

Citrixperience.com

**1Y0-456 Citrix Access Suite 4.0:
Build/Test**

Practice Exam

Version 1.1

(May 7, 2007)

Citrix® Access Suite 4.0: Build/Test Practice Exam

This practice exam was created by Citrixperience.com. Used for creation of this practice exam, besides personal field experience, was the Citrix® courseware CTX-1456AI Citrix® Access Suite 4.0: Build/Test Workshop, which is a copyright of Citrix® Systems.

Along with the courseware listed above, this practice exam is meant to be used in preparation for the 1Y0-456 Citrix® Access Suite 4.0: Build/Test exam. Also suggested for preparation are other books that relate to the subjects and above all, personal experience with the products. Citrixperience.com recommends further preparation by using other 1Y0-456 products found at www.Citrixperience.com.

The license for this practice exam is for one user only. It is a copyright of Citrixperience.com and may not be reprinted, copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including but not limited to electronic, mechanical, photocopying, recording, or other means, in full or in part, without the prior express written permission of Citrixperience.com.

Citrix, the Citrix logo, Citrix ICA, Citrix MetaFrame, Citrix MetaFrame XP, Citrix Nfuse, Citrix Extranet, Citrix Program Neighborhood, Citrix WinFrame, and other Citrix product names referenced herein are registered trademarks or trademarks of Citrix Systems, Inc. in the United States and other jurisdictions. All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.

Citrix® Systems, Inc. is not affiliated with Citrixperience.com in any way.

1Y0-456 Citrix Access Suite 4.0: Build/Test

#Building and Testing Citrix Presentation Server

1. Scenario: An administrator is planning to set up an environment to build and test a new Access Suite product on a small scale before actually implementing it in the live environment. A Presentation Server farm already exists in this enterprise. Which of the following would be the best plan for testing the new product?
 - a. Create a new farm for testing and development purposes only
 - b. Create new zone in the existing farm for testing and development purposes only
 - c. Use an existing zone in the existing farm and disable zone preference and failover in the farm
 - d. Use an existing zone in the existing farm and enable zone preference and failover in the farm

Answer: a.

Explanation: The administrator should segregate the test environment so that it does not impact an existing production environment. Testing and development Presentation Servers should not belong to the same farm as the production servers; setting up a separate zone for the test servers in the production farm is not a good option.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 27

2. Which of the following are true of session reliability? (Choose 3)
 - a. Uses TCP port 2598
 - b. Enabled by default
 - c. Uses the Citrix Common Gateway Protocol
 - d. Uses the Citrix XML Service

Answer: a.b.c.

Explanation: Presentation Server uses the Citrix Server XTE Service for session reliability. Session reliability uses TCP port 2598 and is tunneled by means of the Citrix Common Gateway Protocol. Session reliability is enabled by default in the farm properties of the Presentation Server farm.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 31

3. Use virtual IP addressing: (Choose 3)
 - a. For applications that require each session to have its own IP address for licensing, routing or addressing purposes
 - b. For network monitoring systems that require each session to have its own IP address in order to track individual user's traffic
 - c. For RDP and ICA sessions
 - d. For applications that may be hard-coded

Answer: a.b.d.

Explanation: Virtual IP addressing is available with the Advanced and Enterprise editions of Presentation Server. Virtual IP addressing can manage some of the issues associated with applications that identify the client connection to the back

Visit Citrixexperience.com for more Citrix certification preparation products.

end of Presentation Server-based applications by an IP address. Use virtual IP addressing for applications that require each session to have its own IP address for licensing, routing or addressing purposes; for network monitoring systems that require each session to have its own IP address in order to track individual user's traffic (Without the use of a virtual IP address, all users appear to have the same IP address when connecting from Presentation Server to a backend application. The virtual IP address feature assigns an IP address to a session, not to a user); and for applications that may be hard-coded to a specific port on a loopback interface or that may be hard-coded to listen to a specific port on all interfaces and require more than one IP address when running multiple instances in a Terminal Server environment. Virtual IP addressing is only available for ICA sessions, not for RDP sessions.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 31

4. Scenario: You must create a delegated administrator group for the Help Desk personnel that allows them to make changes to sessions, view all published applications, other administrators, Application Isolation Environments, load evaluators, policies, printers, resource management and server information. (Choose 4)
 - a. Create a group named Help Desk in the Presentation Server Console
 - b. Add the Help Desk group to MetaFrame Administrators in the Presentation Server Console
 - c. Select Full Administration on the Privileges screen of the Add MetaFrame Administrators wizard
 - d. Allow the Help Desk Group the following permissions in the Applications node: View Published Applications and Content, View RM Applications and Content, Sessions (full)
 - e. Allow the Help Desk Group the following permissions in each respective node: View MetaFrame Administrators, View Isolation Environments, View Load Evaluators, View User Policies, View Printers and Print Drivers
 - f. Allow the Help Desk Group the following permissions in the Servers node: View RM Information and Alerts, View Server Information, Sessions (full)
 - g. Allow the Help Desk Group full permissions in the Monitoring and Alerting node
 - h. Create a shadow policy named Help Desk Shadowing, add the Help Desk Group to the policy and filter the policy

Answer: b.d.e.f.

Explanation: To create a delegated administrator group for the Help Desk personnel that allows them to make changes to sessions, view all published applications, other administrators, Application Isolation Environments, load evaluators, policies, printers, resource management and server information, use the following steps: Create a Group in Active Directory named Help Desk Group. In the Presentation Server Console, right-click the MetaFrame Administrators node and click Add MetaFrame Administrator. The Add MetaFrame

Visit Citrixexperience.com for more Citrix certification preparation products.

Administrator wizard launches. On the opening screen, drill down to the correct Organizational Unit in the drop-down list and find the Help Desk Group and add it to Configured Accounts. Click Next. Click Next on the Alert Contact Details screen. Select Custom and then click Next. Select the Applications node and check View Published Applications and Content, View RM Applications and Content and Sessions. Select the MetaFrame Administrators node, be sure that 'Log on to Presentation Server Console' is checked and check View MetaFrame Administrators. Select the Isolation Environments node and check View Isolation Environments. Select the Load Evaluators node and check View Load Evaluators. Select the Policies node and check View User Policies. Select the Printer Management node and check View Printers and Printer Drivers. Select the Resource Manager node and check View Resource Management Configuration and Alerts. Select the Servers node and select View RM Information and Alerts, View Server Information and Sessions. Click Finish. Click Actions in the top left corner of the window. Click Log Off from Server Farm. Click Yes.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 32, 33, 139, 140

5. Scenario: You are asked to allow the Help Desk personnel to shadow Presentation Server users in the company. There is already a group in Active Directory named Help Desk that contains all of the Help Desk personnel. Which of the following steps will allow you to give them the appropriate privileges? (Choose 4)
- Create a policy named Help Desk Shadow in the Presentation Server Console
 - Create a group named Help Desk Shadow in Active Directory and add the Help Desk group to the Help Desk Shadow group
 - In the policy, navigate to User Workspace > Shadowing > Permissions and select Enable
 - Add the Help Desk group to the Help Desk Shadow policy
 - Add the Help Desk Shadow group to the Help Desk Shadow policy
 - Filter users in the Help Desk Shadow policy
 - Filter policies in the Help Desk Shadow group
 - Filter policies in the Help Desk group

Answer: a.c.d.f.

Explanation: To allow the Help Desk personnel to shadow Presentation Server users in the company you should use the existing Help Desk group and follow this procedure: In the Presentation Server Console, right-click the Policies node and click Create Policy. Type Help Desk Shadow in the Policy Name field and click OK. Right-click the Help Desk Shadow policy and click Properties. Navigate to User Workspace > Shadowing > Permissions in the left pane. Click Enabled in the right pane. Click Configure. In the Assign Shadowing Permissions window, drill down to the correct Organizational Unit in the drop-down list and find the Help Desk group, add it to Configured Accounts and click OK. Click OK on the Help Desk Shadow Properties screen. Right-click the Help Desk Shadow policy and click 'Apply this policy to'. Click Users. Find the correct group of users that the Help Desk will be allowed to shadow and select it.

Visit Citrixexperience.com for more Citrix certification preparation products.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 32, 33, 141, 142

6. Scenario: An international company with employees and offices around the world hires you for a consulting job. They have asked you to reduce network traffic by configuring the Presentation Server environment to have employees in Japan connect to the Tokyo servers and employees in North America connect to the Los Angeles servers. Which of the following Presentation Server configurations should you concentrate on? (Choose 3)
- Zone Preference and Failover
 - Session Reliability
 - Creating zones
 - Setting election preferences

Answer: a.c.d.

Explanation: In order to have employees in Japan connect to the servers in Tokyo and employees in North America connect to servers in Los Angeles, you must create one new zone for Tokyo, move the Tokyo server into that zone and set the election preference to that server to Most Preferred. The Los Angeles server will remain in the old zone. Create a Zone Preference and Failover policy for the Japan users, setting the Tokyo zone as the Primary Group and the Los Angeles zone as Backup Group 1. Create another Zone Preference and Failover policy for the North America users, setting the Los Angeles zone as the Primary Group and the Tokyo zone as Backup Group 1. Apply each policy to their respective countries, filtering by IP address.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 34, 35, 143-146

7. Zone Preference and Failover is configured:
- In the Zone settings of the farm properties in the Presentation Server Console
 - In the MetaFrame Settings of the server properties in the Presentation Server Console
 - In a policy
 - In Common Tasks in the farm node of the Access Suite Console
 - In Other Tasks in the farm node of the Access Suite Console

Answer: c.

Explanation: To configure Zone Preference and Failover, create a policy. Right-click on the policy and select Properties. In the left pane of the zone Properties window, navigate to 'User Workspace > Connections > Zone preference and failover'. Click Enabled in the right pane. Select one primary and up to five backup zones. Filter the connections that this policy will be applied to by Access Control, Client IP address, Client Name, Servers or Users.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 144, 145

Visit Citrixexperience.com for more Citrix certification preparation products.

8. Which of the following are steps to create a Presentation Server policy? (Choose 3)
- Open the Access Suite Console, right-click on the Policies node and select Create Policy
 - Open the Presentation Server Console, right-click on the Policies node and select Create Policy
 - Type the name of the policy in the Name field
 - Type the description in the Description field
 - Filter the connections for this policy

Answer: b.c.d.

Explanation: To create a Presentation Server policy, in the Presentation Server Console, right-click on the Policies node and select Create Policy. In the New Policy window, type the name of the policy in the Name field and type the description of the policy in the Description field (Description is optional). Optionally, click the 'Optimize initial policy settings for a connection type' and select WAN, Satellite or Dial-up. Click OK. In the next step, applying the policy, you would filter the connections for this policy, but not during creation.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 144

9. To filter connections for a Presentation Server policy:
- In the Users node, right-click on the user group and select 'Apply policy'
 - In the Policies node, right-click on the policy and select 'Apply this policy to'
 - Click the 'Apply this policy to' drop-down list in the policy properties
 - In Active Directory, create a Group Policy Object and apply it to a Global Group

Answer: b.

Explanation: To filter connections for a Presentation Server policy, after creating a policy in the Policies node of the Presentation Server Console, right-click on the policy and select 'Apply this policy to'. The Policy Filters window will launch. In the Policy Filters window, select among the conditional filters: Access Control, Client IP Address, Client Name, Servers or Users. Configure one of the conditional filters to specify how the policy is applied.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 145, 146

10. Policy filters can be applied using: (Choose 5)
- Access Control
 - Client IP Address
 - Client MAC Address
 - Client Name
 - Time Zone
 - Servers
 - Users

Answer: a.b.d.f.g.

Visit Citrixexperience.com for more Citrix certification preparation products.

Explanation: Policy filters can be applied using Access Control, Client IP Address, Client Name, Servers or Users. To apply filters, right-click on a policy, select 'Apply this policy to' and select one of the filters in the right pane of the Policy Filter screen. Configure the filter.

Source: Field Experience

11. To filter connections to a policy based on MetaFrame Secure Access Manager, use the `_?_` filter.
- Client IP Address
 - Client Name
 - Servers
 - Users
 - Access Control

Answer: e.

Explanation: To filter connections to a policy based on MetaFrame Secure Access Manager, right-click on the policy and select 'Apply this policy to'. The Policy Filters window will launch. Select Access Control in the left pane of the Policy Filters window, check 'Filter based on Access Control' and check 'Apply to connections made through MetaFrame Secure Access Manager (version 4.0 or later)'. Select 'Any connection' or 'Any connection that meets any of the following filters'. If 'Any connection that meets any of the following filters' is chosen, click Add and select a MetaFrame Secure Access Manager farm and a MetaFrame Secure Access Manager filter.

Source: Field Experience

12. Scenario: In your company, the law department has access to highly sensitive data that cannot leak out in any way. In order to comply with company policies, you need to create a very restrictive environment for the members of the Law group. As the Citrix administrator for your company, in your Presentation Server environment, you intend to allow no mapped drives of any kind, no COM ports and no more than one auto-created printer for the Law group. Also, shadowing of the Law group must be disallowed. Which of the following will you do to make these restrictions?
- Create a logon script disabling all mapped drives, disable the COM ports on all Law group members' computers, disable synchronous printing on all published applications used by the Law group and disable shadowing in the Citrix Connection Configuration Tool
 - Create an Active Directory Group Policy Object enabling and configuring the Mappings policy rule, the 'Turn off COM ports' policy rule, the Auto-creation rule and the Permissions policy rule, and apply the policy to the Law group
 - Create a security template enabling and configuring the Mappings policy rule, the 'Turn off COM ports' policy rule, the Auto-creation rule and the Permissions policy rule, and apply the policy to the Law group
 - Create a Presentation Server policy enabling and configuring the Mappings policy rule, the 'Turn off COM ports' policy rule, the Auto-

Visit Citrixexperience.com for more Citrix certification preparation products.

creation rule and the Permissions policy rule, and apply the policy to the Law group

Answer: d.

Explanation: In this Presentation Server environment, to restrict the Law group by allowing no mapped drives, no COM ports, no more than one auto-created printer and no shadowing, create a policy in the Presentation Server Console and in the policy, enable and configure the Client Devices > Resources > Drives > Mappings policy rule, the 'Client Devices > Resources > Ports > Turn off COM ports' policy rule, the Printing > Client Printers > Auto-creation policy rule and the User Workspace > Shadowing > Permissions policy rule.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 36, 37, 147, 148

13. When creating a Presentation Server policy, in which folder of the policy properties would an administrator configure drive mappings?
- Bandwidth
 - Client Devices
 - Printing
 - User Workspace
 - Security

Answer: b.

Explanation: To configure drive mappings for client devices in a policy, navigate to Client Devices > Resources > Drives > Mappings. In the Mapping policy rule, select Not Configured, Disabled or Enabled. If Enabled is selected, select the drives you do not want to map to client devices by checking 'Turn off Floppy disk drives', 'Turn off Hard drives', 'Turn off CD-ROM drives' and/or 'Turn off Remote drives'.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 147

14. When creating a Presentation Server policy, in which folder of the policy properties would an administrator configure COM and LPT ports?
- Bandwidth
 - Client Devices
 - Printing
 - User Workspace
 - Security

Answer: b.

Explanation: To configure COM and LPT ports for client devices in a policy, navigate to Client Devices > Resources > Ports and configure the policy rules 'Turn off COM ports' and 'Turn off LPT ports'.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 147

15. When creating a Presentation Server policy, in which folder of the policy properties under the Printing folder would an administrator configure auto-creation of printers?
- Client Printers

Visit Citrixexperience.com for more Citrix certification preparation products.

- b. Drivers
- c. Auto-creation
- d. Spooler

Answer: a.

Explanation: To configure auto-creation of printers in a policy, navigate to Printing > Client Printers. In the Auto-creation policy rule, select Not Configured, Disabled or Enabled. If Enabled is selected, select to 'Auto-create all client printers', 'Auto-create local (non-network) client printers only', 'Auto-create the client's default printer only' or 'Do not auto-create client printers'. Just an FYI, there are no Auto-creation or Spooler folders under the Printing folder.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 147

16. When creating a Presentation Server policy, in which folder of the policy properties would an administrator configure shadowing?
- a. Bandwidth
 - b. Client Devices
 - c. Printing
 - d. User Workspace
 - e. Security

Answer: d.

Explanation: To configure shadowing in a policy, navigate to User Workspace > Shadowing. Configure the Configuration and Permissions policy rules. In each policy rule, select Not Configured, Disabled or Enabled. If the Configuration rule is enabled, select 'Do Not Allow Shadowing' or 'Allow Shadowing'. If 'Allow Shadowing' is chosen, check 'Prohibit Being Shadowed Without Notification' and/or Prohibit Remote Input When Being Shadowed. If the Permissions policy rule is enabled, select users to give permissions to shadow the connections to which the policy applies.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 147, 148

17. Scenario: You are asked to publish Internet Explorer on two of the servers in your farm, AppServerA and AppServerD. You are supposed to select all of the defaults except to publish it in 16-bit color. The Internet group is the only group to be allowed access to it. Which of the following are some of the steps that you take to publish Internet Explorer? (Choose 3)
- a. Right-click the Applications node in the Presentation Server Console and select Publish Application
 - b. Right-click the farm node in the Presentation Server Console, select Properties, select Applications in the left pane of Properties and select Publish New Application in the right pane of Properties
 - c. Check Isolate Application in the Specify What to Publish screen
 - d. Select True Color in the Specify Application Appearance screen
 - e. Select High Color in the Specify Application Appearance screen
 - f. Click Add All on the Specify Servers screen

Visit Citrixexperience.com for more Citrix certification preparation products.

- g. Drill down to the correct Organizational Unit and select the Internet group on the Specify Users screen

Answer: a.e.g.

Explanation: To publish Internet Explorer for the Internet group in 16-bit color on only AppServerA and AppServerD, right click on the Applications node in Presentation Server and select Publish Application. Type Internet Explorer in the Display Name field of the Welcome screen and click Next. On the Specify What to Publish screen, verify that Application is selected, click browse and navigate to IEXPLORE.EXE. Click Next. Click Next on the Program Neighborhood Settings screen. Select High Color (16 bit) on the Specify Application Appearance screen and click Next. Click Next on the Specify Requirements screen, Specify Application Limits Screen and Configure Access Control screen. On the Specify Servers screen, click on AppServerA, hold down the Control key and click on AppServerD to select them both. Click Add to add both servers. Click Next. Drill down to the correct Organizational Unit and select the Internet group on the Specify Users screen and click Next. Click Finish on the Specify File Type Associations screen.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 149, 150

18. Where can an administrator specify client to server content redirection? (Choose 2)
- a. In the properties of the farm node
 - b. In the properties of a published application
 - c. In the Application Publishing Wizard
 - d. In a policy

Answer: b.c.

Explanation: To specify client to server content redirection in the Application Publishing Wizard, on the Specify File Type Associations screen, check the file types that you wish to associate with the application. To specify client to server redirection in the properties of a published application, select Content Redirection in the right pane of Properties and check the file types that you wish to associate with the application. Server to client redirection can be configured in a policy, not client to server redirection.

Source: Field Experience

19. How can an administrator update file type association data using the Presentation Server Console?
- a. Right-click on the Applications node and select Update File Types from Registry
 - b. Right-click on a published application and select Update File Types from Registry
 - c. In the Application Publishing Wizard, on the Specify File Type Associations Screen click Update File Types from Registry
 - d. Right-click on the farm node and select Update File Types from Registry

Answer: d.

Visit Citrixexperience.com for more Citrix certification preparation products.

Explanation: To update the file type association data in the Presentation Server Console, right-click on the farm node and select Update File Types from Registry. In the Update File Type Association screen, select the servers you wish to add to the update and click OK. Click OK on the pop-up that says 'File type association data is being updated. This may take several minutes to complete'.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 150, 151

20. When you are required to publish multiple applications, which of the following is the most efficient way of doing so?
- Create the first application using the Application Publishing Wizard and make copies of it for each of the following applications
 - Install the application on the first server and then create a package and distribute it using Installation Manager
 - Use the Automatic Publishing Wizard to install each application
 - Launch the Application Publishing Wizard for each individual application

Answer: a.

Explanation: To save time publishing multiple applications, use the Copy Published Application feature. To use this feature, create the first published application using the Application Publishing Wizard, right-click on the published application and select Copy Published Application. Right-click on the copied application and select Rename. Type the name of the application in the Display Name field and click OK. Right-click the new published application and select Properties. In Properties, select Application Location. Click Browse. Browse to the application you wish to publish and click OK. Click Program Neighborhood Settings, click Change Icon, select the correct icon and click OK. Configure anything else in the properties that the new published application warrants.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 40, 151

21. To install and publish an application into an application isolation environment:
(Choose 3)
- Right-click the Applications node in the Presentation Server Console and select Isolation Environments
 - Right-click the Isolation Environments node in the Presentation Server Console and select 'New isolation environment'
 - Right-click a published application in the Presentation Server Console and select 'New isolation environment'
 - Run AIESETUP.EXE
 - Right-click the Applications node in the Presentation Server Console and select Publish Application
 - Right-click the Isolation Environments node and select Publish Application

Answer: b.d.e.

Explanation: To install and publish an application into an application isolation environment, in the Presentation Server Console, right-click on the Isolation

Visit Citrixexperience.com for more Citrix certification preparation products.

Environments node and select 'New isolation environment'. Type the name of the isolation environment in the 'Application isolation environment name' field. Click OK. Open a command prompt and type AIESETUP "<isolation environment name>" <path> and press enter. For example, if you are installing Power Point Viewer 97 and you already created an isolation environment named PowerPointViewer97, you would type the following: AIESETUP "PowerPointViewer97" "c:\Program Files\Microsoft\Power Point Viewer\PPVIEW97.EXE". Run through the application installation. Press Enter at the command prompt to begin the application discovery process. Exit the command prompt after the application discovery completes. Right-click the Applications node in the Presentation Server Console and select Publish Application to launch the Application Publishing Wizard. Type the display name in the Display Name field and click Next. Verify that Application is selected in the Specify What to Publish screen, check Isolate Application and click Settings. Click the correct isolation environment name and select 'Application was installed into environment'. Click the Application name in the 'Choose installed application' drop-down list and click OK. Go through the rest of the Application Publishing Wizard.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 152, 153

22. To apply and confirm the Advanced load evaluator on all of the servers in the farm: (Choose 3)
- Right-click the Load Evaluators node in the Presentation Server Console and select Load Manage Servers
 - Right-click the Servers node in the Presentation Server Console and select Load Manage Servers
 - Click Add under Available Servers
 - Click Add All under Available Servers
 - Click the Servers node and select the Usage Reports tab
 - Click the Load Evaluators node and select the Usage Reports tab

Answer: b.d.f.

Explanation: To apply a load evaluator to all of the servers in the farm, right-click the Servers node in the Presentation Server Console and select Load Manage Servers. Click Add All on the Load Manage Servers screen under Available Servers. Verify Advanced is chosen under Available Load Evaluators. Click OK. To confirm the load evaluator, click the Load Evaluators node and select the Usage Reports tab. Verify that the Advanced load evaluator is listed for all of the servers.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 154, 155

23. To create a new load evaluator based on scheduling: (Choose 4)
- Right-click the Load Evaluators node in the Presentation Server Console and select New Load Evaluator

Visit Citrixexperience.com for more Citrix certification preparation products.

- b. Right-click the Servers node in the Presentation Server Console and select New Load Evaluator
- c. Type a name and description for the load evaluator
- d. Type Scheduling in the Available Rules box
- e. Select Scheduling in the Available Rules box
- f. Select the days of week and times of day under Rule Settings
- g. Type in the days of week and times of day under Rule Settings

Answer: a.c.e.f.

Explanation: To create a new load evaluator based on scheduling, right-click the Load Evaluators node in the Presentation Server Console and select New Load Evaluator. Select Scheduling in the Available Rules box. Select the days of week and times of day under Rule Settings. Click OK.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 155

24. To attach a load evaluator to an application and confirm the configuration on a server: (Choose 5)
- a. Expand the Servers node in the Presentation Server Console
 - b. Expand the Applications node in the Presentation Server Console
 - c. Right-click a published application and select Load Manage Application
 - d. Right-click a server and select Load Manage Application
 - e. Select the published application in the Available Published Applications list
 - f. Select the servers in the Available Servers list
 - g. Select the load evaluator in the Available Load Evaluators list
 - h. Click the Servers node and select the Usage Reports tab
 - i. Click the Load Evaluators node and select the Usage Reports tab

Answer: b.c.f.g.i.

Explanation: To attach a load evaluator to an application and confirm on a server, expand the Applications node in the Presentation Server Console, right-click the desired published application and select Load Manage Application. Select the servers that the application will be monitored on in the Available Servers list and click Add, or if all servers, click Add All. Select the load evaluator in the Available Load Evaluators list. Click OK. To verify the configuration, click the Load Evaluators node, select the Usage Reports tab and click By Application.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 155, 156

25. To enable virtual IP addressing on servers: (Choose 5)
- a. Expand the Servers node, right-click on a server and select Properties
 - b. Right-click on the farm node and select Properties
 - c. Select Virtual IP Address Configuration in the left pane of Properties
 - d. Click Add IP Range in the right pane of Properties
 - e. Select the IP address range from the Add IP Range list
 - f. Select the subnet mask from the Add Subnet Mask list
 - g. Type the IP address range and subnet mask in the Add IP Range window
 - h. Type the server names in the Add Server window

Visit Citrixexperience.com for more Citrix certification preparation products.

- i. Select the servers in the Add Server For window

Answer: b.c.d.g.i.

Explanation: To enable virtual IP addressing on servers, right-click the farm node in the Presentation Server Console and select Properties. In Properties, select virtual IP Address Configuration in the left pane and click Add IP Range in the right pane. The Add IP Range window launches. Type the IP address range and subnet mask in the Add IP Range window. Click OK. Click Yes on the Configure Servers pop up. The Virtual IP Address Range window launches. Click Add in the Virtual IP Address Range window. The Add Server For window launches. Select the servers in the Add Server For window. Click OK.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 156

26. To apply virtual IP addressing to an application: (Choose 3)
 - a. Right-click the farm node in the Presentation Server Console and select Properties
 - b. Right-click the farm node in the Access Suite Console and select Properties
 - c. Select Virtual IP Processes in the left pane of Properties
 - d. Select Virtual IP Addressing in the left pane of Properties
 - e. Click Add Processes in the right pane of Properties and select the application in the Add Process for Virtual IP window
 - f. Click Add Processes in the right pane of Properties and type the application name in the Add Process for Virtual IP window

Answer: a.c.f.

Explanation: To apply virtual IP addressing to an application, right-click the farm node in the Presentation Server console and select Properties. Select Virtual IP Processes in the left pane of Properties. Click Add Processes in the right pane of Properties. The Add Process for Virtual IP window launches. Type the application name in the Add Process for Virtual IP window. Click OK. Restart the server.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 156

27. Scenario: Your IT group gets permission to no longer have to manage print drivers in the Presentation Server environment. Which of the following will make this possible going forward?
 - a. Uninstall all of the native printer drivers, install the universal printer driver and edit the registry on each Presentation Server
 - b. Create a policy to enable the universal printer driver only and disable automatic printer driver installation
 - c. In the Printers folder in Settings, disable the printer driver and enable universal printing for every printer installed on each Presentation Server
 - d. Create a login script to run on every computer in the enterprise disabling native printer drivers and enabling the universal printer driver

Answer: b.

Explanation: To use only the universal printer driver and disable automatic printer driver installation in the Presentation Server environment, create a policy in the Presentation Server Console, right click on the policy and click Properties. In the

Visit Citrixexperience.com for more Citrix certification preparation products.

policy properties, expand Printing > Drivers and select Universal Driver in the left pane. Select Enabled in the right pane. Select 'Use universal driver only' from the 'When auto-creating client printers' drop-down list and click Apply. Select 'Native printer auto-install' in the left pane of the policy properties. Select Enabled in the right pane. Select 'Do not automatically install drivers' and click OK.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 157

28. To create a Web Interface site: (Choose 6)
- a. Open the Web Interface Admin Tool
 - b. Open the Presentation Server Console
 - c. Open the Access Suite Console
 - d. Run Discovery
 - e. Click the Web Interface Node and select 'Create site' in Common Tasks
 - f. In the Create Site wizard, select Web Interface
 - g. In the Create Site wizard, select MetaFrame Presentation Server
 - h. Specify the IIS location
 - i. Specify the server farm
 - j. Specify the Access Gateway Server

Answer: c.d.e.g.h.i.

Explanation: To create a Web Interface Site, open the Access Suite Console. Launch the 'Configure and run discovery' wizard from Common Tasks of the farm node. Click Next on the Welcome screen. Click Next in the Select Products or Components screen. In the Configuration Servers screen, verify 'Contact the following Web Interface configuration servers' is selected. Click Add. The Add Server window launches. Type the server name and click OK. Click Next in the Configuration Servers screen. Select Add Local Computer if desired and click Next. Click Next in the Preview Discovery screen. Wait for Discovery to finish running and click Finish. Click the Web Interface node in the Access Suite Console. Click 'Create site' in Common Tasks. On the Select Site Type screen, select MetaFrame Presentation Server and click Next. On the IIS Hosting screen, select 'Set as the default page for the IIS site' to apply the path and click Next. On the Configuration Source screen, select 'Use local configuration file(s)' or 'Use centralized configuration' and click Next. On the 'Server farm' screen, type the name of the server farm. Click Add to type the name of any servers desired for failover. On the New Site Summary screen, verify the information and click Next. After the new site is created, click Finish.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 159

29. Which of the following management consoles would you use to configure authentication for Web Interface?
- a. Presentation Server Console
 - b. Web Interface Admin Tool
 - c. Access Suite Console
 - d. Citrix Connection Configuration Tool

Answer: c.

Visit Citrixexperience.com for more Citrix certification preparation products.

Explanation: To configure authentication for Web Interface, in the Access Suite Console, navigate to Suite Components > Configuration Tools > Web Interface and click on the desired Web Interface site. Click 'Configure authentication methods' under Common Tasks. The Configure Authentication Methods wizard launches. On the 'Specify authentication methods' screen, choose Explicit, Pass-through, 'Pass-through with smart card', 'Smart card' or Anonymous. If Explicit or Pass-through is chosen, configure the settings. Click Next. Configure 'Define selected methods' screen and click Next. Configure 'Specify authentication type settings' screen and click Next. Verify the information on the Check Summary screen and click Finish.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 160

30. Scenario: You have recently installed and configured a Web Interface site in your organization and now you must deploy the Web Client to the users. Which of the following steps will be included in your Web Client deployment? (Choose 4)
- Copy the Client for Web cabinet file locally
 - Open the Presentation Server Console, right click on the Web Interface node and select 'Manage client deployment'
 - Open the Access Suite Console, navigate to the Web Interface site and click 'Manage client deployment' in Common Tasks
 - Select launch clients, specify launch client settings and specify the Web Client settings
 - Configure Client for Java
 - Configure Client for Mac

Answer: a.c.d.e.

Explanation: To configure the Client for Web deployment, create a new folder named 'en' in C:\Program Files\Citrix\Web Interface\4.0\ICAWEB on the Presentation Server. Inside of the 'en' folder, create a new folder named 'ica32' (make sure it is typed in lower case). Copy the WFICAT.CAB file from the Presentation Server Components CD to the 'ica32' folder. Next, navigate to the Web Interface site in the Access Suite Console and click 'Manage client deployment' in Common Tasks. The Manage Client Deployment wizard launches. Select the clients on the 'Select launch clients' screen, choosing among 'Local client (Default)', 'Native embedded client', 'Client for Java' and Embedded Remote Desktop Connection. You can also allow the user to select. Configure automatic client update, automatic client fallback to Client for Java, installation caption and client version support on the 'Specify launch client settings' screen. Specify the file name, version and class ID on the 'Web Client settings' screen. On the Client for Java screen, choose packages to include with in the Java Client. Packages include Audio, Clipboard, 'Local text echo', SSL/TLS, Encryption, 'Client drive mapping', 'Printer mapping' and Configuration UI. You can also let the user choose. Select a private root certificate, if desired. Review the 'Preview summary' screen and click Finish when satisfied.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 161, 162

31. Which of the following would be one of the steps to test the Web Interface configuration for automatic Web Client download?
- Open Internet Explorer
 - Use the LPT1 port
 - In the Presentation Server Console, expand the Servers node, click a server and select the Users tab
 - In the Presentation Server Console, expand the Servers node, click a server and select the Sessions tab
 - Use the termination hotkey CTRL + *

Answer: a.

Explanation: To test the Web Interface configuration for automatic Web Client download, Open Internet Explorer and browse to <http://<WebInterfaceServer>/Citrix/MetaFrame> (replace <WebInterfaceServer> with the name of your Web Interface server). Logon as a user, click Yes on the download screen to download the Web Client and click Yes on the Citrix License Agreement. The Client software installs without user interaction.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 164

32. Which of the following would be one of the steps to verify that only the universal printer driver is being used for printing in the Presentation Server environment?
- Open Internet Explorer
 - Use the LPT1 port
 - In the Presentation Server Console, expand the Servers node, click a server and select the Users tab
 - In the Presentation Server Console, expand the Servers node, click a server and select the Sessions tab
 - Use the termination hotkey CTRL + *

Answer: b.

Explanation: To verify that only the universal printer driver is being used for printing in the Presentation Server environment, add a printer to use for testing. To add a printer, click Start > Printers and Faxes. Click Add a Printer. Click Next. Verify that 'Local printer attached to this computer' is selected. Deselect 'Automatically detect and install my Plug and Play printer' and click Next. Verify that 'Use the following port: LPT1' is selected and click Next. Select any printer and click Next. Accept the default printer name and click Next. Click Next in the Location and Comment screen. Click No in the Print Test Page screen and click Next. Click Finish. Launch an application from Web Interface. In the application, click File > Print. Select your printer from the drop-down list. Verify that the Citrix Universal Printer is listed as the printer type. Close the Print window.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 163-165

33. Which of the following would be one of the steps to verify that users are connected to the correct servers based on the Zone Preference and Failover policy settings?
- Open Internet Explorer

Visit Citrixexperience.com for more Citrix certification preparation products.

- b. Use the LPT1 port
- c. In the Presentation Server Console, expand the Servers node, click a server and select the Users tab
- d. In the Presentation Server Console, expand the Servers node, click a server and select the Sessions tab
- e. Use the termination hotkey CTRL + *

Answer: c.

Explanation: To verify that users are connected to the correct servers based on the Zone Preference and Failover policy settings, in the Presentation Server Console, expand the Servers node, click a server and select the Users tab. Verify that the users are connected to the correct servers according to the Zone Preference and Failover policy.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 165

34. Which of the following would be one of the steps to verify that virtual IP addresses are applied to applications configured for virtual IP addresses?
- a. Open Internet Explorer
 - b. Use the LPT1 port
 - c. In the Presentation Server Console, expand the Servers node, click a server and select the Users tab
 - d. In the Presentation Server Console, expand the Servers node, click a server and select the Sessions tab
 - e. Use the termination hotkey CTRL + *

Answer: d.

Explanation: To verify that virtual IP addresses are applied to applications configured for virtual IP addresses, in the Presentation Server Console, expand the Servers node, click a server and select the Sessions tab. Verify that virtual IP addresses are assigned for the virtual IP address-configured application sessions.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 165

35. Which of the following are steps to shadow a user? (Choose 2)
- a. Open Internet Explorer
 - b. Use the LPT1 port
 - c. In the Presentation Server Console, expand the Servers node, click a server and select the Users tab
 - d. In the Presentation Server Console, expand the Servers node, click a server and select the Sessions tab
 - e. Use the termination hotkey CTRL + *

Answer: c.e.

Explanation: To shadow a user, open the Presentation Server Console, expand the Servers node and click a server. Select the Users tab. Right click a user and select Shadow. Note the shadow termination hotkey setting (CTRL + *) and click OK. Authenticate with your username and password. When done shadowing, click Stop Shadowing or use the hotkey, CTRL + *.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 166

#Building and Testing Citrix Password Manager

36. An administrator must perform which of the following tasks to use a Windows 2000 Server Active Directory implementation as the central store? (Choose 3)
- Enable schema updates
 - Extend the schema
 - Create a central store and assign permissions to the domain
 - Create a Password Manager Organizational Unit

Answer: a.b.c.

Explanation: To use Active Directory as the central store, an administrator must enable schema updates (Windows 2000 Server only), extend the schema, create a central store and assign permissions to the domain.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 60

37. Which of the following features depend on the Password Manager Service, and cannot be implemented without it? (Choose 4)
- Account Self-Service
 - Automatic Key Recovery
 - Cryptographic Data Integrity Assurance
 - Password Provisioning
 - Password Expiration

Answer: a.b.c.d.

Explanation: The Password Manager Service provides the foundation for the optional features, including Account Self-Service, Automatic Key Recovery, Cryptographic Data Integrity Assurance and Password Provisioning. Password Manager must be installed and configured before implementing any of these features.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 61

38. Which of the following Password Manager features allows users to reset their Active Directory passwords?
- Account Self-Service
 - Automatic Key Recovery
 - Cryptographic Data Integrity Assurance
 - Password Provisioning

Answer: a.

Explanation: Account Self-Service allows users to reset their Active Directory passwords.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 61

39. Which of the following Password Manager features allows users to log on to the network and have immediate access to applications managed by Password Manager without the need to verify their identity?
- Account Self-Service
 - Automatic Key Recovery
 - Cryptographic Data Integrity Assurance

Visit Citrixexperience.com for more Citrix certification preparation products.

d. Password Provisioning

Answer: b.

Explanation: Automatic Key Recovery allows users to log on to the network and have immediate access to applications managed by Password Manager without the need to verify their identity.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 61

40. Which of the following Password Manager features protects the central store data from being compromised while in transit to the agent?

- a. Account Self-Service
- b. Automatic Key Recovery
- c. Cryptographic Data Integrity Assurance
- d. Password Provisioning

Answer: c.

Explanation: Cryptographic Data Integrity Assurance protects the central store data from being compromised while in transit to the agent.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 61

41. Which of the following Password Manager features pre-populates the central store with users' secondary credentials?

- a. Account Self-Service
- b. Automatic Key Recovery
- c. Cryptographic Data Integrity Assurance
- d. Password Provisioning

Answer: d.

Explanation: Password Provisioning pre-populates the central store with users' secondary credentials, ensuring that they do not have to provide their credentials to the agent when launching the application for the first time.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 61

42. The _?_ Service hosts the Password Manager Services.

- a. XTE
- b. XML
- c. IMA
- d. SMA

Answer: a.

Explanation: The XTE Service hosts the Password Manager Services.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 61

43. The Citrix Password Manager Service is run on a web server that uses _?_ to encrypt the data shared by the Citrix Password Manager Service, the console and the agent.

- a. TLS
- b. SSL
- c. RC5
- d. PGP

Visit Citrixexperience.com for more Citrix certification preparation products.

Answer: b.

Explanation: The Citrix Password Manager Service is run on a web server that uses SSL to encrypt the data shared by the Citrix Password Manager Service, the console and the agent.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 61

44. Which of the following are true in order to use the Password Manager Service? (Choose 3)

- a. TLS must be enabled
- b. A server certificate must be installed
- c. Root certificates must be used on all clients
- d. The certificate common name must match the FQDN of the server

Answer: b.c.d.

Explanation: A server authentication certificate must be installed on the server hosting the Password Manager Service to enable SSL configuration. The certificate common name needs to match the FQDN of the server running the Password Manager Service. An administrator must install the certificate in the local machine certificate store on the server running the Password Manager Service and install the trusted root certificate on all systems communicating with the Password Manager Service.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 61

45. Account Self-Service includes the following features: (Choose 2)

- a. Self-Service Password Reset
- b. Self-Service Password Unlock
- c. Self-Service Password Integrity
- d. Self-Service Password Recovery

Answer: a.b.

Explanation: Account Self-Service includes Self-Service Password Reset, which allows Password Manager users in an Active Directory environment to reset their primary domain passwords without the intervention of the Help Desk, and Self-Service Password Unlock, which works in the same way as Self-Service Password Reset to unlock domain accounts.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 62

46. Which of the following provides an additional layer of security to the Password Manager agent software by protecting against impersonation of unauthorized password changes?

- a. Account Self-Service
- b. Automatic Key Recovery
- c. Question-Based Authentication
- d. Password Expirations

Answer: c.

Explanation: Question-based authentication provides an additional layer of security to the Password Manager agent software by protecting against impersonation of unauthorized password changes. This security feature requires

Visit Citrixexperience.com for more Citrix certification preparation products.

that users answer questions in the questionnaire provided by the administrator when they first used the Password Manager agent and when password reset is used. The questionnaire is the same one as used for Account Self-Service.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 62

47. ___ allow(s) administrators to manage regular and transparent changes on applications that do not have password change functionality.
- Account Self-Service
 - Automatic Key Recovery
 - Question-Based Authentication
 - Password Expirations

Answer: d.

Explanation: Password Expirations allow administrators to manage regular and transparent changes on applications that do not have password change functionality.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 62

48. For Java applications, administrators can select the ___ option instead of the SendKeys option to configure the application definitions.
- Control ID
 - Hotkeys
 - Function
 - Scripts

Answer: a.

Explanation: For Java applications, administrators can select the Control ID option instead of the SendKeys option to configure the application definitions. The Control ID option provides visual cues, such as highlighting the selected field, during the configuration process.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 62

49. Scenario: You have been granted permission by the CTO of your company to extend the Active Directory schema so you can proceed in your Password Manager implementation. Which of the following steps will you take to extend the schema and verify its success? (Choose 4)
- Register the Active Directory Schema snap-in
 - Insert the Presentation Server 4.0 Components CD and click 'Prerequisite: Create your Central Store' on the opening screen
 - Click Active Directory > 'Extend your Active Directory Schema for the new directory objects'
 - Click the Classes node and verify Citrix-SSOConfig and citrix-SSOSecret
 - Click the Attributes node and verify citrix-SSOConfigData, citrix-SSOConfigType and citrix-SSOSecretData
 - Click the Users container and verify the CitrixSSO global group

Answer: a.c.d.e.

Explanation: To extend the Active Directory schema and verify it for your Password Manager implementation, first, register the Active Directory Schema

Visit Citrixexperience.com for more Citrix certification preparation products.

snap-in by running REGSVR32 SCHMMGMT.DLL in a command prompt. Type OK to the RegSvr32 message. Open an MMC and add the Active Directory Schema snap-in. Expand the Classes and Attributes nodes to verify there are no Citrix-related items (any item names that begin with 'citrix'). After verification, insert the Password Manager CD, and when the splash screen appears, click 'Prerequisite: Create your Central Store'. On the 'Prerequisite: Create your Central Store' screen, click Active Directory. On the 'Create your Central Store using Active Directory' screen, click 'Extend your Active directory schema for the new directory objects'. This option runs the CitrixSchemaPrep.EXE utility. Click Yes in the warning pop-up. Press Enter to continue. To verify success, open the Active Directory Schema in the MMC and click the Classes node, verifying that citrix-SSOConfig and citrix-SSOSecret were added, and click the Attributes node, verifying that citrix-SSOConfigData, citrix-SSOConfigType and citrix-SSOSecretData were added.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 171, 172

50. To create an Active Directory central store:
- Run SCHMMGMT.DLL
 - In the Password Manager CD installation window click 'Create your central store in the extended schema'
 - Run CitrixSchemaPrep.EXE
 - In the Presentation Server 4.0 Components CD installation window click 'Create your central store in the extended schema'

Answer: b.

Explanation: To create an Active Directory central store, click 'Create your central store in the extended schema'. Clicking this option runs the CtxDomainPrep.EXE utility that updates permissions of the domain root, allowing users to create the objects they need to use Citrix Password Manager. Click Yes in the warning pop-up. Press Enter to continue when prompted.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 173

51. To request and install a web certificate for a Password Manager server: (Choose 4)
- Connect to the Certificate Authority
 - Specify the FQDN of the server running the Password Manager Service
 - Specify the FQDN of the server hosting the central store
 - Save the certificate to the local store
 - Select the option to install the certificate

Answer: a.b.d.e.

Explanation: To request and install a web certificate for a Password Manager server, connect to the Certificate Authority in Internet Explorer by browsing to <http://<ServerName>/certsrv> (Replace <ServerName> with the name of the server running the Certificate Authority). Click 'Request a certificate'. Click 'advanced certificate request'. Click 'Create and submit a request to this CA'. Click Web Server from the Certificate Template drop-down list. Type the FQDN of the

Visit Citrixexperience.com for more Citrix certification preparation products.

server running the Password Manager Service. Verify that 1024 is selected in the Key Size field. Select 'Store certificate in the local computer certificate store'. Click Submit to generate the server certificate. Click Yes in the Potential Scripting Violation warning. Click 'Install this certificate'. Click Yes in the Potential Scripting Violation warning. Close Internet Explorer when the Certificate Installed screen appears.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 66, 174

52. To verify that a server certificate is installed correctly:
- Use Internet Information Services Manager
 - Use Access Suite Console
 - Use Microsoft Management Console
 - Use Presentation Server Console

Answer: c.

Explanation: To verify that a server certificate is installed correctly, open the Microsoft Management Console and add the Certificates snap-in. Expand the Certificates node, expand the Personal node, click Certificates and confirm that the Password Manager FQDN is listed. Double-click the certificate and confirm that no errors appear, the 'Issued to' information is correct, the 'Valid dates' are correct and a message states that a private key corresponds to this certificate. Click the Certification Path tab and confirm that the FQDN path is correct and click OK. Expand the Trusted Root Certificate Authorities node. Click Certificates. Double-click Enterprise, confirm that there is no private key message and click OK. Close the MMC.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 66, 175

53. Scenario: Your IT group's recommendation of key recovery, account self-service and password provisioning has been accepted by the CTO and CEO of your company. Cryptographic Data Integrity Assurance was rejected, as they didn't feel it is essential at this time. You plan to use Active Directory for the central store. Which of the following are steps to integrate Password Manager with desired features? (Choose 9)
- Install the Password Manager Service
 - Enable Key Management
 - Enable Data Integrity
 - Enable Account Self-Service
 - Enable Provisioning
 - Select the correct server certificate
 - Select the Network Service System account credentials
 - Select the certificate expiration
 - Use Active Directory as the central store
 - Specify credentials for data proxy and self-service

Answer: a.b.d.e.f.g.h.i.j.

Visit Citrixexperience.com for more Citrix certification preparation products.

Explanation: To install Password Manager with Key Management, Account Self-Service and Password Provisioning, insert the Password Manager CD and on the Welcome screen, click Advanced Installation Tasks. On the Advanced Installation Tasks screen, click Install Citrix Password Manager Service. Citrix Password Manager Service Setup launches. Click Next on the Welcome screen. Accept the agreement on the License Agreement screen and click Next. On the Select Modules screen, verify Key Management and Account Self-Service are already chosen for installation and click Provisioning and select 'Entire feature will be installed on local hard drive'. Verify Data Integrity is not chosen for installation. Click Next. On the 'Ready to Install the Application' screen, click Install. After installation, click Finish. A configuration wizard launches after Password Manager Service installation finishes. Click Next on the Welcome screen. Verify the correct FQDN is selected in the 'Select local SSL certificate' drop-down list. Click NT Authority\Network Service from the 'System account' drop-down list and click Next. In the 'Create signing certificate' screen, select the certificate expiration and click Next. Click Active Directory, click the correct FQDN from the drop-down list and click Next. Type your user name in the 'User name' field, type your password in the Password field and type the domain in the Domain field. Click Next. If desired, configure the 'Configure data proxy' and click Next. For data proxy and self-service authentication, type your user name in the 'User name' field and your password in the Password field. Click Next. Click Finish. Click Finish in the 'Applying Settings' screen.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 68, 176, 177

54. To install and configure the Password Manager console: (Choose 2)
- On the Citrix Password Manager Main Menu, select Advanced Installation Tasks and on the Advanced Installation Tasks screen, select Citrix Password Manager Console
 - On the Citrix Password Manager Main Menu, select Installation Menu and on the Installation Menu screen, select Citrix Password Manager Console
 - Open the Access Suite Console, select the FQDN in the Active Directory drop-down list
 - Open the Presentation Server Console, select the FQDN in the Active Directory drop-down list

Answer: b.c.

Explanation: To install the Password Manager console, insert the Password Manager CD and if the Password Manager Main Menu doesn't launch, double-click on AUTORUN.EXE in the CD folder. On the Main Menu, select Installation Menu. On the Installation Menu, select Citrix Password Manager Console. Citrix Password Manager Console Setup launches. Click Next on the Welcome screen. Accept the agreement in the License Agreement screen and click next. Select the components you would like to install (the choices are Console, Application Definition Tool, Citrix Access Suite - Licensing, and Citrix Access Suite - Diagnostics) and click Next on the Install Type screen. Click Next on the 'Ready to Install the Application' screen. After installation, click Finish. To configure the

Visit Citrixexperience.com for more Citrix certification preparation products.

Password Manager console, open the Access Suite Console. Launch the 'Configure and run discovery' wizard from Common Tasks of the farm node. Click Next on the Welcome screen. Click Next in the Select Components screen. In the Identify Central Store page, choose among Active Directory, NTFS Network Share and Novell Shared Folder. Select and configure the appropriate choice and click Next. Choose whether or not to configure Data Integrity in the Configure Data Integrity Options screen and click Next (Data Integrity must have been chosen upon installation to configure this option). Click Next in the Preview Discover screen. Click Finish when discover is complete.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 70, 178, 179

55. Scenario: You are tasked with configuring identity verification for the users in your enterprise. You must create two custom questions and choose two default questions for a total of four questions to ask the users. The users must choose two of the questions for use with key recovery. The users' answers must be at least five characters in length and are not case sensitive. Which of the following are some of the tasks you will complete to accomplish this assignment? (Choose 5)
- Expand the Key Recovery node in the Access Suite Console and click Question-Based Authentication
 - Expand the Identity Verification node in the Access Suite Console and click Question-Based Authentication
 - Click 'Create questionnaire' in Common Tasks
 - Click 'Manage questions' in Common Tasks
 - In the list box in the left pane of the configuration window, choose Security Questions and click Add Question
 - In the list box in the left pane of the configuration window, choose Questionnaire and click Add Question
 - In the list box in the left pane of the configuration window, choose Security Questions and click Add to add as many security questions as you desire
 - In the list box in the left pane of the configuration window, choose Questionnaire and click Add to add as many security questions as you desire
 - In the list box in the left pane of the configuration window, choose Questionnaire and check two default questions and two custom questions that you want to allow the users to choose from
 - In the list box in the left pane of the configuration window, choose Key Recovery and check two default questions and two custom questions that you want to allow the users to choose from

Answer: b.d.e.h.j.

Explanation: To configure identity verification for the scenario in this question, under the Password Manager node expand the Identity Verification node in the Access Suite Console and click Question-Based Authentication. Click 'Manage questions' in Common Tasks. The Manage Questions configuration window launches. In the list box in the left pane of the Manage Questions window,

Visit Citrixexperience.com for more Citrix certification preparation products.

Question-Based Authentication will already be chosen. In the right pane, choose the default language and check the 'Perform backwards compatibility check' if desired. In the list box in the left pane, choose Security Questions and click Add Question in the right pane. Create a question, type 5 in the Characters box and leave 'Answer is case sensitive' unchecked. Repeat for your second question. In the list box in the left pane, choose Questionnaire and click Add to add the security questions that you want to allow the users to choose from. In the list box in the left pane, choose Key Recovery and check two default questions and two custom questions that you want to allow the users to choose from. To verify what questions the users will be allowed to choose from, click Security Questions in the list box and Yes should be in the In Use column next to each desired question.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 72, 73, 180, 181

56. To create a password policy: (Choose 9)
- a. Create a new policy in the Password Policies node of the Access Suite Console
 - b. Create a new policy in the Policies node of the Presentation Server Console
 - c. Name the password policy
 - d. Configure the syntax rules and password history rule
 - e. Configure the numeric character rules
 - f. Configure the special character rules
 - g. Configure logon preferences
 - h. Configure password expiration options
 - i. Define the Agent Password wizard options
 - j. Confirm the settings

Answer: a.c.d.e.f.g.h.i.j.

Explanation: To create a password policy for Password Manager, click 'Create a new password policy' in Common Tasks in the Password Policies node of the Access Suite Console. The Password Policy Wizard launches. On the 'Name the password policy' screen, type a name and description for the policy and click Next. On the 'Set basic password rules' screen, configure the syntax rules, which include 'Alphabet case usage', 'Minimum password length', 'Maximum password length', 'Number of times a single character can be repeated' and 'Number of times a character can be repeated sequentially'. Also on the 'Set basic password rules' screen, check 'New password must not be the same as previous password' if desired. Click Next. On the 'Set numeric character rules' screen, configure whether to allow numeric characters in a password, whether the numeric characters can be the first or last character of the password, the minimum number of numeric characters required and the maximum number of numeric characters allowed. On the 'Set special character rules' screen, configure whether to allow special characters in a password, whether the special characters can be the first or last character of the password, the minimum number of special characters required and the maximum number of special characters allowed. Also on this

Visit Citrixexperience.com for more Citrix certification preparation products.

screen, type the allowed special characters in the 'Allowed special characters list'. The special characters allowed by default are: !@#\$%^&*()-_+=[]\|,?. Click Next. On the 'Establish logon preferences' screen, configure whether to allow users to reveal passwords for applications or whether to force users to re-authenticate before submitting application credentials. Also on this screen, configure 'Number of logon retries' and 'Time limit for logon retries'. Click Next. On the 'Set password expiration options' screen, decide whether to use the password expiration settings associated with the application definitions, and if so, configure 'Number of days until password expires' and 'Number of days to warn users before password expires'. On the 'Define Password wizard' screen, choose from the following to select how you want new passwords to be generated and submitted to the application: 'User prompted for action', 'User-created only', 'User-created with system-generated option', 'System-generated, user informed', 'System-generated with user-created option', 'System-generated, silent'. Click Next. Confirm the settings and click Finish.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 74-76 and 182-184

57. Which of the following types of applications can an application definition be created for? (Choose 4)
- Windows
 - Java
 - Host
 - Streaming
 - Web

Answer: a.b.c.e.

Explanation: Application definitions can be created for Windows, Java, host/mainframe and web applications. On the Create Application Definition screen, there are three choices: Windows, Web and Host/Mainframe. To create an application definition for a Java application, choose Windows.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 185-193

58. To create an application definition:
- Right-click the published application under the Applications node of the Presentation Server Console and select Create Application Definition
 - Right-click the Applications node of the Presentation Server Console and choose Properties. In Properties, choose the published application in the left pane and click 'Create Application Definition' in the right pane
 - Right-click the Application Definition node of the Presentation Server Console and select Create Application Definition
 - Click 'Create application definition' in Common Tasks in the Application Definition node of the Access Suite Console

Answer: d.

Explanation: To create an application definition, click 'Create application definition' in Common Tasks in the Application Definition node of the Access

Visit Citrixexperience.com for more Citrix certification preparation products.

Suite Console. The Create Application Definition window launches. Choose among Windows, Web and Host/Mainframe for the application type and then choose between 'Create new' and 'Create from an application template'. Click Start Wizard. In the Application Definition Wizard, on the 'Identify application' screen, type a name and description for the application definition and click Next. On the 'Manage forms' screen, add and configure the application forms the agent software must recognize for submitting and changing user credentials. On this screen, click Add Form. The Add Form Wizard launches. In the Add Form Wizard, identify the form, select the field detection method (Send Keys or Control ID), set the field detection rules, configure whether the agent automatically submits credentials to the application or not, configure class information, control matching and initial delay information in the Advanced Settings and confirm all choices. Click Finish to exit the Add Form Wizard and return to the Application Definition Wizard. Name the custom fields on the 'Name custom field' screen and click Next. Use the default icon or specify a custom icon on the Specify Icon screen and click Next. On the Password Expiration screen, choose to run a script when the password expires and you can choose to use the Citrix Password Manager expiration warning. Click Next. Confirm the settings and click Finish. Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 77-80 and 185-193

59. To create a user configuration in Password Manager:
- a. In the Access Suite Console, click 'Add new user configuration' in Common Tasks of the User Configurations node
 - b. In the Presentation Server Console, right-click the User Configurations node and select 'Add new user configuration'
 - c. In the Presentation Server Console, click the User Configurations node in the right pane and click Add in the left pane
 - d. In the Access Suite Console, click 'Add new user configuration' in the Common Tasks of the Password Manager node

Answer: a.

Explanation: To create a user configuration in Password Manager, in the Access Suite Console, click 'Add new user configuration' in Common Tasks of the User Configurations node. The User Configuration Wizard launches. Type a name, description and data location for the user on the 'Name user configuration' screen and click Next. Add application groups in the 'Choose policies and applications' screen and click Next. Customize how the agent works for this user configuration in the 'Configure agent interaction' screen and click Next. Set the licensing model and licensing communication for this user configuration on the 'Configure licensing' screen and click Next. Set the method used to verify the user's identity and to retrieve the key for stored credentials on the 'Configure key management' screen and click Next. Select self-service features on the 'Enable self-service' screen and click Next. Provide the service location for the Key Management module on the 'Key management module' screen and click Next. Provide the service location for the Provisioning module on the 'Provisioning module' screen

Visit Citrixexperience.com for more Citrix certification preparation products.

and click Next. Confirm the settings on the 'Confirm settings' screen and click Finish.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 194, 195

60. To create a Password Manager agent installation image, click Installation Menu on the Main Menu of the Citrix Password Manager CD.
- True
 - False

Answer: b.

Explanation: To create a Password Manager agent installation image, click Advanced Installation Tasks on the Main Menu of the Citrix Password Manager CD. On the Advanced Installation Tasks menu, click Create Citrix Password Manager Agent Installation Image. Click Next on the Welcome screen that launches. Select a network installation point and click Next. Select the features that you want to install and click Next. Select the type of Central Store and click Next. Verify your selections and click Next to start the installation. Click Finish after the installation is complete.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 198

61. To enable Self-Service Password Reset on Web Interface, an administrator must do which of the following tasks? (Choose 4)
- Generate a Self-Service Password Reset Template
 - Publish LOGOFF.EXE
 - Create an ICA file
 - Update the Web Interface configuration file
 - Add the self-service password reset URL to the Web Interface site

Answer: b.c.d.e.

Explanation: To enable Self-Service Password Reset on Web Interface, an administrator must publish LOGOFF.EXE, found at c:\windows\system32. Next, she must create an ICA file for Account Self-Service and update the WEB.CONFIG file to add the ICA file name to the <appSettings> section. The World Wide Web Publishing Service must then be restarted for the changes to the Web Interface configuration file to take affect. A URL must be added to the Web Interface site by configuring 'Customize appearance for user' in Common Tasks of the Web Interface node.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 89-91 and 201-204

62. Which of the following steps must an administrator do to configure password provisioning?
- Create an ICA file
 - Create a provisioning template
 - Update the Web Interface configuration file
 - Publish LOGOFF.EXE

Answer: b.

Visit Citrixexperience.com for more Citrix certification preparation products.

Explanation: To configure password provisioning, an administrator must create and edit a provisioning template. To create a provisioning template, Click 'Generate provisioning template' in Common Tasks of a user configuration node in the Access Suite Console.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 205

#Building and Testing Access Gateway Advanced Edition

63. ? are the tools available on the network that users employ to help them accomplish tasks.
- a. Endpoint analysis scans
 - b. Filters
 - c. Resources
 - d. Policies

Answer: c.

Explanation: Resources are the tools available on the network that users employ to help them accomplish tasks. Access Gateway Advanced Edition provides the following types of resources: Web sites, web pages, web applications, portals, published applications, file shares, networks, subnets, servers, services, email and email synchronization. By default, a user cannot access resources until an administrator applies a policy that grants them access permissions through action controls.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 106

64. The following types of resources can be provided through Access Gateway Advanced Edition: (Choose 12)
- a. Web sites
 - b. Web pages
 - c. Web applications
 - d. Portals
 - e. Published applications
 - f. File shares
 - g. Networks
 - h. Subnets
 - i. Servers
 - j. Active Directory
 - k. Services
 - l. Email
 - m. Email synchronization

Answer: a.b.c.d.e.f.g.h.i.k.l.m.

Explanation: Access Gateway Advanced Edition provides the following types of resources: Web sites, web pages, web applications, portals, published applications, file shares, networks, subnets, servers, services, email and email synchronization.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 106

65. ___ verify whether or not a client device meets the minimum requirements necessary to access the logon page in an access server farm.
- Endpoint analysis scans
 - Filters
 - Resources
 - Policies

Answer: a.

Explanation: Endpoint analysis scans verify whether or not a client device meets the minimum requirements necessary to access the logon page in an access server farm. This scan is performed before the user sees the logon page. Endpoint analysis scans are specified in logon points and access policies, control access to the logon page, control access to resources, are configured to run only when specific conditions exist on the client device and require the use of an endpoint analysis scan client on the client device.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 107

66. ___ identify when a client device meets the criteria necessary to gain access to an access server farm.
- Endpoint analysis scans
 - Filters
 - Resources
 - Policies

Answer: b.

Explanation: Access policies use filters to identify when a client device meets the criteria necessary to access resources in an access server farm. Filters check to see whether a condition is true or not.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 107, 108

67. ___ control access to all resources in the access server farm by using filters to define the conditions.
- Endpoint analysis scans
 - Continuous analysis scans
 - Web Interface servers
 - Policies

Answer: d.

Explanation: Policies control access to all resources in the access server farm by using filters to define the conditions that decide when a policy should be applied.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 108

68. Scenario: Your company desires to make internal corporate resources available to internal and external users. To meet this requirement, you are charged with installing and configuring Access Gateway Advanced Edition. Which of the following are steps you will take to install and configure Access Gateway Advanced Edition? (Choose 4)

Visit Citrixexperience.com for more Citrix certification preparation products.

- a. Before installing Access Gateway Advanced Edition, run Discovery in the Access Suite Console
- b. Insert the Access Gateway Access Control Option CD and on the Welcome screen, click Product Installations. On the Product Installations screen, click Advanced Access Control
- c. Insert the Citrix Access Gateway 4.2 CD and on the Welcome screen, click Product Installations. On the Product Installations screen, click Advanced Access Control
- d. Ensure that Run Server Configuration is selected and click Finish
- e. Unselect Run Server Configuration and click Finish
- f. After installing, but before configuring Access Gateway Advanced Edition, run Discovery in the Access Suite Console
- g. Select 'Create a new access server farm' and enter user credentials
- h. Select 'Create a new access server farm' and enter administrator credentials
- i. After installing and configuring Access Gateway Advanced Edition, run Discovery in the Access Suite Console

Answer: b.d.h.i.

Explanation: To install and configure Access Gateway Advanced Edition, insert the Access Gateway Access Control Option CD. The Welcome screen will launch. On the Welcome screen, click Product Installations and on the Product Installations screen, click Advanced Access Control. Click Next on the Welcome screen. Read the License Agreement, click 'I accept the license agreement' and click Next. Click Next to install all components. Click OK in the warning message. Click Next to begin the installation. Click OK in the Advanced Access Control Installation dialog box. Verify the selected options are displayed in the Start Installation Screen and click Next. Ensure that Run Server Configuration is selected and click Finish. The Advanced Access Control Server Configuration wizard will launch. Select 'Create a new access server farm'. Click Next. Use administrator credentials for the service account and click Next. Choose the database to use (Microsoft SQL or Microsoft SQL Server Database Engine) and click Next. Verify that 'I would like to use an existing license server' is selected, type the name of the license server in the Host name field and click Next. Verify that the correct options are selected (Choose from Agent Server, Web Server and HTML Preview) and click Next. Click Next to use C:\INETPUB\WWWROOT as the default site path. Verify the information in the 'Ready to Configure' screen and click Next. Click Finish. After installation and configuration is finished, run Discover in the Access Suite Console.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 219, 220

69. Run the following file to install the Access Suite Console 4.2 update:
- a. ASC400W004.MSP
 - b. ASC400W004.MSI
 - c. ASC400W004.EXE
 - d. ASC400W004.ICA

Visit Citrixexperience.com for more Citrix certification preparation products.

Answer: a.

Explanation: Run ASC400W004.MSP to install the Access Suite Console 4.2 update. This must be done along with version 4.2 of Web Interface and Advanced Gateway with Advanced Access Control. For more information, see Citrix Knowledge Base article CTX108237.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 221

70. Which of the following would an administrator do to specify a Presentation Server farm to use with Access Gateway Advanced Edition? (Choose 2)
- In the Presentation Server Console, right-click on the farm node and choose Properties
 - In the Access Suite Console, click the access server farm node and click 'Edit farm properties' in Common Tasks
 - Choose Data Store Location in the properties window
 - Choose Presentation Server Farms in the properties window

Answer: b.d.

Explanation: To specify a Presentation Server farm to use with Access Gateway Advanced Edition, in the Access Suite Console, click the CitrixAAC node and click 'Edit farm properties' in Common Tasks. Click Presentation Server Farms in the properties window. Click New. Type the server farm name in the 'Citrix Presentation Server farm name' field. Click Next. Click Add to add a farm server. Type the farm server's name and click OK. Click Next. Click Finish in the Configure Address Mode screen. Click OK.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 222, 223

71. Event logging can be configured for Access Gateway Advanced Edition in the Presentation Server Console.
- True
 - False

Answer: b.

Explanation: To configure event logging for Access Gateway Advanced Edition, in the CitrixAAC node of the Access Suite Console, click 'Edit farm properties' in Common Tasks. Click Event Logging. Select the type of logging desired and click OK.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 223

72. To create a Web Interface 4.2 web site: (Choose 3)
- In the right pane of the Web Interface Admin Tool, click 'Create site'
 - In the Access Suite Console, expand Suite Components > Configuration Tools and click Web Interface. Click 'Create site' in Common Tasks
 - Click MetaFrame Presentation Server and click Next
 - Click Web Interface and click Next
 - Specify the IIS location
 - Specify the Advanced Access Gateway location

Answer: b.c.e.

Visit Citrixexperience.com for more Citrix certification preparation products.

Explanation: To create a Web Interface 4.2 web site, in the Access Suite Console, expand Suite Components > Configuration Tools and click Web Interface. Click 'Create site' in Common Tasks. The Create Site wizard launches. Click MetaFrame Presentation Server and click Next. Specify the IIS location and click Next. Specify the server farm and click Next. Confirm the information and click Next. After the new site is created, click Finish.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 224

73. Scenario: You must create a web resource for your Web Interface web site. The name of the web resource will be Web Interface 4.2 Site. The Web Interface web site is located on ASPServer01. Windows authentication will be used as the authentication type. Bypass Web proxy URL rewriting will not be used and access will be granted later. (Choose 2)
- Open the Access Suite Console and click the Resources node in the Web Interface node
 - Open the Access Suite Console and click the Resources node in the CitrixAAC node
 - Click 'Create Web resource' in Common Tasks
 - Click 'Create Access resource' in Common Tasks

Answer: b.c.

Explanation: To create a web resource for a Web Interface web site, open the Access Suite Console, expand the Resources node in the CitrixAAC node and click 'Create Web resource' in Common Tasks. The New Web Resource wizard launches. Type Web Interface 4.2 Site as the name and type a description of the new web resource and click Next. In the Configure Addresses screen, click New and type http://ASPServer01/Citrix/CitrixAAC in the URL field. Select 'Citrix Web Interface 4.2 or later' from the 'Application type' drop-down list. Select 'Integrated Windows authentication' and click OK. Select Publish for users in their list of resources. Type http://ASPServer01/Citrix/CitrixAAC/Default/login.aspx in the 'Home page' field. Verify that 'Bypass Web proxy URL rewriting' and 'Use the interface that is common for all browser types' are deselected and click Next. Verify that 'I will create a policy to grant access later' is selected and click Finish.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 225

74. To create a resource for access through Access Gateway Advanced Edition:
- Expand the CitrixAAC node in the Access Suite Console, right-click the Resources node and select the desired resource to create in the pop-up menu
 - Expand the CitrixAAC node in the Access Suite Console, expand the Resources node and click the desired resource node
 - Expand the Web Interface node in the Access Suite Console, expand the desired web site node, expand the Resources node and click the desired resource node

Visit Citrixexperience.com for more Citrix certification preparation products.

- d. Expand the Web Interface node in the Access Suite Console, expand the desired web site node, right-click the Resources node and select the desired resource to create in the pop-up menu

Answer: b.

Explanation: To create a resource for access through Access Gateway Advanced Edition, expand the CitrixAAC node in the Access Suite Console, expand the Resources node and click the desired resource node. Click to the link in Common Tasks to create the resource using the wizard.

Source: Field Experience

75. To create the default logon point for an Access Gateway Advanced Edition

deployment: (Choose 3)

- a. Expand the CitrixAAC node in the Access Suite Console and expand the Logon Point node
- b. Expand the Web Interface node in the Access Suite Console and expand the Logon Point node
- c. Click the SampleLogonPoint node and click 'Edit logon point' in Common Tasks
- d. Click the DefaultLogonPoint node and click 'Edit logon point' in Common Tasks
- e. Click Authentication in the left pane of Logon Point Properties
- f. Click Presentation Server Farms in the left pane of Logon Point Properties

Answer: a.c.f.

Explanation: To create the default logon point for an Access Gateway Advanced Edition deployment, expand the CitrixAAC node in the Access Suite Console and expand the Logon Point node. Click the SampleLogonPoint node and click 'Edit logon point' in Common Tasks. Click Presentation Server Farms in the left pane of Logon Point Properties. Add the appropriate server farm and click OK.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 229, 230

76. To delete the default logon point policy from an Access Gateway Advanced Edition deployment: (Choose 2)

- a. Expand the CitrixAAC node in the Access Suite Console and click the Logon Point node
- b. Expand the CitrixAAC node in the Access Suite Console and click the Policies node
- c. Right-click 'Default Logon Policy for: DefaultLogonPoint' in the right pane and choose 'Delete policy'
- d. Right-click 'Default Logon Policy for: SampleLogonPoint' in the right pane and choose 'Delete policy'

Answer: b.d.

Explanation: To delete the default logon point policy from an Access Gateway Advanced Edition deployment, expand the CitrixAAC node in the Access Suite Console and click the Policies node. Right-click 'Default Logon Policy for: SampleLogonPoint' in the right pane and choose 'Delete policy'. Click Yes.

Visit Citrixexperience.com for more Citrix certification preparation products.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 230

77. When configuring a new web resource, which of the following application types can be chosen? (Choose 5)
- Citrix Web Interface 4.2 or later
 - NFuse 1.51
 - Share Point
 - Share Point with Web Interface Web Part
 - Web Application
 - Web Application (requires session cookies)

Answer: a.c.d.e.f.

Explanation: When configuring a new web resource, in the New URL pop-up screen, choose 'Citrix Web Interface 4.2 or later', Share Point, 'Share Point with Web Interface Web Part', Web Application or 'Web Application (requires session cookies)' in the Application Type drop-down list.

Source: Field Experience

78. Scenario: You must create a file share resource named Home Directory using My H: Drive as the display name. Use the Users share on the FSServer01 server. Publish the resource for the CitrixUsers group in the list of published applications. Create a policy to grant access later. (Choose 3)

- Expand the Resources node in the Access Suite Console, click the Directories node and click 'Create file share' in Common Tasks
- Expand the Resources node in the Access Suite Console, click the File Shares node and click 'Create file share' in Common Tasks
- Type My H: Drive in the 'File share name' field
- Type Home Directory in the 'Display name' field
- Type \\FSServer01\Users\#<username> in the 'File share location' field
- Select 'Publish for users in their list of published resources'
- Select 'Create a default policy granting access to all users'

Answer: b.e.f.

Explanation: To create this file share, expand the Resources node in the Access Suite Console, click the File Shares node and click 'Create file share' in Common Tasks. The New File Share wizard launches. Type Home Directory as the file share name, type a description if desired and click Next. Click New. Type My H: Drive as the display name. Type \\FSServer01\Users\#<username> in the 'File share location' field. Select 'Publish for users in their list of published resources'. Click OK. Click Next. Verify that 'I will create a policy to grant access later' is selected and click Finish.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 228

79. In the Access Suite Console, what is the name of the node you click to configure the default logon point?
- DefaultLogonPoint
 - InstanceLogonPoint
 - SampleLogonPoint

Visit Citrixexperience.com for more Citrix certification preparation products.

d. TemplateLogonPoint

Answer: c.

Explanation: To configure the default logon point, in the Access Suite Console, under the CitrixAAC node, expand the Logon Points node and click the SampleLogonPoint node. Click Presentation Server Farms. Select the desired Presentation Server Farm and click Add. Click OK.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 229, 230

80. When you right-click on an access or connection policy in the Policies node under the CitrixAAC node of the Access Suite Console, which of the following options do you get? (Choose 4)
- Edit
 - Delete
 - Copy
 - Refresh
 - Properties

Answer: a.b.c.d.

Explanation: You may edit, delete, copy or refresh the access and connection policies in the Policy node by right-clicking on them.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 230

81. Scenario: Your assignment is to create an access policy for the default logon point named SampleLogonPoint. The policy will apply to web resources and file shares and must allow logon. All resource settings must be allowed, except Live Edit. A typical filter must be created for this policy. The filter should apply when RSA authentication is used. The policy should be applied to all authenticated users. (Choose 8)

- Click the Policies node in the Access Suite Console
- Click the Policies node in the Presentation Server Console
- Click 'Create access policy' in the right pane of the Presentation Server Console
- Click 'Create access policy' in Common Tasks
- Select Web Resources, File Shares and Allow Logon
- Select Network Resources, File Shares and Allow Logon
- Right-click Live Edit under Allow Logon and select Deny
- Right-click Live Edit under File Shares and select Deny
- Select 'No filter' and click Next
- Click New to create a filter
- Select 'Create a typical filter'
- Select 'Create a custom filter'
- Verify 'Do not filter by authentication' is selected
- Select 'RSA or SafeWord'
- Select 'Apply this policy to all authenticated users'
- Select the Users group from Active Directory

Answer: a.d.e.h.j.k.n.o.

Visit Citrixexperience.com for more Citrix certification preparation products.

Explanation: To create the access policy for SampleLogonPoint as described in the scenario, click the Policies node in the Access Suite Console. Click 'Create access policy' in Common Tasks. The New Access Policy Wizard launches. Type SampleLogonPoint as the policy name and click Next. Select Web Resources, File Shares and Allow Logon. Click Next. Right-click Web Resources and click Allow All. Right-click File Shares and click Allow All. Right Click Live Edit under file shares and click Deny. Right-click Allow Logon and click Allow All. Click Next. Click New to create a filter. The New Filter wizard launches. Type SampleLogonPoint as the filter name. Click Next. Select 'Create a typical filter' and click Next. Select SampleLogonPoint and click Add. Click Next. Select 'RSA or SafeWord' and click Next. Click Next in the Select Endpoint Analysis Outputs screen. Click Finish to close the New Filter wizard. Click Next in the Select Filter screen of the New Access Policy Wizard. Select 'Apply this policy to all authenticated users'. Click Finish.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 230, 231

82. To use a data set in an endpoint analysis scan, save the data set as a(n) file.
- DAT
 - ICA
 - TXT
 - CSV

Answer: d.

Explanation: To use a data set, such as MAC addresses, in an endpoint analysis scan, add the data to a file in comma-separated form and save the data as a CSV file. The file can then be chosen while creating an endpoint analysis scan.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 233

83. Which of the following are the default scan groups in the Endpoint Analysis Scan node? (Choose 7)
- Antivirus
 - Browser
 - Custom
 - Firewall
 - Machine Identification
 - Miscellaneous
 - Network
 - Operating System

Answer: a.b.c.d.e.f.h.

Explanation: In the Access Suite Console, under the CitrixAAC node, expand the Endpoint Analysis Scan node and you will see the default scan groups: Antivirus, Browser, Custom, Firewall, Machine Identification, Miscellaneous and Operating System. To create an Endpoint Analysis Scan, expand one of the scan groups and click on one of the scans below. Click 'Create scan' in Common Tasks and configure the endpoint analysis scan.

Source: Field Experience

84. Two ways to create an endpoint analysis scan are: (Choose 2)
- Right-click the Endpoint Analysis node and select 'Create scan'
 - Click the Endpoint Analysis node and choose 'Create scan' in Common Tasks
 - Click the scan group node under the Endpoint Analysis node and choose 'Create scan' in Common Tasks
 - Expand the Endpoint Analysis node, expand the desired scan group node, click the desired scan package and click 'Create scan' in Common Tasks
 - Expand the Endpoint Analysis node, expand the desired scan group node, right-click the desired scan package node and select 'Create scan'

Answer: d.e.

Explanation: To create an endpoint analysis scan, in the Access Suite Console, expand the CitrixAAC node, expand the Endpoint Analysis node, expand the desired scan group node, click the desired scan package and click 'Create scan' in Common Tasks or right-click the desired scan package node and select 'Create scan'. The Create Scan wizard launches. Type a name for the scan and click Next. Select the conditions of the scan (Client Device Regional Locale and/or Logon Point) and click Next. Type the rule name and click Next. Select the operating systems that the scan package will scan and click Next. If Client Device Regional Locale was selected earlier, choose the languages to use and click Next. Select the logon point and click Next. Enter the property values that the scan will check on the client device and click Finish.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 234, 235

85. To add an endpoint analysis scan to a logon point: (Choose 2)
- Expand the Logon Points node
 - Expand the Endpoint Analysis node
 - Click 'Edit endpoint analysis' in Common Tasks
 - Click 'Edit logon point' in Common Tasks

Answer: a.d.

Explanation: To add an endpoint analysis scan to a logon point, in the Access Suite Console, expand the CitrixAAC node, expand the Logon Points node and click on the desired logon point under the Logon Points node. Click 'Edit logon point' in Common Tasks. The Logon Point Properties window launches. Select Visibility in the left pane. Click Endpoint Analysis Output. The 'Select an Endpoint analysis' window launches. Select the desired endpoint analysis in the window and click OK to close the 'Select an Endpoint analysis' window. Click OK to close the Logon Point Properties window.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 235

86. When creating a new logon point, during which step do you configure which display users will see after they logon?
- Select Home Page
 - Configure Workspace Control

Visit Citrixexperience.com for more Citrix certification preparation products.

- c. Select Session Settings
- d. Visibility

Answer: a.

Explanation: To configure a new logon point, click the Logon Points node under the CitrixAAC node in the Access Suite Console. Click 'Create logon point' in Common Tasks. The New Logon Point Wizard launches. The New Logon Point Wizard contains 10 steps to configure a new logon point. The second step is Select Home Page. This is the step where you configure which display users will see after they logon. The choices are: 'Display the default navigation page', 'Display the home page application with the highest display priority' and 'Display the selected access center'.

Source: Field Experience

87. When creating a new logon point, during which step do you configure to allow users to reconnect?
- a. Select Home Page
 - b. Configure Workspace Control
 - c. Select Session Settings
 - d. Visibility

Answer: b.

Explanation: To configure a new logon point, click the Logon Points node under the CitrixAAC node in the Access Suite Console. Click 'Create logon point' in Common Tasks. The New Logon Point Wizard launches. The New Logon Point Wizard contains 10 steps to configure a new logon point. The seventh step is Configure Workspace Control. This is the step where you configure to allow users to reconnect. The choices are: 'Enable users to configure which options display when they log on', 'Enable users to reconnect' and 'Enable users to configure which options display when they log off'.

Source: Field Experience

88. There are 10 steps involved in creating a new logon point. Which of the following are the 10 steps in the New Logon Point Wizard? (Choose 10)
- a. Define Logon Point
 - b. Select Home Page
 - c. Select Filters
 - d. Configure Authentication Strength
 - e. Select Users
 - f. Configure Group Authorization
 - g. Add Citrix Presentation Server Farms
 - h. Select Sound and Window Settings
 - i. Configure Workspace Control
 - j. Select Resources
 - k. Configure Clients
 - l. Select Session Settings
 - m. Visibility

Answer: a.b.d.f.g.h.i.k.l.m.

Visit Citrixexperience.com for more Citrix certification preparation products.

Explanation: To create a new logon point, click the Logon Points node under the CitrixAAC node in the Access Suite Console. Click 'Create logon point' in Common Tasks. The New Logon Point Wizard launches. The New Logon Point Wizard contains 10 steps to configure a new logon point. The steps, in order, are: Define Logon Point, Select Home Page, Configure Authentication Strength, Configure Group Authorization, Add Citrix Presentation Server Farms, Select Sound and Window Settings, Configure Workspace Control, Configure Clients, Select Session Settings and Visibility.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 239

89. Which of the following consoles is used to deploy a new logon point to a server?
- Access Suite Console
 - Presentation Server Console
 - Server Configuration
 - Logon Point Configuration

Answer: c.

Explanation: To deploy a new logon point to a server, click Start > All Programs > Citrix > Access Gateway > Server Configuration. The Server Configuration tool (also called the Advanced Access Control Configuration console) launches. Click Configured Logon Points in the left pane and select the desired logon point on the right. Click Deploy. Click OK to close the Server Configuration tool.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 240

90. Scenario: You need to give the sales group the URL to access their logon point from inside the secure network. The name of the server is AACServer01. The name of the logon point is SalesPortal. Which of the following URLs will the sales group use?
- <http://SalesPortal/citrixlogonpoint/AACServer01>
 - <http://citrixlogonpoint/AACServer01/SalesPortal>
 - <http://AACServer01/SalesPortal/citrixlogonpoint>
 - <http://AACServer01/citrixlogonpoint/SalesPortal>

Answer: d.

Explanation: For the sales group to access their logon point named SalesPortal on the server named AACServer01, they will need to use the URL

<http://AACServer01/citrixlogonpoint/SalesPortal>.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 242

91. Scenario: Your assignment is to use the Firefox Browser Filter to grant access to a published application named Record Store. The application is published in your Presentation Server Farm as RecordStore. Which of the following steps will you take for this configuration? (Choose 3)
- Expand the Filters node in the Access Suite Console
 - Expand the Applications node in the Presentation Server Console
 - Right-click the Firefox Browser Filter and select Properties
 - Right-click RecordStore and select Properties
 - Select Application in the Firefox Browser Filter Properties screen

Visit Citrixexperience.com for more Citrix certification preparation products.

f. Select Access Control in the RecordStore Properties screen

Answer: b.d.f.

Explanation: To use the Firefox Browser Filter to grant access to the published application RecordStore, expand the Applications node in the Presentation Server Console. Right-click RecordStore and select Properties. In the RecordStore Properties screen, select Access Control. Select 'Any connection that meets any of the following filters'. Click Add. Type CitrixAAC in the name of the MetaFrame Secure Access Manager farm. Type Firefox Browser Filter in the name of the MetaFrame Secure Access Manager filter. Click OK. Click OK in the RecordStore Properties screen. Click OK in the XML Trust Warning message.
Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Page 243

92. Scenario: You are assigned to use the Firefox Browser Filter to disable client drive mapping for Firefox users on the AppServer01 server. Which of the following steps will you take to start this configuration? (Choose 2)
- Click the Policies node in the Presentation Server Console
 - Click the Policies node in the Access Suite Console under the CitrixAAC node
 - Right-click Polices and click Create Policy
 - Click 'Create policy' in Common Tasks

Answer: a.c.

Explanation: To disable client drive mapping for Firefox users on AppServer01, click the Policies node in the Presentation Server Console. Right click Policies and click Create Policy. Type a name for the policy. Click OK. Double click the policy you just created. Expand Client Devices > Resources > Drives. Click Mappings. Click Enabled. Select 'Turn off Floppy disk drives'. Select 'Turn off Hard drives'. Click OK. Right-click Disable Client Drives and click 'Apply this policy to'. Click Access Control. Select 'Filter based on Access Control. Select 'Apply to connections made through MetaFrame Secure Access Manager'. Click 'Any connection that meets any of the following filters'. Click Add. Select CitrixAAC in the MetaFrame Secure Access Manager farm from the drop-down list. Select Firefox Browser Filter from the MetaFrame Secure Access Manager Filter drop-down list. Click OK. Click OK in the Disable Client Drives Policy Filters screen. Click OK in the XML Trust Warning message.

Source: CTX-1456AI Citrix Access Suite 4.0: Build/Test Workshop, Pages 243, 244