HIGHER QUALITY
BETTER SERVICE

CERTTREE

QUESTION & ANSWER

Provide One Year
Free Update!

https://www.certtree.com

Exam : **1Y0-440**

Title : Architecting a Citrix Networking Solution

Version : DEMO

1.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
Answer: A

2.Which three steps should a Citrix Architect complete to configure session settings for different user accounts or groups? (Choose three.)
A. Bind a profile to the authentication virtual server that handles the traffic to which the architect wants to apply the policy.
B. Create policies to select the connections to which to apply particular profiles and bind the policies to users or groups.
C. Create a profile for each user account or group for which the architect wants to configure custom session settings.
D. Customize the default settings for sessions with the global session settings.
E. Bind a policy to the authentication virtual server that handles the traffic to which the architect wants to apply the profile.
Answer: B,C,E

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.
Answer: B,D

4.Scenario: A Citrix Architect has met with a team of Workspacelab members for a design discussion
They have captured the following requirements for the Citrix ADC 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 Citrix Gateway
➪ A domain drop down list must be provided if the user connects to the Citrix Gateway virtual server externally
Which method must the architect utilize for user management between the two domains?
A. Create a global catalog containing the objects of Vendorlab and Workspacelab domains.
B. Create shadow accounts for the users of the Vendorlab domain in the Workspacelab domain
C. Create a two-way trust between the Vendorlab and Workspacelab domains
C. Create shadow accounts for the users of the Workspacelab domain in the Vendorlab domain
Answer: B

5.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 vorsbl 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 vorsbl 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 vorsbl 0-PPE-0 : default AAATM Message 3225373 0 "SAML: ParseAssertion: parsed attribute NameID, value is nameid"
Feb 23 20:35:44 <local0.err> 10.148.138.5 23/02/2018:20:35:44 GMT vorsbl 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 vorsbl 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 vorsbl 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
Answer: C