID sharefile.workspacelab.com
- D. add authentication samlIdPProfile SAMI-IDP –samlSPCertName Cert_1 –samlIdPCertName Cert_2 –assertionConsumerServiceURL https://sharefile.workspacelab.com/saml/acs” –samlIssuerName sharefile.workspacelab.com –signatureAlg RSA-SHA1 –digestMethod SHA1 –encryptAssertion ON –serviceProviderID sharefile.workspacelab.com

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Scenario: A Citrix Architect has configured NetScaler Gateway integration with a XenApp environment to provide access to users from two domains: vendorlab.com and workslab.com. The Authentication method used is LDAP.

Which two steps are required to achieve Single Sign-on StoreFront using a single store? (Choose two.)

- A. Configure Single sign-on domain in Session profile 'userPrincipalName'.
- B. Do NOT configure SSO Name attribute in LDAP Profile.
- C. Do NOT configure sign-on domain in Session Profile.
- D. Configure SSO Name attribute to 'userPrincipalName' in LDAP Profile.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.citrix.com/en-us/storefront/3-12/plan/user-authentication.html>

QUESTION 4

Scenario: A Citrix Architect has implemented two high availability pairs of MPX 5500 and MPX 11500 devices respectively with 12.0.53.13 nc version. The NetScaler devices are set up to handle NetScaler Gateway, Load Balancing, Application Firewall, and Content Switching. The Workspacelab infrastructure is set up to be monitored with NMAS version 12.0.53.13 nc by the Workspacelab administrators. The Workspacelab team wants to implement one more pair of NetScaler MPX 7500 devices with version 12.0.53.13 nc.

The Citrix consulting team has assigned the task to implement these NetScaler devices in the infrastructure and set them up to be monitored and managed by NMAS.

The following are the requirements that were discussed during the project initiation call:

- NMAS should be configured to get the infrastructure information under sections such as HDX Insight, WEB Insight, and Security Insight.
 - Configuration on the new MPX devices should be identical to MPX 11500 devices.
 - Configuration changes after the deployment and initial setup should be optimized using NMAS.
 - NMAS should be utilized to configure templates that can be utilized by the Workspacelab team in future deployment. ▪
- As per the requirement from the Workspacelab team, NMAS should be store the audited data for only 15 days.

Which process should the architect utilize to ensure that the deployment of MPX 11500 devices are optimized and that it is correct, before deploying the devices in production?

- A. Under Stylebooks; Inbuilt and composite stylebook templates should be utilized prior to deployment.
- B. Under Stylebooks; Public and composite stylebook templates should be utilized prior to deployment.
- C. Under Configuration Management; Configuration Audit and Advice should be used prior to deployment.
- D. Under Configuration jobs; Configuration Audit and Advice should be used prior to deployment.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

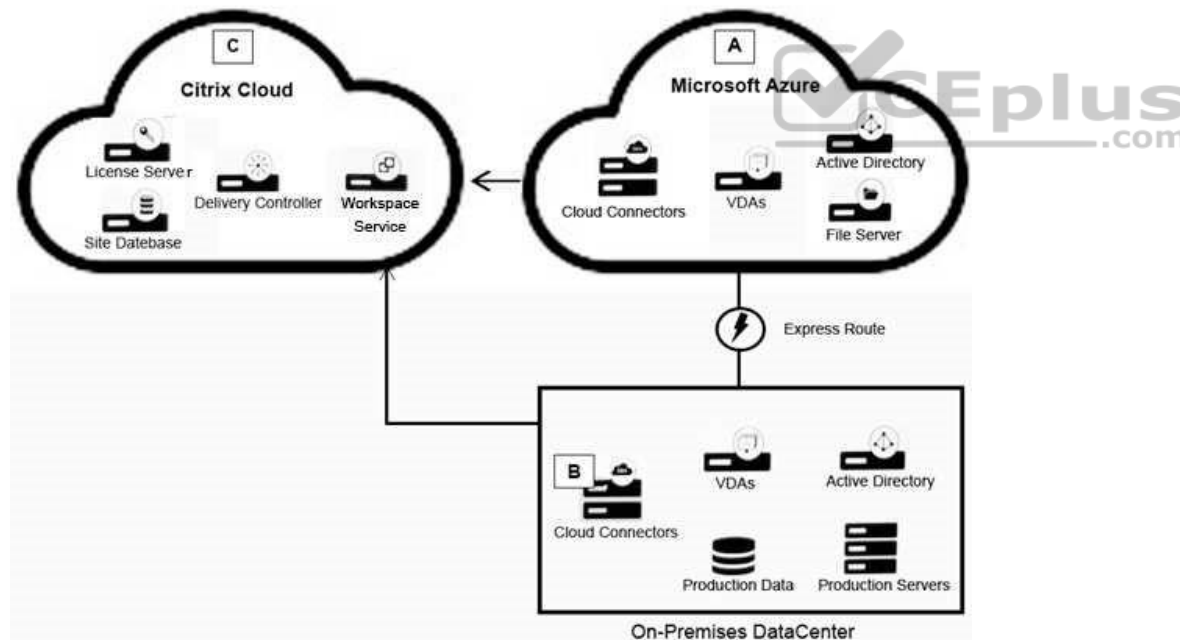
QUESTION 5

Scenario: A Citrix Architect needs to design a hybrid XenApp and XenApp and XenDesktop environment which will include Citrix Cloud as well as resource locations in on-premises datacenter and Microsoft Azure.

Organizational details and requirements are as follows:

- Active XenApp and XenDesktop Service subscription
- No existing NetScaler deployment
- About 3,000 remote users are expected to regularly access the environment
- Multi-factor authentication should be used for all external connections
- Solution must provide load balancing for backend application servers
- Load-balancing services must be in Location B

Click the Exhibit button to view the conceptual environment architecture.



The architect should use _____ in Location A, and should use _____ in Location B. (Choose the correct option to complete the sentence.)

- A. NetScaler Gateway as a Service, no NetScaler products
- B. No NetScaler products, NetScaler ADC (BYO)
- C. NetScaler Gateway as a Service, NetScaler ADC (BYO)
- D. No NetScaler products, NetScaler ICA Proxy (cloud-licensed)
- E. NetScaler Gateway as a Service, NetScaler ICA Proxy (cloud-licensed)
- F. No NetScaler products; NetScaler Gateway appliance

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

A Citrix Architect needs to make sure that maximum concurrent AAA user sessions are limited to 4000 as a security restriction.

Which authentication setting can the architect utilize to view the current configuration?

- A. Global Session Settings
- B. AAA Parameters
- C. Active User Session
- D. AAA Virtual Server

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.carlstalhood.com/category/netscaler/netscaler-11-1/netscaler-gateway-11-1/>

QUESTION 7

Which encoding type can a Citrix Architect use to encode the StyleBook content, when importing the StyleBook configuration under source attribute?

- A. Hex
- B. base64
- C. URL
- D. Unicode

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.citrix.com/en-us/netScaler-mas/12/stylebooks/how-to-use-api-to-create-configuration-from-stylebooks/import-custom-stylebooks.html>

QUESTION 8

Which parameter must a Citrix Architect configure to ensure that HDX Proxy Connection terminates upon AAA Session TimeOut?

- A. ICA session timeout in VPN parameters
- B. Session timeout(mins) in NetScaler gateway Session Profile.
- C. Session timeout(mins) in VPN Parameters
- D. ICA session timeout in netScaler Gateway Session Profile.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: https://www.citrix.com/content/dam/citrix/en_us/citrix-developer/documents/NetScaler/how-do-i-ica-session-timeout-with-aaa.pdf

QUESTION 9

Scenario: A Citrix Architect needs to design a new multi-datacenter NetScaler deployment. The customer wants NetScaler to provide access to various backend resources by using Global Server Load Balancing (GSLB) in an Active-Active deployment.

Click the Exhibit button to view additional requirements identified by the architect.

GSLB Requirements
<ul style="list-style-type: none">• Users should be directed to the nearest available datacenter when they initiate a connection to a backend resource.• The nearest datacenter should be determined by the least Time to First Byte (TTFB) among all the available services, as evidenced by response code 200.• Services with fewer active connections should also be prioritized.

Which GSLB algorithm or method should the architect use for the deployment, based on the stated requirements?

- A. Dynamic round trip time (RTT)
- B. Least response time
- C. Static proximity

- D. least connection
- E. Least packets
- F. Source IP hash

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.citrix.com/en-us/netScaler/12/global-server-load-balancing/methods/configuring-algorithm-based-methods.html>

QUESTION 10

Scenario: A Citrix Architect needs to deploy a load balancing for an application server on the NetScaler. The authentication must be performed on the NetScaler. After the authentication, the Single Sign-on with the application servers must be performed using Kerberos impersonation.

Which three authentication methods can the Architect utilize to gather the credentials from the user in this scenario? (Choose three.)

- A. SAML
- B. OTP
- C. TACACS
- D. WEBAUTH
- E. LDAP



Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

Which three methods can a Citrix Architect use to assess the capabilities of a network infrastructure? (Choose three.)

- A. Review existing monitoring solutions for periods of latency, lost packets, and insufficient bandwidth.
- B. Map the location of the users against the existing network topology.
- C. Alter firewall rules of existing network to fit into the new NetScaler Deployment.
- D. Examine the topology for single points of failure and potential bottlenecks.
- E. Ensure that users and computers are in the correct organizational units (OUs).

Correct Answer: ABD

Section: (none)

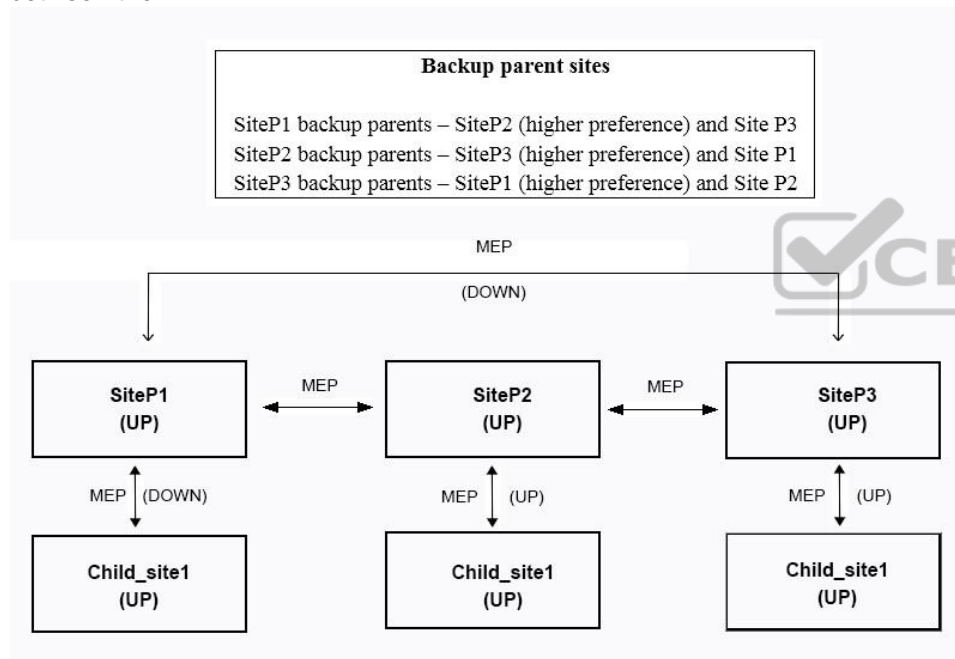
Explanation

Explanation/Reference:

QUESTION 12

Scenario: A Citrix Architect needs to assess an existing NetScaler multi-site deployment. The deployment is using Global Server Load Balancing (GSLB) configured in a parent-child configuration.

Click the Exhibit button to view the diagram of the current GSLB configuration and parent-child relationships, as well as the status of the sites and the connectivity between them.



Based on the displayed configuration and status, Chil_site1 _____ a connection from _____. (Choose the correct option to complete the sentence.)

- A. rejects; SiteP2 and SiteP3; remains a child site of SiteP1
- B. rejects; SiteP3; remains a child site of SiteP1
- C. accepts; SiteP3; becomes its child site

- D. accepts; SiteP2; becomes its child site
- E. does NOT receive; SiteP2 and SiteP3; remains a child site of SiteP1
- F. rejects; SiteP2; remains a child site of SiteP1

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

Scenario: A Citrix Architect and a team of Workspacelab members have met for a design discussion about the NetScaler Design Project. They captured the following requirements:

- Two pairs of NetScaler MPX appliances will be deployed in the DMZ network and 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 XenApp/XenDesktop environment.
- Load balancing must be deployed for the users from the workspacelab.com and vendorlab.com domains.
- The logon page must show the workspacelab logo.
- Certificate verification must be performed to identify and extract the username.
- The client certificate must have UserPrincipalName as a subject.
- All the managed workstations for the workspace users must have a client identifications certificate installed on it.
- The workspacelab users connecting from a managed workstation with a client certificate on it should be authenticated using LDAP.
- The workspacelab users connecting from a workstation without a client certificate 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.
- The domain of the user connecting externally must be identified using the domain selected from the domain drop down list.

On performing the deployment, the architect observes that users are always prompted with two-factor authentication when trying to access externally from an unmanaged workstation.

Click the exhibit button to view the configuration.

```
> show authentication vserver aaa_dmz_001
aaa_dmz_001 (192.168.30.131:443) - SSL Type: CONTENT
State: UP
Client Idle Timeout: 180 sec
Down state flush: DISABLED
Disable Primary Vserver On Down : DISABLED
Network profile name: ???
Appflow logging: ENABLED
Authentication : ON
Device Certificate Check: ???
Device Certificate CA List: ???
CGInfra Homepage Redirect : ???
Current AAA Sessions: 0
Total Connected Users: 0
Dtls : ???      L2Conn: ???
RDP Server Profile Name: ???
Max Login Attempts: 0      Failed Login Timeout 0
Fully qualified domain name: ???
PCoIP VServer Profile name: ???
Listen Policy: NONE
Listen Priority: 0
IcmpResponse: ???
RHlstate: ???
Traffic Domain: 0

1)  LoginSchema Policy Name: LDAP_RADIUS      Priority: 100
    GotoPriority Expression: END

1)  Advanced Authentication Policy Name: cert-upn  Priority: 100
    GotoPriority Expression: NEXT
    NextFactor name: OnlyLDAP

2)  Advanced Authentication Policy Name: No_AUTH  Priority: 110
    GotoPriority Expression: NEXT
    NextFactor name: ldap-radius

3)  Advanced Authentication Policy Name: saml-upn  Priority: 120
    GotoPriority Expressions: NEXT

Done
```

What should the architect do to correct this configuration?

- A. Unbind LoginSchema Policy LDAP_RADIUS from the virtual server.
- B. Bind the Portal theme as Domaindropdown.
- C. Bind the LoginSchema Policy Domaindropdown to priority 90.
- D. Bind the Default LoginSchema Policy as Domaindropdown.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

A Citrix Architect needs to configure advanced features of NetScaler by using StyleBooks as a resource in the Heat service.

What is the correct sequence of tasks to be completed for configuring NetScaler using the Heat stack?

- A. 1. Install NetScaler Bundle for OpenStack
2. Deploy the Heat stack
3. Register OpenStack with NMAS
4. Add NetScaler instances (Optional)
5. Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource
6. Create service packages (Add OpenStack tenants)
- B. 1. Install NetScaler Bundle for OpenStack
2. Register OpenStack with NMAS
3. Add NetScaler instances (Optional)
4. Create service packages (Add OpenStack tenants)
5. Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource
6. Deploy the Heat stack
- C. 1. Install NetScaler Bundle for OpenStack
2. Add NetScaler instances (Optional)
3. Create service packages (Add OpenStack tenants)
4. Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource
5. Register OpenStack with NMAS
6. Deploy the Heat stack
- D. 1. Install NetScaler Bundle for OpenStack

2. Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource
3. Register OpenStack with NMAS
4. Deploy the Heat stack
5. Add NetScaler instances (Optional)
6. Create service packages (Add OpenStack tenants)

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: https://docs.citrix.com/en-us/netScaler-mas/12/integrating-netScaler-mas-with-openstack-platform/integrating_netScaler_mas_with_openstack_heat_services.html

QUESTION 15

Scenario: A Citrix Architect needs to design a new NetScaler Gateway deployment to provide secure RDP access to backend Windows machines.

Click the Exhibit button to view additional requirements collected by the architect during the design discussions.

Topic	Requirements
User experience	Once the user authenticates, they should be directed to a custom home page with the available RDP bookmarks. When a bookmark is clicked, an RDP connection to the backend machine will be established.
Additional considerations	Ensure that users can receive the most optimal RDP connection to backend machines located in different locations.

To meet the customer requirements, the architect should deploy the RDP proxy through _____ using a _____ solution. (Choose the correct option to complete the sentence.)

- A. CVPN: single gateway
- B. CVPN, stateless gateway
- C. ICAPProxy: single gateway
- D. ICAPProxy; stateless gateway

Correct Answer: C

Section: (none)

Explanation**Explanation/Reference:****QUESTION 16**

Scenario: More than 10,000 users will access a customer's environment. The current networking infrastructure is capable of supporting the entire workforce of users. However, the number of support staff is limited, and management needs to ensure that they are capable of supporting the full user base.

Which business driver is prioritized, based on the customer's requirements?

- A. Simplify Management
- B. Increase Scalability
- C. Increase Flexibility
- D. Reduce Costs
- E. Enable Mobile Work Styles
- F. Increase Security

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 17**

Which session parameter does the default authorization setting control when authentication, authorization, and auditing profiles are configured?

- A. Determines the default logging level
- B. Determines whether the NetScaler appliance will allow or deny access to content for which there is no specific authorization policy
- C. Determines the default period after which the user is automatically disconnected and must authenticate again to access the intranet
- D. Determines whether the NetScaler appliance will log users onto all web applications automatically after they authenticate or will pass users to the web application login page to authenticate for each application.
- E. Controls amount of time the users can be idle before they are automatically disconnected.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**QUESTION 18**

Scenario: A Citrix Architect has deployed two MPX devices, 12.0.53.13 nc and MPX 11500 models, in high availability (HA) pair for the Workspace labs team. The deployment method is two-arm and the devices are installed behind a CISCO ASA 5585 Firewall. The architect enabled the following features on the NetScaler devices. Content Switching, SSL Offloading, Load Balancing, NetScaler Gateway, Application Firewall in hybrid security and Appflow. All are enabled to send monitoring information to NMAAS 12.0.53.13 nc build. The architect is preparing to configure load balancing for Microsoft Exchange 2016 server.

The following requirements were discussed during the implementation:

- All traffic needs to be segregated based on applications, and the fewest number of IP addresses should be utilized during the configuration ▪
- All traffic should be secured and any traffic coming into HTTP should be redirected to HTTPS.
- Single Sign-on should be created for Microsoft Outlook web access (OWA).
- NetScaler should recognize Uniform Resource Identifier (URI) and close the session to NetScaler when users hit the Logoff button in Microsoft Outlook web access.
- Users should be able to authenticate using either user principal name (UPN) or sAMAccountName.
- The Layer 7 monitor should be configured to monitor the Microsoft Outlook web access servers and the monitor probes must be sent on SSL Which

monitor will meet these requirements?

- A. add lb monitor mon_rpc HTTP-ECV –send “GET /rpc/healthcheck.htm” recv 200 –LRTM DISABLED
- B. add lb monitor mon_rpc HTTP-ECV –send “GET /rpc/healthcheck.htm” recv 200 –LRTM ENABLED
- C. add lb monitor mon_rpc HTTP –send “GET /rpc/healthcheck.htm” recv 200 –LRTM DISABLED –secure YES
- D. add lb monitor mon_rpc HTTP-ECV –send “GET/rpc/healthcheck.htm” recv 200 –LRTM DISABLED –secure YES

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

Which two NetScaler cookies indicate the validity of the Authentication, Authorization and Accounting (AAA) session for users? (Choose two.)

- A. NSC_WT
- B. NSC_TMAS
- C. NSC_AAAC
- D. NSC_TMAA

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://support.citrix.com/article/CTX202900>

QUESTION 20

Scenario: A Citrix Architect needs to assess an existing NetScaler configuration. The customer recently found that members of certain administrator groups were receiving permissions on the production NetScaler appliances that do NOT align with the designed security requirements.

Click the Exhibit button to view the configured command policies for the production NetScaler deployment.



Requirements

- The "NetScalerAdmins" group should have full access except shell and user configs.
- The "Level2Support" group should have read-only access, except for enable/disable servers/services.
- The "NetScalerArchitect" user, which is part of the "NetScalerAdmins" group, should have full access.
- the "Level2Manager" user, which is part of the "Level2Support" group, should have full access except set/unset SSL and configurations.

Configurations

Name	Type	Bind Point	Action	Commands Spec	Priority
Item 1	Command Policy	"NetScaler Admins" group	ALLOW	^(?!shell)(?!sftp)(?!scp)(?!batch)(?!source)(?!.*superuser)(?!.*nsroot)(?!show\s+system\s+(user cmdPolicy))(?!(set add rm create export kill)\s+system)(?!unbind bind)\s+system\s+(user group)) (?!diff\s+ns\s+ns\s+config)(?!S\s+ns\s+partition).*	1
Item 2	Command Policy	"NetScaler" group	DENY	.*	2
Item 3	Command Policy	"Level2Support" group	ALLOW	(^main.*)((^show\s+(?!system)(?!configstatus)(?!nsns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gsibrunningConfig)(?!audit messages)(?!techsupport).*) (^stat.*) (^enable disable)(server service).*)	1
Item 4	Command Policy	"Level2Support" group	DENY	.*	2
Item 5	Command Policy	"NetScalerArchitect" User	ALLOW	.*	1
Item 6	Command Policy	"Level2Manager" User	ALLOW	(^main.*)((^show\s+(?!system)(?!configstatus)(?!nsns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gsibrunningConfig)(?!audit messages)(?!techsupport).*) (^stat.*)	1

To align the command policy configuration with the security requirements of the organization, the _____ for _____ should change. (Choose the correct option to complete the sentence.)

- A. command spec; item 3
- B. priority; Item 5
- C. action; Item 1
- D. priority; Item 2
- E. action; Item 4
- F. command spec; Item 6

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

A Citrix Architect needs to define the architect and operational processes required to implement and maintain the production environment.

In which phase of the Citrix Methodology will the architect define this?

- A. Define
- B. Deploy
- C. Assess
- D. Review
- E. Manage
- F. Design

Correct Answer: F

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.slideshare.net/davidmcg/designing-your-xenapp-75-environment>

QUESTION 22

Under which two circumstances will a service be taken out of the slow start phase with automated slow start? (Choose two.)

- A. The service does NOT receive traffic for three successive increment intervals.

- B. The server request rate parameters are set above 25 requests per second.
- C. The actual request rate is slower than the new service request rate.
- D. The percentage of traffic that the new service must receive is greater or equal to 50.
- E. The request rate has been incremented 100 times.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.citrix.com/en-us/netScaler/12/load-balancing/load-balancing-advanced-settings/slow-start-service.html>

QUESTION 23

Scenario: A Citrix Architect has set up NetScaler MPX devices in high availability mode with version 12.0.53.13 nc. These are placed behind a Cisco ASA 5505 Firewall. The Cisco ASA 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 MPX 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 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 decided 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 security feature should the architect configure to meet these requirements?

- A. Global Server Load balancing with Dynamic RTT
- B. Global Server Load Balancing with DNS views
- C. Geolocation-based blocking using Application Firewall
- D. geolocation-based blocking using Responder policies

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

Scenario: A Citrix Architect has deployed an authentication setup with a ShareFile load-balancing virtual server. The NetScaler is configured as the Service Provider and Portalguard server is utilized as the SAML Identity Provider. While performing the functional testing, the architect finds that after the users enter their credentials on the logon page provided by Portalguard, they get redirected back to the Netscaler Gateway page at uri /cgi/samlauth/ and receive the following error. "SAML Assertion verification failed; Please contact your administrator."

The events in the /var/log/ns.log at the time of this issue are as follows:

```
Feb 23 20:35:21 <local0.err> 10.148.138.5 23/02/2018:20:35:21 GMT vorsb1 0-PPE-0 : default AAATM Message 3225369 0 : "SAML : ParseAssertion:
parsed attribute NameID, value is nameid"
Feb 23 20:35:21 <local0.err> 10.148.138.5 23/02/2018:20:35:21 GMT vorsb1 0-PPE-0 : default AAATM Message 3225370 0 : "SAML verify digest:
algorithms differ, expected SHA1 found SHA256"
Feb 23 20:35:44 <local0.err> 10.148.138.5 23/02/2018:20:35:44 GMT vorsb1 0-PPE-0 : default AAATM Message 3225373 0 : "SAML : ParseAssertion:
parsed attribute NameID, value is named
Feb 23 20:35:44 <local0.err> 10.148.138.5 23/02/2018:20:35:44 GMT vorsb1 0-PPE-0 : default AAATM Message 3225374 0 : "SAML verify digest:
algorithms differ, expected SHA1 found SHA256"
Feb 23 20:37:55 <local0.err> 10.148.138.5 23/02/2018:20:37:55 GMT vorsb1 0-PPE-0 : default AAATM Message 3225378 0 : "SAML : ParseAssertion:
parsed attribute NameID, value is nameid"
Feb 23 20:37:55 <local0.err> 10.148.138.5 23/02/2018:20:37:55 GMT vorsb1 0-PPE-0 : default AAATM Message 3225379 0 : "SAML verify digest:
algorithms differ, expected SHA1 found SHA256"
```

What should the architect change in the SAML action to resolve this issue?

- A. Signature Algorithm to SHA 256
- B. The Digest Method to SHA 256
- C. The Digest Method to SHA 1
- D. Signature Algorithm to SHA 1

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Scenario: A Citrix Architect needs to assess an existing NetScaler gateway deployment. During the assessment, the architect collects key requirements for different user groups, 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	
<ul style="list-style-type: none"> All users will access the environment using Citrix Receiver for Web. The Accountants group should ONLY have access to assigned desktops and applications in StoreFront. The Managers group should have access to assigned desktops and applications in StoreFront as well as internal web applications and file servers. 	
Configurations	

Location	Type	Setting	Configuration
NetScaler gateway session policy (Gateway-Policy)	N/A	Policy expression	ns_true
NetScaler gateway session policy (Gateway-Policy)	N/A	Session profile	Gateway-Profile
NetScaler gateway session policy (Gateway-Profile)	Client Experience	Clientless Access	ON
NetScaler gateway session policy (Gateway-Profile)	Published Applications	ICA Proxy	ON
NetScaler gateway session policy (Gateway-Profile)	Published Applications	Web Interface Address	http://sf-vip.workspace-labs.net/Citrix/StoreWeb
StoreFront (Store)	Store Settings	Remote Access	No VPN tunnel

Which configuration should the architect make to meet these requirements?

- A. Change the Clientless Access settings in an existing session profile.
- B. Change the remote Access settings in StoreFront.
- C. Change ICA proxy settings in an existing session profile.
- D. Change the policy expression in an existing session policy.
- E. Create a new session profile and policy.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

Scenario: A Citrix Architect needs to assess an existing NetScaler configuration. The customer recently found that certain user groups were receiving access to an internal web server with an authorization configuration that does NOT align with the designed security requirements.

Click the Exhibit button view the configured authorization settings for the web server.

Requirements					
<ul style="list-style-type: none"> By default, no connection should have access to network resources unless authorized based on the other requirements. By default, only connections coming from the internal network (192.168.10.0/24) should be permitted to access the web server. The Accountants group is authorized to access URLs with a ".zip" extension; all other users must NOT be authorized for this. The Executives group is authorized to access the web server from inside OR outside the internal network. 					
Configurations					
Name	Type	Bind Point	Action	Priority	Associated Policy Expressions
Item 1	Authorization setting	Global	DENY	N/A	N/A
Item 2	Authorization Policy	NetScaler traffic management virtual server	ALLOW	1	Client.IP.SRC.IN_SUBNET (192.168.10.0/24)
Item 3	Authorization Policy	NetScaler traffic management virtual server	DENY	2	HTTP.REQ.URL.SUFFIX.EQ ("zip")
Item 4	Authorization Policy	Accountants Group	ALLOW	1	HTTP.REQ.URL.SUFFIX.EQ ("zip")
Item 5	Authorization Policy	Executives Group	ALLOW	1	Client.IP.SRC.NE (192.168.10.0/24)

Which item should the architect change or remove to align the authorization configuration with the security requirements of the organization?

- A. Item 1
- B. Item 3
- C. Item 4
- D. Item 5

E. Item 2

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

For which three reasons should a Citrix Architect perform a capabilities assessment when designing and deploying a new NetScaler in an existing environment? (Choose three.)

- A. Understand the skill set of the company.
- B. Assess and identify potential risks for the design and build phase.
- C. Establish and prioritize the key drivers behind a project.
- D. Determine operating systems and application usage.
- E. Identify other planned projects and initiatives that must be integrated with the design and build phase.

Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

Which step does a Citrix Architect need to ensure during the Define phase when following the Citrix Methodology?

- A. Testing steps were integrated.
- B. The project manager agrees with road map timelines.
- C. A phased roll out was completed.
- D. Existing networking infrastructure is ready.
- E. The redundancy deployment decision was made.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.slideshare.net/davidmcg/designing-your-xenapp-75-environment>

QUESTION 29

Scenario: Based on a discussion between a Citrix Architect and team of Workspacelab has been created across three (3) sites.

They captured the following requirements during the design discussion held for NetScaler design projects:

- All three (3) Workspacelab sites (DC, NDR, and DR) will have similar NetScaler configuration and design.
 - Both external and internal NetScaler MPX appliances will have Global Server Load balancing (GSLB) configured and deployed in Active/Passive mode.
 - GSLB should resolve both A and AAA DNS queries.
 - In the GSLB deployment, the NDR site will act as backup for the DC site. whereas the DR site will act as backup for the NDR site.
 - When the external NetScaler replies to DNS traffic coming in through Cisco Firepower IPS, the replies should be sent back through the same path. ▪
- On the internal NetScaler, both front-end VIP and back-end SNIP will be part of the same subnet.
- USIP is configured on the DMZ NetScaler appliances.
 - The external NetScaler will act default gateway for back-end servers.
 - All three (3) sites (DC, NDR, and DR) will have two (2) links to the Internet from different service providers configured in Active/Standby mode.

Which design decision must the architect make to meet the design requirements above?

- A. Interface 0/1 must be used for DNS traffic.
- B. The SNIP of the external NetScaler must be configured as default gateway on the back-end servers.
- C. ADNS service must be used with IPv6 address.
- D. Policy-Based Route with next hop as CISCO IPS must be configured on the external NetScaler.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

Scenario: A Citrix Architect has sent the following request to the NetScaler:


```
HTTP Method
POST
URL
http://<netscaler-ip-address>/nitro/v1/config?clusterinstance
Requests Headers
Cookie:NITRO_AUTH_TOKEN=<tokenvalue>
Content-Type:application
Request Payload
{
  "clusterinstance":
  {
    "clid":1,
    "preemption":"ENABLED"
  }
}
```

Which response would indicate the successful execution of the NITRO command?

- A. 302
- B. 201
- C. 202
- D. 200

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>