EnSurePass

Easy Test! Easy Pass!

Exam Code: 1Y0-306

Exam Name: Citrix Access Gateway 4.2 with Advanced Access Control Administration

Vendor: Citrix

Version: DEMO

Part: A

1: Where does an administrator configure the conditions that users must meet to be able to see the logon page?

A.In a filter

B.In a policy

C.In logon point properties

D.In the properties of an endpoint analysis scan

Correct Answers: C

2: Which two clients can be used to access published applications on Citrix Presentation Servers? (Choose two.)

A.Web Client

B.Client for Java

C.Live Edit Client

D.Secure Access Client

E.Endpoint Analysis Client

Correct Answers: A B

3: Scenario: An administrator wants to make documents from a defined file share open from a Citrix Presentation Server session. Which policy setting should be enabled for this purpose?

A.Live Edit

B.Download

C.HTML Preview

D.File type association

Correct Answers: D

4.Scenario: An adminstator gives a user the url

https://Accounting1.net/CitrixLogonPoint/AccountAccess to access a login page

"Accounting1.net" is the FQDN of the Advanced Access Control server hosting the logon point and "AccountAccess" is the name of the logon point.

From the URL given to the user, which access method will be used to obtain resources from the access server farm?

A.Default logon point

B.Secure Web Client

C.Browser-only access

D.Secure Access Client

Correct Answers: C

5: Along with Active Directory, which other two authentications could be implemented in order to provide Advanced Authentication? (Choose two.)

A.Smart Cards

B.LDAP authentication

C.RSA Security SecurID

D.Secure Computing SafeWord PremierAccess

Correct Answers: C D

6: Which two tools are used to configure RADIUS authorization for an Advanced Access Control implementation in a Windows domain? (Choose two.)

A.The Access Suite Console

B.The Server Configuration Wizard

C.The Access Gateway Administrator's Tool

D.The remote access policy in Microsoft Internet Authentication Service

Correct Answers: A D

7: When is the "Authentication Credentials" option used in the deployment of a logon point?

A.When RSA SecurID will be used along with the logon point

B.When the logon point is used to connect devices that are not secure

C.When a RADIUS or LDAP profile will be used along with the logon point

D.When the logon point is used by devices to access resources from a secure network over a connection that is not secure

Correct Answers: C

8: When a logon point is renamed just after it is deployed, __________. (Fill in the blank with a listed option.)

A.it can no longer be used

B.it must be redeployed using the update function in the Access Suite Console

C.the Advanced Access Control setup CD must be used to redeploy the updated logon

D.it must be redeployed using the update/refresh function in the Server Configuration Wizard before users can begin using the logon point to access resources

Correct Answers: D

9: An administrator is creating logon points and needs to configure the session settings. What is true about the configuration of session settings for logon points?

A.Session time-out is set by default to 30 minutes.

B.Domain prompting is used to determine whether the domain is available for access.

C.Secure Access Client (VPN) time-out should always be longer than session time-out.

D.Published application usage through the web browser may require an increase in VPN client time-out.

Correct Answers: C

10: An administrator needs to make a change to the default logon point settings for an Advanced Access Control implementation. Where can the administrator locate the default logon point?

A.In the IIS Manager Console

B.In the Access Suite Console

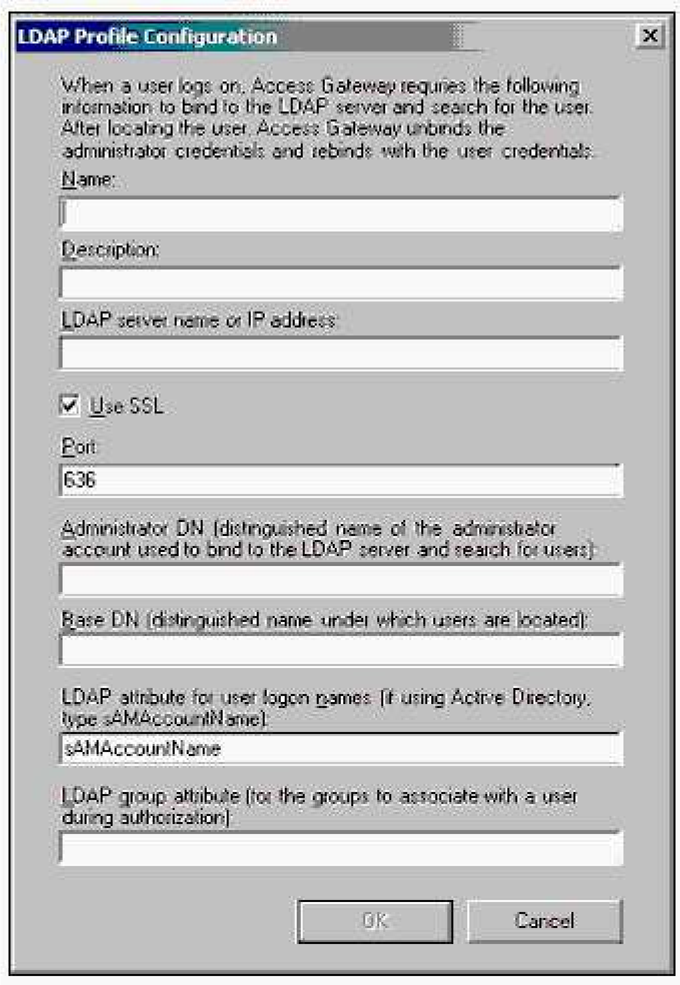
C.In the Access Gateway Administration Tool

D.In the Access Gateway Administration Portal

Correct Answers: B

11: An administrator configuring advanced authentication decides to use an index database with Global Catalog in order to improve the speed of LDAP queries. The administrator is instructed to use Microsoft port number 3268.

What should the administrator do in the "LDAP Profile Configuration" to implement this configuration? (Click on the exhibit button to display the screen shot.)



When a user logs on, Access Gateway requires the following information to bind to the LDAP server and search for the user. After locating the user, Access Gateway unbinds the administrator credentials and rebinds with the user credentials.

Name:

Description:

LDAP server name or IP address:

☑ Use SSL

Port: 636

Administrator DN (distinguished name of the administrator account used to bind to the LDAP server and search for users):

Base DN (distinguished name under which users are located):

LDAP attribute for user logon names (If using Active Directory, type sAMAccountName): sAMAccountName

LDAP group attribute (for the groups to associate with a user during authorization):

A.Type "3268" in the "Port" field and deselect "Use SSL".

B.Type "3268" in the "Port" field and leave "Use SSL" selected.

C.Type "3268" in the "Port" field and in the name field for the "Administrator Bind DN" and the "Base Bind DN".

D.Type "3268" in the "Port" field and type ":3268" after the IP address in the "LDAP Server Name or IP Address" field.

Correct Answers: A

12: How can an administrator control whether users are allowed or denied logon privileges through policies?

A.Include the Allow Logon property in the access filter

B.Include the Allow Logon property in the access policy

C.Include the Allow Logon Resource in the access filter

D.Include the Allow Logon Resource in the access policy

Correct Answers: D

13: Which type of filter should an administrator create, if a filter that specifies a particular NOT logic condition must exist in order for access to be granted?
A.Typical Filter
B.Custom Filter
C.Negative Filter
D.Exclusion Filter
Correct Answers: B

14: In the Access Suite Console, which steps must an administrator take to create an access policy that controls access to all visible servers and services in the network?
A.Select "Network Resources" and choose "Entire Network."
B.Select the farm node and disable network policy enforcement.
C.Select the Access Policies node in the console tree and add all visible servers and services to the access policy.
D.Select the appropriate domain from the domain list and choose to make the access policy the default authentication for that domain.
Correct Answers: A

15: What are two required steps for creating a typical filter that would require users to logon using a specific URL and their client devices to be running a specific anti-virus software? (Choose two.)

A.Choose to filter based on logon points
B.Run the Create Filter Wizard from the logon point
C.Choose to filter based on endpoint analysis scan results
D.Combine logon points and endpoint analysis results with the OR logical operator
Correct Answers: A C
16: What is the name of the policy setting that can be applied to a network resource?
A.Access
B.Download
C.File Type Association
D.Network Authentication
Correct Answers: A

17: Scenario: You are in the process of deploying Advanced Access Control in your company's IT environment. The corporate IT policy requires that all users have access to the company's employee portal website, but only the sales team has access to their web-based CRM application.
Which configurations best meet the requirements of the described environment?
A.Create a single web resource and add the URL for both the employee portal and the CRM application. Create a single access policy and grant only the sale team access to the CRM application.
B.Create two separate web resources; one for the employee portal and one for the CRM application. Create a single access policy and deny all non-sales team employees access to the

CRM application.

C.Create two separate web resources; one for the employee portal and one for the CRM application. Create two separate policies; include the employee portal in one and include the CRM application in the second. Add a filter to the CRM policy that denies all non-sales team employees access.

D.Create two separate web resources; once for the employee portal and one for the CRM application. Create two separate policies; include the employee portal in one and include the CRM application in the second. Grant everyone access to the employee portal policy and only the sales team access to the CRM application policy.

Correct Answers: D

18: Which connection setting should be enabled during a connection policy configuration to ensure automatic drive mapping on client devices using a Windows logon script?

A.Select file shares

B.Execute logon scripts

C.Execute automatic drive mapping

D.Enable pass-through authentication

Correct Answers: B

19: Which two steps must be taken when creating a typical filter? (Choose two.)

A.Construct a logical expression

B.Select an authentication profile

C.Provide a unique name for the filter

D.Select endpoint analysis scan output

E.Choose at least one condition to be included in the filter

F.Enter SSL client certificate requirements will be used to filter access

Correct Answers: C E

20: Which two settings(action controls) should be enabled to allow users to open and edit documents on servers using published resources in server farms running Presentation Server? (Choose two.)

A.Access

B.Live Edit

C.Download

D.File Type Association

Correct Answers: A D